

Security Awareness Day November 14, 2006

Kelley Bogart
Information Security Coordinator
University of Arizona

Agenda

- What is Identity Theft
- Some statistics
- How it happens
- Preventative Measures
- What to do if you're a victim

What is Identity Theft?

The term “identity theft” means a fraud committed or attempted using the identifying information of another person without authority.

The term “identifying information” means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any

- name, social security number, date of birth, official driver's license or identification number, alien registration number, passport number, employer or taxpayer identification number;
- unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
- unique electronic identification number, address, or routing code; or
- telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)).

What is Identity Theft?

Identity theft occurs when someone uses your personally identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.

What is "pretexting"?

Pretexting is the practice of getting your personal information under false pretenses. Pretexters sell your information to people who may use it to get credit in your name, steal your assets, or to investigate or sue you. Pretexting is against the law.

What is Identity Theft?

Wrongfully impersonating someone, typically for financial gain either by exploiting the reputation of the subject person or stealing from him. A person usually steals an identity by using knowledge of personal information about the subject. Some people prefer the term "identity fraud" since the "thief" doesn't deprive the owner of his identity.

How it's characterized:

- Credit Card Fraud
 - Phone or Utilities Fraud
 - Bank/Finance Fraud
 - Government Documents Fraud
 - Other Fraud
- 

A Few Statistics

Identity theft is the fastest growing crime in the United States. It alone accounts for over 42 percent of all complaints filed with the Federal Trade Commission.

The FTC estimates that as many as 10 million Americans have their identities stolen each year. In fact, you or someone you know may have experienced some form of identity theft.

Who is more likely to fall victim?

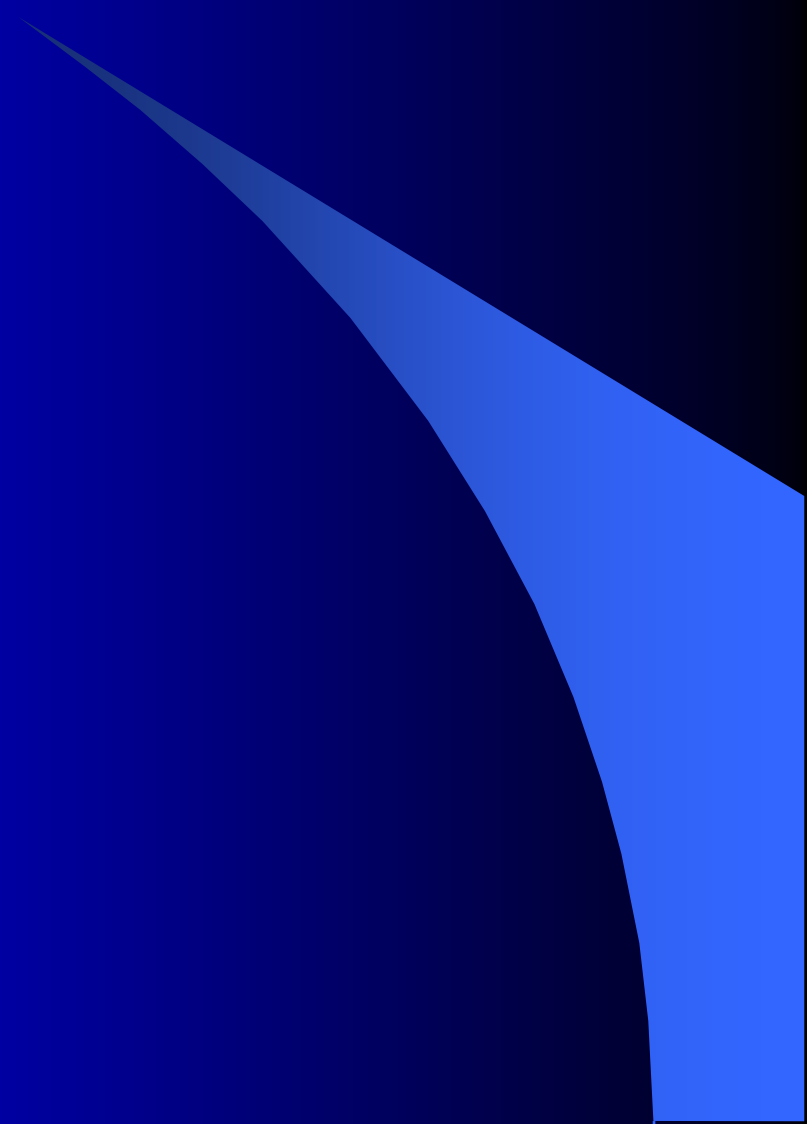
Victims

- Age
- Income
- Geography

Arizona has the highest rate in the nation!

