Networking Academy

Introduction to Cybersecurity

Scope and Sequence

Version 3.0

Contents

Target Audience

The Introduction to Cybersecurity 3.0 course is designed for learners considering a career in cybersecurity. This exploratory course provides learners an introduction to cybersecurity, by exploring ways to be safe online, the different types of malware and attacks, measures used by organizations to mitigate attacks, and researching career opportunities. The online course is appropriate for learners at many education levels and types of institutions, including high schools, secondary schools, universities, colleges, career and technical schools, workforce training, and community centers.

Prerequisites

There are no prerequisites for this course.

Course Description

Introduction to Cybersecurity includes:

- Five modules comprised of key topics.
- Modules emphasize critical thinking, problem solving, collaboration, and the practical application of skills.

Topic-level activities are designed to indicate a learner's mastery of course skills, enabling learners to gage understanding before taking a graded quiz or exam.
Language describing concepts is designed to be easily understood by learners at all levels.

- Assessments and practice activities focused on specific competencies are designed to increase retention and provide flexibility in the learning path.
- Multimedia learning tools, including paper-based labs, videos, and quizzes, address a variety of learning styles, stimulate learning, and promote knowledge retention.
- Labs help learners develop critical thinking and complex problem-solving skills.
- Innovative assessments provide immediate feedback to support knowledge evaluation and skills.
- Learners explore the basics of being safe online.
- Learners are introduced to different types of malware and attacks, and how organizations protect themselves against these attacks.
- Learners explore career options in cybersecurity.

Course Objectives

The course material will assist you in developing learner skills, including:

- Explain the basics of being safe online, including what cybersecurity is and its potential impact.
- Explain the most common cyber threats, attacks, and vulnerabilities.
- Explain how to protect yourself while online.
- Explain how organizations can protect their operations against these attacks
- Access a variety of information and resources to explore the different career options in cybersecurity.

Equipment Requirements

Any device with Internet access (Smartphones/Tablets/Chromebooks/Laptops/Desktops).

Course Outline

Table 1 below details the modules and their associated competencies. Each module is an integrated unit of learning that consists of content, activities, and assessments that target a specific set of competencies. The size of the module depends on the depth of knowledge and skill needed to master the competency.

Table 1: Module Title and Objective

Module Title / Topic Title	Objective
Module 1: Introduction to Cybersecurity	
1.0: Introduction to Cybersecurity	Explain the basics of being safe online, including what cybersecurity is and its potential impact.
1.1 The World of Cybersecurity	Explain what cybersecurity is and its potential impact.
1.2 Organizational Data	Identify types of sensitive information that hackers can use to invade your privacy and/or damage your reputation, where they can access this information, and why it's of interest to cyber criminals.
1.3 What Was Taken?	Explain what organizational data is and why it must be protected.
1.4 Cyber Attackers	Describe who cyber attackers are and what they want.
1.5 Cyberwarfare	Explain what cyberwarfare is and why nations and governments need cybersecurity professionals to help protect their citizens and infrastructure.
Module 2: Attacks, Concepts, and Techniques	
2.0: Attacks, Concepts and Techniques	Explain the most common cyber threats, attacks, and vulnerabilities.
2.1 Analyzing a Cyber Attack	Identify the different types of malware and their symptoms.
2.2 Methods of Infiltration	Describe the different methods of infiltration.
2.3 Security Vulnerability and Exploits	Explain how to find security vulnerabilities.
2.4 The Cybersecurity Landscape	Explain how to categorize security vulnerabilities.
Module 3: Protecting Your Data and Privacy	
3.0 Protecting Your Data and Privacy	Explain how to protect yourself while online.

3.1 Protecting Your Devices and Network	Identify ways to protect their computing devices.
3.2 Data Maintenance	Explain how to protect and preserve your data.
3.3 Who Owns Your Data?	Explain how the service agreements of the Terms of Service define treatment of personal data.
3.4 Safeguarding Your Online Privacy	Implement techniques to maintain data securely.
3.5 Discover Your Own Risky Online Behavior	Explain ways to enhance the security of online data.
Module 4: Protecting the Organization	
4.0 Protecting the Organization	Explain how organizations can protect their operations against these attacks.
4.1 Cybersecurity Devices and Technologies	Explain the different firewalls, security appliances, and software that are used by cybersecurity professionals that protect an organization’s network, data and equipment.
4.2 Behavior Approach to Cybersecurity	Explain how to detect a cyberthreat through behavior-based security approaches.
4.3 Cisco's Approach to Cybersecurity	Explain Cisco’s approach to cybersecurity, including the CSIRT team and the Security Playbook.
Module 5: Will Your Future be in Cybersecurity?	
5.0 Will Your Future be in Cybersecurity?	Access a variety of information and resources to explore the different career options in cybersecurity.
5.1 Legal and Ethical Issues	Identify some of the personal and corporate legal issues that can arise when working in cybersecurity.
5.2 Education and careers	Identify what professional certifications and next steps they need to take to follow a career in cybersecurity.