CertNexus CyberSAFE Extended Edition 2019 (CBS-310)

Overview

Regardless of your computer experience, this class will help you become more aware of technology related risks and what you can do to protect yourself and your organization from them.

This course will help you to:

- Understand security compliance needs and requirements
- Recognize and avoid phishing and other social engineering
- Recognize and avoid viruses, ransomware, and other malware
- Help ensure data security on computers, mobile devices, networks, the Internet, and in the cloud

In this course, you will use discussions, case studies, and the experiences of your instructor and fellow students to explore the hazards and pitfalls of technology and learn how to use that technology safely and securely.

Course includes access to the CyberSAFE assessment. Upon successful completion of the assessment, learners will receive the CyberSAFE credential and digital badge.

Prerequisites

- Using Microsoft Windows 8.1

Prerequisite Comments

To ensure your success in this course, you should have experience with the basic use of conventional end-user technology, including desktop, laptop, or tablet computers; mobile phones; and basic Internet functions, such as web browsing and email.

Target Audience

This course is designed for the non-technical end user of computers, mobile devices, networks, and the Internet, to enable you to use technology more securely to minimize digital risks.
This course is also designed for you to prepare for the Certified CyberSAFE credential. You can obtain your Certified CyberSAFE certificate by completing the Certified CyberSAFE credential process on the CHOICE platform following the course presentation.

Course Objectives

In this course, you will identify many of the common risks involved in using conventional end-user technology, as well as ways to use it safely, to protect yourself from those risks.
You will:
Identify the need for security
Secure devices like desktops, laptops, smartphones, and more

Use the Internet securely

Course Outline

1 - Identifying the Need for Security

Identify Security Compliance Requirements
Recognize Social Engineering and Avoid Phishing and other Attacks

2 - Securing Devices

Maintain Physical Security of Devices
Use Passwords for Security
Protect Your Data
Identify and Mitigate Viruses, Ransomware, and other Malware
Use Wireless Devices Securely

3 - Using the Internet Securely

Browse the Web Safely
Use Email Securely
Use Social Networking Securely
Use Cloud Services Securely

Related Courses, Certifications, Exams

- CBS-310 - CyberSAFE Extended Edition 2019