Fundamentals of Cybersecurity – STM530 - Niagara Falls High School – (10 Week Marking Period)

Digital Fluency Learning Standards (Grades 9-12)	Objectives	Primary Resource	Vocabulary/Major Topics/Concepts	Assessment/ Additional Resources
9-12.CY.1 Determine the types of personal and organizational information and digital resources that an individual may have access to that needs to be protected. 9-12.CY.2 Describe physical, digital, and behavioral safeguards that can be employed to protect the confidentiality, integrity, and accessibility of information. 9-12.CY.3 Explain specific trade-offs when selecting and implementing security recommendations	● **Course Overview** ○ Do you use the Internet? ○ How do you use the Internet? ○ What kinds of information are at risk? ○ What are some different CS career fields? ○ Coding as the new literacy ○ What is this course about? ○ Example activity: ■ Lists steps to take to protect yourself on the Internet ■ What is something you want to know or make by the end of the course? ● **What is Cybersecurity?** ○ Cybersecurity defined ○ Why is cybersecurity important? ○ Cybersecurity in the news ○ Cybersecurity and IoT (Internet of Things) ○ How do we prevent cyber attacks? ○ Example activities:	**CodeHS Fundamentals of Cybersecurity** **Module 1: What is Cybersecurity? (2-3 weeks/10-15 hours)**	● Course Overview ● What is Cybersecurity? ● Impact of Cybersecurity ● The CIA Triad	1.5 What is Cybersecurity Quiz

	■ Summarize and discuss recent cyber attacks ■ Explore a threat map to see where cyber attacks are coming from and which countries are being targeted ● **Impact of Cybersecurity** ○ Why do we care about cybersecurity? ○ What information is at risk? ○ What are the impacts of cyber attacks? ■ Financial impact ○ Cybersecurity workforce ○ What are current cybersecurity career? ○ Example activities: ■ Review resources and reflect on or discuss ● What information do cyber criminals steal? ● What do cyber criminals do with stolen information? ● **The CIA Triad** ○ What is the CIA triad? (confidentiality, integrity, availability) ○ What are "secure systems?" ○ What do confidentiality, integrity, and availability mean in cybersecurity? ○ Example activities:			

	■ Determine where scenarios break part of the CIA Triad			
9-12.CT.9 Systematically test and refine programs using a range of test cases, based on anticipating common errors and user behavior. 9-12.CY.1 Determine the types of personal and organizational information and digital resources that an individual may have access to that needs to be protected. 9-12.CY.2 Describe physical, digital, and behavioral safeguards that can be employed to protect the confidentiality, integrity, and accessibility of information. 9-12.CY.3 Explain specific trade-offs when selecting and implementing security recommendations. 9-12.CY.4 Evaluate applications of cryptographic methods. 9-12.DL.6 Actively manage digital presence and footprint to reflect an understanding of the permanence and potential consequences of actions in online spaces. 9-12.DL.7 Design and implement strategies that support safety and security of digital information, personal identity, property, and physical and mental health when operating in the digital world.	● **Digital Footprint and Reputation** ○ What is a digital footprint? ○ What is your digital footprint and reputation? ○ What does it mean that the internet is public and permanent? ○ Who looks at your digital footprint and reputation? ○ What are some recommended social media guidelines? ○ How can you maintain your digital footprint? ○ What does your digital footprint say about you? ○ Example activities: ■ What is your digital footprint? ■ Are you going to make any changes in what you post on social media? ● **Cyberbullying** ○ What is cyberbullying? ○ What are the impacts of cyberbullying? ○ Are there cyberbullying roles? ○ What do you do if you are being bullied? ○ What do you do if you see bullying?	**CodeHS Fundamentals of Cybersecurity** **Module 2: Digital Citizenship and Cyber Hygiene (2-3 weeks/10-15 hours)**	● Digital Footprint and Reputation ● Cyberbullying ● Internet Safety ● Privacy and Security ● Information Literacy ● Creative Credit and Copyright ● Hacking Ethics	2.8 Digital Citizenship and Cybersecurity Quiz

	○ How can you be an upstander? ○ Example activities: ■ Explore cyberbullying scenarios: What would you do? ● **Internet Safety** ○ What are some ways to stay safe online? ○ What are some online safety guidelines? ○ Example activities: ■ Explore Internet safety scenarios: What would you do? ● **Privacy and Security** ○ What are data privacy and security? ○ How can you keep personal data secure and private? ○ What can happen if you data is stolen and what can you do about it? ○ Example activities: ■ Test out various passwords on a site ■ Explore Google's privacy policy: What do they know about you? ● **Information Literacy** ○ What is information literacy? ○ How can you do effective internet searches?			

