Identity Theft and Information Insecurity

Ming Chow

ming_chow@harvard.edu

April 10, 2008

Motivation

- You receive a letter from an institution that computers containing thousands of records with personal information, including Social Security Numbers and credit card numbers, were compromised. You may have been affected.
- You notice suspicious charges on your latest credit card statement.
- How did these incidents happen? Why did they happen?

About Me

- Born in Boston, MA
- Day: Work at Harvard University
- Night: Instructor at Tufts University (my alma mater)
- Taught *Security, Privacy, and Politics in the Computer Age* in Spring 2005 and Spring 2007
- Frequent guest speaker and instructor:
  - New England Association of Insurance Fraud Investigators (NEAIFI), Association of Certified Fraud Examiners (ACFE), High Technology Crime Investigation Association (HTCIA)
- SANS GIAC Certified Incident Handler (GCIH)

Disclaimer

- Some of the information expressed pertains to Harvard University, while many others are based on personal experiences and work.
- I am not responsible for any damage, accidental or otherwise, that results from the attempted or full utilization of any recommendation presented.

What is Identity Theft?

- The term "identity theft" is a misnomer
- The proper term: fraud
- Fraud is not new, but it has skyrocketed in the recent years
- Why steal an identity?
  - ***Financial gain***
  - Be anonymous
  - Revenge
- Crimes associated with identity theft: espionage, insurance and medical fraud, blackmail, terrorism, illegal immigration
- My presentation goals: provide a complete anatomy of identity theft, from cause to effect to prevention

Crime Doesn’t Pay?

– *In a report released on Thursday, the Internet Crime Complaint Center (IC3) found that the number of complaints decreased slightly, while damage from online fraud grew to $239 million in 2007, up from $198 million in 2006. The IC3, an online portal used by the FBI for receiving cybercrime complaints, processed almost 207,000 reports of criminal activity, a 0.6 percent decrease from 2006. The victims ranged in age from ten- to 100-years old.* (http://www.securityfocus.com/brief/716)

High Risk Information (Home, Work, Business) a.k.a. “Your Identity”

- Social Security Number
- Back accounts
- Credit cards
- Institution ID number
- Driver license
- Passport
- Birth certificate
- Diplomas
- Biometric indicator such as iris scan info
- Naturalization certificate
- Personal health information

How Does Identity Theft Occur?

- Low-tech:
  - Social engineering - Use of influence and persuasion to deceive and manipulate people with or without the use of technology (from flirting to bizarre requests)
  - Disgruntled employees and insider threat
  - Plain-old stealing
  - Lost laptop or mobile device
  - Buying information from a terminally ill person
  - Passwords on sticky notes
  - Phishing and unsolicited e-mails
  - Dumpster diving and camping / unshredded critical documents
  - Change of address
  - Weak passwords
  - “Just ask for it”

How Does Identity Theft Occur? (continued)

- High-tech:
  - Keylogger
  - Insecure web applications and websites
  - Rogue WiFi access points
  - Malware: computer viruses and Trojan Horses
  - Unpatched operating systems and software (e.g., Microsoft Windows, QuickTime, Firefox)
  - No encryption on laptop or mobile device
  - Google
  - Other online search engines (e.g., public records)
  - Card skimming (at ATM machines)

How Your Data Was Lost (From *Wired Magazine*; 2/2007)

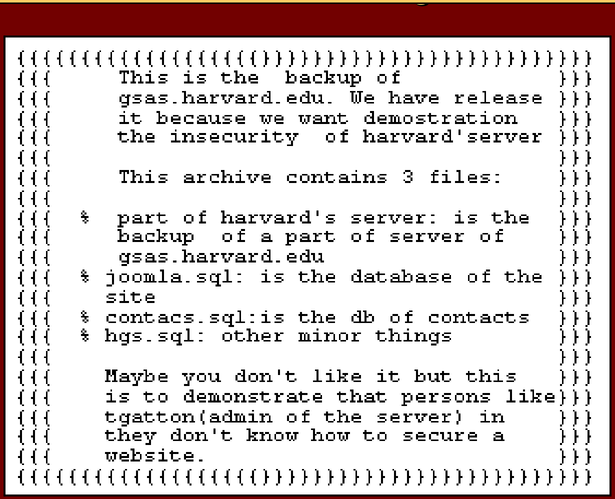
- 35%: Lost laptop or other devices
- 21%: Third party or outsourcer breach (see the US Government)
- 19%: Lost electronic backup
- 9%: Misplaced paper records
- 9%: Inside job or malicious code (including logic bombs and backdoors)
- 7%: Hackers
- Summary: your data was lost most likely due to *low-tech* reasons.

