Overview

This series of modules is designed for general staff in roles such as human resources, legal, marketing, finance, sales, operations and customer service. These highly interactive scenario-based modules equip employees to recognize the value of different types of information; to understand the scope, nature and origin of the diverse risks to such information; and to behave proactively to protect this information in their everyday work. Each module combines instruction with a suite of complementary communications materials, designed to enhance the learning process.

The 9 modules can be combined in any way to design a program to fit diverse customer needs. And, for an even more comprehensive training solution, you can combine this offering with our other role-based elearning for IT and Engineering teams.

Additional Capabilities

Interactive Challenge
Each course combines learning theory and subject matter expertise to deliver a course that is informative and compelling. This content is paired with an interactive exercise that is challenging and engaging.

Eye-Catching Infographics
Putting a graphical and artistic spin on the learning objectives, these high-impact posters are attention-grabbing and excellent for visual learners, data junkies and the casual observer.

Customizable Articles
Short, informative pieces that engage the learner with information related to the module’s theme and content. These can be customized and broken out in a variety of ways.

Printable Tip Sheets
Tied to that month’s training module, the tip sheet is a tangible tool that breaks down a larger concept into short, easy steps. These are meant to be printed and distributed at a weekly team meeting (or by individuals) and put on display at each workstation.

Language localization
Voiceover and on-screen translation in English, Latin Spanish, French Canadian, and Arabic is available.
Course Modules

**Malware Awareness:** In this module, learners will understand the goals of malware, identify the many types of malware, and recognize how to prevent malware infection both at work and at home.

**Social Engineering:** In this module, learners will identify the many forms of social engineering and its potential impacts, identify techniques used by social engineers and understand how to establish validity of requests in order to perform daily business functions in light of the threat of social engineers.

**Password Security:** Learners will recognize the risks surrounding password security, identify safeguards used to protect passwords, and summarize techniques used by attackers to obtain passwords. In an interactive exercise, users will learn how to create and remember strong passwords, eliminating the need to turn to insecure practices.

**Email Security:** Learners will be taught to recognize malicious email before it can become a threat, how to properly handle email, and best practices around how and when to use email to send specific types of information.

**Physical Security:** This module teaches students accepted practices for minimizing breaches and gives them the ability to identify different types of data that may be exposed via hardware theft. Students will be introduced to the risks associated with transporting sensitive data and the importance of maintaining personal security while traveling.

**Mobile Device Security:** In this module, students will learn about mobile devices, the ways in which data can be leaked or lost, and the challenges that arise when the line of what is corporate and what is personal is blurred. This course will look at mobile device security from a number of platforms.

**PCI Compliance:** In this module, students will follow the PCI Security Standards in order to understand how to identify different types of sensitive data and handle it properly.

**Phishing Awareness:** Through this module, learners will recognize malicious email before it can become a threat, understand the various ways in which attackers try to trick and entice users to trigger malicious events through email, and best practices to properly handle and avoid phishing attacks.

**Travel Security:** With the amount of data we are able to carry around in devices as small as a pack of gum, travel security is more important than ever. This module introduces students to the risks associated with transporting sensitive data, offers guidance around how to travel safely with sensitive information and when to leave it at home, and examines the importance of maintaining personal security while traveling.

| Technical Specifications: |  |
|----------------------------|  |
| All courses are SCORM 1.2-compliant. Courses can be integrated into a client’s Learning Management System or delivered as an on-demand service. |  |

| Minimum Requirements: |  |
|-----------------------|  |

**Computer:**
- **Screen Resolution:** 1280x720
- **Standard Operating System:**
  - Mac OSX 10.x or above
  - Windows XP or above

**Web Browser:**
- Microsoft Internet Explorer 7.0 and 8.0
- Mozilla Firefox 9.0 or above
- Google Chrome 16.0 or above
- Windows XP with Safari 4.0
- Mac: 105 with Safari 3.0.4

**Flash Player:**
- Adobe Flash Player v10.1 or above

**Audio:**
- Highly recommended [If sound is unavailable, user can follow on-screen transcript.]