Intro to Cybersecurity

Middle Township Public Schools

216 S. Main Street

Cape May Court House, NJ 08210

Born: April 2025

Introduction

This document serves to meet all requirements for curriculum as per the Middle Township Board of Education and the New Jersey Department of Education and will serve as a guide for lesson planning. Cybersecurity is a crucial skill in today's digital world. With increasing cyber threats, there is a growing need for professionals who can protect data, networks, and systems from unauthorized access. This course introduces students to the fundamentals of cybersecurity, providing them with the knowledge and skills needed to protect digital assets and pursue careers in this field.

Course Descriptions

Garden State Cyber - Introduction to Cybersecurity I

This course is designed to introduce high school students to cybersecurity concepts and inspire interest in cybersecurity careers. The course is delivered completely on Chromebooks with no specialized equipment. It includes access to a cyber range for online labs at zero cost to districts. The course incorporates the New Jersey Student Learning Standards – Computer Science and Design Thinking.

Students will explore cybersecurity fundamentals including the CIA Triad, authentication methods, malware threats, terminal commands, and system hardening. The course also covers human factors in security, including social engineering and phishing. Students will learn about data safety practices, cryptography basics, and networking fundamentals. Each unit integrates current events with cyber ethics and law. An ethics agreement must be signed by all students and parents during the first 2 weeks of class.

Scope and Sequence-

Unit 0: First Day Info & Ethics Agreement (1 day)

- Careers – introduction to reasons for pursuing cybersecurity career and motivations such as job demand, protect society, income, etc.
- Review what will be covered in class – objectives handout to determine what students find most and least interesting
- Ethics agreement – group work to create a Code of Behavior. Present and discuss why we need one. Review real Ethics Agreement for understanding of expectations and consequences.

Unit 1: Foundations & Threats

1. CIA Triad and Authentication (7 days)
    - Cybersecurity goal is to protect CIA of data at rest, in transit and in-use.
    - Define Authentication as a key tool - explore methods including strong passwords, tokens, MFA and biometrics

- Identify attacks on passwords and use of salted hashes as defense.
- Activities: Testing passwords, Have You Been Pwned, CyberChef tool to hash & salt, Create safe password poster, Which Authentication project.

2. Identifying Security Threats (6 days)
    - Define types of malware and the complexity of threats
    - Examine impact on systems and on people.
    - Summarize the best practices for protecting against malicious software
    - Activities: Historic Malware Research/Presentation, Rapper or Malware online game
3. Intro to Command Line (6 days)
    - Define difference between GUI and CLI
    - Learn basic terminal commands in Linux
    - Introduce Virtualization and how to use the course VMs
    - Activities: Terminus game part 1, Try It follow along with PPT

Unit 2: Human Factor

1. Social Engineering (2 days)
    - Define steps hackers take in an attack
    - Define and explore social engineering as the human risk
    - Activities: 7 Steps of an Attack – sorting, CS Interactive: Social Engineering, Social Engineering Toolkit on Ubuntu
2. Phishing & OSINT (6 days)
    - Define phishing, characteristics and specialized types.
    - Define OpenSource Intelligence (OSINT) and explore the tools used in OSINT.
    - How to mitigate human risk – policies, awareness training, etc.

- Activities: Phishing test, OSINT on Tony Stark, Phishing Myself project, Clean Desk Policy Mistakes

Unit 3: Data Safety & Best Practices

1. Securing the System (7 days)
    - Define Vulnerability and Exploit – use Darknet Diaries podcast (abbreviated) for story on these topics.
    - Examine how the Common Vulnerability and Exposure database can be used as a research tool.
    - Review and apply the recommended Best Practices configurations for typical PCs.
    - Activities: Product Analysis with CVE, CIS-CAT Scan + Hardening, Bingo Securing the System, Hardening Backups, Users & Applications, CyberPatriot Demo system.
2. Threat Modeling & IOT (2 days)
    - Understand Threat Modeling to determine what risk you are willing to take and what effort you are willing to put in to secure against threats.
    - Examine vulnerabilities of home Internet of Things (IOT) – Smart devices such as voice assistants, baby monitors, home routers, etc.
    - Activities: Home IOT SPOONS Game, My IOT Threat Model worksheet

