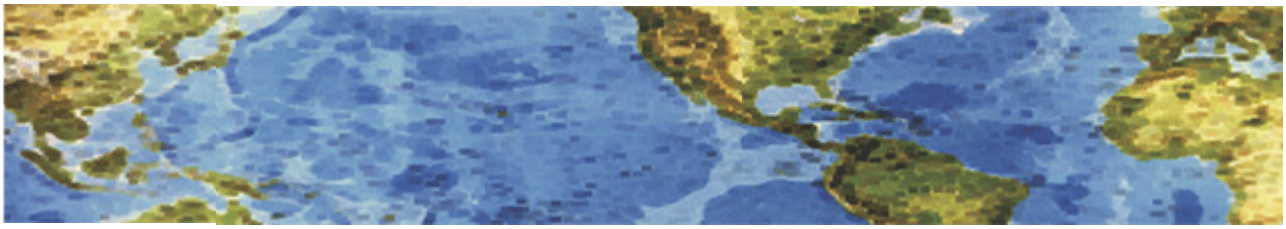
HALL ASSOCIATES



Risk-Based Decision Making Commentary
14 October 2013 Newsletter

Open Enrollment Is Phishing Season
Fraudsters Target Those Signing Up for Health Insurance

Open enrollment has begun for Obamacare as well as for health insurance plans offered by many employers. And that means it's prime time for fraudsters to target consumers with phishing scams, disguised as official-looking open enrollment messages, in an attempt to steal personal information. **Privacy and security experts stress the need to remind those participating in open enrollment about the dangers of phishing, including avoiding clicking on links in suspicious e-mails that bring individuals to fake websites designed to gather information.**

Health Benefits Ploy

The open enrollment scams typically involve e-mails that purport to be official communications about health insurance but link the user to a fake employee or government web portal designed to collect personal information that can be used to commit fraud. In some cases, simply clicking to open the e-mail or a link it contains can lead to an immediate malware infection.

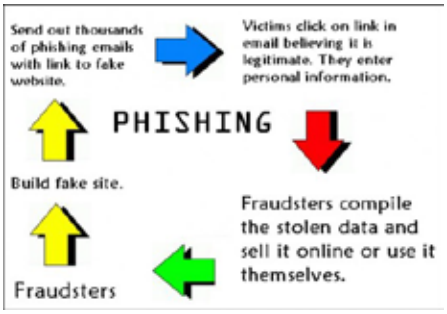
In addition to spear-phishing e-mails targeting employees at specific companies during open enrollment season, scammers are also targeting consumers who are interested in shopping for insurance on new state health insurance exchanges and seniors looking for supplemental Medicare plans. Even before new state health insurance exchanges under Obamacare launched on Oct. 1, scammers began sending consumers spam containing the terms "Medicare," "enrollment" and "medical insurance." The spam contained links taking users to nefarious websites containing surveys asking for personal information in exchange for a chance to win prizes, such as iPhones.

Steps to Take

To prevent employees from becoming victims of these scams, organizations must educate them to avoid opening e-mail from unrecognized senders and refrain from opening attachments or clicking on links that look suspicious. Employers also should take the extra step of alerting employees in advance that the company, or its outside benefits contractor, will be sending employees messages about open enrollment information. Alert employees to notify company officials when they receive suspicious e-mails.

http://www.bankinfosecurity.com/open-enrollment-phishing-season-a-6135

HALL ASSOCIATES



Recent Spear-Phishing Incident

A recent healthcare-related spear-phishing incident at St. Louis University demonstrates that the scams can hit at any time. The scam e-mail about a systems update sent to 180 SLU employees, including physicians at the university's medical group, contained a link to a fake site that looked like the SLU's employee portal. Several employees were fooled into entering personal information related to their direct deposit accounts.

The phishing e-mail contained the university's logo and was well-written. However, a keen eye would have noticed that the link in the e-mail contained an incorrect URL for the university's employee portal. The university's investigation found that 10 employees had direct deposit information changed, although no unauthorized financial transactions had occurred. However, the university also learned that the incident resulted in unauthorized access to about 20 SLU e-mail accounts that contained personal health information for approximately 3,000 individuals. and Social Security numbers of about 200 people. SLU is offering affected individuals a year's worth of free credit monitoring and identity theft protection services. As a result of the phishing incident, SLU is ramping up employee education.

http://www.govinfosecurity.com/open-enrollment-phishing-season-a-6135/op-1

Breaches: Holding Retailers Accountable

The Vermont Attorney General's $30,000 settlement with a breached retailer is significant because it demonstrates that states can play a role in holding retailers accountable for losses associated with card fraud, one banker says. As a result of this case, more banking institutions may ask state attorneys general to conduct investigations after card fraud is linked to a retailer. That's because attorneys general enforce state laws, which may call for timely breach notification and establish security requirements, including compliance with the Payment Card Industry Data Security Standard.

Last month, the Williston, Vt.-based grocery chain Natural Provisions agreed to pay a $15,000 fine to settle allegations that it failed to promptly notify customers of a breach dating back to 2012. Natural Provisions also agreed to spend $15,000 on security upgrades to its point-of-sale system. According to Vermont Attorney General William Sorrell, Natural Provisions' lax security contributed to the breach that resulted in tens of thousands of dollars in fraud losses linked to compromised cards. In the settlement with Natural Provisions, Sorrell claims Natural Provisions failed to address, in a timely manner, security weaknesses that allowed its payments network to be compromised and an undetermined amount of card data was stolen.

http://www.bankinfosecurity.com/breaches-holding-retailers-accountable-a-6138