

#####  
#  
# THE TELEGRAMS CARDING INDEX WITH MANY TUTORIALS #  
#  
#####

WELCOME TO THE MOST IMPORTANT STARTER CARDING E-BOOK ON TELEGRAM  
FOR SURE HERE ARE OLD AND NEW POSTS AND TUTORIALS COMBINED  
I HAVE CREATED AN ALL IN ONE INDEX E-BOOK FOR CARDING  
ALL VIPERZCREW CARDING GUIDES ARE INSIDE OF THIS  
AND ALL TUTORIALS, POSTS, LISTS OF NON VBV BINS, CHECKS BEFORE CARDING,  
WEBSITES, METHODS, ANONYMOUS GUIDES.

CREATED BY @THEMASTERCH OR @MRBLACKX  
RELATED BY T.ME/VIPERZCREW AND T.ME/REBL0X3R

THANKS TO : CARDING FORUMS, CARDERLOUNGES, PDFs , VIPERZCREW  
SPECIAL FRIENDS, SOME SPECIAL GROUPS, DAVICGTECH AND FINALLY AMDOLLAR

# INDEX

**WHAT IS CARDING**

**STAY SAFE WHILE CARDING**

**HOW TO KNOW WHAT IS BRAND OF CREDITCARD**

**HOW TO CHECK CREDITCARD BALANCE (SKYPE METHOD)**

**WHAT IS A PROXY AND WHAT ARE THEIR ANONYMITY LEVELS  
TYPES OF CARDS**

**2020 ANDROID CARDING OPSEC SETUP**

**CARDING - SETUP WINDOWS FOR CARDING**

**HOW TO ACCESS DEEPWEB FOR BUYING ANYTHING**

**WHERE CAN I BUY SOCKS**

**HOW TO CHECKS SOCKS**

**HOW TO CHECK IF YOU ARE CLEAN**

**ZIP CODE SEARCH**

**SEND FAX ONLINE**

**CREDIT REPORTS**

**PHONE REDIRECTS**

**USA PHONE NUMBER SEARCH**

**GERMANY PHONE NUMBER SEARCH**

**INTERNATIONAL PHONE SEARCH**

**MMN SEARCH**

**DOB SEARCH**

**SSN SEARCH**

**VPN/RDP**

**HOW TO SETUP YOUR RDP**

**CARDING TIPS**

**CHECKLIST FOR CARDING**

**CARDING TERMS**

**HOW TO CHECK IF BIN IS NON-VBV/NON-MS**

**DROP**

**CARDING - BUYING BTC AND PROXIES/SOCKS**

**CARDING TIPS FOR BEGINNERS**

**WHAT IS WHAT (TERMS DETAILED)**

**HOW TO KNOW IF WEBSITE IS CARDABLE**

**WHY WE BUY NON-VBV CARDS**

**METHODS TO CHECK IF CREDITCARD IS LIVE**

**HOW TO OPEN .BAZAR LINKS IN BROWSER**

**HOW TO BUY RIGHT CARD FOR CARDING ON SHOPS**

**WHICH CREDITCARD SHOP IS GOOD**

**SOME CREDIT CARD SHOPS (FROM CARDERS)**

**TYPES OF CARDING**

**AVS PASS BINS**

**NON VBV LIST 2020 + 2019**

**WEBSITES BIN 2020**

**7 DROP METHODS**

**DIFFERENT BETWEEN BILLING AND SHIPPING ADDRESS**

**HOW TO GET A BACKGROUND CHECK AND CREDIT CARD REPORT ON ANYONE**

**WHY ORDER GETS CANCELED**

**ONLINE ORDER / PAYMENT [RED FLAGS]**

**HOW MUCH SHOULD WE CARD**

**HOW TO CARD BASIC / NOOB METHOD**

**HOW TO CARD FROM MOBILE**

**TUTORIAL FOR CARDING INTERNATIONAL SHOPS**

**NETFLIX CARDING TUTORIAL APRIL 2020**

**HOW TO CARD WESTERN UNION**

**WHAT IS DUMP & HOW CAN WE CASHOUT THEM**

**HOW TO DECRYPT DUMP**

**CARDING WITH DUMPS**

**DUMPS VS CVV**

**WHAT IS ONLINE CARDING**

**WHAT IS INSTORE CARDING**

**INSTORE CARDING TUTORIAL**

**HOW TO GET DUMPS**

**FREE IPHONE TUTORIAL (VERIZON WIRELESS)**

**HOW TO CHANGE BILLING ADDRESS ON FULLZ**

**HOW TO CASHOUT CREDIT CARDS EASILY**

**HOW TO DELETE EVERYTHING FROM COMPUTER**

**AMAZON CARDING FULL TUTORIAL (DOWNLOAD)**

**SITES CREDITCARD GENERATORS AND CHECKER FOR SUBSCRIPTION CARDING**

**SPAMMING - WHAT IS IT**

**WHY WE SPAM**

**HOW TO SPAM**

**PHISHING TOOLS (7)**

**HOW TO CREATE A GOOGLE VOICE NUMBER(LIKE ANONSIM)**

**OTHER SITES TO GET ANONSIMCARD**

**WHERE TO GET BURNER PHONES**

**BANK DROP CREATION TUTORIAL**

**FIND DROP SITES**

**HOW TO ORDER GOODS**

**POST ORDER ACTIONS**

**PICKING UP YOUR STUFF AT THE DROP POINT**

**POST PICKUP PROCEDURES**

**WHAT TO DO IF YOU GET CONFRONTED**

**MORE ABOUT DROPS**

**HOW TO GET YOUR DUMP BIN LIST**

**WHAT IS A BINLIST, AND WHY DO WE NEED ONE**

**HOW TO GET ANONYMOUS PHONE NUMBER 2.0**

**HOW TO MAKE A ACCOUNT TAKE OVER (ATO)**

**EXPEDIA FLIGHT CARDING PRIVATE METHOD**

**GOOGLE PLAY GIFT CARD PRIVATE METHOD APRIL 2020**

**AMAZON CARDING PC VERSION APRIL 2020**

**CREDITCARD TO BTC METHOD**

**EBAY CARDING METHOD APRIL 2020**

**TOOLS SETUP 2.0**

**HOW TO CHECK FOR LEAKS / IP BLACKLISTS**

**PAYPAL 2020 METHOD**

**PAYPAL VERIFICATION METHOD FOR AUTHORIZED USERS MAY 2020**

**THE ULTIMATE OPSEC GUIDE**

**THE PARANOID SECURITY GUIDE 2020**

**BROWSER FINGERPRINTS**

**CHANGE YOUR IP TO ANY COUNTRY**

**WHAT DO YOU NEED TO CARD TO GET NOT CAUGHT (CHEAP) 3.0**

**WHAT IS A DARKNET FORUM + INTRODUCTION**

**HOW TO SEND UNTRACEABLE EMAIL 2020 GUIDE**

**HOW TO SEND HACKED PAYPAL BALANCE FROM ONE ACCOUNT TO ANOTHER  
ACCOUNT WITHOUT STRESS**

**TIPS TO STAY ANONYMOUSLY**

**HOW TO STAY SAFE WHEN USING PUBLIC WIFI**

**BULLETPROOF HOST LIST 2019-20**

**BULLETPROOF HOSTING 100% 2020**

**HOW TO RECOGNIZE SCAMMERS / RIPPERS**

**RETAINING A LAWYER, HOW TO HANDLE GETTING CAUGHT OR  
INTERROGATED**

**LAST WORDS**

**THE BIG QUESTION: WHAT IS CARDING?**

Well, defined loosely, carding is the art of credit card manipulation to access goods or services by way of fraud. But dont let the "politically correct" definition of carding stop fool you, because carding is more than that. Much more.

Although different people card for different reasons, the motive is usually tied to money. Yea, handling a \$9,000 plasma television in your hands and knowing that you didnt pay one red cent for it is definitely a rush.

But other factors contribute to your personal reason for carding. Many carders in the scene come from poor countries, such as Argentina, Pakistan, and Lebanon where \$50 could mean a weeks pay, on a good day. Real carders (the one that have been in the scene the longest) seem to card for something more, however. The thrill of cc manipulation? The rush that the federalles could bust down your door at any minute? The defiance of knowing that everyday that you are walking among the public is another day that you have gotten away with a federal crime?

Whatever your persona reason for carding is, this tutorial should answer a few noobie questions and take the guessing out of the entire carding game. The resources and techniques mentioned in this tutorial are NOT, I repeat, NOT the only methods of carding. Experience in carding is key. You have to practice your own methods and try out new techniques in carding to really get a system that works for you. This tutorial is meant to get you on your way.

### **Is it Safe?**

As far as I'm concerned it is if we have a proper setup.

### **Can I make Profit With it?**

Yes, it's one of the way In which hakers make profit easily.

## **STAY SAFE Carding**

### **Setup VeraCrypt On Windows Machine**

1 - Download and install Veracrypt in your computer.

2 - Download and install Virtualbox.

3 - Open Veracrypt and I suggest you to either buy another hdd, use a usb sitck with at least 32gb partition or on your pc's HDD

4 - Create your Veracrypt countainer:

4.1 - Click on Create volume

4.2 - Select "Create an encrypted file container"

4.3 - Select "Standard VeraCrypt" Volume.

4.4 - Find and select the location where you want to create your encrypted countainer. Put a name then hit "Save". Check the checkbox "Never save history".

4.5 - Click "Next".

4.6 - In encryption algorithm select "AES(Twofish(Serpent)), hit next.

4.7 - Select the size of the countainer then hit next.

(IGNORE THE SIZE ON THE IMAGE)

4.8 - Create a big password and confirm it. Then hit next.

4.9 - On "Filesystem" select NTFS.

Now move the mouse to help to generate the encryption key. Once the bar reach the other side, click

in "Format"

4.10 - Hit next then close the window.

4.11 - Now click in "Mount", put the password and your encrypted drive will be ready.

4.12 - On the column "Drive" in your Veracrypt you gonna see the name of your "vault" and the

letter

of the driver (for example, A:, C:, etc). Remember the letter.

**Now Let's configure the Virtualbox to make sure that everything will stay on the encrypted vault.**

- 1 - Open the VirtualBox.
- 2 - Click in "Files".
- 3 - Click in "Preferences" then in "General".
- 4 - On the first field "Default machine folder" click above then select the driver where your vault is.

**\*\*Attention:**

If you open the vault in another drive (for example, in the B:, C:, D:....) it's will affect your Virtualbox and the hidden VM will not work. so If you made these changes to the virtual driver A, always open the vault on A:.

- 5 - Now go to the next field called "VRDP Authentication library", do the same, select the place where your vault is (remember, inside the Veracrypt vault

- 6 - Hit Ok.

**Installing and configure Whonix Gateway:**

- 1 - Download the Whonix Gateway from Whonix official website and verify the signature.
- 2 - Move it to your Vault.
- 3 - Open VirtualBox.
- 4 - CLick in "File" then "Import Appliance".
- 5 - Go to your Vault folder then select the Whonix Gateway image.
- 6 - Once imported, click "Ok" and "I agree" for everything on the machine then update it.
- 7 - Now open the terminal inside your Whonix gateway and paste:

```
$ sudo apt-get update && sudo apt-get dist-upgrade
```

It's gonna take a while, chill out.

- 7 - Now back to your Windows VM, click with the right button above the machine then click in "Configurations", then in "Network" then select "Connected to Internal network", on "Name" select "Whonix" (this must be there if everything went fine). Hit OK
- 8 - Now start your Windows box (Both, Whonix and Windows need to be on at the same time).
- 9 - In your Windows open the "Control Panel", find the "Network" and click in "Change adapter settings".
- 10 - Once open the "adapter settings" menu, scroll down then double click in "IPV4" and change it to:  
IP: 10.152.152.XX (on XX you can put what you want).  
DNS Mask: 255.255.192.0  
Gateway: 10.152.152.10  
Preferred DNS: 10.152.152.10
- 10 - Hit ok to save.

11 - Done, your virtual machine will connect to tor using Whonix gateway

## **HOW TO KNOW WHAT IS BRAND OF CREDITCARD**

If CCN (Credit Card Number) start with 3 then it is American Express (AMEX),  
if start with 4 then it is Visa, if start with 5 then it's Mastercard

With VBV CC, most notably would be a password, date of birth, social security number, or mothers maiden name.

In order to get by VBV you need the password, if you want to reset the password then you will need the DOB (date of birth), MMN (mothers maiden name), and SSN (social security number).

So I personally preffer always By NON VBV Credit Card

## **HOW TO CHECK CREDITCARD BALANCE (SKYPE METHOD)**

### **This method only working for US & UK CC only**

Check your BIN in [www.binspro.com](http://www.binspro.com) . There you will got bank name. For above example BIN (430587) bank is Capital One, USA.

Now search phone number of this bank in google. For Capital One its +1-800-935-9935

Call this number from skype its free since Its toll-free number)

Now the automatic robot will ask you few info. Ex. CCN, CVV etc.

Now put your info by using your keyboard.

It will automatically tell you the CC balance.

## **WHAT IS A PROXY AND WHAT ARE THEIR ANONYMITY LEVELS**

An IP or Internet Protocol address is a numerical number assigned to each computer that takes part in a network. Internet protocol is used for communication in this instance.

You can hide your IP address from internet servers in most cases. However, in some instances, it's impossible to conceal Internet Protocol address of a computer as other devices won't have the ability to communicate with it.

One of the common procedures to hide your IP address is the use of Proxy servers. This server is a special purpose computer that allows users to have an indirect connection to other services within the network.

The user connects to the proxy server, and then the file or connection is requested. The resource is provided either by serving it from cache or by a particular server connection. However, the server's answer or user's request may get changed for a few functions.

These kinds of servers are standalone and configure your browser to route the traffic through a machine. This system sends the request from your side and then exhibits the results to you.

In most cases, these servers are free to use, but they are slow since they're accessible publicly. These servers come in different forms:

### **Anonymous Proxy**

This server reveals its identity as a server but does not disclose the initial IP address. Though this



server can be discovered easily it can be beneficial for some users as it hides the Internet Protocol address.

### **Transparent Proxy**

This proxy server again identifies itself, and with the support of HTTP headers, the first IP address can be viewed. The main benefit of using this sort of server is its ability to cache the websites. Sometimes, your IP may get banned as a result of the use of transparent proxy. Your Internet Protocol address is not hidden in this server.

### **Elite Proxy**

This server does not reveal its identity, and it does not allow the visibility of first IP address. Your Internet Protocol address is hidden when this server is used.

## **TYPES OF CARDS**

Each credit card company starts their cards with a different number:

**3 American Express (AMEX)**

**4 Visa**

**5 MasterCard (MC)**

**6 Discover (Disco)**

Each card company has their own specific types of cards, here are some of the basics:

### **Visa**

**Classic** ➤ a universal payment tool, which was adopted worldwide in any locations designated by the logo of Visa, including ATMs, real and virtual stores, and shops offering goods and services by mail and telephone. This card is intended for those who already have experience in the use of bank cards. She also enjoys popularity among consumers of middle-income, as guaranteed convenience, choice and financial flexibility.

**Gold** ➤ - One of the leading products, has been adopted worldwide and allows you to enjoy an impressive financial freedom (aka higher limit)

**Platinum** ➤ These usually have limits over \$10,000 (but remember, just because it has a high limit, doesn't mean it isn't already maxed out)

**Signature** ➤ - No preset spending limit ➤ great bin to get

**Infinite** - ➤ Most prestigious card, virtually no limit. Though there are less in circulation so be cautious when buying these, stick with reputable sellers!

**Business** ➤ - Used for small to medium sized businesses, usually has a decent limit.

**Corporate** ➤ Medium to large size businesses, larger limit than Business.

**Black** ➤ - limited membership, \$500 annual fee, high end card, no limit

### **MasterCard**

**Standard** ➤ - comparable to visa classic


**Gold** ➤ - comparable to visa gold

**Platinum** - ➤ comparable to visa plat


**World** ➤ - very high limit

**World Elite** -  virtually no limit, high end card.

**Amex**

**Gold**  - usually around 10k limit

**Platinum** - usually higher limit, around 35k

**Centurion**  - High limit, 75k+ (also known as the black card, not to be confused with visas black card)

## 2020 ANDROID CARDING OPSEC SETUP

So understand you need a phone powerful enough to run VMOS just make sure it meets the basic requirements.

<https://www.vmos.com/> and add virtual root to add the ability to ROOT on the Virtual machine.

<https://androidvmos.com/how-to-root-vmos.html>

VMOS is a Android VM machine you can run on your phone. You can find on youtube how to do it. A lot of the videos are Pokemon Go related but just still follow the steps.

Install Xposed Framework the following Mods.

1. Hijack Suite Free. Allows you to get a random IMEI, Serial number, and build number. DO NOT CHANGE THE WIFI MAC address setting It messes up the Connection .

2. Serial number changer. verifies the number is changes from the app above.

This is done in the VM. This takes care of the OPSEC of course every few days or after you hit change the config.

So as far as the browser use CHROME CANARY. No addons are needed. I have found that this is the best browser to do Carding on within the VM.

download ANYMAIL as a email client if needed.

OUTSIDE OF THE VM on the host PHONE:

Use APKPURE, APKMIRROR or anything not Google Play and download APK of the following.

1. Fake GPS. To spoof location of the CH. You can download this outside or inside of the VM.

2. BifrostV to add SOCKS5 Proxy close to CH. I use Luxsocks and I am able to get Android Proxy's and IP's and hit with them. I use Public Wifi and hit.

Just throwing this out there I have a peer who is more advanced in this mobile shit that says you only need mobile data and your good. Doesn't matter where the CH is located.

### Other tips:

To track packages do not use the carrier sites use the following sites or APPs:

17track

Aftership

Trackingmore

Fake Camera App. If you need to upload a picture for verification or something using the VM.

Make sure you have good CC's I only use a range World Card Bins and AMEX cards. It depends on the site I want to hit. I have developed some decent methods that I am expanding on. Trust me guys this method works.

## CARDING : SETUP WINDOWS FOR CARDING

So in last tutorial i wrote about installing windows. We are setup our computer now for carding, i will give you the free tools and so on for setup let us begin.

### Requirements(More Useful Websites Down Below):

- DWS ([https://github.com/spinda/Destroy-Windows-10-Spying/releases/download/1.6.722/DWS\\_Lite.exe](https://github.com/spinda/Destroy-Windows-10-Spying/releases/download/1.6.722/DWS_Lite.exe))
- VPN (<https://mullvad.net/en/>)
- Harddisk Changer 1 ( unofficial : <https://gofile.io/?c=nRnKRs> )
- Harddisk Changer 2 ( [https://anonfile.com/b1bdu9q0o5/PBDownForce0331\\_zip](https://anonfile.com/b1bdu9q0o5/PBDownForce0331_zip) )
- Macchanger (<https://www.technitium.com/tmac/>)
- CCleaner (<https://www.ccleaner.com/>)
- Firefox (<https://www.mozilla.org/de/firefox/new/>)
- File Mind Quick Fix ([https://anonfile.com/71i8u4q0o1/FileMindQuickFix\\_Setup\\_exe](https://anonfile.com/71i8u4q0o1/FileMindQuickFix_Setup_exe))
- Tor Browser (<https://www.torproject.org/download/>)
- Socks Checker (<https://www.socksproxychecker.com/>)

### - Setup Methods / To-Do List -

#### How To Change Manually Hard Disk ID?

If the tools of "Harddisk Changer" won't work for you open CMD as administrator, and type:

```
C:\system32>volumeid C: xxxx-xxxx
```

f.e.:

```
C:\system32>volumeid C: 1D3C-4FA2
```

#### How To Clean Computer Of Spying?

Open DWS Exe file, click on "Destroy Windows 10 Spying", after it is done reboot your virtual machine to apply the new configuration.

#### How To Change Default DNS Server?

1. Open control panel, goto "network and internet", go to "network and sharing center", click "changer adapter settings".
2. You have only 1 connection by default, do right click and click on "properties", select "internet protocol version 4 (TCP/IPv4) and click "properties".
3. Click on "use the following dns server addressses", and enter this dns addresses:  
1.1.1.1  
1.0.0.1  
Click ok and it's done

#### How To Clear Images Or Other Media Before Uploading Them?

We are using Filemind Quick fix for clearing meta tags/private information/gps coordinate, use this to clear any picture data before upload on internet otherwise your anonymity could be compromised.

Start the tools, select the pictures you want to erase metadata, and click "Quick Fix Metadata".

#### How To Use CCleaner?

For Chunk Cleaner i do not much talk about, simply select of your browser, also saved passwords and so on, click on scan and then on remove. It's self explained.

## How To Setup Firefox Anonymously?

Go to preferences i will write als 4 main settings down and what to change:

### GENERAL

When firefox starts-: Show a blank page

Network Proxy-: Only necessary if you doing carding, to setup a socks there. not yet

### SEARCH

Default Search Engine: DuckDuckGo

One-Click Search Engines: Remove all ticks, and leave only "DuckDuckGo".

### PRIVACY & SECURITY

Forms & Passwords : Remove tick at "remember logins and passwords for websites" and "Autofill addresses".

History : Clear History first, then "Firefox will never remember history" (this will restart your firefox browser)

Cookies and Site Data :

Accept cookies and site data from websites ... keep until "i close firefox"

Accept third-party cookies and site data (never)

Tracking Protection :

choose never

Sends Websites a "do not track"...

Choose "always"

Enter URL: about:config

Setup following:

geo.enabled = false

geo.wifi.uri = [leave blank]

network.http.accept.default = text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

network.http.use-cache = false

network.http.keep-alive.timeout = 600

network.http.max-persistent-connections-per-proxy = 16

network.proxy.socks\_remote\_dns = true

network.cookie.lifetimePolicy = 2

network.http.sendRefererHeader = 0

network.http.sendSecureXSiteReferrer = false

network.protocol-handler.external = false [Includes all parameres to false]

network.protocol-handler.warn-external = true [Includes all parameres to true]

network.http.pipelining = true

network.http.pipelining.maxrequests = 8

network.http.proxy.keep-alive = true

network.http.proxy.pipelining = true

network.prefetch-next = false

browser.cache.disk.enable = false

browser.cache.offline.enable = false

browser.sessionstore.privacy\_level = 2

browser.sessionhistory.max\_entries = 2

browser.display.use\_document\_fonts = 0

intl.charsetmenu.browser.cache = ISO-8859-9, windows-1252, windows-1251, ISO-8859-1, UTF-8

dom.storage.enabled = false

extensions.blocklist.enabled = false

### **Any Suggetions For Addons?**

<https://pastebin.com/tvuT3F3Z>  
(old post from @mrblackx r.i.p)

After every closing firefox, your history will be erased, also cookies, then start ccleaner and clean it again.

### **HOW TO ACCESS DEEPWEB FOR BUYING ANYTHING(DETAILED GUIDES BELOW)?**

Install torbrowser, start it and you're done. thehiddenwiki.org are a archive of onion urls. Pls remember 99% of the vendors on deepweb are scammer. Never buy something without using escrow. But there are also cases escrow is scam too, so be careful which escrow website you are using. If you want details guide, go down below.

If it is too good to be true, then probably is.

Few example of deepweb address

evo forum - <https://i25c62nvu4cgeqyz.onion/>

evo marketplace - <https://k5zq47j6wd3wdvjq.onion/login>

### **WHERE CAN I BUY SOCKS?**

We are recommending the website:

<https://911.re/> (residental socks)

<https://911.gg/> (residnetal socks)

<https://vip72.org/> (having over 30k proxies in 99 countries)

### **HOW TO CHECK SOCKS?**

Start Socks Proxy Checker.

### **HOW TO CHECK IF YOUR ARE CLEAN?**

Go to [whatleaks.com](https://whatleaks.com)

### **ZIP CODE SEARCH**

<http://www.findlinks.com/>

<http://zipinfo.com/search/zipcode.htm>

<http://www.addresses.com/>

<http://www.mongabay.com/igapo/>

### **SEND FAX ONLINE**

[efax.com](https://efax.com)

[send2fax.com](https://send2fax.com)

[k7.net](https://k7.net)

### **CREDIT REPORTS**

<https://www.annualcreditreport.com/index.action>

<https://www.usa.gov/credit-reports>

<https://www.creditkarma.com/>

<https://www.creditkarma.com/free-credit-report>

<https://www.creditreport.com/>

<https://www.credit.com/credit-reports/>

<https://www.annualcreditreport.com/>  
<https://www.clearscore.com/>

### **PHONE REDIRECTS**

<https://prankcaller.io/>  
<https://www.spooftel.com/freecall/call.php>  
<https://www.spoofmyphone.com/spoof-call>  
<https://www.spoofcard.com/>  
<https://www.spoofbox.com/en/app/spoof-call>  
<http://www.crazycall.net/>  
<https://www.prankowl.com/>  
<https://www.comedycalls.com/>  
<https://www.wackyprankcalls.com/>

### **USA PHONE NUMBER SEARCH**

<https://www.usphonebook.com/>  
<https://www.411.com/>  
<https://www.ussearch.com/>  
<https://www.whitepages.com/reverse-phone>  
<https://free-lookup.net/usa>  
<https://www.thephonebook.bt.com/>

### **GERMANY PHONE NUMBER SEARCH**

<https://www.whitepages.co.com/germany/>  
<https://www.dasoertliche.de/>  
<https://www.dastelefonbuch.de/>  
<https://www.gelbseiten.de>  
<https://www.goyellow.de/>

### **INTERNATIONAL PHONE SEARCH**

<https://www.thisnumber.com/>

### **MMN SEARCH**

<https://www.truthfinder.com/infomania/technology/maiden-name-search/>  
<https://www.searchquarry.com/namesearch/birth-records-lookup/>  
<https://www.192.com/people/>  
<https://findermonkey.co.uk/>  
<https://www.ancestry.co.uk/>  
[findpeoplebymaidenname.com](https://www.findpeoplebymaidenname.com)  
<https://www.thoughtco.com/top-sources-for-locating-maiden-names-1422659>

### **DOB SEARCH**

[privateeye.com](https://privateeye.com)  
<https://ourpublicrecords.org/birth-records/>  
<https://www.dobsearch.com/people-finder/search-dob.php>  
<https://ukdobfinder.com/>  
<https://www.dobsearch.com/>

### **SSN SEARCH**

<https://ssndob.so/login>  
<https://ssnfinder.ru/>  
<https://www.ssn-check.org/lookup/>  
<https://www.ssnvalidator.com/index.aspx>  
<https://www.ssnregistry.org/>  
<https://ssn24.me/?p=login>  
<https://www.ssofficelocation.com/find-your-social-security-number>  
TOR : [ssn24jrrax4mosjr.onion](https://ssn24jrrax4mosjr.onion)

### **VPN/RDP**

<https://protonvpn.com/>  
<http://www.rdp-sh0p.ru/>

Spoofing Tools - Fraud Fox / Anti-Detect Browsers.

Anti Detect & FraudFox [4.40GB]

<https://mega.nz/#F!0fxGmBBI!bqNPeLaQ4tizJpEhwnfW6w>

### **HOW TO SET YOUR RDP**

I have thought you guys very well on how to set all the tools for carding. But I haven't really emphasised on "RDP" so I'll show you were to get it, and how to get. How to set it. Finally How to use it.

RDP Format:

server address: 77.757.174.132:3975

Login: Administrator

Password: 1q2w3&TtRe@W#E\$R

That's how RDP looks like when you get it from one of the many hacking shops.  
Is very simple to set, no stress.

So all you need to do is to pick your PC. Press =Window key and search "Remote Desktop Connection"--

You would see this dialogue box

<https://imgur.com/a/LdgNkau>

When you click connect this is the dialogue box, you would see. Type in the password correctly.

<https://imgur.com/a/ilkSyvI>

Click yes and continue

<https://imgur.com/a/LaTFcCn>

This my rdp screen as you can see

Now you're good to go. Always remember to clear cookies before you logout the "RDP".

<https://imgur.com/a/iIas90x>

My anonymity gives me 100% as you can see.

## CARDING TIPS

- ✓ Use socks5 ( dont use socks4 or http proxies as they might leak DNS info) which match the cardholder's billing address.
- ✓ If your Creditcard is from UK, try to use a UK drop and so on for other countries (if not and you want to order in your country, use creditcard of your country)
- ✓ If the gift option is there, put it so it looks like you are shipping a gift to some friend, girlfriend etc.
- ✓ Try to make orders before holidays like valentines etc. Now this is an old trick but it works for 2 reasons.
  - \*Reason 1: \*The shops get many orders these days, so they can pass your fraud one as legitimate too.
  - \*Reason 2: \* It looks like you are sending a legit gift
- ✓ Use Firefox in private mode with extensions. Find some security related extensions which dont track your links, clear cookies, LSO & flash cookies, etc. Be creative and explore.
- ✓ Dont use gmail/hotmail/yahoo when ordering ! Use @some hipster email provider, one which is not really used by a lot of people. It makes it look legit. ISP emails are preferred but you might not be able to create them if you are reading this article
- ✓ If your card holder is Billy Nye and his birth year is 1988, use email which is similar to his name. (billy.nye1988@protonmail.com)
- ✓ Have a ready VoIP account and call the shop if they have to confirm information. Usually they only ask about CC info and shipping adress. You dont want to call them with a man voice when CC is a female's, do you ? Use voice changers instead. Do this even when confirming orders for man CCs, to mask your identity. (For skype you can use clownfish or use gf)
- ✓ Checking CCs before making purchase is highly discouraged as most checkers flag/kill cc. Try this on your own risk.
- ✓ Check BIN before trying order. If it is credit platinum, chances are you can buy a fuckton of things. If its debit classic, good luck with that.
- ✓ There are some services that offer DOB and SSN checks. You might want to use them if you don't have fullz.
- ✓ Don't sell too much in eBay, it can get suspicious. Try to use different sites and different usernames. However, don't sell brand new iPhone for 100\$ just to sell it. It will become suspicious !
- ✓ Oh and use fake ID, but I probably shouldn't say this.
- ✓ Don't tell anyone, don't show off.
- ✓ Use in 911 socks from same state,city(just enter zip) of Creditcard holder.



- ✓ Get maximum information about the credit card holder. (teaching soon)
  - SSN
  - Date of Birth
  - Mother's Maiden Name
  - full background info (also stalk on facebook maybe)
- ✓ When you card some big Items of a new account from site it is suspicious.  
 So you can make a new account and leave it for some months after that card small items and always give good feedback.  
 But the better way is to buy old accounts of the site with good feedback.
- ✓ Always try to card at weekends, there are no support in shops which can check if your order is suspicious or not. Banks aren't available at weekends.
- ✓ Don't use a cc at Same Site from different Accounts. Use it at one account maximum 3-4 Times.
- ✓ If you are using a Creditcard, make sure you have email of it, invest to any email bomber, and then bomb the email. So many mails will come and if you bought something the mail from the bank will go under. (floodcrm.net)

## **CHECKLIST FOR CARDING (EVERY TIME)**

Step 1. Always clear your history and clean cookies and change mac address

Step 2. Always clear your flash cookies.

Step 3. Vpn is not good for carding now as most of the ip of vpn have been blacklisted by Good shops.

Step 4. Always use socks5 which is live and not blacklisted.

Step 5. you should match the ip of same state and city.

Step 6. Always match the timezone of cc same state.

Step 7. Always try to type the details of cc as many site now have script to check copy paste of cc details as most of the time carders copy paste the details of cc. Actual owner always type all details.

Step 8. Get the maximum information of cc owner from background check sites there you can found DOB, MMN and sometimes SSN.  
 Most of these sites are cardable with public cc.

Step 9. If you want to be a pro carder than stop using free email sites as yahoo, gmail, aol etc.

Step 10. Better solution is first card a domain and hosting and make a small site and then create a email of cc owner their of the same name on cc. you can also use free domain or sub domain sites but carding your host & domain is better.

While carding domain and hosting you should use Amex cc as there is less chances of chargeback.

Step 11. Check the cc live before using site not on checker as sometimes it kills cc. Find a most easy cardable site and make a bogus account and checkout for small amount like 2\$ if it work then go to original site.

Step 12. Always study the site carefully which you want to card and its seller. Most of the time seller who sell refurbished Mobiles etc are in hurry to ship the item. So search them.

Step 13. When you card some big Items of a new account from site it is suspicious. So you can make new a new account and leave it for some months after that card small items and always give good feedback. But the better way is to buy old accounts of the site with good feedback.

Step 14. Always Use Skype ac with credit and call forwarding services. If you call the shop with the number of cc owner and ask customer care of site some help before filling cc details your chances of success or much higher. You should always use it if you want to card high value items.

Step 15. Always Use Trusted drop of same country if you are carding a international Site. Because shipping to another country is always suspicious.

Step 16. Always try to carding on Weekends as shops not able to contact and verify extra details from bank by calling them. You can also check closing time of bank and card after closing timing of bank.

Step 17. Always Send a Email instantly to seller after order complete to ship order fast as you need it urgent as there is some function in your house.

Step 18. Don't use a cc at Same Site from different Accounts. Use it at one account maximum 3-4 Times.

Step 19. One of my friend Using a new trick he calls from the mobile number of cc owner with skype to the cc issuing bank that he is going to shop some goods and they should make the approval fast. I don't know the full trick and working on it you should also find your ways. If you succeed to convince cc issuing bank that you are original cc owner than you will rock with high amount purchase.

Step 20. If you use the pp in carding then buy pp with email access and delete the order related emails from inbox and trash box of email.

## **CARDING : TERMS**

You should know this terms or should ever heard what it's meaning.

### **A**

AFS = Anti Fraud System

AMEX = American Express (credit card provider)

anoSIM = anonymous SIM card for mobile phones  
ATM = Automated Teller Machine (ATM)  
AVS = Address Verification System (Address Verification System)

## **B**

BD = BankDrop (account created with wrong data to receive money anonymously, often used for filling)  
BIN = Bank Identification Number  
BKD = Mailbox drop (see Drop)  
BM = BitMessage (anonymous messenger)  
BTC = Bitcoin (crypto currency)  
BILL=SHIP = means - The CC Billing Address should be the 'Exact Same' as the Shipping Address 100%.

## **C**

Carding = credit card fraud (often also PayPal or invoice fraud)  
CC = Credit Card (credit card)  
CVV = Card Verification Value (check digit)  
CITY + STATE = means - Your IP's location which is Country or State and City must match the Billing City and State on the CC.  
CCSTATE/STATECC = Means - The CC Country and State should be 'Exact Same' as The Drop Address.

## **D**

Debit Card = EC card  
DHL = International parcel service  
DP = German Post  
DPD = German Parcel Service  
DoB = Date of birth (date of birth)  
Drop = Delivery address

## **E**

ED/EXP = Expiration Date  
ELV = electronic direct debit procedure  
Enrolled = complete credit card record with all the trimmings  
Escrow = escrow service or escrow account, which is administered by the market during the transaction.  
Exif = exchangeable image file format - The exchangeable image file format (officially exif, according to JEIDA/JEITA/CIPA specifications) is a standard that specifies the formats for images, sound, and additional tags used by digital cameras (including smartphones), scanners, and other systems that handle image and sound files recorded with or by digital cameras. (see also Metadata)

## **F**

Filling = "Filling" accounts/bank accounts with money people pay for fake ads on e.g. Ebay (form of fraud)  
Full = credit card record with (almost) all information

## **G**

GC = DHL GoldCard  
GLS = German parcel service

## **H**

HD = House drop / house search (Depends on the context)  
HDB = house search command  
Hermes Versand = German Parcel Service

## **J**

Joker = Prepaid payment method

## **M**

M2G = money2go (prepaid means of payment)  
MC = Mastercard (credit card company)  
Metadata = Metadata or metainformation is structured data that contains information about characteristics of other data. They contain information about author, location, time, etc. that deanonymize you.  
Mixer = Anonymization of Bitcoins (disguises original wallet)  
MMN = mothers maiden name  
mTAN = mobile TAN (verification via mobile phone)  
MultiSig = trustee over a common wallet (2/3 confirmations necessary). Also "fraud-proof" fiduciary system, where a temporary wallet with one-time keys is created outside the market.

## **O**

OB = online banking

## **P**

phished PS = Packstation with stolen data  
phishing = stealing passwords or data using fake pages  
PP = PayPal (online payment system)  
PS = packing station  
PSC = paysafecard (prepaid payment method)

## **R**

random = credit card record with limited information  
RE-ROUTE = Means - Calling or Chatting Customer service to Change

## **S**

SC = Secure Code (additional security feature of Amex and MasterCard)  
SE = Social Engineering in the context of information security is the psychological manipulation of people to perform actions or to reveal or obtain confidential information.  
SSN = Social Security Number - In the United States, a social security number is a nine-digit number given to U.S. citizens, permanent residents, and persons with temporary residence status pursuant to Section 205 of the Social Security Act, codified as . The number is issued to a person by the Social Security Administration, an independent agency of the United States government.

## **T**

TC = TorChat (anonymous messenger)  
TH = escrow or escrow service (see Escrow)  
TID = Tracking ID (shipment tracking)  
TPIN = TelePIN (for payment transactions at OB)  
Trustpic = picture of the acquired goods

## **U**

Ukash = Prepaid payment method

UPS = parcel service

## **V**

VB = Virtual Box (simulates a virtual OS)

VBV = Verified by

Visa (additional security feature of Visa)

VicSocks = routes traffic over a victim's PC

VISA = credit card company

VPN = Virtual Private Network - A virtual private network extends a private network over a public network and allows users to send and receive data over shared or public networks as if their computer devices were directly connected to the private network.

## **W**

Wickr = anonymous messenger

## **Z**

ZIPCC/CCZIPCODE = Means - Similar meaning as the case of "City + State".

