

South Carolina Cybersecurity Fundamentals Syllabus

High School (110-130 Contact Hours)

Course Overview and Goals

In this course, students examine the core concepts and terminology of cyber security and information assurance, integrating the importance of cyber threats and vulnerabilities, computer and network architecture, network security, operating systems, operational security, cryptography, system security, incident handling, and other topics.

Learning Environment

The course utilizes a blended classroom approach. The content is a mix of web-based and physical activities. Each module of the course is broken down into lessons. Lessons are composed of short video tutorials, interactive learning pages, quizzes, explorations, simulations, and free-response prompts. Each module ends with a comprehensive quiz that assesses students' mastery of that module's material.

More Information

Browse the content of this course at <https://codehs.com/course/28167/overview>

Prerequisites

This course is designed for complete beginners with no previous background in computer science. The course is highly visual, dynamic, and interactive, making it engaging for those new to computer science.

Technology Requirements

To complete all activities and exercises in this course, students must have access to the 3rd party sites and tools listed here: [South Carolina Cybersecurity Fundamentals Course Links](#)

Course Breakdown

The full standards alignment can be found at https://codehs.com/standards/framework/SC_CYBER/mapping/2219

Module 1: Cybersecurity and You (3 weeks/15 hours)

In this module, students delve into key areas such as personal data collection, the reliability of online information, cyber ethics and laws, personal data security, cybersecurity essentials, and strategies to combat common cyber threats and their prevention, equipping individuals with the knowledge to navigate the digital landscape responsibly and securely.

Topics Covered	<ul style="list-style-type: none"> ● Digital Footprint ● Personal Data Collection ● Media Literacy ● Cyber Ethics and Laws ● Authentication ● Cybersecurity Essentials ● Common Cyber Attacks
Example Assignments	<ul style="list-style-type: none"> ● Cyberbullying Case Study <ul style="list-style-type: none"> ○ Students read a realistic cyberbullying scenario and apply guidance from course materials to answer structured reflection questions about appropriate responses and prevention. ● Take a Stand: Location Tracking <ul style="list-style-type: none"> ○ Students use the "Take a Stand" thinking routine to explore multiple perspectives on school-based location data collection, then defend a position in writing. ● Phishing Response <ul style="list-style-type: none"> ○ Students analyze a phishing scenario, identify the tactics used, and explain how to recognize and respond to the attack.

Module 2: Cryptography (2 weeks/10 hours)

In this module, students will dive into the history of cryptography systems, the motivation behind using encryption systems, and modern cryptography systems. This includes explaining the core concepts of Public Key Infrastructure and hash functions. Students will also explore the importance of digital certificates, and authentication methods.

Topics Covered	<ul style="list-style-type: none"> ● History of Cryptography ● Symmetric Encryption ● Cipher Methods ● Asymmetric Encryption ● Public Key Infrastructure ● Digital Certificates ● Authentication Methods
Example Assignments	<ul style="list-style-type: none"> ● Enhanced Caesar Cipher <ul style="list-style-type: none"> ○ Students strengthen a Caesar cipher by adding a transposition step, then encrypt and decrypt a message using the enhanced method and analyze why layered ciphers are more secure. ● Diffie-Hellman Visualizer Reflection <ul style="list-style-type: none"> ○ Students trace how two parties establish a shared secret key over a public channel using an interactive visualizer, then explain the key exchange process in their own words. ● Digital Certificates Response <ul style="list-style-type: none"> ○ Students explain how digital certificates verify identity in HTTPS connections and describe the role of a certificate authority in

	establishing trust.
--	---------------------

Module 3: Project: Create an Escape Room (1 week/5 hours)

In this module, students apply cryptography concepts by designing a themed escape room built around original cryptographic puzzles, then test and refine the experience based on peer feedback.

Topics Covered	<ul style="list-style-type: none"> ● Applied Cryptography ● Puzzle Design ● Iterative Testing
Example Assignments	<ul style="list-style-type: none"> ● Plan and Create Puzzles <ul style="list-style-type: none"> ○ Students design at least three different types of cryptographic puzzles aligned to their chosen escape room theme and difficulty level. ● Test the Escape Room <ul style="list-style-type: none"> ○ Students conduct a full run-through of their escape room with peer testers, collect feedback, and revise clues, props, and puzzle difficulty before finalizing the design.

Module 4: System Administration (3-4 weeks/15-20 hours)

In this module, 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.

Topics Covered	<ul style="list-style-type: none"> ● Operating Systems ● OS Comparison ● Hardware Compatibility ● Laptops and Mobile Devices ● Software Applications ● Software Licenses ● Application Security ● Browser Configuration ● Command Line Interface
Example Assignments	<ul style="list-style-type: none"> ● Lab: Configuring a Computer <ul style="list-style-type: none"> ○ Students follow a set of setup specifications to configure a computer system, documenting each configuration step and decision. ● Do I Need a Software License? <ul style="list-style-type: none"> ○ Students analyze a scenario in which a student developer is about to publish an app and must determine what software licenses are required before releasing it. ● Lab: Navigating with the CLI

	<ul style="list-style-type: none"> ○ Students practice creating, moving, and managing files and directories using command line interface commands on their operating system.
--	---

Module 5: IT Concepts (3-4 weeks/15-20 hours)

In this module, students explore 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.

