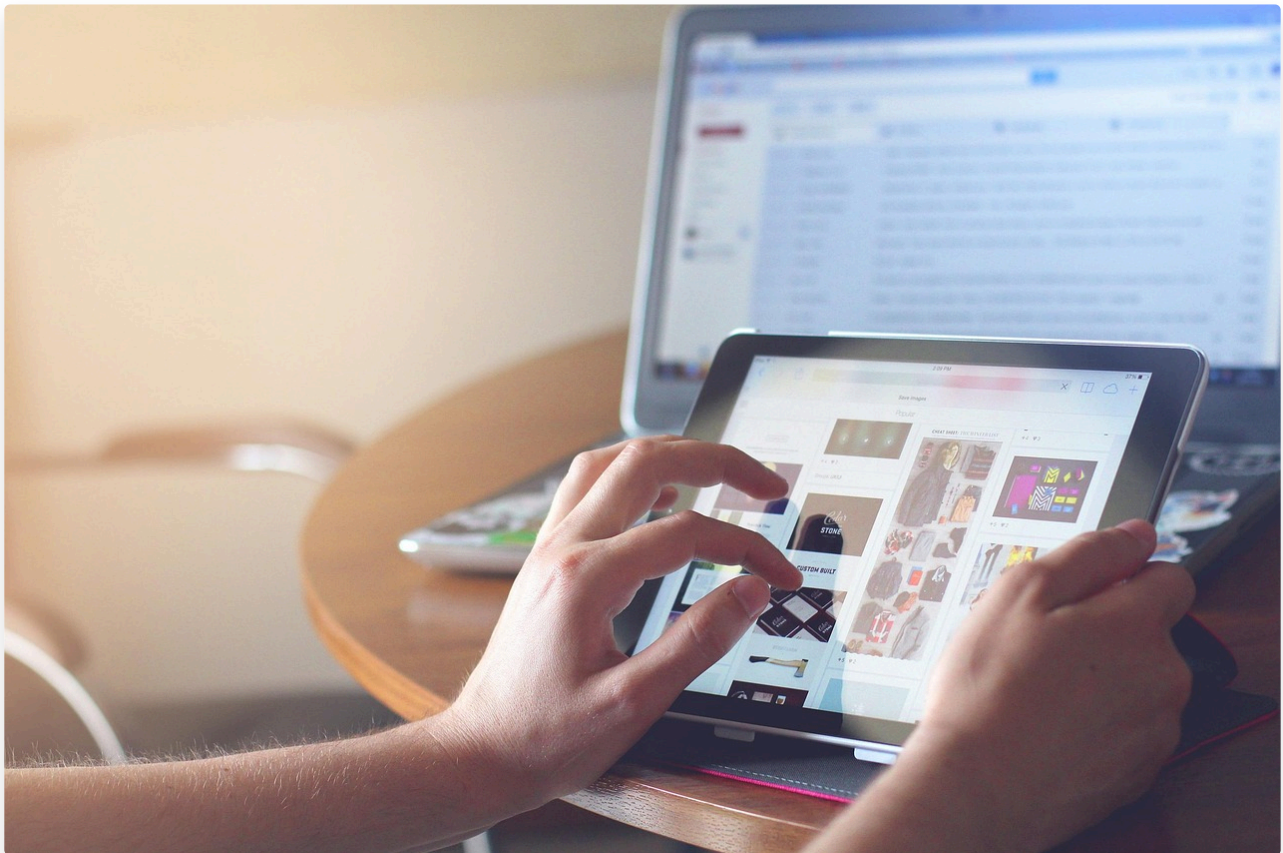


Protecting Your Digital Self

Textbook

Protecting Your Digital Self



What Are Data Vulnerabilities?

A *data vulnerability* is any weakness that could let someone access, steal, or damage private information. These risks often happen when systems don't have strong protection. For example, if a person uses the same simple password on every website, a hacker could easily guess it and break into multiple accounts. Vulnerabilities also include things like outdated software, weak access controls, or unencrypted data.

The Power of Strong Passwords

A password is like a key to your digital life—so it needs to be strong. Good passwords:

- Use a mix of **uppercase and lowercase letters, numbers, and symbols**
- Avoid easy-to-guess information like your name or birthdate
- Are long—ideally **12 characters or more**

Using **two-factor authentication (2FA)** adds another layer of safety. For example, after typing in a password, a user might also need to enter a code sent to their phone. This helps stop attackers, even if they guess your password.