	○ What are some techniques for judging source legitimacy and identifying misinformation? ○ Example activities: ■ Create and test search queries ■ Explore evidence for using sources ● **Creative Credit and Copyright** ○ What is copyright? ○ What are the different types of copyright licenses ○ Example activities: ■ Create citations for sources ■ Explore image search tools ● **Hacking Ethics** ○ What are hackers? ○ Are there different kinds of hackers? (white, black, grey) ○ What are bug bounty programs? ○ Is hacking always illegal? ○ What are the consequences of illegal hacking? ○ Example activities: ■ Explore what penetration testing is ■ Sign ethical hacker agreement			

9-12.CY.1 Determine the types of personal and organizational information and digital resources that an individual may have access to that needs to be protected. 9-12.CY.2 Describe physical, digital, and behavioral safeguards that can be employed to protect the confidentiality, integrity, and accessibility of information. 9-12.CY.3 Explain specific trade-offs when selecting and implementing security recommendations. 9-12.DL.2 Communicate and work collaboratively with others using digital tools to support individual learning and contribute to the learning of others.	● **Project: Create a Public Service Announcement** ○ Create a Public Service Announcement (PSA) to teach your peers about your selected topic in digital citizenship and cyber hygiene. You can select any of the topics covered in this module. Be creative and make it fun! You could make a video, song, poster, or slideshow.	**CodeHS Fundamentals of Cybersecurity** **Module 3: Project: PSA (2 weeks/10 hours)**		3.1 PSA Project
45 Instructional Days Total Days (with 5 Flex Days)	Five days have been added into the marking period pacing in case more days are needed for additional instruction.			

Niagara Falls High School – Fundamentals of Cybersecurity (20 Week Marking Period)

Digital Fluency Learning Standards (Grades 9-12)	Objectives	Text Resources	Vocabulary/Major Topics/Concepts	Assessment/ Additional Resources
9-12.DL.1 Type proficiently on a keyboard. 9-12.CT.4 Implement a program using a combination of student-defined and third-party functions to organize the computation. 9-12.CT.5 Modify a function or procedure in a program to perform its computation in a different way over the same inputs, while preserving the result of the overall program 9-12.CT.6 Demonstrate how at least two classic algorithms work and analyze the trade-offs related to two or more algorithms for completing the same task. 9-12.CT.7 Design or remix a program that utilizes a data structure to maintain changes to related pieces of data. 9-12.CT.8 Develop a program that effectively uses control structures in order to create a computer program for practical intent, personal expression, or to address a societal issue.	● Interpreted vs. Compiled ● Variables and Objects ● Lists and Arrays ● Programming with Karel ● Looping ○ For Loops ○ While Loops ● Branching ○ If statements ○ If/else statements ● Top Down Design ● Comments and Pseudocode	**CodeHS Fundamentals of Cybersecurity** **Module 4: Programming Fundamentals (JavaScript) (3-4 weeks/15-20 hours**	● Programming Concepts ● Looping and Branching ● Code Organization	4.7 Programming Fundamentals Quiz
9-12.CY.1 Determine the types of personal and organizational information and digital resources that an individual may have access to that needs to be protected. 9-12.CY.3 Explain specific trade-offs when selecting and implementing security recommendations. 9-12.CY.4 Evaluate applications of cryptographic methods.	● Cryptography, Cryptology, Cryptanalysis ○ Why do we need some secrecy in our transparent information age? ○ Explain general encryption with data, keys ○ Example activities: ■ Video and discussion on securing the cloud	**CodeHS Fundamentals of Cybersecurity** **Module 5: The ABCs of Cryptography (2-3 weeks/10-15 hours)**	● Cryptography, Cryptology, Cryptanalysis ● History of Cryptography ● Why do we Need to Encrypt Data? ● Basic Cryptography	5.6 The ABC's of Cryptography Quiz