If I Was A Bad Guy, What Do I Want?

- Information is gold (e.g., personnel records, passwords, source code)
- Attack plan:
  - Identify target(s)
  - Research and reconnaissance
  - Pick method(s)
  - Develop and build trust
  - Exploit trust
  - Document and use information
  - Refine strategy (if necessary)
- Defining success:
  - Physical access to protected resources (e.g., critical files)
  - Remote access credentials (e.g., computer networks, Windows Command Prompt)
  - Other security controls (e.g., making victims transfer funds)

Case Study 1: Weak Passwords

- *Potential scenario*: An attacker has your Harvard ID and PIN. The attacker can retrieve all your personal information including SSN via HarvIE > PeopleSoft.
- *Real scenario*: The Harvard University Graduate School of Arts and Science (GSAS) was broken into via content management system thanks to a weak administrator password. The website was taken down from 2/17/2008 – 2/21/2008. Worst of all, the hacker copied all the files on the website, including database files of applicant data, and posted them for download.
  - Official Harvard statement: http://www.news.harvard.edu/gazette/2008/03.13/99-hacked.html
  - The posting from the attacker:

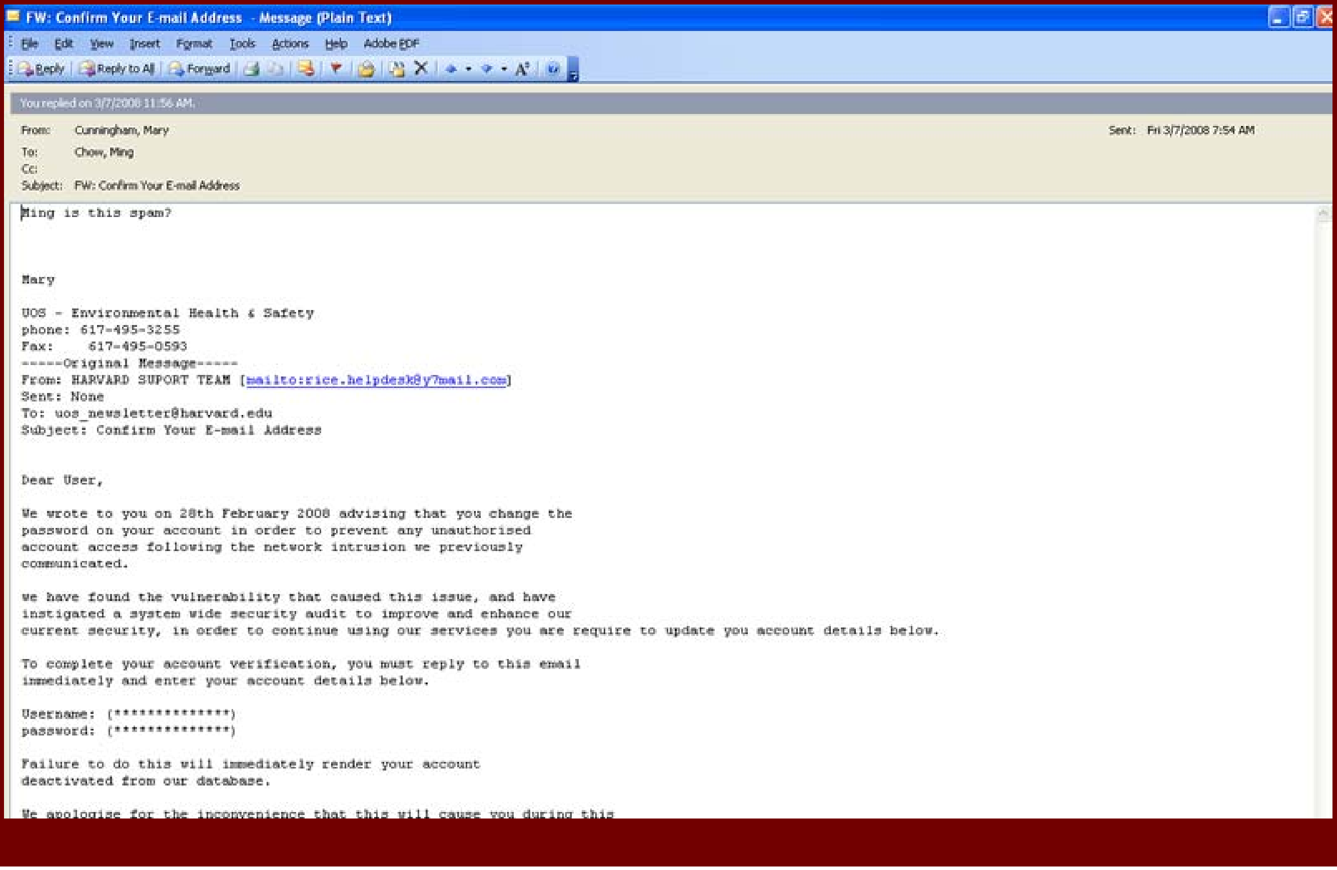


```
{{{{{{{{{{{{{{{{{{{{}}}}}}}}}}}}}}}}}}}}}}}}}
{{{     This is the  backup of           }}}
{{{     gsas.harvard.edu. We have release }}}
{{{     it because we want demostration  }}}
{{{     the insecurity  of harvard'server }}}
{{{                                      }}}
{{{     This archive contains 3 files:   }}}
{{{                                      }}}
{{{  %  part of harvard's server: is the  }}}
{{{     backup  of a part of server of   }}}
{{{     gsas.harvard.edu                 }}}
{{{  % joomla.sql: is the database of the }}}
{{{    site                              }}}
{{{  % contacs.sql:is the db of contacts  }}}
{{{  % hgs.sql: other minor things        }}}
{{{                                      }}}
{{{    Maybe you don't like it but this  }}}
{{{    is to demonstrate that persons like}}}
{{{    tgatton(admin of the server) in   }}}
{{{    they don't know how to secure a   }}}
{{{    website.                          }}}
{{{{{{{{{{{{{{{{{{{{}}}}}}}}}}}}}}}}}}}}}}}}}
```