Unit 4: Cryptography & Linux

1. Bits, Binary & Encoding (7 days)
    - Define bits, bytes and binary number system as computer language
    - Define hexadecimal numbers, use in computing
    - Define encoding and differences from encryption
    - Introduce using Capture The Flag challenges for practice.
    - Activities: Online Binary game, Convert between Decimal, Binary and Hex numbers, Decoding with CTF challenges.
2. Basic Cryptography Concepts (6 days)
    - Define terminology for cryptography

- Define key methods of encryption and examine classic algorithms including Caesar, Transposition and Vigenere
- Define Steganography and tools to find hidden data – hex editor, steghide, Cyberchef, Exifdata, binwalk
- Activities: Breaking Ciphers, Vigenere Try It, Scavenger Hunt, Steganography CTF

3. Advanced Linux CLI (5 days)
    - Review basic terminal commands in Linux and Windows
    - Advanced terminal commands in Linux
    - Create simple bash scripts that demo cybersecurity impact on device
    - Activities: Terminus game part 2, Try It follow along with PPT, Searching with Grep, Shell scripting in Linux
4. Privacy vs Security (4 days)
    - Define difference between privacy and security
    - Review facts of case where FBI demanded access to encrypted iPhone
    - Watch excerpts from debate on the privacy vs security concepts
    - Student teams debate same topic: Government should have lawful access to any encrypted message or device
    - Activities: Class debate

Unit 5: Devices and Networks

1. Computer Components (2 days)
    - Device key components – Input, Memory, CPU, Output plus Motherboard. What can go wrong?
    - Activities: Virtual Desktop Build a PC.
2. Networking Fundamentals (6 days)
    - Networking devices and topologies – WAN, LAN, routers, switches.
    - Define network naming – Mac vs IP addresses (basic formatting of IP addressing and subnetting), IPv4 & IPv6

- Activities: ARP with Wireshark, Network Puzzles, CS Interactives: Pizza Party (review of Mac/IP addressing).

3. Protocols and Packets & Getting to the Internet (4 days)
    - Define packet switching as network method of communication.
    - Define protocols, TCP/IP Suite, ports, 3-way handshake
    - Analyze network packet traffic
    - Activities: Mobster Net, Wireshark Packet Analysis

Introduction to Cybersecurity II Course Outline

Unit 6: Law & Ethics

1. Impact of Law and Ethics on Cybercrime
    - Explore ethical issues associated with information security
    - Examine the laws and rules that apply to digital activities
    - Debate ethics scenarios in cybersecurity

Unit 7: Reconnaissance

1. Recon Introduction and Google Dorking
    - Define techniques for reconnaissance of digital targets
    - Apply Google Dorking methods for advanced searching
    - Conduct ethical information gathering
2. WHOIS and Nslookup
    - Identify how the Internet structure and Domain Name System can be used for reconnaissance
    - Perform domain lookups using WHOIS and Nslookup tools
    - Analyze results to understand target systems

3. Network Scanning
    - Configure network IP addressing and subnetting
    - Use network scanning tools to discover hosts and services
    - Analyze network scan results and identify potential vulnerabilities

Unit 8: Network & System Threats

1. Denial of Service (DoS)
    - Identify types of network-based attacks including DoS
    - Understand the impact of availability disruptions
    - Explore mitigation strategies for DoS attacks
2. Spoofing & Sniffing
    - Define the concepts of spoofing and sniffing attacks
    - Explore man-in-the-middle attack techniques
    - Implement countermeasures against these attacks
3. Wireless, Mobile & VPNs
    - Define the vulnerabilities of Wireless and Mobile technologies
    - Examine the use of Virtual Private Networks to protect public communications
    - Implement security measures for wireless networks
4. Pentesting & Exploits
    - Explore the use of cybersecurity tools for pentesting
    - Understand the ethical considerations of penetration testing
    - Perform basic vulnerability assessment