	■ Passing notes in class (offline activity) ● History of Cryptography ○ Why do we encrypt? ○ What are some classic encryption techniques? ○ What is the flaw in substitution ciphers? ○ What was The Enigma during WW2? ○ What is modern cryptography and how has cryptography changed over time? ○ What is 256-bit key encryption and how does this help cryptography overall? ○ Example activities: ■ How did the Enigma work? ● Why do we Need to Encrypt Data? ○ Explore the CIA Triad and encryption ○ Example activities: ■ Telephone game with math (offline) ■ Modulo math activity sheet ● Basic Cryptography Systems: Caesar Cipher ○ Explore examples of the Caesar cipher ○ Example activities: ■ Practice with a Caesar Cipher JavaScript program ■ Modify the program to		Systems: Caesar Cipher ● Basic Cryptography Systems: Cracking the Caesar Cipher ● Basic Cryptography Systems: Vigenère Cipher	

	create the decrypting Caesar program ● Basic Cryptography Systems: Cracking the Caesar Cipher ○ How do we solve the Caesar Cipher with brute force and using letter frequency analysis? ○ Example activities: ■ Practice cracking Caesar Cipher with brute force ■ Practice cracking Caesar Cipher with letter frequency ● Basic Cryptography Systems: Vigenère Cipher ○ Explore examples of the Vigenère Cipher ○ Example activities: ■ Practice with a Vigenère Cipher JavaScript program			
9-12.CT.1 Create a simple digital model that makes predictions of outcomes. 9-12.CT.1 Create a simple digital model that makes predictions of outcomes. 9-12.CT.6 Demonstrate how at least two classic algorithms work and analyze the trade-offs related to two or more algorithms for completing the same task. 9-12.CT.10 Collaboratively design and develop a program or computational artifact for a specific audience and create documentation outlining implementation features to inform collaborators and users 9-12.CY.4 Evaluate applications of cryptographic methods.	● Project: Create a Newscast ○ Students work collaboratively to research a **classic cipher** (beyond Caesar and Vigenère) to address in their newscast. They will investigate their cipher and write a script that includes how the cipher works, when it was used, and when the cipher stopped being useful.	**CodeHS Fundamentals of Cybersecurity** **Module 6: Project: Classic Cipher Newscast (2 weeks/10 hours)**		6.1 Project: Cipher Newscast

9-12.DL.2 Communicate and work collaboratively with others using digital tools to support individual learning and contribute to the learning of others.				
Midterm Assessment (2 Days)	**Midterm Assessment** is on the CodeHS website, but instructors have the option to create their own. **Modules Covered:** ● What is Cybersecurity ● Digital Citizenship and Cyber Hygiene ● The ABCs of Cryptography			
52 Total Days (with 5 Flex Days)	Five days have been added into the unit pacing in case more days are needed for additional instruction			

Niagara Falls High School – Fundamentals of Cybersecurity (30 Week Marking Period)

Digital Fluency Learning Standards (Grades 9-12)	Objectives	Text Resources	Vocabulary/Major Topics/Concepts	Assessment/ Additional Resources
9-12.CY.1 Determine the types of personal and organizational information and digital resources that an individual may have access to that needs to be protected. 9-12.NSD.2 Explain the levels of interaction existing between the application software, system software, and hardware of a computing system.	● Understanding Operating Systems ● Comparing Operating Systems ○ Installing an OS ● File Management ○ What Processor are you Running? ● Software Licenses ● Antivirus Software ○ Data Backups ● Using Cache ● Popup Blockers ● User Accounts ○ Admin vs. Standard ● Host Security ○ Using a Log ● System Commands ○ cd, ls, mk etc ● Network Commands ○ ipconfig, netstat etc	**CodeHS Fundamentals of Cybersecurity** **Module 7: System Administration (4-5 weeks/20-25 hours)**	● Operating Systems ● Software and Applications ● Application Security ● Browser Configuration ● System Administration ● Command Line Interface	7.2 System Administration Quiz
9-12.CY.1 Determine the types of personal and organizational information and digital resources that an individual may have access to that needs to be protected.	● Inside Web Applications ○ View page source (images, navigation and	**CodeHS Fundamentals of Cybersecurity**		8.12 Software Security Quiz