  - From the *Harvard Crimson*: http://www.thecrimson.com/article.aspx?ref=521987

Case Study 2: Phishing

- Potential scenario (which has already happened numerous times): you receive an e-mail from {PayPal, eBay, Amazon} to update your account information including SSN and credit card information => bank account cleaned out.
- Real scenario:



You replied on 3/7/2008 11:56 AM.

From: Cunningham, Mary
Sent: Fri 3/7/2008 7:54 AM
To: Chow, Ming
Cc:
Subject: FW: Confirm Your E-mail Address

```
Ming is this spam?



Mary

UOS - Environmental Health & Safety
phone: 617-495-3255
Fax:    617-495-0593
-----Original Message-----
From: HARVARD SUPORT TEAM [mailto:rice.helpdesk@y7mail.com]
Sent: None
To: uos_newsletter@harvard.edu
Subject: Confirm Your E-mail Address


Dear User,

We wrote to you on 28th February 2008 advising that you change the
password on your account in order to prevent any unauthorised
account access following the network intrusion we previously
communicated.

we have found the vulnerability that caused this issue, and have
instigated a system wide security audit to improve and enhance our
current security, in order to continue using our services you are require to update you account details below.

To complete your account verification, you must reply to this email
immediately and enter your account details below.

Username: (**************)
password: (**************)

Failure to do this will immediately render your account
deactivated from our database.

We apologise for the inconvenience that this will cause you during this
```

Case Study 3: Lost or Stolen Laptop

- Too many to list
- From the US Department of Veterans Affairs (loss of over 26.5 million vet records) to Boeing (loss of over 400,000 records of retired and current company workers)
  - Many of the government cases are contractor-related
- Hall of Shame: http://www.forbes.com/2006/09/06/laptops-hall-of-shame-cx_res_0907laptops.html
- Bottom line: lost laptop = lost data

Case Study 4: TJX, Hannaford, and Museum of Science (Boston)