5. Cyber War
    - Define cyberwar and nation-state attacks
    - Examine case studies of cyberweapons
    - Discuss international considerations and implications

Unit 9: Online Threats

1. Interactive Web Vulnerabilities
    - Identify vulnerabilities in web applications
    - Understand SSL, input validation, and Javascript security issues
    - Explore cross-site scripting (XSS) and buffer overflow attacks
2. Basic Web Code Attacks
    - Analyze web application vulnerabilities
    - Understand client-side vs server-side security
    - Implement basic web security practices
3. SQL Database Attacks
    - Define databases, SQL and the steps of a SQL injection attack
    - Perform basic SQL injection exercises in a safe environment
    - Learn best practices for protection against database attacks

Unit 10: Defensive Tools and Techniques

1. Network Defense
    - Compare the characteristics of the Defense in Depth and Zero Trust theories
    - Describe defensive hardware/software devices including firewalls

    - Implement network security configurations
2. Monitors and Alarms
    - Understand intrusion detection systems
    - Configure monitoring tools to detect suspicious activity
    - Develop incident response procedures
3. Encryption for Online Security
    - Apply advanced cryptographic ciphers including asymmetric and digital signatures
    - Understand the role of encryption in protecting data in transit
    - Implement encryption solutions for secure communications

Course Activities and Labs

Throughout the courses, students will engage in various hands-on activities including:

- Capture The Flag (CTF) challenges
- Network packet analysis using Wireshark
- System hardening using CIS benchmarks
- Linux command-line exercises
- Encryption and decryption labs
- Web vulnerability assessment
- Social engineering simulations
- Threat modeling exercises

Students will also be introduced to cyber competitions including:

- PicoCTF

- CyberStart America
- CyberPatriot

Cybersecurity I Expectations

After successfully completing this course, the student will:

- Understand the CIA Triad and its importance in cybersecurity
- Identify common security threats and appropriate mitigation strategies
- Use basic terminal commands in Linux
- Configure security settings to protect systems and data
- Recognize social engineering attacks and phishing attempts
- Understand the basics of cryptography and encoding
- Analyze network traffic and identify suspicious patterns
- Apply ethical principles to cybersecurity decisions
- Evaluate the trade-offs between security and usability

Assessments

The teacher will provide a variety of assessments. Among them are:

Summative

- Hands-on labs with documentation
- Group projects simulating security scenarios
- Security configuration projects
- Vulnerability assessments

- Written reports on cybersecurity topics
- Presentations on threat analysis

Formative

- Hands on Labs with documentation
- Capture the Flag Challenges
- Quizzes on technical concepts

Alternative

- Portfolio development of security tools and configurations

Accommodations and Modifications

Differentiating Instruction for Students with Special Needs: Students with Disabilities, Students with 504 Plans, Students at Risk, English Language Learners, and Gifted & Talented Students

Differentiating in this course includes but is not limited to:

Differentiation for Support- Students with Disabilities

- Rephrase directions, questions, explanations
- One-on-one modeling and demonstration of techniques and skills
- Modify assignments as needed
- Preferential seating
- Assign a buddy as needed
- Allow errors in speaking and writing
- Accept participation at any level

- Provide hard copies of direction sheets and project rubrics
- Allow extended time to complete assignments
- Follow IEP accommodations/modifications
- Provide positive feedback and rewards as necessary
- Consult with academic teachers for interventions

Students with 504 Plans

- Rephrase directions, questions, explanations
- One-on-one modeling and demonstration of techniques and skills
- Modify assignments as needed
- Preferential seating
- Assign a buddy as needed
- Allow errors in speaking and writing
- Accept participation at any level
- Provide hard copies of direction sheets and project rubrics
- Allow extended time to complete assignments
- Follow IEP accommodations/modifications
- Provide positive feedback and rewards as necessary
- Consult with academic teachers for interventions

