CSNP
CYBERSECURITY NON-PROFIT

High School Cybersecurity Curriculum

A comprehensive lesson plan for grades 9-12 preparing students for the digital workforce

CAREER READY

INDUSTRY ALIGNED

COURSE OVERVIEW

Building Tomorrow's Security Professionals

What Students Will Learn

This curriculum introduces high school students to fundamental cybersecurity concepts through hands-on, practical applications. Students explore real-world threats, learn defensive strategies, and develop critical thinking skills essential for protecting digital assets.

Each module builds progressively, connecting technical knowledge with career pathways and industry certifications.

Course Structure

- 8 core instructional modules
- Interactive labs and simulations
- Capstone project options
- Assessment rubrics and career connections
- Certification pathway guidance

Understanding the Cybersecurity Landscape

Why It Matters

Cyber attacks occur every 39 seconds, affecting one in three Americans annually. Students need to understand both the scope of threats and the growing demand for security professionals.

Career Growth

The cybersecurity workforce gap exceeds 3.5 million positions globally. This field offers stable, high-paying careers with opportunities across all industries.

Real-World Impact

From protecting healthcare records to securing financial systems, cybersecurity professionals defend critical infrastructure that keeps society functioning.

Module 1: Introduction to Cybersecurity

01

Core Concepts

CIA Triad (Confidentiality, Integrity, Availability), threat actors, attack vectors, and defense-in-depth strategies

02

Historical Context

Evolution from early computer viruses to modern ransomware and nation-state attacks

03

Industry Roles

Security analyst, penetration tester, incident responder, security architect, and compliance specialist

04

Ethical Framework

Legal boundaries, responsible disclosure, and the importance of ethical hacking principles

Teaching Tip: Use recent headline breaches as discussion starters to connect theory with current events.

Module 2: The Threat Landscape

1

Malware Types

Viruses, worms, trojans, ransomware, spyware, and rootkits—understanding how each operates and spreads

2

Attack Methodologies

Phishing, DDoS, man-in-the-middle, SQL injection, and zero-day exploits

3

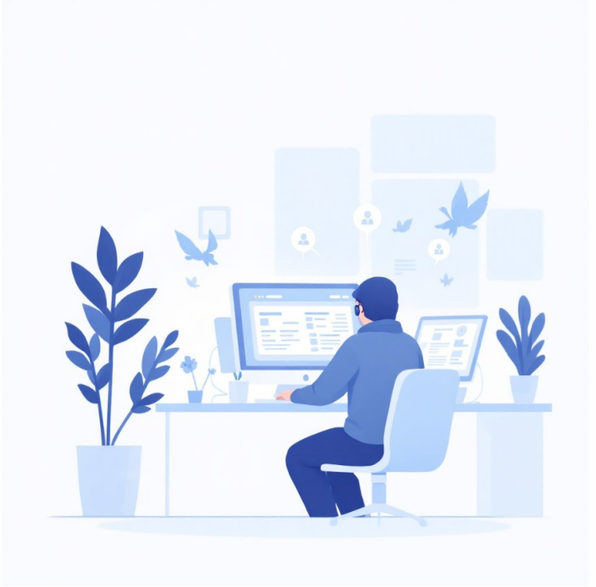
Threat Actors

Hacktivists, cybercriminals, nation-states, and insider threats—motivations and tactics

4

Emerging Threats

IoT vulnerabilities, AI-powered attacks, deepfakes, and supply chain compromises



Activity: Students research a recent major breach, identify the attack vector, and present defensive strategies that could have prevented it.

Module 3: Network Security Fundamentals

Network Architecture

OSI model, TCP/IP protocols, ports and services, network segmentation, and the concept of trust boundaries in enterprise environments.

Defense Mechanisms

Firewalls, intrusion detection/prevention systems, VPNs, network monitoring tools, and implementing security zones.

Wireless Security

WPA3 encryption standards, rogue access points, evil twin attacks, and securing WiFi networks against common vulnerabilities.

Lab Exercise: Students use Wireshark to analyze network traffic, identify protocols, and spot suspicious activity in packet captures.

Module 4: Cryptography Essentials

Encryption Basics

Symmetric vs. asymmetric encryption, understanding how AES and RSA protect data both at rest and in transit.

Hashing & Integrity

Hash functions (SHA-256), digital signatures, certificates, and maintaining data integrity through cryptographic methods.

Practical Applications

SSL/TLS for web security, encrypted messaging, blockchain fundamentals, and password hashing best practices.

Hands-On: Students encrypt/decrypt messages using Caesar ciphers, then progress to understanding modern public key infrastructure.

