

Course Title: Cyber Security**Time Allotment: 9 Weeks****Unit Sequence: 1****Major Concepts to be learned:**

Students learn the basic concepts of cybersecurity by leveraging their familiarity with technology they use every day, such as mobile devices and apps, as well as exploring the risks associated with how they use their email, personal files, and social networking habits.

Expected Skills to be demonstrated:

At the end of the lesson, students role play as victims of a malware attack. They determine how the attack occurred, improve the security of the firewall, and secure their browser.

PA Standards/Anchors: Eligible Content:

3A-NI-04 Evaluate the scalability and reliability of networks, by describing the relationship between routers, switches, servers, topology, and addressing.

3A-NI-05 Give examples to illustrate how sensitive data can be affected by malware and other attacks.

3A-NI-06 Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.

3A-NI-07 Compare various security measures, considering tradeoffs between the usability and security of a computing system.

3A-NI-08 Explain tradeoffs when selecting and implementing cybersecurity recommendations.

3A-DA-10 Evaluate the tradeoffs in how data elements are organized and where data is stored.

3A-DA-11 Create interactive data visualizations using software tools to help others better understand real-world phenomena.

3A-AP-22 Design and develop computational artifacts working in team roles using collaborative tools.

3A-AP-23 Document design decisions using text, graphics, presentations, and/or demonstrations in the development of complex programs.

3A-IC-24 Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.

3A-IC-27 Use tools and methods for collaboration on a project to increase connectivity of people in different cultures and career fields.

Instructional Strategies: Assessments:

Activities

Projects

Teacher Observation

Unit 1: Personal Security

1.1 Introduction to Cybersecurity

Students learn personal and digital security, describe why they are important, and learn to be safe consumers of digital information in a variety of contexts.

Activity 1.1.1 Cybersecurity and Code of Conduct (2 days)

Activity 1.1.2 Password Protection and Authentication (3 days)

Activity 1.1.3 Email and Social Media Security Risks (3 days)

Project 1.1.4 Save the Day (2 days) Lesson

1.2 Security and the Internet

Students learn that the internet is a loosely controlled collection of computers networked together and secured by firewalls. They learn the basic types of malware, security features of their browser, and how not to be a victim. They learn about files and processes, how to manage them, and how to identify suspicious data (potential malware). At the end of the lesson, students role play as victims of a malware attack. They determine how the attack occurred, improve the security of the firewall, and secure their browser.

Activity 1.2.1 Firewalls and Malware (3 days)

Activity 1.2.2 File Management (2 days)

Activity 1.2.3 Process Management (1-2 days)

Activity 1.2.4 Securing Your Browser (3 days)

Project 1.2.5 It's a Trap! (3 days) Lesson

1.3 Protect Your Data Students use their knowledge about files, directories, processes, browsers, suspicious emails, and malware to solve the unit problem.

Problem 1.3.1 A Dangerous Situation (5 days)

Course Title: Cyber Security**Time Allotment: 9 Weeks****Unit Sequence: 2****Major Concepts to be learned:**

Students broaden their cybersecurity knowledge from a personal system to a networked system. They learn how to assess the value of information security and delve deeper into types of malware. They learn the security vulnerabilities of web services and how to secure an Ecommerce site.

Expected Skills to be demonstrated:

Students learn how information can be safely and securely exchanged on a public network. In the end-of-unit problem, students discover a breach, identify the security vulnerabilities, and enhance the system to secure it.

PA Standards/Anchors: Eligible Content:

3A-CS-02 Compare levels of abstraction and interactions between application software, system software, and hardware layers.

3A-NI-04 Evaluate the scalability and reliability of networks, by describing the relationship between routers, switches, servers, topology, and addressing.

3A-NI-05 Give examples to illustrate how sensitive data can be affected by malware and other attacks

3A-NI-06 Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.

3A-NI-07 Compare various security measures, considering tradeoffs between the usability and security of a computing system.

3A-NI-08 Explain tradeoffs when selecting and implementing cybersecurity recommendations.

3A-DA-10 Evaluate the tradeoffs in how data elements are organized and where data is stored.

