SAW1: Security Awareness Workshop Level 1

Course Code: SAW1
Duration: 0.5 day
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

This Workshop aims to stimulate the intensity and need of Security among the user. This workshop is designed to give an exposure on IT Systems Security & Infrastructure, Monitoring Potential Threats & Attacks and Cyberattack.

Every single user is accountable for ensuring that their respective systems are protected against unauthorised access. The ability of a business to protect its information systems from being corrupted or even stolen is directly correlated to the level of that business's overall success. The implementation of effective security measures will not only result in increased efficiency and productivity, but it will also provide protection from liability. This is due to the fact that the measures will prevent potential risks.

This is done with the intention of fostering an environment within an organisation that is security-conscious, as well as providing direction on how to effectively respond to security incidents and reduce the risk that is posed by cyberattacks.

Training for security awareness should be a priority at every organisation, but it should be especially important at organisations that are embracing digitalization. Employees who are working on computers, laptops, or other devices present an easy target for cybercriminals who are looking to take advantage of their victims' lack of awareness.

An effective security awareness training practise in an organisation can motivate employees to take part in security awareness programmes and attend security-related events, which in turn equips them to defend the organisation against cybersecurity risks.

SKILLS COVERED

- Learn about the fundamentals of security, such as vulnerabilities and the role that defensive technologies like malware and network protection play.
- Learn about the methodology used in all of the most recent attacks. Attendees will benefit from this by becoming more aware of the risks and dangers that exist today.
- Learn about the various social media risks, including Facebook, and best practises for recognising and protecting yourself from such attacks.
- Learn the importance of using strong passwords and how to create a secure password.

WHO SHOULD ATTEND?

This training is highly recommended for anyone who uses social media, the internet, a computer, or a mobile phone. NO Confusing Technical Jargon; This Is Suitable for EVERYONE.

PRE-REQUISITES

There are no prerequisite requirements as this is generic user awareness course.

MODULES

Module 1: Latest Cyber Attack Cases

- Ransomware
- Business Email Compromise (BEC)

Module 2: Hacking Human

- Portable Storage Devices Attacks
- Phone Scam

Module 3: Manage Your Password

- Why you need to practice password Hygiene?
- Why u should use unique credential and password for mobile or web application?
- How to create strong Password

Module 4: Communication Security – Email and Chat

- Email Threat
- Phishing, Vishing and Mishing
- Managing Emails
- Chat Messaging security
- Email Messaging hygiene practices

Module 5: Wi-Fi Threats

- What are some of the potential risks associated with using WIFI?
- How to protect your mobile, home and office Wi-Fi networks

END OF PAGE