Pharming, Phishing, SMiShing and Vishing – Beware of Scams!

by Sue C. Quimby, CPCU, AU, CIC, CPIW, DAE

EVERYONE IS CONSTANTLY UNDER ATTACK by identity thieves. It is estimated that there is a new victim every 3 seconds (www.idtheftcenter.org). The scams come in many forms, often preying on people's fears of losing money, being arrested or accused of something they did not do. Helping clients protect their identity is another value-added service of the professional insurance agent.

Dumpster diving has long been a source of stolen personal identifiable information (PII), and one of the easiest to prevent, by using a crosscut shredder to dispose of documents and envelopes that contain such information. Exposure can also be reduced by opting out of preapproved credit card offers, and using the post office or other secure mail boxes when sending mail.

Personal information such as passwords, social security numbers or PINs should never be given out via email or phone unless you initiated the transaction. Care should be used when posting personal information, such as birth dates, on social media sites. Use different secure passwords, with a combination of letters, numbers and symbols, for computers, smartphones and financial institution transactions. "Made up" nondictionary words are a good idea.

As technology becomes more sophisticated, so do the thieves. Pharming, Phishing, SMiShing and Vishing are some of the ways that thieves try to obtain personal information. Red flags of scams are a contact via phone, email or text from someone claiming to be a bank or other entity trying to verify personal information.

Pharming is when someone attempts to hijack a computer by redirecting traffic to another site. Firewalls, anti-spyware and anti-virus software can help prevent identity theft. Check that the website URL you are in is spelled correctly. If you are making a payment, look to see that "https" shows in the address, denoting that the site is secure.

Phishing is the use of emails to bait someone into divulging personal information. According to the AntiPhishing Working Group's Global Phishing Survey, (APWG), in the first half of 2013, there were 13,498 attacks on PayPal alone. (docs.apwg.org) Vishing is similar to phishing, in that it involves voice or telephone spam to solicit information.

SMiShing, or SMS fishing, is the use of Short Message Systems (texts) to direct the victim to a website or phone number. For example, the message may be purported to be from the IRS, with substantial penalties or arrest if the victim does not visit the website or call the number shown. Once at the website, the victim's computer may be infected with malware. According to messaging security experts, "phishing attempts accounted for 55% of reported SMS messages in January of 2014" (www.cloudmark.com).

Smartphones and other mobile devices are useful tools, but they are also a prime target of identity thieves. For example, before downloading an app, check to see what information the app is going to access. This could include your phone number, location, and calling patterns. Data access and storage on mobile devices is also a concern.

Identity theft can mean a major disruption in someone's life, leading to financial loss as well as destruction of credit rating. Helping clients prevent identity theft is another sign of the true insurance professional.

Previously published in the Insurance Advocate®

MSO®, Inc. 139 Harristown Road, Suite 100; Glen Rock, NJ 07452
Web: www.msonet.com; Email: info@msonet.com; Phone (800) 935-6900 / (201) 447-6900; Fax (201) 447-9468