Top 10 Tips for Effective Security Awareness Coaching Programs

SecurityAdvisor

Cybersecurity is everyone's responsibility, yet many employees are unaware of how their online behaviors pose risks for their organizations. Security awareness coaching teaches employees how to identify and remediate cyber threats, including phishing, malware, and social engineering attacks. With effective cybersecurity education – *and the right approach* – organizations can equip their human workforces to combat the deluge of security threats and measurably reduce risk.

TEN TIPS

Follow these tips to establish not only a sound security awareness program, but one that's truly effective in promoting behavioral change and reducing costly security incidents.

1. **Help Employees Understand the Importance of Cybersecurity Safety:** People are the first line of defense for organizations and need to be prioritized. Beyond understanding the specific attacks they face, employees should also understand why security is essential to business and their role in the organization's security posture. Employees are less likely to change their behavior until they understand why security training is required and its importance. **Empowering employees with the knowledge that they are the best defense against cyberattacks fosters a sense of personal responsibility and, ultimately, a cyber immune culture.**
2. **Leverage Engaging Content:** A single 30-minute video or a series of generic email-based phishing simulations does not reduce data breaches. SecurityAdvisor's proprietary research shows that there's a short-term benefit to using traditional courseware training, as the first campaign has a click rate of about 25% and whittles down to about half of that by the fourth campaign. **To make lasting behavior change, learning content must be engaging to prevent employees from multi-tasking and ignoring the content altogether.**
3. **Match Training to Individual Roles and Behaviors:** Sharing generic assessments with all employees leaves no room to address the learning needs of each individual, which varies from person to person based on their roles, risk profile, aptitude, exposure, tenure, and behavior. **Training should be tailored to real-life scenarios each person will experience based on their specific experience and needs.**

TEN TIPS

1 Help Employees Understand the Importance of Cybersecurity Safety
2 Leverage Engaging Content
3 Match Training to Individual Roles and Behaviors
4 Customize Training with Existing Tools
5 Create Digestible Content
6 Share Reminders of Risk in Real Time
7 Make Training an Ongoing Practice
8 Create a Safe Place for Employees to Make Mistakes
9 Ask for Employee Feedback:
10 Measure Employee Progress

4. **Customize Training with Existing Tools:** Instead of relying on generic exercises, businesses can use data from existing security technology, IT, and HR tools to customize coaching based on employees' real-world behavior. **Organizations can also deliver educational content via Slack, Teams, or another collaboration tool for employees who are overwhelmed with email fatigue.**
5. **Create Digestible Content:** Most employees are required to set aside time from their daily responsibilities to make time for awareness training – impacting productivity and something which they can grow to resent. **Organizations that share bite-sized modules of content during 'teachable moments' rather than forcing employees to take mandated seminars, see greater than 90% employee engagement versus less than 25%with traditional training.**
6. **Share Reminders of Risk in Real Time:** An employees' ability to identify and remediate cyber threats diminishes over time, so they should be alerted to potential risky behavior before they act. **Sharing information about a specific threat in the exact moment of risk – for example, when an employee clicks on a link, visits a risky website, or installs an insecure app – helps them understand in real-time when they are about to do something potentially harmful.**
7. **Make Training an Ongoing Practice:** Security awareness training is most useful when delivered as routine and ongoing practice. One annual training is not enough to see real improvement in awareness, and irregular security awareness trainings offer no measurable ROI outside of fulfilling a compliance mandate. **Long-term behavior change results from consistent training and engagement.**
8. **Create a Safe Place for Employees to Make Mistakes:** Training should be a positive experience that helps employees learn. More often than not, blaming employees will make them less likely to report errors in the future. Attacks are only becoming more sophisticated and anyone can easily fall for legitimate-looking attacks. **Creating a security culture that encourages reporting mistakes – and then offering additional contextual training once they occur – will ultimately reduce mistakes from happening.**
9. **Ask for Employee Feedback:** Receiving feedback from employees on the training you deliver– including the relevance of the training and the usefulness of the content is critical. **This helps security managers understand what tactics, techniques and teachable moments are resonating with employees.**
10. **Measure Employee Progress:** To ensure coaching initiatives accomplish their core purpose of reducing incidents and preventing attacks from spreading, security leaders should establish a methodology to quantify employee progress. **This entails identifying high-risk users within the organization, keeping track of the number of times an employee engages in an action that triggers the security microlessons, and measuring their aptitude for preventing specific attack methods over time.**

For organizations seeking to effectively raise awareness of threats, reduce malware detections, and reduce security operations cost, investing in intelligent security awareness coaching is crucial. Creating learning content that is engaging, relevant, conducted in bite-sized increments over time, and measurable is critical for security leaders who want to run effective security coaching programs.

Following the best practices outlined above, SecurityAdvisor's patented cyber immunity platform is proven to modify human behavior and deliver measurable security outcomes that help employees become the best line of defense.