

# Are you at risk for Identity Theft?



January 2005  
DoIT Dialogue

Cathy Hubbs, IT Security Coordinator, ITU Project Office  
<http://security.gmu.edu>

# Why talk about identity theft?

- With the advent of the Information Age, in particular the Internet, electronically stored personal data has become common place.
- Sensitive data— not just credit card numbers- but buying habits and other personal information is being recorded.
- Individuals must protect themselves by strengthening their general security awareness.
- Identity theft is on the rise...



# Why talk about identity theft?

- According to the Federal Trade Commission, 9.9 million Americans were struck by identity thieves in 2003. Costing individuals and businesses \$52.6 billion in expenses.
- Virginia ranks the 19<sup>th</sup> highest in terms of identity theft victims. Alexandria was the top city in VA with 366 reported victims.
- It could be worse...  
we could live in Arizona which had the most victims of any state.



# Why talk about identity theft?

- 52% (5 million) people discovered they were victims by monitoring their accounts.
- 26% (2.5 million) people said their banks or credit-card issuers alerted them to suspicious purchases.
- 8% discovered they were victims after they were turned down for credit.



# Why talk about identity theft?

A little closer to home...colleges that leak personal data:

- January 2004, the Washington Square News, New York University's campus newspaper, reported mailing lists with the names, birth dates, addresses, phone numbers, e-mail addresses and ssn of over 2,100 students, alumni and professors were accidentally posted on a campus Web site.
- In February, California State University at Monterey Bay warned 2,800 applicants, an employee had inadvertently posted their names, addresses and ssns on the Internet by moving the information to a folder that was not secure.
- In April, officials at the University of Kansas called in the FBI when hackers access electronic pharmacy records, ssns, names, addresses, birth dates and prescription records filed from July 1994 to January 2004 at the on campus pharmacy through the Student Health services network.

SOURCE: August 2004, Higher Learning TEACH Magazine, "Stolen ID", Krista Glen.



# At home-January 2005

- Routine log analysis discovers suspicious behavior
- Decision is made to contact Mason police and open investigation.
- Mason police contact state and federal authorities
- Public announcement is made
- Current information is being made available at <http://www.gmu.edu/intrusion>



# Closing remarks about our incident

- Mason's key central servers that contain financial information, student grades, personnel records, and other sensitive information, have not been affected by the break-in and are highly protected.
- Records of applications from prospective students were not on this server and have not been accessed.
- As yet, we have no evidence that any information has been stolen from the server. We only know that software tools for further hacking were placed on the server.
- A company has been hired, specializing in fraud investigation and forensics.



# Why talk about identity theft?

- The Aberdeen Group predicts by the end of 2005, identity theft will result in total personal loss of \$2 trillion.
- As the statistics illustrate, identity theft has reached a critical mass. Some companies have tried to combat this rise with comedic relief in an attempt to raise consumer awareness.
- For those of you that have missed out, let's [watch...](#)



# Who are the thieves?

- Insiders! Notably healthcare and financial institutions.
- Michigan State University's Identity Theft research center reports up to 70% of identity thefts originate in the work place.
- Economically depressed regions often cultivate this type of crime.
- Average person with a motive for easy cash...with one or all of the following:
  - › an internet connection
  - › basic social engineering skills
  - › not afraid to dumpster dive



# How do they do it?

- Using the Internet
- Spoofing
- Phishing
- Spyware
- Social Engineering
- Dumpster Diving



# How do they do it? The Internet

- Search engines like Google and their “Advanced search” features:
  - Numerical range feature
    - (i.e., Visa43660000000000000000..4366999999999999 )
  - By file type (i.e., .doc, .xls, .qdf)
  - Check on yourself site:mysite.com
    - What are the search results?
- Search terms Virus creation , Credit Card Generators de-CMaster
- While we are out on the web, why not try looking up a name, address, telephone. Then use Mapquest to locate where that person lives.
- Next we might use a Web Detective service
- And this one is just scary Raw Services Research



# How do they do it? Phishing

- Creating a legitimate looking email that asks for an update or confirmation on personal data.
- The email generally includes a link to a “spoof web site.”
- Clicking on the link could initiate an installation of key logging software or viruses.



