

# Fight online identity theft with smarts, firewall

By JEFF WEBER • STAFF WRITER • October 28, 2010

It's easy not to think about **identity theft** — until it affects you.

Thousands of cases of identity theft take place every day all over the world.

Some of the methods in which thieves attempt to steal someone's identity include scams, going through the trash and infiltrating personal computers. But it is possible to thwart such thieves without spending a lot of money.

Prateek Malhotra — the information technology manager for Condor Capital, an investment management firm in the Martinsville section of Bridgewater — believes education and a few proactive steps are all that people need to properly ensure their assets are safe from thieves.

Malhotra recently sat down to answer a few questions about the common dirty deeds found online and the methods of protection available.

*What identity theft threats are most prevalent today?*

Personal **computer** infiltration is the greatest risk to your personal information today. Technology changes so rapidly that security holes are created in many of the programs we use on a daily basis. Two common security risks are phishing scams and spyware.

*What is a phishing scam?*

A phishing scam is when an **identity thief** poses as a trusted source, such as your bank, and asks you to provide them with personal information, predominantly via e-mail. The e-mail may request that you submit your information by clicking on a link to a website to fill out and submit an online form or by asking you to download and complete a written form.

*What is spyware?*

Spyware is information-gathering software that gets installed on your computer via sources such as links or downloadable attachments from fraudulent e-mails or websites. Spyware can record your keystrokes to steal passwords and **credit card** numbers, track your search habits and engage in various other annoying activities such as installing unwanted toolbars.

*Is there anything people can do to protect themselves against these dangerous programs, if they are tricked into or accidentally come in contact with an infected file or website?*

There are many security programs that you can purchase to protect yourself from spyware and other types of malware (software designed to harm your computer or steal information). I currently use ESET Smart Security Suite, a bundled antivirus/antispyware/firewall product.

Be aware that not all security bundles protect you against spyware/malware. When selecting a software **package**, make sure it includes this feature. In addition to ESET, I also use Malwarebyte's Antimalware once or twice a month to scan my computer for spyware and malware.

*Are there any other free solutions available to protect users?*

There is a wealth of free content available, but not all free security downloads are legitimate. The simplest free solution is to always use an updated web browser such as FireFox, Internet Explorer 8, Chrome or Safari.

You also can get a free security boost by utilizing a Web content filter called OpenDNS ([www.opendns.com](http://www.opendns.com)), which filters or blocks websites that appear on its comprehensive list of known scams and sources of malware.

*Is there any additional risk associated with a **wireless** network over a hard line connection?*

Wireless home networks are becoming increasingly popular; however, they are often left unprotected creating substantial security risks. If your wireless signal is not protected, anyone in range with a wireless card can intercept your signal and steal your information or install malware.

Keep your home **wireless networks** secure by changing your router's default username, password, and encrypt or scramble your wireless signal. Encrypting your signal is fast and simple, just go to your router's online website and follow the instructions. That said, the level and type of encryption available depends upon your choice of wireless router.

The most common options will be WPA2, WPA and WEP with varying encryption levels, generally 64 or 128 bits. The higher the number of bits the more secure the encryption level will be. WPA2 is the best choice; however, in order to use WPA2 all your wireless devices must have WPA2 capabilities.

*Are there any security or privacy risks associated with using online social networks such as Facebook and MySpace?*

Yes, most Facebook and MySpace users are at risk for identify theft because they reveal too much personal information, use Facebook apps and fail to utilize available privacy functions. If you are going to use these or other online social networks, you can protect yourself and others from identity theft by utilizing privacy functions and refraining from posting the following information:

- Full birth dates
- Addresses
- Middle names
- Employer information
- Telephone numbers
- Mother's maiden name.

Unfortunately, using popular Facebook apps also can put you at risk of identity theft because they can contain spyware and other malware programs. The June 2010 Consumer Reports Magazine ([www.consumerreports.org/cro/magazinearchive/2010/june/june-2010-toc.htm](http://www.consumerreports.org/cro/magazinearchive/2010/june/june-2010-toc.htm)) has some interesting and informative articles detailing the many dangers associated with the use of online social networks.

Jeff Weber: [jweber@MyCentralJersey.com](mailto:jweber@MyCentralJersey.com).