Cyber in Minecraft: Expert – Learning Objectives

ID	Learning Objective	Cyber.Org Standards Alignment	CSTA Standards Alignment
1	**Networking**		
1.1	**Networking**		
1.1.1	Understand the difference between local and online	6-8.CS.COMM.1 Compare and contrast network topologies	
1.1.2	Describe and be able to differentiate between network topologies (LAN and WAN)	6-8.CS.COMM.1 Compare and contrast network topologies	
1.2	**Networking Hardware**		
1.2.1	Describe the components that make up a Local Area Network (NIC, Switch, Router etc)	6-8.CS.COMP Identify the role of connected network components	3A-NI-04 Evaluate the scalability and reliability of networks, by describing the relationship between routers, switches, servers, topology, and addressing.
1.2.2	Identify a MAC address and understand its relevance to network components (inc it being unique)	6-8.CS.COMM.2 Differentiate between a network device's MAC and IP addresses.	
1.2.3	Understand and create network diagrams	9-12.CS.COMP Create a diagram of a network utilizing appropriate network components.	
1.3	**Networking Protocols**		
1.3.1	Identify online services such as email, video streaming, storage etc	6-8.CS.PROT Identify the protocol connection types used for different services available online.	
1.3.2	Describe and identify the difference between the HTTP and HTTPS protocols	6-8.CS.PROT Identify the protocol connection types used for different services available online.	
1.3.3	Describe and identify other network protocols such as TCP, UDP and their use in online services such as email, video and gaming	6-8.CS.PROT Identify the protocol connection types used for different services available online.	2-NI-04 Model the role of protocols in transmitting data across networks and the Internet.

© Prodigy Learning | prodigylearning.com | codingcredentials.com

1.3.4	Identify an IPv4 and v6 address and understand the difference between Public and Private IP address ranges	6-8.CS.COMM.2 Differentiate between a network device's MAC and IP addresses.	
1.3.5	Understand the 7 layers of the OSI model	9-12.CS.COMM Explain layers within the OSI networking model.	1B-NI-04 Model how information is broken down into smaller pieces, transmitted as packets through multiple devices over networks and the Internet, and reassembled at the destination.
1.3.6	Describe the roles of the layers of the OSI model and their relationships	9-12.CS.COMM Explain layers within the OSI networking model.	
1.3.7	Understand, describe and compare various TCP and UDP network protocols	9-12.CS.PROT.1 Compare and contrast the ports and protocols used for different services available online.	
1.3.8	Identify the risks associated with common TCP and UDP protocols	9-12.CS.PROT.2 Identify the risks associated with the different services available online	

© Prodigy Learning | prodigylearning.com | codingcredentials.com

ID	Learning Objective	Cyber.Org Standards Alignment	CSTA Standards Alignment
2	**Hardware & Operating Systems**		
2.1	**Computer Hardware**		
2.1.1	Identify and describe various computer hardware (monitor, keyboard, mouse, webcam, printer, laptop, tablet, etc)	6-8.CS.HARD Develop strategies to raise awareness of hardware vulnerabilities	1A-CS-02 Use appropriate terminology in identifying and describing the function of common physical components of computing systems (hardware).
2.1.2	Identify and describe various hardware connectivity methods (USB ports, Bluetooth, etc)	6-8.CS.HARD Develop strategies to raise awareness of hardware vulnerabilities	
2.1.3	Describe Bring Your Own Device	6-8.CS.HARD Develop strategies to raise awareness of hardware vulnerabilities	
2.1.4	Describe the dangers that can be in hardware such as keyloggers, USB drives with scripts etc	6-8.CS.HARD Develop strategies to raise awareness of hardware vulnerabilities	
2.1.5	Describe and identify methods of compromising security and how to protect against	9-12.CS.HARD Identify methods of mitigating risk associated with connecting devices.	
2.1.6	Understand the implications of a malicious incident	9-12.CS.HARD Identify methods of mitigating risk associated with connecting devices.	
2.2	**Operating Systems**		
2.2.1	Understand what an operating system is and its role	6-8.CS.OS Discuss the risks of outdated operating systems.	3B-CS-01 Categorize the roles of operating system software.
2.2.2	Differentiate between various operating systems	6-8.CS.OS Discuss the risks of outdated operating systems.	3B-CS-01 Categorize the roles of operating system software.
2.2.3	Understand the role of operating system updates and their importance	6-8.CS.OS Discuss the risks of outdated operating systems.	
2.2.4	Understand methods for securing/hardening an operating system	9-12.CS.OS Create a plan for hardening an operating system.	