English Language Learners

- Rephrase directions, questions, explanations
- One-on-one modeling and demonstration of techniques and skills

- Modify assignments as needed
- Preferential seating
- Assign a buddy as needed
- Allow errors in speaking and writing
- Accept participation at any level
- Provide hard copies of direction sheets and project rubrics
- Allow extended time to complete assignments
- Follow IEP accommodations/modifications
- Provide positive feedback and rewards as necessary
- Consult with MLL teachers for interventions

Gifted and Talented

- Provide extension activities
- Allow students to act as peer tutors
- Allow for student choice in project completion
- Build on students' intrinsic interests
- Allow independent study
- Scale project objectives to more challenging outcomes
- Encourage participation in extracurricular cybersecurity competitions

Instructional/Supplemental Materials

Resources include but are not limited to:

- Online platforms: CyberStart America, PicoCTF, TryHackMe
- Software tools: Wireshark, Nmap, CyberChef, Metasploit (in controlled environment)
- Virtual machines with Linux distributions
- Command line tutorials and references
- NIST Cybersecurity Framework documentation
- OWASP Top 10 Web Application Security Risks
- Common Vulnerabilities and Exposures (CVE) database
- Cybersecurity ethics case studies
- Industry certification roadmaps (CompTIA Security+, Certified Ethical Hacker)

New Jersey Student Learning Standards Addressed

Unit 0: First Day Info and Ethics Agreement

- 8.1.12.IC.1: Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.
- 9.4.12.DC.3: Evaluate the social and economic implications of privacy in the context of safety, law or ethics
- 9.3.IT.4: Demonstrate positive cyber citizenry by applying industry accepted ethical practices and behaviors

Unit 1: Foundations and Threats

- 8.1.12.NI.2: Evaluate security measures to address various common security threats.
- 8.1.12.NI.4: Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
- 8.1.12.IC.1: Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.
- 8.1.12.IC.3: Predict the potential impacts and implications of emerging technologies on larger social, economic, and political structures, using evidence from credible sources.
- 9.4.12.IML.7: Develop an argument to support a claim regarding a current workplace or societal/ethical issue such as climate change.
- 8.1.12.NI.3: Explain how the needs of users and the sensitivity of data determine the level of security implemented.
- 8.1.8.NI.3: Explain how network security depends on a combination of hardware, software, and practices that control access to data and systems.
- 8.1.8.NI.4: Explain how new security measures have been created in response to key malware events.
- 8.1.12.CS.1: Describe ways in which integrated systems hide underlying implementation details to simplify user experiences.
- 8.1.12.CS.2: Model interactions between application software, system software, and hardware.

Unit 2: Human Factor

- 8.1.12.NI.3: Explain how the needs of users and the sensitivity of data determine the level of security implemented
- 8.1.12.IC.1: Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.
- 8.1.12.NI.2: Evaluate security measures to address various common security threats

- 9.4.12.DC.6: Select information to post online that positively impacts personal image and future college and career opportunities

Unit 3: Data Safety & Best Practices

- 8.1.12.NI.2: Evaluate security measures to address various common security threats
- 8.1.12.NI.3: Explain how the needs of users and the sensitivity of data determine the level of security implemented.
- 8.1.12.NI.4: Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use
- 8.1.8.CS.1: Recommend improvements to computing devices in order to improve the ways users interact with the devices
- 8.1.8.NI.3: Explain how network security depends on a combination of hardware, software, and practices that control access to data and systems.

