Employee Cyber Security Training - 5 Essential Elements

Cyber security statistics tell a sobering tale. Cyber attacks increased globally by an alarming 38 percent in 2022. And 95 percent of successful cyber security breaches resulted from human error. Businesses cannot afford to ignore the importance of cyber security training in arming their employees against cyber dangers.

For maximum results, training should be targeted to employees' specific circumstances. But the following five topics should form the core of every security awareness training program.

1. Guard Against Phishing and Other Social Engineering Attacks

If users learn nothing else, they should remember three words: Do. Not. Click. That is, resist the temptation to click an attached file or a hyperlink unless you were expecting it. Over 90 percent of attacks begin with a phishing email. Even if an email appears to come from a trusted source, verify with the source before opening the attachment.

Hackers have successfully used social engineering tactics for years. Using human interaction, they trick users into surrendering sensitive information such as usernames and passwords or financial data. With the right information, a hacker can compromise additional users and even infiltrate the company's network.

For instance, a phishing email that appears to come from a trusted financial institution asks for account information to resolve an alleged problem. The email may use familiar logos and names that make it appear legitimate. But if the unsuspecting user supplies the requested information, they will find their accounts compromised.

Phishing awareness training teaches users to recognize common signs of a phishing attempt. These can include items such as spoofed hyperlinks or a suspicious sender address. The training will also inform users how to avoid falling victim to an attack. Phishing simulations will reinforce the training.

2. Share and Store Information Safely

Secondly, employees must learn data protection essentials. With the rise of remote work, employees use cloud services on a regular basis. They collaborate in the cloud with colleagues both internal and external. They store and share files using services such as Microsoft OneDrive or Dropbox. And they regularly share information through email.

Users must understand the risks that accompany the convenience of cloud computing and what protections to apply. Training should also include compliance concerns surrounding the transfer and storage of sensitive information.

For example, to remain HIPAA compliant, employees in healthcare organizations must use strong encryption when transferring protected health information.

3. Passwords 101

In many cases, passwords still represent the keys to the castle. Training should reinforce best practices for password management. For instance, the National Institute of Standards and Technology (NIST) periodically updates its password guidelines. Current guidelines highlight the need for long, randomized passwords, as well as recommendations for storing them.

For instance, user-generated passwords should be at least 8 characters. They should not include sequential or repeated characters. And when people use password managers, the NIST suggests securing the password manager with an easily memorized passphrase. Unusual spelling, capitalization and characters make the passphrase harder for hackers to crack.

To further strengthen security, organizations should implement multi-factor authentication (MFA).

4. Mobile Device Security

As employees increasingly use mobile devices such as cell phones and tablets for business, they need to know how to use them safely. In addition to securing mobile devices with strong passwords, they should avoid risky practices such as using public Wi-Fi.

Your organization should have a detailed policy for mobile device use, and security training should cover the items in the policy. This might include how to configure security controls on the device, including encryption. It could also include standards for remote access, how to report device loss or theft and so forth.

5. Incident Response

Employees play a significant role detecting and reporting cyber incidents. Cyber security training should cover the elements of the company's incident response plan. This includes preparing users to recognize the signs of a potential data breach or cyber attack. Training should also cover how to report the attack and what initial steps to take to limit damage.

Ensure Success with Cyber Security Training Experts

An effective security awareness program will help to change employee behavior by giving them the understanding and tools they need. By partnering with the cyber security experts at eMazzanti Technologies, you gain access to enterprise-level security training, customized to your business needs.