## **HOW TO CHECK IF BIN IS NON-VBV/NON-MSV**

Pick your bins carefully cause you can't check 100s a time.

Create a account at play-asia.com with fake email and credentials

check for 5-15 mins the website and place an item in your cart(I used a japanese movie for \$14)

Place order, create fake info and Fill in the requiredments

Choose pay with credit card, you will be redirected to the page where you insert the CC info.

Go with your bin you want to check to namso.ccgen.co and generate some valid CCs,

Insert the generated CC to the payment page of play-asia.com

CVV, Expiry, name does really not matter !!

the only thing that needs to be valid is the CC with your bin

If you get a prompt with verify blah blah blah.. then your bin is VBV/MSCV

if you got redirected, and you will get an error message with the follow output:

There was a problem with your payment: Payment status - Declined

If you have difficulties to pay by Credit Card directly, you can also choose PayPal to ay by Credit Card.

CONGRATS your bin is non-vbv/non-mcsc

## **DROP:**

Drop is an address which you use for shipping address in carding. Let me explain ( ) am carding with a USA CC. if ) use a USA address as shipping address then order will ship 100% & I will be safe. So we have to manage USA address. If we have friends or relatives then no problem.

Otherwise there is lots of website that give drop service. We will order in drop address..this website will receive our products and will send to us.. they will take few charge for it. No need for every shopping sites. For hard security sites only.

## **CARDING : BUYING BTC AND PROXIES / SOCKS**

## How To Buy Bitcoin?

\*My simple answer is: [paxful.com](https://paxful.com)

Benefits:

- Excepting many payment options without verification (only to specific vendors)
- Has currency worldwide

Disadvantages:

- Lots of fees

You can alternatively buy from [localbitcoins.com](https://localbitcoins.com)

Buy bitcoin for 100\$

Nte: Paxful → You don't need to verify. It's OK if you do but I do not recommend It...

## How To Buy Proxies / Socks?

Before we are really starting with carding, proxies are the most important thing while doing carding.

First we need 50\$ of bitcoin, if you are from another country, please convert your amount into bitcoin. Find a way to pay for bitcoins, [paxful.com](https://paxful.com) has many fees, but it's variable for currency and has a lot of options to buy bitcoin.

Go to :

<https://911.re> or <https://911.gg>

(it's the same)

Register on it (choosing skype or jabber) here a tutorial for jabber : <https://t.me/ViperZCrew/8619>

Now buy it, wait some minutes until payment has been completed. Do not leave the website! (just copy the amount of BTC like..: 0.004232 and paste it on paxful (wallet dashboard), then copy btc address also and then send it after you typed your password)

Now go to [911.re/user](https://911.re/user) (userpanel) and go to "911 S5 Soft Download", password of the software is "911.re"

<https://911fileupdate.s3.amazonaws.com/3.26.zip>

How ever. Download, fire up your virtual machine, and install it.

If you can not follow my step, you can visit

<https://911.re/software>

they uploaded video tutorial on how to use the software in detail.

Open CMD as admin, type following commands:

```
C:> ipconfig /release
```

```
C:> ipconfig /renew
```

```
C:> ipconfig /flushdns
```

If you have already cc's, spoof the hdd serial number, this requires an reboot.

Start the "Client.exe", enter credentials, choose line 1

Clear Browser info are for "clearing browser info" after successfully carding press it.

Program Tab are for software (internet browsers) so drag firefox into it. Proxylist you can use for proxys, you can search for cc holders ZIP, City and State. Go to "settings" tab, enable:

- auto user agent
- auto clear browser info (clear browser info)
- auto close program when change proxy

Click on firefox icon on programs tab and it's done.

Go to

<http://whatleaks.com>

or

<https://whoer.net>

If you want to check if proxy is blacklisted or not.

## **CARDING TIPS FOR BEGINNERS**

★ If your CC is from UK, try to use a UK drop and so on for other countries, get also a proxy near the country of the CC owner itself

★ If the gift option is there, put it so it looks like you are shipping a gift to some friend, girlfriend etc.

★ Try to make orders before holidays like valentines etc. Now this is an old trick but it works for 2 reasons. The shops get many orders these days, so they can pass your fraud one as legitimate too. And it looks like you are sending a legit gift

★ For your security, use cracked/open wifi + changed MAC, VPN in some offshore country + 2-3 socks in a virtual machine. I suggest VMWare and do download a ready made image so just open it. Try to create a proxy chain for your own security, with the last external IP being the one to match cardholders address.

★ Use Firefox in private mode with extensions. Find some security related extensions which don't track your links, clear cookies, LSO & flash cookies, etc. Be creative and explore.(Read above)

★ Use gmail/hotmail/yahoo when ordering or Use @some hipster email provider, one which is not really used by a lot of people. It makes it look legit.

★ If your card holder is John Jones, use email which is similar to his name. Have a ready VoIP account and call the shop if they have to confirm information. Usually they only ask about CC info and shipping address. You don't want to call them with a man voice when CC is a female's, do you? Use voice changers instead. Do this even when confirming orders for man CCs, to mask your identity.

★ Checking CCs before making purchase is highly discouraged as most checkers flag/kill cc. Try this on your own risk.(Check If Creditcard Is Live → Above)

★ Check BIN before trying order. If it is credit platinum, chances are you can buy a fuckton of things. If it's debit classic, good luck with that.

★ There are some services that offer DOB and SSN checks. You might want to use them if you don't have fullz (Listed Above → Setup Section).

★ Try to use different sites and your own tools in different ways. However, don't be lazy because laziness in carding can cost you badly.

★ Don't tell anyone, don't show off. (My Rule), Real Carder likes to earn silently

★ You never ever, use a card more than 1.5k, mainly because most cards, assuming Mastercard/Visa, don't have more than 1.5k in them, even if they do, credit card companies are usually called up before the transaction goes through, and the result is, your finished.

★ It is **STRONGLY** advised that you read the law in your country regarding cyber crimes, so you know what happens to you, in case you get caught, how to deal with the situation

★ Use your brain when you card. It's simple, when you card, buy small items, don't buy big. Think about it, which nutcracker would hire a lawyer, run all over the world, chasing you just for a 150 USD package? The cost of hiring a lawyer for a trial is already much more than his law. Lesson here, buy small, sell big in your country. Convert Virtual cash to REAL cash.

★ Which period of the month is it best to card at? For me, it's the middle of every month. Simple, most CC owners, get their financial papers at the 1st of every month. I find a good date is 15-16-17th.

★ Do not buy anything that has to be delivered to your house. If you do, and the card gets reported, you will get in major trouble. If you do decide to order something, send it to a neighbor, or someone who is out of town.

★ The best items to buy online with any CC, is stuff that does not have to be delivered, such as VIP, site access, or other similar material. This works well because you cannot be traced to an address.

★ Do not create any payment gateway accounts with fraud CCs, it will alert the CC owner due to many security processes and verification of the card, you will most likely **FAIL** to complete it, and the card owner will be notified.

★ If you intend to do money laundering, get yourself some buyers first, buy the items they want with your fraud CC, ask them to pay you via egold. Why egold? Cuz there's no charge back.

## **WHAT IS WHAT?**

### **SOCKS**

Socks 5 SOCKet Secure (SOCKS) is an Internet protocol that routes network packets between a client and server through a proxy server. So with this we can hide our IP. We used it to match our location same with Credit Card holder Location to make a successful transaction. It's don't leak your DNS info but VPN do that so it is more secure than any VPN software.

### **MAC & MAC ADDRESS CHANGER**

MAC (Media Access Control) is a unique identifier assigned to network interfaces for



communications on the physical network segment. A network node may have multiple NICs and each NIC must have a unique MAC address. MAC Address Changer allows you to change (spoof) Media Access Control (MAC) Address of your Network Interface Card (NIC) instantly. You may don't understand it... it's like your iP address. We will change it to stay anonymous and safe.

## **CCLEANER**

CCleaner is a very handy tool to clean your browsing history (temp files, cookies and also your Flash cookies, which many people neglect or don't even know about. Flash cookies are stealthier than regular cookies. Flash can install cookies on your computer without your permission by default, and store the same info that regular cookies do (when you visited etc).

## **RDP (Remote Desktop Protocol)**

RDP is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection. The user employs RDP client software for this purpose, while the other computer must run RDP server software. It will connect you with any computer that is located in others country. We use it for stay anon and safety. In one word you will use someone's pc for carding instead of your own...

## **SSL**

In layman's terms it is the an algorithm that encrypts a message between a receiver and sender to help avoid the message being read by an attacker should it be intercepted in transmission, for example a website that uses HTTP as opposed to HTTPS offers no protection from an attacker intercepting credentials from the network. For a website to be able to support SSL, it requires an SSL certificate.

## **CC - CREDIT CARD**

Read all very carefully. Don't be lazy. This is the main part of carding. As fast as u understand it, success will come as fast.. When you buy CC from shop or somewhere else.

credit card number | exp date| cvv2 code | name on the card | address | city | state | country | zip code | phone (sometimes not included depending on where you get your CC from) |

### **For Example:**

4305873969346315|05|2018|591|UNITED STATES|David Mechanic|23 Stoney Brook Lane|Middleton|MA|01949|

## **WHAT IS BIN (Bank Identification Number)**

The first 6 numbers of CC is the BIN number.  
So from the above example, the bin is 486236

So now we will collect some info about this BIN. For that, there are so many websites. I prefer these below sites:

<http://bins.su/>  
<https://www.bincodes.com/>

Now we can calculate few things from above info.. approx balance, is this bin non vbv or vbv.

## **WHAT IS VBV/ NON-VBV/ MSC**

### **VBV(Verified by Visa)**

Extra verification process initially added by visa, there are different types of authentication used, most notably would be a password, date of birth, social security number, or mothers maiden name. Will send OTP to CC owner mobile No. or need secret Password when doing transaction in any process.

### **NON VBV(Verified by Visa)**

Easy to use.

## **HOW TO KNOW IF WEBSITE IS CARDABLE**

-ANY AND ALL SITES ARE CARDABLE-

Why do I say that? because it's true. Whatever your card, make sure that you have all your info prepared before carding it. If you don't get success first time then you have to use other BIN CC and Others Method. Have used your brain & find different Logic for a different site. You may Kill 2-3 CC when trying any sites. But you will find out the working method for any site

## **WHY WE BUY NON-VBV CARDS?**

Because no need of more info about CC like DOB, SSN, MMN. Also no need OTP when doing transaction.

### **MSC (Mastercard Secure Code)**

As same as VBV We always buy NON VBV CC for carding. Cause the shopping site is VBV or NON VBV we don't care, we have NON VBV CC. So no OTP, no AVS, no need SSN etc. NON VBV is not verified by visa card, you can buy anything with non vbv cards without going through 3rd verification process. How to Buy NON VBV CC will explain later..

### **AVS – (Address Verification System)**

A system used to verify the identity of the person claiming to own the credit card. The system will check the billing address of the credit card provided by the user with the address on file at the credit card company. This was an attempt to help identity theft and fraud over the internet. This is a system we as carders dont have to worry about since we have the billing address of the credit card holder. I mentioned it since it is good to be aware of it and that almost every site has this system. It emphifies the importance of typing in the address correctly.

## **METHODS TO CHECK IF CREDITCARD IS LIVE**

### **Method 1:**

1. Make a temp E-Mail of CC's Owner Name from temp-mail.org
2. Register on any 2d donation site eg. indiegogo.com
3. Donate 1-2\$ ,if success cc is live- if ur card declined then card is dead

### **Method 2:**

1. Make a temp E-Mail like in Method 1.

2. Go to netflix.com and try to add CC
3. If CC is accepted then it's live, if not then dead.

### **Method 3:**

1. Make a temp E-Mail like in Method 1&2
2. Go to amazon.com and try to add CC as payment option.
3. If CC is accepted then it's live, if not then dead

## **HOW TO OPEN .BAZAR LINKS IN BROWSER?**

Install Extension:

<https://addons.mozilla.org/en-US/firefox/addon/b-dns/>

or

<https://chrome.google.com/webstore/detail/blockchain-dns/hlnmiaddfabbklljanmdilbngnookdgn>

And try to open <http://uniccshop.bazar/>

## **HOW TO BUY RIGHT CARD FOR CARDING ON SHOPS**

Mark some specific base which contain bumpy cards Like "US\_SNIFFED" Or "US\_SNIFFED\_P1"  
And try to only buy from these bases. Incase you don't get any other option then go for any other.

When you add cc to cart, there you can see card holder name, city zipcode,  
open any background search site Like, Truthfinder or Whitepages and do a search with that detail,  
if you got matching name with matching city, There is higher chances then that the billing will be  
correct, if you don't get matching results, skip the card and move to any other.

## **WHICH CREDITCARD SHOP IS GOOD**

Personaly I Used All Major shops like validcc, xatas, unicc, bankomat and feshop.  
Although now i'm out of all these shops except one feshop. Some of you still considering its a crapy  
shop but give it a try and stay away from random bases, you will not lose money.

One more thing in any case you buy cc with check time, try not to check it immediatly with any  
checker same for unicc boys' one more important thing for some of you who dont know if feshop  
base updates on 15 Jan, cards always added around 10k-50k usually, and all current day base cards  
costs 9\$ apart from any bin. but it goes for 5\$ on next day early morning or even more earlier so if  
you think your bin is rare and cant be taken easily then you can save 4\$ on each cc, try buying it  
next day early morning the cc will still works well same if you buy that for 9\$ when you done with  
card selection, Move to your job then, Good Luck

## **HERE ARE THE LEGIT CVV SHOP I CAN RECOMMEND FOR THOSE WHO NEED THEM**

### **1. BANKOMAT**

Normal Link: [Bankomat.cc](http://Bankomat.cc)

Tor Link : <https://bankomatccor3gum.onion> (requires javascript so don't enter)

### **2. UNICC**

Normal Link : <http://uniccshop.bazar/>

Tor Link : <http://uniccxide6hker6y.onion/>

### 3. VALIDCC

Normal Link : [valcc.bazar](http://valcc.bazar)

TOR DOMAINS: [HU5IYZFPEYIFE46M.ONION](http://HU5IYZFPEYIFE46M.ONION) | [VALIDCVVMTWP25N5.ONION](http://VALIDCVVMTWP25N5.ONION) | [VALIDCCVLSSFDGAS.ONION](http://VALIDCCVLSSFDGAS.ONION)

### 4. FESHOP

Normal Link : [FE-ACC18.RU](http://FE-ACC18.RU)

Tor Link : [hdjd6wv7hjngjhkb.onion](http://hdjd6wv7hjngjhkb.onion)

**XXX\*\*\*\*DISCLAIMER\*\*\*\*XXX**

Dont use the following FAKE RIPPING domain

1. [Unicc.su](http://Unicc.su) , [Unicc.at](http://Unicc.at) , [Unicc.org](http://Unicc.org)
2. [Validcc.su](http://Validcc.su) , [Validcc.world](http://Validcc.world) , [validccshop.online](http://validccshop.online)
3. [feshop2017.ru](http://feshop2017.ru) , [fe-shop.ru](http://fe-shop.ru) , [fe-shop.cc](http://fe-shop.cc) , [feshop-store.cc](http://feshop-store.cc)

## TYPES OF CARDING

They are listed as follows:-

### Easy Carding:

In this level, a carder do carding of very cheap goods. For example: small phone call bills etc.

Mostly in this level the carder can card goods below \$100 such as GIFT CARDS and it is known as the beginner's level of carding.

### Intermediate Carding:

In this level, a carder do carding of slightly higher goods like background reports or very little physical items like some clothes, writs watches etc. Mostly in this level, carders use to do carding of goods below \$200-\$500. The different between the Level 1 and Level 2 carding is that Level 2 do carding of physical items.

### Hard Carding:

This is regarded as the advance carding. In this level, a carder do carding of everything which includes: cellphones, laptops and other goods that is above \$500-\$2000 and the upper limits is not fixed.

## AVS PASS BINS

Visa: 492142 454623 453904 407220 492942 477912 456469 492942 456004 466188

MasterCard: 523232

## NON-VBV LIST 2020

**402360 = ITALY = DEBIT**

**409015 = SPAIN = CREDIT**

**413585 = GERMANY = CREDIT**

**416029 = ITALY = CREDIT**

**424607 = NETHERLANDS = CREDIT**

**425723 = GERMANY = CREDIT**

**435659 = SPAIN = CREDIT**

450608 = SPAIN = CREDIT  
450625 = SPAIN = CREDIT  
450663 = BELGIUM = CREDIT  
453243 = GERMANY = CREDIT  
454108 = SWEDEN = DEBIT  
454617 = GERMANY = CREDIT  
454618 = GERMANY = CREDIT  
455218 = BELGIUM = CREDIT  
455221 = SPAIN = CREDIT  
455262 = SWEDEN = DEBIT  
401805 = ITALY = DEBIT  
456140 = FRANCE = CREDIT  
465596 [ DEUTSCHE POSTBANK AG VISA CREDIT BUSINESS GERMANY ]  
419403 [ BARCLAYS BANK PLC VISA CREDIT CLASSIC PORTUGAL ]  
462730 [ ZAO RAIFFEISENBANK VISA DEBIT ELECTRON RUSSIAN FEDERATION ]  
460312 [ OLDENBURGISCHE LANDESBANK AG VISA CREDIT CLASSIC GERMANY ]  
520309 [ DEUTSCHER SPARKASSEN UND GIROVERBAND MASTERCARD CREDIT  
STANDARD GERMANY ]  
455600 [ SANTANDER CONSUMER BANK AG VISA CREDIT CLASSIC GERMANY ]  
542555 [ EURO KARTENSYSTEME GMBH MASTERCARD CREDIT STANDARD  
GERMANY ]  
520309 [ DEUTSCHER SPARKASSEN UND GIROVERBAND MASTERCARD CREDIT  
STANDARD GERMANY ]  
546058 [ EURO KARTENSYSTEME GMBH MASTERCARD CREDIT GOLD  
GERMANY ]

#### **NON VBV AND NON MSC LIST 2020**

430858 COMERICA BANK DEBIT CLASSIC UNITED STATES  
463576 BANK OF AMERICA, N.A. DEBIT BUSINESS UNITED STATES  
463572 BANK OF AMERICA, N.A. DEBIT BUSINESS UNITED STATES  
478455 CITIBANK (SOUTH DAKOTA), N.A. CREDIT GOLD/PREM UNITED STATES  
422005 ITAU BANCO DE INVESTIMENTO, S.A. CREDIT CLASSIC BRAZIL  
463575 BANK OF AMERICA, N.A. DEBIT BUSINESS UNITED STATES  
515598 HSBC BANK NEVADA N.A. UNITED STATES  
450004 CANADIAN IMPERIAL BANK OF COMMERCE CREDIT BUSINESS CANADA  
424698 COMMERCE BANK, N.A. CREDIT BUSINESS UNITED STATES  
529149 CAPITAL ONE BANK UNITED STATES 804-967-1000  
465614 FIRST FEDERAL SAVINGS AND LOAN ASSOCIATION DEBIT CLASSIC  
UNITED STATES  
435237 TARGET NATIONAL BANK CREDIT CLASSIC UNITED STATES  
514616 PULSE EFT ASSOCIATION UNITED STATES 1-800-420-2122  
462120 CITIBANK (SOUTH DAKOTA), N.A. CREDIT CLASSIC UNITED STATES  
406095 NAVY F.C.U. CREDIT CLASSIC UNITED STATES  
540168 FIRST USA BANK, N.A. UNITED STATES 800-955-9900  
488893 FIA CARD SERVICES, N.A. CREDIT PLATINUM UNITED STATES  
432630 BANK OF AMERICA, N.A. DEBIT PLATINUM UNITED STATES  
543805 USAA FEDERAL SAVINGS BANK UNITED STATES 800-531-2265  
432845 SOVEREIGN BANK DEBIT CLASSIC UNITED STATES  
551896 PULSE EFT ASSOCIATION UNITED STATES 800-456-4307  
552234 HSBC BANK NEVADA N.A. UNITED STATES  
479126 ESL F.C.U. DEBIT CLASSIC UNITED STATES

427138 CITIBANK (SOUTH DAKOTA), N.A. CREDIT GOLD/PREM UNITED STATES  
480011 FIA CARD SERVICES, N.A. CREDIT GOLD/PREM UNITED STATES  
546068 CITIBANK, N.A. UNITED ARAB EMIRATES 97143242868  
431303 FIA CARD SERVICES, N.A. CREDIT CLASSIC UNITED STATES

#### **NON-VBV BINS LIST 2019**

----- Card BIN ----- 465943  
----- Card BIN ----- 465950  
----- Card BIN ----- 475128  
----- Card BIN ----- 475129  
----- Card BIN ----- 492940  
----- Card BIN ----- 498824  
----- Card BIN ----- 542011  
----- Card BIN ----- 557349  
----- Card BIN ----- 557361  
----- Card BIN ----- 475129  
----- Card BIN ----- 475714  
----- Card BIN ----- 476365  
----- Card BIN ----- 476367  
----- Card BIN ----- 492181  
----- Card BIN ----- 492182  
----- Card BIN ----- 446291  
----- Card BIN ----- 453979  
----- Card BIN ----- 454313  
----- Card BIN ----- 454742  
----- Card BIN ----- 456735  
----- Card BIN ----- 465858  
----- Card BIN ----- 465901  
----- Card BIN ----- 465941

#### **WEBSITES BIN 2020**

414720 - walmart  
546616 - target  
402074 - walmart  
402075 - best buy  
402076 - home depot  
402080 - best buy  
504944 - neimans marcus  
601100 - target  
601120 - walmart  
601149 - target  
414709 - apple  
400344 - nordstorm  
407156 - apple  
407158 - best buy  
407197 - apple  
407199 - home depot  
511985 - cvs  
511986 - walgreen  
511987 - apple

512344 - walmart  
512356 - cvs  
512387 - walmart  
512398 - nordstorm  
515664 - walgreen  
519238 - cvs  
519669 - nordstorm  
515665 - best buy  
521127 - cvs  
521132 - walgreen  
521146 - walgreen

## **7 DROP METHODS**

I've been collecting methods for many things for years.

None of these have been leaked from paid ebooks.

I will include links to the source where possible.

All these are pretty standard, they are just to provide a good intro to newbies.

### **1. General Delivery**

- US Only - USPS Only
- Fake ID Required

In the US, you can send a package to a post office for "General Delivery".

Example:

Bob Smith

General Delivery

160 J ST (Post Office's Address)

FREMONT, CA 94536 (Post Office's Address)

The package will be delivered to the post office. You can then pick it up using an ID matching the name on the package.

If a site will ship to General Delivery if a hit or miss, you'll just have to experiment. (I know Amazon will deliver to general delivery).

### **2. Hotel Delivery**

- Likely Works Internationally - All couriers
- Fake ID likely required

Many times, hotel guests need to receive packages. Call around to hotels and ask if the front desk could hold a package for you during your stay (make up any excuse you want, say you're in town for business and need supplies sent from the office). When tracking shows it as delivered, just go pick up the package at the front desk. Usually, you don't even need to rent a room.

### **3. Wrong Address Delivery**

- Likely Works Internationally - all couriers
- No Fake ID needed, but it might help

Order a package to someone else's address. After it's been delivered, go ask for your package, say it got delivered to the wrong address (or say you mixed up the address).  
A variation would be to let them know ahead of time, and ask them to hold it for you.

### **4. Rent a House**

- International
- All Carriers - Fake ID Required

Rent a cheap house/apartment. For one month, massively card items to the house. Once you're done, leave, stop paying rent, leave no trace.

### **5. Empty Houses**

- International
- All Carriers - No Fake ID needed

This one is pretty standard. Ship to an empty house. If it needs a signature, do some yard work outside on the day it's supposed to arrive (or just break in). You could also leave a note with the tracking number saying to leave it (with a signature).

Houses for sale work well.

Houses with families on vacation work well too.

### **6. Rent a Mailbox**

- Likely International - All Carriers
- Fake ID Required

This is one of my own ideas. Many places offer private mailbox rental (UPS offers this service at some of their stores). They receive and sign for any packages you receive, and you can go in and pick them up (using a slip out of your own keyed mailbox. When using this method, massively card items to the box for 2-3 weeks. Then abandon the box and store. Pay in cash or with a prepaid, untraceable card.

### **7. Setup a Mailbox**

- Likely works international
- USPS only in the US
- Letters and Small packages only
- No Fake ID needed

Find a trailer park where everyone sets up their own box on the road. Simply add a box to the end with a non-existent lot number shortly before you expect the letter. When using any of the methods above, all the rules of staying secure apply. Never do it in your home town. No fingerprints. No trace. When using a fake ID, use a picture that kinda looks like you, but not close enough that it could be used to identify you. Some methods require the ID to be scanned.

I will write later more about Drops.



## **DIFFERENT BETWEEN BILLING AND SHIPPING ADDRESS**

When someone say a site is cardable using bill = ship it basically means the site don't use AVS(address verification system). In these sites you can enter your drop address in both billing and shipping address fields.

For example if you are carding product "XYZ" and you are in checkout page you need to enter details of both Billing and Shipping same.

In short : BILL = SHIP (You add your drop address in both fields - No need to use CC real billing address)

## **HOW TO GET A BACKGROUND CHECK AND CREDIT REPORT ON ANYONE**

Having this information can be very beneficial for answering security questions, opening bank accounts, applying for credit, verifying accounts, among many other things. However, getting this information can be a little tricky, and sometimes unobtainable. With a little luck and this guide, you will have the tools and resources to give you the best chance possible to obtain this information.

There are a couple things you will need first. Some are required and some are very helpful to have. Obviously, it helps to have a person's fullz which include:

1. Persons full legal name
2. Current and/or previous addresses
3. Date of Birth (DOB) and Social Security Number (SSN)
4. Mothers maiden name

However, the only two things that are required are FULL LEGAL NAME and a USA CVV or anonymous debit card. I use This Site.

You will also need to know one of the following things about the person; their city, state, zip code, or DOB. Google is your friend and if the person's name is unique enough you can obtain most of this information with a simple search. To get the persons DOB, the easiest way is to use the online database [familysearch.org](http://familysearch.org).

There are 100's of these services, some are free and some charge a fee.

Just use your CVV if you need to pay for background check. Having a background check will help out when trying to get the credit report described later in this guide but [familysearch.org](http://familysearch.org) has pretty much all the background info you need, and it's FREE.

Once we have located the DOB and any other information on the subject, we can now get their SSN.

Go to [ssnfinder.ru](http://ssnfinder.ru) and register for free.

Once you are logged in they charge \$3.00 per search. You will need the full legal name of the subject and either the city, state, zip code, or DOB. From my experience they are successful finding the SSN about 80% of the time. At this point you should have the needed background information to complete the next step.

First, register at 3 sites offering credit report like

Site #1

Site #2

Site #3

Site #4

Site #5

If you do not find any website, which is good, go to links (first sites).

Again there are tons options and the more you try the better chance you have to be successful.

Start to sign up for these services with all the information you have obtained including SSN and DOB.

At some point they will ask you security questions to verify you are the person you are trying to get information on. Normally, all of them will ask you same questions so keep track of your answers.

Most questions you should be able to answer with the information you previously obtained or simply searching Google. For the questions you have to guess on, make note of how you answered and it helps to capture the screen to remember.

After you click the Submit button you will know if you were successful or not. If it says that you are verified you got all the questions correct!

You don't need to do anything else with the other credit report websites.

But if it says Wrong answers then leave this website and go the second one. Again, the questions should be almost the same. Check the answers you used for the last website and guess a different one. Click submit and wait and see what the webpage says.

If it says you are verified then you're done. Otherwise continue to the third, fourth, so on until you get all answers correct. At this point you will have the background report, credit report, and make sure you save the answers to the security questions you just answered correctly.

These are different than the security questions the user might have created for online banking or accounts they have already created but they will be the same for when you need to create new accounts on Coinbase or creating online bank accounts. You can also use this information to create a Money Gram account to send money with bank account or credit cards.

Register on Money Gram website using all the information you just obtained. When you come to the payment page, they will ask the same questions you had to answer to get the credit report. Answer questions and send transfer! You can use any credit card owned by anyone as long as you change the address on record with MG to the address of the card holder. No need to change MG account name.

Money Gram doesn't make the connection between account owner and credit card owner. They will authorize the transfer as long as you answer the security questions and the Money Gram address matches the CVV address.

## **WHY ORDER GETS CANCELED**

When a website receives an order of about \$1000, we understand that they try to protect themselves. What is the first thing that a website will do to verify the order? That's right, they will call the issuing bank and will check if the billing phone number you entered is correct, otherwise they will ask for it, and will ring it. You can receive the call, or the cardholder will, depending if you ATO'd the account correctly.

This is why orders get canceled when newbies enter a credit card order and expect to receive a free

iPhone from the Apple store. They are not fools and want to protect themselves. However, if you took care of changing the billing number on file, you will get the call and you will be able to confirm the order.

Not so fast, a call is not simply “is everything okay?”, but rather a verification call where they want to see if you are really the cardholder or not. They sometimes ask you for verification questions similar to Verid questions, but all the questions are taken from public reports. They can also ask you if you put the shipping address on file with the bank (you hopefully did), and they will call the bank to verify. Also, in some rare cases, they can make a conference call with you and the bank, but you will be asked for the usual questions, which means last 4 of SSN, DOB, last transactions, etc.

If you are a newbie and just put some credit card information on a website hoping to get a free iPhone, you will just see the order passing to Canceled state without any details and you will not even get a call. This is the reason why people post threads about “carding does not work” and get the same answers.

If you passed the verification call, the representative will tell you that everything is okay and that they will have the order shipped out today. This is good news! At this stage, I received 100% of my items, I never had problems past the verification stage. Now you may be tempted to hit another site; resist to the temptation. Your ATO'd card can almost be considered a level 4 card, at you own the account and can do whatever you want, so it has a high sentimental value. Wait for the order to ship and the package to leave the merchant before you hit another webstore.

I recommend carding in the morning, to avoid letting a charge sit on the card for too long. You never know how often a cardholder checks his statement online. I had cards that died within hours, and other ones lasted 3 months. Once the package is shipped, you can card another store, no need to call the bank, as your drop address is already on file. Repeat until the card is burnt. Once it is burnt, never show your face at the drop again. The alternate address is on the bank's records and they can send Law Enforcement to this place. A drop is like a condom, use it once, do all your business, and trash it, because it becomes dirty.

Another verification step they can take is send you an e-mail asking for scans of your ID documents, such as passport and driver's license. These can easily be photoshopped and there are templates available everywhere. Utility bills are pretty easy to forge too, so don't worry about this part. Do what you have to do, but be quick.

Another step you can take, is to put the shipping name on the package to a family member of yours, for example if the cardholder's name is James Latyon, send the package to a certain Harry Layton (find a name that's on the report and have their DOB, in case) and say you are sending the package to your son / brother / whatever relationship you have on your report.

Also, keep in mind that no method is perfect, and the website can cancel the order simply because they feel it is not safe to process it. Nothing is perfect, but if you ATO'd the account successfully, it should be easy. Remember to stay under \$2000 per order. You never know what other tricks they may use to catch you.

Always choose the fastest shipping method. Some say it raises flags, but if you did everything else correctly, that will not be the reason why your order fails. Besides, it greatly reduces your chances of getting an intercepted package, which is a pain in the ass and makes your efforts worthless.

This brings me to the topic of finding a drop to ship your order to. You can ship it to your house without any problem, if you want the police to knock at your door and make you ride dirty to the

police station, and get in a steaming pile of shit of trouble. So read on to find out how to ship your order safely.

## **ONLINE ORDER / PAYMENT [RED FLAGS]**

Over the years, We've come across dozens of procedure lists for top-tier merchants regarding online transactions and fraud reduction. I'll detail several companies verification procedures below.

While most virtual carders are aware of the various procedures in place to verify orders placed online, few actually understand the implementation of fraud scoring, and the order in which these verification methods are used.

### **The Risk Management Toolkit**

- AVS
- CVV
- IP/GEO/BIN
- Cardholder Authentication (VbV/MS)
- Phone Verifications
- Manual Order Reviews
- Chargebacks & Representments
- PCI Compliance & Data Security

### **AVS - Address Verification Service**

#### **How It Works**

- Provides a Match or Non-Match Result for only the Billing Street # and Billing Zip Code... not the actual address. (i.e. "1234 Test Street" is parsed into "1234" just the same as "1234 Wrong Way" would be).

#### **Implementation**

- Available on any Internet merchant account and virtually any Payment Gateway.
- Most gateways provide an AVS configuration area where you can specify whether you want to automatically "decline" (i.e. do not settle) an authorization that has an AVS mis-match or non-match.

#### **Benefits**

- Easy to implement Limitations
- Works only for U.S., CND, U.K. cardholders so this does not help you scrub most international transactions.
- A growing % of compromised credit cards – especially those obtained through inside jobs or hacked databases– will also contain the necessary information to provide a valid AVS match result.

#### **Recommendation**

- If you handle a mix of int'l and U.S. sales, you will want consider scrubbing with AVS on the U.S. transactions but do NOT scrub via AVS for any international transactions as they will always fail. AVS should not be considered a primary means of verifying the validity of a transaction. Nearly 20% of the fraud can potentially be eliminated by scrubbing "Non-Matched" AVS match results.

## **CVV – Card Verification Value**

### **How It Works**

- A service with many names – CVV2, CVC2, CID – but the premise is the same for all.
- Provides a Match or Non-Match Result for the 3-digit or 4-digit number embossed on the back of the cardholder's card. The CVV is NOT generally encoded on the magnetic stripe and therefore is less likely to be captured as part of a card skimming tactic.

### **Implementation**

- Available on any Internet merchant account and virtually any Payment Gateway.
- Most gateways provide an CVV configuration area where you can specify whether you want to automatically "decline" (i.e. do not settle) an authorization that has an CVV non-match or non-entry.

### **Benefits**

- Works for virtually ALL cardholder accounts – both U.S. and international.
- There is no valid reason why a legitimate cardholder, in possession of the card, would not be able to enter a 100% matching number for this.
- Merchants are not allowed to store CVV and as such the CVV # is less vulnerable than the data used for AVS.

### **Limitations**

- CVV data can only be used for a real-time transaction. CVV data can not be stored and therefore can not be utilized for Recurring Transactions.

### **Recommendation**

- CVV is a recommended service to utilize for ALL initial transactions processed. Based on our internal charge-back analysis, merchants can reduce their fraud rates by as much as 70% by simply requiring a matching CVV result.

## **IP/GEO/BIN Scrubbing**

### **How It Works**

- Compares the IP address of the customer purchasing with their stated geographic location (i.e. why is the customer from California ordering from Europe?)
- Compares the BIN # (first 6 digits) of the credit card with the IP or stated geographic location of the customer (i.e. the customer is using an US-issued credit card but they are from Europe?)

- Based on the IP and BIN # and other customer-inputted data, a vast amount of information can be returned on the transaction.

## **Implementation**

- Custom direct integration into a service such as MaxMind.com
- Use an existing integration that is part of a Shopping Cart such as X-Cart, LiteCommerce, osCommerce, ZenCart, ASPDotNetStorefront.
- Use an existing integration that is part of a Billing System such as WHMCompleteSolution, ClientExec or Ubersmith.
- Use an existing integration that is part of a Payment Gateway such as the Quantum Payment Gateway.

## **Benefits**

- Fast, Cost Effective and Non-Intrusive
- Provides merchants with an excellent “do the pieces fit consistently?” analysis.
- Can block up to 89% of all fraud if properly implemented

## **Limitations**

- Generally not reliable for AOL users due to the way that AOL routes its traffic (AOL users require a merchant-specific approach)
- Proxy database is always in a real-time process of being updated as new proxies open up.

## **Recommendation**

- IP/GEO/BIN fraud scores should be used in the order evaluation process more as a means of flagging transactions as “high risk” for more intensive scrubbing vs. being an outright decline.

Examples of what IP Geo-Location can tell you:

## **YELLOW ALERTS**

- Free E-mail Address: is the user ordering from a free e-mail address?
- Customer Phone #: does the customer phone # match the user’s billing location? (Only for U.S.)
- BIN Country Match: does the BIN # from the card match the country the user states they are in?
- BIN Issuing Bank Name: does the user’s inputted name for the bank match the database for that BIN?
- BIN Phone Match: does the customer service phone # given by the user match the database for that BIN?

## **RED ALERTS**

- Country Match: does the country that the user is ordering from match where they state they are

ordering from?

- **High Risk Country:** is the user ordering from one of the designated high risk countries?
- **Anonymous Proxy & Proxy Score:** what is the likelihood that the user is utilizing an anonymous proxy?
- **Carder E-mail:** is the user ordering from an e-mail address that has been used for fraudulent orders?
- **High Risk Username/Passwords:** is the user utilizing a username or password used previously for fraud?
- **Ship Forwarding Address:** is the user specifying a known drop shipping address

### **IP/GEO/BIN Scrubbing (Continued)**

**Open/Anonymous Proxies:** an open proxy is often a compromised “zombie” computer running a proxy service that was installed by a computer virus or hacker. The computer is then used to commit credit card fraud or other illegal activity. In some circumstances, an open proxy may be a legitimate anonymizing service that is simply recycling its IP addresses. Detecting anonymous proxies is always an on going battle as new ones pop up and may remain undetected for some time.

26% of orders placed with from open proxies on the MaxMind min Fraud service ended up being fraudulent. Extra verification steps are strongly recommended for any transaction originating from an open/anonymous proxy.

