

EMPLOYABILITY SKILLS

CYBERSECURITY ESSENTIALS FOR WORK



Skills for Avoiding Cyber Risk

Cybersecurity is an increasingly important part of organizational structure. From recognizing cybersecurity threats to protecting sensitive information, the CareerSafe Cybersecurity Essentials for Work course provides a solid foundation of the essential cybersecurity knowledge and strategies needed to safely navigate the digital world.

**Best-in-Class** US-based Customer Care**+4.1 Million** Trained and Counting**Aligns** with Employability Skills Framework

"I trained alongside my friends and classmates and developed better communication, problem solving, listening, critical thinking, and leadership skills because of it. The method in which I was taught was through interactive lessons that were simple but effective."



Optimized Learning



Study Guides



Real-World Scenarios

Benefits and Features

- Contains **interactive content and real-world scenarios** to keep courses engaging and give students the opportunity to practice the skills they learn.
- Includes **teacher tools and resources** that make it easy to distribute courses, plan lessons, and manage students.
- Provides resources and techniques for building **essential skills and strategies** applicable in all professional fields.



3 Hour Seat Time

*Part of our Employability Skills Training Library of courses!*

TOPICS AND LEARNING OBJECTIVES

Introduction to Cybersecurity (~40 minutes)

- Recognize why cybersecurity is important to your organization.
- List the different types of cybersecurity threats and vulnerabilities.
- Describe the types of information that must be protected due to federal cyber and privacy law requirements and the consequences for not adequately protecting such data.
- Describe the best practices you can use to reduce cybersecurity risks in your workplace.

Cyber Hygiene (~40 minutes)

- Explain the considerations when sending sensitive information by email, storing it on a shared server, and maintaining physical copies.
- Describe the importance of situational awareness and maintaining physical security of the workplace.
- Recall best practices to keep your information secure when outside the office.
- Define the internet of things (IoT) and cyber hygiene.
- Identify how the use of common, everyday devices can pose cybersecurity risks to both yourself and your employer.
- Describe good cyber hygiene practices when using connected devices.
- Explain instances where IoT and business intersects.
- Select good cybersecurity approaches.

Don't Take the Bait (~60 minutes)

- Explain why phishing poses a threat to themselves and their organization.
- Explain why links and attachments can be dangerous.
- Describe the different ways in which students could be targeted.
- Recognize common indicators of a phishing attack received by email, text messages, and social media.
- Describe common signs that students have been infected by ransomware.
- Explain best practices when receiving phone calls to avoid falling victim to social engineering attacks.
- Describe the importance of timely reporting.

Insider Threats (~40 minutes)

- Describe social engineering and how it is used to trick employees into compromising an organization's security.
- Recognize the importance of detecting and reporting potential insider threats.
- Recall methodologies of adversaries to recruit trusted insiders and collect proprietary or sensitive information.
- Recognize indicators of insider threat behavior.
- Comply with reporting requirements.



Learn more about the CareerSafe Employability Skills
Cybersecurity Essentials for Work course »

