Health Information Compliance Alert

Avoid Phishing Schemes with These 7 Pointers

Hint: Excessive spelling errors are a tip-off that the email might be a scam.

As the risks continue to rise, cybersecurity training has never been more important in the healthcare industry. And as email remains the most basic port of entry for hackers, there's never been a better time to train your staff on email basics.

Reminder: Phishing is a type of social engineering, but phishing emails are becoming more and more sophisticated. "Criminals have gotten smarter and their tactics have evolved," warns **Michael Whitcomb**, CEO of IT security and regulatory compliance firm Loricca in Tampa, Florida. "Train your employees to watch for emails that may contain tricks to access personal or professional information."

Take a look at this phishing primer and pocket it for future practice issues.

1. Authenticate Remote Users. Your staff members may recognize a remote user's name but be tempted to skip over the authentication procedures. Two-factor authentication is becoming more popular for email addresses and can eradicate login phishing ploys.

2. Verify the Subject and the Sender. Be wary of "spoofed" display names or crafty subject lines meant to trick the readers into thinking the email is legitimate. Last year, a phishing scheme went out to healthcare organizations masquerading as governmental emails from the director of the HHS Office for Civil Rights (OCR). (See Health Information Compliance Alert, Vol. 16, No. 12.)

3. Investigate Before You Click. In order to stop social engineers in their tracks, you and your staff need to know what you're up against. Most practices get hundreds of spam emails weekly. If one looks particularly phishy, look at the embedded link but do not click on it. Alert IT instead before deleting, so they can verify the email address or company and block future correspondences.

4. Scan for Grammar and Spelling Blunders. Most professionals have spell-check at the ready, and large corporations have entire departments dedicated to making their communication perfect. Major spelling and grammar errors, a lack of any sentence structure, random references to big-name companies, and awkward phrasing are telltale signs of phishing.

5. Heed Requests for Information for Personal Gain. Never give out your personal information or practice data via email. Many phishing schemes offer something in return for names, passwords, office controls and more. Two popular techniques - "quid pro quo," which refers to the practice social engineers use by offering a gift, prize, or service in return for login credentials, and "baiting," which uses the bait-and-switch technique, offering something either digital (a free healthcare IT download) or physical (a USB-drive or free EHR software) for practice data - open the door for hackers through email infiltration. (See Health Information Compliance Alert, Vol. 17, No. 4)

6. Watch Out for Attachments. Any email from an unknown source that includes an attachment should be looked at with skepticism. Attachments often contain malware that hijacks your office networks once you open the email and download the information.

7. Report Idle Threats. Some hackers target entry-level employees using accusatory language over the phone and by email. As authorization on sensitive data usually comes from higher up, this type of email is easier to uncover and deal with. Education from the get-go is key to overcoming this type of phishing, letting staff know that they won't get in trouble for safeguarding PHI.

Consider this: Hacking incidents are on the rise with no end in sight and affected "over 113 million individuals in 2015" alone, according to a report on the most up-to-date researched statistics on healthcare and cybersecurity from the Office of the National Coordinator for Health Information Technology (ONC). "In 2015, hacking incidents comprised nearly 99% of all individuals affected by breaches, and the number of reported hacking incidents, 57, comprised over 20% of all reported breaches," the ONC study showed. The research also noted that "from 2011 to 2014" only "97 hacking incidents" occurred, impacting "less than 4 million individuals," which was "less than 10% of all reported breaches and impacted individuals during this time."

Resource: Review the ONC's "Breaches of Unsecured Protected Health Information" study at, https://dashboard.healthit.gov/quickstats/pages/breaches-protected-health-information.php.