4565: Computing Foundations for a Digital Age
Unit 2

Day 3 Lesson Plan: Cyber Threats & Protectio

Objective

Students will identify common cyber threats and explain strategies for protecting their devices, accounts, and personal data.

Word Bytes

- **Phishing** – A trick used by scammers to get your personal info, usually through fake emails or messages.
- **Malware** – Harmful software designed to damage your device or steal information.
- **Ransomware** – A type of malware that locks your files and demands money to unlock them.
- **Firewall** – A digital wall that helps block harmful content or hackers from getting into your device or network.

Activities

Hook: Cybersecurity Scenarios

- Share short threat scenarios (e.g., phishing email, infected USB drive) and have students quickly guess what kind of threat it is. This can be done as a class warm-up or bellringer.

Mini-Lesson: Understanding the Threats

- Begin by defining each threat and then provide a real-world example students can relate to. Follow with a brief classroom discussion for each one:

  Phishing – Explain how phishing tricks users into giving away personal information through fake emails or messages.

  - *Example:* An email that looks like it's from your bank says your account is locked and asks you to click a link to verify your credentials.
  - *Discussion prompt:* Why might someone fall for this? What clues help you spot it's fake?

  Malware – Discuss how malware can be unknowingly downloaded and how it affects a device.

  - *Example:* You download a free game and your tablet starts crashing and behaving strangely.

- *Discussion prompt:* Why is it risky to download software from unknown sources?

Ransomware – Describe how ransomware locks a user's files and demands payment.

- *Example:* A school district can't access its system because a message says they must pay to unlock the files.
- *Discussion prompt:* Why might some people pay the ransom? Should they?

Firewall – Explain the role of firewalls in filtering traffic and preventing unwanted access.

- *Example:* A school's firewall blocks gaming websites during school hours.
- *Discussion prompt:* When are firewalls helpful? Can they be too restrictive?

Cybersecurity Escape Room

- Have students complete a digital escape room that reinforces vocabulary and real-world threat recognition. You can use a pre-built Google Forms escape room or create your own with locks based on clues.

  - Sample challenge: "Identify the type of attack based on this email screenshot."

Extension (Optional): Famous Attacks Research

- Students work in small groups to research a real-world cyberattack (e.g., Target, Colonial Pipeline) and present key facts—what happened, how it was prevented (or not), and lessons learned.

Word Bytes Dictionary Update

Students add **"phishing," "malware," "ransomware,"** and **"firewall"** to their Word Bytes dictionary with examples.

Suggested examples:

- Phishing – A fake email that tricks you into sharing your password.
- Malware – A virus that deletes files on your laptop.
- Ransomware – Your files are locked, and someone demands money to unlock them.
- Firewall – A blocker that keeps dangerous websites out.