

IDENTITY THEFT & PREVENTION



Bucknell University
Department of Public Safety

Identity Theft

Learning Objectives

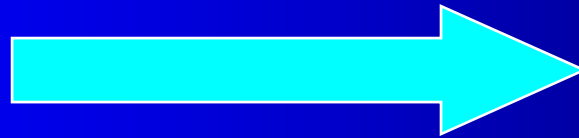
- What is it?
- How pervasive is it?
- How does it occur?
- How potentially devastating it can be?
- How do we detect fraud?
- How can we minimize the risk of being victimized?

Examples

- **Federal Government is Even Susceptible**
 - Department of Veteran's Affairs has stolen computers that contained over 500,000 Social Security numbers
- **Identity Theft Case Exposes Threat of Insider Theft**
 - Credit Card Account verification service realizes internal fraud has resulted in 250,000 compromised credit cards/identities
- **Susquehanna Valley Hit By Credit Card Breach**
 - 10's of thousands notified their Credit Cards were accessed illegally
- **Major fraud and hacking stories appearing weekly**

Victims Per Year

2007



7.8 million

2008



10 million

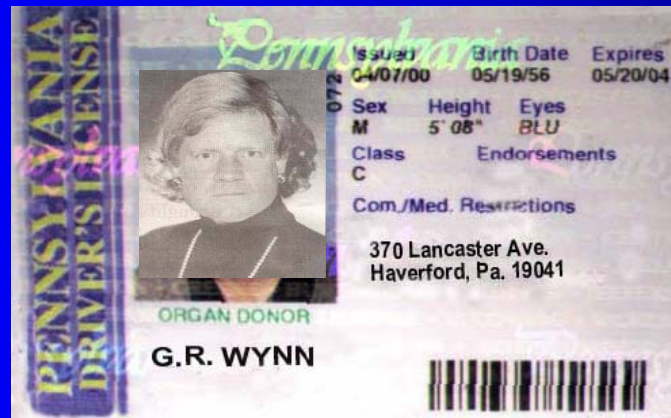


Cost Per Year

- FTC information release:
 - 4.5 million Victims found that a new account was opened in the past year.
 - 46 million total Victims in the last 5 years.
 - An average of 200 hours per person is used to reclaim identity at a cost of \$500.00 / person.

What is Identity Theft?

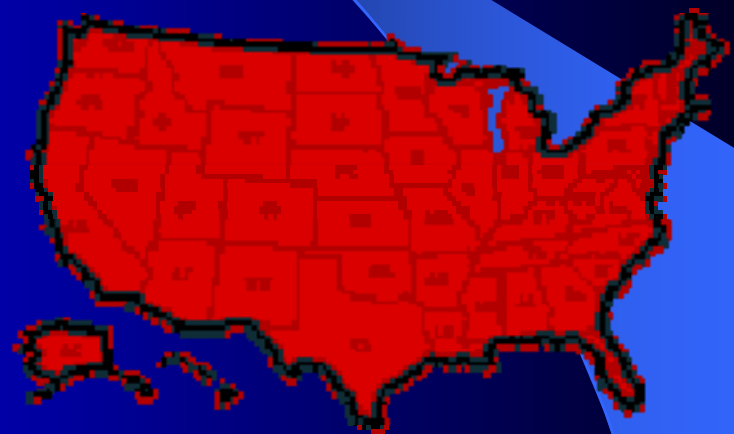
- Personal information



- Account information
- Legal history
- Anything that contains past information

What is Identity Theft?