# How do they do it? Phishing

- January through May 2004 the number of discrete attempted phishing attacks increased twenty fold.
- Attacks are more targeted and sophisticated.
- Phishers modus operandi is “conning”

- Number of attacks:

11/03	21
12/03	107
1/04	185
2/04	282
3/04	402



Source: CSO Magazine, June 2004.

# How do they do it? Spyware

- A small program embedded in a larger application, which allows the developers of the applications to collect and disseminate information about the individuals using them.
- Take advantage of security weakness in MS Windows, Active X, and package with desired software.
- Can track web surfing habits, profiling shopping preferences, hijacking your browser's start page and altering important system files
- Is capable of transmitting information such as keystrokes, passwords and personal information from your PC to a remote location.



# How do they do it? Social Engineering

Hyperdictionary.com

- **Definition:** Term used among *crackers* and *samurai* for cracking techniques that rely on weaknesses in *wetware* rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system's security.
- Classic scams include phoning up a mark who has the required information and posing as a field service tech or a fellow employee with an urgent access problem.
- Dumpster Diving not really social engineering



# What can we do?

## Physical World

- ✓ Think defensively, act cautiously.
- ✓ Check credit regularly-Every 4 months
- ✓ Decide how much information you really need to carry with you.
- ✓ Keep an emergency file at home.
- ✓ Activate a fraud alert feature
- ✓ Check to see if you can get your picture on your credit card
- ✓ Write “Ask for Photo ID” next to your signature on your credit cards.
- ✓ Balance your check book, regularly.
- ✓ Shred financial statements and other sensitive data before trashing.
- ✓ Check merchant credit card receipts-for example, Brion's!



# What can we do?

## Virtual World

- ✓ Create strong passwords
- ✓ Don't open suspicious emails or click on links contained in those emails.
- ✓ Keep Antivirus software installed and current
- ✓ Keep computer software patched
- ✓ Use anti-Spyware/Adware software
- ✓ Use a Firewall- Windows XP Service Pack2



# What can we do?

## Virtual World

- ✓ Do not provide sensitive information via email (even if requested). Call requestor and verify.
- ✓ Look for the “s” after http:// or the padlock icon in your browser window when making online purchases.
- ✓ Tossing or replacing your computer? Use a product to erase sensitive data from the hard drive.
- ✓ Do not email your social security number to anyone.
- ✓ Back up critical files and programs, just in case!



# What can we do?

## Politically

- Write your congressmen. Ask them to promote Opt-In legislation
- Support tougher Identity Theft laws for criminals
- Support favorable laws for consumers
- Speak out about computer vendors. Vendors need to be held accountable for testing software and hardware before commercial release.



# What has been done?

- Amendment to the federal Fair Credit Reporting Act
- White House produced National Strategy to Secure Cyberspace (final draft Feb 2003)
- HIPAA (1996), GLBA (1999), SOX (2002)
- Identity Theft Penalty Enhancement Act (July 2004)
- California SB 1386 (July 2003)
- Educause, DHS, & Infraguard partnered to promote information sharing and notification.



# Summary

- General awareness is critical.
- Credit history should be checked regularly!
- Opt-in privacy policies should be the default.
- Those that collect and hold information must secure that data and be held accountable.
- Vendors must design and sell software that is secure.
- Read End License User Agreements - EULA



# Resources

- eWeek, August 30, 2004. Larry Seltzer, “Don’t Expect Privacy on the Web”
- Freelance Star, August 12, 2004 “Who Are You?” Portia Smith.
- Higher Learning TEACH Magazine, August 2004 “Stolen ID”, Krista Glen
- ITU Support Center website [itusupport.gmu.edu](http://itusupport.gmu.edu)
- Citibank, [www.citibank.com](http://www.citibank.com)
- [www.creditboards.com](http://www.creditboards.com)
- CSO Online Magazine, [www.csoonline.com](http://www.csoonline.com)
- Crime Doctor, [www.crimedoctor.com](http://www.crimedoctor.com)
- Federal Trade Commission, [www.ftc.gov](http://www.ftc.gov)
- HIPAA Advisory, [www.hipaadvisory.com](http://www.hipaadvisory.com)
- Hyperdictionary, [www.hyperdictionary.com](http://www.hyperdictionary.com)
- Privacy Rights organization, [www.privacyrights.org](http://www.privacyrights.org)
- Vericept Corporation, August 15, 2004 Notification of Identity Theft Legislation, [www.vericept.com](http://www.vericept.com)
- Washington Post, September 1, 2004, John Kelly’s Washington

QUIZ-<http://security.gmu.edu>



## Identity Theft IQ Test

### Are You at Risk for Identity Theft? Test Your "Identity Quotient"

\_\_\_\_\_ I receive several offers of pre-approved credit every week. **(5 points)**

\_\_\_\_\_ **Add 5 points** if you do not shred them before putting them in the trash.

