Unit 1 Foundations & Threats

Content Area: **Computer Science**
Course(s):
Time Period: **Marking Period 1**
Length: **4 Weeks**
Status: **Published**

Brief Summary of Unit

Students will be exposed to a general overview of the field of cybersecurity and its multi-faceted nature. The relevance of the field will be discussed, as well as current threats to cybersecurity, and different career opportunities. Students will learn about the importance of the CIA Triad, authentication, best practices for passwords, password vulnerabilities, hashing, historically significant malware and how to protect against malware, how to use online virtual machines, and how to use the Linux command line on a basic level.

Revised Date: July 2025

Standards

MA.9-12.1.2.12prof.Cr	Creating
ELA.L.SS.11–12.1	Demonstrate command of the system and structure of the English language when writing or speaking.
ELA.L.KL.11–12.2	Apply knowledge of language to understand how language functions in different contexts, to make effective choices for meaning or style, and to comprehend more fully when reading or listening.
MA.9-12.1.2.12prof.Cr3	Refining and completing products.
CS.6-8.8.1.8.NI.3	Explain how network security depends on a combination of hardware, software, and practices that control access to data and systems.
CS.6-8.8.1.8.NI.4	Explain how new security measures have been created in response to key malware events.
CS.9-12.8.1.12.CS.1	Describe ways in which integrated systems hide underlying implementation details to simplify user experiences.
CS.9-12.8.1.12.CS.2	Model interactions between application software, system software, and hardware.
CS.9-12.8.1.12.IC.1	Evaluate the ways computing impacts personal, ethical, social, economic, and cultural practices.
CS.9-12.8.1.12.IC.3	Predict the potential impacts and implications of emerging technologies on larger social, economic, and political structures, using evidence from credible sources.
CS.9-12.8.1.12.NI.2	Evaluate security measures to address various common security threats.
CS.9-12.8.1.12.NI.3	Explain how the needs of users and the sensitivity of data determine the level of security implemented.
CS.9-12.8.1.12.NI.4	Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
WRK.K-12.P.8	Use technology to enhance productivity increase collaboration and communicate effectively.

TECH.9.4.12.DC.3	Evaluate the social and economic implications of privacy in the context of safety, law, or ethics (e.g., 6.3.12.HistoryCA.1).
TECH.9.4.12.TL.1	Assess digital tools based on features such as accessibility options, capacities, and utility for accomplishing a specified task (e.g., W.11-12.6.).
TECH.9.4.12.IML.7	Develop an argument to support a claim regarding a current workplace or societal/ethical issue such as climate change (e.g., NJSLSA.W1, 7.1.AL.PRSNT.4).

Essential Questions

- How are passwords stored on a system?
- How can databases be used in password guessing attacks?
- How do authentication and strong passwords help secure data?
- How does malicious software impact computer systems?
- How does the protection of the CIA triad lead to the security of data?
- How does understanding how to use a command line interface (CLI) allow you to continue the use of your device in the event of an issue affecting normal operations?
- What are various methods of authentication?
- What branches of computer science does cybersecurity affect?
- What careers are available to students and what are the benefits of these careers?
- What is meant by the term cybersecurity?
- What is password hashing?
- What is the Linux Command Line Interface?
- Why is a code of behavior important for this course?

Enduring Understandings

- Authentication can be implemented with something you have, something you know, or something that is biometric (something you are).
- By making sure that data is confidential, its integrity is maintained, and that it is available as appropriate, we can achieve a stronger level of security.
- Cybersecurity has many definitions, but we can think of it was the act of protecting our data and devices to mitigate any cyber threats that may occur.
- Cybersecurity is a multi-faceted field.
- Cybersecurity necessarily overlaps with other branches of computer science.
- Hackers have lists, or databases of known passwords, and they can use software to try these passwords very quickly.
- Malicious software can corrupt your data, allow malicious actors to steal data, and/or disrupt devices.
- Many careers are available under the umbrella of cybersecurity that can accommodate a wide range of applicants' interests and strengths.
- Passwords should be stored securely on a device or in the cloud using hashing.
- Strong passwords are much harder for people to guess or break through, and strong authentication procedures help to prevent people from impersonating others to gain access to their online accounts.