© Prodigy Learning | prodigylearning.com | codingcredentials.com

2.3	**Cloud Computing**		
2.3.1	Identify and describe Software As A Service	6-8.CS.PROT Identify the protocol connection types used for different services available online	
2.3.2	Understand the importance of being safe online and identify best practices	6-8.CS.CC Identify the advantages and disadvantages of various cloud computing models	
2.3.3	Describe and identify cloud computing models (public, private, etc)	6-8.CS.CC Identify the advantages and disadvantages of various cloud computing models	
2.3.4	Identify and understand the differences between, SaaS, PaaS and IaaS and their appropriate use cases	9-12.CS.CC Evaluate the risks and benefits of cloud computing.	
2.3.5	Understand and describe the risks associated with common cloud computing services	9-12.CS.CC Evaluate the risks and benefits of cloud computing.	
2.4	**Internet of Things**		
2.4.1	Understand what an IoT device is and common use cases	6-8.CS.IOT Evaluate the risks and benefits of Internet of Things devices.	
2.4.2	Describe and understand that IoT devices collect and share huge amounts of data globally	6-8.CS.IOT Evaluate the risks and benefits of Internet of Things devices.	
2.4.3	Identify common IoT devices	6-8.CS.IOT Evaluate the risks and benefits of Internet of Things devices.	
2.4.4	Understand and describe the risks and benefits of IoT	6-8.CS.IOT Evaluate the risks and benefits of Internet of Things devices.	
2.4.5	Understand the vulnerabilities associated with IoT devices	9-12.CS.IOT Analyze the vulnerabilities of Internet of Things devices	
2.5	**Data & Backup**		
2.5.1	Identify different data storage devices (local and cloud)	6-8.CS.LOSS Explain the role and importance of backups.	

© Prodigy Learning | prodigylearning.com | codingcredentials.com

2.5.2	Understand the importance of backing up	6-8.CS.LOSS Explain the role and importance of backups.	
2.5.3	Understand automatic backing up on cloud services	6-8.CS.LOSS Explain the role and importance of backups.	
2.5.4	Understand redundant data systems	6-8.CS.LOSS Explain the role and importance of backups.	
2.5.5	Describe and understand the role of hardware redundancy and common implementations	9-12.CS.LOSS Develop a plan for risk mitigation that implements redundancy	
2.5.6	Describe and understand other implementations of redundancy such as hot and cold sites	9-12.CS.LOSS Develop a plan for risk mitigation that implements redundancy	

© Prodigy Learning | prodigylearning.com | codingcredentials.com

ID	Learning Objective	Cyber.Org Standards Alignment	CSTA Standards Alignment
3	**Software**		
3.1	**Software Applications**		
3.1.1	Identify and understand the function of various software applications	6-8.CS.APPS Discuss the role that software plays in the protection of a secure system.	
3.1.2	Understand the difference between operating systems and applications	6-8.CS.APPS Discuss the role that software plays in the protection of a secure system.	
3.1.3	Understand what malware is	6-8.CS.APPS Discuss the role that software plays in the protection of a secure system.	
3.1.4	Understand the role of security software (antivirus, antimalware, firewalls, web filter etc)	6-8.CS.APPS Discuss the role that software plays in the protection of a secure system.	
3.1.5	Understand various software applications used to analyse, protect against, and use in a cyber attack	9-12.CS.APPS Discuss how software that exists on and across various platforms can be used to monitor, collect, and analyze information from those platforms.	
3.1.6	Understand the importance of logging and (central) analysis of log files	9-12.CS.APPS Discuss how software that exists on and across various platforms can be used to monitor, collect, and analyze information from those platforms.	
3.2	**Coding and Scripting**		
3.2.1	Understand the role of code in software applications	6-8.CS.PROG Explain the role of scripting in cyber attacks	
3.2.2	Understand that code can be changed which will produce a different result	6-8.CS.PROG Explain the role of scripting in cyber attacks	
3.2.3	Understand the role of scraping (malicious and non-malicious)	6-8.CS.PROG Explain the role of scripting in cyber attacks	
3.2.4	Describe and identify different scripting languages	6-8.CS.PROG Explain the role of scripting in cyber attacks	