Module 5: Social Engineering Defense

The Human Element

Social engineering exploits psychology rather than technical vulnerabilities. Teaching students to recognize manipulation tactics is crucial—93% of breaches involve human error.

- **Phishing Variants**

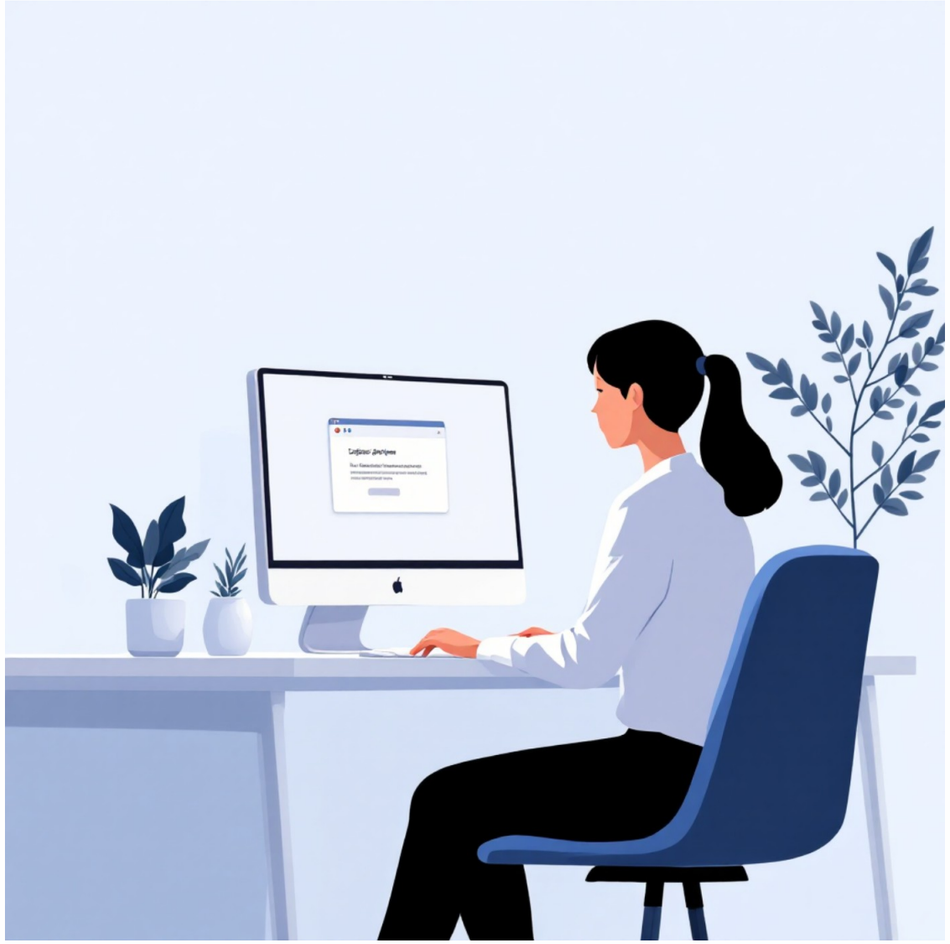
  Email phishing, spear phishing, whaling, vishing (voice), and smishing (SMS)

- **Manipulation Tactics**

  Urgency, authority, scarcity, familiarity, and trust exploitation

- **Prevention Strategies**

  Verification protocols, security awareness training, and building a culture of questioning



> "The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room." — *Gene Spafford, Security Expert*

Module 6: Incident Response Framework

1

Preparation

Establishing response teams, creating playbooks, and implementing monitoring systems before incidents occur.

2

Detection & Analysis

Identifying anomalies, determining scope, classifying severity, and documenting initial findings.

3

Containment

Isolating affected systems, preventing spread, and preserving evidence for investigation.

4

Eradication & Recovery

Removing threats, restoring systems from clean backups, and validating normal operations.

5

Post-Incident

Lessons learned, updating defenses, and improving response procedures for future incidents.

Simulation Activity: Students role-play an incident response scenario, practicing communication, documentation, and decision-making under pressure.

Hands-On Laboratory Exercises

Lab 1: Phishing Analysis

Students examine real phishing emails, identifying red flags such as suspicious URLs, spoofed sender addresses, urgent language, and requests for sensitive information. They document findings using an analysis template.

Lab 2: Password Security

Using password cracking tools in a controlled environment, students discover why password complexity matters. They test rainbow tables, brute force attacks, and learn about password managers and multi-factor authentication.

Lab 3: Network Monitoring

Students set up basic network monitoring using open-source tools, configure alerts for suspicious activity, and analyze logs to identify potential security events. This hands-on experience builds practical defensive skills.