- The Linux CLI is a text-based way to interact with a Linux system, useful for a variety of purposes.
- The Linux CLI, like all CLIs, allow you to use commands to run your computer if the graphical interface is innaccessible due to some kind of damage.
- There are many possible career paths and agencies that require an employee skilled in cybersecurity. The number of unfilled jobs in cybersecurity is large, and growing larger.
- Threats to cybersecurity are constantly evolving, but there are ways to improve your own cybersecurity.
- We must be ethical in our use of cybersecurity tools and knowledge as we go about protecting ourselves from cyber threats.

Students Will Know

- Basic Linux CLI commands and when to use them.
- Best practices for authentication.
- Best practices for mitigating risk from malware.
- Best practices for strong passwords.
- Career choices in cybersecurity.
- Current threats to cybersecurity and a general knowledge of how they work.
- General descriptions of different computer science sub-fields.
- Historically significant examples of malware.
- The sub-fields of computer science that cybersecurity affects.
- The term “CIA” as it relates to a secure network (Confidentiality, Integrity, Availability).

Students Will Be Skilled At

- Communicating an overview of computer science and its subdomains in written and verbal form.
- Communicating the relationship between cybersecurity and some of the subdomains of computer science.
- Communicating the various job responsibilities that someone with a cybersecurity background may need to carry out.
- Identifying manifestations of current cybersecurity threats in the news.
- Identifying scenarios where one or more aspects of the CIA Triad are violated.
- Identifying the key goals and frameworks of cybersecurity.
- Identifying the state of information as stored, transmission, and processing.
- Identifying their own weak passwords and strengthening them.
- Implementing multifactor authentication for their various accounts.
- Updating devices to mitigate risk from malware.
- Using Linux commands to navigate through a Linux system using the command line.

Evidence/Performance Tasks

Assessments

- Formative: Teacher observations, student-centered discussions, classwork, student-centered labs.
- Summative: Quizzes, tests, projects.
- Alternative: Verbal discussions and debriefs.

Learning Plan

This curriculum follows cyber.org's "Cybersecurity 1" course as listed in the "One Semester Plan." Go to https://cyber.instructure.com/login/canvas and apply for a teacher account. Under "High School 9-12," you will find the Cybersecurity 1 course with detailed lesson plans and pacing. They assume roughly 45 minute classes. Below is a modified pacing guide to align more smoothly with our rotating drop schedule.

There are 5 assessment days that can be used throughout the course with the timing below if none of the "if time allows" lessons are taught. These days can be used for quizzes/tests as the teacher sees fit.

- 0.1.1 - First Day Info & Ethics Agreement **(1 Class)**
- Section 1.1 - CIA Triad and Authentication
    - 1.1.1 - Intro to Security Concepts **(1 Class)**
    - 1.1.2 - Authentication **(1 Class)**
    - 1.1.3 Authentication and Password Attacks **(0.5 Classes)**
    - 1.1.4 Password Hashing **(1 Class)**
    - 1.1.5 Methods of Authentication **(2 Classes)**
- Section 1.2 - Identifying Security Threats
    - 1.2.1 - Malicious Code Part 1 **(4.5 Classes)**
    - 1.2.2 - Malicious Code Part 2 **(1 Class)**
- Section 1.3 - Intro to CLI (Command Line Interface)
    - 1.3.1 - Virtualization **(1 Class)**
    - 1.3.2 - Command Line Interface - Linux **(4 Classes)**

Materials

- Core instructional materials: Core Book List
- Supplemental materials: Resources from the cyber.org curriculum "Cybersecurity 1."

- Computers

- Teacher created activiites
- Teacher created notes
- Websites to research current events

Integrated Accommodation & Modifications

Possible accommodations/modification for Introduction to Cybersecurity