- Acquiring key pieces of someone's identifying information in order to impersonate them
 - **Name**
 - **Address**
 - **Date of Birth**
 - **SSN**
 - **Credit Card numbers**
 - **Passport & Drivers License**
 - **Maiden names (you and parents)**
 - **Other personal information**



Identity Theft

Take over financial accounts

- Open new bank accounts
- Applying for loans
- Applying for credit cards
- Applying for social security benefits
- Purchase automobiles
- Renting apartments
- Establishing services with utility and phone companies

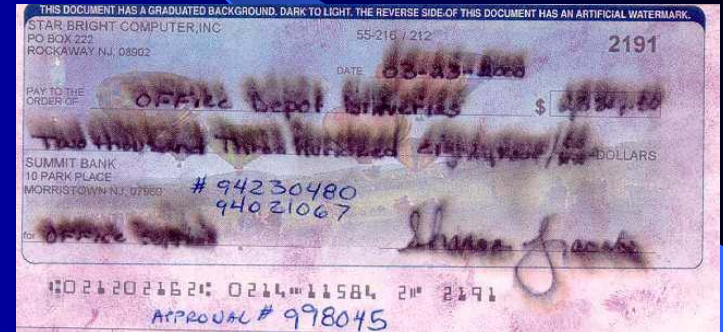


How is it done?

- A combination of low & high-tech methods
 - Low-tech
 - Shoulder surfing at ATMs
 - Theft
 - Wallet – steal wallets and purses
 - Mail
 - Complete a change of address form to divert your mail
 - Dumpster diving
 - Obtain information from the workplace

How is it done?

- High-tech
 - Inside source (at credit card company or bank)
- Checks
 - Check washing
 - Check creation software
- Fraudulently obtain your credit report
- **Phishing *****
- **Pharming *****



What is PHISHING?

PHISHING VIDEO

What is Pharming

- **Pharming** (pronounced farming) is a hacker's attack aiming to redirect a website's traffic to another, bogus website.

The background is a dark blue gradient. A thin, light blue curved line starts from the top left and arcs towards the right. A light blue wedge-shaped area is located on the right side, pointing towards the center.

Deter.

Detect.

Defend.

How many people in this room go
to a restaurant and use a credit
card?

- [Credit Card ID Theft Scheme](#) Video

Credit Cards, Be Careful !

- Restaurant ID Theft Video

Deter.

- The Essentials...the minimums
 - Do not put mail in you mailbox overnight
 - Promptly remove mail from your mail box
 - Cancel mail when going away for more that two business days
 - Never give personal information over the internet or telephone unless you initiated the call
 - Keep items with personal identification (Social Security cards, Birth Cert., Passports, unused Credit Cards, etc.) in a home safe or safe deposit bank box
 - Beware of mail or telephone solicitations offering instant prizes designed solely to obtain your personal information or credit card numbers (do not call list)

Deter.

- The Basics...
 - Keep wallet or purse locked away
 - In your vehicle put them in trunk or glove compartment
 - At home keep them in your bedroom
 - Photocopy the contents of your wallet (put in safe)
 - Empty your wallet/purse of unused cards and Id's
 - NEVER carry your Social Security card
 - Sign all new credit cards upon receipt
 - If a new credit card does not arrived in a timely manner, call the bank or credit card company involved
 - Know your expiration dates
 - Contact issuer if replacements are not received promptly

Detect.

- Constant Vigilance...
 - Reconcile your monthly bank and credit card accounts
 - notify your bank about any discrepancies right away
 - Report any unauthorized transactions to:
 - Bank, and credit card company
 - Credit reporting agencies (Experian, Equifax, TransUnion)
 - The Police and FTC (police **must** take a report and provide you with a packet of information)
 - Report all lost or stolen credit cards immediately
 - Notify bank, credit company, eBay, PayPal... about Phishing and/or pharming. Most times they do not know it is occurring

Defend.

- The Shredder...is your new best friend
 - Rule #1 – when in doubt Shred it!
 - Shred pre-approved credit card applications, credit card receipts,
 - Bills and other financial information past seven years
 - Shred your old credit cards, media Id's and anything with a magnetic strip on back
 - *Never throw away ATM Receipts, credit statements, bank statements... Shred 'em!*

Defend.

