CodeHS

Texas Foundations of Cybersecurity Syllabus
High School (155 contact hours)

Course Overview and Goals

The Foundations of Cybersecurity course is aligned to the 2024 Texas Foundations of Cybersecurity standards. Students will develop the knowledge and skills needed to explore fundamental concepts related to the ethics, laws, and operations of cybersecurity. Students will examine trends and operations of cyberattacks, threats, and vulnerabilities. Students will review and explore security policies designed to mitigate risks. The skills obtained in this course prepare students for additional study in cybersecurity. A variety of courses are available to students interested in this field. Foundations of Cybersecurity may serve as an introductory course in this field of study.

This is a yearlong course that is designed for students with some exposure to computer science, but there are no specific course prerequisites. Students will learn foundational cybersecurity topics including networking fundamentals, software security, system administration, and the basics of cryptography and risk management, all through the CodeHS web-based platform.

The entirely web-based curriculum is made up of a series of learning modules that cover the fundamentals of cybersecurity. Each module is made up of short video tutorials, example programs, quizzes, simulations, programming exercises, and free response prompts. This is not a coding intensive course, but students will learn basic SQL and will utilize basic HTML and JavaScript within specific contexts while being provided with support within those contexts.

Learning Environment: The course utilizes a blended classroom approach. The content is a mix of web-based and physical activities. Students will modify existing code and run it in the browser, investigate cyber related topics and reflect on them and discuss them, create digital presentations, and engage in in-person collaborative exercises with classmates. Teachers utilize tools and resources provided by CodeHS to leverage time in the classroom and give focused 1-on-1 attention to students.

Programming Environment: Students modify and run programs in the browser using the CodeHS online editor. Students will be able to modify text-based programs in HTML, JavaScript, SQL and simulate shell commands. Students will also participate in simulated cyber attacks on safe sites in order to learn how to mitigate cyber attacks. Students will be able to document their processes and discuss best practices for preventing cyber attacks.

Quizzes: Each lesson includes at least one formative short multiple choice quiz. At the end of each module, students take a summative multiple choice quiz that assesses their knowledge of the concepts covered in the module.

Prerequisites: This course is designed for beginners to intermediate computer science students with at least some knowledge and interest in computer science. The course is highly visual, dynamic, and interactive, making it engaging for those new to computer science.

More information: Browse the content of this course at https://codehs.com/course/21289

Course Breakdown

Module 1: What is Cybersecurity? (1 week/5 hours)
This module provides an introduction to cybersecurity. It focuses on why cybersecurity is important, recent threats to cybersecurity, and different careers in the field.

Objectives / Topics Covered	- Course Overview - What is Cybersecurity? - Impact of Cybersecurity - The CIA Triad
Example Assignments / Labs	- Course Overview - 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 - 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: - 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 examples of cybersecurity careers? - 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

Module 2: Digital Citizenship and Cyber Hygiene (1 week/5 hours)
This module includes topics on Internet etiquette and how to stay safe on the world wide web. Students will also look at the potential effects of our digital footprints, how to protect information from online risks, and the implications of cyberbullying. Finally, the module includes how to find and cite quality resources online.

Objectives / Topics Covered	- Digital Footprint and Reputation - Cyberbullying - Internet Safety - Privacy and Security - Information Literacy - Creative Credit and Copyright - Hacking Ethics
Example Assignments / Labs	- 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? - How can you maintain your digital footprint? - Cyberbullying - What is cyberbullying? - What are the impacts of cyberbullying? - What do you do if you are being bullied? - What do you do if you see bullying? - Example activities: - Explore cyberbullying scenarios: What would you do? - Internet Safety - What are some ways to stay safe online? - 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 your 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 - Privacy and Security - How can you keep your data private? - What are some privacy best practices? - Information Literacy - How can you effectively search the Internet? - What makes a source credible? - 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, gray)
	  ○ 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

Module 3: Project: PSA (1 week/5 hours)

Students create a project to apply Digital Citizenship and Cyber Hygiene content by creating a PSA.