- All high-tech breaches
- TJX:
  - Bad wireless security (using the Wireless Encryption Protocol (WEP)) for one
  - “Loss of over 45 million credit card numbers and more than 450,000 SSNs, driver's license numbers, and military identifications...could exceed over $1B in losses for the company.”
  - More information: http://hardware.slashdot.org/article.pl?sid=07/05/05/1812254&from=rss
- Hannaford Supermarkets:
  - Malware
  - “Method in which software was secretly installed on servers at every one of its grocery stores”
  - 4.2 million credit and debit card account numbers compromised; breach has been linked to about 2,000 cases of fraud.
  - More information: http://www.ecommercetimes.com/story/62344.html?welcome=1207761189
- Museum of Science:
  - Contractor error
  - 140 patrons’ names, credit card numbers, and other personal information were exposed on the museum's website
  - More information: http://www.boston.com/news/local/massachusetts/articles/2008/03/28/museum_says_data_of_patrons_was_public/

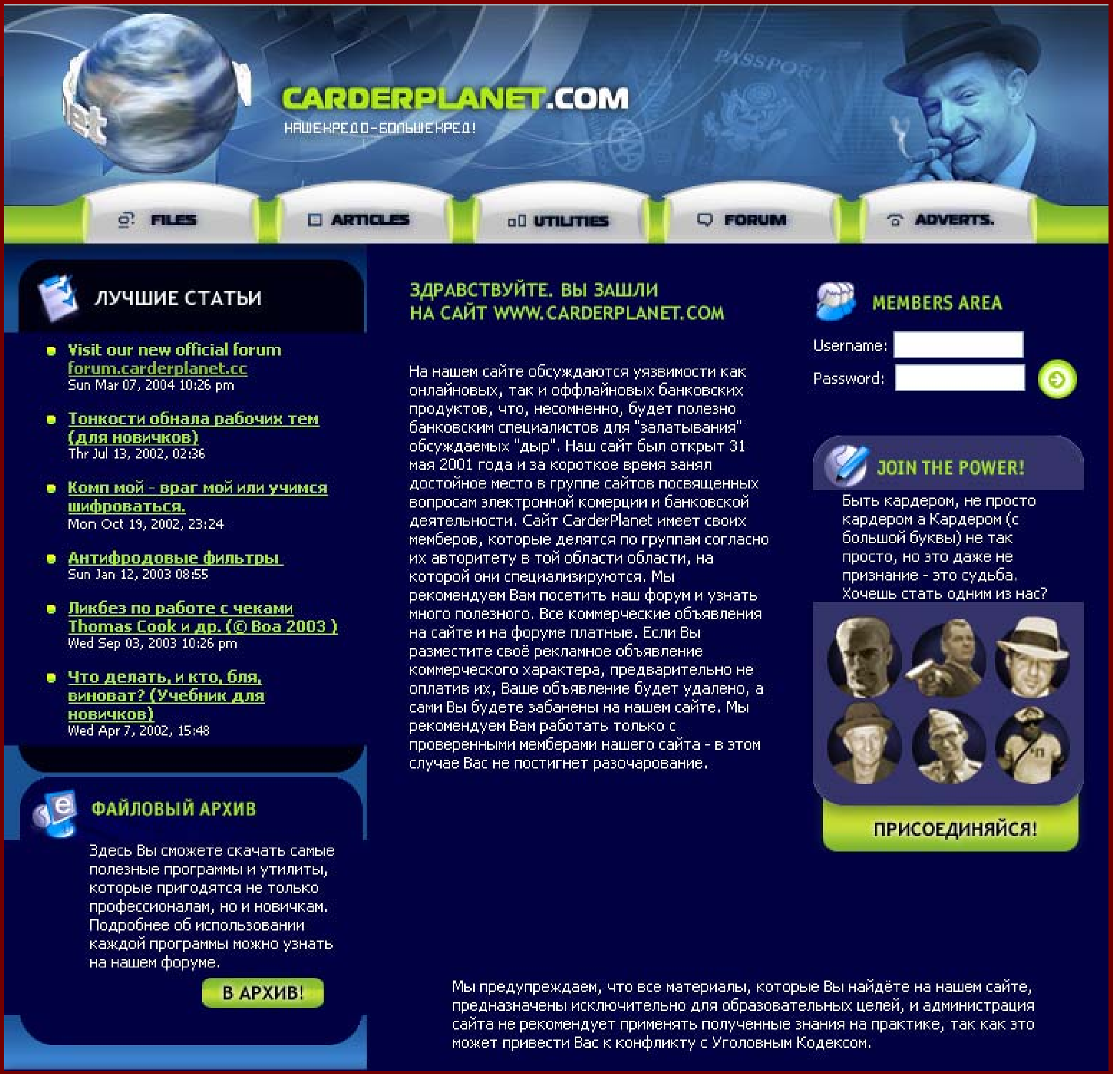
Suspicious Activities: Effects Due to a Breach

