GO ON THE OFFENSE WITH CYBERSECURITY EDUCATION FOR EMPLOYEES

From falling for a phishing email, to failing to patch or update software or reusing weak passwords, it's easy to see why human error is the leading cause of cyber breaches. Attack patterns only continue to become more sophisticated, and data breaches continue to cost more year over year, with the average cost of a data breach expected to reach $5 million in 2023.

The fallout from cyberattacks can cause stress for employees at affected companies and, in worse case scenarios, impact employee job security. A study by email security company Tessian estimated that one in four employees lost their jobs within 12 months of making a mistake that led to a cybersecurity breach.

A study by email security company Tessian estimated that one in four employees lost their jobs within 12 months of making a mistake that led to a cybersecurity breach.

In today's world where many business operations rely on interconnected virtual systems, employees at every level need to have the foundational knowledge to be able to identify and help prevent cyberattacks. Comprehensive, routine cyber security awareness training for your employees should be provided as a first line of defense. Additionally, when you're ready to purchase cyber insurance for your business, most cyber carriers require you to do so before even considering offering coverage.

Let's look at some areas of learning and best practices you should take into consideration when implementing employee cybersecurity awareness training at your business:

- **IT POLICIES**
  Work with your IT department to develop clear cybersecurity policies (password safety, VPN use, work from home protocols, etc.) and ensure your training covers a review of them.

- **ACCOUNTABILITY**
  Explain employees' responsibilities and accountability when using company issued devices, continually emphasizing the importance of data security and legal obligations to protect confidential information.

- **PASSWORDS**
  Train employees about password best practices, including how to choose a strong password, and the importance of not reusing passwords.

- **NOTIFICATION PROCEDURES**
  Should a breach happen, employees need to know how to report the incident to your IT team.

- **UNAUTHORIZED SOFTWARE**
  Inform employees that they shouldn't download unauthorized software on company devices.

- **SUSPICIOUS LINKS**
  Training should show employees how to identify and avoid suspicious links in web browsers, documents, and email.

- **RESPONSIBLE EMAIL USE**
  Employees need to learn the tell-tale signs of email scams, which can include unusual spelling, an unknown sender, or an unexpected, urgent request for credentials or funds.

- **SOCIAL ENGINEERING AND PHISHING**
  Your training needs to help employees recognize the tactics hackers use in these attack types.

- **PHYSICAL SECURITY**
  Tell employees to safeguard their computers by locking them if they walk away.

- **SIMULATE ATTACKS**
  Demonstrating different cyberattack types can help employees better identify them in real-life scenarios.

- **INTERACTIVE MODULES**
  If employees aren't engaged in their training, it won't be as effective. Breaking up your training into shorter, interactive modules encourages meaningful engagement with the information they need to know.

- **CONTINUOUS TRAINING**
  One time is not enough: train your employees thoroughly and regularly.

Though employees might feel like there's a never-ending laundry list of security protocols that they need to keep up with, a lax approach to your company's cybersecurity isn't the answer. By employing an engaging cybersecurity awareness training program, you're empowering your employees by helping them understand the importance both in their specific roles and for the company at large. Employee education is critical for any organization that wants to establish a culture of cybersecurity, as it can help prevent costly mistakes in the future.

Contact us about how to best implement an effective cybersecurity training program and for guidance about your cyber insurance coverage needs.

Contact Us