

ID Theft – It Could Happen to You

Provided courtesy of Capital Credit Union
November 2007

Did you ever see the commercial where an older lady is cleaning her pool and starts talking in a man's voice? After listing all the things she got for "free" using a stolen credit card, she lets out a horrific laugh. While it might seem like just another quirky commercial about how someone could steal an identity from *someone else, somewhere*, the fact is, that it could happen to YOU!



Identity theft is when someone steals information like your Social Security Number, birth date, address, your credit union, bank or credit card account numbers, or other personal information and uses it for their financial gain to pay for things like food, clothing, stereo equipment, and almost anything else. Medical identity theft has become more widespread too, where thieves steal information about medical records and insurance and impersonate the victim in order to seek and fraudulently pay for medical care.

ID Theft Statistics

Source: sonicwall.com

- The Federal Trade commission estimates that **10 million Americans** are victims of identity theft each year
- 6.1 billion phishing emails are sent world-wide each month (Anti-Phishing Work Group – APWG)
- \$1,200 is the average loss per person who is successfully “phished” (Federal Trade Commission)
- 15,451 unique phishing attacks in January 2006 (APWG)
- 7,484 phishing web sites found in January 2006 (APWG)

Two Types of Identity Theft

1. **Account takeovers** – When the ID thief uses your existing account numbers to access your bank accounts and credit cards in order to fraudulently purchase merchandise and services.
2. **True name fraud** – When the ID thief uses your personal information to establish new accounts in your name, including credit cards, bank accounts, loans, utilities, etc., and uses them to make purchases of services or goods.

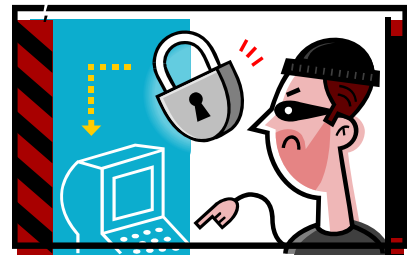
What does it take for someone to steal your identity?

All a thief needs is some basic information about you, like your Social Security Number, your driver's license number, your checking account or credit card information, or your phone

number. In many cases, just typing a phone number into an online search engine, can give the searcher your name, address and even a map to your house.

Some of the ways identity thieves may use to get your personal information:

- Steal your mail, including pre-approved credit card offers, tax information, and other documents with account numbers on them.
- “Dumpster diving,” rummaging through your trash or the trash of businesses.
- Steal your wallet or purse.
- Steal information from your computer (keylogging).
- Solicit information from you by phone or email by posing as someone from a legitimate company, financial institution or survey company (known as “phishing” online and “pretexting” by telephone). For Example:
 - “Do you want to be a mystery shopper? All we need is your birth date and Social Security Number for our records.”
 - “Congratulations! You won our sweepstakes, but we need your Social Security Number to complete our records ...”
 - “We’re currently doing an audit of [Credit Card company or financial institution], and we need to verify your account number and information...”
 - “I’m from [Credit Card Company] and I’d like to offer you a lower rate on your credit card. However, I’ll need just a little more information for our files ...”

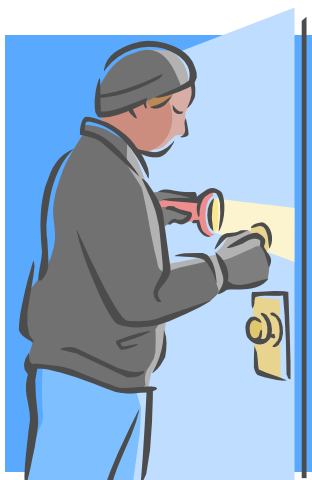


Protecting yourself from Identity Theft (General Tips)

- Don’t carry your Social Security Card with you.
- When asked for your Social Security Number, Driver’s license number or even your phone number, always ask why it is needed and how it will be used. Generally speaking, the only time you need to give out your Social Security Number is for a passport or for some insurance applications. If your Social Security Number is listed as part of an account number, ask to have it changed.
- Don’t print your Social Security Number, Driver’s License Number or your phone number on your checks.
- Shred any documents with account numbers or other personal information on them BEFORE throwing them in the trash.
- Don’t share your passwords or personal identification numbers (PINs) with anyone, even good friends or relatives.
- When using an automated teller machine (ATM) be aware of your surroundings and don’t enter your PIN if someone is watching.
- Carefully look over your checking account and credit card statements to verify that there are no unauthorized charges.
- Check your credit report at least once a year. You are entitled to a free credit report annually from each of the three major credit reporting agencies at annualcreditreport.com. It’s a good idea to spread your requests out (January, May, and September) so that you always have current credit report information.