3A-DA-11 Create interactive data visualizations using software tools to help others better understand real-world phenomena.

3A-DA-12 Create computational models that represent the relationships among different elements of data collected from a phenomenon or process.

3A-AP-22 Design and develop computational artifacts working in team roles using collaborative tools

3A-AP-23 Document design decisions using text, graphics, presentations, and/or demonstrations in the development of complex programs.

3A-IC-24 Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.

3A-IC-27 Use tools and methods for collaboration on a project to increase connectivity of people in different cultures and career fields.

3B-CS-01 Categorize the roles of operating system software.

3B-CS-02 Illustrate ways computing systems implement logic, input, and output through hardware components

3B-NI-03 Describe the issues that impact network functionality (e.g., bandwidth, load, delay, topology).

3B-NI-04 Compare ways software developers protect devices and information from unauthorized access.

3B-DA-05 Use data analysis tools and techniques to identify patterns in data representing complex systems.

3B-IC-25 Evaluate computational artifacts to maximize their beneficial effects and minimize harmful effects on society

Instructional Strategies: Assessments:

Activities

Projects

Teacher Observation

Unit 2: System Security

Students broaden their cybersecurity knowledge from a personal system to a networked system. They learn how to assess the value of information security and delve deeper into types of malware. They learn the security vulnerabilities of web services and how to secure an Ecommerce site. System Security

Lesson 2.1 Information Architecture (8 days)

Students delve into information confidentiality and how it relates to information integrity and assurance, as they compare the value and the risks of sharing information. Students learn how host names relate to digital addresses, demystify the “cloud”, learn how networks evolve, and explore the security of a small network.

Activity 2.1.1 Confidentiality, Integrity, and Availability (3 days)

Activity 2.1.2 Passive Analysis (2 days)

Project 2.1.3 Ecommerce Architecture (3 days)

Lesson 2.2 Server Vulnerabilities (8 days)

Students learn more about the types of malware that are threats to information and the types of delivery systems. Using website applications and the back-end services that support them, they learn how attacks can occur. They explore a vulnerable web server and improve its security measures.

Activity 2.2.1 More on Malware (3 days)

Activity 2.2.2 Server Vulnerabilities (2 days)

Activity 2.2.3 Server Analysis (2 days)

Project 2.2.4 Secure the Server (1 day)

Lesson 2.3 Server Exploits (12 days)

Students delve deeper into how malware propagates and research the symptoms of various exploits. They analyze and secure one of the most common vulnerable environments: a web server hosting client applications.

Activity 2.3.1 Securing Ecommerce Data (2 days)

Activity 2.3.2 Stopping the Spread of Malware (3 days)

Activity 2.3.3 Server Attacks (4 days)

Project 2.3.4 Find the Exploits (3 days)

Lesson 2.4 The Ecommerce Site (5 days)

Students learn how information can be safely and securely exchanged on a public network. In the end-of-unit problem, students discover a breach, identify the security vulnerabilities, and enhance the system to secure it.

Problem 2.4.1 Ecommerce Enrichment (5 days)

Course Title: Cyber Security**Time Allotment: 9 Weeks****Unit Sequence: 3****Major Concepts to be learned:**

Students learn the technical aspects of a highly networked world and the risks to information we all share. They learn operating system and networking concepts, security frameworks, and packet analysis. They learn the types of malware that can attack systems on a network and how to secure and protect a system against them.

Expected Skills to be demonstrated:

Students are given an attack scenario and must identify the exploit, secure the system, and make improvements to prohibit future attacks.

PA Standards/Anchors: Eligible Content:

3A-CS-02 Compare levels of abstraction and interactions between application software, system software, and hardware layers.

3A-NI-04 Evaluate the scalability and reliability of networks, by describing the relationship between routers, switches, servers, topology, and addressing.

3A-NI-05 Give examples to illustrate how sensitive data can be affected by malware and other attacks

3A-NI-06 Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.

3A-NI-07 Compare various security measures, considering tradeoffs between the usability and security of a computing system.

3A-NI-08 Explain tradeoffs when selecting and implementing cybersecurity recommendations.

3A-DA-10 Evaluate the tradeoffs in how data elements are organized and where data is stored.