- 156.9 victims per 100,000
- Phoenix, Mesa, Scottsdale 178.3 victims

How it happens

- Computer based
 - Human based
 - Social Engineering
- 
- A decorative graphic on the right side of the slide, consisting of a large, light blue curved shape that tapers to a point at the top and extends downwards, set against a dark blue background.

Social Engineering

The practice of obtaining confidential information by manipulation of legitimate users. A social engineer will commonly use the telephone or Internet to trick people into revealing sensitive information or getting them to do something that is against typical policies. By this method, social engineers exploit the natural tendency of a person to trust his or her word, rather than exploiting computer security holes.

Social engineering preys on qualities of human nature:

- ✓ the desire to be helpful
- ✓ the tendency to trust people
- ✓ the fear of getting into trouble

Computer Based

- Computer Hacking or Compromise
 - ✓ Phishing
 - ✓ Spyware
 - ✓ Viruses
 - ✓ Using the Internet



Phishing

A form of social engineering, characterized by attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or legitimate business in an apparently official electronic communication, such as an email, pop-up window or an instant message.

Phishing



[? Need Help?](#)

Dear eBay User,

We regret to inform you, that we had to block your eBay account because we have been notified that your account may have been compromised by outside parties.

Our terms and conditions you agreed to state that your account must always be under your control or those you designate at all times. We have noticed some activity related to your account that indicates that other parties may have access and or control of your information in your account.

Please be aware that until we can verify your identity no further access to your account will be allowed. As a result, Your access to bid or buy on eBay has been restricted. To start using your eBay account fully, Please uptake and verify your information by clicking below

<http://signin.ebay.com/aw-cgi/eBayISAPI.dll?Verify>

Regards,

eBay Member Service

****Please Do Not Reply To This E-mail As You Will Not Receive A Response****

[Announcements](#) | [Register](#) | [Safe Trading Tips](#) | [Policies](#) | [Feedback Forum](#) | [About eBay](#)

Copyright ?1995-2003 eBay Inc. All Rights Reserved.

Designated trademarks and brands are the property of their respective owners.

Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).



Spyware: What it is



- spyware is programming that is put in your computer to secretly gather information about You or your pc and relay it to advertisers or other interested parties.
- adware pushes ads, track Internet habits and performs other sneaky tricks

Spyware: What it does

- Corrupt/alter the current software
- Steal passwords, information etc.
- Track browsing habits, sites
- interferes with system settings
 - (registry, startup)

Spyware: How you get it

- Email
- Instant Messaging
- Internet Browsing
- P2P Software (kazaa, limewire, bearshare)
- Downloads and Installs
 - Potentially Unwanted Programs (PUPs)

Using the Internet

- Doing business online
 - Banking
 - Shopping
- Using open unsecured wireless
- Downloading

Information Available Online

“Advanced Search” features:

- Numerical range feature
(i.e., Visa4366000000000000..43669999999999999)
- By file type (i.e., .doc, .xls, .qdf)

Try looking up a name, address, telephone. Then use Mapquest to locate where that person lives.

Ego Surfing

Search terms Virus creation , Credit Card Generators

Human Based

- Skimming
- Dumpster Diving
- Mail theft
 - Changing address
- “Old fashion” theft
 - Purses and Wallets
 - Faxes

Skimming

A hi-tech method by which thieves capture your personal or account information from your credit card, drivers license, or even passport. An electronic device used to capture this information is called a “skimmer,” and can be purchased online for under \$50.00. Your card is swiped through the skimmer and the information contained in the magnetic strip on the card is then read into and stored on the device or an attached computer.

It's predominantly a tactic used to perpetuate credit card fraud. Skimming is a problem, not just in the U.S, but globally.

