Internet Security

Adapting To Scams Is Vital To Internet Safety

(NAPSA)—The words "evolving viruses" conjure up images of illnesses silently mutating until they can evade the defenses of their victim or the latest medication. But another form of mutating threat is claiming thousands of unsuspecting victims each year: cybercrime.

As the security features on computers have become more robust, high-tech criminals have developed a revolving door of increasingly sophisticated scams, particularly because cybercrime has evolved from a hobby for hackers to a lucrative profession. The direct financial losses from these crimes exceed $1 billion a year, according to research commissioned by the U.S. Department of Homeland Security.

A form of social engineering, online scams that con people into sharing personal information or downloading programs that steal their information or harm their computer are expected to be the most common Internet threat this year, according to security experts at Microsoft Corp. Experts say there are no quick fixes against these mutating online threats, but people can avoid becoming a victim by educating themselves on the latest threats and updating their PCs with the latest protections.

Social engineering is what tricked Judy Melloon. After receiving several e-mail messages that appeared to be legitimate, she opened one and typed in the requested bank account information. Her account, which contained several hundred dollars, was soon empty.

"You have to think before you click," said Melloon, who no longer opens e-mail from unknown senders.

Education will be particularly important throughout 2007, predicts Microsoft senior director of Security Outreach, Kristin Johnsen, because many of today's most prevalent online threats attempt to manipulate people, rather than exploit flaws in computers.

"People understand the need to protect their homes or cars in the physical world by locking doors or installing alarms," Johnsen explained. "Applying the same measures to computer use will be the first step to help people protect their PCs, themselves and their families in the cyberworld."

To combat such practices, experts recommend taking these steps:

• Invest 30 minutes up front. That's all the time it takes to set up and monitor an Internet firewall, update your security software, and install and run antivirus and anti-spyware software.

• Think first, click later. Don't click on e-mail attachments from senders you don't know or recognize, and avoid entering personal information into anything directed to you via e-mail.

• Stay current. Regularly visit sites that provide the latest PC security information, including http://www.microsoft.com/protect and http://www.staysafe.org. Invest in software and services that offer security features, such as Microsoft's Windows Vista operating system, which automatically maintains many recommended protection features.