

Guarding the Digital World

Textbook

Guarding the Digital World



What Is Cybersecurity and Why Does It Matter?

Cybersecurity is how we **protect computers, devices, and information** from people who try to steal, damage, or break in.

Why is this important?






- It keeps your **photos, files, and passwords** safe.
- It protects schools, companies, and governments from being hacked.
- It keeps important services running—like hospitals, banks, and electricity.

Cybersecurity isn't just for experts—it starts with all of us. Just like you **lock your front door**, you also need to **lock down your digital life**.

Keeping Personal Devices Safe

Your phone, laptop, tablet, and even your smartwatch are at risk from viruses, hackers, and other digital threats.





Here are simple actions that help protect your devices:

-  **Update your software**—It patches security holes.
-  **Install antivirus software**—It catches harmful programs.
-  **Use strong passwords**—They make accounts harder to break into.
-  **Don't click strange links**—They might carry malware.
-  **Lock your screen** when not using your device.

Even small actions can stop big problems.

Cybersecurity for Businesses, Government, and Organizations

Cybersecurity is even more important for groups that manage **large amounts of data**.

-  **Schools** protect student records.
-  **Governments** secure national secrets and infrastructure.
-  **Banks** guard your money and financial info.
-  **Hospitals** protect medical records and systems that keep people healthy.

These organizations need **cyber teams** to prevent attacks and keep everything running smoothly.

If they're attacked, it could:

- Stop public services
- Leak private information
- Cost lots of money
- Put people in danger

What Is Access Control?

Access control is how systems **decide who is allowed in and what they can do**.




Think of it like your school:

- You need an **ID** to get inside (identification)
- You type in a code on a school laptop (authentication)
- You're allowed to view your own grades, but not the teacher's grades (authorization)
- The system tracks what you do while logged in (accountability)
- You can't deny it later because it's all logged (non-repudiation)

These five parts—**identification, authentication, authorization, accountability, and non-repudiation**—work together to make sure only the right people can access the right things.

Types of Authentication: Proving Who You Are

Authentication is the process of proving you are who you say you are. Here are different levels:




1. **Single-factor authentication:**  Just one method, like a password
2. **Two-factor authentication (2FA):**  Two methods—usually something you **know** (like a password) and something you **have** (like a phone)
3. **Multi-factor authentication (MFA):**  Uses two or more of the following:
 - Something you know (password)
 - Something you have (a code sent to your phone)
 - Something you are (like a fingerprint or face scan—called **biometric** authentication)

Each added step makes it **harder for intruders** to get in, even if they guess your password.






Defense in Depth: Multiple Layers of Protection

Defense in depth means using **more than one type of protection**—just like a castle uses walls, moats, and guards.

In the digital world, that means:

-  **Passwords, encryption, firewalls**
-  **Monitoring systems** that watch for unusual activity
-  **Human training** to recognize scams

In the physical world, it also means:

-  Door locks and keypads
-  ID cards
-  Cameras and lighting
-  Bollards and fencing
-  Security guards

By combining **digital and physical security**, we make it very hard for attackers to succeed—even if one layer fails, others still work.

Class Activity: Build Your Own Cyber Fortress

Instructions:

1. Split into small groups.
2. Each group creates a "cyber building" (e.g., school, hospital, company).
3. You must:

- Describe **what kind of data** the building needs to protect
- List at least **3 digital defenses** (e.g., password policy, firewalls, 2FA)
- List at least **2 physical defenses** (e.g., locks, cameras, guards)
- Explain how you'll handle **access control** (who gets in, how they prove it)

Bonus: Draw or diagram your building and its layered security system.

Critical Thinking Questions

1. Why do you think organizations need more layers of protection than individuals?
2. What are the risks if someone gains access to data without permission?
3. How could someone bypass physical security to get to digital information?

Questions (5)

1. What does cybersecurity help protect?

MULTIPLE CHOICE

Choose the correct answer:

- A. Only games on your computer
- B. Devices and digital information
- C. The way your keyboard works
- D. Your favorite playlist

2. What is an example of two-factor authentication?

MULTIPLE CHOICE

Choose the correct answer:

- A. Logging in with just your username
- B. Unlocking your phone with a password only
- C. Using a password and a code texted to your phone
- D. Typing your email address

3. Which is NOT a component of access control?

Choose the correct answer:

- A. Identification
- B. Encryption
- C. Authorization
- D. Non-repudiation

4. What is defense in depth?

Choose the correct answer:

- A. Keeping your computer off all the time
- B. Using more than one type of security layer
- C. Having only a strong password
- D. Backing up files to a USB drive

5. Which of these is a physical security control?

Choose the correct answer:

- A. A password manager
- B. A fingerprint login
- C. A firewall
- D. A security guard at the door

Answer Keys & Solutions

Questions

1. What does cybersecurity help protect?

MULTIPLE CHOICE

Correct Answer:

- A. Only games on your computer ✗ Incorrect
- B. Devices and digital information ✓ Correct
- C. The way your keyboard works ✗ Incorrect
- D. Your favorite playlist ✗ Incorrect

2. What is an example of two-factor authentication?

MULTIPLE CHOICE

Correct Answer:

- A. Logging in with just your username ✗ Incorrect
- B. Unlocking your phone with a password only ✗ Incorrect
- C. Using a password and a code texted to your phone ✓ Correct
- D. Typing your email address ✗ Incorrect

3. Which is NOT a component of access control?

MULTIPLE CHOICE

Correct Answer:

- A. Identification ✗ Incorrect
- B. Encryption ✓ Correct
- C. Authorization ✗ Incorrect
- D. Non-repudiation ✗ Incorrect

MULTIPLE CHOICE

4. What is defense in depth?

Correct Answer:

- A. Keeping your computer off all the time ✗ Incorrect
- B. Using more than one type of security layer ✓ Correct
- C. Having only a strong password ✗ Incorrect
- D. Backing up files to a USB drive ✗ Incorrect

5. Which of these is a physical security control?

MULTIPLE CHOICE

Correct Answer:

- A. A password manager ✗ Incorrect
- B. A fingerprint login ✗ Incorrect
- C. A firewall ✗ Incorrect
- D. A security guard at the door ✓ Correct