C)SA1: Certified Security Awareness

Course ID #: 7000-810-ZZ-Z

Hours: 2

Course Content

Course Description:

Note: This course is a self-paced only course.
In this course, you will cover the security threats inherent to today's workplace as well as the countermeasures associated with these. Students will learn that the weakest link in any security program is a poorly trained department. The Certified Security Awareness 1, C)SA 1, course teaches general security awareness as well as how to develop a strong security culture within your company's community. The Social Engineering portion of the class is designed to teach the participants the skills used by Social Engineers to facilitate the extraction of information from an organization using technical and non-technical methods.

Course Objectives:

Upon successful completion of this course students will be able to:

- Competently take the C)SA1 exam
- Understand basic cybersecurity principles to keep companies' IP and IT infrastructure safe

Prerequisites:

None.

Target Audience:

- Everyone
- End Users
- Employees
- Managers

Topics:

Lesson 1 - Basic Security Awareness

- What is it and why it's needed?
- End User Risk Trends
  - Who, What and How are people the target
  - What are the losses associated to end user hacks?
    - The policies are as good as the employee who embraces them

Lesson 2 - Social Engineering

- Phishing
  - mail, via phone, social websites are common
- Spear Phishing
  - Example: Fake email sample
- Social media
- Personification

C)SA1: Certified Security Awareness

Course ID #: 7000-810-ZZ-Z

Hours: 2

Lesson 3 - Data Classification and Corporate Use (Safe Guarding)

- Corporate
  - Sensitive, internal or public classification
  - Objectives of securing data (IP, Compliance/legislature)
- Personal vs. Business Use
  - Segregating personal use with business use
- Data management
  - Business standard for deleting data
  - Personal standard of data dumping (old phones/hard drives and usb)
  - Did you know that I can unearth deleted docs from a USB drive from a standard Forensics app off of the internet?
- How to delete and get rid of your old data

Lesson 4 - End User Best Practices

- Internet utilization
  - Hot spots, public places & roaming risks
- Safe Web Site surfing
  - Discerning safe secure sites (never go to a site link indirectly)
  - Locks and HTTPS
- Computer Usage
  - Using computer in non-admin mode
  - Ransomware
- Password management
- Removable Devices
- Mobile, Smart Phones and Tablets (risks associated with mobile devices)
  - Device always locked
  - Device should always be trackable

Accreditations:

Register for this class by visiting us at:
www.tcworkshop.com or calling us at 800-639-3535