CertNexus CyberSAFE®

Duration
1/2 Day

Credentials
CBS-410

Contact Us
📞 800.674.3550

📍 2151 W. Hillsboro Blvd.
Suite 210
Deerfield Beach, FL 33442

Connect with us

Course Overview

CertNexus® CyberSAFE® helps ensure that your end users can identify the common risks associated with using conventional end-user technology, as well as how to safely protect themselves and their organizations from security risks.

A single click can lead to a multi-million dollar breach in seconds, and the employee responsible may not even be aware of their mistake. Many end users aren't aware of the dangers accompanying today's most common cybersecurity threats, much less how to detect them. CyberSAFE helps ensure that your end users can identify the common risks associated with using conventional end-user technology, as well as how to safely protect themselves and their organizations from security risks in office or while working remotely.

Target Audience

IT Cybersecurity Specialist

Junior Cyber Analyst

Security Analyst

Junior Cyber Penetration Tester

IT Associate

INFOSEC Specialist

Course Objectives

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

Prerequisites

While there are no formal prerequisites to complete the CyberSAFE credential process, it is recommended that you have experience with the basic use of digital technology, such as desktop, laptop, and tablet computers; mobile devices; and basic Internet functions like web browsing and email, whether you are working onsite or from a remote location. Once you have obtained this level of skill and knowledge, or if you already possess it, CertNexus also strongly recommends that you prepare for the CyberSAFE credential by taking the CertNexus' CyberSAFE CBS-410 course.

ATA | APPLIED TECHNOLOGY ACADEMY

Sign Up Today!

CertNexus CyberSAFE®

Course Outline

Lesson 1: Identifying Security Compliance Measures

- Identify Organizational Compliance Requirements and Resources
- Identify Legal Compliance Requirements and Resources

Lesson 2: Recognizing and Addressing Social Engineering Attacks

- Recognize Social Engineering Attacks
- Defend Against Social Engineering Attacks

Lesson 3: Securing Devices

- Maintain Physical Security of Devices
- Use Secure Authentication Methods
- Protect Your Data
- Defend Against Malware
- Use Wireless Devices Securely

Lesson 4: Using the Internet Securely

- Browse the Web Safely
- Use Email Securely
- Use Social Networks Securely
- Use Cloud Services Securely
- Work from Remote Locations Securely

AppliedTechnologyAcademy.com