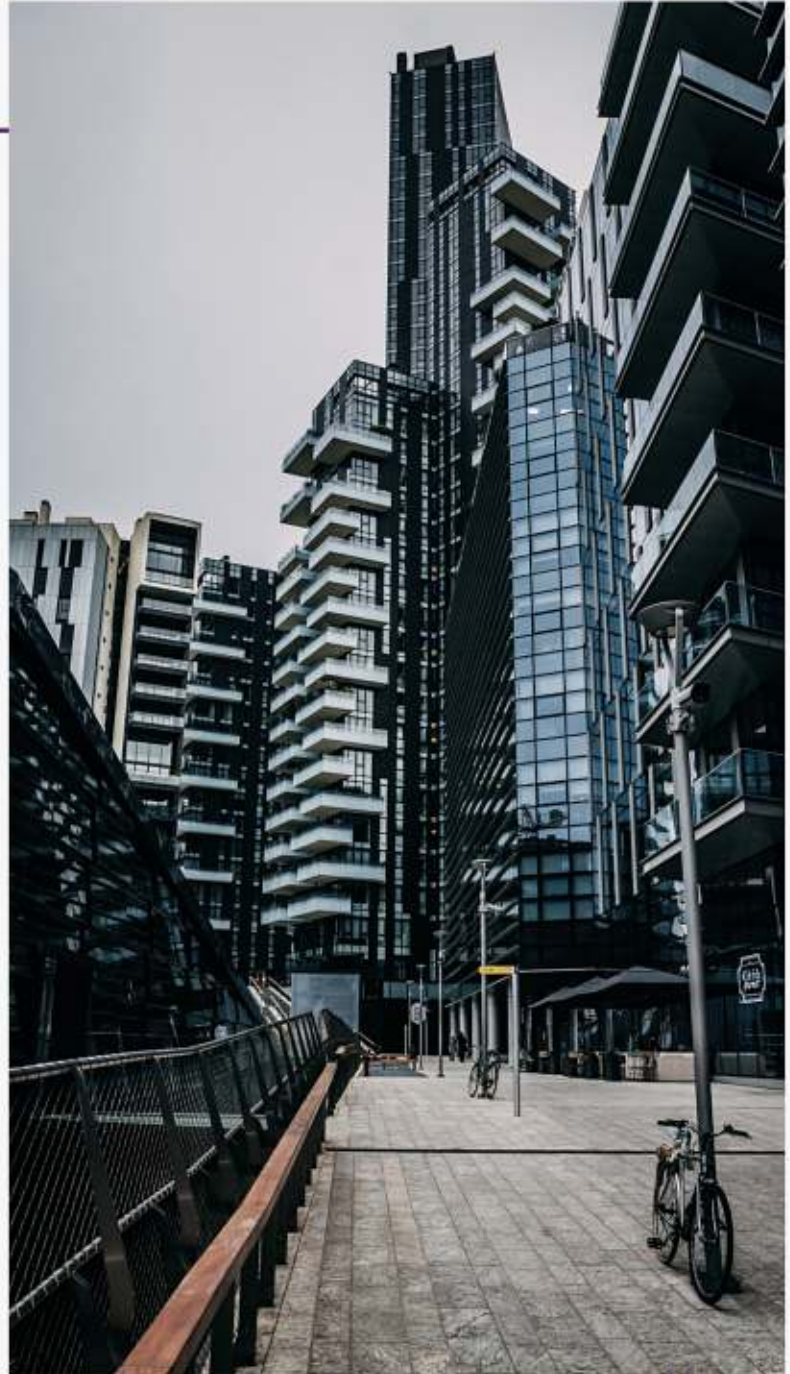


CYBER SECURITY

AWARENESS ●



YOUR
BUSINESS'
BEST
INVESTMENT



CONSTANT C
TECHNOLOGY GROUP
MSP[®] Managed Service and Security Provider

EMPOWERING EMPLOYEES TO BE SECURITY SAVVY STOPS CYBERATTACKS AND SAVES MONEY



Employees are at the heart of your company's security. They are the last line of defense against cyberattacks and the first ones to notice when something unusual is happening at work. This makes them your most valuable security asset.

