Grade Level	Middle School
Duration	4 days
CS Standards Addressed	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

Introduction

This three-lesson unit introduces middle school students to the fundamental concepts of cybersecurity and digital safety. Through discussions, hands-on activities, simulations, and real-world case studies, students explore how information and systems are protected from cyber threats. Each lesson builds on the previous one, helping students understand the goals of cybersecurity, how passwords and authentication systems protect accounts, and how malicious software and cyberattacks can impact individuals and organizations.

Students begin by exploring the core principles of cybersecurity through the CIA Triad: confidentiality, integrity, and availability. They then investigate how passwords are stored and protected using hashing and salting, while examining how weak passwords can be cracked and strengthened through better security practices. In the final lesson, students learn about common types of malware and research major cybersecurity incidents to better understand how cyberattacks spread, cause damage, and influence modern security practices.

By the end of the unit, students will have a foundational understanding of cybersecurity concepts, common cyber threats, and the strategies individuals and organizations use to protect digital information and systems.

This lesson package includes:

- Lesson Plan & Overview
- PPT Slides for Classroom Instruction
- Understanding the CIA Triad – Student Worksheet
- Understanding the CIA Triad – Answer Key
- Infamous Cybersecurity Events – Student Worksheet

Lesson Agenda

Class 1 – What is Cybersecurity

Objective: Students will explore the goals of cybersecurity and learn how confidentiality, integrity, and availability help protect information and systems in the digital world.

Time	Activity	Notes
5 mins	Warm-up: Class Discussion	Display the slide with the warm-up question: "what is cybersecurity" and engage the class in a discussion before sharing the definition. *Optional:* after providing the definition, engage the class around the scenario "a company is hacked and customer data is leaked", along with three discussion questions, if time permits (slide 4)
10 mins	Class Instruction & Discussion	Teach the 3 goals of cybersecurity (CIA): Confidentiality, Integrity, & Availability using the provided slides. Explain that data exists in different states.
10 mins	Activity: Understanding the CIA	Provide students with the "Understanding the CIA Triad" worksheet and allow ~5 minutes for it to be completed. Then, recap and provide answers through a whole-class discussion.
5 mins	Class Instruction & Discussion	Continue teaching about CIA, moving through slides about achieving CIA, focusing on authentication, and password attacks/
5 mins	Activity: Think you can make a strong password?	Ask students to get into pairs, and with their buddy visit cyber.org/find-curricula/test-strength-your-passwords to test their password strength.
10 mins	Class Instruction & Discussion	Staying in pairs, play the video How to Make a Strong Password by CISA on YouTube. Or, if you prefer a non-cartoon video, see the link provided in the notes section underneath the video's slide. Wrap-up the class with discussion questions on slide 16.

Class 2 - Authentication & Password Attacks

Objective: Students will investigate how passwords are protected using hashing and salting, and explore how weak passwords can be cracked and better secured using strong authentication practices.

Time	Activity	Notes
5 mins	Warm-up: Activity	Ask the class to check what data breaches they may have been involved in by visiting haveibeenpwned.com. If they have been in any, make sure they know this is not the end of the world and that they can now make the decision to lock down their account by changing their password. Knowledge is power!
15 mins	Class Instruction & Discussion	Teach the class about how passwords are stored, password "hashing", rainbow tables, & password "salting" using the provided slides.
20 mins	Activity: Hashing & Cracking Passwords	Ask students to get into pairs for this activity. Students will be turning a password into a hash, and the will try to "crack" it. 1. Have pairs visit gchq.github.io/CyberChef/ to access the hashing activity. Only use MD5 for this activity, and explain briefly to them that it is just one of many algorithms that hash passwords. 2. Ask them to first hash an "easy" password (like password123). 3. Have them share this hash with their partner. Make it clear that they should NOT be sharing the password, just the hash. 4. Ask each student to visit crackstation.net and put in their partner's hash. As this was an "easy" password, it will likely be on a rainbow table and the website will give them their partner's original, easy password. 5. Have them try this again, but after salting their "easy" password first. 6. Close out the activity by engaging the class in a discussion using prompts provided below under "Class 2 Educator Guidance".
10 mins	Video, Class Discussion, & wrap-up: How to Turn on MFA!	As a class, watch the CISA video to learn more about using Multi-Factor Authentication. Or, if you prefer a non-cartoon video, see the link provided in the notes section underneath the video slide. Discussion questions: • What's been your experience with biometric (your body) authentication? • How many of the methods from the video have you used? • What's your favorite way to use MFA? (FaceID, TouchID, text message code, authenticator app, email code, etc.) • Which do you think is the most convenient way to use MFA?

Class 2 Educator Guidance

Activity Overview

In this activity, students explore how passwords are protected using hashing and how attackers may attempt to reverse hashed passwords using tools similar to rainbow tables. Students will first create and exchange hashed passwords, then attempt to "crack" them. The activity is then repeated after having "salted" the same password to demonstrate how salting increases password security.

This document includes necessary preparation and items to keep in mind for educators when teaching this lesson.

Your students will need

- A device that can reliably access the internet
- Access to CyberChef (https://gchq.github.io/CyberChef) & Crackstation.net
    - Make sure your school's internet doesn't block these sites!

Activity Instructions

Creating Hashed Passwords:

1. Instruct students to go to CyberChef (gchq.github.io/CyberChef)
2. Have students come up with a simple, fake password (e.g., "dog123").
    a. Emphasize that students should not use real passwords.
3. Students will input this password into CyberChef, and apply a hash function (MD5).
4. Students copy the resulting hashed output.