**High-Risk Countries:** these are countries that have a disproportionate amount of fraudulent orders, specifically Egypt, Ghana, Indonesia, Lebanon, Macedonia, Morocco, Nigeria, Pakistan, Romania, Serbia and Montenegro, Ukraine and Vietnam. 32% of orders placed through the MaxMind min Fraud service from high-risk countries were fraudulent. Extra verification steps should be required for any transaction originating from a high risk country.

**Country Mismatch:** this takes place when the IP geolocation country of the customer does not match their billing country. 21% of orders placed with a country mismatch on the MaxMind m\*\*\*\*\* service ended up being fraudulent. Extra verification steps are recommended for any transaction with a country mismatch.

### **Results that speak for themselves:**

**ChangeIP** – is a DNS and domain name registration provider. The company provides free and custom Dynamic DNS services to more than 50,000 users. Before implementing MaxMind, ChangeIP was losing as much as \$1,000 per month because it sold instantly delivered digital goods and could not recover the losses if the purchase turned out to be fraudulent. After implementing MaxMind, losses were reduced by 90%.

**MeccaHosting** – is a Web hosting company based in Colorado. Since integrating MaxMind, Mecca Hosting has not received a single chargeback. On average, 12-15 fraudulent orders pass through the in-house checks each month but are flagged by MaxMind. Over the last 5 months, this has saved MeccaHosting at least 60 chargebacks and \$6,000 in unnecessary costs.

**Red Fox UK** – is a Web hosting provider and software development company based in the UK which offers solutions for small and medium sized businesses all over the world. By using MaxMind, Red Fox UK was able to increase its revenue by 4% while reducing its chargebacks by 90%.

**365 Inc.** – is a digital media and e-tailer specializing in soccer & rugby with a large international

customer base that processes over 10,000 transactions per month. By integrating MaxMind, chargebacks were reduced by over 96% from more than \$10,000 per month to less than \$500 per month. At this point, most charge backs are general order disputes as opposed to fraud.

## **WHAT TO CARD**

Go for things they won't expect a carder to hit. So things like Small Electronics, Cloths, kitchenware, kitchen appliances, toys etc. It's the things this you would not really expect someone to card. You would also be surprised at the price you can sell these for.

## **HOW MUCH SHOULD WE CARD?**

When it comes to thinking about how much to card in a transaction, I always keep the first Transaction at \$175 to \$325. Now you spent about \$70 getting all setup, you want to at least make your money back. So you buy an item for \$270 and with the right platform to sell it on, you can sell it for about \$220. That's the profit of \$180.

Once you have made a bit of money you can start to experiment with different BINs different sites and then also with varying amounts.

Also, Once you receive an order from a certain Website, you can try to go for them again, as you know your setup worked the first time you just have to repeat and if the card is live with a good balance then it is easy picking.

## **HOW TO CARD- BASIC – NOOB METHOD**

### **From PC**

1. Make a email (gmail, hotmail ) with CC matching name. If CC name Hackerz home then make like john.doe1998@hotmail.com
2. Run Remote Desktop Connection and connect with your RDP Host. if u dont use rdp then do the following steps in your pc
3. Run MAC address changer, change all MAC address.
4. Run CCleaner. Analyze and clean.
5. Set socks5 in Mozilla firefox.
6. Restart Firefox and goto ? [www.check2ip.com](http://www.check2ip.com) and check your ip is blacklisted or not & as same as CC holder address.
7. Now open shopping site. I want to recommend a website shop from your country. Why? Because you dont need to wait a lot for you package
8. Register with credit card holder information, name, country, city, address, and email you made one just for this order.
9. Choose your item & add to cart. Never choose big amount first. Try to card small amount item first within \$500.



10. In shipping address enter your address or your drop address, where u want to deliver product.
11. Go to payment page, choose Credit Card as payment method
12. Enter your CC details. Like CC Number, CC holder name, CVV/CVV, Exp. Date. Dont copy ➡ paste info. Type it one by one. Cause most site have copy-paste detector script)
13. In Billing address enter CC holder address. Now proceed to payment.
14. I'm sure if you do everything right then order will be successfully placed ? ?
15. Wait for order to arrive to your shipping address. When they arrive the corier boy will call you. The ask for any ID card. If you can make fake ID card then good. Otherwise show your any ID card (Adhar Card, Voter ID, College ID card)

## HOW TO CARD FROM MOBILE

Though I don't prefer carding from mobile. But if you follow belowsteps carefully then you can do that.

Basic requirements for carding from Mobile :

1. Mobile must be rooted. (offcourse I prefer any Android smartphone)
2. You must install few apps : IMEI changer, Phone ID changer, Android ID changer, Proxy Droid, CCleaner (apkpure.com has them all)
3. You can use HMA VPN for carding in mobile.
4. You use SOCK5 proxy with Proxy Droid apps.
5. You must change IMEI, Android ID, Serial Number etc everything before starting carding.
6. Now connect proxy droid with SOCKS5 proxy and connect it.
7. Now follow all steps of carding that mentioned above...

Ok, so you got your cc, your drop and try to be anonymous as you can make yourself.

## TUTORIAL FOR CARDING INTERNATIONAL SHOPS

Requirements:

- Creditcard
- Mozilla Firefox

install this firefox extensions:

<https://addons.mozilla.org/en-US/firefox/addon/change-geolocation-locguard/>

<https://addons.mozilla.org/en-US/firefox/addon/ghostery/>

- Gmail Account
- SOCKS
- Mac Changer

Change your IP using VPN and change it to your VICTIM'S Location

Go to <http://check2ip.com/> ( IP SHOULD NOT BE BLACKLISTED AND YOUR INTERNAL IP SHOULD NOT SHOW)

IF YOUR INTERNAL IP SHOWS UP FIX IT --> <http://check2ip.com/htr.htm>

Check Victims address with google maps  
<https://www.google.com/maps>

Change your locaiton if it is correct with this <https://whereamirightnow.com/>

Turn on your Ghostery

Open CCleaner -> Custom Clean -> Applications -> CHECK ALL BOXES ON FIREFOX -> Run Cleaner

Ready your GMAIL ACCOUNT.

Ready your FRESH AND VALID CC

Open a new tab for your target site.

Read Tips and start carding your item.

TIPS:

Don't use copy & paste (type manually)

Don't be greedy

Don't checkout too fast

Act cool just like a read card holder

Know your credit cards limit per transaction

Test first on low value items before carding huge value items.

You should know first if the site is VBV or not.

You shoud know what type of card to use on VBV sites.

## **TUTORIAL FOR USING GEOLOCATION EXTENSION**

1. Get the Coordinates of your Victim (It's latitude and latitude to get the coordinates Search the Address via Google Maps or visit: <https://www.latlong.net/>)
2. Go to extensions click on → options in change geolocation (location guard)
3. Copy and paste the coordinates to your extension
4. Check your location if it is correct with this : <https://whereamirightnow.com/>
5. Yoor good to go

## **NETFLIX CARDING TUTORIAL APRIL 2020**

Requirements:

- CC
- SOCKS
- OTP (any trash number, 2nd is good enough)
- Email

Use your region IP so if they need OTP, you can input your number. You need no OTP, but sometime they asking.

As I said, use your number because it doesn't work with random-sms-receiver. But maybe worked if you have paid-sms-receiver service.

Connect to SOCKS from city of CC holder

Register netflix, fill email with your mail (use email like first and last name of cardholder)

Choose what service you wanted & Fill name information

Use what real name look like, don't use name like 'Uzumaki Naruto' or any weird name.

Place card number you've got.

If declined, use another card number.

**If account blocked:** clear browser data, change MAC Address & repeat step.

**If worked:** chill back and sell your netflix account or share your friends (or for u)

## HOW TO CARD WESTERN UNION

If your always broke like me and you need cash right away the first thing you have to have is 2 valid cc's. You will need 2 because you need 1 to do the actual western union transfer and another to get the tools nessisary to do the transfer. 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 investigation 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 forwarding 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 effect "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 forwarding 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 through 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 investigation. 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 forwarding service I use is accessline.com

## **WHAT IS DUMP & HOW CAN WE CASHOUT THEM**

Dumps are used by carders to clone real cards and then use the clones as the genuine. So, those clones are duplication of the real cards and can be used like the real cards. How is it possible? The answer is Dump!

So what is dump? And here is the answer. Dump is a bank data connected to a bank account and encoded to the magnetic strip of the bank card. So each card is attached to a bank account. The card is a terminal which allows the account owner to access his account fund without necessity to walk into the bank. Cards can be used with ATM or POS, this are also bank terminals. So if someone gets access to the information stored in the magnetic strip of the card then he has full access to the owners card account and the money saved in it.

That is not difficult to steal a dump from the card. Dumps obtained by skimming, sniffing or hacking. So each and every time a person pay with the card he or she assume the risk that the card data could be stolen.

Bank dumps have usual 3 tracks, but if any of the 3 tracks is correct and there is a sufficient quantity of funds on account then the card is good to be used and the requested transaction can be approved.

Track 1 is the only track of the card which contains the holder name. Carder use to change the name from the track to match with the fake ID's they have or with the name embossed on the plastic. This track is written with code known as odd parity or DEC SIXBIT.

Track 1 format is

B5466160081187237^SHORT/JAMES D ^140910100000023001000000415000000

**START SENTINEL** = is 1 character, usual %

**FORMAT CODE** = a single character, financial cards format code is B  
**PRIMARY ACCOUNT NUMBER (PAN)** = usual is the card number, but not always  
**FIELD SEPARATOR** = financial cards use a single symbol for it which is ^  
**NAME OF CARD HOLDER** = contain 2 until 26 characters  
**FIELD SEPARATOR** = symbol for it is ^  
**EXPIRE DATE** = in format YYMM (year, month)  
**SERVICE CODE** = three characters  
**DISCRETIONARY DATA** = which may contain PIN VERIFICATION KEY (it is not the ATM PIN), card verification value, CVV  
**END SENTINEL** = is 1 character, usual ?

Track 2 it is the track developed by the banking industry and it is most important track of a dump. Almost all dumps will work if this track 2 is correct. It is written with a 5 bit-scheme, 4 data bits and 1 parity.

This track data format is

**START SENTINEL** = is usual 1 character ;  
**PRIMARY ACCOUNT NUMBER (PAN)** = usual the card number  
**SEPARATOR** = usual symbol = is used  
**EXPIRE DATE** = in YYMM format  
**SERVICE CODE** = a three digits code  
**DISCRETIONARY DATA** = which may contain PIN VERIFICATION KEY (it is not the ATM PIN), card verification value, CVV  
**END SENTINEL** = usual the symbol ?

Track 3 is virtually unused by the major world wide networks. It was developed by Thrift Saving Industry. Points Of Sales does not read this track.

## **SERVICE CODE**

The card service code is a 3 digits code present in both track 1 and track 2. Each of 3 digits of the code has a meaning and reading this digits together as a service code let us know where and how the card can be used.

### **If the first digit is:**

1= Card is for international use  
2 = Card is for international use but has chip  
5 = Card is for national use  
6 = Card is for national use but has chip  
7 = Card is not good for interchange except for bilateral agreements  
9 = Test card

### **If the second digit is:**

0 = Card is normal, without restriction  
2 = Issuer must be contacted via online means

4 = Issuer must be contacted via online means except under bilateral agreements

**If the last digit is:**

0 = No restriction but PIN is required

1 = No restrictions

2 = Card can be used for goods and services payment but not for cash

3 = ATM use only, PIN is required

4 = Cash only

5 = Card can be used for goods and services payment but not for cash but PIN is required

6 = No restrictions, PIN should be used where is feasible

7 = Card can be used for goods and services payment but not for cash but PIN should be used where is feasible

So, the card magnetic strip or/and chip contain all the information to access and operate a bank account connected to this card. If someone copied a card magnetic strip, that person can use a machine called MSR, Magnetic Strip Reader-Writer and write the data from the card to another card and use the clone as the genuine card.

If you think that it is hard to copy the magnetic strip to a card you must know that a simple swipe to a mini MSR or the swipe of card in a compromised POS is all the carders need to get the data from the genuine card and get the access to the card owners account. So it's easy to start the business.

Be aware of police and have a nice day.

**HOW TO DECRYPT DUMP (TUTORIAL)**

So, the dump of our map consists of three tracks. On the card we will write only the first two, as the third is used in discount cards and affiliate programs, and on Bank cards in 90% of cases is empty.

Buying a dump from the seller, we get a set of symbols of the following type (colors for clarity):

**448343 0123456789=1406101 156780000**

At first glance, just a set of numbers, but it can tell us a lot

1) The First digit gives us information about the payment system. So, the number 3 means that before us the card American Express, 4-Visa, 5-Mastercard, 6-Discover

2) The First 6 digits highlighted in red-BIN gives us information about the Bank that issued the card, its type (credit or debit) and category (classic, gold, platinum and many other options).

In this example, I specifically took an existing bin so you can see the information yourself, for example here:

Free BIN/IIN Lookup Web Service - [binlist.net](http://binlist.net)  
[www.binlist.net](http://www.binlist.net)

3) All together 16 digits before the equal sign form the card number, the one on the front side

4) The " = " Sign carries no information, just a separator character

5) The First 4 digits after the equal sign are the expiration date of the card, in the year/month format. Our card is valid until June 2014.

6) Then comes the service card code, three characters, but a lot of information.(Like above)

**The First digit determines where the card can be used:**

- 0 - Reserved for future use
- 1 - For international use
- 2 - For international use, with restrictions
- 3 - Reserved for future use
- 4 - Reserved for future use
- 5 - For internal use only, except as agreed in advance
- 6 - For internal use only, except as agreed in advance, with restrictions
- 7 - Not for payment, except for pre-agreed agreements
- 8 - Reserved for future use
- 9 - To check

**The Second digit defines the terms of use and authorization of the card:**

- 0 - Transactions are carried out according to standard rules
- 1 - Reserved for future use
- 2 - The transaction is carried out by the emitter, must be online
- 3 - Reserved for future use
- 4 - The transaction is carried out by the emitter, must be online, except for pre-agreed agreements
- 5 - Reserved for future use
- 6 - Reserved for future use
- 7 - Reserved for future use
- 8 - Reserved for future use
- 9 - Reserved for future use

**The Third digit defines the services and conditions of the PIN requirement:**

- 0 - No limit, need PIN
- 1 - No restrictions
- 2 - Goods and services (not cash)
- 3 - Only ATM and need PIN
- 4 - Only money
- 5 - Goods and services (not cash), you need a PIN
- 6 - Unlimited, PIN on demand
- 7 - Goods and services (not cash), PIN on demand
- 8 - Reserved for future use
- 9 - Reserved for future use

7) Forth goes the Intel directly for Bank, and us she essentially not is important, but for common development: 1-code availability of PVV, 5678-himself code PVV, 0000-code CVV/CVC (not cvv2, namely cvv, now not is used, usually there simply zeros)

Ah here is, with the second track figured out. And now on the example of the card I will show how the second track without any sites/programs, generators will receive the first.

So,

1) Take the second track

4483430123456789=1406101156780000

2) Add the front Latin B (says that our card is Bank)

B4483430123456789=1406101156780000

3) Instead of " = "insert the construction" ^LASTNAME/FIRSTNAME^". I for example will insert the, you can write any (^UNEMBOSSSED/NAME^ if the card not nominal)

B4483430123456789^MADISON/DANIEL^1406101156780000

4) Add 6 zeros at the end

B4483430123456789^MADISON/DANIEL^1406101156780000000000

And voila, our first track is ready to be recorded on the map

Finally, I want to say: do not confuse the cards, write visa to visa, and MasterCard to MasterCard.

## CARDING WITH DUMPS

### What do I need for real carding?

For sure 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.

Computer-laptop is the best, as you can carry it with you on your laptop if you desire. If you don't have a laptop you can use your home P.C. but you should keep maximum attention to be secured till you can afford to get one. Of course you can't take home PC with you to your operations.

**Encoder** - If you look around most every has or talks about an MSR206 and it 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. For \$550.00 you get MSR206, Exeba Encoding Software and 50 loco or hico cards. Also UBUYWERUSH 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 into it. Nice to have if you want to take your laptop and encoder on laptop.

**Power Inverter** - Needed to run your encoder and nice to have if you're out for long period of time and laptop is dying. You can get these just about anywhere.

**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. Repeat - do not use your real information even once. There are some good vendors that are quick also. Just look under the reviewed vendor section for more details.

**Dumps** - Get them from the carding shop who sells dumps. 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 works 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 dumps shop both. 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 B41000000000000000000^JOHN/GREEN^0409XXXXXXXXXXXXXXXXXXXX

Track2 41000000000000000000=04091XXXXXXXXXXXXXXXXXXXX

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 it, it's not the good 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 we 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.

**Anonymous 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 we suggest 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. 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. You or somebody wha can 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. Be calm in any situation.

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** - we would suggest staying away from gas stations. Most of them have cameras and why risk someone getting your car info for such a small purchase. Plus some dumps will die quickly when using in 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 we're not going to post which stores do and don't 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 you're 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 we 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 happens you can exit store go in opposite direction and loop around behind the store to your car. Unless you're 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 health 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 appearance.

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 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 your 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 your 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 your 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 their hand.

What to stay away from - If you are new don't try carding a laptop right away. Start small, we 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. good luck and lots of \$\$\$.

## **DUMPS VS CVV**

This is a description of difference between types of dumps and their using. Some people don't

understand the difference between online and instore carding and between CVV and regular DUMP.

## WHAT IS ONLINE CARDING

Online carding is the carding which is done from computer with the help of internet. No matter - online shopping, affiliate marketing, online games with cashback, if is done from computer is called online carding. To do online carding carders use CVV, CVV2.CVN or FULLZ details. When carders buy cvv or fullz they're getting following:

1. Card number
2. CVV card number verification value
3. Card expire date
4. Card real holder name
5. Card real holder address including building number, city, country, zip postcode
6. Card holder phone number (optional)
7. Card holder e-mail address (optional)
8. Card holder SSN (fullz contain this detail)
9. Card holder DL (fullz contain this detail)
10. VBV password (only some fullz contain it)

This so called CVV or FULLZ are used ONLY for do online jobs such as, for example online shopping. You can't use this details to encode preprinted plastic and swipe the card in mall.

**Conclusion is that CVV or FULLZ IS FOR ONLINE CARDING ONLY!**

## WHAT IS INSTORE CARDING

Instore carding is the carding which uses dumps and card clones. Carders who do instore carding encode dumps to the preprinted magnetic strips of cards and go into stores for shopping.

Dump is the data encoded to the the magnetic strip of a card. Dumps may come with 1 or 2 tracks. Dumps can't be used for any online job!

**Conclusion is that DUMPS ARE USED FOR IN STORE CARDING**

## INSTORE CARDING TUTORIAL

Here is an instore carding tutorial for you our friends.

This tutorial is just to start you off with instore carding, most basics and a few tips. Before we start, let's discuss carding terms I will use throughout this tutorial.

### 1. Dumps

Dumps are tracks 1 & 2 or only track2, no adress, no name, no nothing. Just 2 lines of numbers/signs. Here's an example of what you will get when you buy a dump from a vendor:

```
%B426429XXX5504545^JOHN/WANE^110710100000000000000000000000000869011000;426429XXX5504545=11071010000086901100
```

Everything before the ";" is track1, so:

**T1:**

**T2:** 426429XXX5504545=11071010000086901100

## 2. Plastic

Plastic refers to the fake cards that many plastic vendors make to match your dump, meaning they will emboss your dump's numbers as well as the desired name you want onto a blank (not-embossed card). You'd be surprised at the quality of plastics, most cashiers can't differentiate a fake from a real one (unless you have really low quality plastic or the cashier is deep into this).

### 3. 101/201 dumps

What is the difference between 101 and 201 dumps? Well it's very simple: 101 is swipe only and 201 is with chip.

Now you're going to ask: But how am I going to pass a 201 chipped card without knowing the pin? Well there are places for that, especially POS machines that swipe 201's (meaning they dont insert them). You will have to find spots on your own.

Alright, now that we've learned the different terms I will use throughout the guide, here starts the interesting stuff.

There are a lot of ways to do instore carding but basically it comes out to this:

- Hitting it random.
- Insider carding.

Hitting it random: This means you have GOOD quality bank plastic that should include these minimum: good holo, UV marks, tipping, matching numbers. Where i'm located sig stripes don't matter because people are a bit late on this. You will be going into any store and hitting it.

Insider Carding: This is the safest way to go. You will need a connection working inside a store who will let you pass cards. So matching plastic is not a must here and usually you can get away with alot and not look suspicious at all. I suggest you do this to get your funds up to buy machinery for random hitting (or affording strikers).

## POS Types and why you should read this.

There are many POS systems and alot of them are different one from eachother. You will need to know the ones that are easy to swipe and the ones that are slightly harder.

Some POS systems will ask to enter the 4 last digits of the card number, so matching numbers is a must for these. Even with an insider, he must enter the matching numbers or else payment won't go through (you can write them on a piece of paper and let him enter those digits dough).

Other POS' will ask to enter the cvv2 (3 security digits on the back or 4 for Amex) before even swipping the card. Keep in mind that dumps bought on the internet don't contain the cvv because it is encrypted in Track2 and very hard to decrypt (different algorithm for every bank). So if you want cvv2 matching, you will need to skim the dumps and check yourself and note them. Usually big stores have this, for example: The Brick, Future Shop, Best Buy etc...

There also are POS systems that won't let you insert 201 (chipped) cards. These POS's are good to keep in your book because sometimes, the bins or country you want will be out of 101s and you'll get stuck with 201s and you can hit them with these POS's. So they swipe the chipped card, no inserting nor pin required. A good example is Wal-Mart or Blockbuster, only the ones who have a

black pad as a POS with a screen for signature capturing (they have an insert slot but they don't use it).

## HOW TO GET DUMPS

Getting dumps isn't really hard. There are 3 ways to get dumps:

**1. Hacking:** Pretty simple, you hack POS systems for dumps with either malware or logging system. This is for advanced hackers because you will have to code the malware and test it on a POS you will buy yourself. Not experienced in this, can't tell you much.

**2. Skimming:** There is online and offline skimming. You can use pagers and mini-readers too. It would be wiser to invest a bit more and get d+p with an offline.

Two previous ways are not simple. The fastest and most simple way - is to go to online shop where you can chose the stuff by parameters you need:

**3. Buying:** Many vendors sell dumps online, but you will need to find good forums (a forum with russians is always good). Use escrow when possible on forums. Stay safe, don't get ripped, use LR to buy 2 test dumps. If the guy says 10 minimum then make sure he is legit before doing a transaction (and good vendors usually accept escrow and sell test dumps). Try to check if the online store u're buing dumps is not a ripper copy of real store - many rippers are making the copy of famous shops on same-looking domains. Try to chat with shop support. So here on antigreedy we sell good cheap stuff - you can check.

### Bin Selection:

Many people have fuzzy perceptions about BINs. Bins are the first 6 digits of any dump. It represents the financial institution it is from as well as the location of this specific branch and the type of card the dump is.

Usually, people have binlists they personally craft (you should too) to find the best ones. Special bins and hard to find bins are sought after because they usually have special characteristics like these:

- They die slower, so when a base is almost dead, these are still approved.
- They are not region-locked.
- They have high limits
- etc...

There are 2 ways of buying dumps using bins:

### 1. Selective Bins:

Meaning you will ask dump sellers for specific bins that you are after and buy them. One major flaw I have discovered (where I live) is that when I buy 10 pieces of the same BIN and use 3-4, the rest of them all become HOLD-CALL. I don't really know when that seems to happen, but maybe it's because they disable that bin in your area or something.

### 2. Random Bins:

Usually not recommended because vendors give you the shittiest bins. But when you're buying big amounts, it's good to mix it up, you find new bins that are good for you.

### **What to do with dumps? Equipment needed?**

After you have your dumps, you can encode them on bank quality plastics to use them.

You will use an MSR encoder (reader/writer) to encode the tracks 1 & 2 (3 is never used on a cc) on the card. Don't ask me how to use it, when you will open the box you will know how to use it. I'm serious, retarded people can figure it out.

Ok, about MSRs too: THEY ARE ALL THE SAME, EVEN THE CHINESE ONES. If they work and you didn't get scammed, then any model is good. I myself have owned 206, 905 and the 605 and I use the 605 all the time despite how popular the old 206 is.

### **Other equipment that is good investment are these:**

Embosser + Tipper Set: This is a worthwhile investment because non-embossed blank plastics cost 10-15\$ in bulk and embossed are up to 40\$ a piece if individually bought. They are very easy to operate, don't worry. Don't need to be a genius to use them.

Card Printer + Holos: This is for usually for people who have a big operation or want to sell blanks/embossed plastics. I have never owned one because it's too much machinery and it's very expensive (2.5 grans upwards if you want a decent one). Going with blanks is better for me.

Pagers (mini123 etc...): These are good because if you know anyone who works in a fancy restaurant where they pass your card in the back, you can give him a pager that records up to 2000 dumps (like you'll ever get that in a day) and swipe it there before swiping it on the POS and even noting down the cvv2 in the back for better hits.

### **How to properly hit a store**

Hitting stores is pretty easy, but it's a pain in the ass if you have just started or you're nervous or shy because you will have to act like you are the cardholder. Don't dress up like a thug or a kid, wear classic clothing, no matter how gay you think it is (if you already wear classic, then sorry I offended you).

\*Always know what you are getting before entering, make out a scenario and plan it wisely.

Another important part is finding the stupidest or newest cashier. Some cashiers will look at your card and verify it and some even call the manager to come check it. Some jewellery shops even call the toll free bank's number on the back of the card to verify it's legitimacy. So find the youngest/ugliest/caldest girl or the most fucked-up/black/stoner guy because they usually are too naive or don't give a fuck.

### **F\*CK IT GOT DECLINED/HOLD-CALL**

Don't worry, plenty of people have it happen randomly to them.

**Decline:** it means something is wrong with the card, but not exactly stolen, so they don't know what's wrong with it but it's declined. Just tell them you'll call the bank and walk away. No one will

chase you lol.

**HOLD-CALL:** Now this is where it gets shakier, this means the cashier has to hold the card and call the bank. What I usually do is tell them ill call the bank later because im in a rush but keep the card. This means something is definitely wrong with your card.

## **FREE IPHONE TUTORIAL (VERIZON WIRELESS)**

### **What you will need:**

- Profile (650+ credit score)
- Fake ID (must be scannable)
- Netspend prepaid debit card, registered in profile's name (to get a netspend card, go to any local grocery store or pharmacy, find it in the gift card section, load the amount of money that you need on the card in cash at the register...ex. your down payment for the phones is \$125, go to the store, buy a netspend, load \$125 in cash at the register, and then activate the card online.)
- Phone number to receive SMS codes. Can be any number!

### **Now that we have all 3 of these things, we are ready to start...**

(Important note: The profile and the fake ID MUST MATCH! If you are getting the phones shipped, make sure your DROP ADDRESS is on your ID, if you are picking them up in store, make sure the PROFILES ADDRESS is the one printed onto the ID. In terms of the phone number to use, you can use your own personal phone number, use a VOIP service, or just buy a burner phone. DO NOT use google voice.) ...we will be covering both shipments and in-store today.

### **Method (Shipments)-**

The first thing you want to do, is create an email address in the profiles name. Once you've done that, go ahead to Verizon's website and create an account using the email that you created and the PROFILE'S info. Of course the phone # you input will be whatever number you've chosen that you have FULL CONTROL over. Once the account is created, we are going to head over to the iPhones we want. Now, regardless of how good your profiles credit is, you're NEVER want to exceed more than 2 phones on your first try. If you try to do anymore than 2 phones, they will find a way to shut you down, so it is important that your first order is only for 1-2 phones. Once you have the 2 phones in your cart, you're going to want to "proceed to checkout". Here, you will be asked to do a credit check, in which you simply enter in the profiles details, and click "complete". If the profiles credit is good enough, you should get a message saying that you've been approved for \$0 down, or it will say you've approved for monthly financing. Either way, this is what we want. The down payment price of each phone should only be \$75 per phone (iPhone 11pro max 256gb). If your screen says anything different, you must get a new profile and start over, but if your profile has good credit, there is no question that you will be approved.

Once you are approved, you want to click "continue to checkout". At this point you will be asked to input a payment method. Now, this is where it gets a bit tedious: Since we are getting the phones shipped, we are going to need a profile of a person who is no older (younger) than 21. This is because younger people don't have as many addresses on their credit report, allowing us use any address when we are registering to get our phones. With this being said, we are going to register the netspend card that we previously bought, in the profiles name and info. The ONLY info that we are going to change, is the address portion. When it says to enter an address, enter in your DROP! Not the profiles address. The reason for this, is because when we enter the payment method into Verizon, the address of the card and shipping address must match up. Once we have our Netspend



set up this way, we are ready to make the purchase. Simply enter in the card details of the Netspend, and click confirm. The payment will 100% always go through, and you will be greeted with a window that says "Approved. Thank you for choosing Verizon."

Now, we are not done yet. Wait about 30 mins to 1 hour, and you will receive an email from Verizon, asking you to send a picture of the front and back of your ID. Now, this part is very important to listen closely...If you open the email from your phone, you will be taken to a page in which it forces you to use your back camera to take the picture of the ID. If you open the email on your computer, you will have the option to upload an image from your files for the ID. So, basically, you're going to need a physical ID if you're running this operation from your phone. If you're running in from your computer, you will need a high quality scan, which is usually just a picture of a physical ID. (p.s. scanlabb, ssnlab and sites like this are garbage and WILL NEVER WORK! EVER!)

Now, since we are getting these phones shipped, you will have needed to put the DROP address printed on your fake ID, NOT the profiles address, Verizon will only ship to the address given on the ID.

After you send in the picture of your ID, wait another 45 mins to 1 hour, and you will receive an email saying that your identity has been confirmed! THIS MEANS WE'RE IN THE CLEAR! Right after you receive that email, you will receive another right after with the tracking details! Once you have received the tracking # email, you can now relax, the phones are on the way.

After you get your first order, you should be able to log back into the same account and get 2-3 more shipped out the next day. Or, you can buy the phones full price with a CVV, just make sure to ALWAYS use next day shipping.

(There is also another way to do this in which you ship to the profiles address and then go intercept the package at the door, but I find that method to be a bit of a headache even though it does indeed work.)

p.s. ONLY CHOOSE: Next day shipping before 10am....this will ensure that you get the phones the next day before 10 am...

Method (In Store)-

Now that you have an understanding of how Verizon works as a whole, and how shipments work, this next section should be a piece of cake for most of you. This section of the method deals only with in store pickup. It is pretty much the same process, except for a few details.

The ID (MUST BE PHYSICAL. Teslin/Poly-carbonate): Instead of having the drop address printed, you're going to want to get the PROFILE address printed this time...we are going full on identity theft, lol.

The Netspend: Register it in the PROFILE'S ADDRESS AND INFO.

Now, when we are on Verizon's website, we are going to follow the same steps as before. Just grab 1-2 phones at first, we can come back and get more later. Once the phones are in your cart, you're going to want to click checkout, do the credit check, pay for the down payment with your Netspend, but the only difference is, instead of picking the "Next day by 10am" shipping option, we are going to choose, "Instore pickup". Select the closest store to your location, or whatever store you wish, to pick up your phones. Once you pay the fees with your Netspend, it should only take 1-3 hours

before your order is complete and ready to pick up.

Walk in the store, let one of the workers know that you are coming in to pick up an order placed online: Show them the confirmation email that you received. They will then ask you for you ID and the card that you paid with. At this point, pull out your fake ID and Netspend, give it to the worker, he/she will look at it for maybe 5 seconds before giving it back. And dont worry about their being no name on the Netspend. They just look at the last 4 of card number to make sure it matches what they have on the screen. After you show them those 2 things, they will hand you your phones and you can leave. The process of going inside and getting your phones will take about 5-20 mins depending on if you have to wait in line.

In-store is my preferred method, but they can be acquired more than one way, as seen above...

I hope you all enjoyed the read. This is only my second method and I have already received such great feedback/seen such good results.

Let me know down below what sort of method you would like to learn about next...some suggestion would be nice

If there was anything at all confusing about this method, or if you have any questions at all, feel free to shoot me a message on here, or on Telegram: kingasos

(NOT WRITTEN BY ANYONE IT'S FROM A CARDING FORUM!)

## **HOW TO CHANGE BILLING ADDRESS ON FULLZ.**

Ok, so you went along and bought some UK Fullz and you find the site you want to card but they only ship to the billing.. And you really wanted those pair jeans which makes you mad and frustrated. Well here is the answer:

### **What you need:**

- Uk Fullz (Full Name, Address)
- Your Drop Address
- 1 Runner (Somone who is going to go into the bank and get it done )

### **Optional:**

Fake ID, Wallet

NOTE: - This is a really high risky method, be careful, and get a good lawyer before, do not tell him anything but pay him good.

Ok, so you got the above and know your ready.

Find out what bank the Fulls are from (Lloyds TSB, Abbey, Halifax).

Know here is the really important part, your going to need your runner to walk into the bank and request his address to be changed your drop. Now when you walk in there your going to want to say that you recently moved house and that you need your address changed. Now there going to say insert your Credit/Debit card into the machine, pull out your wallet and say " Damn, never brought it with me " or you can say what I usally say " My missus has my credit card for the day, its her birthday ", something imaginative. Now there going to ID you, if you have some GOOD FAKE ID (Passport, Drivers Licence) then pull it out and show it to them, but as many of you won't just say " I

didn't think I will need it".

Now, there going to say can you please put your Full Name and Your Old House Address onto the paper, and below your new one so they can change it there and then. Well just do as they say and they will say can you please wait 5 minutes and have a seat. When they come back to you, they are going to say that your address was changed and is now active (Something along those lines, as different banks say different thing) when they say it is active just thank them and leave, or do what I always do which is just ask for the balance of my account and they should write that down for you..

Ok well that is it

Now that the address is changed to your drop, all you need to do is just card away.

Or, here is an idea for you all to try out ( Not going to write a tutorial as it is pretty easy ).

Get someone you know to walk into the bank and tell them that they have lost their card and pin, the bank will give them

a number to call to request a new card.

That's all. I'm happy to help you.

## **HOW TO CASHOUT CREDIT CARDS EASILY**

### **IMPORTANT : READ THE TUTORIAL BEFORE QUESTIONS**

Requirements:

- Onlinegame
- Proxy
- Creditcard

At first you have to register on an online game site, maybe where you can play poker or backgammon.

It is only important, that you can play with REAL MONEY.

Onlinegames like: Poker Online | Play Poker Games at PokerStars.com

You need 2. account. Ask any friend to help.

One of them must be your own and the second have to be like the Creditcard user.

To make account is in most onlinegames for free.

### **Prox**

Then join your Proxy... Its nice if you use the same Proxy like your creditcard comes from.  
for example : German creditcard and German Proxy .

### **Creditcard**

Now when you connect to the Proxy, join your faked account to play online...

Then purchase Real money from the hacked or stealed Creditcard.

Dont use your own Creditcard . It wouldnt have any effect Big Grin

### **How to Cashout**

Join the game with your Account (your faked and your real) to play.

You have to click on the "Play with Real Money" Button.

To play you need more than 2 players on the Table.

You can make more accounts to shit with all your accounts on the table but i played with some hackerfriends. So they knowed what i did.

Then Play Big Grin

IMPORTANT : Your real account need some real money too ... 10 Lira is enough Big Grin

Then your firends have to give up the round, so that only YOU AND YOUR FAKED account is in .  
Like 1 on 1.

Then Press the "All-In" Button with your faked Account .

And with your real Account the Same...

The effect : your faked account will set all the money from the hacked/stolen Creditcard  
and your real account will set 10 \*\*\*8364; or Lira or \$ . :clap:

Then your faked account have to lose... like give up.

So you will taken all the money and logout from the Game. :51:

Press " Cashout" to cashout your Money to your real Creditcard. Same Thread was already

## **HOW TO DELETE EVERYTHING FROM COMPUTER**

### **[WARNING: THIS DELETING ALL YOUR FILES !]**

If you are scared, that someone trying to follow your traces? Maybe Police?  
Then is this tutorial the best tutorial you can get

For this, we need a tool called "balenaEtcher", it's an rufus.ie alternative for linux, mac and  
windows you can also use rufus(windows).

<https://www.balena.io/etcher/>

<http://rufus.ie> (windows)

After we have download that, execute it, and select the iso file where you can get here:

[https://downloads.sourceforge.net/project/dban/dban/dban-2.3.0/dban-2.3.0\\_i586.iso](https://downloads.sourceforge.net/project/dban/dban/dban-2.3.0/dban-2.3.0_i586.iso)

Now select your USB harddrive, and burn it.

Boot your selected computer into BIOS, most keys to boot into BIOS:

del

f2

f11

f5

Google For Your Computer, you can view for computer information „computer info“ on windows.

In BIOS find "Secure Boot", and disable / custom it.

Then go to boot priority and do your usb harddrive as #1.

If you have done this, save and exit the BIOS it should reboot now, so now enter the DBAN, it will  
ask what you want to do.

You will see this:

**BOOT**

Enter this line now: (remember it's english keyboard in the dban boot menu)

**dban libdata.ignore\_hpa=1**

(for clearest clean, for example if you had viruses or so on)

Or you can type:

**autonuke**

(automatically clean)

After a while, select with [SPACE] your HDD.(it should select with "wipe"-)

**Type M for Method**

**Type R for Rounds**

**Type J for Up**

**Type K for Down**

If you do 7 times or more, it will need upto 3 hours.