© Prodigy Learning | prodigylearning.com | codingcredentials.com

3.2.5	Understand how to protect against malicious code	9-12.CS.PROG Describe the role of scripting in cyber attacks and cyber defense	
3.3	**Software Updates**		
3.3.1	Understand software updates and patches	6-8.CS.SOFT Identify examples of vulnerabilities that exist in software	
3.3.2	Understand the importance of software updates	6-8.CS.SOFT Identify examples of vulnerabilities that exist in software	
3.3.3	Understand and describe examples of vulnerabilities that can be present due to not keeping software and operating systems up to date	6-8.CS.SOFT Identify examples of vulnerabilities that exist in software	
3.3.4	Understand automatic updating along with its advantages and disadvantages	9-12.CS.SOFT Compare the advantages and disadvantages of patching systems in real time	

© Prodigy Learning | prodigylearning.com | codingcredentials.com

ID	Learning Objective	Cyber.Org Standards Alignment	CSTA Standards Alignment
4	**Digital Citizenship**		
4.1	**Personally Identifiable Information (PII)**		
4.1.1	Understand what privacy is and what information is OK to share	6-8.DC.PPI.1 Discuss the risks and benefits of sharing PII	2-IC-23 Describe tradeoffs between allowing information to be public and keeping information private and secure.
4.1.2	Understand what personally identifiable information is and how to keep secure	6-8.DC.PPI.1 Discuss the risks and benefits of sharing PII	2-IC-23 Describe tradeoffs between allowing information to be public and keeping information private and secure.
4.1.3	Understand the risks and benefits of sharing PII	6-8.DC.PPI.1 Discuss the risks and benefits of sharing PII	2-IC-23 Describe tradeoffs between allowing information to be public and keeping information private and secure.
4.1.4	Understand how PII can be disclosed	6-8.DC.PPI.2 Examine techniques to detect, correct, and prevent disclosure of PII	2-IC-23 Describe tradeoffs between allowing information to be public and keeping information private and secure. 3A-NI-05 Give examples to illustrate how sensitive data can be affected by malware and other attacks.
4.1.5	Describe the potential impact of exposing PII online	9-12.DC.PPI.1 Explain the importance of social identity and the implications of online activity regarding private data, long-term career impacts, and the permanence of digital data.	2-IC-23 Describe tradeoffs between allowing information to be public and keeping information private and secure. 3A-NI-05 Give examples to illustrate how sensitive data can be affected by malware and other attacks.
4.1.6	Understand what a data breach is	9-12.DC.PPI.2 Explain the individual risks of a data breach to an organization housing personal data.	3A-NI-05 Give examples to illustrate how sensitive data can be affected by malware and other attacks."
4.1.7	Understand and describe the risks and impact of a data breach to an organization	9-12.DC.PPI.2 Explain the individual risks of a data breach to an organization housing personal data.	

