Codify
BY AAPC

Health Information Compliance Alert

Clip And Save: Add These 10 Buzz Words to Your Cybersecurity Checklist

Yes, vishing is a thing.

Health technologies seemingly evolve at the speed of light - and cyber thugs are always there with ever more sophisticated means to take down systems big and small. Keeping hackers at bay is a slippery slope, but a primary knowledge of the dialogue is a step in the right direction.

Look at these ten terms and put them into your cybersecurity glossary:

1. Botnet: This remotely controlled, digital envoy is really a "collection of computers compromised by malicious code and controlled across a network," notes the Department of Homeland Security's (DHS) cybersecurity guidance. And what name does the criminal who maneuvers the botnet go by? A bot herder, of course.

2. Blended threat: This form of malicious attack combines more than one type of software hack. The cyber criminals could throw a worm, a virus, or other malware technique your way to disrupt or disable your systems across multiple levels.

3. Clear web: This is the basic online venue for most traditional internet users and is easily accessed. "The Clear Web, or Surface Web, ... contains content for the general public that is indexed by traditional search engines (like websites for news, e-commerce, marketing, collaboration, and social networking)," instructs the Federal Bureau of Investigation (FBI). "The FBI's own public website is part of the Clear Web."

4. Deep web: This more in-depth and hidden resource must be accessed by a specific URL but is still open to the general public, the FBI explains. "Examples of Deep Web content are websites and forums that require log-ins, websites that don't allow for indexing or aren't linked to anything, and databases."

See more about the FBI's explanation of the web breakdowns at www.fbi.gov/news/stories/a-primer-on-darknet-marketplaces.

5. Pharming: Social engineers are masters at watching providers' habits and using those tendencies against them. That's how "pharmers" operate. For example, a pharming hacker will redirect you from a real website that you frequently access through private controls and password to an identical but false domain and steal your data.

6. Role-based access control: This type of health IT systems configuration adapts access to both hardware and software based on the role you play in your practice. "Care must be taken to assign staff to the correct roles and then set access permissions for each role correctly with respect for the need to know," advises the Office of the National Coordinator for Health Information Technology (ONC) in its "Top 10 Tips for Cybersecurity in Health Care."

7. Smishing: This common phishing expedition utilizes SMS texting to lure victims to reveal personal or practice information via text. The malware offers up phony webpages, emails, or phone numbers for the clicking - then hacks your phone. "This integration of email, voice, text message, and web browser functionality increases the likelihood that users will fall victim to engineered malicious activity," United States Computer Emergency Readiness Team (US-CERT) guidance warns.

8. Trojan horse: This style of hack is particularly popular with cyber thieves and comes in both the virus and malware coding form. The hackers use software that looks legitimate but is not, then trick you into downloading it. The result: damage and possible destruction to your mobile device.

9. Vishing: Social engineers use strictly voice communication to gain trust and information with this style of cyber hijack. This phishing technique through Voice over Internet Protocol (VoIP) encourages the provider to call a known number, whose caller ID has been spoofed utilizing VoIP, US-CERT advice suggests.

10. Watering hole: Similar to the pharming phishing method, watering hole phishing looks at the sites your entire team visits daily. After pinpointing the favorites, the hackers infiltrate your system by attacking the favored site with malware, taking downyour entire hospital.

Resource: For the most up-to-date malware and virus issues trending daily in the United States, visit www.us-cert.gov.