W WARENESS
knowledge applied

Security Awareness Training

Course Information

Certification: None
Duration: Optional 45/25 minutes
Domain: Information Security
Delivery Method: Online

Accreditor: None
Available Languages: English
Purchase Options: Pay per Use

Course Description:

Despite the best efforts of organizations worldwide, cybercrime is rising rapidly, and it is expected to cost organizations a stunning amount in 2019: $2 trillion. This is because human error continues to be the biggest threat to information security. This course aims to mitigate human error by teaching how to

- Classify data
- Protect confidential/sensitive data
- Secure mobile devices
- Secure remote and home offices
- Avoid social engineering scams like pretexting and phishing, and
- Create strong passwords

The course aims to maximize learning by using a challenge-based approach that helps a user understand the best practices they should follow in the office every day.

Users are frequently asked to resolve common challenges that employees face every day – everything from recognizing the classification level of sensitive files to recognizing phishing and other social engineering attempts.

Audience:

Everyone

Prerequisites:

There are no formal prerequisites for this course.

Learning Objectives:

At the end of this course, you will be able to:

- Classify data: You will be able to determine which classification a given piece of data falls under – confidential, restricted, or public.

- Protect confidential/sensitive data: You will learn the steps you need to take to ensure that data is only shared with relevant people, and that data remains secure from hackers and in public places.
- Secure mobile devices: You will learn the steps you need to take to protect the data stored in mobile devices.
- Secure remote and home offices: You will be able to secure organizational data at your home/remote office by learning how to configure your router and other network devices – and the general best practices to follow when working away from the office.
- Avoid social engineering scams: You will be able to define, recognize, and avoid social engineering scams such as phishing, pretexting, baiting, and quid pro quo.
- Create strong passwords: You will be able to create strong passwords – and the general best practices to take in regards to passwords.

Course Outline:

Module 1: Information Security

- Responsibilities
- Policies & Practices
- Personal Use
- Security Incidents

Module 2: Social Engineering

- Types of Social Engineering
- Avoiding Social Engineering

Module 3: Internet Safety

- Consequences & Prevention

Module 4: Email Safety

- Email Best Practices

Module 5: Access Control & Passwords

- Responsibility
- Prevention
- Creating Strong Passwords

Module 6: Identity Theft

- Prevention

Module 7: Physical Security

- Securing mobile devices

Exam Information

There is no exam for this course.

Accreditation Requirements

This is not an accredited course.