MDS Alert

Cybersecurity: Avoid Cybercriminals With These Tips

Hint: Proceed with caution if you aren't familiar with the contact.

Malware attacks plagued industries in countries across the world this past year, but U.S. healthcare got hit particularly hard, causing headaches and costing millions of dollars in HIPAA violations and lost revenue. With so much of medical care, assessments, and reimbursement documented and submitted on computers and electronic systems, cybersecurity should be a priority for every facility and administration.

If you're thinking cybersecurity is not your forte - you care for residents, after all - think again. The very best cybersecurity plans and systems are only as good as a facility's employee training on the subject. Keep yourself and your team up to date on what strategies criminals areusing to steal information from others in the healthcare industry.

Start 2018 off on the right foot by changing your email password (and reminding others in your facility to do the same). Your facility should also revisit email protocols and make sure all employee training programsfeature at least a few minutes on cybersecurity best practices.

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."

Keep these tips handy and incorporate them into your facility's protocols - and your everyday email usage.

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 meantto 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.

3. **Investigate Before You Click.** In order to stop socialengineers in their tracks, you and your staff need to know what you're up against. Depending on your job description, you may get hundreds of spam emails weekly. If one looks particularly "phishy," look at the embedded link but do not click on it. If your facility has a dedicated IT professional, alert that team memberbefore deleting, so he or she 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 communications perfect. Major spelling and grammar errors, a lack of any sentence structure, random references to big-name companies, and awkward phrasing are all telltale signs of phishing.

5. **Heed Requests for information for Personal Gain**. Never give out your personal information or facility 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.

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 facility's 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 ploy is easier to uncover and deal with.

Top tip: Education from the get-go is key to overcoming this kind of phishing, letting staff know that they won't get in trouble for safeguarding protected health information (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 percent of all individuals affected by breaches, and the number of reported hacking incidents, 57, comprised over 20 percent 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 percent of all reported breaches and impacted individuals during this time."

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