

Simple Identity Theft Protection

Article by: Lyle Sharp

How many of you bank, shop, or transact other business online? There are at least 4 million Department of Defense employees that access their pay records online only. Even offline, stored financial data can be placed at risk in computers that are used on the Internet as well. As one of the fastest growing crimes in America, identity theft is a concern for everyone.

A criminal gaining access to your bank or credit card accounts or personal information can wreak havoc with your credit and leave you holding the bag. Protecting your personal data at home and online is not too painful and lowering your risk for a reasonable effort level is well worth it.

Before we tackle the computer and online environment, let's take a quick look at your other home risks. Your garbage can and mail box are prime targets for identity thieves. Bills, old checks, financial statements, credit offers, the list goes on. All of these documents need to be shredded with a crosscut shredder before discarding and mail should never be left in the mail box for long. Arrange for someone to pickup mail if you are going to be gone from your home for more than a day. In short, anything with your full name combined with any other sensitive information should be shredded before discarding.

Phishing and social engineering are methods to get you to divulge your data to a criminal by making you believe the criminal represents an organization or interest with access or rights to your information. Any phone call you receive from someone requesting your personal information or credit card numbers should be suspect. Request a way to call them back via the organization's published numbers and verify the number is associated with the organization before proceeding. Suspect good deals that come to you out of the blue via the telephone or any other method. If it sounds too good to be true, it probably is.

Now for your computer, there are a few things you should do here. Your online activities pose the greatest risk. You need a hardware, or good software firewall. You need good Anti-Virus and Anti-Spyware software. The software versions will need regular updates to keep ahead of the hackers out there.

You also need to take some precautions with your own personal online and offline habits. Online, you should use different, complex passwords for each identity related account you access. You should set your browser security settings as high as possible for general surfing and avoid clicking advertising links from unknown vendors, or links in emails that come from unknown senders or are out of character for the known sender. Never follow links sent via email purporting to be from your creditors or financial institutions asking you to validate your account information. Call them instead, if you believe it is valid. Most financial or credit organizations will never send you an email unless you have asked to receive account updates. The last thing you need to be aware of online is who you are doing business with. Be careful about providing your credit card numbers online. While ensuring the site is secure is absolutely the bare minimum, ensuring the vendor is honest and keeps your data secure is necessary too.

Offline, you should secure any financial, health, insurance, or other documents containing your personal information by using encryption and password protection. Most financial software packages have this feature built in. Use it as well as Windows encrypted folders to make your private data secure from undetected Spyware, or short term physical access to your computer by a criminal. Don't use Windows auto-logon features and always use complex passwords that are at least eight characters long, contain numbers, letters, and both upper and lower case. Never use a common word, name, or other easily guessed password. Something like T8\$f~lly can be easy to remember, though very hard to guess and extremely time consuming to hack. Finally, change all of your passwords frequently and use a secure password manager to keep them organized.

The last thing you need to do is monitor your accounts and credit. Keep an eye on your financial account activities and your credit record. If you notice something amiss, call the financial organization or credit reporting agency and report it, change your passwords and pat yourself on the back for catching it early.

My own Yahoo account was recently compromised. While this wasn't a costly identity theft situation, it did put my name on some rather unsavory low-level spam operations. A password change was all that was needed to shut down the activity.

Follow the directions I've provided and you will lower your risk of identity theft and fraud related debts to almost zero. Keep in mind that if you have Bill Gate's level of assets, you are in a different class of high risk targets and should hire a security team to manage those risks and lower your insurance rates. You can also call me and I'd be happy to help you put that together. ;-)

Lyle Sharp - President Advotech, LLC

A small to medium business IT services provider that specializes in affordable secure systems and practices.

<http://www.advotechllc.com>