MDS Alert

Reader Questions: Beware Phishing Attempts

Question: The organization I work for takes the Health Insurance Portability and Accountability Act (HIPAA) compliance very seriously. In fact, we regularly utilize risk analysis and management as outlined in the Security Rule. However, we've noticed the phishing and ransomware spikes in the healthcare industry during COVID, and we're worried. Is there any way to stay abreast of emerging threats and trends to protect ourselves before accidents happen?

Virginia Subscriber

Answer: Yes, there are a couple of handy online resources that offer the most up-to-the-minute advice on threats.

One helpful site to look at is the National Vulnerability Database (NVD), which is maintained by the National Institute of Standards and Technology (NIST).

"The NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP)," NIST explains. The NVD resources offer tips on managing and measuring vulnerabilities while alerting the public to known software flaws, misconfigurations, and cyber impacts.

Heads up: As part of their policies and procedures, covered entities (CEs) and their business associates (BAs) must address known and possible vulnerabilities in their risk analysis, reminds the HHS Office for Civil Rights (OCR) in the 2022 Cybersecurity Newsletter for the first quarter.

But you might be wondering what OCR considers a vulnerability? "Exploitable vulnerabilities can exist in many parts of a regulated entity's information technology infrastructure (e.g., server, desktop, and mobile device operating systems; application, database, and web software; router, firewall, and other device firmware)," the Cybersecurity Newsletter says. "Often, known vulnerabilities can be mitigated by applying vendor patches or upgrading to a newer version. If a patch or upgrade is unavailable, vendors often suggest actions to take to mitigate a newly discovered vulnerability," OCR advises.

CISA: The Cybersecurity and Infrastructure Security Agency (CISA) also offers daily updates on a variety of issues - and includes industry-specific guidance. Plus, you can subscribe to CISA's numerous alerts and bulletins on a plethora of topics. Other tools on the site include a dedicated Stop Ransomware page, cyber hygiene services, and regionally based cyber tools and resources.

Resources: Visit the NVD resources at https://nvd.nist.gov and peruse the CISA site and guidance at www.cisa.gov.