EMPLOYEE ✓ CYBERSECURITY TRAINING

EMPOWERING YOUR EMPLOYEES TO CULTIVATE A CYBER-RESILIENT WORKFORCE

With the constant emergence of new cybersecurity risks, it's more important than ever for business owners to maintain proactive security measures. When it comes to cyberattacks, employees often are considered the weakest link of an organization's digital defenses. One wrong move, a moment of oversight or an overall lack of cybersecurity awareness can lead to disastrous outcomes.

This guide is designed specifically to equip you, the MSP, with insights and actionable guidance to help businesses establish and strengthen cybersecurity culture within their organizations. By offering invaluable assistance in crafting, implementing and managing effective employee cybersecurity programs, you can empower businesses to proactively mitigate risks and fortify their security posture. This ultimately ensures employees are better prepared to identify and respond to the latest cyberthreats.

Join us as we uncover the importance of addressing the human element in cybersecurity and how you can play a part in fostering a culture of security in the businesses you partner with.

POWERED SERVICES PRO

PART 1

THE 'WHAT' AND 'HOW' OF CYBERSECURITY AWARENESS TRAINING

Understanding the essentials and effective strategies of cybersecurity awareness training is paramount for ensuring you're providing first-rate guidance to your clients. If you're not qualified to implement the training types mentioned below, consider teaming up with a third party that can assist. The section below highlights crucial training topics and how to execute each effectively.

WHAT: PHISHING AWARENESS

How: Teach employees to identify and avoid suspicious emails, links and attachments. Implement an automated phishing defense platform to protect against cybercriminals posing as trusted contacts.

WHAT: PASSWORD SECURITY

How: Promote good password hygiene, password managers and multifactor authentication (MFA). Provide regular updates on emerging password security practices and implement tools to reinforce secure passwords.

WHAT: SOCIAL ENGINEERING

How: Raise awareness about manipulation techniques used to trick employees into revealing sensitive information or providing unauthorized access. Emphasize the importance of verifying requests and the potential consequences of falling for social engineering attacks.

WHAT: DATA PROTECTION & PRIVACY

How: Reinforce the importance of safeguarding sensitive data, following regulations and using secure file-sharing methods. Tailor content by providing specific examples relevant to the data types handled by different departments.

WHAT: INTERNET SAFETY

How: Educate employees on safe browsing practices to minimize the risk of malware and phishing attacks. Develop engaging content through real-life examples and interactive exercises to illustrate the importance of internet safety.

WHAT: MOBILE DEVICE SECURITY/BYOD

How: Ensure employees follow security best practices even on personal devices used for work purposes. Address the latest threats targeting mobile devices and highlight the importance of regularly updating software.

WHAT: SOCIAL MEDIA RISKS

How: Educate employees about the dangers of oversharing and raise awareness around social engineering attempts through social media. Measure effectiveness and gather feedback by assessing employees' understanding and behaviors related to social media security.

WHAT: INCIDENT REPORTING

How: Encourage employees to promptly report possible security incidents and suspicious activities. Evaluate the incident reporting process's effectiveness and provide transparent reporting procedure guidelines.

WHAT: PHYSICAL SECURITY MEASURES

How: Educate employees on protecting devices, workstations and other sensitive areas from physical threats. Incorporate physical security practices into the overall cybersecurity awareness program.

POWERED SERVICES PRO

PART 2

SUSPECT ZERO: EMPLOYEES IN THE CROSSHAIRS OF CYBERATTACKS

Cybercriminals exploit employees as prime targets for malicious activities for a myriad of reasons. By delving into why this is the case, it's easier to identify and leverage resources that can help businesses take their employees from vulnerable to vigilant.

EMPLOYEES ARE A KEY FOCUS FOR CYBERATTACKS DUE TO:

Their lack of awareness surrounding common cybersecurity threats, techniques and best practices.

Security awareness training can affordably reduce cyber risks caused by human error.

Their access to critical systems, sensitive data or administrative privileges that cybercriminals want to get their hands on.

