

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

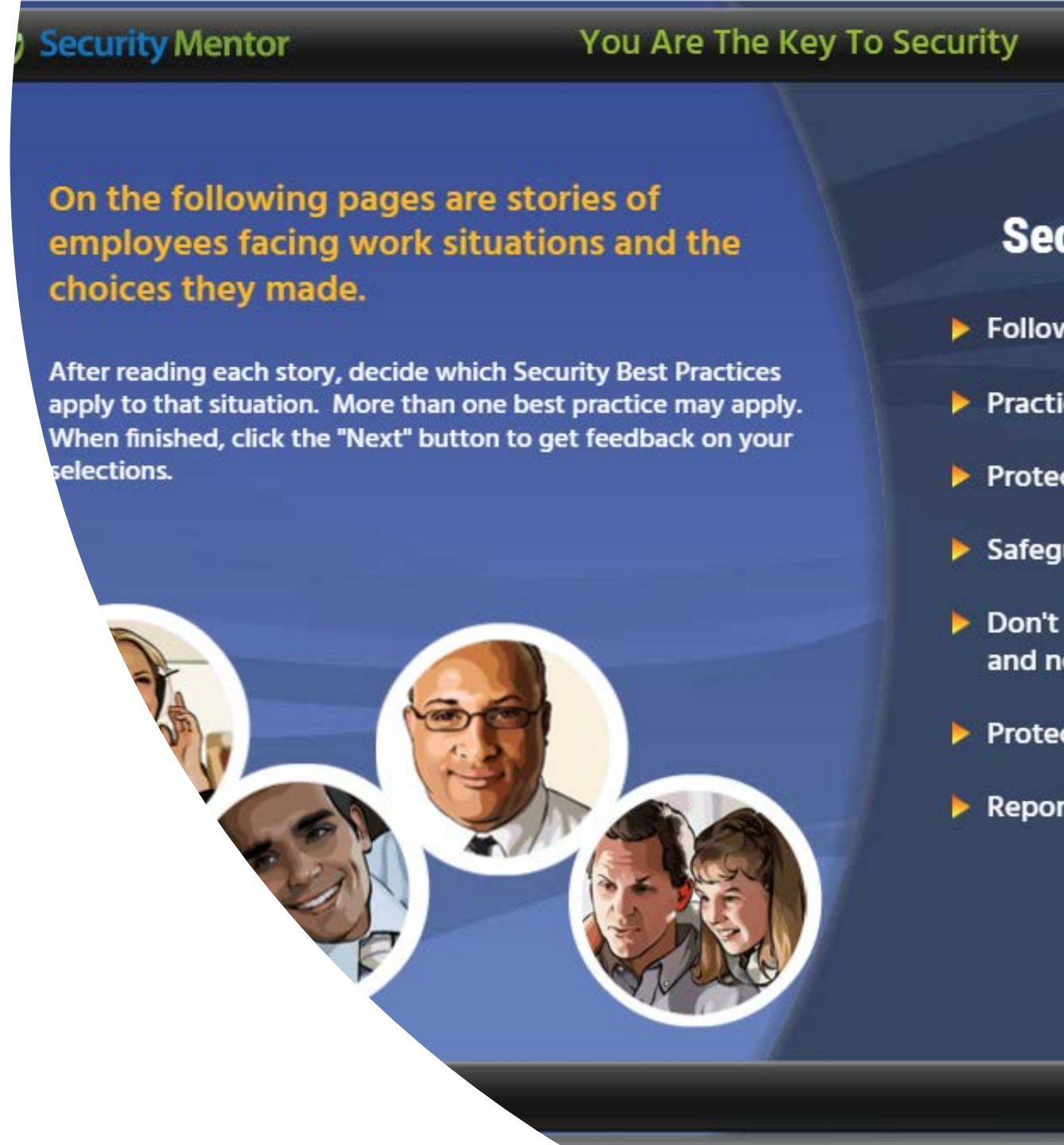
In the reporting incidents lesson, trainees learn how to recognize a variety of security incidents through interactive exercises. The lesson covers what information should be included when reporting incidents. Finally, the lesson also discusses why people don't report incidents and the importance of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

Security Mentor You Are The Key To Security Welcome Scott [Exit](#)

Sandy Morrison loves music.

