Risk Advisory Services

Cybersecurity User Training

As Certified Public Accountants and Advisors, BRC is proud to outline our services focused on Cybersecurity User Training. **Phishing** is behind 80-90% of successful cyberattacks. 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, each year Verizon's Data Breach Investigations Report continues to find that phishing continues to play a very large role in incidents and breaches alike. The same Verizon reports find that the majority of all malware entered the IT Environment via email. The Willie Sutton Rule states: "When diagnosing, first consider the obvious." Therefore, criminals phish because email is where their targets are reachable.

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.

BRC can help develop a culture of security in your company.

Cybersecurity User Training Services

- Launch an effective awareness campaign across the organization to help keep the potential of phishing on employee 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 all units of the organization to ensure that each employee understands the risks, their potential exposure, and appropriate responses if they suspect an issue.
    - Conduct monthly, 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 and outline their responsibility to uphold those standards in a contractual document
- Encourage the use of two-factor authentication to mitigate the misuse of stolen passwords

brc 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.

Let's get started today. For more information please contact: Kyle Corum, Partner, CPA, CFE at (336).232.4414 (kcorum@brccpa.com) or any of our dedicated service line leaders.

brccpa.com

Bernard Robinson & Company