

SECURITY TRAINING

SOLUTION

cyberSAFE

CYBERSEC FIRST RESPONDER



The Importance of People

Organizations allocate significant resources to network security, yet we see an ever-increasing incidence of highly disruptive and costly cyber-attacks. We've become heavily reliant on building impenetrable systems, and lean on hardware and software solutions to detect and respond to hackers that are able to access our information systems. Despite this, many organizations have neglected their most valuable cybersecurity resource: the end-user.

Don't Let Human Error Put Your Network at Risk

The large majority of successful cyber-attacks are due to some sort of human error. This could be someone within IT failing to identify malicious traffic, or an end-user falling victim to a phishing attack. Both are preventable with the right education and training. In the case of end-users, organizations have a great opportunity to make one of their biggest cybersecurity liabilities an asset.

Better Security through Education

By educating end-users about the simple ways they can positively influence their organizations' cybersecurity posture, CyberSAFE equips every employee with the knowledge necessary to play a proactive role in network security. From identifying social engineering attacks to recognizing the difference between an encrypted and unencrypted website, CyberSAFE establishes a baseline knowledge of cybersecurity best practices for all end-users to follow.



The Importance of People

There's no lack of resources available to secure a network. From hardware and software solutions to third-party services, the marketplace is full of options. Yet, for all of the talk of technology-based solutions, the threat of cyber-attacks continues to grow. When securing an information system, we can't forget about the wetware. For too long, people have played a supporting role in the fight against cybercrime, and have been under-utilized in the defense of our information systems.

95% of Data Breaches Are Due to Human Error

With so many attacks due to human error, the need for a better training solution is apparent. Are your employees helping or hurting your cybersecurity efforts? What role is your IT team playing in securing the organization? The resources are there, but a more holistic approach to educating our security teams is needed.

Prevent, Detect, Respond & Evolve

A varied and sophisticated threat requires a varied approach. Traditional training programs have focused on specific aspects of securing a network, failing to equip security professionals to act before, during, and after an attack. Organizations today need a training solution that prepares professionals to act throughout the attack spectrum.

CYBERSAFE: WHY YOU SHOULD CARE

95% The percentage of all cyber-attacks caused by some form of human error.

\$12.7 M The average cost of a cyber-attack, per organization.

CFR: WHY YOU SHOULD CARE

170 The average amount of days it takes to realize a breach has occurred.

45 The average amount of days it takes to clean up after an incident.

CORPORATE BENEFIT



CyberSAFE allows organizations to increase their security posture quickly and with minimal investment by ensuring that end-users are equipped with the knowledge necessary to be good stewards of their organizations' data.

CORPORATE BENEFIT



CFR takes a holistic approach to preparing employees to analyze threats, secure networks, handle incidents, and utilize other critical security skills to protect your organization with a single course.

EMPLOYEE PROFILE



This course is designed for non-technical end-users of computers, mobile devices, networks, and the Internet, enabling employees of any organization to use technology more securely to minimize digital risks.

STUDENT PROFILE



Designed for information assurance professionals whose job functions include development, operations, management, and enforcement of secure systems and networks.

COURSE OUTCOMES



Students will identify many of the common risks involved in using conventional end-user technology, as well as ways to use it safely, to protect themselves and their organizations from those risks.

LABS



At Logical Operations, we feel there is no substitute for practice. Hands-on practical activities, written with open-source software, can be recreated or rented to provide this experience.

TRAINING CREDENTIAL



This course is designed to prepare students for the Certified CyberSAFE credential. Students can obtain their Certified CyberSAFE certificate by completing the Certified CyberSAFE credential process on the CyberSafeCert.com platform after completing this training.

CERTIFICATION



Upon completion of the CFR course, students are able to sit for the high-stakes Certified CyberSec First Responder exam virtually or in-person through Castle Worldwide. The CFR course is approved for CompTIA CEU credits towards CompTIA A+, Network+, Security+, and CASP. Students taking both the course and the exam are eligible for up to 44 CEU credits.

SAMPLE TRAINING PATH



