How to Succeed at Company-Wide Security Awareness Training

A recent survey by Security Magazine indicated that eighty percent of companies experienced at least one cybersecurity incident over the previous year. Firewalls and antivirus alone will not protect essential information from attack. Organizations must mitigate the human error factor with targeted, relevant security awareness training for every employee, including executives.

Security awareness training teaches employees how to recognize and reduce cyber security risks. All too often, employees at all levels fail to realize how their own behavior opens the door to attack. Likewise, they may not understand and follow best practices to protect both the organization and customer data.

However, to prove effective, cyber security training must engage the learner. Effective training presents small chunks of information, targeted to the employee's role and system access. And when employees receive the right information at regular intervals, they retain and use it.

Make Training Relevant and Engaging

Too many security awareness training programs fail. Employees attend by requirement, but often they find the information dry and uninteresting or filled with scare tactics. Consequently, they pay little attention and fail to apply the training when presented with real-life cyber security situations.

On the other hand, when presenters use training techniques that engage, learners absorb the material more readily. For instance, a real-world scenario, ideally one the employees or execcutives could encounter in their day-to-day work, pulls the learner in. Interactive examples prove especially useful. In short, make the training interesting, positive, and hands-on.

Provide Focused Chunks of Training

Cyber security covers a broad range of topics, from phishing and social engineering to mobile computing and password management. Covering all possible information in a single training session would require hours and induce overload.

Instead, break up the content into focus areas, presented over multiple training events. For instance, an organization might choose to deliver short monthly training events. One training might focus on how to recognize and report phishing emails. The next training might cover proper file sharing or safe use of social media.

Target Training to Learner's Role and Access

A sales executive faces different security threats than a technician on the assembly line. For instance, the accounting executive may well become the target of a spear-phishing campaign. Factory technicians, on the other hand, need to understand how to recognize cyber security threats to the internet-connected machinery they operate.

When training reflects the learner's job duties and level of access, it provides relevant, actionable information. This engages the learner more fully, because they can easily see how it relates to their daily work. When it comes to effective security awareness training, one size does not fit all.

Timing is Key

Decades ago, annual cyber security training may have sufficed. But today, with cyber security threats and best practices evolving so quickly, employees need more frequent reminders. In fact, a recent study suggests that most of us need quarterly refreshers.

With that in mind, consider a layered training strategy. Present hour-long, interactive training sessions every few months, with reminders in between. Those reminders could include online refresher sessions or just-in-time hints. For instance, an embossed stress ball on executive's desks might include a reminder about safe password strategies.

Security Awareness Training as Part of Broader Strategy

Security awareness training plays a key role as part of an overall cyber security plan. When focused, timely training engages learners, it helps to strengthen the human defenses against cyber-attack. Back up that training with effective policies, automated where possible. This will add an important layer of protection on top of security technology.

The cyber security specialists at eMazzanti can help you build the right security strategy for your organization. We can clarify the myriad options at your disposal, helping you decide the most effective combination of tools to keep your employees and executives aware, your information safe, and your company reputation secure.