Identity Theft: Understanding and Prevention

What is identity theft? It is illegally obtaining private information, such as a person's credit card information, driver's license, social security information, bank account information, address (if not listed), or unlisted phone numbers. This information can be obtained through a person's personal or work computer, from documents retrieved from the garbage, from stolen documents, or through information given out verbally. In this article, I am going to discuss only identity theft in relation to your computer.

Here is an actual identity theft case: You receive an e-mail from someone claiming affiliation with the IRS asking you to provide information for an audit. You comply, since it seems like a legitimate request. They ask for personal information: your social security number, street address, bank account numbers, credit card numbers, date of birth, and telephone number. The e-mail letter has the IRS logo on it and looks official. But is it? Those people who provide their information are in for a rude awakening. They will find their credit card fraudulently charged, bank accounts drawn down, and other theft. This theft is on the rise according to Federal Trade Commission statistics. Once the thieves get your information, they can open accounts in your name, take out loans in your name, get a job using your name, or file fraudulent taxes in your name. Another example is you receive a phone call or email link or popup from Microsoft or an assumed Microsoft Partner that your computer is compromised with infections or license issues. They say they need to take remote control of your computer to remedy the problem. Instead of solving problems they are data mining your sensitive data info or trying to sell you a product or service that you do not need in order to generate revenue for themselves by holding you hostage. This is not Microsoft or its legitimate partners!

The following information is on the Federal Trade Commission's website at http://www.consumer.ftc.gov/features/feature-0014-identity-theft. I recommend you read this information thoroughly. It will change the way you do things and hopefully save you from identity theft. The most current scam alerts page is at http://www.consumer.ftc.gov/scam-alerts

What are the steps I can take to prevent identity theft?

- Shred all paper documents, and destroy old credit cards, CDs, and DVDs containing personal information before discarding them.
- When disposing of an old computer, make sure the hard drive is erased with a program such as Active@KillDisk. www.killdisk.com

Both free and professional versions are available for all operating systems. There are other programs available too. This is done so thoroughly that the data can never be retrieved. This process does not damage the hard drive, but wipes it clean. You can also physically destroy your hard drive with a hammer or strong magnet.

- Do not give out your social security number, PIN, or bank account numbers on the Internet. Credit card purchases are OK from online vendors you trust with well-known names, like Amazon, EBay, Walmart, etc.
- Always look for a VeriSign Secured label, or other verification of site privacy, like hacker-tested, BBB Reliability Program (Better Business Bureau Online), Trusted Commerce for online transactions, or Trusted Bank Sites for online banking that were originally set up through your bank.
- In case you did not know, the "*s*" in https:// means your connection is secured. It will appear on secure online banking web pages and other transaction sites. Unfortunately, no indicator is totally foolproof, and some sites have forged icons and security certificates.
- SSL Certificates secure all of your data as it is passed from your browser to the website's server. To get an SSL Certificate, the company must go through a validation process.
- Do not reply to e-mails that are too good to be true. Some examples: "You won $100,000 in a sweepstakes; we need all your personal information to process the check" or "Send us money and you'll receive something more in return."
- Make sure your computer is set up properly to begin with and get a thorough tune-up when needed. Make sure it is not infected with keyloggers, back-door Trojans, or other malware. It's your information, so take care of it.
- Use an Internet security software program, an antispyware-and-malware removal program, a firewall behind a router, and a Junk file removal program.
- Keep updates current for all programs. Hackers love security holes. Make sure automatic updates are turned on.
- Use strong passwords with letters and numbers. Use combined upper and lowercase letters, numerals, and symbols. A minimum of eight digits is a rule of thumb. Pick a password that someone else will not guess or is not easily available. With online passwords, users are generally locked out after three incorrect attempts, but policies do vary. Do not use your mother's maiden name, your date of birth, the digits of your social security number, your pet's name, consecutive numbers, your date of graduation, your children's names, your address, or anything someone might guess to protect sensitive data. Here is a strong password example (8@Tee!3Hx&)
- Make sure you initiate contact before giving information over the phone, in person, through the mail or on the computer. Always know the person or company before giving the information, or obtain a recommendation from someone you trust.
- The best policy is not to open files, programs, internet sites, or e-mails from people or companies you do not know. Delete Junk mail on a regular basis. Be careful with file sharing programs by knowing whom you share your information with.
- Copying machines with hard drives or other storage media can keep a record of all copies run through a machine, which is a security threat if those copies are not erased or disposed of properly. http://www.cbsnews.com/8301-18563_162-6412439.html
- Two-factor authentication (2FA) -- also known as two-step verification or multifactor authentication -- is widely used to add a layer of security to your online accounts. The most common form of two-factor authentication when logging into an account is the process of entering your password and then receiving a code via text on your phone that

you then need to enter. The second layer in two-factor authentication means a hacker or criminal individual would need to steal your password along with your phone in order to access your account.

- Encrypt, lock, hide, and password-protect personal files, folders, drives, USB flash drives, and other storage devices. Reviews for encryption software are at https://www.pcmag.com/article/347066/the-best-encryption-software. These programs are for sensitive data.
- Identity theft protection reviews and their prices can be found at http://www.nextadvisor.com/identity_theft_protection_services/compare.php. The listed top-rated services combine multiple types of monitoring, such as credit reports, bank accounts, medical records, public records, credit cards, and social security.

Identity theft is a serious problem. Taking the steps outlined above can help reduce or eliminate the chance that you will be a criminal's next target. Mark Wilcox at Mark Wilcox Computer Services Inc. can be reached at 218-735-8212 or 218-290-1339 or at markwilcox@wilcoxcomputerservicesinc.com His website is www.wilcoxcomputerservicesinc.com. Check Google Maps for Directions and Reviews.