However, they can also be a vulnerability. When an employee makes a mistake, like mishandling data, clicking on a malicious link or giving a cybercriminal their password, they are opening the doors to expensive compliance failures and security nightmares for your organization.

Empower your team to fight
cybercrime

HOW ?

Create a comprehensive security awareness training program that arms them with the knowledge they need to avoid pitfalls — your company is only secure when everyone knows they are part of every security team.

When you have a well-trained team, they can promptly flag a possible threat. The faster you identify a threat, the better your chances of minimizing the impact it has on your business. After all, security is about more than just technology; it's about people and processes, too



CONSTANT C
TECHNOLOGY GROUP
MSP[®] Managed Service and Security Provider

HOW DO EMPLOYEE CHOICES IMPACT SECURITY?



HUMAN ERROR IS RESPONSIBLE FOR AN ESTIMATED 82% OF SECURITY BREACHES.²



Every time someone logs on to your company's network, answers an email or takes work home, they're taking an action that could have security repercussions whether they mean to or not. The actions that employees take can result in insider risk for your organization.

As companies become increasingly dependent on technology to get the job done, employees have more opportunities to take actions that could be harmful. Insider threats have nearly doubled in the past two years both in frequency and cost.¹ While insider risk is not something that can be eliminated completely, it can be mitigated, and security awareness training is an affordable and effective way to do it.



CONSTANT C
TECHNOLOGY GROUP
MSP¹ Managed Service and Security Provider

EVERYONE NEEDS TO BE ON BOARD TO BUILD A STRONG SECURITY CULTURE



WHY ?

Companies with a strong security culture have a high level of security awareness — and that's a powerful asset. However, many businesses face challenges in getting the entire leadership in their company on the same page about the vital role their security culture plays in both defense and compliance.

Taking a zero-trust approach to cybersecurity can safeguard your business by removing implicit trust and consistently authenticating each level of a digital interaction. Many companies have been implementing a zero-trust strategy to lower the risk of remote work and insider threats, limit third-party risk, manage cloud risk and improve their security culture. 60% OF ORGANIZATIONS WILL EMBRACE ZERO TRUST AS A STARTING POINT FOR FOSTERING A STRONG SECURITY CULTURE BY 2025.³

BENEFIT ?

A major barrier to your organizational risk management might be a lack of strategic alignment. Often, a company's leadership overlooks strategic risk management because they don't realize the potential damage cyberattacks can cause.

In 2025, 70% OF CEOs WILL MANDATE THAT ORGANIZATIONS EMBRACE A CULTURE OF RESILIENCE TO BETTER COPE WITH THE HIGH VOLUME OF EVOLVING THREATS, INCLUDING CYBERCRIME, SEVERE WEATHEREVENTS, CIVIL UNREST AND POLITICAL INSTABILITY.⁴

SECURITY AWARENESS TRAINING HAS CONCRETE BENEFITS

Looking at some of the concrete benefits of security awareness training shows exactly how valuable the training is and why smart companies are making this small investment that gives them a big security advantage. Expecting your staff to study your policy and adopt security procedures on their own is unrealistic. The training you give your employees leads to adoption. They are informed and better understand risks post-training.



EXPAND YOUR SECURITY TEAM WITHOUT ADDING HEADCOUNT

Security awareness training changes this mindset. When employees gain security savvy, they realize that maintaining security to fight back against cybercrime is everyone's job.



MAINTAIN COMPLIANCE WITH INDUSTRY-SPECIFIC REGULATIONS

Security awareness training is required under many data privacy and data handling statutes. Implementing this training equips your employees to identify potential risks and defend your organization from cyberattacks.



LOWER SECURITY EXPENSES, LIKE THE COST OF PHISHING

The cost of just dealing with the headache of phishing altogether can be devastating for your business. According to the DBIR 2022 report, 82% of breaches involved phishing or social attacks.

