knowcyber®
Cybersecurity Through Learning

Security Awareness Now!

High-impact cybersecurity training for all employees

PHISHING . . . RANSOMWARE EXPLOITS . . . SOCIAL ENGINEERING . . . SUPPLY CHAIN ATTACKS . . .

Your employees need to be your organization's first line of defense—not its weakest link—against these cyber threats and more.

Even when your organization employs cyber defense technology, it remains vulnerable. More than ever, attackers are targeting points where human actions—such as opening emails, clicking on links, opening and sending files, installing and using apps, working remotely on multiple devices—can expose organizational data and systems, putting revenue and reputation at risk.

KnowCyber's *Security Awareness Now!* video-based micro-learning modules

- **Prepare your employees to defend your organization, and themselves, from the full range of cyber threats encountered today**
- **Provide engaging instruction and ongoing reinforcement to keep your organization protected against cyber attack**
- **Can be completed anytime, anywhere, on any device**
- **Track employee progress and completion, include quizzes to measure comprehension, and provide downloadable tip sheets for quick reference**

Keep Cybersecurity Top of Mind, Across Your Organization

INFUSION PLAN

For comprehensive instruction and reinforcement, deploy our entire suite of *Security Awareness Now!* modules, one per month or as you prefer. Employees stay alert to cyber threats and mindful of their behaviors.

Modules are shown on the reverse side in recommended sequence.

SERIES BY SERIES

Assign a targeted series of modules to address your organization's top concerns or provide intensive training during onboarding.

Threat Defense series

Shows employees why and how data breaches occur, with devastating consequences. Builds employees' ability to thwart attackers across the board.

Anti-Phishing series

Enables employees to recognize, and resist being hooked by, the common, insidious forms of email, text messaging, and voice-based attack that lead to at least one-third of today's cyber breaches.

Password & Data Protection series

Prepares employees to build a bulwark of defense around valuable and confidential data and systems, both business and personal.

Online Security series

Alerts employees to cyber vulnerabilities in an environment of 24/7 connectivity; shows them how to avoid or reduce the risks.

CUSTOMIZED APPROACH

KnowCyber can augment or tailor any module or set of modules to reflect your organization's branding and policies and to meet your organization's needs and objectives.

Please contact Joan Phillips at joan.phillips@knowcyber.com.

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 harmless 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.

Phishing Plus
Workplace-related phishing scams have become more sophisticated and targeted. This module builds on our Phishing module — increasing ability to spot spammers' psychological ploys, recognize the telltale signs of phishing, and thwart spear phishing, business email compromise, and whaling attacks.

Vishing & Smishing
All employees are increasingly vulnerable to non-email-based phishing attacks in the form of vishing (voice-based phishing) phone calls and smishing (SMS, or "short message service") text messages. This module dispels common misconceptions as it prepares learners to recognize and resist these attacks.

Password Security
Passwords provide access, and weak passwords are the easiest way for an organization or individual to be breached.This module motivates learners to take password security seriously. It enables them to create strong passwords and practice effective password management.

Creating Strong Passwords
Most passwords in use today are completely ineffective—either too common, short, and easy to crack or impossible to remember. This module augments our Password Security module. It dissuades learners from using overworked password strategies that can easily be hacked and demonstrates how to come up with strong passwords they can actually remember!

Password Management & Authentication
Most users have unique passwords for scores of active accounts—a lot of passwords to manage! This module emphasizes the pitfalls of ineffective password management and surveys the advantages and features of password management software. It also prepares learners to choose identity-authentication questions and answers that won't be easily hacked.

Mobile Device Security
Mobile devices—phones and tablets—have become a preferred way to connect with the on-line world. And they have become 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 their 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.

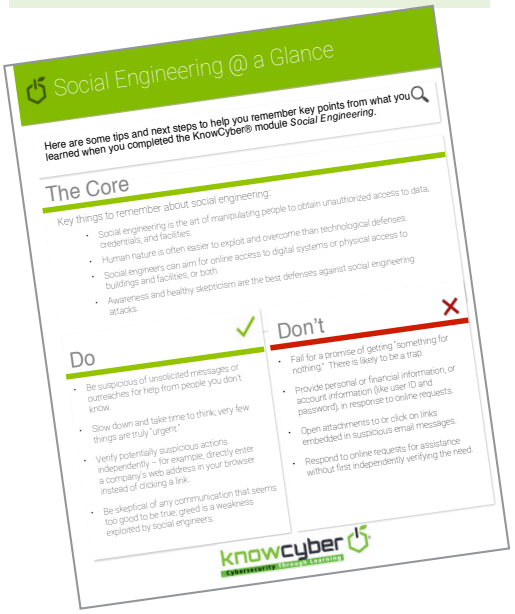
Social Engineering
Social engineering refers to efforts to turn the most basic elements of human nature against people so as to gain unauthorized access to data and systems. This module demonstrates how social engineers use human psychology to create relationships that become stepping stones to cybersecurity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

Protecting Against Malware
Infecting devices with malicious software–ransomware or other types of malware or spyware–is one of the most common ways of collecting information or, worse, gaining deep, unauthorized access to enterprise systems and assets. In this module, employees learn how to recognize the signs of malware attack and respond to them, keeping their 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
This module alerts employees to the many ways that internal cyber threats, intentional and unintentional, may arise in the daily operations of any organization. Employees learn how to respond to safeguard the organization's critical assets.

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 arise when engaging with social media, and how cybercriminals and hackers exploit them. They acquire practical, effective ways to avoid or reduce the associated cyber risks. ■



knowcyber®
Cybersecurity through learning.

info@knowcyber.com
www.knowcyber.com