F10 will start your wiping HDD

## **AMAZON CARDING FULL TUTORIAL**

[https://anonfiles.com/r3Sbp2u4o8/How\\_To\\_Card\\_Amazon\\_Full\\_Tutorial\\_pdf](https://anonfiles.com/r3Sbp2u4o8/How_To_Card_Amazon_Full_Tutorial_pdf)

## **SITES CREDITCARD GENERATORS AND CHECKER FOR SUBSCRIPTION CARDING**

### **SOME ARE DOWN SOME NOT**

- 1.- [https://www.elfqrin.com/discard\\_credit\\_card\\_generator.php](https://www.elfqrin.com/discard_credit_card_generator.php)
- 2.- <http://mohadu31.com/bin/>
- 3.- <https://namso-gen.com>
- 4.- <http://namso.ezyro.com/?i=1>
- 5.- <http://archive.li/gvfdN>
- 6.- <https://ia1000.com>
- 7.- <http://sourcebinccgen.ml/CCGENSBC1/>
- 8.- <http://sourcebinccgen.ml/CCGENSBC2/>
- 9.- <https://obtain-link.com/checker2/Index.php>
- 10.- <http://namsocc.net>
- 11.- <https://ccgen.srijo.tech>
- 12.- <http://www.b7k-checker.club>
- 13.- <https://tnb-generator.000webhostapp.com>
- 14.- <http://profetaschek.xyz/gen/>
- 15.- <https://holk.xyz>
- 16.- <https://www.ondroid.ga>
- 17.- <https://cccardgen.es.tl>
- 18.- <http://x-secret.net/ccgen/>
- 19.- <http://ad365.me/>
- 20.- <https://www.ccgen.mx>
- 21.- <https://cc.namsoelite.com/>
- 22.- <http://www.b7k-checker.club/>
- 23.- <http://hitlerccgen.com>
- 24.- <http://blckcardgen.xyz/~blckcard/>

25.- <https://cc.ajpro.ml/>  
26.- <https://www.ccggen.mx/>  
27.- <http://namsodebit.co/>  
28.- <http://vpncclub.ml/cg/>  
29.- <http://educapro.mx>  
30.- <http://namsopirates.xyz>  
31.- <http://www.bv1.tech>  
32.- <https://namso.gdn/gen/>  
33.- <http://www.beshoycc.com>  
34.- <http://safra.000webhostapp.com/cassa/>  
35.- <https://bin.isecurity.pw>  
36.- <http://virusteamdlg.com/gen/>  
37.- <https://namso5.com/>  
38.- <http://sourcebinccgen.ml/CCGENSBC3/>  
39.- <http://bingenerator.ml/>  
40.- <http://cc.zchecker.xyz/>  
42.- <https://www.ondroid.ga/>  
43.- <https://darrkfriendccgen.000webhostapp.com/>  
44.- <https://namso-gen.com/>  
Checker  
45.- <http://thor2cards.gq/ch/>  
46.- <https://obtain-link.com/>

## **SPAMMING – WHAT IS IT ?**

First of we will see what do we mean by term spamming.

Wikipedia definition:

Email spam, also known as unsolicited bulk Email (UBE), junk mail, or unsolicited commercial email (UCE), is the practice of sending unwanted email messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients.

In simple language spamming means to send bulk mails to people in order to flood there mails or to make them fool and make some real Shit.

## **WHY WE SPAM**

👑 To get Bank Logs by spamming different banks.

👑 To get cc,fullz.

👑 To get Accounts like paypals,dating sites etc.

👑 To spread our malware like zeus,keyloggers etc.

👑 To spam lottery scam aka 419 scams.

There are endless reasons to spam but these were some of common reasons for spamming.

Now we learned what is spamming and why we spam or for what purpose we spam lets learn

## HOW TO SPAM

Before we learn how to spam we need to know the meaning of general terms:

👑 Leads: Leads is the term used to refer to email list, its basically another name for the common term email list. Leads aka email list is list of email addresses of people we are going to spam.

👑 AMS(Advanced Mass Sender): It is a windows based tool which we used to spam, here we add our SMTP, load our email list aka leads, add email from which mail will be delivered for example if we are spamming chase bank we add email of chase bank like no- reply@chase.com and add our scam letter.

👑 Scam Pages: Scam pages is another name of the Phishing page, its basically a replication of the original page. Its used to get logs from our victims.

👑 PHP mailer: PHP mailer is a script which is used to spam our leads, this is another method of spamming. In this we don't use AMS tool, we spam via this PHP script.

👑 Cpanel: Cpanel is is the hosting panel of a website, in simple language it's a panel from where a admin of a particular site manages his/her website. We use cpanel to host our scam page.

**Now question arises why we don't used our own Cpanel host to host our scam page?**

The answer is simple hosting websites don't allow scam pages on there servers so we used hacked Cpanels to host our pages.

👑 SMTP (Simple mail Transfer Protocol): SMTP is generally an application which runs on a server which is used to transmit and receive emails, in simple language we use SMTP to send our mails to our victims.

## Methods of Spamming?

There are two ways of spamming:

- ★ Spamming Via SMTP and AMS.
- ★ Spamming Via PHP Mailer.

SPAMMING VIA SMTP AND AMS.

This method is divided into 2 parts.

- ★ First part is scam page uploading via cpanel.
- ★ Second part is loading leads to AMS, adding SMTP and start our spam

### **PART1: scam page uploading via cpanel.**

First of login to Cpanel

Now click on file manager

Now click on new folder and make a new folder named site and double click on the dir created site  
Now Click on upload

Now go back to your main cpanel page and refresh page and select file and click extract

Now we need to edit a php file where we need to enter our email id where scam page will send logs, its different in all case in my case its  
l0gx.php (Select file and click edit)

At the place of \$send = "ourmail@mail.com";  
Add your mail. It depends on scampage you are using.

Now after you have followed all the steps we will check that our page is working or not.

If your cpanel website is abc.com then you will access scam page from [www.abc.com/site/](http://www.abc.com/site/)

We successfully uploaded our scam page, now we will move on to second part of this method.

**NOTE:** Spamming is illegal as per laws so we should not spam from our own system.

For Scampages, and more of spamming contact me on Telegram:  
[@TheMasterCH](https://t.me/TheMasterCH)

## **PHISING TOOLS**

### **Best Phishing from 2020**

#### **Ghost Phisher – Phishing Attack Tool With GUI**

Ghost Phisher is a Wireless and Ethernet security auditing and phishing attack tool written using the Python Programming Language and the Python Qt GUI library, the program is able to emulate access points and deploy. The tool comes with a fake DNS server, fake DHCP server, fake HTTP server and also has an integrated area for automatic capture and logging of HTTP form method credentials to a database. It could be used as a honey pot and could be used to service DHCP requests, DNS requests or phishing attacks.

#### **Ghost Phisher Features:**

- HTTP Server
- Inbuilt RFC 1035 DNS Server
- Inbuilt RFC 2131 DHCP Server
- Webpage Hosting and Credential Logger (Phishing)



- Wifi Access point Emulator
- Session Hijacking (Passive and Ethernet Modes)
- ARP Cache Poisoning (MITM and DOS Attacks)
- Penetration using Metasploit Bindings
- Automatic credential logging using SQLite Database
- Update Support

Download:

<https://github.com/savio-code/ghost-phisher>

## **SPF (SpeedPhish Framework) - E-mail Phishing Toolkit**

SPF (SpeedPhish Framework) is a an e-mail phishing toolkit written in Python designed to allow for quick recon and deployment of simple social engineering phishing exercises.

### **Requirements**

- dnspython
- twisted
- PhantomJS

You can download SPF here:

<https://github.com/tatanus/SPF/archive/master.zip>

## **Phishing Frenzy – E-mail Phishing Framework**

Phishing Frenzy is an Open Source Ruby on Rails e-mail phishing framework designed to help penetration testers manage multiple, complex phishing campaigns. The goal of the project is to streamline the phishing process while still providing clients the best realistic phishing campaign possible. This goal is obtainable through campaign management, template reuse, statistical generation, and

### **How It Works**

Email Phishing in it's simplest form consists of three (3) primary components.

- Sending Emails
- Hosting Websites
- Tracking Analytics

There obviously are more complex forms of email phishing that include additional components, but for the sake of our conversation we are going to break it up to this simple structure.

### **Features:**

- Website Cloning
- E-mail Harvesting
- Credential Harvesting
- UID tracking for users
- Reporting and Analytics
- Action Mailer
- Dynamic E-mails
- Preview E-mails
- Sharing Templates
- DataTables

- Export XML
- PDF Reports

You can download Phishing Frenzy by cloning the Github repo:

```
$ git clone https://github.com/pentestgeek/phishing-frenzy.git /var/www/phishing-frenzy
```

## **Gophish – Open-Source Phishing Framework**

Gophish is a phishing framework that makes the simulation of real-world phishing attacks very straight forwards. The idea behind gophish is simple – make industry-grade phishing training available to everyone. There are various other similar tools available such as Simple Phishing Toolkit and sptoolkit Rebirth.

### **Features:**

- One-click Installation
- Standalone, portable binary with static assets
- Point-and-click Phishing
- Beautiful Web UI
- Automated Phishing campaigns
- RESTful API (JSON)
- Automated Training
- Open-Source

You can download user guide here : <http://getgophish.com/documentation/Gophish%20User%20Guide.pdf>

### **Installation guide:**

<https://t.me/rebl0x3r/204>

### **Introduction:**

<https://t.me/rebl0x3r/218>

<https://t.me/rebl0x3r/219>

<https://t.me/rebl0x3r/222>

## **sptoolkit Rebirth – Simple Phishing Toolkit**

The sptoolkit (rebirth) or Simple Phishing Toolkit project is an open source phishing education toolkit that aims to help in securing the mind as opposed to securing computers.

### **Requirements:**

- Apache
- PHP
- MySQL

### **Features:**

- Templates & Visual editor
- Education completion tracking
- Support for URL shorteners
- Support for sending SMTP via SSL

- Forms display inline errors for correction
- Accurate e-mail tracking times
- Browser Detection

You can download the new sptoolkit 0.80.1 here:

<https://github.com/simplephishingtoolkit/sptoolkit-rebirth/archive/v0.80.1.zip>

Other Phishing Tools:

### **Zphisher - Automated Phishing Tool**

Zphisher is an upgraded form of Shellphish. The main source code is from Shellphish. But I have not fully copied it . I have upgraded it & cleared the Unnecessary Files . Zphisher has 37 Phishing Page Templates ; including Facebook , Twitter & Paypal . It also has 4 Port Forwarding Tools . You can Find the Templates here: <https://github.com/htr-tech/zphisher/blob/master/websites/Pages.md>

#### **Features :**

- Latest Login Pages !
- New Instagram Auto Follower Page !
- All types of Bugs Fixed !
- Useful for Beginners !

#### **Installation:**

```
$ apt update && apt install git php curl openssh -y && git clone  
https://github.com/htr-tech/zphisher && cd zphisher && chmod +x zphisher.sh && bash  
zphisher.sh
```

AdvPhishing Tool – OTP Bypass

This is Advance Phishing Tool ! OTP PHISHING

When victim enter his credentials, you need to go to original website and use those credentials to send real OTP to victim. Once he enter that OTP such OTP will also be there with you and you will be allowed to login the account before him.

#### **TUTORIALS:**

GOOGLE OTP - <https://youtu.be/MhSb4My1lZo>

PAYTM OTP - [https://www.youtube.com/watch?v=3TB\\_sISTw9U](https://www.youtube.com/watch?v=3TB_sISTw9U)

TIKTOK - <https://www.youtube.com/watch?v=5qc0Mgyhr7E>

#### **Installation**

```
$ git clone https://github.com/Ignitetch/AdvPhishing.git
$ cd AdvPhishing/
$ chmod a+x setup.sh
$ ./setup.sh
$ ./AdvPhishing.sh
```

## **Hack Using Umbrella Dropper- A Phishing Tool**

Hello, hackers, Today we are going to know about Umbrella Dropper, which is dedicated to most pen-testing, it downloads files on the target system and executes them without a double execution of .exe, only of embed.

I know most of you might want to hack victims only by sending a real file, which when opened open ups a malicious link which automatically downloads the payload from a remote server and executed it without the need of double execution of .exe file which has been downloaded.

### **Installation**

```
$ git clone https://github.com/4w4k3/Umbrella.git
$ cd Umbrella
$ chmod +x install.sh
$ ./install.sh
$ python umbrella.py
```

If you have another version of Python:

```
$ python2 umbrella.py
```

## **HOW TO CREATE A GOOGLE VOICE NUMBER(like anonsim)**

1. Firstly download tunnelbear VPN from store
2. Goto [voice.google.com](https://voice.google.com) and click on "GET FREE NUMBER" , pick one number according to area code you want and continue to next step.
3. To verify number download Textplus app from store , to get a virtual USA number.
4. Paste the number generated on Textplus to verify your Google voice number.
5. Enter verification code sent to your Textplus number on your Google voice page .
5. Now you have successfully gotten a Google voice number.

## **OTHER SITES TO GET ANON SIM CARDS**

<http://www.secretgsm.com/>

<https://vipline.co.uk/>

<https://www.bestbuy.com/site/entertainment-gift-cards/prepaid-minutes/abcat0801003.c?id=abcat0801003>

<https://www.burnerapp.com/>

Search on E-Bay there are selling people always activated cards.

You can buy some cards from legit seller:

@Amdollar (If ID not works, join t.me/rebl0x3r or hit me up @TheMasterCH)

## **WHERE TO GET BURNER PHONES**

<https://www.wired.com/2017/02/7-great-burner-phones/>

<https://www.carphonewarehouse.com/>

## **BANK DROP CREATION TUTORIAL**

This is a noob friendly guide on creating unlimited bank drops for all of your PayPal/Stripe/Square/Loans/etc. cashout operations.

## **COMPUTER SETUP**

This setup is good only for this kind of job and not for carding. Read the next chapter for a complete setup.

Install a windows virtual machine.

Now, on in the Virtual Machine you will install the next things:

- Tmac (to change mac address every time you connect to internet)

<http://www.technitium.com/tmac/>

- XboxHardDrive (To change HDD serial)

<http://www.xboxharddrive.com/freeware.html> • Ccleaner (to clean your cookies, temp data, etc.)

<http://www.piriform.com/ccleaner/download/standard>

- BleachBit (Clean free space and system, another layer of protection)

<http://bleachbit.sourceforge.net/>

I presume you know the next part: start cmd and run these lines:

```
ipconfig /release
```

```
ipconfig /renew
```

```
ipconfig /flushdns
```

You will run them every time you start the machine.

Now it's time to install a VPN. Go to <http://mullvad.net> (I use it and I recommend it, as it does not hold logs and accepts Bitcoin) buy a VPN, download and install their application (make sure you note down the account number)

Let's get started with the real deal .

## **FULLZ**

There are many vendors on Empire Market that sell fullz. Checkout <http://dark.fail>

What you will need from these fullz is a background check, and a credit record. All of these are available on AB, unfortunately I cannot recommend a specific vendor due to fluctuations in pricings and quality of the batch, I recommend you use the forums/feedbacks to find a reputable one and go for it.

How to create fulls: For this, you will have to you the OPSEC setup for the bank drops, that's

written above and upgrade it into a carding setup. Most of you know that are purchasing my guide know how to card, so you can skip this chapter, for those who don't know please read the next section carefully.

A carding setup it's a setup that will try to impersonate the card holder in order for you to obtain the products (either digital or physical) by purchasing with the CC you have. This next carding setup that i will describe here is for carding digital items like Background Checks, so it's a basic one, not a specific one. (like it would be for newegg, amazon, etc.)

So, let's begin. What is needed:  
Good Socks5/RDP  
Good Ccs

### **SOCKS5/RDP:**

In order to make the best of impersonating the cardholder, one of the most important things you must do is to connect to the site you want to card from an IP that is close to the CH (Card Holder) address. I will give you here two resources that i personally use so i can vouch for them

### **SOCKS5:**

<https://luxsocks.ru/>  
<https://911.gg/>

One of the best socks resources i ever saw. Why? Because you have the option of seeing if they are blacklisted or not. Buy 345 from the same city, so you can be sure you will have a bigger chance of success. In the same time look at the CCs resource and choose the same city on the search to see if they have cards from there. (It's important to have enough socks and enough CCs for this to work).

### **RDP:**

<https://xdedic.biz/registration/d3xk54yl5k>

> Again, this resource is very rare on English DNM, so please, do not share this guide or the resources inside as you will loose on the long term by burning methods/resources. When you register with them, you will have to give a REAL Jabber account, where you will be approved instantly, so open your jabber account when registering. If you don't have a jabber account, download Pidgin from here:

<https://www.pidgin.im/download/>

Install Pidgin, open it and go to "Tools">"Plugins" and install OfftheRecord Messaging, so you encrypt your conversations. After that, if you don't have a jabber account, just register a jabber account at jabber.se (my personal pick). So, now that you are done, let's get back to xdedic.biz: Here you will find tons of personal RDP's (which is absolutely paramount when carding from them) and you have the ability to check them if they are blacklisted for free and check their IP Score for only \$0.2 (IP Score is a score that will reveal how reliable is the IP in "the eyes" of antifraud/scam/spam companies).

Look in their FAQ and you will see there that you will need to patch the RDP's you buy from them so you will have shared access, as if the Admin will see you, it will kick you and change the password. If you don't know how to do that, ask support and they will help you stepbystep. Now that you have a working RDP from the City of your choice, let's go to the next step.

**CCs:** In order to get some nice CCs for your bank drops, i will offer you here a resource that is know probably by 0.1% of DNM users, so you will have the privilege to get them from a source that is always fresh. So get to <http://gocvv.cc/en/> and click on the registration button from upright corner of your screen. Copy that password and paste it into "password" dialog box and

hit Enter.

Keep that password that it was given to you as you will never receive it back again and it's the only way to login to your account. So if you have Bitcoins inside and you forgot the password, you lost your funds. Now that you are inside the autoshop, ofc you have to buy Ccs from the same City were your Socks5/RDP is.

Do not look only for Business/Platinum or any high class cards. Keep in mind that you need some background checks, not an Iphone 6 Plus, so any card will do as long as it has \$50 on it. Buy more than one card as you might need more than one profile, or you might not succeed the first time you try. Now that you have the Socks5/RDP and the CCs, I will not talk here about browser canvas fingerprint or user agent. Just use Firefox and you should be ok for carding [instantcheckmate.com](http://instantcheckmate.com). Yes, make sure you have the same system time as local time (check on [whoer.net](http://whoer.net)) and same language.

Now go to

<http://www.instantcheckmate.com/>

I just love their website, and after you card the CH background check you can card from inside the account their sibling background checks (as you will see, that for some drops will be needed). Use the Name and Address that you already have from CCs info and buy the background check with their own card.

### **So far now you have this:**

Name, Address, Past Addresses, Siblings Names and Age, Assets/Property informations, Date of Birth, SSN Issue State and date Issued, (Not the SSN itself) Criminal Record, Marriage/Divorce Records, Phone Numbers, Facebook/LinkedIn/Google+ accounts.

So you will now need DOB and SSN. Go to <http://ssndob.so> or <http://robocheck.cc> and you will find them there 90%. If not, choose another CC, rinse and repeat. (Dont ask me why i'm not doing it the other way around, meaning SSN+DOB and after that Background Check. You can do it that way too, it's your choice)

Now comes the hardest part in this process, Credit Report. This is not a "science" method, it involves a bit of luck. So, I will give you more free Credit Report websites to access and try to get into them. That means you will not need a Credit Card, but you will have to know the answers for the verification questions. The answers are...inside the Credit Report that you want to get, so pay attention to each and every question, write them down on a piece of paper if needed. After accessing 23 services like this you will probably see that some answers repeat themselves. Those are the right one. Keep them in mind and on the next site you will be able to get inside and download the report. You might get it even after only 1 try.

### **Here are the websites:**

<https://www.quizzle.com>

<https://my.bankrate.com>

[freecreditreport.com](http://freecreditreport.com)

[creditkarma.com/freecreditreport](http://creditkarma.com/freecreditreport)

There is no required order.

After this step you will need only another thing: Driver License Number. I will share here a tool

that i use when i don't have fulls already with DLN:

[http://www.highprogrammer.com/cgi-bin/uniqueid/dl\\_mi](http://www.highprogrammer.com/cgi-bin/uniqueid/dl_mi)

This works for the next states so make sure you keep this in mind when you buy the CCs and **Socks5/RDP**: Florida, Illinois, Wisconsin, Maryland, Michigan, Minnesota, New Hampshire, New York, Washington, New Jersey, Nevada. I know those are not all 51 states, but i believe that for the purpose of opening all bank drops below, this will do. So you got to the website and you don't know what to do? Click on "Other Tools" dropdown method and choose state "Calculator" > Now put your Card Holder First and Last Name day and month of birth, and you will receive a "test number".

For expiration date i always use a future date for the year and the same day and month as from the date of birth. (ie. if CH is born on 09/02/1975 for DL expiration date i will use 09/02/2017 or 2016) I believe bank do not have access to the DL number database, or they wont access it till you raise flags. (I know for a fact that this year Bank of America is doing such things and starting to close Bank Accounts that look suspicious).

## VPS/RDP

I know everybody it's looking for RDP's with GEO IP closed to Fulls address, but from my experience with those Bank Drops and never having problems with this, I will give you a resource that I use what accepts Bitcoins.

<http://www.aminserve.com>

Create an account with fake ID (use <http://www.fakenamegenerator.com/> if you don't want to think of names and addresses, but make sure you have an email address created before that.

OFC you want to be fully anonymous doing this, so head to [www.safemail.com](http://www.safemail.com) and open a free account and use it to open the account on aminserve.com)

Choose the service you want. I recommend US RDP, but US VPS that I used is good too. If you don't want to see your RDP working like a Pentium I computer, choose a RDP with at least 1 GB of RAM. That's \$18.

Pay with Bitcoin through BitPay. The service will be accessible after 34 confirmations. After you see the service is on, head to your email and there you will find the IP, User and Password for logging into the account.

If you really want to be sure you will never raise any flags, choose a package that will allow you to choose what OS is on the RDP/VPS. That one is \$18 and you should choose Windows 7 OS. Connect to the RDP (inside the Virtual Machine that's inside Veracrypt encrypted volume that is already running the VPN!) and go to gmail.com and create an account. I'm using the fulls details, without the phone number (i'm changing the last digit) but this is not mandatory. You can always use a fake name. Once you have the email it's time to start opening the Bank drops.

## BANK DROPS

### ✪ Bank of America ✪

#### OPENING:

Go to <http://bankofamerica.com>

> Banking > Checking > Select your state (use the Fulls state) >

Under I want the Basics click Learn More > Open Now > Choose Bank of America Core Checking > Enter all info details (DOB, SSN, Name, Address, etc.) > Choose Unemployment > Do not select

Coapplicant > At the question Are you adding money to you account now select No, i'll make my first deposit after my account is open > Answer the Verify identity questions using the fulls



information > At the question Would you like a new debit card choose No (you can ask to send it to your drop after) > Accept the next terms > Submit application.

**IMPORTANT:** If you have a drop in US and you want to ship the card to your drop, when entering your address, select living less than 6 months on this address and put the real Full address after so when you will want to ship the Debit card, you could use it!

Done! You have an Bank of America account. Now enroll to Online Banking. This should be a no brain work. Choose username, password, security questions, image token, etc. All this information will be send to your gmail. Now, you are ready to fund and use your BofA account. Login to the account and go Paperless! So you wont get any documents in the victims mail as that means a burned Bank Drop.

Connect it to PayPal, Stripe, Square, Flint, etc. but only using the same RDP that you used when you created it.

### **DEPOSIT:**

1. Buy an American Express Prepaid (if not in US, ask a vendor to do it for you, pay \$10 more) go to AmericanExpress.com and register it.

2. For first deposit you can use localbitcoins.com and sell \$20\$30 BTC for cash deposit/bank transfer

3. Link it to a Paypal (not your own) and deposit from there. (small amounts)

4. For your new debit card, you can find tons of public information on how to create a drop (if you are US based) and if you are not, partner with someone from deep web to use he/she's drop and reship it wordwide using a reship service like:

<http://reship.com>

### **✪ Fidelity ✪**

#### **OPENING:**

The same basics as with Bank of America, you will have to have the Credit Report and the Background Check and Motor Record opened so you can answer those id verification questions.

So, open <http://www.fidelity.com>

click on Open an Account > Investing and Trading / Brokerage Account click on Open Online > Individual Account > Are you already a Fidelity customer answer is No > Enter Name from fulls and email that you created earlier and click on Get Started > Fill the information needed there (DOB+SSN etc) at trades pet year select 035 and click next > Answer the id verification question. Here you will have some minutes to fill the info, make sure you are precise and quick about it. It will be 3 questions and if you answered bad on one you will have another shot on the forth question that will popup. Fidelity tends to ask about your victims car and siblings month of birth. If you want, card peoplefinder.com and find their birth dates. If you don't pass the questions the first time you will have a second chance to open the account. Wait for 24 hours and you will get an email that will let you know how pleased they are if you will continue your application. It happened to me many times and at random times I did not have to answer the questions again if I clicked on the link from the mail.

After you completed the questions you will get a confirmation message, that the account is opened and your account number. (starting with X) After this, you will have to agree with emailed documents, meaning you will go Paperless. Accept the terms, when asked if you are a proffesional or non professional trader, select nonprofessional, don't check the box that's talking about you having problems with IRS.

After this you will be invited to enroll to Online banking, accept, create a username and password, select a Security Question and Answer and you are DONE!

At one point you will be asked if you will use all the time this computer . If you are not sure on about your RDP (if you choose not to go with what I recommended) select No, otherwise, select

Yes and make sure you don't change the RDP/VPS/IP.

#### **DEPOSIT:**

Same as with Bank of America. This will be the same to all of the accounts.

#### **☼ SunTrust ☼**

##### **OPENING:**

Basically you follow the same steps as with first 3 accounts, the only difference here is that you need the issue date for the Driver License. I use a invented one every time and every time it works.

Questions are the same as for Fidelity, so make sure you have the Motor Record open along with Credit Record and Background Check. I never used this bank drop to payment processors so I can't tell you if it's great or not. It's easy to open it (and this is what this guide is all about) but I don't know how it will work with Stripe/Square/etc. I heard different feedbacks on AlphaBay forum... so it's up to you if you want to use it for that or you want to use it for loans or cashing out Paypals or other stuff. Sometimes they will send the card to your drop automatic, if that happens and you don't have a US partner to receive the card, the account is burned. Rinse and repeat.

#### **DEPOSIT:**

Same old, same old.

#### **☼ E\*TRADE ☼**

##### **OPENING:**

Click on E\*trade bank and then on the right hand you will see "Open Account" on a green button. Click it. On the next screen, click on "apply now".

On the next screen, fill the info below "Are You New to E\*TRADE?". Remember that, in order to fully use this account you will need a US drop as they will mail you the "Welcome Kit". If you don't have a drop, and you think you are good enough with english language, you can always spoof your phone number and call them, telling them you don't want the "Welcome Kit" to be send to your mail because your mother thinks banks are evil and she is old and has some mental problems and you don't want to disturb her health. For spoofing numbers, use Spooftel.com (i won't get into much here, as there are free info on forums). Create a username and a password and click on continue. For this drop you will need to know the driver license number style to use it for opening it. Enter the address of last employer and when asked for the purpose of the account i always choose "Personal family account...". Now, as for all, choose individual account and click continue. No Choose E\*Trade Checking. Don't accept card right now. They will ask you about funding your account. The minimum funding is \$100 and you can do it as ACH QuickTransfer, an E\*TRADE service (you must give the debited account number and routing) or wire or check. No matter what you choose for the moment you will be able to change it after the account is opened.

On the next screen you will have to choose the funding amount. Anything north of \$100 is ok. Good, now your account is opened. Next step is go "Accounts>MyAccounts>Paperless Settings" and choose full paperless.

The bank will send the card to your address, so it very important to make the account on Saturday, chat with them and tell them that you are not in the country for the next 34 weeks. They will ask you to call them and tell them that and they should hold the card till you arrive in the country. Call them in one day, from a number from any country that you say you are in. Keep the background report and credit report open in case they ask anything from inside them.

(i had no such questions, only about when the account was opened, what type of account, what you want to do with it (invest, dooh))

You should be fine with the account for the next 34 weeks, enough to handle the transactions through it.

**DEPOSIT:**

Same old, same old.

✪ **FIFTH THIRD BANK** ✪

**OPENING:**

Available in:

- Ohio
- Florida
- Georgia
- Illinois
- Indiana
- Kentucky
- Michigan
- Missouri ● North Carolina
- Pennsylvania
- Tennessee
- West Virginia

I will not detail on every bank drop on what to click, but as everybody in this business has at least the knowledge of reading and using internet, always find the open account after that checking account or brokerage account .

You will have 3 minutes to answer 3 questions. Mostly you will be asked about your relatives that own properties on other states and you will need the motor vehicle report. If you don't have it, keep in mind that most of US citizens will buy a car as NEW with an autoloan, so if the question is from what year is your Chevrolet Cavalier and your answers are 1999, 2003, 2005 and 2010 and on your credit report you see an auto loan in 2003, you have a big chance that this car is from 2003.

After questions no dot select Fifth Third Debit Card if you don't have US drop, no Overdraft Coverage, do not order checks and select YES for paperless statements.

Accept terms, click on continue, etc. and now click on "Fund Now" (make sure you save your account number and routing number). The minimum deposit is \$50. Click cancel and that continue. Now you will be prompted with "Create online banking".

You will have to call

18009723030. Spoof your number and call them, you will have to tell them you don't want a card and you want to use your SSN for User ID. They will ask you some verification questions (Mothers Maiden Name that you put when fulfilling the account info. Have your credit report and background check opened. They will normaly only ask you for MMN, DOB and SSN, when you applied for the account why don't you want a card, etc.) and tell them you want to create a password for your account. When done use them to login your account and use it

**DEPOSIT:**

Same old, same old.

✪ **WELLS FARGO (US DROP NEEDED)** ✪

**OPENING:**

Same basic opening steps. Asks more about family location and age of family members. Asks about past addresses, but it's easy to get throught them, as you have all the thing needed to

extract the info. You will have to fund the account, but that wont be any problem as you can write a check and mail it to the bank. You will receive at your drop and you will have to sign Customer Account Application in maximum 3 days from account opening and the card and pin in another 7 to 10 calendar days.

**DEPOSIT:**

**Same old, same old.**

✪ **HUNTINGTON BANK** ✪

**OPENING:**

Same basic opening steps. Will ask about your cars, will have trick questions and will ask about your family. First will ask 3 questions and after that another 1 if you fucked up somehow on the first 3 ones. After selecting design of card, you will be asked to open your online account. From that moment your account is working. Make sure you enter the "My Profile" and you change the mailing address to a wrong one so you can save some time. This account is specially made to quickly transfer money into and out from it. That means you will have to work fast and do your

**DEPOSIT:**

**Same old, same old.**

✪ **ALLY BANK** ✪

**OPENING:**

Same basic opening steps. Working like a charm, this is the easiest bank drop opening i've ever encountered. The only problem is that the bank is very strict, so make sure you use it as it would your own bank account. That means, age it normally. Deposit from local bitcoins if you find trades, starting \$50-\$70. ACH them out if needed. Deposit again, rinse and repeat a few times in first two weeks before using it for your main business. You enter 0 for bank deposit. When asked for deposit method you say wire or mail, and when you first deposit, you deposit from local bitcoins, with bank transfer. You add the email for security code.

**DEPOSIT:**

**Same old, same old.**

**OTHER INFO**

Why is this guide valuable? Lets say you use one bank account on Stripe and it gets burned. You want to continue carding from the same clean RDP on Square? What would you do? Buy another bank drop? No, you make another one. Buy another RDP for the next Stripe account and make another bank drop. So just for this, instead of paying ~\$450 for 3 Bank drops + 2 RDP, you will spent about \$85 for 2 Fulls and 2 RDP's. That means ~\$300 in left in your pocket. If you work with 2 Stripe and 2 Square and you have to do this 2 times / month...you just made \$1200 /month economy, that means profit! I got lots of questions about emails used for opening drops. I dont use gmail or yahoo mail

anymore. I use and I recommend tutanota.com

I know that some of the people on forums know about the next resource I will give you, but that's probably 0.1% of total people. People who would die to know it. This is true for most of the information that is in this Guide. Thats why it does not make it a public knowledge. This is intended to be a help for newbies that don't know where to search or don't want to waste time reading tons and tons of forums. Time is money, I remember when I first asked MH9 about carding some long time ago (I was under other nick – just in case MH9 reads this) and let me understand exactly that. Now I thank him for that.

I know other Bank Drop sellers might make a fuss about this, but this is not intended to kill this business (i'm one of them) because there will always be customers who will want to buy a done job, rather to work for it. So, let's get back.

**SCANS:** Go to <http://secondeyesolution.com> and order there what ever scan you want. They are amazing and for me, all of their scans passed verification for payment processors. So I would recommend them to anybody.

<http://ordaproject.me>

→ Here you have tons of things to buy. It's an amazing resource that it pretty unknown to most of users.

### **CASHOUT:**

It's not the purpose of this guide but some simple tips:

1. Find a drop and ship the Debit Card to the drop > Cashout to ATM 2. Find a drop and ship the Debit Card to the drop > wire transfer to localbitcoins.com > BTC 3. Link the bank account to a Prepaid US card > Cashout to ATM 4. ACH to Paypal 5. If nonUS, reship a Prepaid US card to your local Drop > Link the bank account > Cashout to ATM

**IMPORTANT:** Always make the first deposit BEFORE linking it to a payment processor!!!

If you think I can help you with any other information you can find me on AlphaBay Market, Nucleus Market and Dream Market, do not hesitate to ask questions.

### **FIND DROP SITES**

You need a drop, drop site, drop point, whatever. You don't want to use anywhere closeby if you can help it. The little old lady down the street is OK, but try to be diversified in where you go. If you do alot of times in one area, the Secret Service get's calls and then they come out there. While on the topic of the law, the ONLY branch of law enforcement that investigates Credit card fraud is the Secret Service.

They are a branch of the Treasury department. The FBI has NOTHING to do with credit card fraud. So if you see some Aries K (actually Chevy Corsicas now!)

cars with municipal plates around your neighborhood, be WEARY! They don't just follow the president around with earpieces and black 3 piece suits!

These bastards will NAIL you. I almost found out the hard way!

OK back to the drops. Keep your ears open. I find that people ALWAYS blab about when they are going away on vacation for a week or two or three. It's human nature. I used a drop site one time for 2 straight months while the residents were away. Things to look for are closed shades, floodlights that

are on, lights that go on at a specific time every night, old newspapers in the driveway, whatever. Get the adress, Zip code, and city, and if you can, who lives there (just look in the mailbox).

### **Getting the Acutal Credits Card Numbers!**

A few good ways to get carbons are to go trashing (looking in dumpsters of gas-stations, and other stores that get alot of credit card business) or you can get a JOB at a place like that! (Great, I did it myself) or you can use a

credit bureau such as TRW. Don't use this unless you ABSOLUTELY know what you're doing. I still don't use it too much.

OK, so you have your drop and you have your card number. So you want to order, right? Well sort

of. Take your time and decide what EXACTLY it is you want. Don't be on the phone making the order sounding unsure of yourself.

Salespeople know what's going on then. Then call the place, and have the name and address and phone number ready. (You can make up a phone number, or use one that rings and rings and rings, but don't use the one from the drop point).

## **HOW TO ORDER GOODS**

### **Sample Order:**

Computer Products, this is Steve, how may I help you?

Yes sir, I am looking to place an order on an item I saw in blah-blah magazine. Can I ask you the price just for confirmation? (Stuff like this makes it sound like you are the real guy, and are worried about your money!)

Steve: Yes, it is \$699.

You: OK, that's what it says here. OK, I'd like to place an order for one computer card.

Steve: OK, may I have your name?

You: John Smith

Steve: OK Mr Smith, and how would you be paying for this?

You: With my mastercard

Steve: The number please?

You: 5217 5478 0004 9812

Steve (reads back for confirmation)

You: Yes sir

Steve: OK, may I have your billing address?

You: (OK this is where it gets tricky. Sometimes the place will have to call for confirmation when the billing and shipping addresses don't match. I'll supply you with places that don't care). 1616 Mockingbird Lane, Anytown, Anystate. 99457.

Steve: Alright, we'll ship that out to you today.

You: (The wisest choice is OVERNIGHT. Then they are in a rush to get it out, and you get it ASAP without worries.). Do you ship UPS Red label?

Steve: Yes we do. That's an additional \$28.

You: OK, that's fine. Sir, could I have a total on that? (Sound serious)

Steve: Yes, that comes to \$727.

You: OK, thank you very much.

Steve: Thanks for calling Computer Products, have a good day.

## **POST ORDER ACTIONS**

Allright, you placed the order and it seem to go flawlessly. What you need to do now is to call back and get a shippers routing number (if you are not sure that the place is totally GULLIBLE!). ALWAYS ALWAYS ALWAYS ALWAYS use United parcel Service if you can. They just leave the package at the door and leave. Airbone Express, Federal Express, and DHL all require signatures. You either have to risk being remembered by the guy, or you have to leave a note on the door of the drop point. UPS is the easiest by far.

So, you call back to see if it shipped, and if it did, COOL! You're in business.

Guy, or you have to leave a note on the door of the drop point. UPS is the easiest by far.

So, you call back to see if it shipped, and if it did, COOL! You're in business.

## **PICKING UP YOUR STUFF AT THE DROP POINT**

When I started out, I was under the legal driving age. So I had a friend of mine go in on me with this deal. He drove. If it's closeby, you could get away with walking or riding a bike, but you look suspicious lugging a box around with you. The onyl real way to get around the car problem is to go at night so you aren't spotted.