- Bills do not arrive as expected
- Unknown users connected to your computer or network
- Unexpected credit cards or account statements
- Unexpected credit card charges on your statement
- Denials of credit for no apparent reason
- Calls, letters, or visits (from one of the government agencies or from a collection agency) about purchases that you did not make
- Case-in-point: MA Attorney General Martha Coakley received a call from Dell regarding a computer order that she did not place (http://www.infoworld.com/article/07/01/22/HNmarthacoakley_1.html)

A Little About the Underground Economy: How Your Information is Sold and Channeled

- Cybercriminals take cues from mafia
- *"This organized crime group, Carderplanet, organized themselves into the same structure as the Italian Mafia"* –Thomas X. Grasso, FBI
- The crime group's website resembles that of a legitimate business
- Carderplanet.com (from Eastern Europe) –no longer in operation
- More details at http://www.f-secure.com/weblog/archives/carderplanet_index.htm (don't worry, legitimate website)

A Little About the Underground Economy: How Your Information is Sold and Channeled (Screen 1)



ЛУЧШИЕ СТАТЬИ

- Visit our new official forum forum.carderplanet.cc
  Sun Mar 07, 2004 10:26 pm
- Тонкости обнала рабочих тем (для новичков)
  Thr Jul 13, 2002, 02:36
- Комп мой - враг мой или учимся шифроваться.
  Mon Oct 19, 2002, 23:24
- Антифродовые фильтры
  Sun Jan 12, 2003 08:55
- Ликбез по работе с чеками Thomas Cook и др. (© Boa 2003)
  Wed Sep 03, 2003 10:26 pm
- Что делать, и кто, бля, виноват? (Учебник для новичков)
  Wed Apr 7, 2002, 15:48

ФАЙЛОВЫЙ АРХИВ

Здесь Вы сможете скачать самые полезные программы и утилиты, которые пригодятся не только профессионалам, но и новичкам. Подробнее об использовании каждой программы можно узнать на нашем форуме.

ЗДРАВСТВУЙТЕ. ВЫ ЗАШЛИ
НА САЙТ WWW.CARDERPLANET.COM

На нашем сайте обсуждаются уязвимости как онлайновых, так и оффлайновых банковских продуктов, что, несомненно, будет полезно банковским специалистов для "залатывания" обсуждаемых "дыр". Наш сайт был открыт 31 мая 2001 года и за короткое время занял достойное место в группе сайтов посвященных вопросам электронной комерции и банковской деятельности. Сайт CarderPlanet имеет своих мемберов, которые делятся по группам согласно их авторитету в той области области, на которой они специализируются. Мы рекомендуем Вам посетить наш форум и узнать много полезного. Все коммерческие объявления на сайте и на форуме платные. Если Вы разместите своё рекламное объявление коммерческого характера, предварительно не оплатив их, Ваше объявление будет удалено, а сами Вы будете забанены на нашем сайте. Мы рекомендуем Вам работать только с проверенными мемберами нашего сайта - в этом случае Вас не постигнет разочарование.

MEMBERS AREA

Username:

