Codify
BY AAPC

Health Information Compliance Alert

Toolkit: Beef Up Your Cybersecurity Glossary With These 7 Definitions

Feds warn of ransomware attacks on weekends and holidays.

Whether your organization supports staff working remotely or you're revisiting virtual options to combat COVID surges, you need to be mindful of the security risks. And, now the feds advise IT staff to prepare for the heightened threat of cyber attacks during downtimes.

Details: The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) issued a joint cybersecurity advisory, warning organizations to be on high alert for ransomware spikes during weekends and holidays. We "have observed an increase in highly impactful ransomware attacks occurring on holidays and weekends - when offices are normally closed - in the United States, as recently as the Fourth of July holiday in 2021," the joint advisory cautions.

The FBI and CISA offer a breakdown of recent actions on Mother's Day, Memorial Day, and the Fourth of July in the brief. Ransomware attacks on those holidays impacted critical infrastructures in the energy sector, food and agricultural sector, and the IT sector. Due to these past issues, "the FBI and CISA encourage all entities to examine their current cybersecurity posture and implement the recommended best practices and mitigations to manage the risk posed by all cyber threats, including ransomware," urges the advisory.

Additionally, CISA has updated its extensive ransomware resources with a "one-stop location, the "Stop Ransomware" website. The new offering combines an amalgam of federal tips and online tools across all industries with specific sector links, preparation guides, education, incident response, and more. Find the new guidance at www.cisa.gov/stopransomware.

Add These 7 Terms to Your Digital Dictionary

Data security incidents continue to be a serious concern for providers and hospitals. Recent studies suggest that the average cost of a breach in 2020 for a healthcare organization was more than $4.6 million (see Health Information Compliance Alert, Vol. 21, No. 8).

Understanding the IT terminology and identifying hackers' modus operandi can help your team safeguard systems and bolster security, saving your organization both money and headache. Consider adding these seven additions to your cybersecurity glossary for future reference.

1. Adware: If your work is constantly being interrupted by annoying advertisements popping up while you're accessing research or a website, then you are dealing with adware. Sometimes adware is just a nuisance that flashes or prompts you to download harmless software. However, there is malicious adware, which hackers use to control your browsing history and systems while infecting your devices. If you notice that your computer lags or redirects you to new pages, you may be a victim of an adware hack.

2. Clickjacking: If you've ever gone to click on a link - but then are redirected to click on a different link - you've been clickjacked. "Clickjacking, also known as a 'UI redress attack,' is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top level page," explains the Open Web Application Security Project (OWASP), a nonprofit foundation that promotes software security, in its online resource.

3. Cyber Hygiene: One way to clean up your cybersecurity and assess threats is by practicing cyber hygiene. In

technical terms, "cyber hygiene describes recommended mitigations for the small number of root causes responsible for many cybersecurity incidents," explains the National Institute of Standards and Technology (NIST) in its Computer Security Resource Center (CSRC) guidance. And, by "implementing a few simple practices," organizations "can address these common root causes," NIST says.

4. Indicator of Compromise: After a ransomware attack, you may enlist a forensic investigator to figure out how and when cybercriminals infiltrated your systems. The incident response team will likely search for indicators of compromise (IOCs) among the network and host artifacts, CISA guidance suggests. Furthermore, incident responders will "assess [the] results for further indications of malicious activity to eliminate false positives," explains the agency.

5. Ingress and Egress Traffic: These terms relate to the in-and-out traffic of network communications. For example, when traffic is coming towards you that would be ingress traffic, which refers to all data communications entering your network from an external source. On the other hand, egress traffic is data that originates in your network that you send out externally to other destinations.

6. Rootkit: Cybercriminals use this set of tools to access and take hold of your system at the root level. One of the biggest problems with rootkit attacks is that hackers obtain this "root-level access" covertly, and then remotely control the systems with the malicious software without users realizing it, suggests NIST.

7. Threat Hunting: The best way to stop cyber attacks is to prepare ahead of time, and threat hunting is a great technique to assist with that process. "Threat hunting is a proactive strategy to search for signs of threat actor activity to prevent attacks before they occur or to minimize damage in the event of a successful attack," expounds the FBI and CISA in the advisory. Alert systems, data logging, behavior-focused analytics, and tracking programs are all critical threat hunting tools, according to the FBI and CISA.

Resource: Review the joint advisory at https://us-cert.cisa.gov/sites/default/files/publications/AA21-243A-Ransomware_Awareness_for_Holidays_and_Weekends.pdf.