EMPLOYEES AND PHISHING ARE A DISASTROUS COMBINATION

Inexperienced employees often fall for phishing lures that entice them to click on malicious links, download suspicious files and email attachments, enter their credentials on a fake site and even correspond with cybercriminals. That's a huge problem for businesses like yours.

58%

58% of employees have clicked on at least one malicious URL on their mobile devices.⁶

16%

16% of employees have downloaded malware or riskware apps on their mobile devices.⁷

75%

More than 75% of supply chain attacks include three steps – phishing is one among them.⁸

If a malicious file is attached as a Microsoft Office document, it can be even harder for your employees to understand whether the email is legit or not. Security awareness training teaches employees how to identify suspicious attachments carrying malware that masquerade as routine files.

RANSOMWARE AND MALWARE



A new cyberattack is launched every 39 seconds.⁹ That's bad news for organizations that aren't prepared since only 16% of employees are able to recognize sophisticated threats without security awareness training.¹⁰

According to a recent study, 70% of malware-related breaches involved ransomware, one of the most common tactics used by capable threat actors in system intrusions and supply chain attacks, irrespective of the size of your business.¹²

Ransomware attacks have surged by 13% to 25% in one year, which is more than the past five years combined.¹¹

Employees encounter these threats every day but are unlikely to detect them without training — if your employees are adequately trained, aware of threat patterns and know which actions lead to a threat, they will behave responsibly



EMPOWERED EMPLOYEES PROTECT COMPANIES FROM TODAY'S MOST DANGEROUS THREATS



ACCOUNT TAKEOVER

A bad actor taking over a user account is a nightmare for every small business, especially if the bad guys hijack an account that contains sensitive customer data. Account takeover (ATO) fraud takes a number of forms, including phishing attacks, phone scams or credential compromises.

Effective training keeps your users aware of the signs of an ATO as well as the dangers of ATO risks, like phishing and credential compromise, and prevents these attacks from landing.

BUSINESS EMAIL COMPROMISE

In a common business email compromise (BEC) scenario, bad actors target a victim and pose as a company the victim's organization would do business with to fraudulently obtain money or sensitive data. BEC also endangers a company's reputation and relationships, with employees encountering this hazard daily.

Employees who have strong cybersecurity awareness are more likely to be suspicious when they experience unusual behavior when communicating with third-party service providers or suppliers.

REMOTE & HYBRID WORKERS

We are living in an era where 60% of knowledge workers are working remotely and 18% of them have no plans to go back to the office.¹³ The modern way of working remotely, coupled with greater use of public clouds, highly connected supply chains and cyber-physical systems, exposes your business to new and challenging attack surfaces.

Often, employees think they can get away with risky behavior like writing down passwords or opening suspicious emails when working remotely. Plus, cybercriminals know that remote workers are more likely to fall for phishing tricks and less likely to report a problem or ask for help if they don't even know whom to ask.



INSIDER RISK

Every employee is an insider, and every employee brings a certain degree of risk to the table whether they intend to or not. A recent study reveals that negligent employees were responsible for 56% of insider threats, while malicious insiders caused 26% of attacks.¹⁴

A strong security culture is a major determinant in reducing your company's overall risk, and security awareness is the foundation on which it is built. If security is top of mind for everyone, employees make fewer mistakes and notice suspicious behavior faster.

INTRODUCE CYBER SECURITY AWARENESS TRAINING & REAP IMMEDIATE BENEFITS



CONSTANT C TECHNOLOGY GROUP



204.272.1458



sales@constantc.com



www.constantc.com



North America



CONSTANT C
TECHNOLOGY GROUP
MSP® Managed Service and Security Provider

References: 1,14 The Cost of Insider Threats, 2022 | 2,6,7,8,11,12 DBIR, 2022 3,4 Gartner, 8 Cybersecurity Predictions for 2022-23 | 5 IBM Cyber resilient Organization Study, 2021 9 University of Maryland | 10 HIPAA Journal, 2021 | 13 Gartner, 7 Top Trends in Cybersecurity for 2022