Capstone Project Options

1

Security Audit

Students conduct a comprehensive security assessment of a fictional small business, identifying vulnerabilities and proposing remediation strategies with cost-benefit analysis.

2

Awareness Campaign

Design and implement a cybersecurity awareness program for younger students or community members, including educational materials, presentations, and interactive demonstrations.

3

Incident Response Plan

Create a complete incident response plan for a school or organization, including procedures, communication protocols, roles and responsibilities, and testing recommendations.

4

Security Tool Development

Build a simple security tool such as a password strength checker, basic firewall rule generator, or automated vulnerability scanner using Python or another programming language.

Assessment: Rubrics evaluate technical accuracy, presentation quality, practical applicability, and demonstration of learned concepts.

Career Pathways & Certifications

Industry Certifications

Entry Level

CompTIA Security+, Cisco CyberOps Associate, CEH (Certified Ethical Hacker)

Advanced Paths

CISSP, OSCP, CISM—building toward specialized security roles

Educational Resources

- CyberPatriot high school competition
- picoCTF and other capture-the-flag events
- SANS Cyber Aces tutorials
- TryHackMe and HackTheBox platforms

Career Statistics

$103K

Median Salary

Entry-level security analyst position

35%

Job Growth

Projected through 2031 (much faster than average)

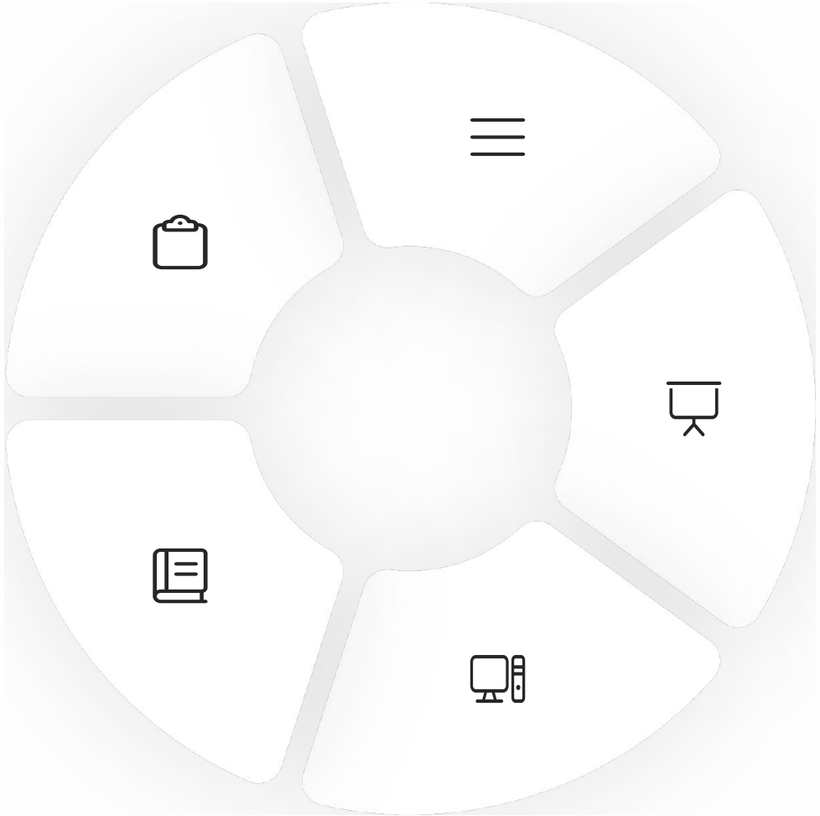
Teacher Resources & Assessment

Lesson Plans

Detailed daily plans with learning objectives, activities, time allocations, and differentiation strategies for diverse learners.

Reading Materials

Curated articles, case studies, and supplementary resources to extend learning beyond the classroom.



Assessment Rubrics

Project rubrics, lab completion checklists, quiz banks, and performance-based assessments aligned with learning outcomes.

Presentation Slides

Ready-to-use slide decks for each module with embedded videos, diagrams, and discussion prompts.

Lab Guides

Step-by-step instructions for hands-on exercises, including required software, setup procedures, and troubleshooting tips.

About Cybersecurity Non-Profit

> *Making cybersecurity knowledge accessible to everyone through education, community, and practical resources.*

Our Programs

- Business & Non-Profit Security
- Family Cybersecurity
- Kids Safety
- Senior Digital Safety
- Women's Security
- Parents & Educators

Free Resources

Everything we offer is completely free because we believe cybersecurity education should be accessible to everyone, regardless of background or budget.

Website: csnp.org
Resources: csnp.org/resources

FREE FOR EVERYONE COMMUNITY DRIVEN