Bernard Robinson & Company

IT Risk Advisory Services

Cybersecurity User Training Overview

As Certified Public Accountants and Advisors, BRC is proud to outline our services focused on Cybersecurity User Training. Phishing, Social Engineering, Spear Phishing, Business Email Compromise……whatever the term you use or are most familiar with; this type of attack is "behind 90% of successful cyberattacks".[1] Phishing takes advantage of the idea that the human user is still the weakest link in the data security chain. Despite the increased press and awareness of successful attacks (Mecklenburg County, Dec 2017), Verizon's 2017 Data Breach Investigations Report found that roughly 7% of people will automatically click on any attachment or link they receive – and 25% of them were tricked into clicking more than once. The same Verizon report found that two-thirds of all malware (malicious software) attacked the computer systems via email attachments. While only 7% of users would automatically click on an attachment, an Intel Security survey in 2015 found that 97% of users could NOT tell the difference between an authentic email and a well-done fake one.

It is not a matter of if, but when. However, with proper training users can avoid falling for the phishing scheme. Users can also be trained to recognize when a mistake happens, how to respond and who to call as soon as the mistake happens to mitigate the damage. A culture of security can be developed in your company.

Cybersecurity User Training Services

- Launch an effective awareness campaign across the organization to help keep the potential of phishing on the employees minds by providing recurring and visual reminders about common risks, best practices, and the importance of security to the organization
    - Provide on-site or online role-based training to users across the organization, from the C-suite to accounting, HR, IT staff, administrative workers and every other group to ensure that each employee understands the risks, their potential exposure in their specific role, and ways to respond if they suspect an issue.
    - Conduct semi-annual simulated social engineering phishing attacks to evaluate the employee's susceptibility to such tactics
- Review / help develop clear security policies and procedures. Facilitate communication to ALL employees
    - Have the employees sign a document outlining their own responsibility to uphold those standards on the company's infrastructure and equipment
- Encourage the use of two-factor authentication to mitigate the misuse of stolen passwords

Bernard Robinson & Company

Benefits to Clients

- Cybersecurity becomes a business process.
- **Increased Security**. Phishing simulation provides quantifiable results that can be measured. These measurements allow improvement to be identified and tracked.
- **Visibility**. With the comprehensive reporting, key stakeholders can understand the security weaknesses. This reporting helps obtain executive management buy-in for current and future security initiatives.
- **Demonstrated Responsibility**. As responsible organizations, you need to demonstrate to your stakeholders that you understand the current threat environment and are taking steps to reduce risk. By ignoring the threats from social engineering attacks, you could be exposing yourselves to litigation.
- **Improved Training Retention**. Employees can receive training on what to do and what to avoid, but until an employee experiences it, their actions are unknown. After seeing what is capable, employees understand and are more security conscious. This fact will help improve training retention.
- **Net Reduced Training Cost.** By pinpointing employees who are more susceptible, such as via the Repeat Failures Report, additional training can be provided to those employees without the cost and burden to other employees.

BRC has created a multi-faceted, risk-based, scalable approach to your cybersecurity concerns.

Let's get started today! For more information please contact: Ben Hunter III, CPA, CITP, CISA, CRISC, CFE at (336).294.4494 (bhunter@brccpa.com) or any of our dedicated service line leaders.

1. Former Rep. Mike Rogers, R-Mich., who served as chairman of the U.S House Intelligence Committee from 2011 to 2015, speaking at the U.S. Chamber of Commerce's cybersecurity summit in late 2015.