Cyber Crimes

Report Reveals Hackers' New Tricks

(NAPSA)—Have you ever seen a small but strange charge on your bank or credit card statement? Or clicked on a link in a status update on a social networking site? Or maybe clicked on a link sent to you via e-mail or instant message?

You're not alone, and you may already be a victim of a huge and growing problem—cyber crime.

The recent Internet Security Threat Report from computer security company Symantec, makers of Norton, revealed that there were more than 3.2 billion cyber attacks in 2009 alone, which equals one attack for every two people in the world.

And with technology changing at an ever-increasing pace, many of the things you thought you knew, even a year ago, are no longer true.

For example, hackers used to be "nerds" who knew everything there was to know about computers. Today, criminals can buy "crimeware toolkits" that allow someone with little or no technical experience to become a full-fledged hacker almost overnight. These kits let criminals create their own types of "cyber attacks" to steal your personal information.

These "cyber criminals" aren't only going after rich people and big businesses anymore. They've learned that it's much easier to steal a little bit of money from a lot of different people and they're using technology to do just that.

As technology changes, so do the tricks used by cyber criminals to penetrate a computer's defenses.

"It used to be that you could tell pretty quickly if your computer was infected," said Adam Palmer, Norton's lead cyber-security adviser. "Your system would slow down. It would do strange things or have a billion different 'pop-up' windows that you couldn't ignore."

However, that's not always the case now. "Today's cyber criminals have learned something important from the animal kingdom," said Palmer. "A good parasite never kills its host. The criminals don't want you to know you've got a problem on your computer. The longer they can go undetected, the more damage they can do and the more personal information they can steal from you."

Here are some tips on how you can protect yourself against these sneaky criminals:

- Use an Internet security solution that combines anti-virus, firewall, intrusion detection, and vulnerability management for maximum protection.
- Make sure that your security is up to date—many security suites offer automatic "live" updates as new threats are discovered.
- Use passwords that are a mix of letters and numbers, and change them often. Passwords should not consist of words from the dictionary.
- Never view or open any e-mail attachment unless you're expecting it.
- Routinely check to see if your operating system is vulnerable to threats. A free security scan is available through the Norton Security Scan at www.symantec.com/securitycheck.
- Review bank, credit card and credit information frequently to monitor any irregular activities. For further information, the Internet Crime Complaint Center (IC3) has also released a set of guidelines on how to avoid Internet-related scams. See www.ic3.gov/default.aspx for more information.

For more information on the report and how to protect yourself from criminals online, visit Norton's site www.everyclickmatters.com.