Minimize Risk with Effective Cyber-Security Training

Employee security training tips from Dena Kamel

You can (and should) install firewalls and antivirus, define email filters and policies and even deploy advanced threat detection. But if you fail to fully address human error, you have missed the most vulnerable aspect of information security. The solution lies in delivering effective cyber-security training, a goal that can prove difficult to achieve.

Employees inadvertently create security problems by using weak passwords, clicking malicious links, failing to properly delete data and ignoring other basic rules of data protection. Providing ongoing, engaging and pertinent training can potentially save your organization millions of dollars in data breach remediation.

Emphasize the "Why"

When employees understand not just the security policies, but also the reasons behind those rules, they are more likely to follow them. Why should I care about password guidelines and email safety? Because damage from cyber-attacks can prove catastrophic, costing you your job, and because the responsibility for cyber-security lies with every person in the company who touches data.

For example, in one of the most publicized data breaches of 2019, international hackers gained access to the Citrix network by exploiting weak passwords. And in an infamous incident that changed the face of the U.S. presidential race, staffers on Hilary Clinton's campaign fell victim to targeted spear-phishing attacks.

Make sure employees know how to recognize potential threats. Then give them the tools to counter those threats and teach them how to use them. They represent the first line of defense, and they need to know what they face.

A Multi-faceted Approach to Effective Cyber-Security Training

Everyone knows how not to conduct training. Simply herd employees into a conference room once a year and watch them fall asleep during a two-hour lecture. Instead of a single annual seminar, conduct ongoing training and integrate security awareness into company culture. Your approach could include:

- Ongoing formal training – Limit sessions to one hour, make them interactive and provide refreshers throughout the year. Show real-life examples. Consider online training that employees can complete at their desks.
- Visuals – Visual reminders throughout the workday provide just-in-time hints. For example, hang posters in the hallways or elevator or give employees a stress ball embossed with a security reminder.
- Special events – Consider launching a security week, complete with t-shirts, fliers and security-related contests.
- On-line training – Use quick 5 to 10-minute sessions that can track and report on who views and takes the tutorial, ensuring participation.

Focus Training for Impact

Resist the temptation to overload employees with information. Instead, focus each training event on one or two main themes, such as recognizing phishing scams or safe file-sharing.

In addition, keep in mind that effective cyber-security training targets information according to the audience. The billing department, human resources and IT all approach data from different angles. Target training according to the needs and priorities of each area.

Be sure to include cyber-security in onboarding training for new employees. Also consider ongoing validation of your training through synthesized phishing attacks which can track vulnerabilities and measure improvement.

If You Can Only Teach Three Things, Start with These

You have a limited window of opportunity to provide training. Begin with the essentials.

1. **Do. Not. Click.** – Do not click on attachments or links unless you were expecting them. Even though an email looks like it came from a trusted source, verify the source before opening an attachment.

2. **Be careful what you write or share** – Never send financial or other sensitive information through email. And if you must communicate passwords, use a separate means of communication. For example, send the password-protected document in email but deliver the password via text or phone call.

3. **Use strong passwords** – When it comes to passwords, keep them long, preferably at least 10 to 16 characters. The National Institute of Standards and Technology (NIST) suggests password phrases. But avoid common phrases or personal information and never, ever store passwords in your browser.

Keep in mind that these same rules apply not just to email, but also to texts and social media. Your entire phone, including personal contacts and apps, impacts the security of the organization.

Ensure Success with Expert Help

For over 20 years, Messaging Architects has helped organizations protect their information assets and provide effective cyber-security training. With deep expertise in data compliance and email security, we can help you address the human factor in your comprehensive approach to information security.

Dena Kamel is the Consulting Director at Messaging Architects and has worked with the company for nine years. While directing the work of the project management and consulting teams, she also manages large or client-sensitive projects. Kamel combines a background in accounting with a talent for issue resolution. Her favorite part of her job is turning problems around and seeing the client's satisfaction when a project gets back on track.