

Preventing Identity Theft

By

George Bourrie

February 7, 2011

Preventing Identity Theft

- There are many ways that your personal information may be accessed by people who shouldn't have it:
- Off of a computer, there is tossing information in the trash, revealing too much to unknown callers on the telephone, putting the flag up on your mailbox to indicate mail to go, etc.

Preventing Identity Theft

- On a computer, some of these are not having adequate firewall, anti-virus, and anti-spyware software running, choosing guessable passwords, revealing too much on social sites, using public networks to transmit personal data, installing software from unknown sources, and succumbing to e-mail scams.
- At this presentation, tactics for dealing with these will be discussed.

What is your ID information?

- Your ID information includes your:
- Name
- Address
- Date of Birth
- Social Security Number
- Mother's Maiden Name
- Bank or other Financial Account Numbers
- User Names, Passwords and PINs (Personal Identification Number)

OFF the Computer

- Shred all papers with any ID information on them to prevent “Dumpster Diving”.
- Don’t leave papers with ID information on them, such as bank receipts, in your car.
- Don’t give or “verify” personal information over the phone to strangers or unsolicited callers.
- Do not put outgoing mail in a mailbox; the flag up tells thieves there is mail to steal.
- If possible, use a locked mailbox to discourage mail theft.
- Arrange for direct deposit of checks and automatic payment of bills.

OFF the Computer

- Do not leave a purse or wallet out of your sight in a public place, even at your workplace. Put a picture of a baby in your wallet; studies have shown it encourages people finding your wallet to return it.
- Do not write passwords or PIN numbers on papers, and especially do not carry such papers on your person or next to your computer at work or home.

OFF the Computer

- Watch that someone behind you in a checkout or ATM line could be taking photos of your cards using a phone camera.
- Be wary of a check that looks legitimate (e.g., government grant or lottery) but requires a “finder’s fee” or administrative cost to be paid by you; the check will eventually bounce but you will have already paid the sender the fee.

OFF the Computer

Debit Cards

- Be careful of Debit Cards: a stolen one can be used as a credit card by using a signature rather than a PIN but your losses are not limited to \$50 as with a credit card; repeated use can clean out an account and you might even be responsible for overdraft charges.
- If your bank issued you a combined ATM/Debit Card and you don't need the Debit Card, ask them to exchange it for an ATM-only card; the ATM card can only be used with your PIN.

OFF the Computer

Credit Cards

- If available, get a Credit Card that allows your picture to be put on it.
- If you have a newer credit card with an embedded RFID (Radio Frequency ID) chip, put the card in a protective sleeve to prevent it being read by a nearby thief with a scanner.

OFF the Computer

Skimmers

- Watch for “card skimmers” at ATMs or gas stations; they are hardware added to the front of the card reader to steal your card number; jiggle a suspected one to see if it will come off. Hide your entry of a PIN from a possible snooping camera installed with the skimmer.
- At the gas pump, use a Credit card or choose CREDIT when using your debit card so you don't need to use your PIN, or pay inside the station, where there is less chance of a skimmer at the register.

OFF the Computer

Check Your Balances

- Check your bank and credit-card balances several times a month and your statements to catch discrepancies or suspicious activity.

OFF the Computer

Social Security Number

- Your Social Security Number is very valuable to an ID thief; protect it.
- Do not put Social Security number(s) on checks.
- Question why a company that asks for it actually needs it; if only for identification, try to use something else.
- Don't carry your Social Security card.
- Don't carry your MEDICARE card except when you need it to show it to a Health Professional. Instead, carry a photocopy with the last four digits blanked out; you can supply them when necessary.

OFF the Computer

Protecting Your Credit

- There are three Credit Reporting Bureaus: Experian, Equifax, and Trans Union. They keep track of your credit history. When you are trying to open a new credit card account, get a job, buy a car, or house, or rent, or engage in a similar major financial activity, the bank, mortgage company, etc. checks your credit first by checking with one or more of these bureaus.
- You can protect your credit by limiting access at the Credit Bureaus with a Fraud Alert or Security Freeze.

OFF the Computer

Protecting Your Credit

- Fraud alerts: companies checking your credit get an alert that they need to take extra precautions because there is an increased risk that a fraud is being perpetrated. You can provide a telephone number for them to contact you first before granting credit. Initial fraud alerts are available for free if you believe you have been or are about to be an ID theft victim. They do delay the credit process.

OFF the Computer

Protecting Your Credit

- A Security Freeze is a preemptive act: you prevent the credit reporting bureaus from giving your file to anyone without your direct authorization. To do this, you must write a letter (samples are on their websites), pay a fee (\$10) and send via certified mail.

