IDENTITY THEFT

As Online Fraud Grows, Experts Offer Tips

(NAPSA)—Online banking and shopping have made life easier, helping customers avoid long lines and run their lives with more efficiency. But it also has opened the doors to a new form of attack that is becoming a household word: phishing.

Phishing is an attempt to solicit confidential information for financial gain using fraudulent e-mails as bait. It begins with an e-mail or pop-up that appears to be from a well-known bank, credit card company or e-commerce Web site asking customers to update or verify their account information. Some phishing scams convince consumers to click on a link in the e-mail, which redirects them to a spoofed Web site where they are asked to enter their account number, PIN, or other confidential information.

Customers are lured into divulging information because the phishing e-mails, pop-ups and Web sites often look official. In reality, phishers copy and transfer the branding of a legitimate company and even spoof URLs to make their communication appear not just official but secure.

Phishing attacks have increased by 4,000 percent in just five months, according to the Anti-Phishing Working Group (APWG). In July 2004, the average number of phishing attacks per day was 63.7, up significantly from the 47.4 per day for June.

The growing prevalence of phishing attacks has led information security leader Symantec Corp. to name it one of the top Internet threats to watch out for in its latest Internet Security Threat Report. Symantec offers consumers the following tips:

Don’t let thieves get your identity or your money.

- Don’t respond to unsolicited e-mails that request personal information. If you think the e-mail might be legitimate, call the company that the e-mail appears to be from to verify.
- Never click on a URL in a suspicious e-mail.
- When visiting your bank, credit card company or other e-commerce site, pay close attention to the URL at the top of the browser. Extra letters, numbers of symbols added to the beginning of the company’s name in the URL, or an entirely different URL from the company’s standard Web address, should raise a flag.
- When on a Web page that asks for personal information, look for the yellow lock icon on the bottom status bar. Double-click on the lock icon to display the security certificate. The name following “Issued to” should match the site that you think you are on. If the name differs, it may be a spoofed Web site.
- Make sure your operating system and software programs are updated for patches regularly to protect against exploits that target known vulnerabilities.
- Before filling out an online form, even on secure Web sites, look for a privacy statement that states whether or not the site shares information with outside parties. If possible, opt out of sharing your information with third parties.
- Create secure, complex passwords and change them frequently. Consumers should also prevent computer programs or Web sites from remembering passwords or credit card numbers.

In addition to these tips, experts encourage consumers to use spam filtering and privacy control software, such as Symantec’s Norton Internet Security 2005. Anti-spam solutions can detect certain characteristics in phishing e-mails and tag them as spam. Privacy control software gives consumers the ability to specify the Web sites that their personal information is allowed to go out to, thus preventing confidential data from being sent to fraudulent Web sites.

For more information on phishing, visit the following Web sites:

- National Cyber Security Alliance (www.staysafeonline.info)
- National Consumers League (www.phishinginfo.org)
- Federal Trade Commission (www.ftc.org)