Unit 4: Cryptography and Linux

- 8.1.8.DA.2: Explain the difference between how the computer stores data as bits and how the data is displayed
- 8.1.12.DA.3: Translate between decimal numbers and binary numbers
- 8.1.12.DA.4: Explain the relationship between binary numbers and the storage and use of data in a computing device
- 8.1.8.DA.1: Organize and transform data collected using computational tools to make it usable for a specific purpose.
- 8.1.12.NI.2: Evaluate security measures to address various common security threats
- 8.1.12.CS.1: Describe ways in which integrated systems hide underlying implementation details to simplify user experiences.
- 8.1.12.CS.2: Model interactions between application software, system software, and hardware.
- 9.4.12.TL.1: Assess digital tools based on features such as accessibility options, capacities, and utility for accomplishing a specified task
- 8.1.12.NI.3: Explain how the needs of users and the sensitivity of data determine the level of security implemented.
- 9.4.12.DC.3: Evaluate the social and economic implications of privacy in the context of safety, law, or ethics
- 9.4.12.DC.5: Debate laws and regulations that impact the development and use of software

Unit 5: Devices & Networks

- 8.1.12.CS.2: Model interactions between application software, system software, and hardware

- 8.1.12.CS.3: Compare the functions of application software, system software, and hardware
- 8.1.12.NI.1: Evaluate the scalability and reliability of networks, by describing the relationships between routers, switches, servers, topology, and addressing.
- 8.1.12.NI.4: Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use
- 8.1.8.NI.1: Model how information is broken down into smaller pieces, transmitted as addressed packets through multiple devices over networks and the internet, and reassembled at the destination.
- 8.1.8.NI.2: Model the role of protocols in transmitting data across networks and the internet and how they enable secure and errorless communication.

Unit 6: Law & Ethics

- 8.1.12.NI.2: Evaluate security measures to address various common security threats.
- 8.1.12.NI.3: Explain how the needs of users and the sensitivity of data determine the level of security implemented.
- 8.1.12.IC.1: Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.

Unit 7: Reconnaissance

- 8.1.12.NI.2: Evaluate security measures to address various common security threats.
- 8.1.12.NI.3: Explain how the needs of users and the sensitivity of data determine the level of security implemented.
- 8.1.12.NI.4: Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
- 8.1.12.DA.2: Describe the trade-offs in how and where data is organized and stored.
- 8.1.12.IC.1: Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.
- 8.1.8.NI.1: Model how information is broken down into smaller pieces, transmitted as addressed packets through multiple devices over networks and the Internet, and reassembled at the destination.
- 8.1.8.NI.2: Model the role of protocols in transmitting data across networks and the Internet and how they enable secure and errorless communication.

- 8.1.12.NI.1: Evaluate the scalability and reliability of networks, by describing the relationship between routers, switches, servers, topology, and addressing.
- 8.1.12.DA.3: Translate between decimal numbers and binary numbers.

Unit 8: Net & System Threats

- 8.1.8.NI.1: Model how information is broken down into smaller pieces, transmitted as addressed packets through multiple devices over networks and the Internet, and reassembled at the destination.
- 8.1.8.NI.2: Model the role of protocols in transmitting data across networks and the Internet and how they enable secure and errorless communication.
- 8.1.12.NI.1: Evaluate the scalability and reliability of networks, by describing the relationship between routers, switches, servers, topology, and addressing.
- 8.1.8.NI.3: Explain how network security depends on a combination of hardware, software, and practices that control access to data and systems.
- 8.1.12.NI.2: Evaluate security measures to address various common security threats.
- 8.1.12.NI.3: Explain how the needs of users and the sensitivity of data determine the level of security implemented.
- 8.1.12.NI.4: Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
- 9.4.12.DC.3: Evaluate the social and economic implications of privacy in the context of safety, law, or ethics
- 9.4.12.DC.5: Debate laws and regulations that impact the development and use of software

Unit 9: Online Threats

- 8.1.12.CS.1: Describe ways in which integrated systems hide underlying implementation details to simplify user experiences.
- 8.1.12.DA.2: Describe the trade-offs in how and where data is organized and stored.
- 8.1.12.IC.1: Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.
- 8.1.12.NI.2: Evaluate security measures to address various common security threats
- 8.1.12.NI.4: Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.

Unit 10: Encryption Security Tools

- 8.1.8.DA.1: Organize and transform data collected using computational tools to make it usable for a specific purpose.
- 8.1.12.NI.2: Evaluate security measures to address various common security threats.
- 8.1.12.NI.4: Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.