Cyber Resilience Begins With Raising Security Awareness

A security-savvy team is a critical building block for cyber resilience - In chess, two rows of pieces are placed on either side of the board. These rows consist of eight pawns as the first line of defense against the enemy. The rest of the pieces behind them can move about effectively, depending on how you direct your pawns. But what if you can't always dictate how your pawns move? What if the enemy could influence how your pawns behave? Sounds like an easy win for your opponent, right? Well, that's what happens with email-based phishing and social engineering scams, such as business email compromise attacks. There's only one way to solve this problem — **security awareness training**.

In this current digital-first business landscape, the biggest threat to an organization comes from within. While malicious insiders are a real threat, unintentional actors — also called pawns or goofs — cause over 65% of reported insider incidents by interacting with a phishing message. In this blog, we'll delve into the undeniable need for comprehensive security awareness training and its role in empowering a company's management and employees to improve their resilience against today's ever-evolving cyber threat landscape.

Top three phishing simulation emails that successfully drew clicks

1. Office 365: "Suspicious Login" with 10,879 clicks.
2. FedEx: "Package Delivery" with 6,535 clicks.
3. Google Docs: "Invitation to Edit" with 4,492 clicks.

Top three phishing simulation campaigns that captured credentials and data

1. FedEx: "Package Delivery" with 2056 captures.
2. Office 365: "Suspicious Login" with 1736 captures.
3. COVID-19: "SharePoint Webinar" with 1440 captures.

Clueless Employees Create Security Incidents - Cybercriminals have become more adept at creating sophisticated, convincing emails and scams that can hardly be distinguished from authentic emails or SMS texts from a trusted source. Over the last five years, companies across the globe have lost over $43 billion due to BEC attacks. If that statistic isn't scary enough, Microsoft discovered that for every 1,000 mailboxes, bad actors averaged 104 BEC attacks weekly. That's about 40 attacks every business day. These numbers are based on mid-market enterprises (MME) with a little over 1,500 employees. It's safe to say that the larger the organization, the greater the number of attempted attacks. That still isn't the biggest problem, though. The main challenge to an organization's IT security team revolves around the fact that employees don't report security incidents — and this is a growing trend. Employees simply aren't equipped to properly handle such email-based cyber threats, which inevitably increases the chances of a data breach. Training fixes that problem. Here are five employee behavioral trends currently rampant across all industries — particularly in the transportation, automotive and healthcare sectors — that can lead to a cyberattack.

- Employees report about 2% of all known attacks to their security team.
- Employees often report graymail (not to be confused with spam) as phishing, wasting a security professional's time.
- Employees assume that a peer may have reported suspicious emails as phishing instead of doing their part to minimize risk.

- Employees don't realize they might be the only target of an attack and leave it to someone else to raise an alarm.
- Employees tend to reuse passwords on corporate devices and networks as they would on personal devices that aren't as thoroughly secured. This creates an entry vector for bad actors.

It's clear that most of these issues don't require new security software implementation or a massive overhaul of corporate security policies. A simple but effective security awareness training program will educate employees on cybersecurity best practices and get them battle-ready to handle even the most innovative infiltration tactics a cybercriminal may utilize. Security awareness training is the cornerstone of establishing a strong security culture that promotes due diligence and vigilance in any organization, ultimately helping that company resist email-based cyberattacks and other dangers. It goes beyond just being a mere requirement for better compliance management. It helps employees at every level be more alert and responsible about their cyber hygiene and emphasizes accountability as well. While there are many areas to focus on when it comes to training employees on security practices and internal policies, these are the most common:

Phishing Attacks - Did you know 9 out of 10 cyberattacks begin with a phishing email? Phishing is a prevalent threat and is typically a precursor to BEC attacks. It hinges on deceiving employees into divulging sensitive information. Equipping employees with the ability to recognize telltale signs of phishing emails and links, spoofed credentials or imposter websites immediately and dramatically lowers cyber risk. With voice phishing (vishing) and SMS phishing (smishing) on the rise as well, the U.S. National Institute of Standards and Technology (NIST) frequently stresses the importance of training employees against phishing as an effective way to avoid security incidents.

Social Engineering - Social engineering is a potent threat vector, becoming more advanced by the minute. Cybercriminals may not launch a full-fledged attack immediately because it most likely won't succeed. Instead, they seek out easy-to-manipulate employees and play the long con. Biding their time, bad actors may communicate with employees under false pretenses to gain their trust. The employees may then be influenced to behave in favor of the criminals and become more likely to open any malicious emails or links shared with them. Employees must be trained to recognize manipulation tactics and understand the importance of verifying requests for sensitive information to avoid trouble

Passwords and Authentication - Employees take the responsibility of changing passwords very lightly. Reusing old passwords or retaining the same one for long periods of time can make it easier for hackers to steal your credentials. Changing passwords once every three months is a popular and effective practice followed by companies worldwide to ensure strong password hygiene among their employees. However, there's more that can be done, like implementing multifactor authentication (MFA), to significantly improve IT security.

Hybrid and Remote Working - The modern business demands remote and hybrid work readiness. Many cybersecurity guidelines highlight the significance of secure connections, regular software updates and adherence to organizational policies while working from hybrid or remote workstations. Employees need to be educated and trained on the nuances of connecting to external networks that won't always have the level of security their corporate office networks normally boast. Companies must outline clear security requirements for home network environments. They have to train remote employees to secure their home networks, protect devices and establish boundaries between personal and work activities to stay away from major risks.

Navigating Cloud Security - Cloud-based workflows have been adopted by global organizations unanimously. The benefits they offer are incredible but, at the same time, open several channels of risk to a business. Employees need to understand the security responsibilities they share between themselves, the company and their peers. Training familiarizes them with secure data handling and their organization's chosen cloud security controls and policies.

Use of Personal Digital Assets - With mobile devices serving as extensions of the workplace, the Cybersecurity and Infrastructure Security Agency (CISA) emphasizes the need for securing them. Employees must learn to set strong passcodes, enable encryption and avoid unsecured networks to thwart potential breaches. Connecting such devices to any public network could also increase the risk of a cyberattack.

Social Media - There are over 1.4 billion attacks launched via social media platforms every month. Bad actors leverage social media as an attack surface, attempting to manipulate employees. Through seemingly harmless online polls or sweepstakes, cybercriminals can obtain credentials. The workforce needs to be educated about oversharing, recognizing fake accounts and adhering to company social media policies.

Removable Device Management - How the workforce manages their hardware plays an important role in security. NIST has specified guidelines on this matter as well. Improperly used removable media can compromise an organization's security. Educating employees about the risks posed by USB drives and external devices and implementing policies for their controlled usage can make all the difference. The current business landscape demands a well-rounded approach to security awareness training, and educating employees on these topics empowers them to be proactive defenders of their organization's security and their own privacy.

Security awareness training, while offering an incredible layer of protection against bad actors, comes with its own set of challenges. Carrying out enterprise-wide training on cybersecurity — a facet of technology that evolves in the blink of an eye — places a lot of strain on the professionals tasked to do the job. Updating content to stay relevant with the latest trends, motivating and engaging employees to complete the training and improving knowledge retention are the biggest challenges companies face when effectuating security awareness training. However, a professional IT support team can help you navigate these challenges and take your cyber resilience to the next level with efficient and affordable security awareness training.