

Teaching AP Cybersecurity

CodeHS Professional Development Course

Details

- Course delivery method: Online delivery
- Contact Hours: Approximately 40 contact hours
- Prerequisite(s): N/A
- Recommended: Best for individuals planning on teaching AP Cybersecurity within a year of completing this course

Description

This course equips participants with the skills to teach AP Cybersecurity to high school students. Participants will explore core cybersecurity concepts—including social engineering; cryptography; risk assessment; and network, device, and application security—through CodeHS lessons. They will analyze real-world attack and defense strategies, configure security controls, and examine how AI is used in cyberattacks and cyber defense. Additionally, participants will explore best practices for engaging and accessible cybersecurity instruction, learn strategies for facilitating collaboration with all levels of students in a blended classroom, and become familiar with the format of the AP course and how to best prepare students for the exam. By the end of this course, participants will be empowered with the skills, pedagogical knowledge, and confidence to run a successful AP Cybersecurity class.

Course Goals

Educators will understand the importance of providing quality cybersecurity instruction to diverse learners. Participants will be prepared to teach a successful and engaging AP Cybersecurity course, with a strong understanding of content and how to facilitate student learning.

Lab Environment

Teachers complete hands-on labs and exercises in the browser using the CodeHS editor and integrated terminal. No downloads or additional software are required.

Course Objectives

1. Participants will be prepared to teach students how to identify common cyberattacks and defend against them across physical, network, device, and application layers.
2. Participants will learn how to assess risk and share those skills with students.
3. Participants will learn about a variety of IT security controls and skills, from setting up firewalls and access controls, to encryption and analyzing log files to better explain these concepts with students.
4. Participants will be prepared to teach students how AI is used in both cyber attacks and cyber defense.
5. Participants will explore lessons and activities that make cybersecurity instruction engaging, accessible, and inclusive for all students.
6. Participants will be equipped with strategies and resources to prepare their students for success on the AP Cybersecurity exam.

Course Breakdown (40 hours)

Note: The online course is self-paced, so times listed are estimates for each module. Participants may complete each module in more or less time than is noted. Browse the content of this course at https://codehs.com/course/AP_Cyber/overview

Title	Description	Approximate Time
Module 1: Welcome	Explore the course syllabus, learn how to get help, connect with the CodeHS Educator Community, and set learning goals.	1 Hour
Module 2: How CodeHS Works	Learn how to use the CodeHS platform effectively in the classroom.	5 Hours
Module 3: What is AP Cybersecurity?	Overview of the College Board's AP Cybersecurity curriculum framework and its five units, the AP Classroom Resources and Exam details, and the CodeHS AP Cybersecurity curriculum.	5 Hours
Module 4: Teaching AP Cyber - Planning Your First Month	Strategically plan the first month of instruction using CodeHS resources, beginning with Unit 1 and the start of Unit 2. Lessons model effective instructional techniques across topics like social engineering, password attacks, AI in cybersecurity, the CIA Triad, risk assessment, and securing physical spaces.	8 Hours
Module 5: Teaching AP Cyber - Spotlight Lessons	Deep dives into more complex topics from Units 2 through 5, addressing areas of common student difficulty such as network attacks, firewall configuration, cryptography, and log analysis.	7 Hours

Module 6: Tools and Resources for Teaching AP Cybersecurity	This module covers all of the tools and resources on CodeHS for supporting AP Cybersecurity teachers, including the CodeHS AP Cybersecurity Hub, Question of the Day, and optional review of the CodeHS Cyber Range that students can access as a student.	4 Hours
Module 7: Computer Science Pedagogy	This module examines key teaching strategies for computer science, including fostering computational thinking, managing cognitive load, and employing a range of instructional approaches.	5 Hours
Module 8: Project-Based Learning & CS	This module prepares educators to implement high-quality Project-Based Learning (PBL) strategies for computer science.	3 Hours
Module 9: Collaboration in CS	Learn what collaboration in the cybersecurity classroom looks like and how to foster a collaborative, inclusive setting.	2 Hours
Module 10: Course Wrap Up	Complete end-of-course survey and get the course completion badge.	< 1 Hour

Assessment and Learning Resources

- To pass the course, participants must complete 85% of the course assignments and activities.
- Participants will receive formative feedback and may redo assignments as needed.
- CodeHS PD instructors will communicate to participants and grade work through the CodeHS platform on a daily basis Monday-Friday.
- The CodeHS Learning Management System includes all assigned readings, articles, videos, quizzes, scenario-based examples, lab exercises, and other assignments in each module's content area.
- CodeHS Cyber Range access granted to teachers as students to explore lessons and get hands-on experience with the tool to understand specific lessons and how the Cyber Range and similar tools can be leveraged in the classroom.