Bellevue University

Eric Wellmaker

Week 12 Writing Assignment

Human Aspects of Cybersecurity

February 25th, 2024

Security awareness training provides an insight into what to look for when something doesn't seem right. Based on the feedback from my classmates, I have revised my security awareness slides by adding more content. These training slides can be used to help users identify the red flags regarding cyber security and personnel threats. For this assignment I will explain my campaign and the meaning behind my quote focusing on the importance of security awareness and security compliance training. I will also discuss the added content totaling four slides. The first is Security Awareness Training, next is Phishing, followed by the Importance of Keeping your System Current and ending an explanation about Social Engineering.

Security Awareness Training Message.

The message that I decided to come up with is, "Security Awareness Training, because we must adapt to an ever-changing environment". This quote took me a while to sort out, but it basically means that as our cyber defenses improve so do the adversaries that do whatever it takes to bypass those same defenses that were created. This never-ending cycle of update/upgrade to bypass and hack are synonymous with each other like ying and yang. It's up to the user to determine how they will educate themselves. In the following section, I will discuss Security Awareness Training and why I believe it's an important aspect of my security awareness training.

Security Awareness Trainings

For security awareness training, there should be training modules. This can be online or in the classroom setting. Training awareness is the foundational part of ensuring a person does not compromise the system due to inadequate training. Training like security awareness should be mandatory for everyone in a business or corporate setting to ensure the best chances of reducing the likelihood of a security incident,

Security Compliance Training. As for security compliance training, this bit ensures data protection at all levels. This includes training on policies and procedures along with employee knowledge and education. The "human factor" is always in my opinion the most important factor in security training.

Phishing. For this slide, I chose the picture of a person fishing to hyperbolize phishing. The person viewing the slide can quickly relate fishing to phishing and how a person uses bait to lure a target. If enticing enough, the target will bite the bait which is when the phisher (fisher) will reel in the prize. As such phishing in the digital world is a malicious factor convincing a target that they are authentic and can be trusted. Some examples of this include Clicking on an email link because of a gift card promotion or reading a text message that your Amazon account is locked, and you are required to enter your information to unlock the account. Vendors would never text you. The person would have to call the company to inquire why their account isn't working properly.

Keeping your system current. This one goes without saying. Keeping your devices up to date is important. What goes on behind the scenes is a company may discover that there is a vulnerability found and an update or patch will correct the issue. Or the latter is that an exploit was discovered by a malicious actor and to stop other systems from falling victim an update is required. Yes, these can be an inconvenience sometimes, but on the bigger scheme of things, keeping a system updated will help ensure you are protected.

Social Engineering. The final slide talks about social engineering. Also known as human hacking, these people can convince others they are authentic by bypassing a person's red flags. This is accomplished by building rapport with the target, smiling and looking the part like they belong in that environment. The best way to overcome an attack like this is to ask to verify their

credentials, see if they are employed at that institution and finally ask a few questions only certain workers would know based on the level of access that should be granted.

Security assets in the cyber world will always be finding innovative ways to guard against security threats. Security Awareness training is vital to reducing the odds of a security incident. The human factor is also needed because the medium between the Hardware and the internet are its people. If taken seriously, security awareness training can help prevent a security incident.

References

What are the 4 Types of Security Training. (2023). Haekka. https://www.haekka.com/blog/what-are-the-4-types-of-security-training