Health Information Compliance Alert

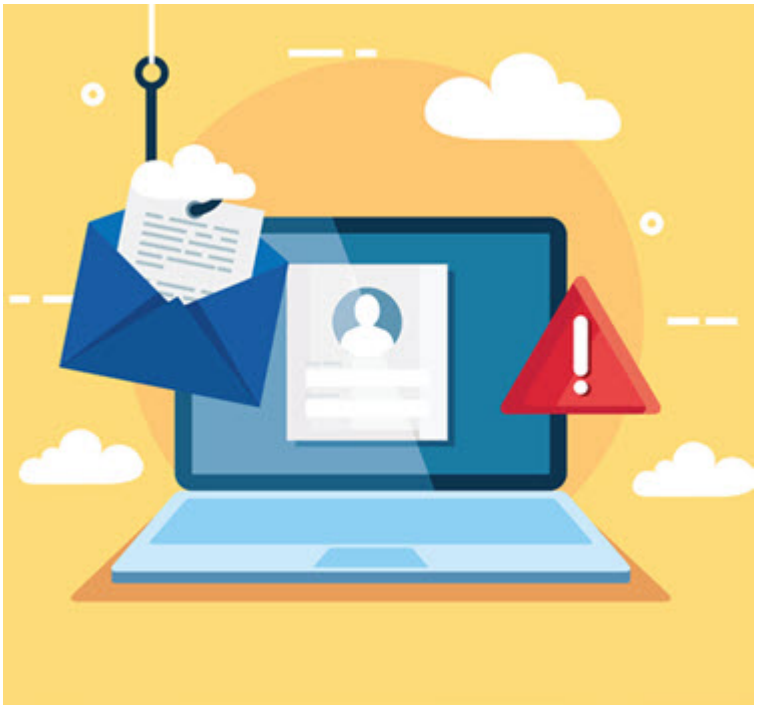
Revenue Booster: Bolster Your Email Security with 10 Top Tips

Hint: Quiz staff on phishing ploys.

Even the most tech-savvy folks get duped by email phishing and malspam. It's critical that you take the time to educate your staff members on how to react to even the simplest virus or hoax - or you risk leaking your patients' electronic protected health information (ePHI).

Here are 10 tips for protecting ePHI and your organization against an accidental malware attack:

1. Remain skeptical: Even if an email was sent to you by a colleague or from an email address that looks like a colleague's, that doesn't necessarily make it legitimate. Attackers can create fake email addresses that look like the ones you know. Do your due diligence and check with the supposed sender to make sure the email was purposely sent before opening any attachments.



2. Stay on top of software updates: Operating systems and software developers release updates regularly when they discover vulnerabilities, security flaws, or any number of other problems. By running these updates as they're released and vetted by your practice's IT department, you'll protect your devices against attackers.

3. Turn off automatic downloads: Your email software settings may have an option to automatically download attachments. If so, disable this feature to protect your computers against possibly dangerous files.

4. Perform frequent backups: If a cyberattack occurs, you'll be able to get your computer and network back up and running sooner if your practice has backups on hand.

5. Secure legacy systems: If your organization depends on a legacy system to keep things running smoothly, ensure

it's compatible with new software. The chances of a cybersecurity incident are higher with legacy systems, so it's critical that you manage updates and implement strict authentication protocols.

6. Consider cloud-based email security: Many of your staff may still be working from home. A cloud-based email system can help curtail ransomware woes and secure your data more efficiently as your IT team and vendor have easier access to shut down issues.

7. Employ a phishing test: Time and again, phishing is the culprit that takes systems down with just one click on a link. Phishing tests are important to sidestep these common attacks. "A phishing test is the practice of sending phishing messages to employees and if someone clicks on it, they are afforded the opportunity to learn more about phishing," recommends **Adam Kehler**, director of RSP Healthcare Services at Online Business Systems. "This is an extremely effective training method and is relatively inexpensive."

"Do not exempt physicians and executives. They are the biggest target and often the most likely victims," he expounds.

8. Utilize encryption: Your employees may lack the skills to identify a phishing scheme, and that's where encryption technology comes into play. Email encryption can help your organization authenticate emails with tools to ensure that the email isn't a phishing attack.

9. Make training ongoing: Your employees are going to get a wealth of HIPAA and IT training when they start at your firm - but that shouldn't be the end of their data security education. With each new threat - and especially if an incident occurs - you must update and re-train staff, keeping them in the loop and offering tools and guidance.

10. Trust your gut: Don't open any email or attachment if it seems suspicious. Your computer's antivirus software could even be fooled into thinking the message is safe. Attackers constantly release new threats before protection software has been updated. If you feel uneasy, trust your gut.

Keep these tips handy to serve as a reminder the next time you receive an unsolicited email with an attachment.