WHAT IS THE SECURITY AWARENESS TRAINING?

The Security Mentor CORE curriculum trains employees on 12 critical security awareness topics.

Each lesson focuses on a single topic and takes approximately 10 to 12 minutes to complete.

Lessons are assigned and completed every couple months to keep content fresh in employees minds and to relieve the burden of hours-long training.

Interactive lessons engage trainees to learn by doing. All lessons include custom interactions or games that are designed to maximize learning and provide context-sensitive feedback.

Includes real-world facts, references to recent security news stories, and security tips for work and home provide relevancy.

Security Mentor content is written by certified information security professionals.

LESSON LIST - YEAR 1

Intro to Security Awareness

This is the introductory lesson for Security Mentor's security awareness training. The lesson shows why each person is critical to security, and how the actions of one person, even if unintentional or unknowing, can put their organization at risk.

Office Security

The office security lesson focuses on both internal and external threats to information security in personal office spaces. Through lesson interactions, trainees learn to identify and remove office security risks. Afterwards, trainees assess their own office security through a series of questions.

Computer Security

The computer security lesson teaches how layers of security are important to protect computing devices. Topics covered include firewalls, anti-malware, software auto-updating, data backups, and safe software installation.

Passwords

In the passwords lesson, trainees interactively learn what makes a strong password and then are given techniques for creating strong, memorable passwords. The second half of the lesson focuses on how to manage passwords and keep them safe.

Email Security

The email security lesson first describes general threats by email including malicious messages, malicious attachments, and spam. This is followed by tips on how to deduce the safety of email messages. Lesson interactions teach trainees how to look for clues that emails are malicious, and receive feedback based on their choices.

Web Security

The web security lesson first teaches about the risks trainees face when on the Web. Trainees next learn about safe web searching techniques, general browser security and security settings, SSL, and protecting against web attacks.

LESSON LIST – YEAR 2

Phishing

The phishing lesson delves into what phishing is and why people fall for it. Spear phishing is given special attention in the lesson. Trainees learn how to identify phishing messages by looking for clues. Trainees then complete interactions designed to reinforce the skills learned in the lesson.

Information Protection

This lesson discusses what the risks are when information is exposed. The lesson introduces three different types of sensitive information: Personally Identifiable Information (PII), Protected Health Information (PHI), and business confidential information. Examples are given for each. Through exercise, trainees then learn to identify sensitive documents, and are given feedback on their choices. The remainder of the lesson focuses on how to protect and manage sensitive information.

Mobile Security

The mobile security lesson discusses the pervasiveness of mobile devices and the risks, particularly for data breaches, related to these devices. Best practices are given for protecting common mobile devices like smartphones, laptops, and mobile storage, as well as for using Bluetooth, WiFi networking, and device disposal.

Social Networking

Social networking impacts everyone, whether through direct participation or through associations. The social networking lesson teaches why security is so important in social networking. Topics addressed include choosing online relationships, personal information to keep private online, and business information to protect. Phishing and malware on social networks are also discussed.

Public WiFi

Public WiFi is everywhere and so easy to use, but what are the risks and how can they be avoided? The Public WiFi lesson first teaches about what malicious hotspots are and then introduces trainees to SSL and VPN. Next, the lesson covers topics including how to avoid malicious hotspots, a summary of the best practices for using public WiFi, and the danger of connecting Ad Hoc to other computers.

Reporting Incidents

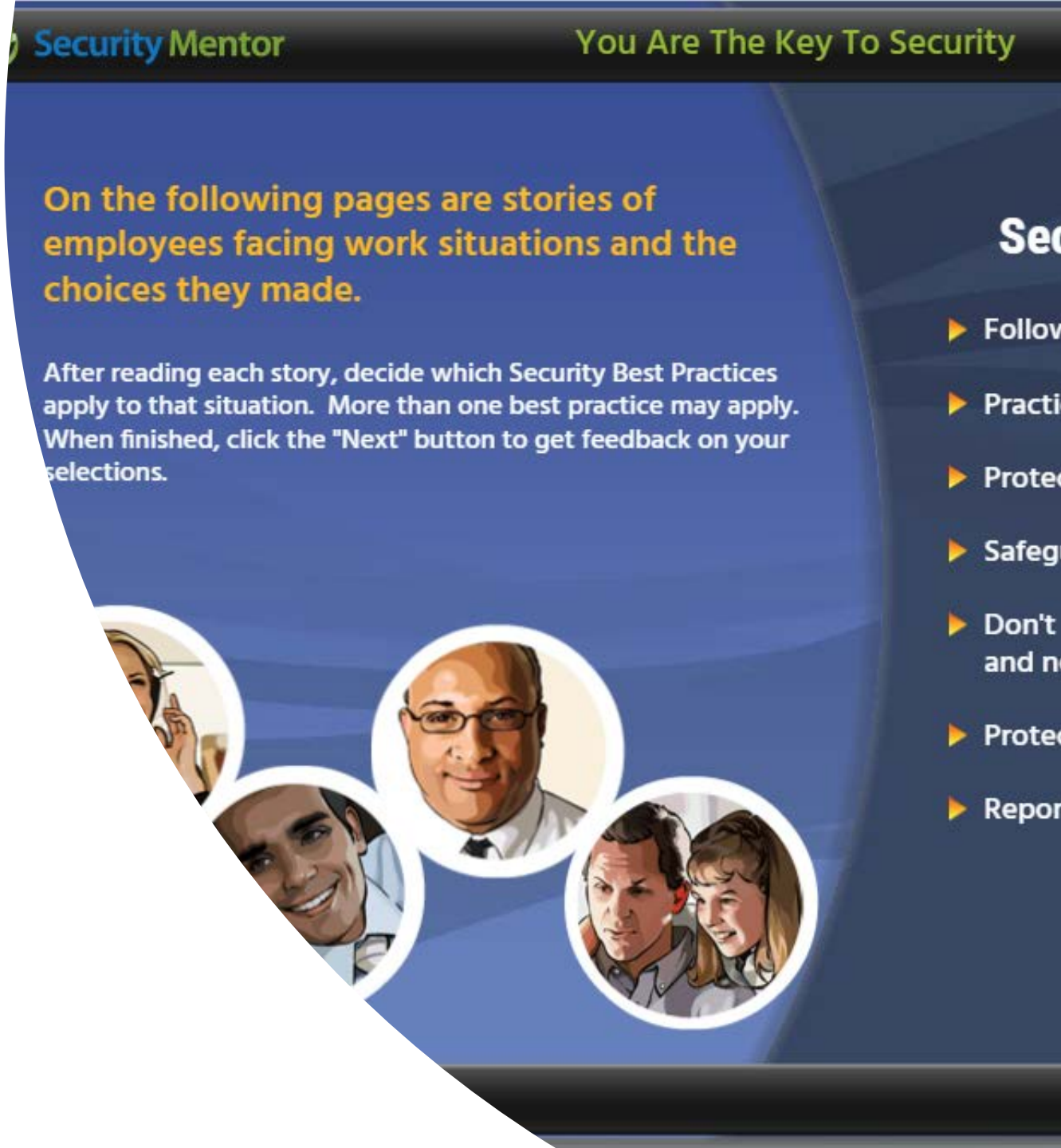
In the reporting incidents lesson, trainees learn how to recognize a variety of security incidents through interactive exercises. The lesson covers what information should be included when reporting incidents. Finally, the lesson also discusses why people don't report incidents and the importance or reporting incidents quickly.