9-12.CY.5 Recommend multiple actions to take prior and in response to various types of digital security breaches. 9-12.NSD.2 Explain the levels of interaction existing between the application software, system software, and hardware of a computing system.	page layout, stylesheets, JavaScript, minified code ○ Example activities: ■ View page source scavenger hunt ■ Getting started with OWASP ● Developer Tools ○ Use the inspect tools to look more deeply inside of web apps ○ How does view page source compare to inspect in terms of information about the site / app? ○ Example activities: ■ Practice using the Chrome developer tools ■ Change a favorite site using the Chrome developer tools on your end only. Take a screenshot of your change. ● Data Visualizations ● Design a Survey ● SQL Overview ○ What is SQL? ○ How do we structuring data using SQL? ○ How do we query databases using SQL? ○ Example activities: ■ Use the SELECT statement to query a database	**Module 8: Software Security (4-5 weeks/20-25 hours)**		

	■ Use the WHERE clause to query a database ● Clients, Servers, Databases ● Common Security Problems ○ What is the "Fortification Principle"? ○ What are some tips about HTTP vs. HTTPS, password fields and CAPTCHA that can help us to navigate more securely on the Web? ● SQL Injection ○ SQLi Overview ■ What is SQLi? ■ Why is SQLi a problem? ■ What happens during a SQLi attack? ■ What is the the fallout of a SQLi attack? ■ How does SQLi work? ■ How do hackers use SQL in a SQLi? ○ What are the types of SQLi (error-based, union-based, blind) ■ What is the underlying SQL behind the scenes that hackers may be trying to hack? ○ How to we mitigate or prevent SQLi? ■ What are the OWASP recommendations?			

	■ How can we tell if our code is vulnerable? ○ Example activities: ■ Discuss the Equifax SQL injection attack ■ Practice basic SQLi on a safe site ■ Research SQLi prevention			
50 Total Days (with 5 Flex Days)	Five days have been added into the unit pacing in case more days are needed for additional instruction			

Niagara Falls High School – Fundamentals of Cybersecurity (40 Week Marking Period)

Digital Fluency Learning Standards (Grades 9-12)	Objectives	Text Resources	Vocabulary/Major Topics/Concepts	Assessment/ Additional Resources
9-12.CY.1 Determine the types of personal and organizational information and digital resources that an individual may have access to that needs to be protected. 9-12.DL.5 Transfer knowledge of technology in order to use new and emerging technologies on multiple breaches. 9-12.NSD.2 Explain the levels of interaction existing between the application software, system software, and hardware of a computing system. 9-12.NSD.3 Develop and communicate multi-step troubleshooting strategies others can use to identify and fix problems with computing devices and their components. 9-12.NSD.4 Describe the components and design characteristics that allow data and information to be moved, stored and referenced over the Internet. 9-12.NSD.5 Describe how emerging technologies are impacting networks and how they are used.	● Introduction to the internet ○ What is the Internet? How does it work? What have been its impact on society? ○ Why do we need protocols for the Internet? ○ Example Activity ■ Explore the different levels of the internet. ● Decimal to Binary ● Hexadecimal ● Bits to ASCII ○ Hello World in Bits ● Internet hardware ○ Why are protocols so important? ○ How do we send data over the Internet? ○ Example Activities ■ Explore how data is able to be transmitted across the ocean by using underwater cables ■ Explore the role of simple and complex networks and routers ● Internet Addresses	**CodeHS Fundamentals of Cybersecurity** **Module 9: Networking Fundamentals (3-4 weeks/15-20 hours)**	● Introduction to the Internet ● Notational Systems ● Data Representation ● Internet Hardware ○ Vocabulary: bandwidth, bitrate, latency ● Internet Addresses ○ Vocabulary: Internet Protocol (IP) ● Domain Name System (DNS) ● Routing ● Packets and Protocols ● The Internet and Cybersecurity ● Impact of the Internet	9.11 Networking Fundamentals Quiz