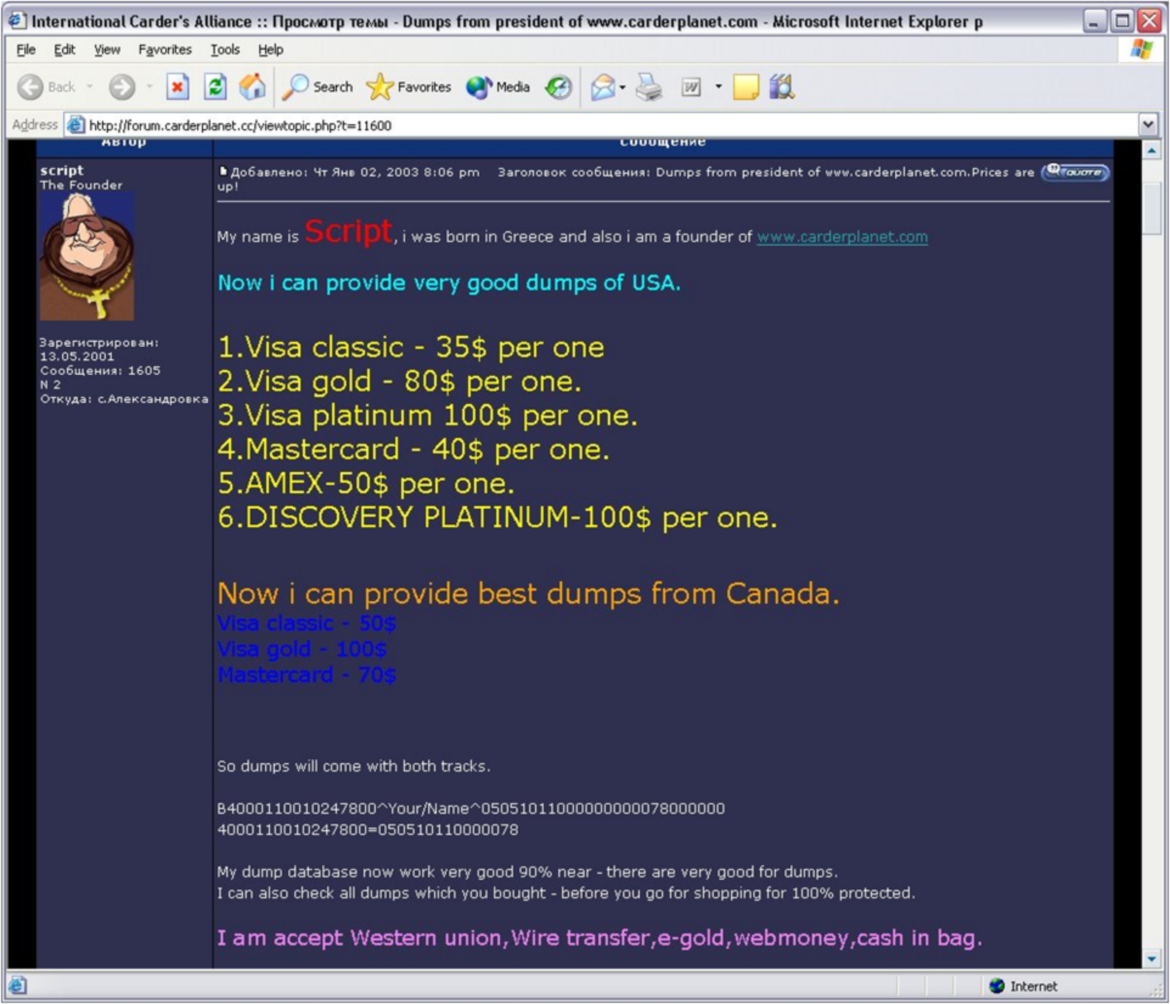
Password:

JOIN THE POWER!

Быть кардером, не просто кардером а Кардером (с большой буквы) не так просто, но это даже не признание - это судьба. Хочешь стать одним из нас?

Мы предупреждаем, что все материалы, которые Вы найдёте на нашем сайте, предназначены исключительно для образовательных целей, и администрация сайта не рекомендует применять полученные знания на практике, так как это может привести Вас к конфликту с Уголовным Кодексом.

A Little About the Underground Economy: How Your Information is Sold and Channeled (Screen 2)


International Carder's Alliance :: Просмотр темы - Dumps from president of www.carderplanet.com - Microsoft Internet Explorer p
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address http://forum.carderplanet.cc/viewtopic.php?t=11600
Автор
Сообщение
QUOTE
Internet

script
The Founder

Зарегистрирован: 13.05.2001
Сообщения: 1605
N 2
Откуда: с.Александровка

Добавлено: Чт Янв 02, 2003 8:06 pm   Заголовок сообщения: Dumps from president of www.carderplanet.com.Prices are up!

My name is Script, i was born in Greece and also i am a founder of www.carderplanet.com

Now i can provide very good dumps of USA.

1.Visa classic - 35$ per one
2.Visa gold - 80$ per one.
3.Visa platinum 100$ per one.
4.Mastercard - 40$ per one.
5.AMEX-50$ per one.
6.DISCOVERY PLATINUM-100$ per one.