\*\*\*\*\* ATTENTION \*\*\*\*\*

If you are TRULY desperate for a drop site (Such as me, I had to get my girlfriend something special [ a \$1200 diamond ring from BEST Products]) then call the place you ordered from and get the routing number. Then get the number for the local UPS/Airborne/DHL in your area. Tell them that you will pick the package up on your way to work (or some shit like that). You go in there, and SIGN THE SHEET WITH THE OPPOSITE HAND THAT YOU USUALLY WRITE WITH.

Then there is no way that you can be matched with it. Wear clothes that you usually don't, but don't go in there in a clown suit, or you'll be remembered. You can only do this once in a while though.

## **POST PICKUP PROCEDURES**

After you pick the package up, take ALL the stickers and marking that the shipper and place you ordered it from put on there. This way, its untraceable. Keep the box though, unless you are TRULY paranoid about your parents or whatever. Also, try and get all the serial numbers off of it. Use rubbing alcohol, a pen knife or whatever to scratch them out or peel them off. Keep the nubmers somewhere (taped on the TOP part of your door) or some other place that no one would ever dream of. They may come in handy once you know what you are doing.

Also, if you are going to resell the item (It financed part of my childhood until I got into other things) DO NOT give the person the registration and warranty unless you really trust them. If they register an item with the

company, and there happens to be serial numbers in ROM or under some obscure chip, you could be fucked.

## **WHAT TO DO IF YOU GET CONFRONTED(FROM REAL CARDER – THANKS!)**

If you are ever confronted by anyone (Police, Shipper, retailer) do not admit anything. Just deny you even know what they are talking about. The only way you can be caught is if they actually record you placing the order, and find you picking it up. Even then there are a lot of ways out of that (Ask a trustworthy lawyer, I am not giving away ALL my secrets!). If you need an alibi in the way of "Where you got this?" just say you went to a computer show and a guy sold it to you off the back of a truck. You didn't ask him any questions, and he said he'd send you a receipt in the mail.

Now you have a way to get whatever the fuck you want, when you want it! It works, believe me. I have tallied up all the stuff I have ever done (Most is still with me) and I got a total of \$67,000. Yes sixty-seven THOUSAND. That's after 3-4 years of straight carding. It would take the average kid about 67 years to save that much up. Not you though!

MacWareHouse- 1-800-ALL-MACS (255-6227). They carry stuff for IBM's Macs and Apple II's and maybe even Amiga's. They give you a catalog with your first order (and every time after that) or you can call them and ask for a catalog. They accept Visa/MC/Amex. Their only drawback is that they usually Ship Airborne Express. However, they GUARANTEE overnight shipping for \$3. Yes, 3 bucks. Not that money is a matter to you now, but it shows that they are fucking in a hurry to get your order out the door. I have found out that they do the billing 3-4 days after you get the package. GREAT place to get what you want. UPS RED is available, however, no one in their right mind would use it, since it's like 10 times more expensive than Airborne (Macwarehouse has a deal with Airborne, Macwarehouse is their biggest sender on the East coast!). Whenever I go UPS from Macwarehouse, I just give the operator some bullshit like "Airborne won't deliver to my location overnight and I need it quickly". That's all.

Quality Computers- 1-800-443-6697. Another Gullible place. They sell stuff for a lot of computers too. They take Visa/MC/Discover. Nice place, uses UPS and ships overnight too.

BEST Products, INC. 1-800-950-BEST. They sell EVERYTHING (if you happen to live near one of their outlets, go in there, and either grab a catalog, or write down the product numbers of what you want and give them to the operator when you order! They take everything and ship every way.

OK, now that I am just about out of this business for good (Heheh, nothings definite!) I want you to take over in my tradition of glory. It is the greatest thing that happened to my financial (and sexual) life. What chick couldn't dig you if you gave her a \$1200 piece of ICE???

If you're careful, and don't go overboard, you'll never get caught. Don't tell anyone except your most trusted friends (and not even them unless you get them involved so they can't rat on you if your friendship goes sour). Even though you virtually can't get caught (even if someone rats on you) It's always nice to be anonymous.

## **MORE ABOUT DROPS**



A "drop" is a place, or location, where you have illegal, carded, or stolen goods shipped to. It has to be a place that has no link with your current life and is in no way linked to you. Finding a drop is not really hard. You can go on Craigslist and find houses for rent, or just drive around your neighborhood looking for houses for sale where you can ship goods to. Make sure the house has no big windows that allow the driver to see that the house is empty. You don't want to have the package returned to the sender because of that. Just use your brain to find a decent house that you think is worth shipping a package to. Usually pick a town close to yours, but not in your neighborhood. The big day has come: UPS tracking shows "Out for Delivery". Yeah! Now check if the package requires a signature. All carriers require it, except UPS. For UPS, you can see if Signature Required is written on your tracking page. If nothing mentions a signature, or if you are not sure, then signature is not required.

### **Method 1: Acting like you are away**

If you don't need a signature, you can leave a note on the door, "we are away, please leave package here, take this as my signature" and you might as well print the order confirmation page showing the tracking number and put it with your note to make your case stronger. The driver makes the final decision about leaving the package or not, but usually there is no problem with UPS when they don't need signature. Sign the note, put the order confirmation page with it, stick it in the door, and wait in your car not far from the place. When the driver leaves the place, grab the package, and put it in your car. Then skip method 2, and continue reading.

### **Method 2: Acting like you own the place**

The second method is when a signature is required. You will have to meet face to face with the driver. Remember one thing, you can relax. The driver's job is not to investigate fraud, but only to make sure the package does to the right received. So you must just make him believe the package is yours, they don't care about fraud (but don't be stupid and talk about your crime). Carry a printout of the order confirmation page, the tracking number open on your smartphone (use VPN!), and look like you've been waiting for him. You might wait at the drop, sitting on the front lawn, or doing whatever you want. However keep in mind that waiting in the car when the driver sees you get out of the car is highly suspicious. If you choose to wait at the drop while being visible, take down any "for sale" or "for rent" signs, and call the bank's automated system prior to showing up to ensure the card is still valid and the police is not waiting for you. Greet the driver, show papers, sign the cardholder's name, and proceed to the next section.

Sometimes, the driver might get cocky and ask, why your name is not the same one than what's written on the package, or why you're not inside. You can tell that you recently moved, and you put it under someone else's name because you have "problems with customs". When they get cocky, you can threaten them to make a complaint at their local UPS hub, they usually calm down and hand over the package. I had a cocky driver in my last carding trip in Minnesota, and I had to use this method, and I finally got my package. By experience, when you have brokerage fees to pay (like international package), you can call UPS before getting the order and ask the amount. Leave a money order on the door and the driver will take it and leave the package. You will avoid getting a InfoNotice that way, and the driver will believe you own the place. I did that a lot of times and no failure so far.

### **Picking your package at the UPS facility**

In some unfortunate circumstances, the package can end up at the local UPS facility and will require government-issued ID to be picked up. This happens if you missed your drop, for example.

In that case, don't bother making a fake ID, as there is a better trick.

The package is usually held for 5 business days before it is sent back to the sender. The day the package arrives at the facility is day 0. Two scenarios can happen:

**Scenario 1:** You get a call from the UPS branch

They will probably call you and say something along the lines of, we have a package for James Fakename waiting at the facility for pickup. Just tell them that you don't know this person. Here's a sample script of what it should look like:

UPS: Hello, may I talk to James Fakename please?

You: I think you may have the wrong number, who is speaking?

UPS: This is the UPS branch, we called the phone number we had on the package.

You: Oh, I was waiting for a package too, and it didn't get delivered. Is this a package from Newegg, a small box?

UPS: Yes, we have one small box waiting here, for James Fakename.

You: I have a tracking number, can you check if the last 4 digits are 3382?

UPS: Yes they are.

You: I'm very surprised, because my name is Fake Name and I was waiting for this one. I have no idea who James Fakename is. They looked confused when I placed the order too.

UPS: Well, the package will be sitting here, just come pick it up when you are ready.

This worked me twice. I had 2 drops to watch at the same time and I missed one package. This allowed me to pick it up.

**Scenario 2:** You do not get a call

On the morning of day 5, call the toll-free number and ask to be transferred to the local branch. You can do the same scenario, and inquire about a package waiting there for you. You must look confused a bit in your voice and look like someone who was victim of a mistake from the online store, and they will gladly hand over the package to you. Everytime I did it, I never got asked for any form id ID and it was all smooth. Do not give your real name. Test the card before going (call the bank), and only do it if the card is still live, otherwise it can be dangerous. You can also send a mule if you are too afraid, but I showed my face a few times when the card was still live and never ran into issues.

**After getting your package**

I sometimes skip this part when I am lazy, but you should be extra careful. Your freedom has no price tag, so take 5 more minutes to do this precaution. Drive to a nearby park or public place, and open the cardboard packaging. Look for any device that may be tracking your position, such as bugs, GPS devices, etc. Then destroy the shipping label (you can burn it to make sure), throw the cardboard packaging away, and you now have in your hands a precious item you carded using your ATOD card. Also burn the order confirmation page if you decided to go this route and you brought it to the drop! At this point, you can consider your carding heist a "success"! Drive home, relax, you owned the bank and the website. You can brag about it on the forums with reason. If the card is still valid and there was no tracking device, you can card to the same drop again until the card burns. Get as much as you can out of it. Burn the card to a crisp. I remember getting \$10,000 worth of electronics on a Chase card at the same drop, split on 5 orders. This was a money-making week. All right, you carded the item, ATO'd the account, got items, more items, burnt that drop to a crisp too, now the card is dead... either over the credit limit, or flagged by the cardholder. Never show your face to that drop again, and enjoy your goods!

## **HOW TO GET YOUR DUMP BIN LIST**

So you've gone instore carding a couple times and you buy batches of cards that you know are valid however you still get declines, why is this? Well declines can happen for multiple reasons several being that you went to high for the card to handle the transaction, coding error, the actual cardholder used their card 1 hour and then the next you try half way across the country, or Region block, which is what we are trying to focus on eliminating with our binlist

## **WHAT IS A BINLIST, AND WHY DO WE NEED ONE?**

To answer this question we first must know what a BIN or IIN is, both of these are acronyms for Bank Identification number or Issuer Identification number. The BIN or IIN is the first 6 digits on a credit card that determines the bank and level of the card, a BIN List is a list of BINs that you know will slide for your region, having a BIN list is the difference between guessing for approve and hoping to eliminating the guess and knowing it will work

## **So now that we know what a BIN and BIN list is how do we get one?**

Alright so here is the tricky part, it takes money to make money so the first round of dumps you invest on should be a learning experience, I would suggest buying a mixpack of all different BINs and testing out one by one which ones work in your area, now I know what you are thinking How can I test these cards since I don't know my bins and it's a guessing game whether it's a decline or not, even worse what happens if it shows Hold call or Stolen??!!, Don't worry!,

## **What to do in order to test your card I would suggest:**

1. Going to ANY self slide checkout, some areas have more than others
2. Go to one of those movie ticket vending machines where you can pay with CC,
3. Coca Cola or vending machines that take CC
4. And i've heard about these worldwide parking meters, apparently some have something where you can slide and pay

As your rolling through 1 by 1 in your list of dumps anyone that approves make sure to write that bin down, if you have any declined cards check with your vendor and if it is approve it is most likely a region blocked card,

Any card that approves you know is a BIN that works for you,

Now i know it seems like somewhat of a waste of money if you don't profit but after your going through your dumps if you have a dump that approved and you have duplicates of that BIN you can go try for a bigger purchase since you know that it's a working BIN, the true reward from the first batch is getting that BIN-list since it is the CRUCIAL FACTOR!!! In determining your long term success, and you walking out of the store safe and sound with your item. After you have a good list, the bigger the list the better, you can ask your vendor for a batch of BINs making your next round of dumps a Sound Investment guaranteeing your success since you are more aware this time around

After you get your binlist don't get to comfortable with the list, always be adding since overuse of 1 BIN in a region will cause that BIN to block,

Hope this information can be helpful to someone out there  
Good luck Carders!! and as always  
Stay Safe

## **HOW TO GET ANONYMOUS PHONE NUMBER 2.0**

There are some methods which able to receive CC sms verification is not revealed yet.

1. Create some free email like gmail or yahoo.
2. Go to <https://www.phone.com>
3. Apply for 30 days trial. It not requires CC
4. Go to mailbox and use link to activate account.

In your account you see phone number.

You can use this or you can add another number.

When you add number you need to setup default extension for that number, to be able to receive sms. Anyway with this service you can receive sms, receive automated calls (just setup voicemail) and also you can redirect calls. So when they call to your number in USA your phone in Russia rings wink

Don't go to this site with tor, you need socks or vpn.

If you not receive sms, then try add another number wink

Ahh anyway its fucking easy to find out how this thing works wink Good luck wink

### **How to obtain USA number**

#### **Requirements :**

iOs device/iPhone

- Reset everything to delete all the data
- Create a new email
- Create a new apple id, choose payment none, no need enter credit card details
- Use new apple id to sign in iOS device
- Download Textfree app and sign up, you will get a free USA/UK number. if cannot, get free USA number by sign up at <https://www.pinger.com/tfw/> first.. then login the app
- Download Burner App on ios.. install the app, it will ask u to enter existing USA number. enter it from TextFree. and it will give u new number
- Works on ebay sms verification, gmail

#### **Another method : card Ringcentral account.**

They will give voip setting, either you need to setup physical voip phone or mobile voip client on ios.

Make sure voip connect to vpn to stay anonymous

UK Landline phone numbers - <https://www.ereceptionist.co.uk/>

## **HOW TO MAKE A ACCOUNT TAKE OVER(ATO)**

Find out CC bank & Hotline

<https://www.bindb.com/bin-database.html>

[binbase.com/search.html](https://binbase.com/search.html)

<https://bins.pro/>

<https://binchecker.com/>

Go to above websites and enter first 6 digit of PAN/BIN and search, it will tell you which bank provider. Then you go to google and search the bank website.. and look for its hotline number.  
Example

Capital one : 1-800-955-7070 (require SSN)  
Wells fargo : 1-800-642-4720 (require SSN)  
FIA card services : 1-800-655-1491  
Chase bank : 1-800-432-3117  
Chase bank debit : 1-800-935-9935  
Greendot : 1-866-795-7597 -- press 1 and enter zip code

Branch banking and trust company : 1-800-476-4228..press 2, then enter zip code  
Call forwarding 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 forwarding service so when you call the 10 digit number from the call forwarding service it will forward to bank hotline. Links are below.

### **FREE CALL FORWARDING**

<https://countrycode.org/free-call-forwarding>  
<https://www.sendmycall.com/>  
<https://www.inphonex.com/>  
TollFreeForwarding.com  
<https://www.JetNumbers.com>

Call the Bank  
<https://www.spoof.tel.com/>  
Telespoof.com  
Teleturd.com  
PhoneGangster.com  
[Covertcalling.com/freecall/index.php](https://covertcalling.com/freecall/index.php)

Change male/female voice. impersonate cc owner number call the bank hotline, if you can't change get a girl and she'll do, but talk with her what she must talk. Provide all the verification, then you can request reset the VBV password.

The same method also can be use to add new contact number and shipping address  
Bank will ask personal details for verification, so get ready your SSN, MMN, DOB, driving license number, CR and BR. (same steps for reset VBV password) inform the agent, you want to add additional phone number (ur burner number). done.

Wait 3-5 days  
Call again.. perform verification again done. inform want to add new address (u give fake drop address!) done..  
Wait 3-5 days again

When you are at shipping info..enter the same address which u gave the bank. merchant will call (ur burner number)for confirmation..just cooperate and give out cc info/reconfirm shipping address

check the tracking frequently, during delivery day.. call the courier asked to delivery another address due to at work or something etc. this is to prevent merchant blacklist your real drop address. they will blacklist the fake drop address after a while..even u use fresh cc they wont deliver no matter how

Some merchant will ask you email them the following : Credit/Debit card scans Driver license scans so be prepared!

## **GOOGLE PLAY GIFT CARD PRIVATE METHOD APRIL 2020**

1. To card Google play gift card ,first clear your Cookies in browser\par
2. Then go to any app that is paid and below like 2\$ or less if you go to payment info and select first column
3. Get your card from atn or buy from shop\par
4. Bin recommended 517805,372739 ,417409 or amex gold ,capital one bank (only USA cc)  
Even if card dont have name amd zip you can add any name and us zip because those bin are non avs
5. Now ready to go if paymenr succesfull for 0.99\$ then go to buy google play credit and select your gift card 5\$,10\$,15\$,25\$ or 50\$ .now all done and it success

## **EXPEDIA FLIGHT CARDING PRIVATE METHOD 2020**

Card Any Flight In The World  
Site: Expedia.com

### **Requirements :**

1. Rdp/911
2. CapitalOne Platinum CC = 400344 (Tested Works 100%) Important. (Dont kill Card)

Steps:

1. Use This 440056,400344 BIN CC
2. Checkout any ticket of any flight you want to travel in available on expedia.
3. Use your legit name. They will ask you for identity proof when you checkin.
4. Username = Your name = cc name
5. Enjoy your flight.

Source : Carding.us forum.

## **AMAZON CARDING PC VERSION APRIL 2020**

Make an email (Gmail, Hotmail ) with CC matching name. If CC name Susan Tokar then make like [susantokar1995@hotmail.com](mailto:susantokar1995@hotmail.com)

Step 1) Run Remote Desktop Connection and connect with your RDP Host. if u don't use RDP then do the following steps in your pc

Step 2) Start MAC address changer and change all MAC address.

Step 3) Open CCleaner. Analyze and clean.

Step 4) Set socks5 in Mozilla Firefox. I already explain how to do it

Step 5) Restart Firefox and go to [www.check2ip.com](http://www.check2ip.com) and check your IP is blacklisted or not &

assume as CC holder address.

Step 6) Now open the shopping site. I want to recommend a website shop in your country. Why? Because you don't need to wait a lot for your package

Step 7) Register with credit card holder information, name, country, city, address, and email you made one just for this order.

Step 8) Choose your item & add to cart. Never choose a big amount first. Try to card small amount item first within \$500.

Step 9) In shipping address enter your address or your drop address, where u want to deliver the product.

Step 10) Go to a payment page, choose Credit Card as the method

Step 11) Enter your CC details. Like CC Number, CC holder name, CVV/CVV, Exp. Date. Don't copy – paste info. Type it one by one. Cause most sites have copy-paste detector script)

Step 12) In Billing address enter CC holder address. Now proceed to payment.

I m sure if you do everything right then the order will be successfully placed

## **CC TO BTC METHOD**

Need:-

- 1] CCs
- 2] ANON sim cards (1 per renter and 1 per customer)
- 3] Your computer
- 4] Photo Exif Editor Apps (Runs with Android free app)
- 5] Anon Offshore CC with IBAN attached (optional but very useful for quick big cashouts)

This method will allows you to cashout all CCs to BTC easily with fake listings on 9flats.com. 9flats.com works in Europe and America, have no security (but it would be better if you use VPN, SOCKS5 etc..) no chargeback and bitcoins are accepted.

Steps:-

1] Open an account (renter) on 9flats with a fake e-mail address, during the first 3 days log-in your account and visit the website, take quick looks on the listings (act like a real renter ).

2] During these 3 days, you will need to pick up some pictures of flats for rent (the best way is groups on Facebook). Once you have your pictures, you will need to change the exif datas (use « Photo exif editor » for that), to the geolocation of your fake listing (use a real geolocation, google maps is your friend) and very important change also the info « photo taken the ... » and chose a date during these 3 days (very good to increase your scoring) and don't forget your pics in .jpg (important ! ! )

3] After these 3 days create your listing on 9flats, the best way is to make a good standing flat in a chic place (approx \$150 – \$200 per day). Be a comedian ! Put periods of unavailability to look like to a regular renter. After that you will need to wait 48h to 72h before your rental ad is online.

4] After 72h max your ad is online, good ! Log-in sometimes everyday (or every 2 days) during 1 week to look like as same as a normal renter.

5] 1 week after Day 1 open a customer account (name must be as same as cc holder of course), act like a real customer, take your time to visit ads near the area of your fake flat, ask questions to other renters (4 days), after the 4th day : Card your own ad and don't forget to contact the fake renter (you ! ) before, ask some questions etc...

6] Once your fake booking is OK, you will receive an e-mail from 9flats, again be clever, log to your 9flats account by the link provided on your e-mail from 9flats, but it would be better if you let few hours before your booking and your cashout. At the cashout the options are : Bank wire or Bitcoins, of course choose bitcoins.

7] The best way to clean your dirty BTC is grams they provide a new address every 10 hours.

8] TRICKS:

If after the booking you will have only 1 option : « payment in cash » the reason is that you have not been clever enough, so don't forget to send some messages to others renters also with the owner of your fake flat (you ! ) during the booking.

You can also bypass the option payment in cash : make a distant booking of about 1month, this process is useful because it allows you to cashout the funds of your 1st booking.

**The anon SIM cards may be useful if they need SMS verification (but not every time, I needed it one time only).**

## **EBAY CARDING METHOD 2020**

1. Firstly you need fresh , clean RDP server. You can buy them from tools shop(I use this: <http://superded.biz>), or just find some providers who offer free trial (for few days, week or two). When you got RDP server, connect and do everything in that server.

2. If there's no mozilla firefox browser, download it.

3. Now you need some socks 5. DON'T USE FREE SOCKS POSTED ON FORUMS OR FACEBOOK, YOUR SOCKS5 SHOULD BE PRIVATE. You can buy them on VIP72 shop.

4. When you got your socks, connect with them and go to ebay.com, ebay.co.uk or any other country ebay.

5. This step what you gonna do is part of my method. Firstly, check out some items(any item, just click on it, go back and check other one). Close ebay and leave it for a while. You needed this to get ebay cookies generated.

6. Now you need VALID working CC. This is the most important thing, because to get right card for ebay is very hard these days. Personally to get cards i use a seller on telegram @reliableseller he sells valid cards for 25 btc he also sells methods and bank logs.

7. Now, when you are ready to buy a card, ask for BARCLAYS or CHASE bank, they're best for ebay. Doesn't matter BIN, just any of these banks cards work.



8. Go back to your server, open again ebay site and register a new account. Fill information as card owner's(even create new email with card owner's name).
9. Now when your account is created, again check out few items(just click on them, don't buy) and pick one item for about 10-20\$, add to cart and checkout. PUT YOUR(OR YOUR DROP) ADDRESS AS SHIPPING, continue checkout, choose credit card payment and you will be redirected to paypal site.
10. Fill all card holder's info(address, card details, but email yours) and continue checkout. If everything good, you will see confirmation page, just click on Confirm payment, and you will get successful order page! If you got error, that's mean card could be dead or maybe it's already linked to another paypal account. So you need to clear all date and start again. But with these bank's cards, everything should be ok.
11. Now, if you got successful order, you can choose anything up to 200\$(sometimes works on 300-400\$) That's all!

## **TOOLS SETUP STEP BY STEP 2**

One of the main things when becoming "ANON" is changing your location this can be done by successfully changing your IP, Mac Address, Keyboard language and Time zone Settings (Some websites such as Paypal can even see you HDD serial number).

IP's can be changed with VPN's and proxies. There are many places to get these, so before starting the steps below, make sure you have a VPN or Socks service and know how the software works.

Below steps are the exact way that most carders when wanting to go off the radar for anonymity or if Carding/Paypal then you will be using a specific location whatever your reasons are its all setup the same.

### **✓ Step By Step**

1. Run Ccleaner and clean all your browsers etc have everything selected it may take a few minutes but you do not want anything that may leak your old IP  
(ccleaner : <https://www.ccleaner.com/de-de/ccleaner/download>)

2. Open Command Prompt  
(win + r --> cmd or search for cmd and run as administrator)

3. Enter the following

```
$ Ipconfig /release (Press enter)
$ Ipconfig /renew (Press enter)
$ Ipconfig /flushdns (Press enter)
```

4. Now close Command Prompt

5. Now open your VPN or Socks5 and connect to a location/Server  
If you want to use both then connect to your VPN then connect to a Socks5

6. Now open TMac and change your Mac Address  
(tmac: <https://technitium.com/tmac>)

7. If you are using a country that is different to your Time Zone then change your Time Zone and Keyboard settings to the country you have a used

8. Head to Check2IP or Whatleakes this will check if there is any leaks etc if you have followed the above then you should have no problems if you have any problems it will tell you what needs to be fixed.

If You Are Doing Any Work With Paypal Then Also Use HDD SERIAL NUMBER Spoofer Because PAYPAL Can See Your PC Account Name So a VMWAREE Machine Would Be Recommended.

Do The Above Everytime your Change your IP

Or You Will Get Leaks

if you just want to browse the web anon then tor can act as your vpn but do not use this for any other reason such as market places, carding etc you would definitely need better security such as vpn and socks firefox should be your number one choice browser when doing carding or any illegal activity Because this one to be the easiest to clean (via ccleaner).

That's All, You Have a Perfect Setup Of Anonymity & You are good to go for your job

## **HOW TO CHECK FOR LEAKS / IP BLACKLIST**

<https://browserleaks.com/>  
<https://www.dnsleaktest.com/>  
<https://ipleak.net/>  
<https://privacy.net/analyzer/>  
<https://panoptickick.eff.org/>  
<https://whatleaks.com/>  
<https://whoer.net/>  
<https://whatismyipaddress.com/blacklist-check>  
<https://www.whatismyip.com/blacklist-check/>  
<https://dnschecker.org/ip-blacklist-checker.php>

## **PAYPAL 2020 METHOD**

### **Requirements:**

- RDP
- Email (drop email)
- Credit Card

Make Sure That The Flash Plugin On The RDP Server Is Up To Date.

Make Sure All Browsers Are Up To Date!

Open The Browser, If Your Checking Out From A Online Store That Supports Paypal Go To It &

Add Whatever It Is Your Carding To Cart & Begin The Checkout / Payment Process, When Your At The Paypal Check Out Page It Will Prompt You To Login & You Will Also Get A Option To Check Out With CREDIT / DEBIT , Click On That.

Once Your At That Checkout As Guest With CREDIT / DEBIT Card. Enter The Fresh You Acquired , For Email Use Your Email / Drop Email , For Phone Either Change Last Digit of CC Owners Real Phone Number or If Thats No Available Use Google To Find out What The Area Code Using The Fresh CCs Billing Information e.g Google “Whats The Are Code 90210” Once You Filled Everything Out, Click Pay Now! , & WALL If You Get A Bank Declined Message That Means Either CC Is Dead or Insufficient Funds! If You Get Redirected To A Error Page That Says “WE CANT PROCESS YOU PAYMENT AS THIS TIME” That Means IP Has Been Used On PayPal Before or That The CVV Has Been Used To Process A Transaction Before!

IF YOU GOT THE WE CAN'T PROCESS NOW ERROR OR THE BANK DECLINED ERROR Start Over With Another Fresh CVV & New RDP.

ON THE GUEST CHECK OUT PAGE IT WILL GIVE YOU A OPTION TO JOIN OR JUST KEEP CHECKING OUT AS GUEST OBVIOUSLY SELECT AS GUEST.

IF IT DOES NOT GIVE YOU THE GUEST OPTION & IS FORCING YOU TO CREATE A ACCOUNT THAT MEANS THAT RDP IP IS NO GOOD.

### **SENDING MONEY TO PAYPAL ACCOUNTS :**

If your not trying card online shops but are in fact trying to send/transfer funds to a paypal account all you have to do it go to a paypal link generator paste the email of the paypal you want to card the funds to & enter a payment/product description [e.g For Goods Already Picked Up generate the link and then go to the link and bam something as checking out with a online store accept PayPal!

RECENTLY PREFORMED MULTIPLE TRANSACTIONS CARDING FUNDS TO PAYPAL ACCOUNTS FOR THE AMOUNTS OF 1000/1700/1800 & Had A Success Rate Back to Back. THIRD 5TH BANK DEBIT CARDS WORK GOOD

**440066** WORKS GOOD

SIGNATURES FROM CAPITAL ONE / BOA Work Good

Business Debit Bins Work Good

BUT REMEMBER CC MUST HAVE NEVER BEEN USED ON PAYPAL!

### **PAYPAL VERIFICATION METHOD FOR AUTHORIZED USERS 2020 MAY**

I know it's not may yet, but the method has been leaked at 29th april.

First, we will need a VPN (I recommend private one with dedicated IP).

We will need a new email to use on Paypal. (So head over to cock.li and hit register, sign up for the email you want and then login to it at mail.cock.li. or any other mail provider you choose)

Now, we will need a US number; Head over to textnow with a US VPN on and get a number. If TextNow doesn't work you can use twilio or smsvpa (\$0.10) or you can buy numbers. (make sure that it's not used on paypal before)

Now we will head over to Paypal.com with our US VPN on and sign up for a personal account. You can use a fake name but not a blatantly fake name (Don't use James Bond or smth).

Now, for the address bit we will head over to <https://www.randomlists.com/new-york-addresses> and put in an address from there (Be sure to take a note of everything you put in).

We will put in the number we've got but not verify it. After this, verify your email. It will then tell

you to add a card or bank which we do not have, so let's get one.

Close out of paypal and connect to a UK VPN. Then, head over to <https://www.payoneer.com> and sign up. Use the same name as your paypal account, and use a Gmail address as the email (You need access to it).

Get the rest of the info from <https://fake-it.ws/gb/> and for the ID number just put in 9 random numbers. Wait 6-12 hours to get verified and then head over to Payoneer again and sign in to the account you made. Choose the "Global Payment Service" option, and then navigate to the "USD" bit. You will see your bank which you now have (If it says under review just wait another day and re-login). Copy your bank details and then connect to your US VPN again and login to Paypal. Add those bank details on there and choose "Verify Bank". It will say they sent two amounts to your bank which you need to put in.

Wait 24h and login to Payoneer again (With a UK VPN) and go to view transactions to see the amounts. Login to Paypal with your US VPN and then put in the amounts. Then our account is verified (hope so). But not so fast, you must wait 24h again and then log back in (Using your US VPN). Your account will be limited. You must go to the remove limitations page and choose Verify Bank with the amounts and then put them in. Now, go to Verify Identity and hit resolve then choose continue. It will send a SMS to your number, put in the code (If you verified your phone number before and it showed up as verified in account settings it will not work and say the phone number doesn't belong to you).

Then, Hit resolve next to change password and change it. Log out and log back in and your account is fully verified with its limitations removed.

(This step is optional) Next, go to <https://www.ssn-verify.com/> generate and choose New York and the year of the DOB on your account and hit generate. Go to account settings and put in that SSN for further verification

## THE ULTIMATE OPSEC GUIDE

DIIn the past few days I've seen many questions about OPSEC and how to set up your system and be almost untraceable while doing naughty things, therefore I decided to post this ultimate guide which will cover everything that is necessary and even more (if you want to be extra safe). I will begin with first part and if there is many people who are interested in this topic I will continue posting on this topic. It will probably consist of couple parts. So there we go:

As a fraudster, the first thing you need to have done, is your Opsec (Operational Security). If you live and do fraud in high risk countries such as USA, Canada, UK, then your Opsec must be rock solid.

If you live in Africa, India and other low risk countries, in that case OPSEC matters less. The good thing of fraud is that if you have decent opsec, you will never worry about ending up in jail, unlike selling drugs etc. The opsec that I give here is simple yet extremely effective. Follow it to the line and you will be safe, rest assured.

**Hardware:** You will require a burner laptop, avoid at all costs desktop pcs, as you can't bring them with you, plus if there is a raid going on from LE, you will find it harder to get rid of it/hide it. Here are the general specs that you will need to work proficiently: a minimum of a 8GB RAM and I5 processor laptop will be enough to handle all the apps and processes running into the VM. Don't include any of your personal information here. Another thing you will need is a burner

smartphone. I highly recommend an android one, as iOS is far too limited. You might need this one when you will do mobile carding, although you can execute mobile carding even from your laptop (not gonna get too much into this).

**USB Stick key:** Make sure it has plenty of gigabytes, you will store all your portable applications and some of the illegal data here. In case you are in troubles, you can throw away/ destroy it and all the evidence will be gone. Now, where to execute your fraud activities? I hear non-sense on forum such as going to the public library, use their wi-fi, go to an internet cafe and use their internet. Avoid at all costs public places. It doesn't look good that you browse some onion site and/or a clearnet cc autoshop. Long story short, make sure you are in a place where no one can spy on you.

**Software:** Now that you have a laptop, you need to install the software, first of all, you will install VMware or VirtualBox. They both basically serve the same purpose, however VMware is not free, therefore it runs a little bit smoother, however I would suggest avoid buying legit licenses, or using licenses that you get at university/work etc. You can find it free on the internet too if you dig deep enough, but personally I use VirtualBox since it's free and as I said, serves literally the same purpose. Anyway it is up for you to decide on this one .

After installing VMware or VirtualBox, proceed and create a virtual machine, and install an operating system on that. I would suggest using Windows7, since believe it or not, majority of the computers are still running. In addition, getting a copy of win7 is pretty easy and you can find activation keys all over the internet. Make sure to give plenty of space for windows VM, since it takes a bunch of space, and the more space you give the better it will run (given the fact that your pc is not a potato).

Now Install the following softwares on the machine: Mozilla Firefox (regular browsing), Mozilla Thunderbird (email management) Tor browser, ICQ(messaging) Team Viewer, Viscosity (DNS leak prevention) Cleaner (system cleaner) Bleachbit (additional cleaner) Mozbackup (Profile saver for Firefox). These are the basics that you will most likely need with whatever method you will use(except mobile emulator setups). **AND VERY IMPORTANT PART FOR CARDING. GET Yourself a LINKEN SPHERE browser, since nowadays it is the most reliable browser for carding. Not many people know this but even AD 7.4 is trashed now for like 4 months and it leaks data that indicates that you are not who you are claiming to be. As a result, you will burn many cards and will struggle a lot with carding, however LINKEN SPHERE covers all your tracks and does not leak anything.**

**Encryption:** Ok let's touch a fundamental topic about security, encryption. Here's the bad news, encryption won't always hide 100% your illegal files, as a matter of fact many fraudsters get caught and the evidence extracted, but I still highly suggest to encrypt your illegal data. You can use Veracrypt to encrypt your virtual machine. I strongly suggest to encrypt your Virtual machines. You can look it up on youtube, however it is not an easy task if you don't have a clue what you're doing. I might share it later if many people will try to set up their OPSEC and will struggle on this part .

**VPN:** Now, you also need to install a good VPN. It stands for Virtual Private Network, it will aid in hiding your real IP and keep you protected online. A good VPN must pass this checklist:

- 1) Does not store logs: this is important as if they store your IP and Law Enforcement demands for it, you are practically screwed
- 2) Non- Usa one: American VPNS are forced to give logs if LE asks for it by law hence avoid VPNs from USA even if they claim they do not keep logs
- 3) Fast: Virtual carding is slow itself when you add a VPN and socks, so make sure your VPN is blazing fast and pick a server that is closest to your location
- 4) Has a killswitch: Let's assume the connection from vpn server drops, your real IP is practically

naked! (except if you are under a socks5, but LE can still do a traceback and find you), so your VPN provide must have a killswitch feature that kills your App if that happens.

5) DNS leak protection: This can be annoying so make sure your VPN provider helps you with that

6) Payment by BTC allowed: Of course you want to keep yourself anonymous even by payment method wise, so make sure the VPN accepts BTC

7) Auto login and connect and start up: It's annoying to always launch the VPN and connect it by yourself, so make sure your VPN allows you to connect and login on windows start.

Luckily boys, I'm here for you and I suggest using Mullvad, since it is probably the most reliable VPN on the market and passes this checklist. It costs like 7\$ a month and is fairly simple to use.

After your illegal operations, you have to clear all your traces from both your host and Virtual Machine. We do so by running CCleaner and Bleachbit. You have to check all the checkboxes, ensuring that all the traces in your computer will be removed, don't check wipe free space or it's going to take too long. Also, you have to use the 35 Gutmann steps cleaning, ensuring that the files will be permanently deleted.

In the options of Ccleaner make sure to check "secure file deletion box" and very complex overwrite (35 passes) is chosen.

**Final words on security:** Yes, being safe is important, but don't push it too far, there's a mental disease that I call opsec paranoia, as if their security setup is never enough, I also learned that the more security you add the more frustrating fraud gets, in fact I've seen some fraudsters with double kill switched VPN. One is more than enough. Remember that there's always a small risk that you get caught. From my experience, a burner laptop with encrypted illegal data and a kill switched VPN is more than enough to keep you safe without too many hassles, also make sure your key apps like browser etc are killswitched, many forget about this (don't need to do that on Mullvad, since it blocks the internet connection on default killswitch settings).

I think this is it for the security, so if you find this information useful, please click the like button and comment on the post, therefore I will know that I'm not doing this for nothing. Don't be lazy boys set up your OPSEC as it will save your asses. This is a very basic security setup, however it is crucial for any fraudster. Personally, I'm using a bit more complex system, which is pretty hard to setup, but if you are new just stick to this one .

If I missed some crucial parts just hit me up and I will try to cover it, by editing this post.

On the next part we will cover spoofing and I'll give you information on how webpages track all your information and how to minimize what they can see, which is also crucial part for success.

