Identify cybersecurity threats and protect against them. Detect intrusions and respond to attacks. Begin to examine your own digital footprint and better defend your own personal data. Learn how organizations protect themselves in today's world.

Whether seeking a career in the growing field of cybersecurity or learning to defend their own personal data or a company's data, students in Cybersecurity establish an ethical code of conduct while learning to defend data in today's complex cyberworld.

Cybersecurity is a full-year course implemented in 10th grade or above. The course is designed to expose high school students to the ever-growing and far-reaching field of cybersecurity. This will be accomplished through problem-based learning, where students roleplay as cybersecurity experts and train as cybersecurity experts do.

Cybersecurity is designed with strong connections to the National Cybersecurity Workforce Framework (also known as the NICE Framework or NCWF). Created by the National Institute of Standards and Technology (NIST), this framework identifies standards that have been developed by numerous academic, industry, and government organizations. The framework objectives address topics that span K-12 education and guide learning progressions. The objectives also incorporate many of the big ideas and learning objectives outlined by the College Board and addressed in AP CSP and AP CSA. In addition, the course integrates Computer Science Teachers Association (CSTA) standards.

The course provides students with a broad exposure to the many aspects of digital and information security, while encouraging socially responsible choices and ethical behavior. It inspires algorithmic and computational thinking, especially "outside-the-box" thinking. Students explore the many educational and career paths available to cybersecurity experts, as well as other careers that comprise the field of information security. The following is a list of the units of study in the course:

Unit 1	Personal Cybersecurity
Unit 2	System Security
Unit 3	Network Security
Unit 4	Applied Cybersecurity

Unit 1: Personal Cybersecurity

Students learn the basic concepts of cybersecurity by leveraging their familiarity with technology they use every day, such as mobile devices and apps, as well as exploring the risks associated with how they use their email, personal files, and social networking sites.

Personal Cybersecurity

Lesson 1.1	Introduction to Cybersecurity
Lesson 1.2	Security and the Internet
Lesson 1.3	Protect Your Data

Lesson 1.1 Introduction to Cybersecurity
Students learn personal and digital security, describe why they are important, and learn to be safe consumers of digital information in a variety of contexts.

Activity 1.1.1	Code of Conduct
Activity 1.1.2	Password Protection and Authentication
Activity 1.1.3	Email and Social Media Security Risks
Project 1.1.4	Save the Day

Lesson 1.2 Security and the Internet
Students learn that the internet is a loosely controlled collection of computers that are networked together, secured by firewalls. They learn basic types of malware, security features of their browser, and how not to be a victim. They learn about files and processes, how to manage them, and how to identify suspicious data (potential malware). At the end of the lesson, students roleplay as victims of a malware attack. They determine how the attack occurred, improve the security of the firewall, and secure their browser.

Activity 1.2.1	Firewalls and Malware
Activity 1.2.2	Securing Your Browser
Activity 1.2.3	Managing Your Data
Project 1.2.4	It’s a Trap!

Lesson 1.3 Protect Your Data
Students use their knowledge about files, directories, processes, browsers, suspicious emails, and malware to solve the unit problem.

Problem 1.3.1	A Dangerous Situation

Unit 2: System Security

Students broaden their cybersecurity knowledge from a personal system to a networked system. They learn how to assess the value of information security and delve deeper into types of malware. They learn the security vulnerabilities of web services and how to secure an e-commerce site.

System Security

Lesson 2.1	Information Architecture
Lesson 2.2	Information Vulnerabilities
Lesson 2.3	Client-Server Security
Lesson 2.4	The Hacked Site

Lesson 2.1 Information Architecture
Students delve into information confidentiality and how it relates to information integrity and assurance, comparing the value and the risks of sharing information. Students learn how host names are related to digital addresses, demystify the “cloud”, learn how networks evolve, and explore the security of a small network.

Activity 2.1.1	Confidentiality, Integrity, and Availability
Activity 2.1.2	LAN Architecture
Project 2.1.3	Analyzing a Network

Lesson 2.2 Information Vulnerabilities
Students learn more about the types of malware that are threats to information and their delivery systems. They learn how attacks can occur using website applications and the back-end services that support them. They explore a vulnerable web server and improve its security measures.