\_\_\_\_\_ I carry my Social Security card in my wallet. **(10 points)**

\_\_\_\_\_ My state driver's license has my SSN printed on it, and I have not contacted the Department of Motor Vehicles to request a different number. **(10 points)**

\_\_\_ I do not have a PO Box or a locked, secured mailbox. **(5 points)**

\_\_\_ I use an unlocked, open box at work or at my home to drop off my outgoing mail. **(10 pts.)**

\_\_\_ I carry my military ID in my wallet at all times. **(10 points)**

\_\_\_ I do not shred or tear banking and credit information when I throw it in the trash. **(10 pts.)**

\_\_\_ I provide my Social Security number (SSN) whenever asked, without asking questions as to how that information will be safeguarded. **(10 points)**

\_\_\_ **Add 5 points** if you provide it orally without checking to see who might be listening.

\_\_\_ I am required to use my SSN at work as an employee ID or at college as a student ID number. **(5 points)**

\_\_\_ My SSN is printed on my employee badge that I wear at work or in public. Or it is posted on my time card in full view of others, or is on other documents frequently seen by many others in my workplace. **(10 points)**

\_\_\_ I have my SSN and/or driver's license number printed on my personal checks. **(10 points)**

\_\_\_ I am listed in a "Who's Who" guide. **(5 points)**

\_\_\_ I carry my insurance card in my wallet and either my SSN or that of my spouse is the ID number. **(10 points)**

\_\_\_ I have not ordered a copy of my credit reports for at least 2 years. **(20 points)**



# FTC Phishing Tips

- Call 877-FTC-Help for FREE copy

“How Not to Get Hooked by a “Phishing Scam”

<http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm>



## Understanding Your Score:

### 100 + points

Recent surveys\* indicate that 7-10 million people were victims of ID theft last year. You are at high risk. We recommend you purchase a paper shredder, become more security-aware in document handling, and start to question why people need your personal data.

### 50-100 points

Your odds of being victimized are about average. Higher if you have good credit.

### 0-50 points

Congratulations. You have a high "IQ." Keep up the good work and don't let your guard down now.

For information on recent identity theft survey findings, visit the Privacy Rights Clearinghouse web site at [www.privacyrights.org/ar/idtheftsurveys.htm](http://www.privacyrights.org/ar/idtheftsurveys.htm).

For a list of tips on reducing your risk of identity theft, read our Fact Sheet 17, "Coping with Identity Theft: Reducing the Risk of Fraud," at [www.privacyrights.org/fs/fs17-it.htm](http://www.privacyrights.org/fs/fs17-it.htm). Remember, you cannot prevent identity theft. Criminals can commit identity theft relatively easily because of lax credit industry practices and the ease of obtaining SSNs. But you can reduce your risk of fraud by following the tips in Fact Sheet 17. The most important advice we can give you is to check your credit report at least once a year. If you are a victim of identity theft, you will catch it early by checking your credit report regularly.

The Identity Theft IQ Test was developed by the Privacy Rights Clearinghouse (PRC) <http://www.privacyrights.org/>, and the Utility Consumers' Action Network, <http://www.ucan.org/>.

Please contact the PRC for permission to use this document. Phone (619) 298-3396, or E-mail [bgivens@privacyrights.org](mailto:bgivens@privacyrights.org).

The Privacy Rights Clearinghouse is a nonprofit consumer education, research, and advocacy program. Our publications empower you to take action to control your personal information by providing practical tips on privacy protection.

Copyright © 1999-2004, Utility Consumers' Action Network / Privacy Rights Clearinghouse.

Revised Sept. 2003.