	○ How do IP addresses compare to postal addresses? ○ How IP addresses work? ○ Example Activities ■ Explore the differences between IPv4 and IPv6. Why are we running out of addresses? ■ Trace a website request from the server, through the network, and to your computer ● Domain Name System (DNS) ○ How does DNS help with sending digital information and IP addresses? ○ Example Activities ■ Explore the process of how requesting a web resource works ● Routing ○ How is routing used to send messages / data? ○ Why is redundancy a good thing for the Internet? (fault tolerant) ● Packets and Protocols ○ How data is transmitted? ○ How are internet packets able to find their way to your computer? ○ Example Activities:			

	■ Explain in your own words how a request from your computer travels through the various levels of servers to reach and return the correct webpage and resources? ■ As a class, create a protocol that will allow one classmate to send another classmate a note, without the need for talking to each other. ○ What are the standard protocols for the Internet and how do they work? (TCP/IP, HTTP) ● The Internet and Cybersecurity ○ What are cybercrime and cyberwarfare? ○ How do we network attacks? (certificate authorities, public key encryption)			
9-12.CY.1 Determine the types of personal and organizational information and digital resources that an individual may have access to that needs to be protected. 9-12.CY.5 Recommend multiple actions to take prior and in response to various types of digital security breaches. 9-12.NSD.2 Explain the levels of interaction existing between the application software, system software, and hardware of a computing systems	● Different Types of CPU ● RAM vs. Hard Drive ● Wireless Internet Connections ○ Speed Test ● Security of Cloud Storage ● Ethernet Standards ● Setting Up a Firewall	**CodeHS Fundamentals of Cybersecurity** **Module 10: IT Infrastructure (2-3 weeks/10-15 hours)**	● Internal Components of a Computer ● Peripheral Devices ● Network Devices ● Storage and Network Options ● Network Communication ● Network Management	10.8 IT Infrastructure Quiz

	○ Establish Firewall Rules ● SSH Logs ○ Reading Logs			
9-12.NSD.3 Develop and communicate multi-step troubleshooting strategies others can use to identify and fix problems with computing devices and their components. 9-12.CT.1 Create a simple digital model that makes predictions of outcomes. 9-12.CT.1 Create a simple digital model that makes predictions of outcomes. 9-12.CT.6 Demonstrate how at least two classic algorithms work and analyze the trade-offs related to two or more algorithms for completing the same task. 9-12.CT.9 Systematically test and refine programs using a range of test cases, based on anticipating common errors and user behavior. 9-12.CT.10 Collaboratively design and develop a program or computational artifact for a specific audience and create documentation outlining implementation features to inform collaborators and users 9-12.CY.5 Recommend multiple actions to take prior and in response to various types of digital security breaches. 9-12.DL.2 Communicate and work collaboratively with others using digital tools to support individual learning and contribute to the learning of others.	Troubleshooting: In this project, students will learn more about each step of the troubleshooting methodology and use these steps to repair and improve faulty network systems. ○ Poor Signal Strength ○ Interference	**CodeHS Fundamentals of Cybersecurity** **Module 11: Project: Troubleshooting (2 weeks/10 hours)**	● Troubleshooting Methodology ○ Identify the problem ○ Research past solutions ○ Establish a theory ○ Test the theory ○ Establish a plan of action ○ Implement the solution ○ Verify functionality ○ Document findings	11.1/11.2 Troubleshooting Project
Final Assessment (2 Days)	12.1 Final Assessment is on the CodeHS website, but instructors have the option to create their own. **Modules Covered**: ● What is Cybersecurity? ● Digital Citizenship and Cyber Hygiene ● The ABCs of Cryptography ● Software Security ● Networking Fundamentals			
49 Total Days (with 2 Flex Days)	Two days have been added into the unit pacing in case more days are needed for additional instruction			

Additional Supplementary Units for Advanced Students (optional)	● **Cryptocurrency – 62 activities** (no prerequisites) - Blockchain - Hashing - Proof of Work - Cryptocurrencies - Bitcoin ● **SQL Part II: The SQL – 35 activities** (prerequisite: Software Security) - Filtering - Ordering - Renaming - Joining ● **Web Development – 75 activities** (no prerequisites) - HTML - Formatting Text - Links, Images, Lists, Tables - CSS by Tag, Class, ID