Now i can provide best dumps from Canada.
Visa classic - 50$
Visa gold - 100$
Mastercard - 70$

So dumps will come with both tracks.

```
B4000110010247800^Your/Name^05051011000000000078000000
4000110010247800=050510110000078
```

My dump database now work very good 90% near - there are very good for dumps.
I can also check all dumps which you bought - before you go for shopping for 100% protected.

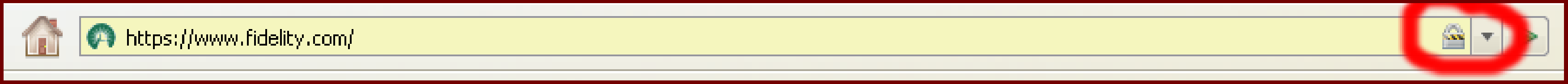
I am accept Western union,Wire transfer,e-gold,webmoney,cash in bag.

Protect Yourself: Your Basic Responsibilities at Work

- (Largely) from the Harvard University High Risk Information brochure:
  - Protect high risk information
  - Destroy high risk information properly (e.g., W4 forms, IDs)
  - Secure human subject information
  - Safeguard personally identifiable medical information
  - New contracts for services where the contractor obtains Social Security, credit card, or bank account numbers of Harvard-associated people from Harvard or on behalf of Harvard must include a contract rider (available at http://www.security.harvard.edu/for_employees/web_privacy.php)
  - You should review any approved use and protection of confidential information with your local IT group and HR
  - Disclose any security breach involving high risk information
    - Can be a rather tricky issue: best to contact your local IT group and HR first
  - Be educated (as you are doing here!)

Protect Yourself: Low-Tech

- Buy a shredder
- View your credit report
- Credit freeze
- Don’t sign the back of that card
- Don’t carry Social Security Card in your wallet or purse
- Don’t mark your SSN on checks
- Keep good backups of important files (manually)
- Limit storage of critical documents on mobile devices unless it is necessary
- Monitor your bank accounts online
- Use strong passwords (definitely nothing obvious)
- Log off or lock your computer when you leave your desk
- Web browsing basics (see screenshot below):
  - Verify the URL
  - When performing a financial transaction (e.g., online banking), make sure that you see a lock icon on your web browser and verify that the certificate is verified by a legitimate certificate authority via double-clicking on the lock (e.g., Verisign)



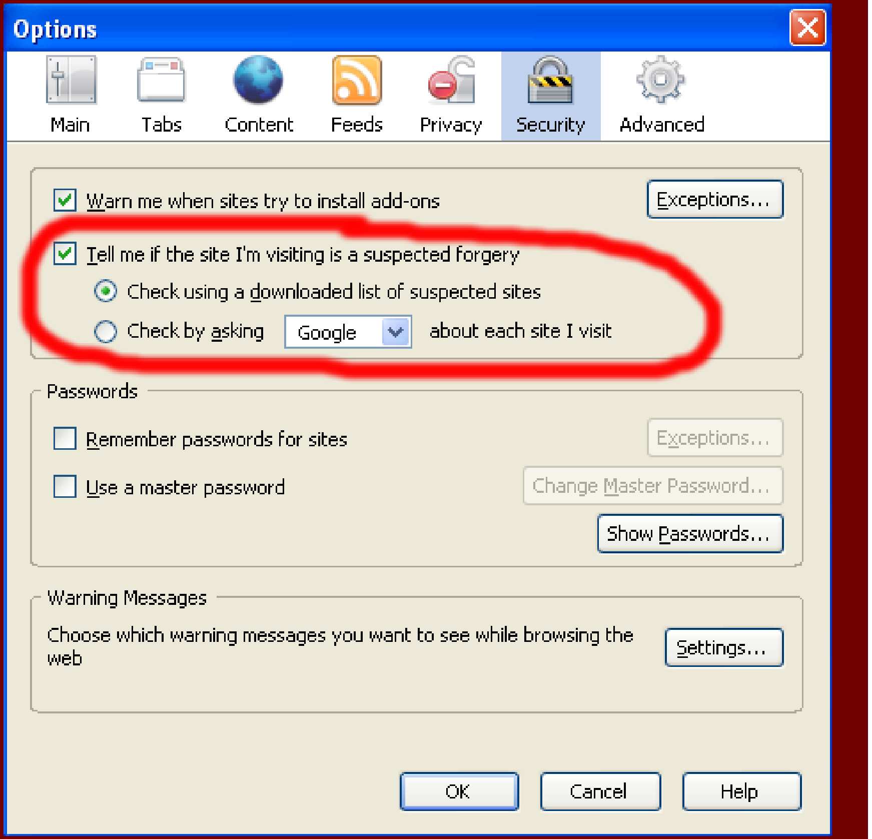
https://www.fidelity.com/

Protect Yourself: E-Mail (a.k.a. how to not get hooked into a phishing trip)