-----  
**WRITTEN BY UNKNOWN CARDER BUT THANKS FOR SHARING**

## **THE PARANOID SECURITY GUIDE 2020**

### **Table of Contents:**

#### **Introduction**

#### **Basic Considerations**

## **BIOS-Passwords**

### **Encryption**

**Making TrueCrypt Portable**

**Hardware Encryption**

**Attacks on Full-Disk-Encryption**

**Attacks on encrypted Containers**

**Debian's encrypted LVM pwned**

**Solutions**

**eCryptfs**

**Encrypting SWAP using eCryptfs**

**Tomb**

**Advanced Tomb-Sorcery**

### **Keyloggers**

**Software Keyloggers**

**Defense against Software Keyloggers**

**Hardware Keyloggers**

**Defense against Hardware Keyloggers**

### **Secure File-Deletion**

**BleachBit**

**srm [secure rm]**

**Other Ways to securely wipe Drives**

### **Your Internet-Connection**

**ipkungfu**

**Configuring /etc/sysctl.conf**

**Modem & Router**

### **Intrusion-Detection, Rootkit-Protection & AntiVirus**

**Snort**

**RKHunter**

**RKHunter-Jedi-Tricks**

**chkrootkit**

**Tiger**

**Lynis**

**debsums**

**sha256**

**ClamAV**

### **DNS-Servers**

**Using secure and censor-free DNS**

**DNSEncrypt**

### **Firefox/Iceweasel**

**Firefox-Sandbox: Sandfox**

**Firefox-Preferences**

**Plugins**

**Addons**

**SSL-Search-Engines**

**Flash-Settings**  
**about:config**  
**Prevent Browser-Fingerprinting**

**TOR [The Onion Router]**  
**TOR-Warning**

**I2P**

**Freenet**

**Secure Peer-to-Peer-Networks**

**Mesh-Networks**

**Proxies**  
**Proxy-Warning**

**VPN (Virtual Private Network)**

**The Web**  
**RSS-Feeds**

**Secure Mail-Providers**

**Disposable Mail-Addresses**

**Secure Instant-Messaging/VoIP**  
**TorChat**  
**OTR [Off-the-Record-Messaging]**  
**Secure and Encrypted VoIP**

**Social Networking**  
**Facebook**  
**Alternatives to Facebook**

**Passwords**  
**pwgen**  
**KeePass**

**Live-CDs and VM-Images that focus on security and anonymity**  
**Further Info/Tools**

**Introduction**

Hi all!

This is my first attempt to contribute something to the community. Basically you can find everything I write here somewhere else on the web or in some book - but exactly that is the problem. You can literally spend weeks digging up all this stuff. And to save you some trouble I thought: "Heck, let's just put this into a little manual."



You're dealing with a somewhat paranoid security setup for debian-based systems like #!.  
[This is the end-user and not the |-|4xx0|2-version. We are not getting into virtual-virtual-virtual-machine-double-vpn-ssh-proxy-chain-from-your-internet-cafe-type-stuff.]

In this small guide I simply provide several "recipes" for securing both your box and your internet-connection and web-applications. I won't go into the why of all of this in too much detail as I want to provide a simple how-to that people can follow to make their system more secure without having to read through hundreds of pages of explanations. This information can easily be found elsewhere. If you're interested in a certain topic then just fire up a web-search and give it a read.

This guide is not exhaustive of course. As they say, security is a process - and so this guide can only be a place to start which needs to be adjusted to your personal needs.

If you consider to use this information and you find something to be too overcautious for your particular need - just ignore it and move on. One last thing before we begin: I am not a "security-guru" (far from it) - but more appropriately (as my nick suggests) some dude wrapping his head around things...

## **Basic considerations**

### **BIOS-Passwords**

For the physical security of your data you should always employ encrypted drives. But before we get to that make sure you set strong passwords in BIOS for both starting up and modifying the BIOS-settings. Also make sure to disable boot for any media other than your harddrive.

## **Encryption**

With #! this is easy. In the installation you can simply choose to use an encrypted LVM. (For those of you who missed that part on installation and would still like to use an encrypted partition withouth having to reinstall: use these instructions to get the job done.) For other data, e.g. data you store on transportable media you can use TrueCrypt - which is better than e.g. dmccrypt for portable media since it is portable, too. You can put a folder with TrueCrypt for every OS out there on to the unencrypted part of your drive and thus make sure you can access the files everywhere you go.

This is how it is done:

### **Making TrueCrypt Portable**

Download yourself some TC copy.

Extract the tar.gz

Execute the setup-file

When prompted choose "Extract .tar Package File"

go to /tmp

copy the tar.gz and move it where you want to extract/store it

extract it

once it's unpacked go to "usr"->"bin" grab "truecrypt"-binary

copy it onto your stick

give it a test-run

There is really not much more in that tarball than the binary. Just execute it and you're ready for some crypto.

I don't recommend using TrueCrypt's hidden container, though. Watch this vid to find out why. If you don't yet know how to use TrueCrypt check out this guide. [TrueCrypt's standard encryption is AES-256. This encryption is really good but there are ways to attack it and you don't know how advanced certain people already got at this. So when prompted during the creation of a TrueCrypt container use: AES-Twofish-Serpent and as hash-algorithm use SHA-512. If you're not using the drive for serious video-editing or such you won't notice a difference in performance. Only the encryption process when creating the drive takes a little longer. But we get an extra scoop of security for that... wink]

## **Hardware Encryption**

There are three different types of hardware encrypted devices available, which are generally called: SED (Self Encrypting Devices)

- Flash-Drives (Kingston etc.)
- SSD-Drives (Samsung etc.)
- HD-Drives (WD, Hitachi, Toshiba etc.)

They all use AES encryption. The key is generated within the device's microprocessor and thus no crucial data - neither password nor key are written to the host system. AES is secure - and thus using these devices can give some extra protection.

But before you think that all you need to do is to get yourself one of these devices and you're safe - I have to warn you: You're not.

So let's get to the reasons behind that.

## **Attacks on Full-Disk-Encryption**

Below we will have a look at a debian specific attack using a vulnerability common with encrypted LVMs.

But you need to be aware that all disk-encryption is generally vulnerable - be it software- or hardware-based. I won't go into details how each of them work exactly - but I will try to at least provide you with a short explanation.

For software-based disk-encryption there are these known attacks:

- DMA-Attacks (DMA/HDMI-Ports are used to connect to a running, locked machine to unlock it)
- Cold-Boot-Attacks (Keys are extracted from RAM after a cold reboot)
- Freezing of RAM (RAM is frozen and inserted into the attacker's machine to extract the key)

- Evil-Maid-Attacks (Different methods to boot up a trojanized OS or some kind of software-keylogger)

For hardware-based disk-encryption there are similar attacks:

- DMA-Attacks (same as with SW-based encryption)

- Replug-Attacks (Drive's data cable is disconnected and connected to attacker's machine via SATA-hotplugging)

- Reboot-Attacks (Drive's data cable is disconnected and connected to attacker's machine after enforced reboot. Then the bios-password is circumvented through the repeated pressing of the F2- and enter-key. After the bios integrated SED-password has been disabled the data-cable is plugged into the attacker's machine. This only works on some machines.)

- Networked-Evil-Maid-Attacks (Attacker steals the actual SED and replaces it with another containing a trojanized OS. On bootup victim enters it's password which is subsequently send to the attacker via network/local attacker hot-spot. Different method: Replacing a laptop with a similar model [at e.g. airport/hotel etc.] and the attacker's phone# printed on the bottom of the machine. Victim boots up enters "wrong" password which is send to the attacker via network. Victim discovers that his laptop has been misplaced, calls attacker who now copies the content and gives the "misplaced" laptop back to the owner.)

A full explanation of all these attacks been be found in this presentation. (Unfortunately it has not yet been translated into English.) An English explanation of an evil-maid-attack against TrueCrypt encrypted drives can be found here

### **Attacks on encrypted Containers**

There are also attacks against encrypted containers. They pretty much work like cold-boot-attacks, without the booting part.

An attacker can dump the container's password if the computer is either running or is in hibernation mode - either having the container open and even when the container has been opened during that session - using temporary and hibernation files.

### **Debian's encrypted LVM pwned**

This type of "full" disk encryption can also be fooled by an attack that could be classified as a custom and extended evil-maid-attack. Don't believe me? Read this!

The problem basically is that although most of the filesystem and your personal data are indeed encrypted - your boot partition and GRUB aren't. And this allows an attacker with physical access to your box to bring you into real trouble.

To avoid this do the following:

Micah Lee wrote:

If you don't want to reinstall your operating system, you can format your USB stick, copy /boot/\* to it, and install grub to it. In order to install grub to it, you'll need to unmount /boot, remount it as your USB device, modify /etc/fstab, comment out the line that mounts /boot, and then run grub-install /dev/sdb (or wherever your USB stick is). You should then be able to boot from your USB

stick.

An important thing to remember when doing this is that a lot of Ubuntu updates rewrite your `initrd.img`, most commonly kernel upgrades. Make sure your USB stick is plugged in and mounted as `/boot` when doing these updates. It's also a good idea to make regular backups of the files on this USB stick, and burn them to CDs or keep them on the internet. If you ever lose or break your USB stick, you'll need these backups to boot your computer.

One computer I tried setting this defense up on couldn't boot from USB devices. I solved this pretty simply by making a grub boot CD that chainloaded to my USB device. If you google "Making a GRUB bootable CD-ROM," you'll find instructions on how to do that. Here's what the `menu.1st` file on that CD looks like:

```
default 0
timeout 2
title Boot from USB (hd1)
root (hd1)
chainloader +1
```

I can now boot to this CD with my USB stick in, and the CD will then boot from the USB stick, which will then boot the closely watched `initrd.img` to load Ubuntu. A little annoying maybe, but it works.

(Big thanks to Micah Lee!)

Note: Apparently there is an issue with installing GRUB onto USB with `waldorf/wheezy`. As soon as I know how to get that fixed I will update this section.

## Solutions

You might think that mixing soft- and hardware-based encryption will solve these issues. Well, no. They don't. An attacker can simply chain different methods and so we are back at square one. Of course this makes it harder for an attacker to reach his goals - but he/she will not be stopped by it. So the only method that basically remains is to regard full-disk-encryption as a first layer of protection only.

Please don't assume that the scenarios described above are somewhat unrealistic. In the US there are about 5000 laptops being lost or stolen each week on airports alone. European statistics indicate that about 8% of all business-laptops are at least once either lost or stolen.

A similar risk is there if you leave the room/apartment with your machine locked - but running. So the first protection against these methods is to always power down the machine. Always.

The next thing to remind yourself off is: You cannot rely on full-disk-encryption. So you need to employ further layers of encryption. That means that you will have to encrypt folders containing sensitive files again using other methods such as `tomb` or `TrueCrypt`. That way - if an attacker manages to get hold of your password he/she will only have access to rather unimportant files. If you have sensitive or confidential data to protect full-disk encryption is not enough!

When using encrypted containers that contain sensitive data you should shutdown your computer after having used them to clear all temporary data stored on your machine that could be used by an attacker to extract passwords.

If you have to rely on data being encrypted and would be in danger if anyone would find the data you were encrypting you should consider only using a power-supply when using a laptop - as opposed to running on power and battery. That way if let's say, you live in a dictatorship or the mafia is out to get you - and they are coming to your home or wherever you are - all you need to do when you sense that something weird is going on is to pull the cable and hope that they still need at least 30 secs to get to your ram. This can help prevent the above mentioned attacks and thus keep your data safely hidden.

## **eCryptfs**

If for some reason (like performance or not wanting to type in thousands of passwords on boot) you don't want to use an encrypted LVM you can use ecryptfs to encrypt files and folders after installation of the OS.

To find out about all the different features of ecryptfs and how to use them I would like to point you to [bodhi.zazen's excellent ecryptfs-tutorial](#).

But there is one thing that is also important for later steps in this guide and is generally a good idea to do:

### **Encrypting swap using ecryptfs**

Especially when using older machines with less ram than modern computers it can happen quite frequently that your machine will use swap for different tasks when there's not enough ram available to do the job. Apart from the lack of speed this isn't very nice from a security standpoint: as the swap-partition is not located within your ram but on your harddrive - writing into this partition will leave traces of your activities on the harddrive itself. If your computer happens to use swap during your use of encryption tools it can happen that the passwords to the keys are written to swap and are thus extractable from there - which is something you really want to avoid.

You can do this very easily with the help of ecryptfs.

First you need to install it:

```
$ sudo apt-get install ecryptfs-utils cryptsetup
```

Then we need to actually encrypt our swap using the following command:

```
$ sudo ecryptfs-setup-swap
```

Your swap-partition will be unmounted, encrypted and mounted again.

To make sure that it worked run this command:

```
$ sudo blkid | grep swap
```

The output lists your swap partition and should contain "cryptswap".

To avoid error messages on boot you will need to edit your `/etc/fstab` to fit your new setup:

```
$ sudo geany /etc/fstab
```

Copy the content of that file into another file and save it. You will want to use it as back-up in case something gets screwed up.

Now make sure to find the entry of the above listed encrypted swap partition. If you found it go ahead and delete the other swap-entry relating to the unencrypted swap-partition. Save and reboot to check that everything is working as it should be.

## **Tomb**

Another great crypto-tool is Tomb provided by the dyne-crew.

Tomb uses LUKS AES/SHA-256 and can thus be consider secure. But Tomb isn't just a possible replacement for tools like TrueCrypt.

It has some really neat and easy to use features:

- 1) Separation of encrypted file and key
- 2) Mounting files and folders in predefined places using bind-hooks
- 3) Hiding keys in picture-files using steganography

The documentation on Tomb I was able to find, frankly, seems to be scattered all over the place. After I played around with it a bit I also came up with some tricks that I did not see being mentioned in any documentation.

And because I like to have everything in one place I wrote a short manual myself:

Installation:

First you will need to import dyne's keys and add them to your gpg-keylist:

```
$ sudo gpg --fetch-keys http://apt.dyne.org/software.pub
```

Now verify the key-fingerprint.

```
$ sudo gpg --fingerprint software@dyne.org | grep fingerprint
```

The output of the above command should be:

```
Key fingerprint = 8E1A A01C F209 587D 5706 3A36 E314 AFFA 8A7C 92F1
```

Now, after checking that you have the right key you can trust add it to apt:

```
$ sudo gpg --armor --export software@dyne.org > dyne.gpg  
$ sudo apt-key add dyne.gpg
```

After you did this you want to add dyne's repos to your sources.list:

```
$ sudo geany /etc/apt/sources.list
```

Add:

```
deb http://apt.dyne.org/debian dyne main
deb-src http://apt.dyne.org/debian dyne main
```

To sync apt:

```
$ sudo apt-get update
```

To install Tomb:

```
$ sudo apt-get install tomb
```

Usage:

If you have your swap activated Tomb will urge you to turn it off or encrypt it. If you encrypt it and leave it on you will need to include `--ignore-swap` into your tomb-commands. To turn off swap for this session you can run

```
$ swapoff -a
```

To disable it completely you can comment out the swap in `/etc/fstab`. So it won't be mounted on reboot. (Please be aware that disabling swap on older computers with not much ram isn't such a good idea. Once your ram is being used fully while having no swap-partition mounted processes and programs will crash.)

Tomb will create the crypto-file in the folder you are currently in - so if you want to create a tomb-file in your documents-folder make sure to

```
$ cd /home/user/documents
```

Once you are in the right folder you can create a tomb-file with this command:

```
$ tomb -s XX create FILE
```

XX is used to denote the size of the file in MB. So in order to create a file named "test" with the size of 10MB you would type this:

```
$ tomb -s 10 create test
```

Please note that if you haven't turned off your swap you will need to modify this command as follows:

```
$ tomb --ignore-swap -s 10 create test
```

To unlock and mount that file on `/media/test` type:

```
$ tomb open test.tomb
```

To unlock and mount to a different location:

```
$ tomb open test.tomb /different/location
```

To close that particular file and lock it:

```
$ tomb close /media/test.tomb
```

To close all tomb-files:

```
$ tomb close all
```

or simply:

```
$ tomb slam
```

After these basic operations we come to the fun part:

### **Advanced Tomb-Sorcery**

Obviously having a file lying around somewhere entitled: "secret.tomb" isn't such a good idea, really.

A better idea is to make it harder for an attacker to even find the encrypted files you are using. To do this we will simply move its content to another file.

Example:

```
$ touch true-story.txt true-story.txt.key  
$ mv secret.tomb true-story.txt  
$ mv secret.tomb.key true-story.txt.key
```

Now you have changed the filename of the encrypted file in such a way that it can't easily be detected.

When doing this you have to make sure that the filename syntax tomb uses is conserved:

```
filename.suffix  
filename.suffix.key
```

Otherwise you will have trouble opening the file.

After having hidden your file you might also want to move the key to another medium.

```
$ mv true-story.txt.key /medium/of/your/choice
```

Now we have produced quite a bit of obfuscation. Now let's take this even further:

After we have renamed our tomb-file and separated key and file we now want to make sure our key can't be found either.

To do this we will hide it within a jpeg-file.

```
$ tomb bury true-story.txt.key invisible-bike.jpg
```

You will need to enter a steganography-password in the process.



Now rename the original keyfile to something like "true-story.txt.key-backup" and check if everything worked:

```
$ tomb exhume true-story.txt.key invisible-bike.jpg
```

Your key should have reappeared now. After making sure that everything works you can safely bury the key again and delete the residual key that usually stays in the key's original folder.

By default Tomb's encrypted file and key need to be in one folder. If you have separated the two you will have to modify your opening-command:

```
$ tomb -k /medium/of/your/choice/true-story.txt.key open true-story.txt
```

To change the key-files password:

```
$ tomb passwd true-story.txt.key
```

If, let's say, you want to use Tomb to encrypt your icedove mail-folders you can easily do that. Usually it would be a pain in the butt to do this kind of stuff with e.g. truecrypt because you would need to setup a container, move the folder to the container and when using the folder you would have to move back to its original place again.

Tomb does this with ease:

Simply move the folders you want to encrypt into the root of the tomb-file you created.

Example:

You want to encrypt your entire .icedove folder. Then you make a tomb-file for it and move the .icedove folder into that tomb. The next thing you do is create a file named "bind-hooks" and place it in the same dir. This file will contain a simple table like this:

```
.icedove .icedove  
.folder-x .folder-x  
.folder-y .folder-y  
.folder-z .folder-z
```

The first column denotes the path relative to the tomb's root. The second column represents the path relative to the user's home folder.

So if you simply wanted to encrypt your .icedove folder - which resides in /home/user/ the above notation is fine. If you want the folder to be mounted elsewhere in your /home you need to adjust the lines accordingly.

One thing you need to do after you moved the original folder into the tomb is to create a dummy-folder into which the original's folders content can be mounted. So you simply go into /home/user and create a folder named ".icedove" and leave it empty.

The next time you open and mount that tomb-file your .icedove folder will be where it should be and will disappear as soon as you close the tomb. Pretty nice, hu?

I advise to test this out before you actually move all your mails and prefs into the tomb. Or simply

make a backup. But use some kind of safety-net in order not to screw up your settings.

## **Keyloggers**

Keyloggers can pose a great threat to your general security - but especially the security of your encrypted drives and containers. If someone manages to get a keylogger onto your system he/she will be able to collect all the keystrokes you make on your machine. Some of them even make screenshots.

So what kind of keyloggers are there?

### **Software Keyloggers**

For linux there are several software-keyloggers available. Examples are lkl, uberkey, THC-vlogger, PyKeylogger, logkeys.

### **Defense against Software Keyloggers**

#### 1) Never use your system-passwords outside of your system

Generally everything that is to be installed under linux needs root access or some privileges provided through /etc/sudoers. But an attacker could have obtained your password if he/she was using a browser-exploitation framework such as beef - which also can be used as a keylogger on the browser level. So if you have been using your sudo or root password anywhere on the internet it might have leaked and could thus be used to install all kinds of evil sh\*t on your machine. Keyloggers are also often part of rootkits. So do regular system-checks and use intrusion-detection-systems.

#### 2) Make sure your browser is safe

Often people think of keyloggers only as either a software tool or a piece of hardware equipment installed on their machine. But there is another threat that is actually much more dangerous for linux users: a compromised browser. You will find a lot of info on how to secure your browser further down. So make sure you use it.

Compromising browsers isn't rocket science. And since all the stuff that is actually dangerous in the browser is cross-plattform - you as a linux-user aren't safe from that. No matter what short-sighted linux-enthusiasts might tell you. A java-script exploit will pwn you - if you don't secure your browser. No matter if you are on OSX, Win or debian.

#### 3) Check running processes

If your attacker isn't really skilled or determined he/she might not think about hiding the process of the running keylogger. You can take a look at the output of

```
$ ps -aux
```

or

```
$ htop
```

or

\$ pstree

and inspect the running processes. Of course the attacker could have renamed it. So have a look for suspicious processes you have never heard of before. If in doubt do a search on the process or ask in a security-related forum about it.

Since a lot of keyloggers come as the functionality of a rootkit it would be much more likely that you would have one of these.

#### 4) Do daily scans for rootkits

I will describe tools for doing that further below. RKHunter and chkrootkit should definitely be used. The other IDS-tools described give better results and are much more detailed - but you actually need to know a little about linux-architecture and processes to get a lot out of them. So they're optional.

#### 5) Don't rely on virtual keyboards

The idea to defeat a keylogger by using a virtual keyboard is nice. But is also dangerous. There are some keyloggers out there that will also capture your screen activity. So using a virtual keyboard is pretty useless and will only result in the false feeling of security.

### **Hardware Keyloggers**

There is also an ever growing number of hardware keyloggers. Some of which use wifi. And some of them can be planted inside your keyboard so you wouldn't even notice them if you inspected your hardware from the outside.

### **Defense against Hardware Keyloggers**

#### 1) Inspect your Hardware

This one's obvious.

#### 2) Check which devices are connected to your machine

There is a neat little tool called USBView which you can use to check what kind of usb-devices are connected to your machine. Some - but not all - keyloggers that employ usb will be listed there. It is available through the debian-repos.

\$ sudo apt-get install usbview

Apart from that there's not much you can do about them. If a physical attack is part of your thread-model you might want to think about getting a laptop safe in which you put the machine when not in use or if you're not around. Also, don't leave your laptop unattended at work, in airports, hotels and on conferences.

### **Secure File-Deletion**

Additional to encrypted drives you may also want to securely delete old data or certain files. For those who do not know it: regular "file deletion" does not erase the "deleted" data. It only unlinks the file's inodes thus making it possible to recover that "deleted" data with forensic software.

There are several ways to securely delete files - depending on the filesystem you use. The easiest is:

### **BleachBit**

With this little tool you can not only erase free disc space - but also clean your system from various temporary files you don't need any longer and that would give an intruder unnecessary information about your activities.

To install:

```
$ sudo apt-get install bleachbit
```

to run:

```
$ bleachbit
```

Just select what you need shredding. Remember that certain functions are experimental and may cause problems on your system. But no need to worry: BleachBit is so kind to inform you about that and give you the chance to cancel your selection.

Another great [and much more secure] tool for file deletion is:

### **srm [secure remove]**

```
$ sudo apt-get install secure-delete
```

Usage:

Syntax: `srm [-dflrvz] file1 file2 etc.`

Options:

- d ignore the two dot special files "." and "..".
- f fast (and insecure mode): no /dev/urandom, no synchronize mode.
- l lessens the security (use twice for total insecure mode).
- r recursive mode, deletes all subdirectories.
- v is verbose mode.
- z last wipe writes zeros instead of random data.

### **Other ways to securely wipe drives**

To overwrite data with zeros:

```
# dd if=/dev/zero of=/dev/sdX
```

or:

```
$ sudo dd if=/dev/zero of=/dev/sdX
```

To overwrite data with random data (makes it less obvious that data has been erased):

```
# dd if=/dev/urandom of=/dev/sdX
```

or:

```
$ sudo dd if=/dev/urandom of=/dev/sdX
```

Note: shred doesn't work reliably with ext3.  
Your Internet-Connection

Generally it is advised to use a wired LAN-connection - as opposed to wireless LAN (WLAN). For further useful information in regards to wireless security read this. If you must use WLAN please use WPA2 encryption. Everything else can be h4xx0red by a 12-year-old using android-apps such as anti.

Another thing is: Try only to run services on your machine that you really use and have configured properly. If e.g. you don't use SSH - deinstall the respective client to make sure to save yourself some trouble. Please note that IRC also is not considered to be that secure. Use it with caution or simply use a virtual machine for stuff like that.

If you do use SSH please consider using Denyhosts or SSHGuard. (If you want to find out what might happen if you don't use such protection see foozer's post.)

So, let's begin with your firewall. For debian-like systems there are several possible firewall-setups and different guis to do the job. However, I found ipkungfu [an iptables-script] to do the best job while being easy to set up. This is how you set it up:

### **ipkungfu [basic configuration]**

download and install:

```
$ sudo apt-get install ipkungfu
```

configure:

```
$ sudo geany /etc/ipkungfu/ipkungfu.conf
```

uncomment (and adjust):

```
# IP Range of your internal network. Use "127.0.0.1"
# for a standalone machine. Default is a reasonable
# guess.
LOCAL_NET="192.168.1.0/255.255.255.0"
```

---

```
# Set this to 0 for a standalone machine, or 1 for
# a gateway device to share an Internet connection.
# Default is 1.
GATEWAY=0
```

---

```
# Temporarily block future connection attempts from an
```

```
# IP that hits these ports (If module is present)
FORBIDDEN_PORTS="135 137 139"
```

---

```
# Drop all ping packets?
# Set to 1 for yes, 0 for no. Default is no.
BLOCK_PINGS=1
```

---

```
# What to do with 'probably malicious' packets
#SUSPECT="REJECT"
SUSPECT="DROP"
```

---

```
# What to do with obviously invalid traffic
# This is also the action for FORBIDDEN_PORTS
#KNOWN_BAD="REJECT"
KNOWN_BAD="DROP"
```

---

```
# What to do with port scans
#PORT_SCAN="REJECT"
PORT_SCAN="DROP"
```

enable ipkungfu to start with the system:

```
$ sudo geany /etc/default/ipkungfu
```

change: "IPKFSTART = 0" ---> "IPKFSTART=1"

start ipkungfu:

```
$ sudo ipkungfu
```

fire up GRC's Shields Up! and check out the awesomeness.

(special thanks to the ubuntu-community)

### **Configuring /etc/sysctl.conf**

Here you set different ways how to deal with ICMP-packets and other stuff:

```
$ sudo geany /etc/sysctl.conf
```

```
# Do not accept ICMP redirects (prevent MITM attacks)
net.ipv4.conf.all.accept_redirects=0
net.ipv6.conf.all.accept_redirects=0
net.ipv4.tcp_syncookies=1
```

```
#lynis recommendations
#net.ipv6.conf.default.accept_redirects=0
net.ipv4.tcp_timestamps=0
net.ipv4.conf.default.log_martians=1
# TCP Hardening - http://www.cromwell-intl.com/security/security-stack-hardening.html
net.ipv4.icmp_echo_ignore_broadcasts=1
net.ipv4.conf.all.forwarding=0
net.ipv4.conf.all.rp_filter=1
net.ipv4.tcp_max_syn_backlog=1280
kernel.core_uses_pid=1
kernel.sysrq=0
#ignore all ping
net.ipv4.icmp_echo_ignore_all=1
# Do not send ICMP redirects (we are not a router)
net.ipv4.conf.all.send_redirects = 0
# Do not accept IP source route packets (we are not a router)
net.ipv4.conf.all.accept_source_route = 0
net.ipv6.conf.all.accept_source_route = 0
# Log Martian Packets
net.ipv4.conf.all.log_martians = 1
```

After editing do the following to make the changes permanent:

```
sudo sysctl -p
```

(thanks to tradetaxfree for these settings)

## **Modem & Router**

Please don't forget to enable the firewall features of your modem (and router), disable UPnP and change the usernames and admin-passwords. Also try to keep up with the latest security info and updates on your firmware to prevent using equipment such as this. You might also want to consider setting up your own firewall using smoothwall.

Here you can run a short test to see if your router is vulnerable to UPnP-exploits.

The best thing to do is to use after-market-open-source-firmware for your router such as dd-wrt, openwrt or tomato. Using these you can turn your router into an enterprise grade device capable of some real Kungfu. Of course they come with heavy artillery - dd-wrt e.g. uses an IP-tables firewall which you can configure with custom scripts.

## **Intrusion-Detection, Rootkit-Protection & AntiVirus**

### **snort [basic configuration]**

The next thing you might want to do is to take a critical look at who's knocking at your doors.

For this we use snort. The setup is straight forward and simple:

```
$ sudo apt-get install snort
```

run it:

\$ snort -D (to run as daemon)

to check out packages live type:

\$ sudo snort

Snort should automatically start on reboot.

If you want to check out snort's rules take a look at: /etc/snort/rules

To take a look at snorts warnings:

\$ sudo geany /var/log/snort/alert

Snort will historically list all the events it logged.

There you will find nice entries like this...

```
[**] [1:2329:6] MS-SQL probe response overflow attempt [**]  
[Classification: Attempted User Privilege Gain] [Priority: 1]  
[Xref => http://www.securityfocus.com/bid/9407]
```

...and will thank the flying teapot that you happen to use #! wink

## **RKHunter**

The next thing to do is to set up RKHunter - which is short for [R]oot[K]itHunter.

What does it do? You guessed it: It hunts down rootkits.

Installation again is simple:

\$ sudo apt-get install rkhunter

The best is to run rkhunter on a clean installation - just to make sure nothing has been tampered with already.

One very important thing about rkhunter is that you need to give it some feedback: everytime you e.g. make an upgrade to your sytem and some of your binaries change rkhunter will weep and tell you you've been compromised. Why? Because it can only detect suspicious files and file-changes. So, if you go about and e.g. upgrade the coreutils package a lot of change will be happening in /usr/bin - and when you subsequently ask rkhunter to check your system's integrity your log file will be all red with warnings. It will tell you that the file-properties of your binaries changed and you start freaking out. To avoid this simply run the command rkhunter --propupd on a system which you trust to not have been compromised.

In short: directly after commands like apt-get update && apt-get upgrade run:

\$ sudo rkhunter --propupd

This tells rkhunter: 'sall good. wink



To run rkhunter:

```
$ sudo rkhunter -c --sk
```

You find rkhunter's logfile in /var/log/rkhunter.log. So when you get a warning you can in detail check out what caused it.

To set up a cronjob for RKHunter:

```
$ sudo geany /etc/cron.daily/rkhunter.sh
```

insert and change the mail-address:

```
#!/bin/bash
/usr/local/bin/rkhunter -c --cronjob 2>&1 | mail -s "RKHunter Scan Details" your@email-address.com
```

make the script executable:

```
$ sudo chmod +x /etc/cron.daily/rkhunter.sh
```

update RKHunter:

```
$ sudo rkhunter --update
```

and check if it functions the way it's supposed to do:

```
$ sudo rkhunter -c --sk
```

Of course you can leave out the email-part of the cronjob if you don't want to make the impression on someone shoulder-surfing  
your email-client that the only one who's sending you emails is your computer... wink

Generally, using snort and rkhunter is a good way to become paranoid - if you're not already. So please take the time to investigate the alerts and warnings you get. A lot of them are false positives and the listings of your system settings. Often enough nothing to worry about. But if you want to use them as security tools you will have to invest the time to learn to interpret their logs. Otherwise just skip them.

## **RKHunter-Jedi-Tricks**

If you're in doubt whether you did a rkhunter --propupd after an upgrade and you are getting a warning you can run the following command:

```
$ sudo rkhunter --pkgmgr dpkg -c --sk
```

Now rkhunter will check back with your package-manager to verify that all the binary-changes were caused by legitimate updates/upgrades. If you previously had a warning now you should get zero of them. If you still get a warning you can check which package the file that caused the warning belongs to.

To do this:

```
$ dpkg -S /folder/file/in/doubt
```

Example:

```
$ dpkg -S /bin/ls
```

Output:

```
coreutils: /bin/ls
```

This tells you that the file you were checking (in this case /bin/ls) belongs to the package "coreutils".

Now you can fire up packagesearch.

If you haven't installed it:

```
$ sudo apt-get install packagesearch
```

To run:

```
$ sudo packagesearch
```

In packagesearch you can now enter coreutils in the field "search for pattern". Then you select the package in the box below. Then you go over to the right and select "files". There you will get a list of files belonging to the selected package. What you want to do now is to look for something like:

```
/usr/share/doc/coreutils/changelog.Debian.gz
```

The idea is to get a file belonging to the same package as the file you got the rkhunter-warning for - but that is not located in the binary-folder.

Then you look for that file within the respective folder and check the file-properties. When it was modified at the same time as the binary in doubt was modified you can be quite certain that the change was caused by a legitimate update. I think it is safe to say that some script-kiddie trying to break into your system will not be that thorough. Also make sure to use debsums when in doubt. I will get to that a little further down.

Another neat tool with similar functionality is:

### **chkrootkit**

To install:

```
$ sudo apt-get install chkrootkit
```

To run:

```
$ sudo chkrootkit
```

Other nice intrusion detection tools are:

### **tiger**

Tiger is more thorough than rkhunter and chkrootkit and can aid big time in securing your box:

```
$ sudo apt-get install tiger
```

to run it:

```
$ sudo tiger
```

you find tiger's logs in /var/log/tiger/  
Lynis

If you feel that all the above IDS-tools aren't enough - I got something for you:

### **Lynis**

Lynis wrote:

Lynis is an auditing tool for Unix (specialists). It scans the system and available software, to detect security issues. Beside security related information it will also scan for general system information, installed packages and configuration mistakes.

This software aims in assisting automated auditing, software patch management, vulnerability and malware scanning of Unix based systems

I use it. It is great. If you think you might need it - give it a try. It's available through the debian repos.

```
$ sudo apt-get install lynis
```

To run:

```
$ sudo lynis -c
```

Lynis will explain its findings in the log-file.

### **debsums**

debsums checks the md5-sums of your system-files against the hashes in the respective repos.

Installation:

```
$ sudo apt-get install debsums
```

To run:

```
$ sudo debsums -ac
```

This will list all the files to which the hashes are either missing or have been changed. But please don't freak out if you find something like: /etc/ipkungfu/ipkungfu.conf after you have been

following this guide... wink

## **sha256**

There are some programs that come with sha256 hashes nowadays. For example: I2P

debsums won't help with that. To check these hashes manually:

```
$ cd /folder/you/downloaded/file/to/check/to -sha256sum -c file-you-want-to-check
```

Then compare it to the given hash. Note: This tool is already integrated to debian-systems.

## **ClamAV**

To make sure everything that gets into your system is clean and safe use ClamA[nti]V[irus].

To install:

```
$ sudo apt-get install clamav
```

To update:

```
$ sudo freshclam
```

To inspect e.g. your download folder:

```
$ sudo clamscan -ri /home/your-username/downloads
```

This will ClamAV do a scan recursively, i.e. also scan the content of folders and inform you about possibly infected files.

To inspect your whole system:

```
$ sudo clamscan -irv --exclude=/proc --exclude=/sys --exclude=/dev --exclude=/media --exclude=/mnt
```

This will make ClamAV scan your system recursively in verbose mode (i.e. show you what it is doing atm) whilst excluding folders that shouldn't be messed with or are not of interest and spit out the possibly infected files it finds. To also scan attached portable media you need to modify the command accordingly.

Make sure to test everything you download for possible infections. You never know if servers which are normally trustworthy haven't been compromised. Malicious code can be hidden in every usually employed filetype. (Yes, including .pdf!)

Remember: ClamAV is known for its tight nets. That means that you are likely to get some false positives from time to time. Do a web-search if you're in doubt in regards to its findings.

After you set up your host-based security measures we can now tweak our online security.

Starting with:

## **DNS-Servers**

### **Using secure and censor-free DNS**

To make changes to your DNS-settings:

```
$ sudo geany /etc/resolv.conf
```

change your nameservers to trustworthy DNS-Servers. Otherwise your modem will be used as "DNS-Server" which gets its info from your ISP's DNS.

And nah... We don't trust the ISP... wink

Here you can find secure and censor-free DNS-servers. The Germans look here.

HTTPS-DNS is generally preferred for obvious reasons.

Your resolv.conf should look something like this:

```
nameserver 213.73.91.35
#CCC DNS-Server
nameserver 85.214.20.141
#FoeBud DNS-Server
```

Use at least two DNS-Servers to prevent connectivity problems when one server happens to be down or experiences other trouble.

To prevent this file to be overwritten on system restart fire up a terminal as root and run:

```
$ sudo chattr +i /etc/resolv.conf
```

This will make the file unchangeable - even for root.

To revoke this for future changes to the .conf run:

```
$ sudo chattr -i /etc/resolv.conf
```

This forces your web-browser to use the DNS-servers you provided instead of the crap your ISP uses.

To test the security of your DNS servers go here.

## **DNSCrypt**

What you can also do to secure your DNS-connections is to use DNSCrypt.

The thing I don't like about DNSCrypt is one of its core functions: to use OpenDNS as your resolver. OpenDNS has gotten quite a bad rep in the last years for various things like aggressive advertising and hijacking google-searches on different setups. I tested it out yesterday and couldn't replicate these issues. But I am certain that some of these "features" of OpenDNS have been actively blocked by my Firefox-setup (which you find below). In particular the addon Request Policy seems to prevent to send you to OpenDNS' search function when you typed in an address it couldn't resolve. The particular issue about that search function is that it apparently is powered by yahoo! and thus yahoo! would log the addresses you are searching for.

Depending on your threat-model, i.e. if you don't do anything uber-secret you don't want anybody to know, you might consider using DNSCrypt, as the tool seems to do a good job at encrypting your DNS-traffic. There also seems to be a way to use DNSCrypt to tunnel your queries to a DNS-server other than OpenDNS - but I haven't yet checked the functionality of this.