© Prodigy Learning | prodigylearning.com | codingcredentials.com

4.2	**Digital Footprint**		
4.2.1	Understand what good and bad online behaviour is	6-8.DC.FOOT.1 Recognize the many sources of data that make up a digital footprint.	
4.2.2	Describe what a digital footprint is	6-8.DC.FOOT.1 Recognize the many sources of data that make up a digital footprint.	
4.2.3	Understand how a digital footprint can be harmful	6-8.DC.FOOT.1 Recognize the many sources of data that make up a digital footprint.	
4.2.4	Understand how data can be gathered by third parties to create a digital footprint (app, location, web history etc)	6-8.DC.FOOT.1 Recognize the many sources of data that make up a digital footprint.	3A-IC-29 Explain the privacy concerns related to the collection and generation of data through automated processes that may not be evident to users.
4.2.5	Understand that once information is online it may not be possible to fully remove	6-8.DC.FOOT.2 Recognize the permanence of a digital footprint.	
4.2.6	Understand and describe the potential implications of a digital footprint (positive and negative, ethical, financial etc)	9-12.DC.FOOT Examine the implications of both positive and negative digital footprints.	
4.3	**Cyberbullying**		
4.3.1	Understand what cyberbullying is and recognize it taking place	6-8.DC.CYBL Develop strategies to raise awareness of the effects of, and methods to identify and prevent, cyberbullying	1A-IC-17 Work respectfully and responsibly with others online.
4.3.2	Understand what actions can be taken to prevent cyberbullying	6-8.DC.CYBL Develop strategies to raise awareness of the effects of, and methods to identify and prevent, cyberbullying	
4.3.3	Understand what actions can be taken when discovering cyberbullying	6-8.DC.CYBL Develop strategies to raise awareness of the effects of, and methods to identify and prevent, cyberbullying	
4.3.4	Demonstrate how to reduce or prevent cyberbullying	9-12.DC.CYBL Prepare a plan to raise awareness of the effects of cyberbullying.	

© Prodigy Learning | prodigylearning.com | codingcredentials.com

ID	Learning Objective	Cyber.Org Standards Alignment	CSTA Standards Alignment
5	**Ethics & Legal Issues**		
5.1	**Ethics**		
5.1.1	Understand and identify unsafe content such as malicious links or emails	6-8.DC.ETH Distinguish between ethical and malicious hacking.	3A-NI-05 Give examples to illustrate how sensitive data can be affected by malware and other attacks.
5.1.2	Understand and describe what a cyber attack is and reference recent cyber attacks	6-8.DC.ETH Distinguish between ethical and malicious hacking.	3A-NI-05 Give examples to illustrate how sensitive data can be affected by malware and other attacks.
5.1.3	Understand what ethical hacking is	6-8.DC.ETH Distinguish between ethical and malicious hacking.	
5.1.4	Understand what malicious hacking is	6-8.DC.ETH Distinguish between ethical and malicious hacking.	3A-NI-05 Give examples to illustrate how sensitive data can be affected by malware and other attacks.
5.1.5	Understand and describe how integrity and reputation can be affected by actions taken online	9-12.DC.ETH Discuss the role that cyber ethics plays in current society.	3A-NI-05 Give examples to illustrate how sensitive data can be affected by malware and other attacks. 3A-IC-30 Evaluate the social and economic implications of privacy in the context of safety, law, or ethics.
5.2	**Threats**		
5.2.1	Understand proper and improper use of devices	6-8.DC.THRT Describe various types of threat actors.	1A-IC-18 Keep login information private, and log off of devices appropriately.
5.2.2	Understand how devices can be used with good and bad intentions	6-8.DC.THRT Describe various types of threat actors.	
5.2.3	Understand and describe different types of threat actors	6-8.DC.THRT Describe various types of threat actors.	
5.2.4	Understand and describe the motive of various types of threat actors	9-12.DC.THRT Analyze the motives of threat actors.	

