AP Cybersecurity Summer Assignment

Cybersecurity in Everyday Life

Welcome to AP Cybersecurity. This course **does not** require previous computer science experience. Some students may have taken AP Computer Science Principles, and others may be taking their first computing-related course. This assignment is designed to give everyone a common starting point.
You do not need to know how to code to complete this assignment. You should use your own words, think carefully, and be ready to discuss your ideas during the first week of class.

Part 1: Personal Cybersecurity Reflection

Answer each question in 3–5 complete sentences.

1. Describe a time when you, or someone you know, received a suspicious email, text, direct message, phone call, or pop-up. What made it seem suspicious?

2. What makes a password strong? What makes a password weak?

3. What is multi-factor authentication, and why might it protect an account better than a password alone?

4. What are some possible risks of using public Wi-Fi in places like airports, hotels, coffee shops, or restaurants?

5. How might AI make scams or cyberattacks more convincing?

6. How might AI also help people defend against cyberattacks?

Part 2: Mini Case Studies

For each scenario, answer the following:

1. What are the warning signs?
2. What could happen if the person makes the wrong choice?
3. What should the person do next?

Scenario A: Account Warning

You receive a text message that says:
“Your Microsoft account will be locked in 10 minutes due to suspicious activity. Click here immediately to verify your password.”
The link looks slightly different from the real Microsoft website.

1.
2.
3.

Scenario B: Verification Code

A friend messages you and says they are locked out of an account. They ask you to send them a verification code that was just texted to your phone.

1.
2.
3.

Scenario C: Public Wi-Fi

You are at a coffee shop and see two networks:

- CoffeeHouse Guest
- CoffeeHouse Free Guest WiFi

You are not sure which one is real. You need to log in to an important account.

1.
2.
3.

Part 3: Vocabulary Preview

Define each term in your own words. Then give a simple real-world example. **Do not copy and paste definitions.** Your definitions should sound like something you could explain to a classmate.
For the vocabulary section, use the CISA NICCS Cybersecurity Glossary as your starting point. You may also use the CIS Terms & Definitions page if you need a simpler explanation. *Your final definitions and examples must be written in your own words*.

1. vulnerability
2. threat
3. risk
4. adversary
5. attack
6. mitigation
7. authentication
8. multi-factor authentication
9. social engineering
10. phishing
11. encryption
12. indicator of compromise

Part 4: Secure One Thing

Choose one safe cybersecurity improvement you can make before the first day of class. You may choose one of these options or propose your own:

- Turn on multi-factor authentication for a personal account.
- Update a phone, laptop, tablet, or app.
- Review app permissions.
- Check whether you reuse the same password on multiple accounts.
- Create a stronger passphrase strategy.
- Review privacy or security settings on an app you use.
- Learn how to identify suspicious links or URLs.

Write one paragraph explaining:

1. What you chose to improve.
2. Why it matters.
3. What you learned.
4. One question you still have about cybersecurity.

Important: Do not submit passwords, personal account information, private screenshots, security codes, or anything sensitive.

Submission

Submit your completed assignment in Canvas by the first week of class. Your work will be graded for completion, thoughtfulness, use of your own words, and participation in our first few class discussions.