OFF the Computer

Security Freeze

- According to Experian:
- “Security freezes are designed to prevent a credit reporting company from releasing your credit report without your consent. However, you should be aware that using a security freeze to take control over who is allowed access to the personal and financial information in your file may delay, interfere with or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, insurance, government services or payments, rental housing, employment, investment, license, cellular telephone, utilities, digital signature, Internet credit card transaction or other services, including an extension of credit at point of sale.”

OFF the Computer

Security Freeze - continued

- “When you place a security freeze on your file, you will be provided a personal identification number or password to use if you choose to remove the security freeze from your file or authorize the temporary release of your credit report for a specific person or period after the security freeze is in place.”

OFF the Computer

Security Freeze - continued

- Again, according to Experian:
- “To provide that authorization [for release of your report], you must contact the reporting agency and provide all the following:
 - 1) Sufficient identification to verify your identity.
 - 2) Your personal identification number or password provided by the credit reporting company.

OFF the Computer

Security Freeze - continued

“3) A statement that you choose to remove the security freeze from your file or that you authorize the reporting agency to temporarily release your consumer report. If you authorize the temporary release of your consumer report, you must name the person who is to receive your consumer report or the period for which your consumer report must be available.”

OFF the Computer

Credit Monitoring

- For a monthly fee, you can sign up at one of the bureaus to have all three reports monitored, get immediate access to your reports and scores, be able to lock and unlock access to your file at that bureau, and get notified when there is a critical change to any of the three reports.
- For more information, go to their websites:
www.experian.com
www.equifax.com
www.transunion.com

OFF the Computer

Free Credit Reports

- By law, you are entitled to a free credit file disclosure, commonly called a credit report, once every 12 months from each of the bureaus. There is a website where you can get these reports:

www.annualcreditreport.com

- You can space out the requests through the year so you can request a report first from one bureau, followed by a report from another 4 months later, and a report from the third bureau 4 months after that.

OFF the Computer

Free Credit Reports

- There are other companies that try to con you into thinking you can do the same through their sites; this is the one that is truly free.
- On the site, you will also find a phone number, 1-877-322-8228, and a form and address for requesting the reports by mail if you prefer.

OFF the Computer

Removing Yourself from Marketing Lists

- Remove yourself from marketing lists for preapproved” credit card and insurance offers, which could be stolen by mail thieves or dumpster divers, by contacting each of the three credit reporting bureaus or calling.
- 1-888-5-OPTOUT

OFF the Computer

Companies Offering ID services

- Some companies offer services promising to protect you from ID theft; they may just be offering to put a fraud alert or freeze on your reports.
- Companies offering to rebuild your identity sometimes get a limited power of attorney from you to let them work on your behalf with bureaus, creditors, and other information sources.

OFF the Computer

Reporting an ID Theft

- If your ID is stolen:
 - 1) Report it to the police
 - 2) Report it to all three credit report bureaus to put a fraud alert on your account
 - 3) Close the compromised account
 - 4) File a complaint with the FTC (26% of complaints are for ID theft).

ON the Computer

Software Barriers

- Use Firewalls, Anti-Virus, and Anti-spyware software and keep operating system, and web browser(s) up to date. Use pop-up blockers (within many packages) that require you to agree to a pop-up before showing it.

ON the Computer

Routers

- Use a hardware firewall, i.e., router, as well.
- If using wireless, use encryption at the router such as WEP (very weak) or WPA. In addition, don't broadcast your SSID (the public name of your wireless network), and restrict access to only those devices whose MAC addresses you authorize. This is all done through the router menus, which are initially accessible only through hardwired access, i.e., using an Ethernet cable between a computer and the router.

ON the Computer

Passwords

- Use strong passwords that are not guessable (10 characters or more, preferably with a mixture of upper and lower case and other characters). Try the first letters of a phrase or a word backwards, etc.
- Use different passwords on different sites; keep passwords in a password-protected virtual-safe program, like “Passwords Plus” or “Keepass”.

ON the Computer

E-mails

- Don't use words that are easy for someone to find or guess, like your mother's maiden name, for passwords or password hints. Choose hints that only you would know the answer to. Use hint answers that are wrong but that you'll remember.
- In Outlook and similar e-mail handlers, don't look at messages in the Preview Pane; that could be enough to let malware in.
- Watch what you click – “If it's too good to be true,...”. Don't open attachments from strangers or links in their e-mail messages.

ON the Computer

E-mails - continued

- Don't automatically display images in e-mails; sometimes malware is embedded in them
- You can choose to read e-mails in plain text rather than HTML to be safer.
- When you install software, be careful of which boxes may be checked by default; they may permit third parties to send you e-mails.
- Be cautious of something that is free from somewhere you don't know; e.g., games; it could be a source of spyware.

ON the Computer

E-mails - continued

- Be aware of latest scams; like “The Stranded Traveler”: you receive an e-mail, apparently from an acquaintance, that they are abroad and have been mugged and need you to send them money.
- Before getting panicked when you receive a report of a new virus, etc., check www.snopes.com for “the definitive Internet reference source for urban legends, folklore, myths, rumors, and misinformation”.

