SAW101 - SECURITY AWARENESS

Course Learning Objectives

By the end of this course, you will be able to explain the consequences of poor information security habits, and how to protect sensitive information about you or your company from attackers. You will also be able to promote a corporate culture that prioritizes security so that your company can significantly reduce the risk of data breaches and other malicious activities that could compromise its operations and reputation.

Description

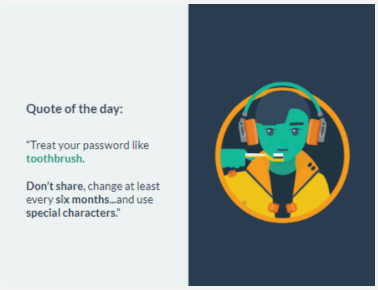
What does it mean to have an awareness of cybersecurity? You've probably heard of tips for making strong passwords, or avoiding malware, phishing, social engineering, and maybe even ransomware–but it goes further than that. With technology moving faster than ever, it can be hard to keep up with best practices. What do you need to watch out for? What can you do to keep your devices safe? Is there a way to protect information about you and your workplace? Let's take a look at how security awareness affects you, the company you work for, and everyone in between.

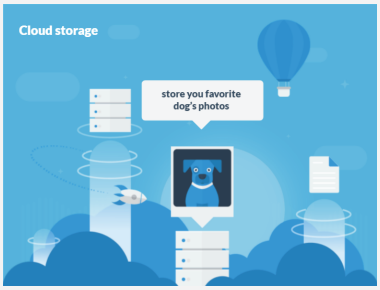
Audience

General Staff

Time Required

Tailored learning - 45 minutes total





SAW101 - SECURITY AWARENESS

Course Outline

1. Introduction

- What is Security Awareness?
- Fish tank example
- Value of information
- You and your company
- Course objectives

2. Passwords

- Section objectives
- Passwords can be a pain
- Strong passwords
- Passphrases
- Password survey
- Password managers
- Sharing accounts and passwords
- 2FA authentication
- Password game
- Summary

3. Social Engineering

- Section objectives
- Altruism
- What is social engineering?
- Tailgating
- Defend against tailgating
- Dumpster diving
- Defend against dumpster diving
- Shoulder surfing
- Defend against shoulder surfing
- Phone call attacks and pretexting
- Examples
- Pretexting example review
- Phone call example review
- Defend against pretexting and phone calls
- Texting pretexts
- Summary

4. Phishing

- Section objectives
- What is phishing?
- Types of phishing
- Email phishing
- Email phishing game
- Executable attachments
- Email encryption
- Summary

5. Ransomware

- Section objectives
- Newsflash: Dallas ransomware
- Defending against Ransomware
- Summary

6. Internet and Wi-Fi

- Section objectives
- Using the Internet responsibly
- Be careful with QR codes
- Social media
- Social media - personal
- Social media - work
- Cloud storage
- Unsecured Wi-Fi
- Only use secured Wi-Fi
- Social media game
- Summary

7. Computer and Smartphone

- Section objectives
- Your devices
- Locking your computer and smartphone
- Apps and operating system
- Lost or stolen phones and laptops
- Physical storage
- Working from home
- Top 10 security practices
- Secure home Internet router
- Summary

8. Artificial Intelligence

- Section objectives
- AI and cybersecurity
- Using AI to combat AI cyber threats
- Defend against AI attacks
- Summary

SecurityCompass