10 Cyber Security Awareness Education Tips

CyberTalk.org

IN TODAY'S WORLD, CYBER SECURITY THREATS ABOUND. YOU ARE THE GUARDIAN OF YOUR ENTERPRISE.

End user education is a moving target. The best end user education involves a multi-faceted approach that takes human behavior, corporate objectives, emerging threats and end user limitations into account. Moreover, it presents cyber security as a prudent means of collectively moving towards the same valuable business goal, rather than a potential hindrance or a negotiable responsibility.

Although you might already have a security awareness program, consider new ways to make it more engaging and ultimately, effective. Lasting behavioral changes, a growth mindset security culture, and improved cyber security outcomes derive from carefully constructed end user awareness campaigns and programming.

Whether you're starting from the ground up or building on an existing program, does your program include the recommendations below?

10 END USER CYBER SECURITY AWARENESS EDUCATION TIPS

1. A cognitive science-based approach. Your mission is to nudge people towards incorporating minor changes into their daily routines. Experts state that one of the best ways to build new habits is to connect them with existing habits. Consider how this can be accomplished in relation to cyber security.

2. Start small. Habits and new mindsets take time to develop. Avoid overwhelming employees, especially new hires, with cyber security communications or content.

3. Reward good habits. Rewards are key in habit formation. Rewards can be built into security software programs (in the form of badges or achievement thresholds), or they can be physical, ranging from points, to cool swag, to team lunches.

4. Make end user compliance simple. Policies can be so complex as to be self-defeating. In these cases, users often want to ignore them and take shortcuts to navigate around them, potentially compromising security in the process.

5. Keep it simple on your side and avoid security team burnout. Deploy 1-click style user education software programs that can scale and that offer seamless, automated delivery year-round. This removes a time-consuming component of end user info security education and ensures that your security team can focus on other priorities.

6. Deploy software programs with strong backend metrics offerings. After program deployment, get granular insights into what worked, what didn't and why. Some cyber security training programs come with customizable and boardroom-ready reports.

7. Create a programming calendar. Inconsistent programming can leave both executives and rank-and-file employees confused. No one appreciates programming that's dumped on them at the last-minute, especially if there is a completion deadline. Ensure that everyone in your organization knows what to expect and when.

8. Consider creating an internal cyber security engagement site. This is where you can keep a multitude of cyber security resources that employees can refer to at any time. You can also include information about who to reach out to if employees have basic questions or need assistance.

9. Provide role-based cyber security training. Different roles, different threats. The HR department should understand threats posed by disgruntled employees or employees departing the organization on difficult terms, while the finance department should understand how to spot and report payroll schemes.
10. Focus on phishing. As many as 90% of cyber security breaches start with a phishing email. Deceptive phishing tactics commonly fool employees and deserve an outsized portion of everyone's attention. *For phishing program development insights, see below.*

CYBER SECURITY AWARENESS PHISHING PROGRAM DEVELOPMENT

- Simulate the most sophisticated phishing threats. Enable your employees to identify emerging, real-world phishing threats through simulated, same-domain spoofing techniques, typosquatting and more.
- Use any of 1,000 existing phishing templates to help inform employees about the most dangerous phishing lures.
- Pre-built automated reports can help you obtain granular insights into the efficacy of your campaign. Plus, automated reports translate to boardroom-ready charts, easy-access to compliance data, and other essential, must-have metrics.

Get a custom SmartAwareness demo here. For more info, contact smartawareness@checkpoint.com.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com