126 SW 148th Street
Suite C100-105
Seattle, WA 98166
206-400-7290
seattlepro.com

SP4000 – Cybersecurity Awareness Training Course Outline

Target Audience

This training is a subset of SeattlePro's Security Awareness & Training Program. It is specifically designed for the information workers (end users), but all employees can benefit from it. It's a good starting point for more advanced level courses that build on the fundamentals covered in this course. This course can be customized to tailor the needs of an organization and is offered in multiple formats.

Course Format and Duration

1. Instructor-led Presentation (90 minutes, includes Q&A)
2. Video Training (60 minutes)
3. Hands-on Training: 4 hours

Lesson 1: Understanding Cybersecurity

This lesson explains the general concepts of cybersecurity so the students have a better understanding of the dangers of cyberattacks and how they may be personally impacted. It also addresses identity theft and other privacy issues.

a) What is Cybersecurity?
b) How are Privacy and Security Related?
c) Why Should You Care About Cybersecurity?

Lesson 2: Social Engineering Attacks

Several examples of social engineering attacks are discussed in this lesson, along with useful tips on how to avoid being a victim of these common attacks.

a) Identifying Social Engineering Attacks
b) Defending Against Social Engineering Attacks

Lesson 3: Protecting Business Assets

This lesson is focused on raising students' awareness so they can be part of a security culture that actively protects business assets, such as equipment, computer devices, and people. Physical security, protection of corporate data, and application security are also discussed in this lesson.

a) Physical Security
b) Securing Business Data

126 SW 148th Street
Suite C100-105
Seattle, WA 98166
206-400-7290
seattlepro.com

c) Application Security Tips

Lesson 4: Browsing the Internet Securely

In this lesson, the students will learn how to browse the Internet securely to protect their privacy and defend against cyberattacks. They will also learn to identify unsafe or suspicious sites so they can be avoided.

a) Web Browsers and Cyberattacks
b) Identifying Unsafe Web Sites
c) Why is HTTPS Important?
d) What to Do if You Are Hacked?

Lesson 5: Email Security

This lesson addresses cybersecurity risks associated with the use of email and provides numerous tips on how to avoid phishing and other dangerous attacks.

a) Understanding the Email Security Issues
b) How to Avoid Phishing and Other Dangerous Cyberattacks

Lesson 6: Password Management

Password management is one of the biggest challenges in people's digital life. This lesson explains how password managers can be used to easily create complex, secure passwords and eliminate the need to memorizing them. It also shares techniques to further enhance mobile security with the use of authenticator apps and multi-factor authentication.

a) Password Managers
b) Authenticator Apps
c) Multi-Factor Authentication (MFA)

For your cybersecurity training and consulting, go with the pros at SeattlePro.