Health Information Compliance Alert

Cybersecurity Quiz: See If You're Up-to-Speed on the Latest Social Engineering Tactics

Infiltrators continue to push healthcare's cybersecurity envelope.

Phishing is the most common type of social engineering in healthcare. And due to its prevalence in the news, you probably know to be wary of email correspondences from dubious origins.

But does your cybersecurity savvy include an understanding of the differences between baiting and whaling? Or could you identify whether you've been the victim of a man-in-the-middle or a spoof attack?

Definition: Social engineering is "an unauthorized attempt by someone masquerading as a legitimate party to elicit information from a staff member that may be used in attempts to compromise the security of systems or accounts," says **Jim Sheldon-Dean**, founder and director of compliance services for Lewis Creek Systems, LLC in Charlotte,VT.

Recognizing attackers modus operandi will help safeguard your practice systems and your office security, saving you both money and headache. Test yourself with these six quiz questions.

Question 1: You've won a new x-ray machine from a drawing at the adjacent hospital, but in order to get it for your orthopedic practice, you must send them your credentials.

This type of social engineering is known as _____.

A. Phishing
B. Baiting
C. Quid pro quo
D. Ransomware

Answer: C. Quid pro quo refers to the practice social engineers use by offering a gift, prize, or service in return for your log-in credentials or office data.

Question 2: After returning from lunch, you see a stack of office supplies at your desk, which includes a new USB-drive. You pop it in, and malware chaos ensues. What kind of social engineering maneuver is this?

A. Baiting
B. Replay
C. Wireless assault
D. Spear phishing

Answer: A. Baiting uses the bait-and-switch technique, offering something either digital (a free download) or physical (a USB-drive), which once downloaded corrupts your health IT system.

Question 3: A hospital email went out, but only the people in your department received it. A targeted attack like this is called _____.

A. Man-in-the-middle
B. Spying
C. Spear phishing
D. Filtering

Answer: C. Spear phishing targets a particular person, practice, department, or organization with an email scam.

Question 4: During the ER shift change, you notice a new guy walk in with some of your co-workers. Dressed in scrubs, he logs into one of the staff computers without question. The next day he's not there, but the hospital tech guys are. The entire hospital IT system has been crippled by a virus. This is what kind of social engineering scheme?

A. Whaling
B. Tailgating
C. Interception
D. Worm

Answer: B. Tailgating, also known as piggybacking, happens when a person poses as a co-worker, enters restricted areas, and eventually accesses a large practice, clinic, or hospital IT system. The tailgater's goal to corrupt the system and/or steal patient and practice data.

Question 5: During online research, a chat window pops up, offering medical advice about your problem. You submit your credentials and list the patient's issues, divulging sensitive information. Unfortunately, the online communication was hacked by a third party, and electronic protected health information (ePHI) was lost from both ends. This digital infiltration is known as _____.

A. Doubling
B. Phishing
C. Correspondence
D. Man-in-the-middle

Answer: D. Man-in-the-middle happens when a third party interrupts online communication between two entities. During the intercourse, the third party responds and alters the communication, posing as if he is one of the two original communicating entities. Currently, man-in-the-middle (MITM) attacks are a major focus of the Office for Civil Rights. See the OCR's April Cyber Awareness Newsletter for an overview at: https://www.hhs.gov/sites/default/files/april-2017-ocr-cyber-awareness-newsletter.pdf?language=es.

Question 6: The hospital's entire system is in the throes of a ransomware malaise. And, whose email ends up being the source of entry? The chief physician. The executive-directed cyber assault refers to _____.

A. Whaling
B. Replay
C. Encryption
D. Focusing

Answer: A. Whaling is a type of phishing that targets executive emails, stealing the most sensitive practice or company information and corrupts systems from the top down.

Reminder: "Social engineering tactics are designed to obtain secure information (login, customer, patient, or corporate data) by conning a person into revealing the information," explains **Michael Whitcomb**, CEO of the IT security and regulatory compliance firm Loricca in Tampa, Fla. These types of attacks exploit the overly trusting nature of most people. But remember with a combination of training, concrete policies, and skepticism, social engineers can be stopped in their tracks.