- Yearly follow-through
 - Order copies of your credit reports
 - Experian, Equifax, TransUnion, must provide a copy free once a year
 - Notify the credit bureau in writing of questionable entries and follow through until they are explained or removed

Credit Reports/ Reporting Fraud

Who to contact:

- Security/Police

- Also;

Equifax

P.O. Box 105873

Atlanta, GA 30348-5873

www.equifax.com

TransUnion

P.O. Box 390

Springfield, PA 19064-0390

www.tuc.com

Experian Information Solutions

(Formerly TRW)

P.O. Box 949

Allen, TX 75013-0949

www.experian.com

Internet and Online Services

- Make sure you receive a secured authentication key from your provider (example on next page)
- When you subscribe to an on-line service, you may be asked to give credit card information
 - When you enter an interactive service site, beware of con artists who may ask you to “confirm” your enrollment service by disclosing passwords or the credit card account number you used to subscribe
- Always “logout” after a session. This prevents usage by another on your computer or through your computer by another
- Obtain “Single use” credit card number for online purchase (available from select companies)



Service1st@Home

- ◆ If you have forgotten your username, please contact us at 1-800-562-6049 during regular business hours.
- ◆ If this is your first logon, you need to have requested an access code. If you requested an access code on your membership application, please use that code. Else, you can contact us during regular business hours or complete the printable form and mail it to us.
- ◆ Access codes are case-sensitive and can range from 4 to 20 letters and numbers.
- ◆ Browser Requirement: Internet Explorer 4 or above, Netscape Navigator 6 or above, Mozilla Firefox 1 or above.
- ◆ Javascript and Cookies must be enabled
- ◆ Secure connection using 128-bit encryption
- ◆ Pop-up blocker must be disabled

Your account has been secured.
[CLOSE](#)

[Restart Session](#)



Page Info

General Forms Links Media Security

Web Site Identity Verified

The web site www.service1-home.org supports authentication for the page you are viewing. The identity of this web site has been verified by VeriSign Trust Network, a certificate authority you trust for this purpose.

[View](#) View the security certificate that verifies this web site's identity.

Connection Encrypted: High-grade Encryption (RC4 128 bit)

The page you are viewing was encrypted before being transmitted over the Internet. Encryption makes it very difficult for unauthorized people to view information traveling between computers. It is therefore very unlikely that anyone read this page as it traveled across the network.

into Intuit Quicken, please

Certificate Viewer: "www.service1-home.org"

General Details

This certificate has been verified for the following uses:

- SSL Server Certificate
- SSL Server with Step-up

Issued To

Common Name (CN)	www.service1-home.org
Organization (O)	Service 1st Federal Credit Union
Organizational Unit (OU)	Service 1st Federal Credit Union
Serial Number	7E:40:01:2C:69:C5:F2:D9:8C:07:25:B3:BB:EB:4F:13

Issued By

Common Name (CN)	<Not Part Of Certificate>
Organization (O)	VeriSign Trust Network
Organizational Unit (OU)	VeriSign, Inc.

Validity

Issued On	5/30/2007
Expires On	6/2/2009

Fingerprints

SHA1 Fingerprint	CE:E3:DA:C6:30:A9:CB:D1:64:71:8D:F6:72:7D:9A:02:E5:03:AD:83
MD5 Fingerprint	9D:5F:5D:F8:C1:7E:81:88:26:99:A9:41:34:47:D7:14

Close

Look Here



Resources

- The Federal Trade Commission operates an extensive website at: **www.consumer.gov/idtheft**
- The FTC Identity Theft Hotline is:
(877) IDTHEFT (483-4338)

By mail at: **Identity Theft Clearinghouse**

Federal Trade Commission

600 Pennsylvania Avenue, NW

Washington, DC 20580

- **www.bankersonline.com/infovault/infovault.html**
- Local and State Police Departments
- Bucknell University Public Safety

What your packet contains:

- You packet contains Identity Theft Prevention Tips.
- Web sites and contact information for identity theft prevention and the steps to take if you are a victim of Identity Theft.
- And a sample letter of request for a credit report.

Thank You ! Questions?



Jeffrey Ettinger

Detective of Bucknell University Public Safety

570-577-3333

jettinge@bucknell.edu