Advanced Password Protection: Biometrics and Encryption

Some systems use **biometric access**, such as fingerprints or face scans. These are hard to fake and make logging in more secure. Others use **encryption** to scramble data into unreadable code unless someone has the correct key. Common encryption types include:

- **Caesar cipher** – A simple letter-shift code
- **Vigenère cipher** – A more complex, repeating-key cipher
- **MD5 hashing** – A one-way cryptographic function used to store passwords securely

Encryption protects data from being read by outsiders—even if they get their hands on it.

Keep It Confidential

Not all information should be shared. Things like your passwords, social security number, medical records, and bank details are examples of **confidential information**. If shared in the wrong way, it could lead to identity theft, scams, or serious privacy problems.

How Passwords Help Keep You Safe Online

Using strong passwords is one of the simplest and most important steps in staying safe online. A strong password is often your first and best defense against hackers and cybercriminals. Whether you're protecting your email, social media, or online homework account, good password habits make a big difference.

Recognizing and Reporting Suspicious Online Behavior

The internet is an amazing place to learn, play, and connect—but it's also important to stay safe. Just like in real life, not everyone online has good intentions. Sometimes, people might try to trick you into giving away personal information, downloading harmful files, or clicking on unsafe links. These behaviors can be signs of **suspicious activity**, and recognizing them is the first step to staying protected.

If something feels "off"—like a message from a stranger asking for private details, a pop-up that looks too good to be true, or a friend acting oddly online—it's important not to ignore it. Reporting suspicious behavior to a trusted adult, teacher, or school technology specialist helps keep **you and others safe**. Schools, websites, and security teams can only stop harmful activity if they know it's happening.

Remember: **staying silent can put others at risk**, but speaking up helps build a safer online world for everyone. Trust your instincts, and if something seems strange, report it!

Critical Thinking Questions

1. Why do you think some websites require two-factor authentication instead of just a password?
2. How would you explain encryption to someone your age using a simple example?

Questions (5)

1. What is an example of a data vulnerability?

MULTIPLE CHOICE

Choose the correct answer:

- A. Using two-factor authentication
- B. Having strong password habits
- C. Using the same password for every website
- D. Installing antivirus software

2. Which of the following is the strongest password?

MULTIPLE CHOICE

Choose the correct answer:

- A. Password123
- B. Baseball99
- C. John2024
- D. A7\$kQ!bX3Z1f

3. What does two-factor authentication do?

MULTIPLE CHOICE

Choose the correct answer:

- A. Stores your passwords automatically
- B. Sends your password to your email
- C. Requires another step (like a phone code) after entering a password
- D. Lets anyone use your account if they guess the password

4. Which of these is considered confidential information?

MULTIPLE CHOICE

Choose the correct answer:

- A. Your favorite food
- B. Your social security number
- C. Your dog's name
- D. Your favorite video game

5. What does encryption do to your data?

Choose the correct answer:

- A. Scrambles it so only certain people can read it
- B. Deletes it permanently
- C. Translates it into emojis
- D. Uploads it to the cloud

Answer Keys & Solutions

Questions

1. What is an example of a data vulnerability?

MULTIPLE CHOICE

Correct Answer:

- A. Using two-factor authentication ✗ Incorrect
- B. Having strong password habits ✗ Incorrect
- C. Using the same password for every website ✓ Correct
- D. Installing antivirus software ✗ Incorrect

2. Which of the following is the strongest password?

MULTIPLE CHOICE

Correct Answer:

- A. Password123 ✗ Incorrect
- B. Baseball99 ✗ Incorrect
- C. John2024 ✗ Incorrect
- D. A7\$kQ!bX3Z1f ✓ Correct

3. What does two-factor authentication do?

MULTIPLE CHOICE

Correct Answer:

- A. Stores your passwords automatically ✗ Incorrect
- B. Sends your password to your email ✗ Incorrect
- C. Requires another step (like a phone code) after entering a password ✓ Correct
- D. Lets anyone use your account if they guess the password ✗ Incorrect

MULTIPLE CHOICE

4. Which of these is considered confidential information?

Correct Answer:

- | | |
|--------------------------------|-------------|
| A. Your favorite food | ✗ Incorrect |
| B. Your social security number | ✓ Correct |
| C. Your dog's name | ✗ Incorrect |
| D. Your favorite video game | ✗ Incorrect |

5. What does encryption do to your data?

MULTIPLE CHOICE

Correct Answer:

- | | |
|--|-------------|
| A. Scrambles it so only certain people can read it | ✓ Correct |
| B. Deletes it permanently | ✗ Incorrect |
| C. Translates it into emojis | ✗ Incorrect |
| D. Uploads it to the cloud | ✗ Incorrect |