Online Fraud Prevention

Protect Your Business From Online Fraud

Source Materials:

The definitions of spyware and malware, as well as online protection tips, came from OnGuard Online, http://www.onguardonline. gov/#. OnGuard Online provides practical tips from the federal government and technology industry. Additional source material – and a great source for protection against identity theft – came from the Federal Trade Commission, http://www.ftc.gov/bcp/edu/ microsites/idtheft/.

Protect Your Computer

For many of us, the mere notion of conducting everyday business activities without using the Internet seems implausible. We've become so accustomed to its convenience and speed that our reliance upon the powerful combination of the World Wide Web and the personal computer has never been greater. Internet surveys report that nearly forty-five percent of American adults pay bills online and an increasing number of business owners use Web-based tools to process payroll.

Unfortunately, Internet fraud has also increased. According to spamlaws.com, the Federal Bureau of Investigation estimates that one million personal computers in America have been compromised; yet too often business owners neglect the single most important means of protecting their company's computers from online identity theft and fraud: installation of anti-virus/anti-spyware software along with a security firewall.

This oversight, however, can be quickly corrected.

Spyware & Malware

Information technology (IT) experts recommend that business owners check their computers to ensure: 1) that anti-virus software has been properly installed and 2) that anti-spyware is a component of that protection. IT experts warn that neglecting to install anti-virus software is akin to leaving the front door of your business unlocked and propped open: you're simply inviting theft and mayhem.

Anti-virus software serves to protect your computer against two particular malicious types of software infiltration: spyware and malware. So what exactly are spyware and malware?

Spyware is software installed on your computer without your consent that monitors ("spies") on your computer activities. It may be used to redirect your computer to Web sites, observe your Internet habits, or record your keystrokes, which, in turn, could lead to identity theft. Malware, short for "malicious software," includes viruses and spyware designed to steal personal information, send spam, and commit fraud. Online criminals create appealing Web sites, desirable downloads, and compelling stories to lure you to links that will download malware – especially on computers that don't use adequate security software.

Protection Tips

Short of tossing your computer out the door and vowing to never use the Internet again (which really isn't an effective solution, no matter how tempting the thought), here are a few online security and identity theft protection tips provided by OnGuard Online:

- Update your operating system and Web browser software. Your operating system (like Windows or Linux) may offer free software "patches" to close holes in the system that spyware could exploit. Set your operating system and security software to update automatically to be sure you have the latest protections.

- Use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly. You can download this software from Internet Service Providers or software companies, or buy it in retail stores. Look for anti-virus and anti-spyware software that removes or quarantines viruses and that updates automatically on a daily basis.

- Download free software only from sites you know and trust. It can be appealing to download free games, file-sharing programs, or customized toolbars. Be aware, however, that some of these free software applications bundle other software, including spyware. If you share a computer with children, talk with them about safe computing.

- Don't install any software without knowing exactly what it is. Take the time to read the end-user license agreement (EULA) before downloading any software. If the EULA is hard to find — or difficult to understand, think twice about installing the software.

- Minimize "drive-by" downloads. Make sure your browser security setting is high enough to detect unauthorized downloads; for example, set to at least the "Medium" setting for Internet Explorer.

- Don't click on any links within pop-ups. If you do, you may install spyware on your computer. Instead, close pop-up windows by clicking on the "X" icon in the title bar.

- Don't click on links in spam or pop-ups that claim to offer anti-spyware software. Some software offered in spam or pop-ups actually installs spyware. In fact, ads that claim to have scanned your computer and detected malware are a tactic scammers have used to spread malware, so resist the urge to respond or click on those messages.

- Install a personal firewall to stop uninvited users from accessing your computer. A firewall blocks unauthorized access to your computer and will alert you if spyware is already on your computer and sending information out.

- Back up your data. Whether it's text files or photos that are important to you, back up any data that you'd want to keep in case of a computer crash. Do this as regularly as you update your security software.

Finally, if you simply don't have the time or inclination to personally tackle online security make sure to enlist the help of an expert. Many local firms provide IT assistance. Ask a colleague or business associate who they use as an IT resource or contact the local chamber of commerce for a referral.

The Internet, like any other form of technology, can be both a help and hindrance. And while all online security issues may not be stopped by the use of anti-virus software, it only makes sense to protect yourself from those who would do you wrong.