3A-DA-11 Create interactive data visualizations using software tools to help others better understand real-world phenomena.

3A-DA-12 Create computational models that represent the relationships among different elements of data collected from a phenomenon or process.

3A-AP-21 Evaluate and refine computational artifacts to make them more usable and accessible.

3A-AP-22 Design and develop computational artifacts working in team roles using collaborative tools

3A-AP-23 Document design decisions using text, graphics, presentations, and/or demonstrations in the development of complex programs.

3A-IC-24 Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.

3A-IC-27 Use tools and methods for collaboration on a project to increase connectivity of people in different cultures and career fields.

3B-CS-01 Categorize the roles of operating system software.

3B-CS-02 Illustrate ways computing systems implement logic, input, and output through hardware components

3B-NI-03 Describe the issues that impact network functionality (e.g., bandwidth, load, delay, topology).

3B-NI-04 Compare ways software developers protect devices and information from unauthorized access.

3B-DA-05 Use data analysis tools and techniques to identify patterns in data representing complex systems.

3B-DA-06 Select data collection tools and techniques to generate data sets that support a claim or communicate information.

3B-AP-10 Use and adapt classic algorithms to solve computational problems.

3B-AP-15 Analyze a large-scale computational problem and identify generalizable patterns that can be applied to a solution

3B-IC-25 Evaluate computational artifacts to maximize their beneficial effects and minimize harmful effects on society

3B-IC-28 Debate laws and regulations that impact the development and use of software.

Instructional Strategies: Assessments:

Activities

Projects

Teacher Observation

Unit 3: Network Security

Students learn the technical aspects of a highly networked world and the risks to information we all share. They learn operating system and networking concepts, security frameworks, and packet analysis. They learn the types of malware that can attack systems on a network and how to secure and protect a system against them.

Network Security

Lesson 3.1 Files and Processes (11 days)

They learn how an operating system organizes information using command line tools to manage and secure digital information.

Students learn about user and system processes and how malware spreads around a network. Then, they identify suspicious software running on the system and determine the problems it may have caused.

Activity 3.1.1 Commanding the OS (2 days)

Activity 3.1.2 Access Control (2 days)

Activity 3.1.3 Analyzing Processes (4 days)

Project 3.1.4 Find the Secrets (2-3 days)

Lesson 3.2 Attacks from the Net (14 days)

Students explore network topologies and go deeper down the abstraction path to learn more about network security. They analyze network traffic, find patterns that may represent exploits, and identify security vulnerabilities.

Activity 3.2.1 Where Can I Learn More About Cybersecurity? (2 days)

Activity 3.2.2 Baseline Network Traffic (2 days)

Activity 3.2.3 Unknown Network Traffic (2 days)

Activity 3.2.4 Analyze and Defend Network Attacks (4 days)

Activity 3.2.4 Exploring Security Frameworks (3 days)

Project 3.2.6 Eradicate the Vulnerabilities (4 days)

Lesson 3.3 Analyzing the Net (13 days)

Students analyze network traffic to witness, and then protect against, a malware attack. Students analyze packets to find telltale signs and patterns of malicious exploits. They apply what they've learned to perform a penetration test and secure a network against further attacks.

Activity 3.3.1 Analyzing Address Resolution (2 days)

Activity 3.3.2 Analyzing Control Messages (2 days)

Activity 3.3.3 Analyzing Packet Fragmentation (2 days)

Activity 3.3.4 Analyzing Wireless Authentication (2 days)

Project 3.3.5 Analyzing the Attack (5 days)

Lesson 3.4 Secure the Net (8 days)

Students are given an attack scenario and must identify the exploit, secure the system, and make improvements to prohibit future attacks.

Problem 3.4.1 Is the Network Under Water? (8 days)

Course Title: Cyber Security

Time Allotment: 9 Weeks

Unit Sequence: 4

Major Concepts to be learned:

Students explore cybersecurity in an applied field. They learn methods of cryptography and practice basic tenets of digital forensics. They process a crime scene to solve the mystery and explore the possible consequences of the crime.

Expected Skills to be demonstrated:

Students use their knowledge from the entire course to investigate a crime and provide digital evidence to solve it.