Exchanging and Cracking Hashes:

1. Students exchange their newly hashed passwords with a partner (not their original password).
2. Using crackstation.net , students will paste their partners hashed password in and attempt to determine their partner's original password.

Adding a Salt:

1. Reiterate that a salt is additional random data added to a password before hashing.
2. Ask students to modify their original, easily guessed password (not hashed) by adding a short string of numbers (e.g., "dog123839265").
3. Students repeat the hashing process in CyberChef using the new salted password.
4. Students exchange hashes again and attempt to crack them using the same tool.

Discussion & Debrief

Facilitate a class discussion using prompts such as:

- Why were some passwords easy to crack in the first round?
- What changed when a salt was added?
- How does this relate to real-world password security?
- Why might companies store hashed passwords instead of actual passwords?

Guide students toward the following key understandings:

- Passwords are stored as hashes, not plain text
- Weak passwords can still be cracked using large databases (rainbow tables)
- Adding randomness (salt) makes passwords significantly more secure

Miscellaneous Tips for Educators

- Encourage students to use simple passwords initially so the cracking process is successful and visible.
- If students are unable to crack a password, use this as a discussion point about password strength.
- Keep explanations of "rainbow tables" high-level; focus on the concept rather than technical detail.
- Reinforce connections to earlier content (e.g. CIA Triad):
    - Confidentiality is protected through secure authentication practices like strong passwords

Class 3 – Hacking & Malicious Code

Objective: Students will learn about common types of malware and investigate real-world cybersecurity incidents to understand how cyberattacks spread, cause harm, and impact people and organizations.

Time	Activity	Notes
5 mins	Warm-up: Class Discussion	Display the slide with the warm-up question: "A hospital's computers suddenly stop working. A message appears on all the screens: Pay $100,000 or your data is gone forever. *What do you think just happened?".* Engage the class in a discussion before moving on to the instructional slides.
15 mins	Class Instruction & Discussion	Teach the class about hacking and malware using the provided slides: 1. Explain what it means to "hack" something. 2. Explain what Malware is, and introduce the common types. 3. Explain the common types in slightly more detail, including what each does, how they spread, why they are dangerous, and how to best protect yourself using the provided slides.
15 mins	Activity: Researching Infamous Cybersecurity Events	1. Assign each student one major cybersecurity incident from the past to research. Reference the below educator guidance for a bank of history cybersecurity events below. 2. Provide them with the accompanying worksheet titled "Infamous Cybersecurity Events" to complete as they research.
10 mins	Wrap-up: share research	Engage the classroom in a discussion surrounding their findings. Ask for students to share their research. • Was anything surprising? Interesting? • What did they learn from this activity? • What changes can they implement to protect themselves from these kinds of attacks?

Class 3 Educator Guidance

Below is a bank of historic cybersecurity incidents to assign to students for the classroom research activity within Class 3: Malicious Code.

- **The Melissa Virus (1999, virus)**
  - One of the first major email viruses, Melissa spread through infected Word documents sent via email. It overwhelmed email systems, forcing companies like Microsoft to shut down their servers.
- **The NASA Cyber Attack (1999, hacking)**
  - A teenage hacker gained access to NASA computers and shut down systems, including those controlling parts of space operations. The attack caused major disruptions and showed how vulnerable government systems could be.
- **The Sony PlayStation Network Outage (2011, hacking)**
  - Hackers broke into Sony's PlayStation Network, exposing personal data from about 77 million users. Sony shut down the network for weeks, affecting millions of gamers worldwide.
- **Yahoo Data Breach (2013, hacking)**
  - One of the largest data breaches ever, hackers stole information from billions of Yahoo accounts, including emails and passwords. The breach wasn't fully revealed until years later.
- **WannaCry Ransomware Attack (2017, ransomware + worm)**
  - A global ransomware attack that spread like a worm, locking files on computers and demanding payment. It affected hospitals, businesses, and governments, especially in the UK.
- **The Equifax Data Breach (2017, hacking)**
  - Hackers exploited a security flaw to steal sensitive personal information (like Social Security numbers) from about 147 million people. It raised major concerns about data protection.
- **The Log4j Vulnerability (2021, exploited security weakness)**
  - A serious flaw in widely used software (Log4j) allowed hackers to remotely take control of systems. Because so many companies used it, millions of systems were at risk worldwide.
- **The MOVEit Cyberattack (2023, exploited security weakness)**
  - Hackers exploited a vulnerability in MOVEit file transfer software to steal data from hundreds of organizations. It impacted governments, schools, and businesses globally.
- **Morris Worm (1988, worm)**
  - One of the first internet worms, it spread rapidly across early internet systems and caused major slowdowns. It helped lead to the creation of modern cybersecurity practices.
- **"Mafiaboy" hack (2000, DDoS attack)**
  - A 15-year-old hacker launched attacks that shut down major websites like Yahoo, Amazon, and CNN. It was one of the first major examples of large-scale website shutdown attacks (DDoS).
- **ILOVEYOU Virus (2000, virus)**
  - A fast-spreading email virus that arrived as a "love letter" message. When opened, it infected the computer and sent itself to everyone in the user's contact list, causing widespread damage around the world.
- **Colonial Pipeline Attack (2021, ransomware)**
  - A ransomware attack that forced a major U.S. fuel pipeline to shut down, leading to gas shortages. The company paid millions of dollars to regain control of its systems.
- **Stuxnet (2010, worm)**
  - A highly sophisticated worm designed to target industrial machines. It damaged equipment used in Iran's nuclear program and is considered one of the first major cyberweapons.