Tips For A Safe Online Shopping Experience

(NAPSA)—The National Retail Federation expects that 47 percent of consumers plan to purchase holiday items online this year. Online purchases made on Cyber Monday (after Thanksgiving) alone increased 26 percent to a record $608 million, according to comScore Networks. But, as more consumers have moved online, so have criminals. Phishing, the act in which cyber criminals imitate legitimate companies through e-mail campaigns, and other forms of online fraud continue to grow, and consumers need to be aware of the dangers that lurk in cyber space.

In a year, the number of unique phishing reports (fraudulent e-mail campaigns) doubled to more than 28,000 per month, according to the Anti-Phishing Working Group. Attacks are increasing not only in number but sophistication. In addition to phishing, many cyber crooks have begun using a technique called keylogging, which can be much harder for consumers to identify. Keylogging is when a hidden spyware program is installed on the computer and records the keystrokes, providing visibility to personal information such as your username, password and Social Security number, so cyber criminals can build a profile with your personal information.

A leading expert in enabling and protecting online transactions, VeriSign offers consumers tips on what they should look out for when shopping online. VeriSign helps verify online retailers such as Orbitz, Overstock.com and eBay, so shoppers are confident they're making purchases on a legitimate site rather than a spoofed one. VeriSign-verified sites use SSL certificates to secure their customers' transactions, and advised that although online threats are increasing, there's plenty consumers can do to protect themselves.

"The most important thing consumers can do to protect themselves from online fraud is be sensible and know what to look for. On top of checking for the padlock in the browser and checking to make sure the transaction is going over an encrypted connection, such as the address displayed as https://, it is also important to check if the site itself is using a trusted SSL certificate and displaying a trusted security symbol," said Tim Callan, director of product marketing, SSL, for VeriSign. "If the site displays a recognized trust mark, you can feel confident in that site's security."

Smart Tips

1) Look for the padlock at the bottom right-hand corner of the Web site.

2) Look for https://.

3) Know your vendor and check to make sure the business has a phone number and postal address.

4) Verify before you buy by checking the certificate details on a Web page.

5) Monitor your bank and credit card accounts for any sign of fraudulent activity.

For more information, go to www.verisignsecured.com.