Is Your Security Awareness Training a Snoozer? Gamify it!

It's that time of year again: security awareness training. Ugh! For many businesses, this is a dreadfully dull "death by PowerPoint" affair, with instructors reading dry bullets that transform a room full of well-meaning employees into glassy-eyed zombies. Attendees often fail to appreciate the importance of security awareness and allow the training to go in one ear and out the other. In some cases, employees skip it entirely, hoping to avoid another boring presentation.

For cybersecurity professionals, this presents a big challenge. We know that employees are the first line of defense against cyberattacks, and that lack of security awareness can expose businesses to significant security risks. One great way to address this challenge is to incorporate elements of game playing (gamification) in your security awareness training.

Risks of Poor Security Awareness

Employees often put their companies at risk of cyberattack by using weak passwords, browsing dangerous websites, clicking on malicious emails, and doing other insecure things that could have been prevented with effective security awareness training. While these employees generally do not mean to cause harm, their actions can result in significant financial and reputational impacts for their companies. According to the FBI's Internet Crime Complaint Center, suspected internet crime incidents resulted in losses in excess of $3.5 billion in 2019.

Most businesses claim to have strong security policies, controls, and awareness training in place to guard against cyberattacks. Unfortunately, Tevora's incident responders, and countless media reports, are seeing a different reality. Cybercriminals are increasingly exploiting vulnerabilities introduced by poorly-trained employees to attack companies' valuable systems and data. Recent research indicates most data breaches are enabled by employees that lack adequate security awareness.

As cybercriminals continue to increase the frequency and sophistication of attacks, companies must find new, creative, and effective ways to improve employee security awareness.

Gamification to the Rescue!

Gamification is the use of game mechanics and game thinking to engage users in solving problems and motivate them by introducing elements of competition and reward. Gamification techniques leverage our natural desires for socializing, learning, mastery, competition, achievement, status, self-expression, altruism, closure, or simply our response to the framing of a situation as game or play. Many companies have been using forms of gamification to assist

with onboarding and customer engagement, but they now realize the benefits are equally applicable to security awareness training.

A study by Pulse Learning found that 75 percent of participants would be more motivated and productive if their learning curriculum was more like a game. The study also noted the benefits of gamification, including increased engagement, improved motivation, better performance, and enhanced productivity.

How Tevora Uses Gamification for Security Awareness Training

Our clients come to us on an annual basis for the latest in security awareness trends and training. Unlike the typical boring PowerPoint training, we have always prided ourselves in making security awareness training engaging by telling real-life stories and relating it to real news headlines. While our clients have appreciated these efforts, we felt we could do more. Using a combination of gamification, interactive content, and traditional teaching, we have significantly improved our cybersecurity training effectiveness. As a result, we now find that clients are much more proactive in their approach to cybersecurity and receptive to security awareness training.

We lead your team through an interactive slideshow peppered with tips and tricks for protecting your systems and data. True/false, multiple-choice, and fill-in-the-blank questions are posed to participants between slides, and team members compete with each other by answering via mobile app or web browser. Participants are scored after each question based on the speed and accuracy of their answers. Excitement builds dramatically as the scoreboard reveals the top three scores after each question. Competitive juices flow, and users are deeply engaged as they compete for the highest score.

With apologies for the pun, gamification has truly been a game-changer for our security awareness training programs.

Elements of Successful Gamification

For anyone looking to gamify their cybersecurity training, it's helpful to understand the key elements of successful game-based training.

1. **Make it Fun:** Games are fun. Make sure your training is too. This can be easy to forget when you are heads-down designing your training.
2. **Visual Aids:** Pictures, videos, and real news articles can help drive the content home while keeping employees engaged.
3. **Reward Users**: Incentivize and motivate participants by using rewards. Rewards can be anything from virtual badges to physical gifts such as gift cards.

4. **Know Your Audience:** Provide a solid foundation for effective training by researching what employees like, what motivates them, and what devices they use most frequently. If your company uses G-Suite on Android, use G-Suite on Android in your examples.
5. **Training is Ongoing:** Training should be done at least annually. Track employee progress with badges and rewards to keep them engaged throughout their career.

Gamification is changing how organizations think about security awareness training. We believe this innovative learning technique can be an essential weapon in your company's arsenal for fighting cybercrime.

Let Tevora be Your Trusted Training Partner

Tevora's expert team has deep experience with cybersecurity and gamified training, and we would welcome the opportunity to be your trusted partner as you design, implement, and conduct gamified security awareness training.

Learn more about our training services on the Tevora website.