Trojans, Viruses, Phishing Scams, Oh My: Protecting Yourself from Malware & Fraud

Posted At : November 20, 2012 3:27 PM | Posted By : Julia Bernd - Staff Writer
Related Categories: Internet security

Perhaps you read our recent alert regarding a fraudulent e-mail circulating that was trying to get unsuspecting folks to supply their credit union account information. This is what is known as a phishing attempt. Unfortunately, these types of attacks are common in the financial industry. And the cyber criminals are getting smarter and smarter - fraud and identity theft cases are on the rise.

Fortunately, there are several simple things you can do right now to make yourself less vulnerable to these types of attacks.

1) **Update your software**. Software companies are constantly releasing updates to their operating systems and browsers. One of the primary reasons they do this is to provide "patches" for security threats that have been identified. **If you are running out of date software your computer is more susceptible to be infected by a virus or trojan**. If you haven't already, set up your operating system and browser to automatically update. Or check for updates regularly.

2) **Install anti-virus software, preferably with an anti-phishing component**. This is so important. Running a computer without anti-virus software is like driving a car without insurance. Eventually it's going to catch up with you. Paid anti-virus software like Norton 360 and BitDefender AntiVirus Plus are going to offer you the most comprehensive protection. However, if you can't afford those versions, there is high-quality, free anti-virus software available for download on the web. Here are some of the heavy-hitters:

AVG Antivirus
avast! Antivirus
Microsoft Security Essentials
MacScan

3) **Download a safe-browsing add-on** for your browser. Add-ons like **WOT** are available for all popular browsers including Microsoft Internet Explorer, Mozilla Firefox, Google Chrome and Apple Safari. WOT will place color-coded reputation symbols on links in search engine results, social media, online email, and many popular sites to show how much other users trust a site. Ratings are based on information from millions of users and trusted third-party sources. Installing an add-on of this sort will help you decide whether or not a link in your

e-mail is safe and help protect you from a phishing scam, for example.

4) Speaking of phishing scams, **keep in mind that your financial institution will never ask you to provide or "update" information like your account number via e-mail.** If you receive an e-mail of this sort, delete it. Cyber criminals have gotten very good at making an e-mail look as though it's coming from your financial institution. If it asks for your account information, no matter how legitimate it may seem, delete it.

5) Lastly, simply **be mindful of your web activity**. Try to only visit sites you trust and pay attention to what you're clicking on and downloading. If something seems "off", don't proceed. Use your gut instinct. Often sites that contain free downloads, games, etc. are fraught with malware. Be especially careful when using peer-to-peer sharing sites.

Following these tips will help ensure a safe online experience. Happy surfing!