Objectives / Topics Covered	● Project: PSA
Example Assignments / Labs	● 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.

Module 4: The ABCs of Cryptography (1 week/5 hours)

In this module, students will dive into the history of cryptography systems, the motivation behind using encryption systems, and basic cryptography systems. Additionally, they will explore topics on how to use cryptography, cryptology, and cryptanalysis to decode a message without the use of a key.

Objectives / Topics Covered	● Cryptography, Cryptology, Cryptanalysis ● History of Cryptography ● Why do we Need to Encrypt Data? ● Basic Cryptography Systems: Caesar Cipher ● Basic Cryptography Systems: Cracking the Caesar Cipher ● Basic Cryptography Systems: Vigenère Cipher ● Hash Functions ● Digital Certificates

Example Assignments / Labs	● 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
	    ■ 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?
	○ 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 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

Module 5: Project: Classic Cipher Newscast (1 week/5 hours)

Students complete a project to apply cryptography content.

Objectives / Topics Covered	● Project: Classic Cipher Newscast
Example Assignments / Labs	● Project: Create a Newscast ○ Students work collaboratively to research a **classic cipher** (beyond Caesar and Vigenere) 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.

Module 6: System Administration (3 weeks/15 hours)

Students will compare and contrast common operating systems (Windows, Linux, OS) and explain the importance of application security. They will investigate security options and implement user accounts to enforce authentication and authorization. Students will also demonstrate how to work with basic and advanced command prompts.

Objectives / Topics Covered	● Operating Systems ● Software and Applications ● Software Licenses ● Application Security ● Browser Configuration ● System Administration ● Command Line Interface
Example Assignments	● Understanding Operating Systems

/ Labs	- 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

Module 7: Software Security (3 weeks/15 hours)

In this module, students will learn what happens when running a web application and how to look inside web apps using developer tools, source code, and more. They will learn basic SQL and common attacks like SQLi. Students will also be able to recommend solutions for flawed security systems.

Objectives / Topics Covered	- Clients, Servers, Databases - SQL Overview - What is SQL? - Structuring Data in SQL - Basic Querying in SQL - Filtering Queries in SQL - Common Security Problems - SQL Injection - SQLi Overview - Types of SQLi - Preventing SQLi
Example Assignments / Labs	- SQL Overview - What is SQL? - How do we structure data using SQL? - How do we query databases using SQL? - Example activities: - Use the SELECT statement to query a database - 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 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 do 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

Module 8: Project: Security Assessment Report (SQLi) (1 week/5 hours)

Students complete a project that has them test a website for vulnerabilities and write a security assessment report based on their findings.

Objectives / Topics Covered	● Project: Security Assessment Report

Example Assignments / Labs	● Project: Security Assessment Report
	    ○ SQLi Testing
	    ○ Create a Security Assessment Report
	    ○ Project Reflection

Module 9: Networking Fundamentals (3 weeks/15 hours)

This module explores the structure and design of the internet and networks, and how this design affects the reliability of network communication, the security of data, and personal privacy. Students will learn how the Internet connects computers all over the world by use of networking protocols.

Objectives / Topics Covered	● Introduction to the Internet ● Notational Systems ● Data Representation ● Internet Hardware ● Internet Addresses ● Domain Name System (DNS) ● Routing ● Packets and Protocols ● Viewing a Webpage ● Access Control ● Impact of the Internet

Example Assignments / Labs	● Introduction to the internet
	    ○ What is the Internet? How does it work? What has 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
	○ Vocabulary: bandwidth, bitrate, latency
	○ 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
	○ Vocabulary: Internet Protocol (IP)
	○ How do IP addresses compare to postal addresses?
	○ How do 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)
	● Access Control
	○ How can you ensure secure authentication?
	○ What is 2FA?

