Cyber Security NEWSLETTER

Heritage Provider Network Volume 4, Issue 1

Social Engineering

Social engineering involves manipulating people into divulging confidential information or performing actions that may compromise security. It can take many forms, such as phishing emails, fake websites, and phone scams. The consequences of falling victim to these attacks can be devastating, including financial loss, identity theft, and reputational damage. It is a technique cybercriminals use to trick individuals into giving away sensitive information or performing actions that may compromise security. It relies on psychological manipulation rather than technical exploits. Some common tactics used by cybercriminals include Phishing, Pretexting, Baiting, Tailgating and Impersonation.

Preventing Social Engineering Attacks

It is important to be cautious of unsolicited emails and calls, especially those that request personal information or require immediate action. Verify requests through a trusted source before taking any action. Educate yourself and your employees about cybersecurity risks and best practices, such as using strong passwords, keeping software up-to-date, and being cautious of suspicious activity.

Develop a healthy skepticism towards unsolicited requests, especially those involving sensitive information. Verify the request's legitimacy by contacting the supposed sender through a trusted channel. Be cautious about sharing personal or sensitive information online and offline. Limit the personal information you share on social media platforms, and be mindful of what you post publicly.

Common Attacker Tactics

Phishing: Imagine you receive an email that claims to be from a bank or financial institution, a social media platform, or a government agency. The emails may contain urgent messages, such as a security breach or account suspension, that prompt the recipient to act immediately by clicking on a link or downloading an attachment.

Pretexting: Pretend you receive a call from someone claiming to be from a reputable organization or authority figure. They might fabricate a scenario, like needing your personal information for a survey or to resolve a problem. In reality, they are trying to extract confidential details from you.

Baiting: Picture finding a USB drive or a CD left intentionally in a public place, like a coffee shop or parking lot. The device may be labeled with verbiage that is tempting, such as "Confidential Employee Salary Information." Curiosity might lead you to insert it into your computer, unknowingly infecting your system with malware or giving unauthorized access to the attacker.

Tailgating: Imagine a scenario where you enter a building using your access card, and someone you don't recognize asks to come in behind you, claiming they forgot their card. If you let them in without verifying their identity, you may unintentionally grant access to unauthorized individuals.

Impersonation: Think of someone posing as a coworker, friend, family or an institutional support representative. They might use this deception to gain your trust and convince you to share sensitive information or perform actions that could compromise your security.

Cyber Security Contacts

HPN/HSMG	Mihir Shah (shahm@heritagemed.com)	Anshul Rawat (arawat@heritagemed.com)
BFMC/CCPN	Jeffrey Mooneyham (jmooneyham@bfmc.com)	Michael Flowers (mflowers@bfmc.com)
DOHC	Mark Grant (mgrant@mydohc.com)	Scott Kohnert (skohnert@mydohc.com)
HDMG	Darron Edwards (dcedwards@hdmg.net)	Aalon Gordon (agordon@hdmg.net)
HVVMG	Miguel Guillen (mguillen@hvvmg.com)	Kevin K. Pascascio (kkpascascio@hvvmg.com)
RMG/LMG/ADOC/GCMG	Jim Haggard (jhaggard@regalmed.com)	Dennis Ogtong (dogtong@regalmed.com)