Five Tips For Avoiding Phishing Scams

(NAPSA)—Every year, tax time brings new challenges for consumers. Not only do they have the regular hassle of filing returns by the April 15th deadline, they also have to worry about new tax scams, including phishing. For example, last year the Treasury Inspector General for Tax Administration found 12 separate Web sites hosting such phishing schemes.

Phishing scams attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials and other sensitive information. Phishers have historically used timely subjects to draw in victims, such as the Hurricane Katrina scam, but because it is a money-making scheme, they also hover around financial topics. In fact, Symantec found that during the tax season last year, financial services was the most heavily phished sector, accounting for 84 percent of all phishing activity. Tax time this year is no exception.

Between January and June 2006, Symantec detected 157,477 unique phishing messages, an 81 percent increase over the 86,906 unique phishing messages detected during the last half of 2005. Comparing last year's tax season to tax time in 2005 also shows a significant increase. With 97,592 unique phishing messages detected during the first half of 2005, 2006 showed a 61 percent increase in these messages.

Solving the phishing epidemic seems simple. If users didn't give out their personal information to these scams, they would dissolve rapidly. However, phishing continues to be a problem because fraudsters constantly find ways to lure victims into giving away their personal information.

However, the following five tips will help consumers avoid the hook behind phishing attacks.

1. Be extremely wary of e-mails asking for confidential information—especially of a financial nature. Promises of a tax rebate or other incentives are more likely ploys to steal personal information. If people receive this kind of request, they need to call to confirm the sender's identity and the validity of the request.

2. Don't feel pressured into providing sensitive information. Phishers like to use scare tactics, employing urgent language to pressure victims. They may threaten with fines, account suspension or service delays until the person updates certain information.

3. Be aware that e-mails from legitimate government entities, banks or ISPs should directly address the individual. It is best to contact the organization that sent the e-mail to confirm its authenticity.

4. Never submit confidential information via forms embedded within e-mail messages. Rather, users should communicate that information over the phone or through a secure Web site.

5. Don't click on a suspicious e-mail containing a URL. Instead, navigate to the Web site by typing the URL directly into their browser's address bar. Just because the site's address begins with https doesn't necessarily mean the site is secure. Phishers may use URL masking techniques to mimic the secure address of an authentic company. Before submitting information, individuals should confirm the URL's authenticity by clicking on their browser's "locked" symbol. Consumers can also use transaction security products such as Norton Confidential to notify them when they encounter fraudulent Web sites.

In the event that individuals inadvertently gave a phisher their financial information, they should monitor their online accounts, making sure all transactions are valid. If they aren't, victims need to contact their bank or credit card company immediately.

Users don't need to be computer experts to protect themselves. Cultivating caution and common sense is the best defense against these attacks. If any questions remain, it's best to contact the organization directly to confirm the legitimacy of an issue.

To learn more, visit www.symantec.com.