PA Standards/Anchors: Eligible Content:

3A-CS-02 Compare levels of abstraction and interactions between application software, system software, and hardware layers.

3A-NI-04 Evaluate the scalability and reliability of networks, by describing the relationship between routers, switches, servers, topology, and addressing.

3A-NI-05 Give examples to illustrate how sensitive data can be affected by malware and other attacks

3A-NI-06 Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.

3A-NI-07 Compare various security measures, considering tradeoffs between the usability and security of a computing system.

3A-NI-08 Explain tradeoffs when selecting and implementing cybersecurity recommendations.

3A-DA-09 Translate between different bit representations of real-world phenomena, such as characters, numbers, and images.

3A-DA-10 Evaluate the tradeoffs in how data elements are organized and where data is stored.

3A-DA-11 Create interactive data visualizations using software tools to help others better understand real-world phenomena.

3A-DA-12 Create computational models that represent the relationships among different elements of data collected from a phenomenon or process.

3A-AP-13 Create prototypes that use algorithms to solve computational problems by leveraging prior student knowledge and personal interests.

3A-AP-14 Use lists to simplify solutions, generalizing computational problems instead of repeatedly using simple variables.

3A-AP-21 Evaluate and refine computational artifacts to make them more usable and accessible.

3A-AP-22 Design and develop computational artifacts working in team roles using collaborative tools

3A-AP-23 Document design decisions using text, graphics, presentations, and/or demonstrations in the development of complex programs.

3A-IC-24 Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.

3A-IC-26 Demonstrate ways a given algorithm applies to problems across disciplines.

3A-IC-27 Use tools and methods for collaboration on a project to increase connectivity of people in different cultures and career fields.

3B-CS-01 Categorize the roles of operating system software.

3B-CS-02 Illustrate ways computing systems implement logic, input, and output through hardware components

3B-NI-03 Describe the issues that impact network functionality (e.g., bandwidth, load, delay, topology).

3B-DA-05 Use data analysis tools and techniques to identify patterns in data representing complex systems.

3B-DA-06 Select data collection tools and techniques to generate data sets that support a claim or communicate information.

3B-AP-15 Analyze a large-scale computational problem and identify generalizable patterns that can be applied to a solution

3B-IC-25 Evaluate computational artifacts to maximize their beneficial effects and minimize harmful effects on society

3B-IC-28 Debate laws and regulations that impact the development and use of software.

Instructional Strategies: Assessments:

Activities

Projects

Teacher Observation

Unit 4: Applied Cybersecurity

Students explore cybersecurity in an applied field. They learn methods of cryptography and practice basic tenets of digital forensics.

They process a crime scene to solve the mystery and explore the possible consequences of the crime.

Applied Cybersecurity

Lesson 4.1 Cryptography (19 days)

Students learn the history of encryption and ciphers and use frequency predictors to try to break the codes. They practice data hiding techniques, such as cryptography and steganography. Finally, they attempt to decrypt each other's encrypted messages.

Activity 4.1.1 Ciphers and Early Cryptography (4 days)

Activity 4.1.2 Symmetric and Asymmetric Encryption (3 days)

Activity 4.1.3 Storage Encryption Techniques (3 days)

Activity 4.1.4 Steganography (4 days)

Project 4.1.5 Down the Rabbit Hole (5 days)

Lesson 4.2 Digital Forensics (16 days)

Students learn the process of gathering digital evidence, analyzing it, tracing the criminal through their digital footprint, and preparing to prosecute the criminal.

Activity 4.2.1 Evidence Handling (3 days)

Activity 4.2.2 Data Integrity (2 days)

Activity 4.2.3 Imaging Files and Devices (3 days)

Activity 4.2.4 Establishing Identity in Cyberspace (3 days)

Activity 4.2.5 Forensic Tool Suites (2 days)

Project 4.2.6 Phishing at Work (3 days)

Lesson 4.3 Criminal Justice and Computer Science (7 days)

Students use their knowledge from the entire course to investigate a crime and provide digital evidence to solve it.

Problem 4.3.1 Solve the Crime! (7 days)