Skimming

Who

- Restaurant Servers
- Store Clerks

How

- Skimming Devices

What

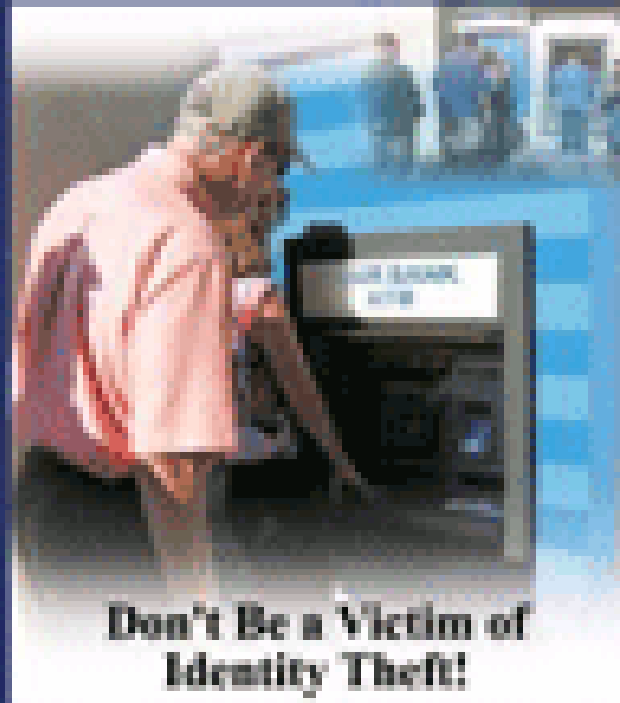
- Sell your information to other criminals
- Commit Credit Card Fraud
- Make counterfeit cards

Dumpster Diving

Dumpster Diving is when an identity thief will go through your trash in order to obtain copies of your checks, credit card or bank statements, or other records--all for the sake of harvesting your personally identifiable information to steal your identity.

Shoulder Surfing

sec-U-R-I-T-y



**Don't Be a Victim of
Identity Theft!**

YOU ARE IT!



The University of Arizona,
Information Security Office
www.iso.arizona.edu

Mail theft

Many convicted identity thieves unashamedly claim that new blank checks and credit offers are their most prized catch. Once in their hands, they have immediate access to money in the victim's checking account and can open up new accounts in the victim's name.

For incoming mail, they strike shortly after it is delivered.

For outgoing mail, they will strike just before the mail is delivered. Mail thieves are known to drive through a neighborhood looking for that little red flag in the upward position on a mailbox. They stop quickly, remove the outgoing mail and no one is the wiser.

Preventative Measures

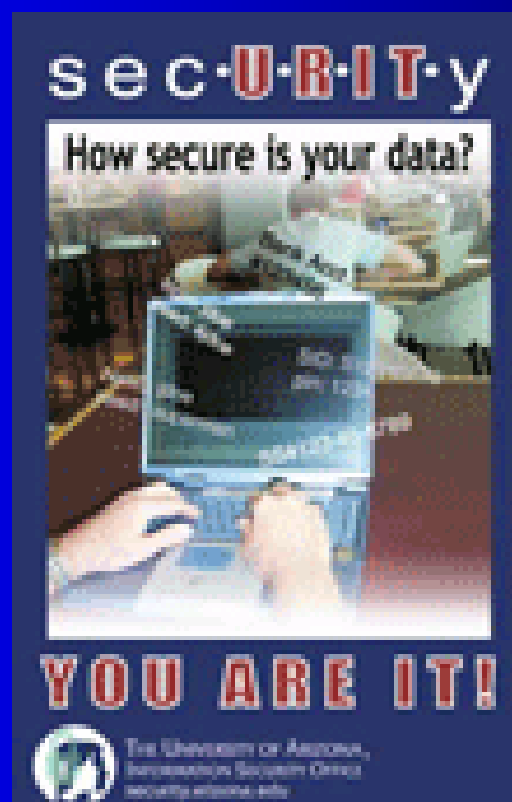
- Watch for Shoulder Surfing
- Require Photo ID verification
- Protect your Social Security Number
- Shred Information
- Be diligent about checking statements
- Order and analyze your check report
- Read Online Privacy Policies
- Be careful who you do business with
- Destroy Digital Data
- Pay bills at the Post Office

Preventative Measures

- Use strong passwords
- Keep anti virus running and up to date
- Patch your Operating System
- Use Anti-spyware software
- Surf wisely
- Don't get hooked by phishing
- Be careful of downloads
- Log on as user not administrator
- Take the time to understand what you need to do to protect your computer system and data

Other Measures to Consider

- Keep a list of all credit cards numbers and the numbers to call to report them if sold or missing.



How to detect if you've been a victim

Be alert to signs that require immediate attention:

- Bills that do not arrive as expected
- Unexpected credit cards or account statements
- Denials of credit for no apparent reason
- Calls or letters about purchases you did not make

What to do if you are a victim

- Place a "Fraud Alert" on your credit reports
- Close suspect accounts
- Use the FTC's ID Theft Affidavit
- Keep Documentation about conversations
- File a police report with local Law Enforcement
- Report the theft to FTC
 - Online at Ftc.gov/idtheft
 - By phone 1-877-ID-THEFT (438-4338)
 - By mail