- Treat e-mail like postcards
- Make sure that e-mail is coming from who it seems to be from. If you were not expecting an attachment, write back and request that sender embeds text in email.
- Never respond to an email asking for personal information
  - It goes without saying, legitimate businesses will never ask you to send personal information, including passwords and bank account information
- Do not send personal or financial information by e-mail
- Be cautious about opening any attachment or downloading any files from e-mails you receive regardless of who sent them
- Do not reply to e-mail or pop-up messages that ask for personal or financial information, and don't click on links in the message
- Do not cut and paste a link from the message into your web browser - phishers can make links look like they go one place, but actually send you to a different site
- Read my former student, Pavan Nyama's, presentation and quiz at: http://www.eecs.tufts.edu/~mchow/excollege/s2007/students_works/final_pnyama.pdf

Protect Yourself: High-Tech Methods and Tools

- SiteAdvisor (http://www.siteadvisor.com/) – A plugin for either Internet Explorer or Firefox; warns user of malicious or fradulent websites
- Utilize the Google “blacklist”: http://sb.google.com/safebrowsing/update?version=goog-black-url:1:1
  - The Firefox web browser has the capability to identify fraudulent websites via Google blacklist (see right)
- Enable WPA2 encryption on your wireless router / network at home --not WEP because it can be broken rather easily
- Keep anti-virus definitions up-to-date
- Patch software, especially the operating system (e.g., Microsoft Windows via Windows Update)



☑ Warn me when sites try to install add-ons [Exceptions...]

☑ Tell me if the site I'm visiting is a suspected forgery

● Check using a downloaded list of suspected sites

○ Check by asking [Google] about each site I visit

Passwords

□ Remember passwords for sites [Exceptions...]

□ Use a master password [Change Master Password...]

[Show Passwords...]

Warning Messages

Choose which warning messages you want to see while browsing the web [Settings...]

Protect Yourself: Encryption with TrueCrypt

- Some encryption is better than no encryption
- The downside: password-dependent
- TrueCrypt: http://www.truecrypt.org/ - Disk encryption software for Windows (XP / Vista), Linux, and Mac OS X
- Free and open source software
- Features:
  - Creates a virtual encrypted disk within a file and mounts it as a real disk.
  - Encrypts an entire partition or storage device such as USB flash drive or hard drive.
  - Encrypts a partition or drive where Windows is installed (pre-boot authentication).
  - Encryption is automatic, real-time (on-the-fly) and transparent.
- My old instructions: http://www.oreillynet.com/onlamp/blog/2006/11/give_the_gift_of_security_and.html

Eradication and Recovery

- Wipe your computer using DoD Standard 5220.22-M (e.g., 3 - 6 wipes; 3 - 9 hours depending on size of hard drive) and reinstall all software
  - Software to do this: AccessData's WipeDrive (commercial), Darik's Boot and Nuke (DBAN) –free at http://dban.sourceforge.net
- Place a "fraud alert" on credit reports via three credit agencies (Equifax, Experian, TransUnion)
- Place a credit freeze
- Close accounts that have been tampered with
- File a police report
- Report the theft to the Federal Trade Commission (FTC)
- Restore from backups
- Do not create backup of compromised machine for future use
- Change passwords
- Keep good documentation
- Learn from your experiences

Conclusion

- The weakest link of security: *humans*
- Technology and tools can only do so much for security
- The best advice: *use your common sense*
- Problems are only getting worse thanks to the ubiquitousness of technology: the gap between growth and knowledge is getting wider
- Education / training is arguably one of the best solution for prevention

Resources

- SANS Institute – Security Awareness Tips: http://www.sans.org/tip_of_the_day.php
- Federal Trade Commission (FTC)'s ID Theft Site: http://www.ftc.gov/idtheft
- Harvard University Information Security and Privacy (includes Enterprise Security Policy): http://www.security.harvard.edu/
- SecurityFocus: http://www.securityfocus.com/