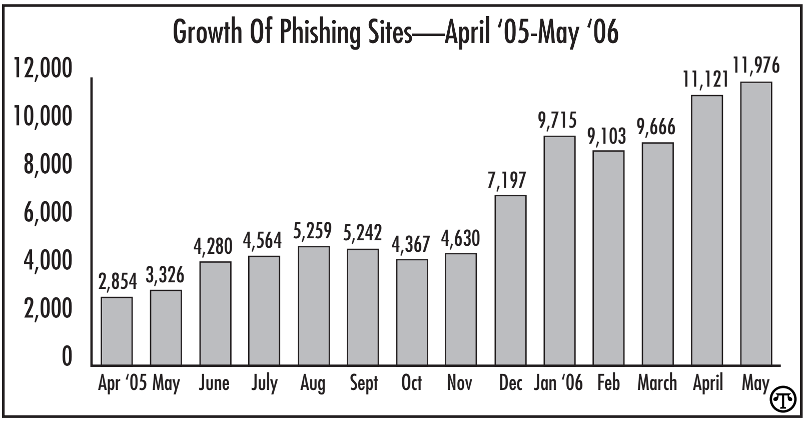
How To Be The One That Got Away In “Phishing” Attacks



Phishing is on the rise.

(NAPSA)—Every dad worth his weight in salmon eggs and shiny lures has at least one great fishing story—usually about the great catch that got away. Unfortunately, too few dads have stories about how they avoided getting caught in a different kind of fishing caper—the online variety known as “phishing.”

Phishing attacks are perpetrated by criminals using fake Web sites and other tactics to trick people into sharing personal information online. These scams are helping fuel the nationwide escalation in identity theft. According to the Anti-Phishing Working Group, the number of phishing sites reported each month more than quadrupled, from 2,854 sites in April 2005 to 11,976 in May 2006.

“People can avoid phishing attacks by learning the telltale signs of these scams and using phish-fighting technology,” said John Scarrow of Microsoft Corp., which offers free technology to help protect people from phishing e-mail and Web sites.

The Microsoft Phishing Filter alerts people to and blocks known or suspected phishing sites. Already available for no charge in the Windows Live Toolbar and as an MSN Search Toolbar Add-in, the filter is also included in Internet Explorer 7 and Windows Vista. In addition, the SmartScreen e-mail filtering technology available in Windows Live Mail, MSN Hotmail, Office Outlook and Exchange Server helps block e-mail messages that can lure people to phishing sites.

Weekend fisherman Robert Marvin has learned how to avoid phishing scams by applying tactics similar to those of the wily salmon that evade his lures. “We carefully review e-mails and Web sites that request personal information,” said Marvin, a father of two who runs a mutual fund. “We don’t ‘bite’ just because it looks official.” He also maintains a credit card with a low limit for all online purchases.

Staysafe.org offers the following tips to avoid phishing scams:

• Never enter personal information, such as credit card or Social Security numbers, into Web sites reached via links in anonymous e-mail messages.

• Avoid clicking on links to Web sites contained in e-mail messages, particularly when updating account information or changing passwords. Instead, type addresses directly into the browser or use personal bookmarks.

• Check for misspellings or typos in the online address, as well as e-mail addresses containing “@” somewhere other than directly before the business’ or Web site’s name.

• Double-click on the yellow padlock icon in the bottom right-hand corner of business Web sites. The name that comes onto the screen should match the name of the site.

Microsoft also recommends that users create different log-in names and passwords for different sites.

For more tools and tips: http://www.microsoft.com/athome/security/email/phishing.mspx; http://www.microsoft.com/athome/security/online/phishing_filter.mspx; http://safety.msn.com/phishing and http://www.staysafe.org/toolbox/scams/default.html.