August 16, 2013 Release # 228

-- Begin Transmission --

What You Need to Know to Avoid Identity Theft - Part 3

How Can You Protect Yourself

Watch out for Phishing Websites —A Phishing website is one that presents itself as a legitimate business website however in reality is a fake one looking for your information. Be vigilant if a site asks for a username and password, credit card number, bank account number, address and other personal information.

Shop only at Reputable Websites—While one of the reasons that the internet is so great is that you can find sites that sell about everything, how do you know that a company website is authentic and secure? You might check the website's SSL certificate which ensure secure transactions between web servers and browsers. The protocol uses a third party Certificate Authority (CA) to identify one end or both end of the transactions. The secure page is accessible via https protocol.

Unique Passwords for Every Website—Another method criminals may use to obtain your personal information is by logging into your email and other online accounts and glean information from there. That is the reason that it is so important to maintain password security across all of your online accounts. Generating a secure password is the first step to prevent identity theft by keeping your accounts secure.

Use an Anti-virus/Anti-Malware Program—When you are surfing the web, use a comprehensive security suite, such as Sophos Anti Virus software, which not only protects you against viruses, spyware, and other emerging threats, but also provides safe search technology to help you steer clear of fake websites that try to collect your information. In addition, make sure you use a firewall to block unauthorized access to your computer or network.

Practice safe surfing on public hotspots—If you are using a public computer or accessing the Internet from a public hotspot or an unsecured wireless connection, do not log in to banking and credit card sites. Do your surfing at home or on a secure network.

Review your financial statements promptly—Check your credit card and bank statements each month to make sure there are no fraudulent charges and to confirm that you authorized all transactions

Shred documents—The only way to keep thieves from digging up your personal information from the trash is to shred sensitive documents, such as financial statements, credit card offers, and expired identification cards.

Keep your documents safe—Put personal documents in a lockable drawer, safe, or cabinet at home, and consider storing valuable financial documents such as stock certificates at your bank.

Monitor credit history—Because it can take a long time to discover that you've become a victim of identity theft, you should monitor your credit history to see if there are accounts or delinquent payments of which you may be unaware. There are a number of websites that offer free access to your credit reports, as well as paid services that monitor your credit for you.

To be continued…

-- End of Transmission --

Information Security: It's a Shared Responsibility

REFERENCE(S): www.lifelock.com ; www.mcafee.com ; http://www.makeuseof.com