So, if you don't mind that OpenDNS will know every website you visit you might go ahead and configure DNSCrypt:

Download the current version.

Then:

```
$ sudo bunzip2 -cd dnscrypt-proxy-*.tar.bz2 | tar xvf -  
$ cd dnscrypt-proxy-*
```

Compile and install:

```
$ sudo ./configure && make -j2  
$ sudo make install
```

Adjust -j2 with the number of cpu-cores you want to use for the compilation or have at your disposal.

Go and change your resolv.conf to use localhost:

```
$ geany /etc/resolv.conf
```

Modify to:

```
nameserver 127.0.0.1
```

Run DNSCrypt as daemon:

```
$ sudo dnscrypt-proxy --daemonize
```

According to the developer:  
jedist1 wrote:

DNSCrypt will chroot() to this user's home directory and drop root privileges for this user's uid as soon as possible.

I have to admit that OpenDNS is really fast. What you could do is this: You could use OpenDNS for your "normal" browsing. When you start browsing for stuff that you consider to be private for whatever reasons change your resolv.conf back to the trustworthy DNS-servers mentioned above - which you conveniently could keep as a backup file in the same folder. Yeah, that isn't slick, I know. If you come up with a better way to do this let me know. (As soon as I checked DNSCrypt's function to use the same encryption for different DNS-Servers I will make an update.)

The next thing on our list is:

**Firefox/Iceweasel**

**Firefox-Sandbox: Sandfox**

Sandbox is a neat little script provided by IgnorantGuru which runs firefox (and other applications) in a sandboxed environment which prevents firefox's access to crucial filesystem-areas in case it gets compromised.

To install:

```
$ sudo -s
$ gpg --keyserver keys.gnupg.net --recv-keys
7977070A723C6CCB696C0B0227A5AC5A01937621
$ gpg --check-sigs 0x01937621
$ bash -c 'gpg --export -a 01937621 | apt-key add -'
$ echo "deb http://ignorantguru.github.com/debian/ unstable main" >> /etc/apt/sources.list
$ apt-get update
$ apt-get install sandbox
```

(Thanks to tradetaxfree)

To run:

```
$ sudo sandbox firefox
```

Type "/" into firefox address-bar to check out whether it works. Firefox should now only have access to files it really needs to function and not e.g. /root.

To be able to download stuff from the web you need to add a bind in sandbox's default profile:

```
$ sudo geany /etc/sandbox/default.profile
```

add:

```
bind=/home/$user/downloads
```

Check your systems filename-capitalization to make sure you really grant sandbox access to the right folder

In #! you can easily set this configuration as your default: simply go to "settings"->"openbox"->"GUI Menu Editor"->"Openbox"->"Web Browser". Then simply add the command "sandbox firefox". For this to work you need to once run

```
$ sudo sandbox firefox
```

after a system start to create a sandbox. If you happen to find this too much hassle simply go with tradetaxfree's init-script.

After you successfully sandboxed your browser we now continue to make that particular application much more secure than it is by default.

First go to:

**Firefox-Preferences**

and change these settings:

[Some of these are defaults already - but depending on who was/is using the machine you access the interwebs with and other varying factors you might want to control these settings.]

"General"->"when Firefox starts"->"Show a blank page"  
"General"->"save files to:"Downloads"  
"Content"->check:"Block pop-up windows"  
"Content"->unchecked:"Enable JavaScript" [optional - NoScript Add-on will block it anyway]  
"Content"->"Fonts & Colors"->"Advanced"->"Serif": "Liberation Sans"  
"Content"->"Fonts & Colors"->"Advanced"->"Sans-serif": "Liberation Sans"  
"Content"->"Fonts & Colors"->"Advanced"->unchecked:"Allow pages to choose their own fonts"  
"Content"->"Languages"->choose \*only\*: "en-us" [remove all others, if any]  
"Applications"->choose: "Always ask" for every application - if not possible: choose: "Preview in Firefox/Nightly"  
"Privacy"->"Tracking"->check: "Tell websites I do not want to be tracked"  
"privacy"->"History"->"Firefox will: "Use custom settings for history"  
"privacy"->"History"->unchecked: "Always use private browsing mode"  
"privacy"->"History"->unchecked: "Remember my browsing and download history"  
"privacy"->"History"->unchecked: "Remember search and form history"  
"privacy"->"History"->unchecked: "Accept cookies from sites"  
"privacy"->"History"->unchecked: "Accept third-party cookies"  
"privacy"->"History"->check: "Clear history when Firefox/Nightly closes"  
"privacy"->"History"->"settings": check all -> except: "Site Preferences"  
[to enable cookies for certain trusted sites: use: "Exceptions" and paste URL of site and modify settings according to your preference. If you additionally use Cookie-Monster (Add-on) you need to uncheck "Block all cookies" in CM-Options]  
"privacy"->"location bar"->"When using the location bar, suggest: "->choose: "Nothing"  
"security"->check: "Warn me when sites try to install add-ons"  
"security"->check: "Block reported attack sites"  
"security"->check: "Block reported web forgeries"  
"security"->"Passwords"->unchecked: "Remember passwords for sites"  
"security"->"Passwords"->unchecked: "Use a master password"  
"advanced"->"General"->"System Defaults"->unchecked: "Submit crash reports"  
"advanced"->"General"->"System Defaults"->unchecked: "Submit performance data"  
"advanced"->"Update"->check: "Automatically install updates"  
"advanced"->"Update"->check: "Warn me if this will disable any of my add-ons"  
"advanced"->"Update"->check: "Automatically update Search Engines"  
"advanced"->"Encryption"->"Protocols"->check: "Use SSL 3.0"  
"advanced"->"Encryption"->"Protocols"->check: "Use TLS 1.0"  
"advanced"->"Encryption"->"Certificates"->"When a server requests my personal certificate"->check: "Ask me every time"

## Plugins

at the most use:

Java

Flash [Be aware of the latest security holes in flash!

Only allow them to run on trusted sites!



## Addons

Empty Cache Button [optional]

Calomel SSL Validation [cool little addon which does exactly what its name says and also has some more tweaks in the settings]

Adblock Edge

[---> Filter Supscriptions: make sure you get some anti-tracking filters up and running! (depending on location & internet use)]

Easylist

EasyPrivacy

fanboy-adblock

Fanboy's Tracking List

Fanboy's Annoyance List

[---]

BetterPrivacy [LSO/Flash-Cookie-Protection]

Cookie Monster [Allows you to Manage your Cookie-Policies. For less baggage use Firefox/Iceweasel "Preferences" -> "Privacy"]

HTTPS-Everywhere [Download via EFF.org] [settings: enable SSL-Observatory but don't allow to transmit ISP-data]

HTTPS Finder

NoScript [go to "settings" and check "also apply on whitelisted sites"]

Perspectives [SSL-Certificate-Control - go to settings: "notary servers" -> check "only contact when websites cause security error"]

RefControl [controls your HTTP-Referers - setting: "block" -> "3rd parties only"]

Request Policy [rejects cross-site requests]

WOT [Web of Trust - user based website ratings that show up in websearches. Caution: Not very accurate. Always double check when in doubt. This addon tends to get abused by different groups of users who either give malicious sites good ratings - or flag perfectly good sites.]

PwdHash [Nice addon to help your password management. Use "F2" when entering a password into a password field when setting up a new account somewhere to create a MD5-hash using your password and the domain. (When logging in you have to select the password-field and press F2 again to run the hashing.) This way you can use the same password on different sites without having

to worry about security implications - because every site gets its own password generated through the hash. The tool is provided by Stanford University and can be trusted. No data is actually transmitted to their servers. The hash is generated using your local java-script. If you need to login from a machine that doesn't have pwdhash installed: go to <https://www.pwdhash.com/> -> their SSL is very strong.]

FoxyProxy [a convenient Proxy Switcher]

Useragent Switcher [Does exactly that. But be careful: If you set your user-agent as shown below - using this addon it will overwrite these settings and will not automatically restore them if you turn off the switcher. So you would have to manually reconfigure about:config again. Which kinda sucks. But you can get a whole load really cool user agents here. Simply download the .xml and import it to the Useragent Switcher. There are really neat current agents in there: e.g. all kinds of different web browser for all OSs and of course various bots. Google bot comes in handy when you need access to some forum... wink]

Web Developer [Has some cool features. If you like inspecting websites just check it out.]

Bloody Vikings [Creates disposable mail-addresses]

Note: You don't need Ghostery. The above mentioned Adblock lists do a much better job protecting you from web-tracking without using the additional resourced Ghostery uses.

Of course there are more addons you could use. But I don't really see the point of them. Most of them either are snake-oil or even dangerous. But please inform me if you happen to come across something really cool which could help improve security which none of the setting provided here can do.

To keep your ISP and possible MITM-attackers from reading what you do on the web always use SSL - as far as it is available. To help with this use:

### **SSL-Search Engines**

To get them go here.

The user "SSL Search Bar" has provided easily installable SSL-searchbar-plugins

You get SSL-plugins for all the alternative search-engines like ixquick, duckduckgo etc. there. Install those you happen to use.

Privatelee also looks promising. But I haven't tried it out extensively.

The next thing to do is to change macromedias flash-settings:

### **Flash-Settings**

Go here.

And fight yourself through their nasty settings-manager. Set everything to "0" or "never allow"/"never ask again" and delete all stored website-content. Give special attention to the "webcam and mic"-options... wink

You might as well set the permissions of your .macromedia folder to read only - but that's kind of unnecessary because you want to make sure to edit the options mentioned above - to make sure that you don't allow websites to use your mic or webcam... [I actually take this one step further by disabling them in BIOS and sticking some neatly cut little piece of black cardboard on my webcam. Just because you're paranoid doesn't mean they aren't after you... big\_smile ] And if you set the parameters in the settings-manager accordingly nothing will be written to that folder anyway.

Now we come to the fun part. Finetuning Firefox using about:config. If you've never done this before: No reason to freak out. It's really easy.

### **about:config**

[You can simply copy/paste these variables into the search-bar at the top: e.g. "browser.cache.disk.enable" and then double-click on the entry that shows up to modify the settings.]

---disable browser cache:

```
browser.cache.disk.enable:false
browser.cache.disk_cache_ssl:false
browser.cache.offline.enable:false
browser.cache.memory.enable:false
browser.cache.disk.capacity:0
browser.cache.disk.smart_size.enabled:false
browser.cache.disk.smart_size.first_run:false
browser.cache.offline.capacity:0
dom.storage.default_quota:0
dom.storage.enabled:false
dom.indexedDB.enabled:false
dom.battery.enabled:false
```

---disable history & localization

```
browser.search.suggest.enabled:false
browser.sessionstore.resume_from_crash:false
geo.enabled:false
```

---misc other tweaks:

```
keyword.enabled:false
network.dns.disablePrefetch:true -> very important when using TOR
network.dns.disablePrefetchFromHTTPS -> very important when using TOR
dom.disable_window_open_feature.menubar:true
dom.disable_window_open_feature.personalbar:true
dom.disable_window_open_feature.scrollbars:true
dom.disable_window_open_feature.toolbar:true
browser.identity.ssl_domain_display:1
browser.urlbar.autocomplete.enabled:false
browser.urlbar.trimURL:false
privacy.sanitize.sanitizeOnShutdown:true
network.http.sendSecureXSiteReferrer:false
network.http.spdy.enabled:false ---> use http instead of google's spdy
plugins.click_to_play:true ---> also check each drop-down-menu under "preferences"->"content"
security.enable_tls_session_tickets:false ---> disable https-tracking
security.ssl.enable_false_start:true ---> disable https-tracking
extensions.blocklist.enabled:false ---> disble Mozilla's option to block/disable your addons
remotely
```

webgl.disabled:true ---> disable WebGL (<http://security.stackexchange.com/questions/13799/is-webgl-a-security-concern>)  
network.websocket.enabled:false ---> \*\*\*Tor Users: This is extremely important as it could blow your cover! See: <http://pastebin.com/xajsbiyh>\*\*\*  
---make your browsing faster:  
network.http.pipelining:true  
network.http.pipelining.ssl:true  
network.http.proxy.pipelining:true  
network.http.max-persistent-connections-per-proxy:10  
network.http.max-persistent-connections-per-server:10  
network.http.max-connections-per-server:15  
network.http.pipelining.maxrequests:15  
network.http.redirection-limit:5  
network.dns.disableIPv6:true  
network.http.fast-fallback-to-IPv4:false  
dom.popup\_maximum Mine:10  
network.prefetch-next:false  
browser.backspace\_action:0  
browser.sessionstore.max\_tabs\_undo:5  
browser.sessionhistory.max\_entries:5  
browser.sessionstore.max\_windows\_undo:1  
browser.sessionstore.max\_resumed\_crashes:0  
browser.sessionhistory.max\_total\_viewers:0  
browser.tabs.animate:0

[thanks to machinebacon for these last entries.

### **Prevent Browser Fingerprinting [still in about:config]**

For all Firefox Versions after 17.0 [you should be using current versions and update them regularly anyway - to do this go to "preferences"->"advanced"->"update" select: "automatically install updates" & "warn me if this will disable any of my addons"] [not required for iceweasel]

For the following changes right-click in about:config and select "new"->"string" and enter in this order:

Variable: Value:

general.useragent.override Mozilla/5.0 (Windows NT 6.1; rv:10.0) Gecko/20100101 Firefox/10.0  
general.appname.override Netscape  
general.appversion.override 5.0 (Windows)  
general.oscpu.override Windows NT 6.1  
general.platform.override Win32  
general.productSub.override 20100101  
general.buildID.override 0  
general.useragent.vendor [enter variable - but leave value blank]  
general.useragent.vendorSub [enter variable - but leave value blank]  
intl.accept\_languages en-us,en;q=0.5  
network.http.accept.default text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8  
network.http.accept-encoding gzip, deflate

This creates a fake-profile of your browser via the readable HTTP-headers it sends.

Check out if your browser is profilable.

With all the above settings I get 8.1 bits of identifying information at Panopticlick for my browser - which is really good.

Considering:

"In particular, a fingerprint that carries no more than 15-20 bits of identifying information will in almost all cases be sufficient to uniquely identify a particular browser, given its IP address, its subnet, or even just its Autonomous System Number."

Source: EFF's "Browser Uniqueness" [page 3]

Also check your settings on ip-check.info - but don't rely on it. Apparently they are quite busy promoting their JonDonym-Browser and services - which quite frankly I don't think anyone needs. I would rather warn you to use it since according to this defcon-talk JAP/JonDonym has implemented tracking-features which are disabled by default but can be activated anytime. So don't use it.

Now, after having configured your host-based security and your web-browser we can start connecting to the web. But there are different options:

## **TOR [The Onion Router]**

TOR is probably the most famous anonymizing-tool available. You could consider it a safe-web proxy. [Update: I wouldn't say that any longer. See the TOR-Warning below for more info.] Actually, simply put, it functions as a SOCKS-proxy which tunnels your traffic through an encrypted network of relays in which your ip-address can not be traced. When your traffic exits the network through so-called exit-nodes the server you are contacting will only be able to retrieve the ip-address of the exit-node. It's pretty useful - but also has a few drawbacks:

First of all it is slow as f\*\*k. Secondly exit-nodes are often times honey-pots set up by cyber-criminals and intelligence agencies. Why? The traffic inside the TOR-network is encrypted - but in order to communicate with services on the "real" internet this traffic needs to be decrypted. And this happens at the exit-nodes - which are thus able to inspect your packets and read your traffic. Pretty uncool. But: you can somewhat protect yourself against this kind of stuff by only using SSL/https for confidential communications such as webmail, forums etc. Also, make sure that the SSL-certificates you use can be trusted, aren't broken and use secure algorithms. The above mentioned Calomel SSL Validation addon does a good job at this. Even better is the Qualys SSL Server Test.

The third bummer with TOR is that once you start using TOR in an area where it is not used that frequently which will be almost everywhere - your ISP will directly be able to identify you as a TOR user if he happens to use DPI (Deep Packet Inspection) or flags known TOR-relays. This of course isn't what we want. So we have to use a workaround. (For more info on this topic watch this vid: How the Internet sees you [27C3])

This workaround isn't very nice, I admit, but basically the only way possible to use TOR securely.

So, the sucker way to use TOR securely is to use obfuscated bridges. If you don't know what this is please consider reading the TOR project's info on bridges

Basically we are using TOR-relays which are not publicly known and on top of that we use a tool to hide our TOR-traffic and change the packets to look like XMPP-protocol.

Why does this suck? It sucks because this service is actually meant for people in real disaster-zones, like China, Iran and other messed up places. This means, that everytime we connect to TOR using this technique we steal bandwidth from those who really need it. Of course this only applies if you live somewhere in the Western world. But we don't really know what information various agencies and who-knows-who collect and how this info will be used if, say, our democratic foundations crumble. You could view this approach as being proactive in the West whereas it is necessary and reactive in the more unfortunate places around the world.

But, there is of course something we can do about this: first of all only use TOR when you have to. You don't need TOR for funny cat videos on youtube. Also it is good to have some regular traffic coming from your network and not only XMPP - for obvious reasons. So limit your TOR-use for when it is necessary.

The other thing you/we can do is set up our own bridges/relays and contribute to the network. Then we can stream the DuckTales the whole darn day using obfuscated bridges without bad feelings... wink

How to set up a TOR-connection over obfuscated bridges?

Simple: Go to -> The Tor project's special obfsproxy page and download the appropriate pre-configured Tor-Browser-Bundle. wink

Extract and run. (Though never as root!)

If you want to use the uber-secure webbrowser we configured above simply go to the TOR-Browsers settings and check the port it uses for proxying. (This will be a different port every time you start the TOR-Bundle.)

Then go into your browser and set up your proxy accordingly. Close the TOR-Browser and have fun! - But don't forget to: check if you're really connected to the network.

To make this process of switching proxies even more easy you can use the FireFox-addon: FoxyProxy. This will come in handy if you use a regular connection, TOR and I2P all through the same browser.

Tipp: While online with TOR using google can be quite impossible due to google blocking TOR-exit-nodes - but with a little help from HideMyAss! we can fix this problem. Simply use the HideMyAss! web interface to browse to google and do your searchin'. You could also use search engines like ixquick, duckduckgo etc. - but if you are up for some serious google hacking - only google will do... wink [Apparently there exists an alternative to the previously shut-down scroogle: privatelee which seems to support more sophisticated google search queries. I just tested it briefly after digging it up here. So you need to experiment with it.]

But remember that in case you do something that attracts the attention of some three-letter-organization HideMyAss! will give away the details of your connection. So, only use it in combination with TOR - and: don't do anything that attracts that kind of attention to begin with.

Warning: Using Flash whilst using TOR can reveal your real IP-Address. Bear this in mind! Also, double-check to have network.websocket.enabled set to false in your about:config! -> more info on

that one here.

Another general thing about TOR: If you are really concerned about your anonymity you should never use anonymized services along non-anonymized services. (Example: Don't post on "frickkkkin'-anon-ops-forum.anon" while browsing to your webmail "JonDoe@everybodyknowsmyname.com")

And BTW: For those who didn't know it - there are also the TOR hidden services...

One note of caution: When dealing with darknets such as TOR's hidden services, I2P and Freenet please be aware that there is some really nasty stuff going on there. In fact in some obscure place on these nets everything you can and can't imagine is taking place. This is basically a side-effect of these infrastructure's intended function: to facilitate an uncensored access to various online-services from consuming to presenting content. The projects maintaining these nets try their best to keep that kind of stuff off of the "official" search engines and indexes - but that basically is all that can be done. When everyone is anonymous - even criminals and you-name-it are.

What has been seen...

To avoid that kind of exposure and thus keep your consciousness from being polluted with other people's sickness please be careful when navigating through these nets. Only use search-engines, indexes and trackers maintained by trusted individuals. Also, if you download anything from there make sure to triple check it with ClamAV. Don't open even one PDF-file from there without checking.

To check pdf-files for malicious code you can use wepawet. Or if you are interested in vivisecting the thing have a look at Didier Steven's PDFTools or PeePDF.

Change the file-ownership to a user with restricted access (i.e. not root) and set all the permissions to read only. Even better: only use such files in a virtual machine. The weirdest code thrives on the darknets... wink I don't want to scare you away: These nets generally are a really cool place to hang out and when you exercise some common sense you shouldn't get into trouble.

[Another short notice to the Germans: Don't try to hand over stuff you may find there to the authorities, download or even make screenshots of it. This could get you into serious trouble. Sad but true. For more info watch this short vid.]

## **TOR-Warning**

The above mentioned issues unfortunately aren't the only ones. I have come across more and more reasons not to use TOR:

- When using TOR you use about five times your normal bandwidth - which makes you stick out for your ISP - even with obfuscate bridges in use.
- TOR-nodes (!) and TOR-exit-nodes can be and are being used to deploy malicious code and to track and spy on users.
- There are various methods of de-anonymizing TOR-users: from DNS-leaks over browser-info-analysis to traffic-fingerprinting.

I won't explain all these issues in detail but if you are interested in finding out why TOR isn't safe to

use (and you should if you actually think that TOR is making you anonymous) I recommend you watch these talks:

Attacking TOR at the Application-Layer

De-TOR-iorate Anonymity

Taking Control over the Tor Network

Dynamic Cryptographic Backdoors to take over the TOR Network

Security and Anonymity vulnerabilities in Tor

Anonymous Internet Communication done Right (I disagree with the speaker on Proxies, though. See info on proxies below.)

Owning Bad Guys and Mafia with Java-Script Botnets

And if you want to see how TOR-Exit-Node sniffing is done live you can have a look at this:

Tor: Exploiting the Weakest Link

To make something clear: I have nothing against the TOR-project. In fact I like it really much. But TOR is simply not yet able to cash in the promises it makes. Maybe in a few years time it will be able to defend against a lot of the issues that have been raised and illustrated. But until then I can't safely recommend using it to anybody. Sorry to disappoint you.

## **I2P**

I2P is a so-called darknet. It functions differently from TOR and is considered to be way more secure. It uses a much better encryption and is generally faster. You can theoretically use it to browse the web - but it is generally not advised and even slower as TOR using it for this purpose. I2P has some cool sites to visit, an anonymous email-service and a built-in anonymous torrent-client. wink

For I2P to run on your system you need Open-JDK/JRE since I2P is a java-application. To install:

Go to-> The I2P's website download, verify the SHA256 and install:

```
$ cd /directory/you/downloaded/the/file/to && java -jar i2pinstall_0.9.4.jar
```

Don't install as root - and even more important: Never run as root!

To start: `$ cd /yourI2P/folder ./i2prouter start`

To stop: `$ cd /yourI2P/folder ./i2prouter stop`

Once running you will be directed to your Router-Console in FireFox. From there you have various options. You should consider to give I2P more bandwidth than default for a faster and more anonymous browsing experience.

The necessary browser configuration can be found here.

For further info go to the project's website.

## **Freenet**

A darknet I have not yet tested myself, since I only use TOR and I2P is Freenet. I heard that it is not that populated and that it is mainly used for filesharing. A lot of nasty stuff also seems to be going on on Freenet - but this is only what I heard and read about it. The nasty stuff issue of course is also



true for TOR's hidden services and I2P. But since I haven't been on it yet I can't say anything about that. Maybe another user who knows Freenet better can add her/his review.

Anyhow...:

You get the required software here.

If you want to find out how to use it - consult their helpsite.

### **Secure Peer-to-Peer-Networks**

GNUnet

RetroShare

### **Mesh-Networks**

If you're asking yourself what mesh-networks are take a look at this short video.

guifi.net

Netsukuku Community

OpenWireless

Commotion

FabFi

Mesh Networks Research Group

Byzantium live Linux distro for mesh networking

(Thanks to cyberhood!)

### **Proxies**

I have not yet written anything about proxy-servers. In short: Don't ever use them.

There is a long and a short explanation. The short one can be summarized as follows:

- Proxy-servers often sent xheaders containing your actual IP-address. The service you are then communication to will receive a header looking like this:

X-Forwarded-For: client, proxy1, proxy2

This will tell the server you are connecting to that you are connecting to him via a proxy which is fetching data on behalf of... you!

- Proxy servers are infested with malware - which will turn your machine into a zombie within a botnet - snooping out all your critical login data for email, banks and you name it.

- Proxy servers can read - and modify - all your traffic. When skilled enough sometimes even circumventing SSL.

- Proxy servers can track you.

- Most proxy servers are run by either criminals or intelligence agencies.

Seriously. I really recommend watching this (very entertaining) Defcon-talk dealing with this topic. To see how easy e.g. java-script-injections can be done have a look at beef.

## **VPN (Virtual Private Network)**

You probably have read the sections on TOR and proxy-servers (do it now - if you haven't) and now you are asking yourself: "&\*\$%\$!, what can I use to browse the web safely and anonymously????"

Well, there is a pretty simple solution. But it will cost you a few nickels. You have to buy a premium-VPN-service with a trustworthy VPN-provider.

If you don't know what a VPN is or how it works - check out this video.

Still not convinced? Then read what lifehacker has to say about it.

Once you've decided that you actually want to use a VPN you need to find a trustworthy provider. Go here to get started with that.

Only use services that offer OpenVPN. Basically all the other protocols aren't that secure. Or at least they can't compare to OpenVPN.

Choose the most trustworthy service you find out there and be paranoid about it.

A trustworthy service doesn't keep logs. If you choose a VPN, read the complete FAQ, their Privacy Policy and the Terms of Service. Check where they're located and check local privacy laws. And: Don't tell people on the internet which service you are using.

You can get yourself a second VPN account with a different provider you access through a VM. That way VPN#1 only knows your IP-address but not the content of your communication and VPN#2 knows the content but not your IP-address.

Don't try to use a free VPN. Remember: If you're not paing for it - you are the product.

## **The Web**

If for some unimaginable reason you want to use the "real" internet wink - you now are equipped with a configuration which will hopefully make this a much more secure endeavour. But still: Browsing the internet and downloading stuff is the greatest vulnerability to a linux-machine. So use some common sense. Wink

## **RSS-Feeds**

Please be aware that using RSS-feeds can be used to track you and the information-sources you are using. Often RSS-feeds are managed through 3rd-party providers and not the by the original service

you are using.

Web-bugs are commonly used in RSS-tracking. Also your IP-address and other available browser-info will be recorded.

Even when you use a text-based desktop-feedreader such as newsbeuter - which mitigates tracking though web-bugs and redirects - you still leave your IP-address.

To circumvent that you would want to use a VPN or TOR when fetching your RSS-updates.

If you want to learn more about RSS-tracking read this article.

### **Secure Mail-Providers:**

Please consider using a secure email-provider and encourage your friends and contacts to do the same. All your anonymization is worthless when you communicate confidential information in an unencrypted way with someone who is using gmx, gmail or any other crappy provider. (This also applies if you're contemplating setting up your own mail-server.)

If possible, encrypt everything, but especially confidential stuff, using gpg/enigmail.

lavabit.com [SSL, SMTP, POP]

hushmail.com [SSL, SMTP, no POP/IMAP - only in commercial upgrade]

vfemail.net [SSL, SMTP, POP]

I found these to be the best. But I may have missed others in the process.

Hushmail also has the nice feature to encrypt "inhouse"-mails, i.e. mail sent from one hushmail-account to another. So, no need for gpg or other fancy stuff. wink

The user cyberhood mentioned these mail-providers in the other #! thread on security.

autistici.org [SSL, SMTP, IMAP, POP]

Looks alright. Maybe someone has tested it already?

mailoo.org [SSL, SMTP, IMAP, POP]

Although I generally don't trust services that can not present themselves without typos and grammatical errors - I give them the benefit of the doubt for they obviously are French. roll Well, you know how the French deal with foreign languages... tongue

countermail.com [SSL, SMTP, IMAP, POP]

See this Review

riseup.org

You need to prove that you are some kind of activist-type to get an account with them. So I didn't bother to check out their security. This is how they present themselves:

Riseup wrote:

The Riseup Collective is an autonomous body based in Seattle with collective members world wide. Our purpose is to aid in the creation of a free society, a world with freedom from want and freedom of expression, a world without oppression or hierarchy, where power is shared equally. We do this by providing communication and computer resources to allies engaged in struggles against capitalism and other forms of oppression.

Edit: I changed my mind and will not comment on Riseup. It will have its use for some people and as this is a technical manual I edited out my political criticism to keep it that way.

## **Disposable Mail-Addresses**

Sometimes you need to register for a service and don't want to hand out your real mail-address. Setting up a new one also is a nuisance. That's where disposable mail-addresses come in. There is a firefox-addon named Bloody Vikings that automatically generates them for you. If you rather want to do that manually you can use some of these providers:

anonbox  
anonymouse/anonemail  
trash-mail  
10 Minute Mail  
dispostable  
SilentSender  
Mailinator

It happens that websites don't allow you to register with certain disposable mail-addresses. In that case you need to test out different ones. I have not yet encountered a site where I could not use one of the many one-time-address out there...

## **Secure Instant-Messaging/VoIP**

Using Skype is not advised from a security standpoint. Although Skype communication is encrypted there are a few ways to attack it. Also, you probably don't want to trust Skype to keep all your data safe, do you?

Instead you can use:

### **TorChat**

To install:

```
$ sudo apt-get install torchat
```

TorChat is generally considered to be really safe - employing end-to-end encryption via the TOR network. It is both anonymous and encrypted.

Obviously you need TOR for it to function properly.

Here you find instructions on how to use it.

### **OTR [Off-the-Record Messaging]**

OTR is also very secure. Afaik it is encrypted though not anonymous.

Clients with native OTR support:

Jitsi  
Climm

Clients with OTR support through Plugins:

Pidgin  
Kopete

XMPP generally supports OTR.

Here you find a tutorial on how to use OTR with Pidgin.

## **Secure and Encrypted VoIP**

As mentioned before - using Skype is not advised. There is a much better solution:

Jitsi

Jitsi is a chat/VoIP-client that can be used with different services, most importantly with XMPP. Jitsi doesn't just offer chat, chat with OTR, VoIP-calls over XMPP, VoIP-video-calls via XMPP - but also the ZRTP-protocol, which was developed by the developer of PGP, Phil Zimmerman.

ZRTP allows you to make fully end-to-end encrypted video-calls. Ain't that sweet? wink

If you want to know how that technology works, check out these talks by Phil Zimmerman at Defcon. [Defcon 15 | Defcon 16]

Setting up Jitsi is pretty straightforward.

Here is a very nice video-tutorial on how get started with Jitsi.

## **Social Networking Facebook**

Although I actually don't think I need to add this here - I suspect other people coming to this forum from google might need to consider this: Don't use Facebook!

Apart from security issues, malware and viruses Facebook itself collects every bit of data you hand out: to store it, to sell it, to give it to the authorities. And if that's still not enough for you to cut that crap you might want to watch this video.

And no: Not using your real name on Facebook isn't helping you anything. Who are your friends on Facebook? Do you always use an IP-anonymization-service to login to Facebook? From where do you login to Facebook? Do you accept cookies? LSO-cookies? Do you use SSL to connect to Facebook? To whom are you writing messages on Facebook? What do you write there? Which favorite [movies | books | bands | places | brands]-lists did you provide to Facebook which only need to be synced with google-, youtube-, and amazon-searches to match your profile? Don't you think such a massive entity as Facebook is able to connect the dots? You might want to check out this vid to find out how much Facebook actually does know about you. Still not convinced? [Those who

understand German might want to hear what the head of the German Police Union (GDP), Bernhard Witthaut, says about Facebook on National TV...]

For all of you who still need more proof regarding the dangers of Facebook and mainstream social media in general - there is a defcon-presentation which I urge you to watch. Seriously. Watch it.

Well, and then there's of course Wikipedia's collection of criticism of Facebook. I mean, come on.

## **Alternatives to Facebook**

Friendica is an alternative to Facebook recommended by the Free Software Foundation

Lorea seems a bit esoteric to me. Honestly, I haven't wrapped my head around it yet. Check out their description:

Lorea wrote:

Lorea is a project to create secure social cybernetic systems, in which a network of humans will become simultaneously represented on a virtual shared world.

Its aim is to create a distributed and federated nodal organization of entities with no geophysical territory, interlacing their multiple relationships through binary codes and languages.

Diaspora - but there are some doubts - or I'd better say: questions regarding diasporas security.

But it is certainly a better choice than Facebook.

One last thing:

## **Passwords**

Always make sure to use good passwords.

To generate secure passwords you can use:

### **pwgen**

Installation:

```
$ sudo apt-get install pwgen
```

Usage:

```
pwgen [ OPTIONS ] [ pw_length ] [ num_pw ]
```

Options supported by pwgen:

-c or --capitalize

Include at least one capital letter in the password

-A or --no-capitalize

Don't include capital letters in the password

-n or --numerals

Include at least one number in the password

-0 or --no-numerals

Don't include numbers in the password  
-y or --symbols  
Include at least one special symbol in the password  
-s or --secure  
Generate completely random passwords  
-B or --ambiguous  
Don't include ambiguous characters in the password  
-h or --help  
Print a help message  
-H or --sha1=path/to/file[#seed]  
Use sha1 hash of given file as a (not so) random generator  
-C  
Print the generated passwords in columns  
-1  
Don't print the generated passwords in columns  
-v or --no-vowels  
Do not use any vowels so as to avoid accidental nasty words

Example:

```
$ pwgen 24 -y
```

Pwgen will now give you a list of password with 24 digits using at least one special character.

To test the strength of your passwords I recommend using Passfault. But: Since Passfaults' symmetric cypher is rather weak I advise not to use your real password. It is better to substitute each character by another similar one. So you can test the strength of the password without transmitting it in an insecure way over the internet.

If you have reason to assume that the machine you are using is compromised and has a keylogger installed you should generally only use virtual keyboards to submit critical data. They are built in to every OS afaik.

Another thing you can do is use:

### **KeePass**

KeePass stores all kinds of password in an AES/Twofish encrypted database and is thus highly secure and a convenient way to manage your passwords.

To install:

```
$ sudo apt-get install keepass2
```

A guide on how to use it can be found [here](#).

### **Live-CDs and VM-Images that focus on security and anonymity**

Tails Linux The classic. Debian-based.

Liberté Linux Similar to Tails. Gentoo-based.

Privatix Live-System Debian-based.

Tinhat Gentoo-based.

Pentoo Gentoo-based. Hardened kernel.

Janus VM - forces all network traffic through TOR

### **Further Info/Tools:**

TOR

I2P

Securing Debian Manual

Electronic Frontier Foundation

EFF's Surveillance Self-Defense Guide

Schneier on Security

Irongeek

SpywareWarrior

SecurityFocus

Wilders Security Forums

Insecure.org

CCC [en]

Eli the Computer Guy on Security

Digital Anti-Repression Workshop

The Hacker News

Anonymous on the Internets!

#! Privacy and Security Thread [Attention: There are some dubious addons listed! See my post there for further info.]

EFF's Panopticklick

GRC

Rapid7 UPnP Vulnerability Scan

HideMyAss! Web interface

Browserspy

ip-check.info

IP Lookup

BrowserLeaks

Whoer

evercookie

Sophos Virus DB

f-secure Virus DB

Offensive Security Exploit DB

Passfault

PwdHash

Qualys SSL Server Test

MyShadow

Security-in-a-Box

Calyx Institute

CryptoParty

Self-D0xing

Wepawet



## **German only:**

awxcnx  
anondat  
SemperVideo  
SemperVideo [youtube]  
Fefes Blog  
heise  
golem  
CCC [de]  
FoeBud  
German Privacy Foundation  
Postscript:

If you find any error in this guide please don't hesitate to reply with an explanation. Also, if you have anything to add please also use the reply function. Since this is my first "real" post on the #! forums I don't know how long the edit-function is available for regular posts. Should it be usable indefinitely I will edit this original post to include all the additional information you will provide. This way we keep all the required info in one place. Thanks!

...and keep sorcerering!

## **BROWSER FINGERPRINTS**

### **Webrtc**

About webRTC: ( Web Real-Time Communication) is an API definition drafted by the World Wide Web Consortium (W3C) that supports browser-to-browser applications for voice calling, video calling and P2P file sharing without the need of either internal or external plugins.

We might be vulnerable to Webrtc IP leaks, WebRTC leaks your actual IP address from behind your VPN, by default. Luckily Fraudfox can spoof Webrtc, the latest Antidetect has a Webrtc changer too.

You can do a WebRTC leak test here: <https://browserleaks.com/webrtc>

Please don't disable Webrtc from about:config, it really doesn't look legit.

### **Plugins**

Plugin Detection: all the plugins that you have installed can leave a footprint, both AD and Fraudfox can help to avoid this.

### **Time zone and Clock**

When you perform operations of carding or impersonating identities of people residing in different places with different time zone you are in the position of having to change your time zone to have to align with the one of the victim.

You should match the time zone of the socks you are currently using, fortunately, with Windows this operation is very simple, just go to the clock in the bottom right of windows and click: 'Edit Time and Date Settings'.

## Font Detection

Font fingerprinting – is what fonts you have, and how they are drawn. Based on measuring dimensions of the filled with the text HTML elements, it is possible to build an identifier that can be used to track the same browser over time. Long story short, if we install new fonts, that would leave a fingerprint. This is really a minor fact from my experience but we can still randomize and spoof that, so, no problem.

## IP Spoofing

We will need to spoof the Cardholder location, we do that via SSH, RDP, Socks5, etc.