Activity 2.2.1	More on Malware
Activity 2.2.2	The Vulnerable Host
Activity 2.2.3	Client/Server Vulnerabilities
Project 2.2.4	Secure the Server

Lesson 2.3 Client-Server Security
Students delve deeper into how malware propagates and research the symptoms of various exploits. They analyze and secure one of the most common vulnerabilities: a web server hosting client applications.

Activity 2.3.1	Stopping the Spread of Malware
Activity 2.3.2	Analyzing an App
Activity 2.3.3	Front-End Back-End Attacks
Project 2.3.4	Secure the Client

Lesson 2.4 The Hacked Site
Students learn how information can be safely and securely exchanged on a public network. In the end-of-unit problem, students discover a breach, identify the security vulnerabilities, and enhance the system to secure it.

Activity 2.4.1	Paired Key Encryption
Activity 2.4.2	E-commerce Enrichment

Unit 3: Network Security

Students learn the technical aspects of a highly networked world and the risks to information we all share. They learn networking concepts, such as subnets, dynamic host configuration, packet analysis, and virtual networks. They learn the types of malware that can attack systems on a network and how to secure and protect a system against them.

Network Security

Lesson 3.1	Files and Processes
Lesson 3.2	Attacks from the Net
Lesson 3.3	Analyzing the Net
Lesson 3.4	The Security Race

Lesson 3.1 Files and Processes

Students learn how an operating system organizes information using command line tools to manage and secure digital information. Students learn about user and system processes and how malware spreads around a network. Then, they identify suspicious software running on the system and determine the problems it may have caused.

Activity 3.1.1	Commanding the OS
Activity 3.1.2	Processes
Project 3.1.3	Find the Secrets

Lesson 3.2 Attacks from the Net

Students explore network topologies and go deeper down the abstraction path to learn more about network security. They analyze network traffic, find patterns that may represent exploits, and identify security vulnerabilities.

Activity 3.2.1	Exploring Network Security
Activity 3.2.2	Exploring Security Frameworks
Activity 3.2.3	Where Can I Learn More About Cybersecurity?
Project 3.2.4	Find the Exploits

Lesson 3.3 Analyzing the Net

Students analyze network traffic to witness, and then protect against, a malware attack. Students analyze packets to find telltale signs and patterns of malicious exploits. They apply what they've learned to perform a penetration test and secure a network against further attacks.

Activity 3.3.1	Packets
Activity 3.3.2	Attack Analysis
Problem 3.3.3	The Attack

Lesson 3.4 The Security Race

Students race to see which team can identify an exploit, stop the attack, secure the system, and make improvements to prohibit future attacks.

Problem 3.4.1	The Security Race

Unit 4: Applied Cybersecurity

Students explore cybersecurity in an applied field. They learn methods of cryptography and practice basic tenants of digital forensics. They process a crime scene to solve the mystery and explore the possible consequences of the crime.

Applied Cybersecurity

Lesson 4.1	Cryptography
Lesson 4.2	Digital Forensics
Lesson 4.3	Red-Team, Blue-Team

Lesson 4.1 Cryptography

Students learn the history of encryption and ciphers, and use frequency predictors to try to break codes. They practice data hiding techniques, such as cryptography and steganography. Finally, they attempt to decrypt each other's encrypted messages.

Activity 4.1.1	Ciphers and Early Cryptography
Activity 4.1.2	Uses of Encryption
Problem 4.1.3	Decrypt the Encrypted

Lesson 4.2 Digital Forensics

Students learn the process of gathering digital evidence, analyzing it, tracing the criminal through their digital footprint, and preparing to prosecute the criminal.

Activity 4.2.1	Tools of the Trade
Activity 4.2.2	Tracing Identity
Activity 4.2.3	Make Your Discovery
Problem 4.2.4	Solve the Crime!

Lesson 4.3 Red-Team, Blue-Team

Students compete to infiltrate and defend a network.

Problem 4.3.1	Red-Team, Blue-Team