Identity and access management (IAM) solutions ensure access from the correct people from the right devices and locations.

The potential of being fooled by social engineering tactics. These attack methods are highly effective at manipulating employees into disclosing sensitive information, sharing credentials or taking actions that compromise an organization's security.

Anti-phishing software acts as protection against numerous digital threats that organizations face daily.

The bring your own device (BYOD) trend. This movement has led to increased access to business information and systems from personal devices that often lack proper security controls.

Reduce risk and cost of downtime that can be tied to BYOD through remote monitoring and management (RMM) solutions that allow you to monitor, manage and secure any endpoint from anywhere.

Remote/hybrid work raises additional security challenges, such as unsecured home networks, shared devices and distractions, that can impact an employee's focus on cybersecurity best practices.

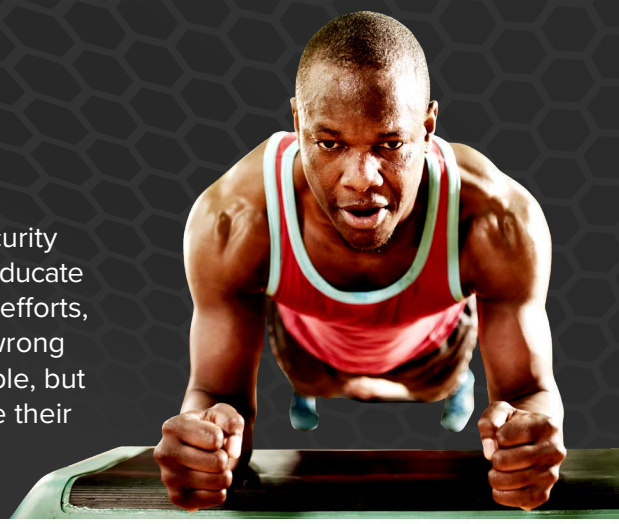
Secure Access Service Edge (SASE) can be implemented to ensure secure and fast network access to remote employees.

POWERED SERVICES PRO

PART 3

FOOL ME ONCE, TWICE, THRICE

Consistency is often a significant hurdle when it comes to cybersecurity training. To reduce cyberattacks, organizations need to continuously educate employees on threats, exploits and vulnerabilities. Despite training efforts, employees can still fall prey to malicious actors by clicking on the wrong things. Complete elimination of these incidents is not always possible, but educating your clients on the following active measures can reduce their frequency.



Approach cybersecurity training as a regular, ongoing part of employees' job requirements

- Cybersecurity training is not something that can be done one time successfully – it's an ongoing process. Employees need constant reminders of new threats, updated resources and modern mitigation techniques. Training should be a requirement for all employees.

Deliver training that is both engaging and relevant

- Training programs are often monotonous slideshows or dull videos. People tend to daydream during these because there is no real-life connection. Use real examples relevant to every employee's daily workflow to keep them engaged in the content and messaging.

Measure actively rather than passively

- You cannot gauge how well a cybersecurity training program performs if you only monitor the number of emails sent or simulations completed yearly. Behavior metrics, such as clicks or open rates for phishing simulations, are more helpful in determining who clicks on them, what type of content gets the most clicks and why they fail.

Remove the finger-pointing

- Training is not an opportunity to point fingers and assign blame. For many, it's often a learning experience and should be treated as such. Present the outcomes of a failed cybersecurity training incident to the business and discuss lessons learned to help protect the organization in the future.

Lack of support from leadership

- If the importance of security and a training program does not come from the top, there is an issue. The security of data and sensitive information should be the top priority of everyone, starting with the leadership team.

Ask for help

- If an incident occurs, create a culture where reporting incidents or issues is not seen negatively. Instead, use them as opportunities to teach others how to prevent these problems in the future.

Maximize your business opportunities by scheduling a coaching session with your Channel Enablement Manager.

During your appointment, they'll work with you to develop a strategy that leverages campaign materials and promotes your ability to help businesses build a strong security culture.

POWERED SERVICES PRO