Music gets her through the day with an upbeat attitude. Sandy is always searching for new indie artists with free music downloads. She even installed file sharing software on her work computer so she could download music.

Sandy knew that the file sharing software violated company policy but figured what's the harm. "The company just wants to make sure I don't violate any copyrights, and I never would! Musicians rock!"

Which of the Security Best Practices did Sandy violate?

Check all that apply.

- Follow corporate policy
- Practice safe computing
- Protect sensitive information
- Safeguard login credentials
- Don't negatively impact computer and network resources
- Protect mobile devices and media
- Report security incidents

[Help](#) [Glossary](#) [Replay](#) [Back](#) 9 of 17 [Next](#)

Feedback

Security Mentor You Are The Key To Security Welcome Scott [Exit](#)

How did you do? 3 out of 4

Pretty good! All correct answers are described below.

Follow corporate policy
Sandy was so sure that the company policy restricting file sharing was to avoid copyright infringement. And she was right, but there was a bigger reason, to protect her company.

Practice safe computing
Besides exposing information, file sharing networks often are hot beds for malware.

Protect sensitive information
Although Sandy didn't realize it, the default configuration of the file sharing software shared all her computer's files with everyone on the file sharing network. So her company's sensitive information was shared with the world!

Don't negatively impact computer and network resources
Sandy's downloading of music from file sharing networks also used up her company's network bandwidth, making the networks slower for everyone.

Which of the Security Best Practices did Sandy violate?

Rollover each response box to see what it means.

- Follow corporate policy Correct
- Practice safe computing Correct
- Protect sensitive information Missed
- Safeguard login credentials
- Don't negatively impact computer and network resources Correct
- Protect mobile devices and media
- Report security incidents

What does Sandy have in common with the security breach of Marine One, the President of the United States' helicopter?
[Click here to see.](#)

[Help](#) [Glossary](#) [Replay](#) [Back](#) 9 of 17 [Next](#)

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

The screenshot shows a software interface for 'Security Mentor' with the title 'Keeping Your Office Secure'. The user is identified as 'Scott'. The main content is an 'Office Security Checklist' featuring a quote by George Orwell: 'To see what is in front of one's nose needs a constant struggle.' Below the quote, there are two sections: 'Remember to ask yourself these 5 questions when you leave your office:' and 'Never do the following:'. The first section contains five bullet points: 'Do I have my keys and/or access card with me?', 'Where is my smartphone, tablet, or other mobile device?', 'Is my laptop physically locked?', 'Is my computer locked?', and 'Have I protected any sensitive data in my possession?'. The second section contains four bullet points: 'Write down your password and hide it in your office.', 'Put unencrypted, sensitive data on portable media (CD, DVD, Flash Drive, external hard drive).', 'Leave sensitive information exposed.', and 'Discard sensitive information in the trash.' On the right side of the interface is a cartoon illustration of a man in a suit pointing upwards. At the bottom, there are navigation buttons for 'Help', 'Glossary', 'Print or Save', 'Share', 'Replay', 'Back', and 'Next', along with a page indicator '7 of 8'.



Security Mentor Public WiFi: Be Careful Out There Welcome Scott Exit

3 If a public WiFi hotspot requires signing in with a username and password, then it is safe to send private information.

TRUE

FALSE

True or False

Security Mentor Public WiFi: Be Careful Out There Welcome Scott Exit

3 If a public WiFi hotspot requires signing in with a username and password, then it is safe to send private information.

FALSE

Your communications are not safe from eavesdroppers unless they are encrypted using SSL, or even more securely by using a VPN (Virtual Private Network).

Help Glossary Replay Back 5 of 19 Next

LESSON EXAMPLE