INTERFACE EXAMPLES

Clean and easy to read

Explains core principles

Provides “real world” examples to back up hypothetical scenarios



INTERFACE EXAMPLES

Scenario

Feedback

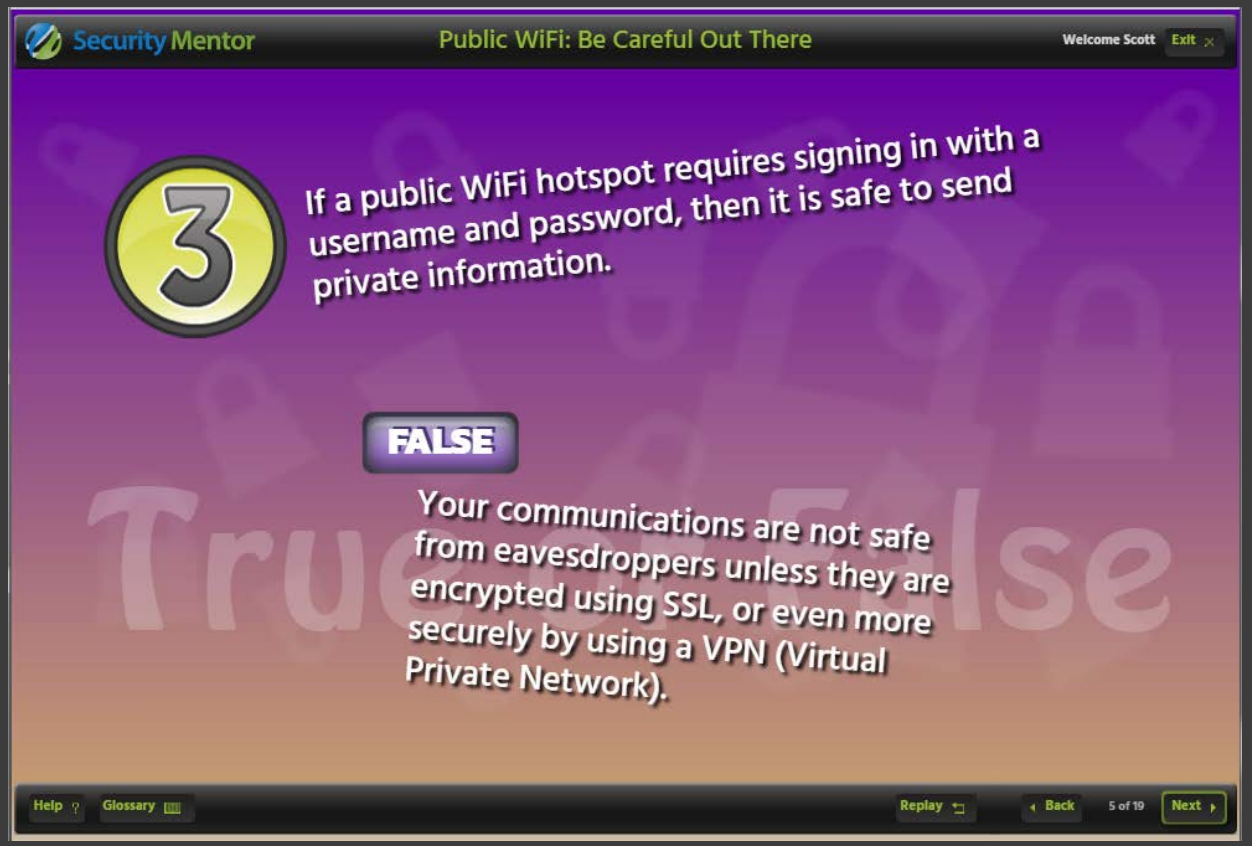
Mouse-overs and links provide additional feedback to help explain answers

INTERFACE EXAMPLES

Security products like checklists and info cards available as part of the lessons

Tips, tricks, and best practices reinforce the overall lesson of security awareness

Summaries tie each lesson to desired objectives



LESSON EXAMPLE