© Prodigy Learning | prodigylearning.com | codingcredentials.com

5.3	**Intellectual Property (IP)**		
5.3.1	Understand what copyright is and how it can be equated to ownership	6-8.DC.IP Explain how intellectual property and copyright relate to fair use.	
5.3.2	Understand and describe how copyright relates to fair use	6-8.DC.IP Explain how intellectual property and copyright relate to fair use.	
5.3.3	Understand what Creative Commons License is and the types available	6-8.DC.IP Explain how intellectual property and copyright relate to fair use.	1B-IC-21 Use public domain or creative commons media, and refrain from copying or using material created by others without permission.
5.3.4	Understand the differences between trademark, copyright, patent etc	6-8.DC.IP Explain how intellectual property and copyright relate to fair use.	
5.3.5	Understand and describe who owns content when content is remixed	9-12.DC.IP Debate the importance of intellectual property laws.	1B-AP-14 Observe intellectual property rights and give appropriate attribution when creating or remixing programs. 3A-IC-28 Explain the beneficial and harmful effects that intellectual property laws can have on innovation.
5.4	**Laws & Regulations**		
5.4.1	Understand the potential implications of actions online and their real-world consequences	6-8.DC.LAW Analyze specific federal, state, and local laws as they relate to cybersecurity and privacy.	3A-NI-05 Give examples to illustrate how sensitive data can be affected by malware and other attacks.
5.4.2	Understand and describe how safety is protected online though policies and laws	6-8.DC.LAW Analyze specific federal, state, and local laws as they relate to cybersecurity and privacy.	
5.4.3	Understand and describe laws that relate to cybersecurity in the US	6-8.DC.LAW Analyze specific federal, state, and local laws as they relate to cybersecurity and privacy.	
5.4.4	Understand and describe international cybersecurity laws and regulations	9-12.DC.LAW Compare and contrast local, state, federal, and international cyber laws and regulations for individuals and businesses.	

© Prodigy Learning | prodigylearning.com | codingcredentials.com

5.5	User Agreements		
5.5.1	Understand and describe how Acceptable Use Policies are designed to protect the user	6-8.DC.AUP Understand the various agreements and how they protect users and owners of technology.	
5.5.2	Understand and describe agreements such as AUPs, Terms of Service and End User License Agreements (EULA)	6-8.DC.AUP Understand the various agreements and how they protect users and owners of technology.	
5.5.3	Understand how some agreements favor companies over individuals and vice-versa	9-12.DC.AUP Differentiate between the various agreements that protect individuals and organizations in their digital environments.	

© Prodigy Learning | prodigylearning.com | codingcredentials.com

ID	Learning Objective	Cyber.Org Standards Alignment	CSTA Standards Alignment
6	**Security**		
6.1	**CIA Triad**		
6.1.1	Understand what confidentiality, integrity and availability are	6-8.SEC.CIA Explain the effects of a failure of the CIA Triad.	
6.1.2	Understand and describe concepts related to CIA such as authentication and encryption	6-8.SEC.CIA Explain the effects of a failure of the CIA Triad.	
6.1.3	Describe a scenario where a part of the CIA Triad has failed	6-8.SEC.CIA Explain the effects of a failure of the CIA Triad.	
6.1.4	Understand the three states of data	9-12.SEC.CIA Explain various interactions between the CIA Triad and the three states of data.	
6.1.5	Understand and describe the relationship between the CIA Triad and the three states of data	9-12.SEC.CIA Explain various interactions between the CIA Triad and the three states of data.	
6.2	**Access Control**		
6.2.1	Understand what privileged data is	6-8.SEC.ACC Explain the concept of access control and how to limit access to authorized users.	2-IC-23 Describe tradeoffs between allowing information to be public and keeping information private and secure.
6.2.2	Understand and describe different levels of authority and the data they may require access to	6-8.SEC.ACC Explain the concept of access control and how to limit access to authorized users.	
6.2.3	Understand what access control is	6-8.SEC.ACC Explain the concept of access control and how to limit access to authorized users.	
6.2.4	Understand the principle of least privilege	9-12.SEC.ACC Compare and contrast the concepts presented by access control principles, access control modules, and the principle of least privilege access.	