- Unsolicited, bogus emails that can look legitimate, and may even use some real facts to throw you off. Never respond to an unsolicited email that asks you to call or visit a web site to enter your credit card number, three-digit code from the back of your card, or PINs or account numbers. If you do receive such an email or phone call, be sure to contact your credit union or other financial immediately, using the phone number you have on file (not the phone number listed on the email or letter).

Protecting yourself from Online Identity Theft



- Don't use your Social Security Number or your mother's maiden name as a PIN or password.
- Never reply to an email regarding your account numbers, Social Security Number, name and address, or any other personal information.
- Don't open or reply to suspicious emails from unfamiliar senders—delete them immediately.
- When ordering or doing account transactions online, look for the "https" in the address bar which indicates a secure connection.
- Always look for and click on the "lock" icon on a web site's status bar to verify that it is secure.
- Use strong passwords and change them often. Make sure they're at least eight characters long, combining numbers, symbols, and upper and lower-case letters.
- Install a good anti-virus software and firewall (like Norton or McAfee) on your computer, and keep them up to date.

To get your FREE credit report

Go to annualcreditreport.com, or call 1-877-322-8228 to request the information by phone or to request that a copy of your report be mailed to you.

AnnualCreditReport.com is a centralized service for consumers to request free annual credit reports. It was created by the three nationwide consumer credit reporting companies - Equifax, Experian and TransUnion.

AnnualCreditReport.com provides consumers with the secure means to request and obtain a free credit report once every 12 months from each of the three nationwide consumer credit reporting companies in accordance with the Fair and Accurate Credit Transactions Act (FACT Act).

Important note about free credit reports: One of the well advertised sites to get your "free" credit report is freecreditreport.com. However, when you order your reports from that site, you are automatically entered to begin a 30-day trial membership to a credit monitoring service. And unless you cancel the subscription, you will be billed a fee for the service each month until you request to stop it.



Internet ID Theft Terms

Phishing – *Fraudulent emails claiming to be from a financial institution or credit card company.* The email usually directs you to a spoofed, yet authentic-looking website where you are asked to fill in account numbers, card numbers, PIN numbers, and other sensitive information to supposedly keep your account current.

The newest “phishing” scam includes an email that asks you to respond to an “online customer satisfaction survey,” offering cash rewards for answering questions that include information like credit card numbers, the three digit security number on the back of the card, Social Security Number, and other personal/financial details.

Pharming – *Emails that appear to be from someone you know, but which are actually from a hacker hoping to pull information from your computer.* Be sure to check all the “FROM” lines in your emails, and if any of the senders seem suspicious, DO NOT open it—delete it immediately.

Keylogging – *Once you open a “pharming” email, keyloggers can get into your computer and remotely track each key stroke you make.* This gives them unlimited, easy access to your personal information, account numbers, and anything else you type on your computer keyboard.

Vishing – Where someone calls and asks you to verify account information by calling a toll-free number instead of clicking on a Web link, but that phone number belongs to a crook who collects the personal information you punch onto the keypad.

SMiShing – Phishing via SMS, or short message service. It’s targeted at mobile phone users who use text messaging. One of the first known SMiShing attacks involved the following text message: "We're confirming you've signed up for our dating service. You will be charged \$2 a day unless you cancel your order." The message included a Web link that routes you to the main phishing page, where you're prompted to download a program—a Trojan horse that turns your computer into a zombie controlled by hackers and used within a larger network to steal personal account information and perform other malicious activities (*Computerweekly.com* Sept. 6, 2006).

Identity Theft Quizzes

ID Theft Face Off – Game by the Federal Trade Commission
http://onguardonline.gov/quiz/idtheft_quiz.html

Interactive Identity Theft Quiz (Privacy Rights Clearinghouse)
<http://www.privacyrights.org/ITquiz-interactive.htm>

Phishing IQ Test
<http://sonicwall.com/phishing>