Topics Covered	<ul style="list-style-type: none"> ● Binary Representation ● Text and Number Encoding ● Image Encoding ● Internet Architecture ● IP Addresses ● Routing and Packets ● Web Protocols ● OSI Model ● Impact of the Internet
Example Assignments	<ul style="list-style-type: none"> ● Create a Black and White Pixel Image <ul style="list-style-type: none"> ○ Students design pixel art by representing image data in binary values, applying their understanding of how computers encode and store visual information. ● Troubleshooting with the OSI Model <ul style="list-style-type: none"> ○ Students analyze a network problem scenario, identify which OSI layer is responsible for the issue, and propose a resolution. ● An Internet Story <ul style="list-style-type: none"> ○ Students trace the complete journey of an HTTP request from a browser to a web server, describing the role of each protocol and component along the way.

Module 6: IT Infrastructure (3-4 weeks/15-20 hours)

In this module, 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.

Topics Covered	<ul style="list-style-type: none"> ● Internal Components ● Peripheral Devices ● Storage Options ● Network Devices ● Distribution Frames ● Network Options ● Network Communication ● Network Management
----------------	--

Example Assignments	<ul style="list-style-type: none"> ● Lab: Computer Disassembly <ul style="list-style-type: none"> ○ Students identify and document internal hardware components by examining a physical or virtual computer, labeling each part and describing its function. ● Peripheral Port Scavenger Hunt <ul style="list-style-type: none"> ○ Students locate and identify all ports and connectors on available devices, cataloguing each port type and its use case. ● Lab: Design a Distribution Frame <ul style="list-style-type: none"> ○ Students design a structured cabling distribution frame layout for a building network, justifying their device placement and cable routing decisions. ● Windows Command Prompt Spy <ul style="list-style-type: none"> ○ Students use command prompt networking tools to investigate active connections and running processes, analyzing what they reveal about system activity.
---------------------	---

Module 7: 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. In this project, students will explore the troubleshooting methodology and utilize it to solve sample IT support issues.

Topics Covered	<ul style="list-style-type: none"> ● IT Career Exploration ● Customer Communication ● Troubleshooting Methodology ● Technical Documentation ● Knowledge Base Articles ● Instructional Video Creation
Example Assignments	<ul style="list-style-type: none"> ● Act it Out! <ul style="list-style-type: none"> ○ Students role-play an IT support call at a fictional company, applying professional communication skills to help a user who has forgotten their password. ● You're On Your Own Now! <ul style="list-style-type: none"> ○ Students independently diagnose and resolve two IT support tickets using the troubleshooting methodology, without step-by-step guidance from the course. ● Draft a KB Article <ul style="list-style-type: none"> ○ Students research and write an external knowledge base article for a customer audience, then revise it based on peer feedback before submitting a final version.

Module 8: Data Security (3-4 weeks/15-20 hours)

In this module, students will learn about the benefits and dangers of collecting and storing large sets of data. They will learn how to prevent attacks such as SQLi and XSS using programming controls. Students will also learn about risk management and how to identify, assess, prioritize, and minimize risks.

<p>Topics Covered</p>	<ul style="list-style-type: none"> ● Data as a Resource ● Databases and SQL ● XSS and SQL Injection ● Developer Tools CTF ● Environmental Controls ● Penetration Testing ● Risk Identification and Assessment ● Monitoring and Recovery
<p>Example Assignments</p>	<ul style="list-style-type: none"> ● Dev Tools Capture the Flag <ul style="list-style-type: none"> ○ Students use browser developer tools to find hidden flags embedded in a web page, exploring how developers can unintentionally expose sensitive data in client-side code. ● XSS Response <ul style="list-style-type: none"> ○ Students compare cross-site scripting and SQL injection attacks, explain how each works, and describe the threat to a non-technical audience. ● Pen Testing Report <ul style="list-style-type: none"> ○ Students conduct a guided penetration test in a simulated environment, documenting reconnaissance findings, exploited vulnerabilities, and recommendations in a formal report. ● Prioritize Risks and Reduce Risk <ul style="list-style-type: none"> ○ Students assess a set of security vulnerabilities, rank them by likelihood and impact using a risk matrix, and propose mitigation strategies for each.

Module 9: Project: The Game of Risk (1 week/5 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.

<p>Topics Covered</p>	<ul style="list-style-type: none"> ● Risk Identification ● Security Vulnerabilities ● Game Design and Prototyping ● Iterative Improvement
<p>Example Assignments</p>	<ul style="list-style-type: none"> ● Brainstorm and Plan <ul style="list-style-type: none"> ○ Students research game types, collaboratively define their game's objective and rules, and produce a materials list and rough design plan. ● Prototype Game and Instructions <ul style="list-style-type: none"> ○ Students build a complete rough prototype of their game, including all cards, boards, or components, along with written instructions a

	<p>new player could follow.</p> <ul style="list-style-type: none"> ● Improve Your Game <ul style="list-style-type: none"> ○ Students review tester feedback, identify weaknesses in game balance and clarity, and revise the game before creating and submitting the final version.
--	---

(Optional Module) Career and Workplace (10-15 hours)

Students explore computing career pathways, student organizations, certification opportunities, and workplace skills. They practice professional communication through resume writing and mock interviews, and learn essential personal safety practices in technology environments. Students taking more than one CodeHS course in their pathway may have already completed some of these activities in a previous course.

<p>Topics Covered</p>	<ul style="list-style-type: none"> ● Computing careers ● Student organizations ● Certifications ● Resume and interviewing ● Workplace safety
-----------------------	---