Health Information Compliance Alert

Clip And Save: Safeguard Your Practice with These Tips to Fight Social Engineers

Tip: Check IDs at the front desk every day, every time.

As social engineering becomes more sophisticated, providers and their staffs need to defend against the mastery of these information-stealing thugs. Whether they enter through the front door or access your systems through online trickery, you need to protect your CEHRT, your patients, and your livelihood.

"Criminals have gotten smarter and their tactics have evolved," warns **Michael Whitcomb**, CEO of the IT security and regulatory compliance firm Loricca in Tampa, Fla. And it is essential to "train your employees to watch for emails that may contain tricks to access personal or professional information."

Take a look at this primer to address social engineering in your office:

- Educate your staff on both the nuances of the various types of digital deception as well as the importance of physically securing health IT.
- Implement strict policies in regard to badged entry, identification, and office security.
- Encourage employees and practice leadership to verify email addresses before opening notes from unknown senders.
- Revisit HIPAA compliance standards and follow the rules of PHI and ePHI disclosure.
- Do not insert, upload, or download anything questionable until consulting with your office IT staff first.
- Check with management when in doubt about suspicious correspondence email, phone call, or other communication.
- Use multi-factor authentication and data-at-rest encryption to protect practice devices.
- Refrain from giving personal practice or patient information over the phone, especially to a caller with an unverified number.

Reminder: "Education is low-hanging fruit once a year is not enough to train your people," stresses **Larry Whiteside, Jr.,** vice president of healthcare and infrastructure for Optiv**,** a Denver-based cybersecurity solutions firm. Healthcare organizations "must emphasize cybersecurity education" for their employees to ensure that they understand how best to mitigate risks.