knowcyber™

Cybersecurity through learning.

Security Awareness *Now!*™
Our core series of practical, high-impact on-line training modules

Phishing...malware...social engineering...social media attacks...

More and more, cyber attackers use such techniques to target users—people—rather than attack an organization's networks and systems directly. Too often, they succeed.

But your people shouldn't be your organization's weakest link when it comes to cybersecurity. They can, in fact, be your greatest resource... if they are aware, knowledgeable, and motivated...when they are prepared to think and act effectively.

Security Awareness *Now!*™ provides the necessary baseline of cybersecurity competence for any 21st century enterprise's first line of defense—its people.

Our recommended Infusion Plan™

For maximum effectiveness, we recommend deploying** the **Security Awareness Now!** Series **per our Infusion Plan**™. **As employees complete one module every 3 to 4 weeks, cybersecurity remains top of mind; employees stay alert to threats and mindful of their own behaviors.

Modules are shown here in recommended Infusion Plan sequence. This sequence may be modified to address your learners' needs.

THE MODULES

A Tale of Two Breaches

Cybersecurity threats come from many directions, and even innocuous incidents can have far-reaching repercussions. This module traces the origins and implications of two large data breaches. Learners see how seemingly innocuous individual actions can be critically important to an organization's cybersecurity. They begin acquiring specific steps for improving their security consciousness and preparedness.

Using Email Securely

As email connects employees with the outside world, it presents one of the biggest opportunities to gain unauthorized access to enterprise systems. In this module, learners explore email vulnerabilities. They master key email do's and don'ts, and learn what to do when email is hacked or compromised.

Phishing

Phishing is aptly named because it uses bait to dupe unsuspecting victims into providing access to enterprise systems. In this module, employees learn how to spot phishing scams, avoid taking the bait, ensure their devices are protected, and deal with phishing emails they receive.

Password Security

Passwords provide access. Poor password construction and hygiene account for more cybersecurity breaches than any other factor. This module motivates learners to take password security seriously. It enables them to create strong passwords and practice effective password management.

~Continued on reverse side

Mobile Device Security

Mobile devices—phones and tablets—are increasingly our preferred way to connect with the on-line world and, accordingly, increasingly a preferred target of hackers. This module alerts employees to key vulnerabilities and demonstrates how to know whether a device has been compromised. Employees learn specific techniques for keeping devices secure.

Wireless Network Security

Wireless networks afford all of us unprecedented opportunity to maintain on-line presence and boost work productivity. They also invite unprecedented security vulnerability, as many public wireless networks lack even the most fundamental security measures. In this module, learners come to recognize the potential threats and learn how to protect themselves and their organizations.

Social Engineering

Social engineering refers to efforts to turn the most basic elements of human nature against people so as to gain unauthorized access to data and systems. This module demonstrates how social engineers use human psychology to create relationships that become stepping stones to cybersecurity breaches. It prepares employees to both recognize and resist social engineering exploits.

Protecting Against Malware

Infecting devices with malicious software—malware or spyware—is one of the most common ways of collecting information or, worse, gaining deep, unauthorized access into enterprise systems and assets. In this module, learners master how to spot various forms of malware and spyware, what to do if they are encountered, and how to keep devices safe.

Protecting Personal Data

Data is increasingly the lifeblood of any enterprise, and protecting data is one of the key responsibilities of every employee. Through this module learners come to recognize the different types of enterprise data that are critical to protect, and the key do's and don'ts for effective data protection.

Protecting Against Insider Threats

The world of cybersecurity threat has become an entire universe. This module alerts employees to the different types and sources of cybersecurity threats, intentional and unintentional, and how those threats can appear in the daily routine of any organization. Employees acquire best practices for safeguarding the organization's critical assets.

knowcyber™

Cybersecurity through learning.

571.210.4710
info@knowcyber.com
www.knowcyber.com

Cybersecurity and Social Media

Social media are an increasingly prevalent part of daily life and work. In this module learners explore the cyber vulnerabilities that come with engaging in social media, and how cybercriminals and hackers exploit them. They acquire practical, effective ways to avoid or reduce the associated cyber risks.