FrankelZacharia LLC
TECHNOLOGY SERVICES

Your Biggest Cybersecurity Risk: Your Employees

Training … Awareness … Repeat. Cybercriminals work around the clock to detect and exploit vulnerabilities in your business' network for nefarious gains. The only way to counter these hackers is by deploying a robust cybersecurity posture that's built using comprehensive security solutions. However, while you're caught up in doing this, there is a possibility you may overlook mitigating the weakest link in your fight against cybercriminals — your employees.

With remote work gaining traction and decentralized workspaces becoming the new norm, all businesses must strengthen their cybersecurity strategies to counter human errors and data breaches perpetrated by malicious insiders. All employees, regardless of their position/title, can expose your business vulnerabilities to cybercriminals.

Implementing routine security awareness training for employees can help you prevent a vulnerability from escalating into a disaster. As the first line of defense against cyberattacks, your employees must be thoroughly and regularly trained to identify and deflate potential cyberthreats.

Why Employees Pose a Risk to Businesses?

According to IBM's Cost of a Data Breach Report 2020, 23% of data breaches in an organization occurred because of human error. An untrained employee can compromise your business' security in multiple ways. Some of the most common errors committed by employees include:

1. **Falling for phishing scams**: With the onset of COVID-19, hackers masquerading as the World Health Organization (WHO) tricked people into clicking on malicious links and sharing sensitive information. Cybercriminals are using improved techniques, like spoofed emails and text messages, to propagate the ongoing scam. Your employees must be well-trained to counter it.
2. **Bad password hygiene**: A section of your employees might reuse the same password or a set of passwords for multiple accounts (business and personal), which is a dangerous habit that allows cybercriminals to crack your business' network security.
3. **Misdelivery**: Even slight carelessness can lead to an employee sending sensitive, business-critical information to a hacker. Such an act can cause lasting damage to your business, which is why you must be prepared to counter it.
4. **Inept patch management**: Often, employees can delay the deployment of a security patch sent to their device, which can lead to security vulnerabilities in your business' IT security left unaddressed.

The bottom line is that with cybercriminals upgrading their tactics every day and exploring vast options to trap your employees, security awareness training has become more important than ever before.

Security Awareness Training: An Essential Investment

A one-time training program will neither help your employees repel cyberthreats nor help your business develop a security culture. To deal with the growing threat landscape, your employees need thorough and regular security awareness training.

You must never back out of providing continual security awareness training to your employees just because of the time and money you need to invest in it. The return on investment will be visible in the form of better decision-making employees who efficiently respond in the face of adversity, ultimately saving your business from data breaches, damage to reputation, and potentially expensive lawsuits. The following statistics highlight why you must deploy regular security awareness training and consider it a necessary investment:

- Eighty percent of organizations experience at least one compromised account threat per month. [1]
- Sixty-seven percent of data breaches result from human error, credential theft, or social attack. [2]
- Since the start of the COVID-19 pandemic, phishing attacks have gone up by 67 percent. [3]

Expecting your employees to train themselves on how to detect and respond to cyberthreats certainly isn't the best way to deal with an ever-evolving threat landscape. You must take on the responsibility of providing regular training to your employees to ensure you adequately prepare them to identify and ward off potential cyberattacks.

Every employee must realize that even a minor mistake can snowball into a terrible security disaster for the company. They need to understand that your business' cybersecurity is also their responsibility.

You can transform your business' biggest cybersecurity risk – your employees – into its prime defense against threats by developing a security culture that emphasizes adequate and regular security awareness training.

Making all this happen will require continued effort and may seem like an uphill climb, but with the right partner by your side, you can easily integrate security awareness training into your business' cybersecurity strategy. The first step towards training and empowering your employees starts with an email to us. Feel free to get in touch anytime.

FZTS Managed Security Services

In addition to our cybersecurity reviews and personalized annual security awareness training sessions, FZTS also provides a package of managed security services:

Password Management

Using MyGlue, your company can store and share passwords in an encrypted fashion. You can also share security policies, procedures, and documentation with staff, separating these from general storage and bringing focus to important security elements.

Dark Web Monitoring

Dark Web Monitoring combines human and sophisticated Dark Web intelligence with search capabilities to identify, analyze, and proactively monitor for an organization's compromised data or stolen employee credentials.

Phishing Testing

BullPhish ID™ complements other security measures with simulated phishing attacks and security awareness training campaigns to educate employees, making them the best defense against cybercrime.

Security Monitoring

Ongoing security monitoring provides a weekly “double check” to ensure anti-virus and patching are working and to help discover potential misconfigurations. This combines machine learning and intelligent tagging to identify anomalous activity, suspicious changes, and threats. When an issue is detected, an alert is generated and delivered along with potential steps for remediation.

If you have questions or are ready to implement a training program, give us a call today!

Tim Weidman – 402-963-4375 – tweidman@fzacpa.com

Sources:

1. McAfee Cloud Adoption & Risk Report
2. Verizon 2020 Data Breach Investigations Report
3. Security Magazine Verizon Data Breach Digest