Unit 3 Data Safety & Best Practices

Content Area: **Computer Science**
Course(s):
Time Period: **Marking Period 1**
Length: **1-2 weeks**
Status: **Published**

Brief Summary of Unit

Students start this unit with learning how those in the Cybersecurity field classify known vulnerabilities to software and hardware, as well as the effect that vulnerabilities that have not been discovered that are "in the wild" can have on our systems. Students then learn how existing vulnerability scanners can be used to help people detect these vulnerabilities and "harden" their systems. The unit concludes with an examination of "Threat Modeling," which individuals and organizations can use to gauge the benefit to be realized by expending money and effort to improve their security. This allows them to make an informed decision about the level of risk they're willing to tolerate.

Revised Date: July 2025

Standards

8.1.8.CS.1	Recommend improvements to computing devices in order to improve the ways users interact with the devices.
P.6	Model integrity, ethical leadership and effective management.
P.8	Use technology to enhance productivity increase collaboration and communicate effectively.
9.4.12.CT.2	Explain the potential benefits of collaborating to enhance critical thinking and problem solving (e.g., 1.3E.12profCR3.a).
L.VL.11–12.3	Determine or clarify the meaning of unknown and multiple-meaning words and phrases based on grades 11–12 reading and content, including technical meanings, choosing flexibly from a range of strategies.
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.
8.1.8.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.4	Explain how decisions on methods to protect data are influenced by whether the data is at rest, in transit, or in use.
L.VI.11–12.4	Demonstrate understanding of figurative language, word relationships, and nuances in word meanings, including connotative meanings.

Essential Questions

- How can we use defensive tools to harden and restrict access to better secure a system?
- How does the least privilege principle play an important part in cybersecurity?
- What are system vulnerabilities and how can systems be hardened?
- What is the process of threat modeling and how does it apply to IOT devices?

Enduring Understandings

- Defensive tools can help us discover vulnerabilities before they pose a threat so that we can work to better secure our systems before an attack.
- The least privilege principle says that people should only have the minimum level of access needed to complete their work in an organization. This helps to minimize what "disgruntled insiders" and hackers can access inside of a system.
- Threat modeling involves examining vulnerabilities and measuring what the "cost" would be to mitigate risk from that vulnerability so that one can make an informed decision about the level of risk they're willing to tolerate in order to use a certain device/program.
- Vulnerabilities are weaknesses in systems that can be exploited either in practice or theoretically by malicious actors. Systems can be hardened by reviewing the "Common Vulnerabilities and Exposures" database and implementing recommended patches/fixes, and/or by using third-party software that scans for these vulnerabilties.

Students Will Know

- How to use a vulnerability scanner to help secure a system.
- The general information available in the CVE database.
- The importance of threat modeling in their personal lives and in the operation of an organization.

Students Will Be Skilled At

- Navigating the CVE database to look up information about the programs and devices they use.
- Practicing threat modeling for devices students use in their lives.
- Using a vulnerability scanner to secure a system.

Assessment

Assessments

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

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.

- Section 3.1 - Securing the System
    - 3.1.1 - System Vulnerabilities **(1 Class)**
    - 3.1.2 - System Hardening Part 1 **(2 Classes)**
    - 3.1.3 - System Hardening Part 2 **(1 Class)**
- Section 3.2 - IoT Threat Modeling
    - 3.2.1 - Threat Modeling & IoT **(1 Class)**

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

Suggested Strategies for Integrated Accommodation & Modifications

Possible accommodations/modification for Introduction to Cybersecurity