Module 10: IT Infrastructure (2 weeks/10 hours)

Students will learn about the physical elements of computers and networking such as motherboards, RAM, routers, and the use of port numbers, ethernet and wireless devices.

Objectives / Topics Covered	● Internal Components of a Computer ● Peripheral Devices ● Network Devices ● Storage and Network Options ● Network Communication

	● Network Management ● Private Networks
Example Assignments / Labs	● Different Types of CPU ● RAM vs. Hard Drive ● Wireless Internet Connections 　○ Speed Test ● Security of Cloud Storage ● Ethernet Standards ● Setting Up a Firewall 　○ Establish Firewall Rules ● SSH Logs 　○ Reading Logs

Module 11: Project: Troubleshooting Project (1 week/5 hours)

Students will explore the troubleshooting methodology and utilize it to solve sample IT support issues.

Objectives / Topics Covered	● 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
Example Assignments / Labs	● 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

Module 12: Project: IT Professional (2 weeks/10 hours)

In this project, students will explore cybersecurity career pathways and build skills that will be needed within these fields such as communication.

Objectives / Topics Covered	● Building a Resume ● Cybersecurity Career Pathways ● Customer Service and Communication ● Contributing to a Knowledge Base ● Creating an Instructional Video
Example Assignments / Labs	● Act it out! Pair up with a partner and create a short script of a customer support scenario based on a common mobile device issue. ● Write a KB Article: Create an internal knowledge base article that will be shared with other technicians. ● Star in a Video! Create a 2-5 minute video tutorial based on a common mobile device issue

Module 13: Project: Digital Forensics (1 week/5 hours)

In this project, students will explore aspects of digital forensics that include the types of data that can be collected and used as well as the chain of custody that must be kept throughout the whole process.

Objectives / Topics Covered	● Chain of Custody ● Event Logs ● Exif Data
Example Assignments / Labs	● Students will work through fictitious forensic cases to practice collecting, examining, analyzing and reporting on data that they have unveiled.

Module 14: Cyber Defense (4 weeks/20 hours)

Students will explore different types of network attacks and how to build up security walls to defend against them.

Objectives / Topics Covered	● Network Attacks ● Malware Types and Prevention ● Common Network Attacks ● Additional Attacks ● Cross-Site Scripting ● Internal Threats

Example Assignments / Labs	● Network Attacks
	   ○ What is the difference between a threat, a vulnerability and an exploit?
	   ○ What do cyberattacks commonly take advantage of?
	   ○ Example activity:
	      ■ What are the open ports designated for?
	      ■ What do you notice about the commonly attacked ports and the open ports?
	● Malware Types and Prevention
	   ○ What is the difference between anti-malware and antivirus software?
	   ○ What is a virus, work, trojan, rootkit?
	   ○ Example activity:
	      ■ What type of built-in malware protection does your operating system provide?
	      ■ View all of the running processes on your computer.
	● Common Network Attacks
	   ○ What is DoS and DDoS?
	   ○ What is spoofing and why can it be dangerous?
	   ○ Example activity:
	      ■ What makes social engineering such an effective technique for hackers?
	      ■ Does the IoT make us more or less vulnerable to DDoS attacks?
	● Additional Attacks
	   ○ What is a rainbow table?
	   ○ What is a zero-day attack?
	   ○ What is a botnet and how are they used?
	   ○ Example activity:
	      ■ Explore the United States Computer Emergency Readiness Team (US-CERT) web page and draw conclusions about the current environment of cyber threats.
	● Cross-Site Scripting
	   ○ How does XSS attack a website?

	○ Who is the victim in an XSS attack?
	○ Example activity:
	   ■ Try some basic XSS on Google's Tutorial for XSS site.
	   ■ What are some ways to detect XSS vulnerabilities on websites?
	● Internal Threats
	○ What is the main function of UEFI?
	○ What can you do to prevent someone from booting an alternative operating system?
	○ What is data loss prevention?
	○ Example activity:
	   ■ Explore your computer's BIOS/UEFI!
	   ■ Which data breaches can be prevented by DLP tools?

