Introduction to Cyber Security 2.0

The Introduction to Cybersecurity 2.0 explores the field of cybersecurity, specifically the importance of cybersecurity, data confidentiality, best practices for using the internet and social media safely, and potential career opportunities in this growing field. The 15-hour self-paced course with instructor led option has been updated with the interactive, multimedia and instructional format, leveraging the same graphical user interface (GUI) as in the CCNA Routing and Switching curriculum.

Cyber security is important because the Internet is a staple in our everyday lives. It is an excellent resource for connecting and sharing information. It is also full of unseen threats. Staying safe on the internet needs to be a conscience concern as we have much to lose if we don’t exercise caution. Introduction to Cybersecurity presents the importance of cybersecurity, data confidentiality, and the best practices necessary for using the internet and social media safely. The course steps students through security aspects in a broad, easy to understand way, explaining the value of securing data, both personal and business related.

This course exposes students to the increasing demand for cybersecurity professionals and the career opportunities available. The course modules define cybersecurity, explaining why it’s important, the impact of cyberattacks, and introduces the processes for securing data.

The course offers the following:
- Interactive content
- Activities and lab exercises that reinforce learning
- Links to articles and websites helping you explore cybersecurity on your own
- Quizzes to check your understanding

Target Audience
The target audience is anyone who desires a practical and technical introduction to the field of networking. This includes field technicians, headend technicians, network operations center (NOC) staff, network engineers, network administrators, and IT help-desk staff.

What’s new in version two & Prerequisites:
- Easy to use graphical user interface
- Interactive, instructional and updated content:
- Personal device, data protection and privacy
- Safe guarding online privacy
- Updates on cyber threats, attacks, and impact
- Updates on security vulnerabilities
- Legal and ethical issues in cybersecurity
- Suitable for non-IT students
- 8 Activities and 7 Labs reinforces learning
• Assessments include end-of-module quizzes and 1 final exam
  • No Prerequisites

Required Skills
The successful completion of this course requires the following:
• Reading Age Level (RAL) of 13
• Basic computer literacy and awareness of the Internet
• Prior experience with computer hardware, binary math, and basic electronics

Course Objectives
Introduction to Cybersecurity is delivered through the Cisco NetAcad.com learning environment where students can enroll into the self-paced course. Instructors can enroll students and teach through the same process used for other NetAcad™ courses.

The Need for Cybersecurity
• Learn the need for and importance of cybersecurity.
• Understand the characteristics and value of personal data, and data within an organization.

Attacks, Concepts and Techniques
• Recognize the characteristics and operation of a cyberattack.
• Interpret the trends in the cyber threat landscape.

Protecting Your Data and Privacy
• Understand how to protect devices from threats.
• Master how to safeguard your privacy.

Protecting the Organization
• Learn techniques to protect organizations from cyberattacks.
• Recognize the behavior-based approach to cybersecurity.
• Explain Cisco’s approach to cybersecurity.

Will Your Future Be in Cybersecurity?
• Explore the opportunities for pursuing an education and a career in cybersecurity.

Course Outline
Chapter 1: The Need for Cybersecurity
• What your online identity and data is, where it is, and why it is of interest to cyber criminals.
• What organizational data is, and why it must be protected.
• What cyber warfare is and why organizations, nations, and governments need cybersecurity professionals to protect their citizens and infrastructure.
• Define personal dat.
• Explain the characteristics and value of personal data.
• Explain the characteristics and value of data within an organization.
• Describe the impact of security breach.
• Describe the characteristics and motives of an attacker.
• Describe the legal and ethical issues facing a cybersecurity professional.
• Explain the characteristics and purpose of cyberwarfare.
Chapter 2: Attacks, Concepts and Techniques
- Security vulnerabilities and the different types of vulnerabilities and malware.
- The techniques used by attackers to infiltrate a system.
- The characteristics and operation of a cyberattack.
- The trends in the cyber threat landscape.
- Identify examples of security vulnerabilities.
- Explain how a security vulnerability is exploited.
- Describe types of malware and their symptoms, methods of infiltration, methods used to deny service.
- Describe a blended attack and the importance of impact reduction

Chapter 3: Protecting Your Data and Privacy
- Tips for protecting your personal devices and data by creating strong passwords and using wireless networks safely.
- Authentication techniques helping you maintain your data securely with tips about what to do and what not to do online.
- Protecting devices from threats.
- Safeguarding your privacy
- Explain how to protect your devices and network from threats.
- Describe safe procedures for data maintenance.
- Explain how to safeguard your privacy by using strong authentication methods and practicing safe online behaviors.

Chapter 4: Protecting the Organization
- Equipment, data, and the commonly used security terms such as botnets, the kill chain, and behavior based security.
- Cisco’s approach to cybersecurity using a CSIRT team and a security playbook.
- Techniques for protecting organizations from cyber attacks.
- The behavior-based approach to cybersecurity.
- Cisco’s approach to cybersecurity
- Describe the various types of firewalls and security appliances.
- Describe different methods of detecting malware and attacks in real time.
- Describe security best practices for organizations.
- Define botnet, kill chain, and behavior-based security.
- Explain how Netflow can help defend against cyberattacks.
- Identify the function of CSIRT within Cisco.
- Explain the purpose of a security playbook.
- Identify tools used for incident prevention and detection.
- Define IDS and IPS.

Chapter 5: Will Your Future Be in Cybersecurity?
- Certification prerequisites for Specialization
- Certificates in many areas of networking, including cybersecurity.
• Explore the opportunities for pursuing an education and a career in cybersecurity
• Describe the certification opportunities provided by Cisco and other vendors.
• Describe the job opportunities provided by Cisco and other vendors.