Internet Security

Online Shoppers, Beware Of Cyber-Grinches

More Vigilance Means Better Protection For Online Shoppers This Holiday Season

(NAPSA)—Rosy red cheeks from a nip of frost in the air; precious time with friends and family; cybercriminals trying to victimize you and your family. The holiday season is changing, but not everyone needs to fall victim to online crime.

According to a recent JupiterResearch survey, more than 117 million people made purchases online during last year's holiday season and even more are expected to do so this year. But the increase in online shopping has also given rise to a whole new breed of criminal: online crooks who spend their holidays trying to ruin those of other people by taking control of their computer and then accessing their bank accounts or even stealing their identity—something like a cyber-Grinch.

A favorite tactic of cyber-Grinches is called phishing. With specific tricks, they use enticing offers—e-mailing under the guise of gift ideas, e-coupons or even online greeting cards—designed to trick people into opening attachments or clicking on links inside the e-mail message. Lottery scams via e-mail are another example of this trickery, offering too-good-to-be-true awards of prize money in exchange for personal information or a small down payment. Consumers who fall for these traps could unwittingly install a program that gives a criminal access to their personal and financial information. In 2006 alone, the estimated cumulative financial losses from phishing attacks exceeded $2.8 billion, according to Gartner Research.

A recent study commissioned by Microsoft and conducted by Harris Interactive revealed that about one in five online adults (17 percent) has been the victim of at least one Internet scam, with 81 percent of victims acknowledging that they mistakenly took the cybercriminal's bait.

This year, Microsoft offers the following useful tips to help consumers safeguard themselves against phishing attacks:

- Properly set up and use an Internet firewall on your PC.
- Keep your security software up to date.
- Install an anti-virus program and check for updates regularly.
- Make sure your operating system and software are equipped to help protect against spyware. Essentially, think first and click later.

Also, Microsoft recommends that people use a phishing filter and a spam filter on their computers, exercise caution when using public computer networks for online banking and sales transactions, avoid opening e-mail attachments from unknown senders and be wary about file sharing due to the increasing risk of worms, viruses and spyware.

Even more information on Internet safety and online shopping is available at http://www.microsoft.com/protect.