Module 15: Project: Put It In Writing! (1 week/5 hours)

In this project, students will develop a training policy that informs employees on matters of network security and details the company policy on preventative measures employees should take.

Objectives / Topics Covered	● User Training ● Incident Response Plans ● Data Policy and Privacy ● Change Management
Example Assignments / Labs	● Develop a training policy that informs employees on matters of network security. ● Create an Incident Response Plan. ● Develop a strong data policy for a company. ● Develop a change management plan to ensure that the new policy is adopted and implemented by the team effectively.

Module 16: Risk Management (4 weeks/20 hours)

Students will demonstrate skills in conducting vulnerability scans and recognizing vulnerabilities in security systems. They will conduct a security audit and examine port scanning, packet sniffing, and proxy servers to discover exploits in a system. Students will recommend security measures to mitigate the vulnerabilities.

Objectives / Topics Covered	● Identifying Risks ● Assessing Risks ● Risk Response ● Penetration Testing

Example Assignments / Labs	● Identifying Risks
	○ What are the steps of a risk assessment?
	○ What potential risks can be checked by a vulnerability scan?
	○ How is packet sniffing and password cracking used in a legal manner?
	○ Example Activity:
	   ■ What information can be determined by an IP address?
	   ■ Create a "story" using the data shown of what was happening during this packet transfer.
	   ■ Why is past data important in trying to assess how to best set up a cyber defense system for the present?
	● Assessing Risks
	○ What is a race condition?

	○ What is error handling and input handling? Why is input validation important?
	○ What is buffer overflow and integer overflow?
	○ Example Activity:
	■ Draft an argument that insists upon the importance of upgrading a system that has reached its end-of-life.
	■ Read a scenario and access the level of risk.
	■ Examine (and fix) poor input and error handling.
	● Risk Response
	○ What are some risk response strategies?
	○ How do you calculate the SLE and ALE of a threat event?
	○ How do you effectively and efficiently mitigate risk?
	○ Example activity:
	■ Read a sample assessment report. What types of methods did the assessors use to collect data? Do you feel this report provides you with sufficient information to determine priorities and next steps?
	■ What role might chaos engineering play in risk assessment and response?
	● Penetration Testing
	○ What are the stages of penetration testing?
	○ What tools are used in passive reconnaissance?
	○ What is an escalation of privilege?
	○ Example activity:
	■

Module 17: Project: The Game of Risk (2 weeks/10 hours)

In this project, students will design and create a board game or a card game that will help players to identify randomized security vulnerabilities and their appropriate defenses.

Objectives / Topics Covered	● Quantitative and Qualitative SLE ● Prototypes ● Testing
Example Assignments / Labs	● Create a Game: Students will design and create a board game that will help players to identify randomized security vulnerabilities and their appropriate defenses. They will create a prototype and test the game to receive feedback to consider before building their final game.

Supplementary Unit Guide:

These units can be used during the course for added practice or after the course has been completed for further review.

Supplementary Unit	Prerequisite/Recommended Unit(s)	# of activities
Cryptocurrency - Blockchain - Hashing - Proof of Work - Cryptocurrencies - Bitcoin	No prerequisites	62
SQL Part II: The SQL - Filtering - Ordering - Renaming - Joining	Software Security	35
Web Development - HTML - Formatting Text - Links, Images, Lists, Tables - CSS by Tag, Class, ID	No prerequisites	75
Midterm	Modules Covered: ● What is Cybersecurity ● Digital Citizenship and Cyber Hygiene ● The ABCs of Cryptography	1
Final	Modules Covered: ● What is Cybersecurity? ● Digital Citizenship and Cyber Hygiene ● The ABCs of Cryptography ● Software Security ● Networking Fundamentals	1
Final Course Project	Choose Your Own Adventure ● Research ● Choose Target Audience ● Draft Presentation ● Draft a Flyer	4