Importance of Cyber Security Awareness Training

For several years now, most cyber security attacks have attempted to exploit the human factor through phishing attempts and related efforts. Most attackers gain entry to systems through successful phishing scams and this has reinforced the need for ongoing employee education. Malicious hackers and attackers trick users into granting them access to a digital resource before hacking their way in. It is easier for a hacker to trick a person into giving them their password than running a complicated script to compromise a system.

From another perspective why would someone get into the hustle of trying to pick a lock yet they can easily trick a person to give them a key. Human beings are the weakest link in any organization's cybersecurity defense and thus are the first target for cyber attackers who use tactics and tools such as ransomware, spear phishing, malware, and social engineering. This creates a greater need for cyber awareness training to all employees within an organisation.

Security awareness training also referred to as cyber awareness training is the process of formally educating a workforce on the various cyber threats that exist, how to recognize them, and steps to take in order to protect them and their organization. This is viewed as a long-term strategy and part of a larger security program.

Threats That Can Be Reduced with Cyber Awareness Training

By constantly promoting a culture of cyber awareness training, an organization can have a greater chance in protecting itself against the following threats.

Spam: These are irrelevant messages sent to computer users using the internet as a medium with a motive of advertising, phishing or releasing malware. Spam attacks are not only limited to direct emails but they are also via social media sites. Hackers can embed password-stealing malware from a simple LinkedIn invitation.

Phishing: Phishing is a common practice whereby hackers go after a broad target of users with emails that look genuine but are intended to lure the uneducated user to click on dangerous links. This is usually to trick the users in divulging usernames, passwords, personally identifiable information and even financial information. Phishing is like throwing out a wide net full of bait and pulling in whatever you catch.

Spear phishing: Spear phishing is a phishing campaign with a highly targeted approach to attacking specific individuals. Spear phishing attacks target high-profile individuals or people with access to valuable digital assets. The email is customized to use all the available information about the targeted individual in order to make the email appear as if it is from a friend or colleague.

Malware: Malware refers to "malicious software". Malware is any type of software designed to cause harm to a device, this can be in the form of viruses, rootkits, spyware, worms and Trojan horses. Advanced Malware has a specific target and mission typically aimed at an organization or enterprise.

Ransomware: Ransomware is used by attackers to extort money or other resources from the target organization. It encrypts files on the drive, extorts for money usually in the form of bitcoins, attempts to steal credentials in the memory and attempts to propagate through the network using stolen credentials or exploits.

Next Page>>>

Given the different threats faced, it is prudent for organizations to constantly administer cyber awareness training by looking at the impending risks within the company and customising the training sessions accordingly. Usually there is a challenge to make users become engaged in the cyber awareness trainings, but this can be resolved by gamifying the training sessions.

NB: BDO Zimbabwe is in partnership with Terranova and Checkmark to provide cyber awareness trainings through the Terranova Platform. For more information on this you can contact: it@bdo.co.zw.

This article was contributed by IT Audit Department of BDO Zimbabwe.

THE END.