© Prodigy Learning | prodigylearning.com | codingcredentials.com

6.2.5	Understand an access control list	9-12.SEC.ACC Compare and contrast the concepts presented by access control principles, access control modules, and the principle of least privilege access.	
6.3	**Data Security**		
6.3.1	Understand that data can be changed by mistake or on purpose and how it can be altered	6-8.SEC.DATA Describe data in its three states and potential threats to each state.	
6.3.2	Understand and describe the threats to data in each of the three states of data	6-8.SEC.DATA Describe data in its three states and potential threats to each state.	
6.3.3	Understand and describe measures available to protect data in each of the three states of data	9-12.SEC.DATA Formulate a plan to apply security measures to protect data in all three states.	
6.4	**Threats and Vulnerabilities**		
6.4.1	Understand and describe what malware is and how it could be used and how to respond	6-8.SEC.INFO Analyze threats and vulnerabilities to information security for individuals and organizations.	
6.4.2	Understand and describe email threats and how to respond	6-8.SEC.INFO Analyze threats and vulnerabilities to information security for individuals and organizations.	
6.4.3	Understand and describe how threats and attacks may be used against individuals and organizations	9-12.SEC.INFO Distinguish the different types of attacks that affect information security for individuals and organizations.	1B-NI-05 Discuss real-world cybersecurity problems and how personal information can be protected.
6.5	**Cryptography**		
6.5.1	Understand what is cryptography is and how it protects information	6-8.SEC.CRYP Discuss methods and the need for encrypting information when it is being exchanged, e.g., http vs. https.	2-NI-06 Apply multiple methods of encryption to model the secure transmission of information. 3B-NI-04 Compare ways software developers protect devices and information from unauthorized access.
6.5.2	Understand and describe how simple (Caesar cypher etc) and more complex (Enigma etc) encryption methods work	6-8.SEC.CRYP Discuss methods and the need for encrypting information when it is being exchanged, e.g., http vs. https.	2-NI-06 Apply multiple methods of encryption to model the secure transmission of information.

© Prodigy Learning | prodigylearning.com | codingcredentials.com

6.5.3	Understand what encoding is and how it can benefit encryption	6-8.SEC.CRYP Discuss methods and the need for encrypting information when it is being exchanged, e.g., http vs. https.	2-DA-07 Represent data using multiple encoding schemes.
6.5.4	Understand and discuss scenarios where there is a need for encryption	6-8.SEC.CRYP Discuss methods and the need for encrypting information when it is being exchanged, e.g., http vs. https.	2-NI-06 Apply multiple methods of encryption to model the secure transmission of information. 3B-NI-04 Compare ways software developers protect devices and information from unauthorized access.
6.5.5	Understand the difference between symmetric and asymmetric encryption	9-12.SEC.CRYP Analyze how modern advancements in computing have impacted encryption.	2-NI-06 Apply multiple methods of encryption to model the secure transmission of information.
6.5.6	Understand public and private key encryption	9-12.SEC.CRYP Analyze how modern advancements in computing have impacted encryption.	2-NI-06 Apply multiple methods of encryption to model the secure transmission of information.
6.6	**Authentication**		
6.6.1	Understand and describe the characteristics of a good/strong password	6-8.SEC.AUTH Explain how authentication and authorization methods can protect authorized users.	1A-NI-04 Explain what passwords are and why we use them, and use strong passwords to protect devices and information from unauthorized access.
6.6.2	Understand and describe authentication and authorization and the difference between the two	6-8.SEC.AUTH Explain how authentication and authorization methods can protect authorized users.	2-NI-05 Explain how physical and digital security measures protect electronic information.
6.6.3	Understand and describe the various method of authentication such as passwords, biometrics, multi-factor authentication	6-8.SEC.AUTH Explain how authentication and authorization methods can protect authorized users.	2-NI-05 Explain how physical and digital security measures protect electronic information.
6.6.4	Understand and describe authentication using certificates	9-12.SEC.AUTH Evaluate authentication and authorization methods and the risks associated with failure.	2-NI-05 Explain how physical and digital security measures protect electronic information.

