Promoting and Implementing Security Awareness

Liéla Pressley

College of Science, Engineering, and Technology, Grand Canyon University

ITT-307, Cybersecurity Foundations

Ingrid Gaviria

March 20, 2023

Promoting and Implementing Security Awareness

Security awareness amongst all employees is one of the most important lines of defense for any company. Two major risk factors of any company are people (and people errors) and devices. Users need to be aware of how their actions and security hygiene can be one error away from creating a vulnerability or open the door for an attack. As Christians, we are to honor the Lord in all we do, this includes our everyday tasks and doing our part of ensuring the protection of what we have been blessed with. We are not to be negligent in our actions or turn a blind eye to suspicious activity, but to do justice. It is important for leadership to find different ways to promote effective and responsive security amongst all of its users/employees. This can be done by sending out surveys or baseline tests to evaluate where users/employees are in their security understanding or by being creative, proactive, and urgent in their presentation of security concepts.

By promoting teamwork and boosting morale within an organization, the employees and teams will be stronger and more aware of their actions or suscpicous activity that happens all around them. Implementing fun incentives to a secure space such as prizes, gamifications, certifications, fun luncheons, etc. to promote security, not only allows employees to build connections but also be more encouraged/aware.

The ten most important topics that every organization should prioritize include, but are not limited to the following: phishing attacks, removable media, passwords and authentication, physical security, mobile device security, working remotely, public Wi-Fi, cloud security, internet/email usage, and social engineering. Each of these topics can be taught in a variety of formats that are effective for an organization's users. Phishing can be presented through a short lecture but primarily through phishing simulations to help employees understand how this attack looks like and what the consequences look like. For removable media such as USB, Smartphones, CDs, and SD cards, the easiest and most effective training can be computer-based training. In order to make passwords and authentication protocols and risk more interesting and still provide their importance, gamification methods could be a great way to boost morale and attentiveness. Physical security may require various methods such as posters and gamification to help employees stay alert on sticky notes, leaving documents, unlocked/abandoned devices, or messy desks. Mobile device security and working remotely will best be presented in a webinar or computer-based training, this will allow users to have easy access to security that is catered to

their device. Role-based awareness training can be for employees who work remotely and on public Wi-Fi or need to travel with their mobile devices, this can be done through computer training, email communication reminders, and more. Cloud security is more role-based training unless every user in the organization handles comes in contact with the cloud database at some point. It would be beneficial teach via webinars and engaging lectures. Internet/email usage can be taught and followed up through baseline tests, random games/testing, and allowing your employees to gain certifications through the company this builds incentive to stay aware and diligent on internet and email usage. Social engineering training should start with scenario videos to provide a basic understanding of what different methods could look like. After that organizations should allow 1-2 penetration testings solely for social engineering, to evaluate how employees interact, observe, and are aware of suspicious activities.

References

Ciampa, M. (2021). *EBook: CompTIA security+ guide to network security fundamentals*. (pp. 464-465)Cengage.

Daly, J. (2022, December 20). *12 Essential Security Awareness Training Topics for 2023*. https://blog.usecure.io/12-security-awareness-topics-you-need-to-know-in-2020#phishing

Samson, R., Jr. (2021, September 29). *Email Security Awareness Training for Your Employees: The Importance and Reducing the Risks of Successful Cyber Attacks.* ClearNetwork, Inc. https://www.clearnetwork.com/email-security-awareness-training/