

Introduction to Cybersecurity

Credits: 0.5

Course Overview and Goals

Introduction to Cybersecurity is a one-semester course. At the beginning of the course, you will delve into cybersecurity concepts and threats. You will also explore how to protect yourself and your computer system from cyberattacks. As you progress in the course, you will learn about the importance of firewalls, wireless networks, and cryptography in boosting cybersecurity. You will become familiar with cybersecurity strategies, including risk management and contingency planning. Additionally, you will understand the laws, standards, and ethics associated with cybersecurity. Finally, you will learn about the different careers and job opportunities available in the field of cybersecurity.

This course consists of 13 lessons organized into four units, four Course Activities, and five Discussions. Each lesson contains one or more Lesson Activities. You will grade your work in the Lesson Activities by comparing it to sample responses. You will submit the Course Activities to your teacher for grading.

By the end of this course, you will be able to do the following:

- ❖ Identify common threats to cybersecurity and outline the features of a robust cybersecurity program.
- ❖ Apply various prevention measures to protect yourself and your computer from cyberattacks, such as hoaxes, phishing, and cyberbullying.
- ❖ Assess the ways in which firewalls, virtual private networks, wireless networks, and cryptography contribute to cybersecurity.
- ❖ Evaluate the importance of risk management and the types and benefits of cyber insurance.
- ❖ Design and implement contingency and incident handling plans to safeguard your computer system from unexpected threats.
- ❖ List various cybersecurity laws and summarize ethical issues related to cybersecurity.

Course Components and Grading Rubric

The table gives a breakdown of the weight for each component in the course. Weight represents the percentage of the total score coming from each activity.

Course Components	Count	Weight
Pretests. <i>Pretests are optional assessments, typically designed for credit recovery use. If a student shows mastery of a lesson's objective, the student may be automatically exempted from that lesson in the upcoming unit. Typically, teachers do not choose to employ exemptive pretests for first-time credit courses. Pretests are not included as a component of the student's final grade.</i>	4	0%
Module. <i>Each module in this course contains an interactive tutorial and an associated mastery test. Tutorials may include one or more Lesson Activities that constitute tasks associated with the tutorial. This course also includes practice questions to prepare students for the mastery test. The module score comes from a student's score on the mastery test.</i>	13	30%
Discussion. <i>Online discussions allow for higher-order thinking about terminal objectives. An online threaded discussion mirrors the educational experience of a classroom discussion. Teachers can initiate a discussion by asking a complex, open-ended question. Students can engage in the discussion by responding both to the question and to the thoughts of others. Each unit in a course has one predefined discussion topic; teachers may add more discussion topics.</i>	5	15%
Posttest. <i>The posttest appears at the end of the unit and mirrors the pretest in structure, content, and complexity.</i>	4	20%
Course Activity. <i>Course Activities are similar to Unit Activities in scope but may be found at any point in the course, either to prepare the student for new learning or to act as a performance-based activity required for a learning objective. Like Unit Activities, Course Activities include simple rubrics, and sample answers are available for teachers. Course Activities are teacher graded.</i>	5	20%
End of Semester Test. <i>The end of semester test (EOS) appears at the end of the course. Students are delivered a few items from every tutorial in the course in order to assess the major course objectives.</i>	1	15%
Total	32	100%

*Teachers may manually adjust these weights if desired, per district grading requirements.

UNIT 1: CYBERSECURITY CONCEPTS AND THREATS (DAYS 1 – 14)

In this unit, you will learn about the different types of cybersecurity errors and threats, including malicious software, cybercrime, and cyber terrorism. You will identify various kinds of networks and the dangers associated with insecure networks. You will understand cybersecurity concepts and explore the key aspects of cybersecurity programs. You will discuss the importance of e-commerce security. You will outline how cyber forensics, cyber forensics tools, and steganography enhance cybersecurity. You will examine the importance of operational security (OPSEC).

Lesson	Lesson Objective
Syllabus and Orientation	Review the Student Orientation and Course Syllabus at the beginning of this course.
Cybersecurity Errors and Threats	Examine the different types of cybersecurity errors and threats.
Cybersecurity Concepts and Programs	Examine cybersecurity concepts and identify the key elements of cybersecurity programs.
Encrypting, Decrypting, and Recovering Deleted Files	Evaluate the importance of steganography in encrypting and decrypting messages.

UNIT 2: PROTECTING A SYSTEM (DAYS 15 – 35)

In this unit, you will learn about measures to secure your computer hardware, desktop, and email. You will identify different types of web security attacks. You will analyze web security and database security options to protect your devices. You will explore the role and features of an operating system (OS). You will delve into the types and applications of antivirus software. You will outline ways to use social media safely and prevent cyberattacks, such as identity theft.

Lesson	Lesson Objective
Protecting Your Computer System	Examine various security measures to safeguard a computer system.
Operating System Security	Analyze various security measures to safeguard an operating system.
Protecting Yourself from Cyber Attacks	Examine various safety measures that prevent cyberattacks.
Securing an Operating System	Assess how to protect an operating system.

UNIT 3: ADVANCED NETWORK SECURITY: FIREWALLS, WIRELESS PROTECTION, AND CRYPTOGRAPHY (DAYS 36 – 61)

In this unit, you will learn about the different types of firewalls, including their features and advantages. You will explore the concept of DMZ and list common services placed in the DMZ, such as web and mail servers. You will outline ways to create a network with a DMZ. You will discuss the types of virtual private networks and their security options. You will delve into wireless networks, examining their components, threats, and security options. You will identify the applications, tools, and techniques of cryptography. You will understand the use of digital signatures. You will compare different encryption algorithms, differentiating between public and private encryption keys.

Lesson	Lesson Objective
Firewalls and Server Management	Examine the different types of firewalls and outline how to create a network with a demilitarized zone (DMZ).
Security of Virtual Private Networks	Analyze the security options for virtual private networks (VPNs) and other evolving technologies.
Security of Wireless Networks	Analyze wireless networks, their threats, and security options.
Cryptography	Analyze the applications and techniques of cryptography.
Decrypting Cipher Text	Compare different types of ciphers.

UNIT 4: CYBERSECURITY STRATEGIES: RISK, RESPONSE, AND ETHICS (DAYS 62 – 90)

In this unit, you will understand the importance of risk management and mitigation. You will learn about uncertainty analysis and cyber espionage. You will delve into cyber insurance, exploring its types and benefits. You will identify the key aspects of contingency planning and incident handling. You will outline the different kinds of incidents that could threaten your computer system. You will examine the importance of technical support and communication for effective incident handling. You will list various cybersecurity laws and define intellectual property rights. You will discuss ethical issues related to cybersecurity, such as ethical hacking. You will analyze the skills and qualifications needed to succeed in the field of cybersecurity.

Lesson	Lesson Objective
Risk Management and Insurance	Outline the process of risk management and evaluate various elements of cyber insurance.
Contingency Planning and Incident Handling	Analyze the process of contingency planning and the key elements of incident handling.
Risk Assessment and Incident Handling Plan	Design a risk assessment and incident handling plan for an OWASP top 10 attack.
Laws, Standards, and Ethics in Cybersecurity	Examine laws, standards, and ethical issues related to cybersecurity.
Careers in Cybersecurity	Outline the evolution of cybersecurity and identify career opportunities in the field.
Audit Plan and Career Plan	Construct an audit plan and assess the duties and skills required to succeed in your chosen cybersecurity career.