© Prodigy Learning | prodigylearning.com | codingcredentials.com

ID	Learning Objective	Cyber.Org Standards Alignment	CSTA Standards Alignment
7	**Network & Physical Security**		
7.1	**Securing Networks**		
7.1.1	Understand and describe how Defense in Depth can be implemented to secure networks	6-8.SEC.COMP Describe Defense in Depth strategies to protect simple networks.	2-NI-05 Explain how physical and digital security measures protect electronic information. 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.
7.1.2	Understand firewalls and how they use allow and block lists	6-8.SEC.COMP Describe Defense in Depth strategies to protect simple networks.	2-NI-05 Explain how physical and digital security measures protect electronic information. 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.
7.1.3	Describe how network hardware components and their configuration can be used to implement Defense in Depth	6-8.SEC.COMP Describe Defense in Depth strategies to protect simple networks.	2-NI-05 Explain how physical and digital security measures protect electronic information. 3A-NI-06 Recommend security measures to address various scenarios based on factors such as efficiency, feasibility, and ethical impacts.

© Prodigy Learning | prodigylearning.com | codingcredentials.com

			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.
7.1.4	Describe and understand network segmentation and how it can secure networks	9-12.SEC.COMP Evaluate Defense in Depth strategies that can protect simple networks.	2-NI-05 Explain how physical and digital security measures protect electronic information. 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.
7.1.5	Understand and describe how Defense in Depth can be implemented to secure networks	6-8.SEC.COMP Describe Defense in Depth strategies to protect simple networks.	2-NI-05 Explain how physical and digital security measures protect electronic information. 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.
7.2	**Network Threats and Vulnerabilities**		
7.2.1	Describe different methods of exchanging information online	6-8.SEC.NET Explain how malicious actions threaten network security	

© Prodigy Learning | prodigylearning.com | codingcredentials.com

7.2.2	Understand and describe potential vulnerabilities when exchanging information online	6-8.SEC.NET Explain how malicious actions threaten network security	
7.2.3	Understand and describe different types of malicious actions (malware, social engineering etc)	6-8.SEC.NET Explain how malicious actions threaten network security	
7.2.4	Understand and describe attacks and how they can be responded to	9-12.SEC.NET Analyze the different types of attacks that affect network security.	
7.3	**Access Control**		
7.3.1	Understand and describe physical security measures and how they relate to cybersecurity	6-8.SEC.PHYS Explain how malicious actions threaten physical security.	2-NI-05 Explain how physical and digital security measures protect electronic information.
7.3.2	Understand the need to protect places and people using physical means	6-8.SEC.PHYS Explain how malicious actions threaten physical security.	2-NI-05 Explain how physical and digital security measures protect electronic information.
7.3.3	Understand and describe how malicious actions may threaten physical security	6-8.SEC.PHYS Explain how malicious actions threaten physical security.	
7.3.4	Understand and describe the various types of attack that threaten physical security	9-12.SEC.PHYS Analyze the different types of attacks that affect physical security.	
7.4	**Access Control**		
7.4.1	Understand identity verification	6-8.SEC.CTRL Describe Defense in Depth and how physical access controls work together.	2-NI-05 Explain how physical and digital security measures protect electronic information. 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.

© Prodigy Learning | prodigylearning.com | codingcredentials.com

7.4.2	Understand physical security controls	6-8.SEC.CTRL Describe Defense in Depth and how physical access controls work together.	2-NI-05 Explain how physical and digital security measures protect electronic information. 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.
7.4.3	Understand and describe how physical security controls can introduce Defense in Depth	6-8.SEC.CTRL Describe Defense in Depth and how physical access controls work together.	2-NI-05 Explain how physical and digital security measures protect electronic information. 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 andsecurity of a computing system. 3A-NI-08 Explain tradeoffs when selecting and implementing cybersecurity recommendations.
7.4.4	Understand and describe how different physical security controls are appropriate in different scenarios	9-12.SEC.CTRL Justify the use of Defense in Depth and the need for physical access controls.	2-NI-05 Explain how physical and digital security measures protect electronic information. 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 andsecurity of a computing system. 3A-NI-08 Explain tradeoffs when selecting and implementing cybersecurity recommendations.

© Prodigy Learning | prodigylearning.com | codingcredentials.com

© Prodigy Learning | prodigylearning.com | codingcredentials.com