ON the Computer

E-mails - continued

- Use alternate free e-mail accounts with different names. You can then provide one of these accounts when you are registering software, or signing up on a website. Just be sure to check them one in a while to see if you have any important messages such as update notices.
- Likewise, use an alternate identity for casual web surfing.

ON the Computer

E-mails - continued

- “Phishing”: Beware of e-mails asking for information to validate an account; they appear to be from banks, credit card companies, mortgage brokers, internet service providers, etc. but the real companies do not do this.
- Go to the sites directly rather than clicking on the link. If you don't know the correct address, do a search for the company using a search engine like Google or Bing.

ON the Computer

Be Site Savvy – continued

- When shopping or engaging in any other financial activity online, ensure that the internet connection is secure; look for the little lock.
- For on-line purchases, use a Credit Card reserved for the purpose; it's easier to determine if there are illegitimate charges.
- Sites requiring the three-digit security code when you use a Credit Card provide enhanced protection, preventing someone who just knows your Credit Card number but doesn't have the physical card from using it.

ON the Computer

Be Site Savvy - continued

- Another payment alternative is to use PayPal (www.paypal.com). You pay for your purchase without sharing your financial information; the retailer never sees your bank or card numbers. To pay, you are taken to your PayPal account to authorize the payment from your registered bank account, debit card, or credit card as the payment source.
- Avoid file-sharing and dangerous sites. Shop only on secure sites, preferably ones you know.

ON the Computer

Be Site Savvy - continued

- Don't blindly follow a link to get to a site; enter the address yourself. Check that you have typed in the site address exactly; phony sites that look legitimate could come up if you make an error.
- Do not deal with shopping sites that do not have a phone number listed.

ON the Computer

Be Site Savvy - continued

- Be wary of requests to download a codec (coder/decoder software) or other software to permit an activity, like viewing a video, on a site that you do not know.
- To close a window that has popped up unsolicited, click on the X, not on “Agree” or “Okay” or “Close”.

ON the Computer

Be Site Savvy - continued

- Don't believe any popup message that your computer is infected with malware and that presents you with a link to software that will clean it. When you get such a message, use Task Manager (CTRL-ALT-DEL) to kill the browser by killing the browser process, e.g., iexplore.exe for Internet Explorer, and do not reload the pages when the browser is restarted.

ON the Computer

Be Site Savvy - continued

- “Ransomware”: a demand for a payment to be wired to obtain a code or for you to purchase software in order to release your computer from the disabling of an essential system service or the encryption of your personal files.
- Don’t pay; instead restore the system to a prior state using System Restore (click Start and type System Restore in the search window). If that fails, restart the computer in safe mode (press F8 key during boot-up) and run your internet security software.

ON the Computer

Social Networks (like Facebook)

- Tweak account settings to minimize what strangers can find out; check periodically to determine if they've changed the rules.
- Take care what information you post; it could last forever and be used differently from what you intended. It could also tell someone your plans.
- Don't friend strangers.
- Be careful about games and quizzes; they might allow someone to access your ID data on that social site. First, read the fine print on the window that pops up when you are about to run the application.

ON the Computer

Protect your Computer's Data

- Set up an account on your PC which does not have administrative rights, and use that account when you are on the internet. Also, set up a guest account for others using it.
- If you take a laptop out of the house, password it so nobody else can operate it if it is lost or stolen. Don't forget the password! This is also true for flash drives with sensitive data.
- Be aware that data (including passwords) transmitted over a wi-fi connection in a public place could be captured. Do not do financial transactions there.

ON the Computer

Protect your Computer's Data

- To protect sensitive data on your computer, you can encrypt your files.
- Monitor your children's use of the computer. Teach them what you have learned about security and safety.
- When getting rid of an old computer or hard drive, wipe the hard drive; formatting won't prevent data from being retrieved. Use a free program like "Darik's Boot and Nuke" from CNET or ZDNET. To be really sure, physically destroy the drive.

Summary

In short, whether or not you are on the computer, keep thinking about making it as hard as possible for someone to get your ID information and steal from you.

Good luck!

Information Sources

Thanks to the following websites for being the source of the information used in this presentation:

AARP – www.aarp.org

Tech Republic – <http://techrepublic.com>

Reader's Digest – www.rd.com

Lavasoft – www.lavasoft.com

PCWorld – www.pcworld.com

Symantec – www.symantec.com

Hewlett Packard – www.hp.com

Information Sources - continued

The Philadelphia Inquirer –
<http://epaper/philly.com>

NitroPDF Software – www.nitropdf.com

Federal Trade Commission – www.ftc.gov

Experian – www.experian.com

MaximumPC – www.maximumpc.com