- 1) The IP should Country/State/City match the cardholder. The closer the better.
- 2) The chosen IP should have immaculate blacklisting (you can check blacklists on: <http://www.ip-score.com> and click MORE BLS) but truth be told, sometimes it's hard to tell whether a site has really blacklisted a given IP or not, as most have an internal blacklisting, for instance, Paypal might have its own internal blacklisting. Checking blacklists is still a good indicator though. Also you might notice that your personal IP might be blacklisted, even if you never did spam/fraud with it, so take that in consideration, even my real IP is blacklisted for I don't know what reason.
- 3) The chosen IP should have a low RiskScore, try to keep this riskscore at less than 5 it's a metric from Minfraud, you can read more here: <https://www.maxmind.com/en/explanation-of-minfraud-riskscore>. I use: <http://mcs.sx> for checking RiskScore. You can also check it on [xdedic.biz](http://xdedic.biz)
- 4) Low Proxyscore: Go at [getipintel.net](http://getipintel.net) and test the IP, the proxy score should be 0.
- 5) The IP has to be residential: you want to avoid datacenter IPs as they don't really look legitimate in the eyes of anti-fraud systems, also business IPs look good. If you are wondering whether the IP is residential or not, simply go to [whoer.net](http://whoer.net), and on the top you will read ISP. Generally if the IP has an American ISP, then you are on a good track, simple google: 'list of American Internet service Provider' to get a good list of American ISP. Datacenter IPs have "data", "hosting", "Cloud and related words as ISP.
- 6) The IP should be as close as possible to FULLZ location, at least within 80 miles, I use [distancebetweencities.com](http://distancebetweencities.com).

## SOCK5, RDP and SSH

Socks5 is a protocol that works with the proxy server, a popular choice amongst carders, I believe it's the most effective way of spoofing your IP. However, most of fraudsters are carding through SSH nowadays, so I suggest SSH as your main way of IP Spoofing. I use like to use; proxifier or Foxyproxy to link socks to my machine.

Some proxy providers: <http://www.seproxysoft.com/en>  
[luxsocks.ru](http://luxsocks.ru) (provider has closed registration but still worth mentioning )  
[Premsocks.com](http://Premsocks.com), [truesocks.net](http://truesocks.net), [ironsocket.com](http://ironsocket.com), [sockslist.net](http://sockslist.net), [isocks.biz](http://isocks.biz)  
[Vip72.com](http://Vip72.com) (overly blacklisted but they have plenty of locations worth mentioning)

For linking socks to machine I recommend you proxifier and Foxyproxy. RDPs stands for Remote Desktop Protocol, you are basically connecting to a remote computer. In fraud they are generally used to maintain Bank Drops and PayPal Middleman Accounts. But they are also used for carding. You can get RDPs from the clearnet, just googling rdp will do. The problem with non-hacked RDPs is that their IPs come from a range of database IPs that have some history with fraud. That's where HACKED RDP comes in handy, hacked RDP generally have a clean residential IP, there are plenty of illegal autoshops selling them: You can buy them from: [xdedic.biz](http://xdedic.biz),

store.ru, pp24.ws, tunastock.ru, rdpterminals.tw.

Once you login to the RDP, remember to change the password and create an hidden username aka ghost user, so that the real owner will not notice, there is a tutorial on both xdedic and uas-store.ru for it. Also, you can card from there, you don't have to think much about spoofing as they are an identity themselves and a real device.

## **Socks5 vs RDP vs SSH**

RDPs are more expensive but they identify themselves, you can card from there, absolutely no spoofing needed whereas socks are more cost effective but they require a spoof setup. There's a rumor that in 2019 carding with socks is dead, I say its bullshit its probably because these people have bad socks and/or crappy spoof setup. I suggest to start from RDP carding then move onto Socks one you are more confident. SSH is a middle way and should be the most used way of spoofing IP for intermediate carders, they cost slightly more than socks.

## **SSH Tunnel**

Port forward via SSH (SSH Tunneling) creates a secure connection between a local computer and a remote machine through which services can be relayed. Because the connection is encrypted, SSH tunneling is useful for transmitting information that uses an encrypted protocol, such as IMAP, VNC or IRC.

Now the thing about SSH Tunnels, is that we get the IP of another machine and we can use it in our machine, I generally make a new virtual machine, use SSH Tunnel, and there we go. I buy SSH from: pp24.ws and tunastock.ru. in order to use SSH you need to:

- 1) Download and install bitvise client from bitvise.com
- 2) Launch the software and go to SSH tab, click on all the blue links such as Key Exchange Algorithms and tick all the Checkboxes for all links.
- 3) Go to services tab and tick the "enabled" box in the SOCKS/HTTP proxy forward part
- 4) Now, on that part, the listen interface should be 127.0.0.1, Listen Port on 5555
- 5) You are done with bitvise, you will need to click on "login" tab and put the login data for SSH.

Another step is to install proxifier if you have not done it already, proxifier allows to tunnel SSH IP to ALL your VM softwares.

- 1) Open Proxifier and go to profile -> Proxy Servers -> Add
- 2) On "Server" put 127.0.0.1 and on Port put 5555
- 3) On Protocol check SocksV5 Server
- 3) Go to Profile -> Name Resolution -> Uncheck "Detect DNS automatically" -> Check "Resolves Hostnames Through Proxy"
- 4) We are done with Proxifier, now all we have to do is to go on tunastocks.ru or pp24.ws and get an SSH.

## **Accept Language**

Is together with the User-Agent HTTP header another HTTP header, which identifies the network, the language used by the system that is making the navigation.

Use an Accept Language header that matches language of the victim.

Flash version spoofing: Always spoof the latest flash version.

## **Email Spoofing**

We will need to use an e-mail that looks legit. This is not really that discussed on forums, according to emailage, Square and Western Union are their clients  
So emailage checks on plenty of things:

- 1) It checks if the email has the name and surname of the customer.
- 2) It calculates the score of the email domain.
- 3) It calculates the age of a specific email, fraudster are well known for creating quickly e-mails, and that how they can spot us.

So depending on the score you get from them, they will either approve you attempt, put your order on review or simply decline it. To make things worse, they have an internal blacklist of e-mails, so reusing emails with them isn't wise. They also have all the other IP validation stuff that any other anti-fraud protection provider has.

For private emails, I suggest to get an anonymous email provider, one like domain cheap (They accept BTC) and get who is protection. Also, will you attach the domain to an anonymous hosting provider. You can make as many emails as you wish with same domain from cpanel. Emailage doesn't reveal all the info about their measures, but I think somehow they can also check the age of free emails, private emails are very easy as you can check the domain age of a website. Now let's go to the actual spoofing softwares, I believe there are 3 mainly choices here: A Configured Portable Browser, Antidetect and Firefox

## **HOW TO MAKE FAKE ID CARD**

I am sorry, i will share only the link from ViperZCrew because the Guide is too big.

<https://t.me/ViperZCrew/10335>

PVC ID Card Printing (Short & Complete Guide)

<https://www.youtube.com/watch?v=jcY-MveHh48>

ID Card Making with Fusing Maschine (Complete Tutorial)

[https://www.youtube.com/watch?v=T6\\_t-dU-RE](https://www.youtube.com/watch?v=T6_t-dU-RE)

Pasting ID Card Tutorial

[https://www.youtube.com/watch?v=6wB-L9QVi\\_Y](https://www.youtube.com/watch?v=6wB-L9QVi_Y)

Best ID Photo Software (ID Photo Pro 8)

<https://www.youtube.com/watch?v=BFtEEcI1lYM>

Screen Printing Tutorial

[https://www.youtube.com/watch?v=dU5Tj\\_EH7GY](https://www.youtube.com/watch?v=dU5Tj_EH7GY)

If they are all not available download this file i downloaded all:

[https://anonfiles.com/N8Y6xauf02/Downloads\\_zip](https://anonfiles.com/N8Y6xauf02/Downloads_zip)

## **CHANGE YOUR IP TO ANY COUNTRY**

So First What We Have To Do Is To Download Mozilla Firefox!

You Can Download By Yourself Or Search On This Site: [filehippo.com](http://filehippo.com)

Now When You Have installed Mozilla Firefox

Go To Add-ons for Firefox (en-US)

And Search For AnonymoX Add Ons

Now Download This Add-ons

And You Will Found various option Of configuring To Various Country Ip In Just A Second!!

I am Using This from 1 Months And I am Enjoying This Great!!

Forgot The Express VPN , Socks ,And Proxy !!

Use The Better And Advance!

### **WHAT DO YOU NEED TO CARD TO GET NOT CAUGHT(CHEAP) 3.0**

I know the setup is the same, but if you are asking then here:

- Good VPN (Perfect Privacy or Mullvad)(VPN must have good record, no logs, strong encryption and killswitch.)
- MAC changer (TMAC gets the job done)
- Extra DNS leak protection (DNSCrypt)
- SOCKS5/RDP (911.gg or UAS RDP)
- Virtual Box (If not using RDP) (It is extremely important you do this off of a clean virtual computer!!)
- Browser with WEBrtrc protection, fingerprinting and trackers blocker. (Strict mode on Firefox) (Read post above)
- Ccleaner (Secure deletion, 35 wipes, check everything other than wipe free disk space.)
- Bleachbit (Check everything except wipe free disk space.)
- Run CMD and do ipconfig /flushdns after every operation.

Note: If you're doing big operations you will need to use everything here + connect to secure RDP, it's pretty much untraceable.

### **WHAT IS A DARKNET FORUM**

- A hidden Internet exists underneath the 'surface web,' hidden from the view of ordinary web users. It always aroused my curiosity, but I never really followed up to see whether I could access it.
- The dark web is intimidating. I assumed it was full of criminals and would have little to offer a law-abiding citizen such as myself. I also thought it would be difficult to access and that it would require some kind of advanced technical skill, or perhaps a special invitation from a shadowy figure on seedy bulletin boards. I decided to investigate these assumptions.
- One of the things that really struck me was how easy it is to access and start exploring the darknet—it requires no technical skills, no special invitation, and takes just a few minutes to get started.
- In this article I will share information on how to access and navigate the dark web, as well as my personal experiences and thoughts.

### **WHAT IS THE DARKNET**

- Most people are confused about what exactly the darknet is.
- Firstly, it is sometimes confused with the deep web, a term that refers to all parts of the Internet which cannot be indexed by search engines and so can't be found through Google, Bing, Yahoo, and so forth.
- Experts believe that the deep web is hundreds of times larger than the surface web (i.e., the Internet you get to via browsers and search engines).
- In fact, most of the deep web contains nothing sinister whatsoever. It includes large databases, libraries, and members-only websites that are not available to the general public. -Mostly, it is composed of academic resources maintained by universities. If you've ever used the computer

catalog at a public library, you've scratched its surface. It uses alternative search engines for access though. Being unindexed, it cannot be comprehensively searched in its entirety, and many deep web index projects fail and disappear. -Some of its search engines include Ahmia.fi, Deep Web Technologies, TorSearch, and Freenet.

-The dark web (or dark net) is a small part of the deep web. Its contents are not accessible through search engines, but it's something more: it is the anonymous Internet. Within the dark net, both web surfers and website publishers are entirely anonymous. Whilst large government agencies are theoretically able to track some people within this anonymous space, it is very difficult, requires a huge amount of resources, and isn't always successful.

## **ANONYMOUS COMMUNICATION**

Darknet anonymity is usually achieved using an onion network.

Normally, when accessing the pedestrian Internet, your computer directly accesses the server hosting the website you are visiting.

In an onion network, this direct link is broken, and the data is instead bounced around a number of intermediaries before reaching its destination.

The communication registers on the network, but the transport medium is prevented from knowing who is doing the communication.

Tor makes a popular onion router that is fairly user-friendly for anonymous communication and accessible to most operating systems.

## **WHO USES THE DARKNET**

Perhaps unsurprisingly, the onion network architecture of the darknet was originally developed by the military—the US Navy to be precise.

Military, government, and law enforcement organisations are still amongst the main users of the hidden Internet.

This is because ordinary internet browsing can reveal your location, and even if the content of your communications is well-encrypted, people can still easily see who is talking to whom and potentially where they are located.

For soldiers and agents in the field, politicians conducting secret negotiations, and in many other circumstances, this presents an unacceptable security risk.

The darknet is also popular amongst journalists and political bloggers, especially those living in countries where censorship and political imprisonment are commonplace.

Online anonymity allows these people, as well as whistleblowers and information-leakers, to communicate with sources and publish information freely without fear of retribution. The same anonymity can also be used by news readers to access information on the surface web which is normally blocked by national firewalls, such as the 'great firewall of China' which restricts which websites Chinese Internet users are able to visit.

Activists and revolutionaries also use the darknet so that they can organise themselves without fear of giving away their position to the governments they oppose.

Of course, this means that terrorists also use it for the same reasons, and so do the darknet's most publicized users—criminals.

### **What Is Tor And How Can We Use It?**

Tor(The Onion Router) is a browser which was created for the Military but misused by criminals for selling drugs, weapon and anonymous purposes. Installing and surfing with Tor is legally, if you buy anything is illegally.

Tor using plugins like HTTPS Everywhere and No Script and it's changing your IP address, i will

not talk deeper i already wrote and tutorial in ViperZCrew\*<sup>1</sup> I wrote many tutorials about Tor any you can find many post from me.

1\* = i really recommend you to read the post you can find it at "useful to read" - at the end of this post.

Download the Tor browser from here:

<https://torproject.org/>

Make sure you choose the version of your device, a quick tip: do not use windows, i prefer to use linux.

While Tor is downloading and installing, you can setup an VPN.

Why we use a VPN?

1.) Your ISP(Internet Service Provider) can see your Tor traffic, if police is on trace to your backwards, and asking for routerprotocols then police can see your traffic through the tor browser — A VPN is encrypting your VPN traffic while you are using it.

2.) Over tor there are very much scammers worldwide, they are using traps etc. to scam you. An MITM can see your real IP address, he can be a tor node and see where the request is coming from, and if he is the first node, your IP is leaked, and they can find your location, receive information over the network you are using.

Many governments are spying the so called exitnodes, they want to find vendors of illegal stuff.

Can we know if we are using a spied exit node?

1.) Yes we can, if you read the tor guide, then you maybe read about "exitnodes", exitnodes can be hosted by anyone, if you want to check if your tor is safe :

<https://torcheck.xenobite.eu/index.php>

The Tor Project has a tool to do this at:

<https://exonerator.torproject.org/>

For automated lookups, they also provide a DNSBL-based lookup information on that is available at:

<https://www.torproject.org/projects/tordnsel.html.en>

I have installed tor what now?

The shield in the right of the url box is the security level click and enable “safer” you can do strong but this is only for browsing very good.

Next click on the right item and restart with new identity.

Useful to read:

<https://t.me/ViperZCrew/6550>

<https://protonvpn.com/blog/tor-vpn/>

<https://hackertarget.com/tor-exit-node-visualization/>

<https://nakedsecurity.sophos.com/2015/06/25/can-you-trust-tors-exit-nodes/>

## HOW TO SEND UNTRACEABLE EMAIL 2020 GUIDE

There can be many reasons why anyone would want to send an anonymous mail that can't be traced back to the original sender. It could be something secret between two people or among some persons of any organization, or it could be investigative blogging and reporting. If you want to send an anonymous email, here are some good methods:

### 1] Use VPN for anonymous emails

You can use VPN (Virtual Private Network) to send material to someone in a way that can't be traced back. When you use a VPN, you are already using a different IP address. But your mail ID will identify you.

### 2] Use Burner email accounts

Burner email accounts allow you to create a random email ID so that you can enter it on websites when browsing. This way, everything on the Internet who asks for your IP address, gets a fake IP address. Using burner mails to sign up and verification can help you stay away from spam. The burner email ID can be connected to your real email account so that any mail that reaches your burner email accounts is transferred to your real mail ID.

### 3] Create a disposable email account

If you intend to use the burner email only once, it is better to create a disposable email ID as the latter can be set to self-destruct after a period of time. Please note that the burner email ID is different from disposable mail accounts. The burner mail accounts can be used for longer compared to disposable email accounts. The disposable mail accounts can be set to self-destruct as soon as any incoming mail is read. Or the person using disposable mail ID can simply set a timer so that the mail ID is disposed of after a certain time.

How to send an anonymous email to somebody

The following are some websites that allow you to send an anonymous mail to somebody free that can't be traced:

#### 1] Temp Mail – Disposable Temporary Email

You can send an mail using temp-mail.org. You may use it for things like mail-verification upon signups. You can later delete the entire email address and its content without having to receive further emails from sites where you used the temporary mail.

You do not have to create an account. You don't have to provide data about yourself. You simply type the mail content and then enter the destination email address to send mail.

#### 2] Guerrilla Mail – Disposable mail ID

GuerrillaMail.com helps in sending anonymous messages anywhere, to anyone, in this world. This is actually a disposable mail ID provider.

You can create a disposable mail ID by selecting the server using the drop-down menu. In the text box preceding the server name, you can enter an ID that is going to be cleaned every hour.

There is a Scramble Address option available so that you can convert your mail ID to random characters so that it becomes difficult for the receiver to trace you and the origination of the mail you sent.

You don't have to provide any details about yourself. All emails in Guerrilla Mail are deleted after one hour of reaching the inbox.



### 3] AnonEmail Email Account

The AnonEmail is short for Anonymouse.org. You need not provide any information to use this service. It can be used for outgoing emails only. Simply fill in the target destination mail, type a subject for the mail, type the mail, and then click on Send Anonymously button.

### 4] Send Anonymous mail

SendAnonymousEmail.net is another free service that lets you send anonymous emails. I have tested it and it works.

### 5] Anonymous mail

Anonymousemail.me is similar to the AnonEmail listed above. It's plus point is a "Reply-To" address to which you can direct any replies. A Premium plan is also available that allows sending unlimited emails along with tracking features.

The free plan allows you to access the fields "To", "Subject", and "Compose" text box as seen in the image. The free plan allows up to three attachments.

### 6] Mailnesia – For incoming mail

Mailnesia.com is also a quick set up inbox for receiving website sign up notifications. For example, you need to enter a valid email for accessing certain artefacts from the web. You can quickly create a Mailnesia inbox account and use the mail address for incoming mail. A feature of this service is that it automatically clicks verification links and opens the related target window.

## **HOW TO SEND HACKED PAYPAL BALANCE FROM ONE ACCOUNT TO ANOTHER ACCOUNT WITHOUT ANY STRESS**

Today I will show you how to send hacked PayPal balance from one account to another without any hassle in confirming credit card number, bank account number, SSN number or security answers. After buying it some people try it without socks5 comes with the PayPal and gets a security measures notification or gets it limited and can't do anything about it. It is very disappointing and a total waste of your LR Balance.

Let me tell you the instruments you must get before you move on to the next steps.

- A virtual Credit Card.
- hacked PayPal account with mail access.
- Two more PayPal accounts made by you.
- Strong and appropriate socks5 to the location of hacked PayPal account.

Let me make you clear about how will you get your instruments ready.

So, I am going to share my private technique to transfer funds from one PayPal account to another and securing Them from further charge backs or refunds.

OK, let me tell you the instruments you must get before you move on to the next steps.

First of all, purchase a Virtual credit card. Virtual credit cards are like normal credit cards without any physical existence.

Now you have to get your desired hack PayPal. You can either buy it, you don't have hacked PayPal.

You have to create two non-US PayPal accounts first. I prefer creating PayPal account from Cyprus and Singapore (I mentioned them because, if you fail to secure funds for any reason then there are possibilities to cash them out later using this service). OK fine, but be cleared that you must use different socks5 for both accounts.

It's not mandatory to use Cyprus socks or Singapore socks here. For example You can use

California socks for Cyprus

PayPal but after your sock died, you must use socks again from California to access your account everytime.

You need strong socks5 for hacked PayPal to manipulate location of hacked PayPal.

Now the main job to do. First try sending money from hacked PayPal to one of your created PayPal using socks given with PayPal. Sometimes you may get lucky and can send funds to another account successfully without any confirmation messages to verify Credit Card or Bank Account Number. But luck doesn't support one every time. So you need to buy a Virtual Credit Card and add that to hacked PayPal account and confirm that card.

So when you will try to send money and get a message to confirm Credit Card or Bank then you can input the virtual credit card Number and bypass the Credit card confirmation.

In next step type in message to seller box:

"Got the item. And it's working fine. Thanks lot."

And send the money to your secondary PayPal.

Immediately remove the notification in hacked PayPal email inbox and archive the recent transaction. It will make

The time lengthy for the hacked PayPal account holder to know that he's getting his ass fucked.

Then clear your cache and cookies and login to your secondary PayPal account with different socks5.

And send the money to your Primary PayPal account and don't forget to type something impressive in seller note message.

Now I can say, your hacked moneys are 90% secured. But don't keep them forever there.

Cash them out or spend them however you can quickly.

## **TIPS TO STAY ANONYMOUSLY**

Hey guys welcome back again, some tips about privacy and so on.

Starting talking now lol.

- Get an Anonymous OS (Qubes OS, Tails, Whonix)
- Get off from social media (if you register use any fake data : <https://www.fakenamegenerator.com/> )(get off your social media: [suicidemachine.org](https://suicidemachine.org))
- Before Posting a picture use a exif tag editor for deleting your GPS location (windows: <http://www.exifpurge.com/>)  
Linux:

```
$ exiftool image.jpg
```

Removing files though this command:

```
$ exiftool -all= image.jpeg
```

- Get VPN (protonvpn, holavpn)

Trick:

Step 1) Register on <https://protonmail.com/signup>

Step 2) After log in goto settings, and then protonvpn and you see your data for login

Step 3) Download the ProtonVPN exe or ProtonVPN App

Step 4) Enter login data and you are connect randomly

(otherwise download holavpn)

- Get Anonymous Browser (Tor: <https://www.torproject.org/download/> )
- Use Anonymous Add-Ons already written a guide ( short paste: <https://pastebin.com/85HwgSzq> )
- Don't use online any credits cards
- If you register on Paypal, use not your real PC, use a PC from internet coffee shop. (paypal for example saves your hard disk serial id => they can you)
- Never use Free Wifi Hotspots
- Don't use as an search google engine, use DuckDuckGo.
- Share files anonymously ( use <https://onionshare.org/> )
- Turn off your windows location :

Step 1) Goto settings > privacy > location

Step 2) Click change button from on to off

- Destroy Windows Spying. I already shared a post about DWS, here you can get it (Windows : <https://github.com/Nummer/Destroy-Windows-10-Spying/releases/tag/2.2.2.2> )
- Get a private encrypted E-Mail (Protonmail: [protonmail.com](https://protonmail.com))
- Delete Cookies (<https://www.ccleaner.com/de-de/ccleaner>) and Browsing History (Chrome and Firefox allows, to do never create a history)
- Use End-To-End message Software for really secret conversations (Android: WickR ( <https://play.google.com/store/apps/details?id=com.mywickr.wickr2> ) iOS: <https://wickr.com/products/all-downloads/> )  
Another apps are Signal or Wire.
- Use secure passwords ( already shared big password guide, you can generate passwords aswell here: <https://passwordsgenerator.net/> )
- Use Temp Mails for trash or something else  
( Temp mail: <https://temp-mail.org/> )
- Disbale Notification on locked screen.
- Check your app settings, a file explorer should not have a calling option.

- Attach your laptop camera too, hackers can Access to them and take pictures.
- Enable 2-Factor Authentication on every Social Media Account.
- Use https everywhere.  
(https is an encrypted connection from user to the website)
- Use Adblocker, it's good for youtube and any other website, ads will try to track your location.  
(lucky patcher will delete ads on apps)
- Wipe your mobile after 3 months if you do any illegal things. (delete every account which is connected to your phone like youtube, google, mega.nz)
- Don't do any backup of chats. I know it's usefull but for good privacy you don't need.
- Encrypt your HDD and encrypt your files.
- Root your phone and change your model number

Step 1) Root Access

Step 2) Goto /system folder and open "build.prop"

Step 3) Rename "ro.product.model=xx-xxx" to any model name. (google for random names) like Samsung Galaxy J5 model name replace it with your model name and reboot.

- Use everytime Anti Virus.
- Disable Auto-Fill options - this can be important because Auto Fill has personal infos
- Spoof GPS

Step 1) Download Fake GPS : <https://play.google.com/store/apps/details?id=com.lexa.fakegps>

Step 2) Now navigate to Settings > System > About phone > Build number

Tap 7 times on Build Number to activate Developer Mode

Step 3) Scroll down and select "Select Mock Location App" and choose Fake-GPS

Step 4) Goto Fake-GPS App and navigate to random location.

Step 5) Start VPN

Step 6) Open WhatsApp and send live location, it will be there where you choosed the fake gps

- If you don't need Location, disable it on android.

## **HOW TO STAY SAFE WHEN USING PUBLIC WIFI**

You are out of your home to another place and unfortunately you spotted a WiFi with no passkey . you know that felling, Especially when you're tired of buying Data plans, public Wi-Fi is the only way to keep up with work and friends while you out or broke.

But do you know you will never sip water from a public tap unless you are pretty sure it is safe to drink, but in terms of Public WiFi, you don't care if it is safe to use, instead you just connect to it...

It's bad dudes☹

You need to be cautious about the Public Wi-Fi networks you connect into. Most of us don't take precautions and that's one reason why cyber-crimes and hacking are still prevailing.

Hackers most used means of attack is known as MIMT (Man In The Middle Attack) they make use of the security flaw in the routers of the cafe or Public wifi and exploits it to access the data that passes between you and the wifi.

So how are we gonna save our ass from falling victim since we can't do without this public WiFi, since it's Free, so you have to start checking whether the public WiFi network you want to use is secured or unsecured before you join it.

A lot of all public Wi-Fi hotspots are entirely unencrypted. So, only use networks that require a log-in and password.

Even the most secure-looking public WiFi networks are targeted by hackers. So you can also improve security on your end, by avoiding signing in to sensitive websites (such as online banking) while you are away from home.

But if it seems that you got no choice than to use this Public Wifi, then try to maintain different passwords for each account you use, and always sign out when you've finished with whatsoever you're doing.

Public Wi-Fi is actually a good thing!, It's great to have it around. am proud of those countries that have that, cause here in my country there's nothing like free WiFi , if you see a Free WiFi networks, it's probably that someone mistaken turn on his/her hotspot .

But while none of us 'expects' to get hacked, millions get Hacked each year so why not tune up your online security with this new guide to keep staying safe on public Wi-Fi

The benefits of Wi-Fi-on-the-go only outweigh the risks until trouble strikes. With the right precautions, you can seriously reduce the chances of that happening.

## **BULLETPROOF HOST LIST 2019/20**

Check links please!

<https://www.1984hosting.com>

<https://ecodissident.net>

<http://www.ok.is>

<http://www.advania.com>

<http://www.hub.org>

<https://www.hostname.cl>

<https://www.zgh.cl>

<http://insacom.cl>

<https://servidores.gamerlive.cl>

<http://tchile.com>

<http://ironservers.cl>

<https://www.deltasystem.cl>

<http://pro-managed.com>

<http://hosting.nic.ru>

<http://cloud.volia.com>

<https://ru-tld.ru/en/>

<https://vstoi.ru>

<http://www.superhosting.net>

<http://www.2X4.ru>

<http://avk-com.ru>

<http://www.tomtel.ru>

<http://hosting.tel.ru>

<http://www.anders.ru>  
<http://www.hoster.ru>  
<http://www.datahouse.ru>  
<http://www.fastvds.ru>  
<http://planetahost.ru>  
<https://www.rusonyx.ru>  
<https://neoserver.ru>  
<http://www.hts.ru>  
<https://www.ihc.ru>  
<https://simplecloud.ru>  
<http://infiumhost.com>  
<http://timeweb.com>  
<https://www.globatel.org>  
<http://thost.ru>  
<https://bulletproof-web.ru>  
<http://agava.ru>  
<https://masterhost.ru>  
<http://www.valuehost.ru>  
<http://hc.ru>  
<https://hosting.reg.com>  
<http://www.hostalot.ru>  
<http://tehnodom.com>  
<http://renter.ru>  
<http://abusehosting.ru>  
<http://netplace.ru>  
<http://berihoster.ru>  
<https://www.ihor.ru>  
<https://geekhost.pro>  
<https://vscale.io>  
<http://www.memvds.ru>  
<https://takewyn.com>  
<https://vhoster.net>  
<https://firstbyte.ru>  
<https://firstvds.ru>  
<https://gmhost.hosting>  
<http://melbicom.net>  
<https://cloudlite.ru>  
<http://ispserver.com>  
<https://selectel.com>  
<http://pw-service.com>  
<http://www.ultratechhost.com>  
<https://www.rackend.com>  
<https://solarcom.ch>  
<https://www.artmotion.eu>  
<http://www.deltalis.com>  
<http://en.datasource.ch>  
<https://www.nine.ch>  
<https://www.infomaniak.ch>  
<https://www.hostthink.net>  
<http://ukrdc.net>  
<http://unit-is.com>  
<http://uniteddc.net.ua>

<http://uanode.net>  
<http://www.urdn.com.ua>  
<http://netassist.ua>  
<https://ohp.ua>  
<http://www.ukraine.com.ua>  
<http://rx-name.ua>  
<http://www.server.ua>  
<http://en.ukrtelecom.ua>  
<http://www.colocall.net>  
<http://www.uar.net>  
<https://ekvia.com>  
<https://vdsinside.com>  
<http://hosting.ua>  
<https://goodnet.com.ua>  
<http://www.besthosting.ua>  
<https://www.ukrnames.com>  
<https://blazingfast.io>  
<http://tucha.ua>  
<http://netengi.com>  
<http://iprosrv.com>  
<http://deltahost.com>  
<https://itldc.com>  
<http://en.hostsolutions.ro>  
<https://www.voxility.com>  
<https://www.m247.ro/en/>  
<http://www.gemenii.ro>  
<http://www.smart-hosting.ro>  
<http://www.xservers.ro>  
<https://www.elvsoft.com>  
<http://seohosting.com.tr>  
<https://vit.com.tr>  
<http://semele.com.tr>  
<http://hosting.turk.net>  
<http://www.trvps.net>  
<http://www.kriweb.com>  
<http://natro.com>  
<http://www.sadecehosting.com>  
<https://www.trabia.com>  
<http://innovahosting.net>  
<http://magicnet.md>  
<http://tophost.md/en/>  
<http://NovoGara.com>  
<http://netbrella.net>  
<http://3nt.com>  
<https://www.tilaa.com>  
<https://www.altushost.com>  
<http://www.webuzo.net>  
<http://www.portlane.com>  
<http://www.glesys.com>  
<http://asiapacifichosting.com>  
<http://www.xeonbd.com>  
<http://mycloud.by>

<https://www.bacloud.com>  
<https://balkanvps.com>  
<https://www.virtono.com>  
<https://www.vps.ag>  
<http://www.albahost.net>  
<https://offshorededi.com>  
<http://www.global.ba>  
<https://www.qsscloud.ba>  
<http://teleklik.ba>  
<http://pttrs.net>  
<http://www.serveria.com>  
<http://zomro.com>  
<http://itools.mn>  
<http://dedicado.com.uy>  
<http://hostparatuvida.com>  
<http://networksdelmanana.com>  
<http://udasha.com>  
<http://latinoserver.com>  
<http://ispcompania.com>  
<https://www.nonamehosts.com>  
<https://www.wavecom.ee>  
<https://www.host.al>  
<https://www.eserver.ru>  
<http://kras.host>  
<https://infobox.ru>  
<https://mirohost.net>  
<http://freehost.com.ua>  
<https://lunarvps.com>

## **BULLETPROOF HOSTING 100% 2020**

<https://bullhost.co>

Port scanning, managing botnets, phishing sites, mass mailing etc. allowed!

No abuses, support with installing software

Special (!) offer for people from this great forum for all VPS services:

20% discount, promo code: Q2QB0SYI5D

## **HOW TO RECOGNIZE SCAMMERS / RIPPERS**

TheMaster, [26.01.20 13:37]

Hey

TheMaster, [26.01.20 13:38]

How much cost it

Dadon Niki, [26.01.20 17:51]

It cost 500€ delivery free inclocive



TheMaster, [26.01.20 19:15]  
Technical details please

Dadon Niki, [26.01.20 20:33]  
[In reply to TheMaster]  
??

TheMaster, [26.01.20 20:46]  
Tell me details of weapon

TheMaster, [26.01.20 20:46]  
Name and so on

Dadon Niki, [26.01.20 20:57]  
[In reply to TheMaster]  
??

Dadon Niki, [26.01.20 20:58]  
Am here to sell

TheMaster, [26.01.20 20:58]  
You sell weapons

TheMaster, [26.01.20 20:59]  
but you do not know the name

TheMaster, [26.01.20 20:59]  
hahahah

TheMaster, [26.01.20 20:59]  
I want to check if you are a experienced seller, and not a scammer

Dadon Niki, [26.01.20 21:01]  
[In reply to TheMaster]  
You have to tell me you need this

TheMaster, [26.01.20 21:01]  
i do

TheMaster, [26.01.20 21:01]  
but i do not want to get ripped

Dadon Niki, [26.01.20 21:01]  
Not asking me for details

TheMaster, [26.01.20 21:01]  
Bye

**Also remember the following points:**

- Never make a purchase without Escrow
- Hasting sellers are scamer/rippers
- Once you are before the end of a live buy, ask for screens / proofs. (weird behavior -> scamer)

- Chashapp I would never take is scammer behavior
- BTC will be suggested by everyone because it's anonymous
- Too cheap prices, e.g. 1G Weed for 5\$ is scam/ probable.
- Check proofs of goods at : <https://tineye.com/> or <https://images.google.com/>
- Not all Escrow services are real, use any admin of a trusted group!

Many rippers use 3-4 Telegrams and if you got ripped by bob, bob2 install a second telegram to msg you that he will get back your money and he needs your account data or you need to pay him for service and you got ripped second time.

## **RETAINING A LAWYER, HOW TO HANDLE GETTING CAUGHT OR INTERROGATED**

Let us face it. We are all human and we make mistakes. Unfortunately, you only need to make one mistake, and the Law Enforcement, commonly referred to as LE on these forums can bust you. Maybe they will wait for you to do something more serious before they nab you, but if you slip up and they feel you are worth going after, you can expect them to get you no matter where you live, with rare exception.

The main question is, should I keep an emergency lawyer fund on hand? And how much should it be. The response I think was most appropriate for this question was the following.

Give your lawyer 50k and put him on a retainer.

Don't have a emergency fund 'stash' lying around if that is what you mean.... you should already have your lawyer paid + plus extra in case he needs to post bond for you and they seize the majority of your drug funds.

Once you get arrested by LE, they can seize your money based on the assumption that it is drug related. So you need to have a lawyer paid for ahead of time. That way, in the unfortunate case that you get a visit from the feds, you have a lawyer ready to go. The agreed upon amount was around \$50,000.

The take homes from this thread are basically. Keep your moouh shut. The feds are going to try all types of tactics on you to get you to admit to guilt of the crimes you are being accused of. They will likely use the good cop, bad cop on you. First they will tell you that they want to help you, and that they are after the big guys. They just need your help to put away the big guys. Do not listen to this, I have never cooperated with a good cop LE and have it end up working in my favor. Once you admit to being guilty, you can kiss your freedom good bye.

Secondly, if you refuse to cooperate, their attitude will change to bad cop. They will say, "OK fine, you do not want to cooperate? I tried to help but now you are going to be in a lot of trouble. Do you have any idea what kind of charges you are facing? You are going away for a long time unless you start talking."

They are going to try and scare you into admitting guilt. Again, keep your mouth shut and continue to ask for a lawyer, hopefully the one you put on a \$50,000 retainer prior to this happening. Never speak without a lawyer present and never do anything you do not have to do legally. If you have the right to remain silent, then exercise that right. I know there are some circumstances in which you do not have that right, but unless that is the case, you are better off staying quiet.

Third, drop the attitude. Do not argue with the cops about having nothing on you, or something for that matter. Act scared, anxious and confused. Act like you have no idea what is going on and that you are scared for your life. Tell the cops they are scaring you and you want to see your lawyer because you do not know what this is about. They need evidence, and solid evidence at that, to charge you with a crime.

They are going to try and correlate posts you made on forums, phone numbers you called, perhaps a package shipped to your home, all forms of communication, bank transfers, and so forth, until they can find a way to link you to the crime you are being accused of. But the biggest piece of evidence

will always be your willingness to admit your guilt for a lesser sentence.

When Sabu found that he was facing 112 years in federal prison, he quickly spilled everything and started working for the feds. Again, talk to your lawyer, find out the evidence against you and only answers questions your lawyer advises you to answer, and answer them in a way your lawyer advises you to answer them.

Try and be as honest as possible with your lawyer. Your lawyer can not and will not share any admittance of guilt you have with the prosecutors or LE, this is called Attorney-client privilege.

Please note there are a few instances where this does not apply.

[https://en.wikipedia.org/wiki/Attorney%E2%80%93client\\_privilege#When\\_the\\_privilege\\_may\\_not\\_apply](https://en.wikipedia.org/wiki/Attorney%E2%80%93client_privilege#When_the_privilege_may_not_apply)

How to card Western Union just like to say not my work, taken from another forum, hope it helps someone that

dont know who wrote this tutorial so can give credits

not sure if its posted before, but havent seen it as yet

## **LAST WORDS**

### **No Any True Carder Will Card For Others Guy**

- Their Are Too Many fake Pages On Instagram and Telegram Who Introduce Them as Carder
- Don't Get Ripped From Any Fake Carder
- They Will Just Take Ur Money & Will Block U
- To Avoid This All " Learn Urself , Do Urself "
- Card For Own & Get Ur Product
- Learn From Legit Carders & Do Urself
- Don't Trust Anyone For Product They Will Take Advance & Block U ...

✓ **Learn & Do yourself** ✓