Codify
BY AAPC

Health Information Compliance Alert

Cybersecurity: Identify Phishers With This Expert Advice

Recognize these common hackers' tricks.

Even in the best of times, phishing can take down an organization. Unfortunately, these are not the best of times. And as the healthcare industry struggles with a pandemic, hackers are now homing in on providers with COVID-19 schemes and hoaxes.

Now: Both the **FBI** and the **HHS Office for Civil Rights** (OCR) have issued warnings about cyberattackers targeting medical providers in the U.S. with phishing attacks through emails. The FBI released an FBI Flash bulletin in late April outlining known attacks, including some of the file names employed by the attackers. The FBI cautioned that the files were not actually supplying information as COVID-19, as the file names suggested, but actually were "malicious attachments, which exploited Microsoft Word Document files, 7-zip compressed files, Microsoft Visual Basic Script, Java, and Microsoft Executables."

Read the alert at https://content.govdelivery.com/attachments/USDHSCIKR/2020/04/27/file_attachments/1436494/COVID_Phishing_FLASH_4.20_ FINAL.pdf.

Definition: Phishing is a form of social engineering, which refers to "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, Vermont.

Pinpoint Phishing With These Tips

Though your practice may be in the throes of COVID-19, there are still many things you can do to thwart cyberattacks.

For example, "remind employees to be cautious when opening emails about COVID-19, especially those from outside the organization," indicates the **Center for Internet Security** (CIS) in its Resource Guide for Cybersecurity During the COVID-19 Pandemic.

CIS adds, "They should exercise caution when entering credentials into a website, linked from an email, text message, or social media account, or when downloading attachments."

Remember, however, that even the most tech-savvy folks get duped by 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 you risk leaking your patients electronic protected health information (ePHI) and your practices' secrets to hackers and identity thieves.

Reminder: "Scammers often update their tactics, but there are some signs that will help you recognize a phishing email or text message," advises **Federal Trade Commission** (FTC) consumer guidance.

"Phishing emails and text messages may look like they're from a company you know or trust. They may look like they're from a bank, a credit card company, a social networking site, an online payment website or app, or an online store," the FTC warns.

Spot phishing attacks with these five tips:

1. Don't be fooled by log-in questions: Be wary of suspicious log-in activity followed by a prompt or link to reset your

account. This kind of email phishing tries to hijack your credentials by tricking you into thinking there's a problem - don't fall for it and don't click on the link.

2. Look for fake updates or confirmations: Phishing attempts often try to trick you into exposing data with faulty links for software updates, fake invoices, or identity confirmations. The links often lead down the malware hole - avoid at all costs.

3. Watch out for spoofers: If you start getting random emails from a trusted organization asking you to update your credentials by clicking on an embedded link, you're likely getting spoofed. A spoofing attack occurs when hackers disguise communication, pretending to be a known organization in the email when the link actually connects you to a malware attack.

4. Scan for spelling snafus: Chances are you have spell-check at the ready, and so do other organizations. That's why major spelling and grammar errors, a lack of sentence structure, random references to big-name companies, and awkward phrasing are all telltale signs of phishing.

5. Use caution with attachments: Any email from an unknown source that includes an attachment should be looked at with skepticism. Attachments often contain malware that usurps your practice's networks once you open the email and download the information.

Strategy: Beat data thieves at their own game by alerting IT management to the issues and deleting these emails immediately. A follow-up call to the institution the hackers were supposedly contacting you from is a helpful tool to circumvent future data security incidents, too.

Warning: Never share your financial or other confidential information via email - even if you are positive the sender is legitimate.