Postlethwaite & Netterville

Cyber Security: Phishing & Employee Education

By Michael Richmond

Recently, an employee of one of our clients received an email from the CEO asking for her cell phone number so she could complete a task for him. Luckily, she knew that he already had her cell phone number, and had been trained to be very wary of emails like this. But not all employees are as prepared for these situations.

Consider these statistics from the Verizon 2018 Data Breach Investigations Report, an in-depth annual cyber security study.

- Phishing is the #1 delivery vehicle for ransomware and other malware, accounting for 93% of network breaches.
- Users only reported 17% of phishing campaigns to company leadership.
- Oftentimes, they don't even know they've been a victim, because more than 60% of breaches take months to discover.

So, what are these cyber criminals looking for? They are looking for the same things they always have: data and money. And they often find it where you least expect: 58 percent of malware attack victims are categorized as small businesses.

The risk of companies falling victim to employees' behavior in responding to phishing scams is astronomical.

The risk of companies falling victim to employees' behavior in responding to phishing scams is astronomical, and while technology solutions are critical, they are not enough. But there is hope, and it lies at your employees' fingertips.

While results will vary from company to company, some studies have shown that a comprehensive employee training program can yield over 60 percent improvement in employee avoidance of phishing attacks in the first 30 days alone. The programs include components such as baseline assessments, identification of risk areas, employee training, ongoing testing, and re-education for specific individuals who are most susceptible to risky clicking.

Going back to our original example, the employee who received the phishing attack had been a part of a comprehensive, multi-pronged training program designed to keep phishing top of mind. In this instance, the cybercrime was avoided. Without the comprehensive cyber security training program, the dutiful

employee may have simply complied with the request of the “CEO,” opening the door for cyber criminals to enter. Would your employees know what to do?

For more information on employee cyber training services, contact our Technology Services Group.