

Unit 2: Cybersecurity, Digital Safety & Emerging Technologies

Unit Length: 1.5 weeks

Unit Introduction

This unit introduces students to core concepts in cybersecurity, digital privacy, and emerging technologies. Through debates, case studies, collaborative projects, and hands-on exploration, students will learn how to protect their digital lives, understand the balance between privacy and security, and examine the ethical implications of advanced technologies such as AI and facial recognition.

Unit Objective

Students will understand how to identify and respond to cybersecurity threats, evaluate personal and public privacy risks, and analyze the ethical and societal impacts of emerging technologies.

Standards Covered

- 4565.D4.1: Describe the dynamics of privacy versus security.
 - 4565.D4.5: Explain the importance of cybersecurity and examine its ethical implications.
 - 4565.D4.6: Demonstrate how to optimize operating system and security settings.
 - 4565.D5.4: Analyze the impact of emerging technologies on society.
-

Word Bytes

Students will build a personal "Word Bytes" digital dictionary throughout the unit. Key terms include:

- Digital Footprint – The trail of data you leave behind every time you go online.
- Online Reputation – What others think about you based on what they see online.
- Data Tracking – The way websites, apps, or companies collect info about your activity.
- Privacy – Your ability to control who can see your personal information or activities.
- Security – The protection of your devices, data, and identity from threats.
- Personal Data – Information that can identify you, like your name or address.
- Data Breach – When private information is stolen, shared, or exposed.

- Phishing – A scam using fake emails or messages to get your information.
 - Malware – Harmful software meant to damage your device or steal data.
 - Ransomware – Malware that locks your files and demands money to unlock them.
 - Firewall – A protective digital barrier blocking harmful content or hackers.
 - Two-Factor Authentication (2FA) – An added login step requiring a second form of identification.
 - VPN (Virtual Private Network) – A tool that hides your online activity and location.
 - Password Security – The use of strong, unique passwords to protect your accounts.
 - Permissions – Settings that control what apps or websites can access on your device.
 - AI (Artificial Intelligence) – Programs that can learn or make decisions like recommending videos.
 - Deepfake – Fake images or videos created using AI to look very real.
 - Facial Recognition – Technology that identifies people by scanning their faces.
 - Data Bias – When unfair decisions are made due to flawed or limited training data.
-

Daily Breakdown

Day 1: What is a Digital Footprint?

Objective: Students will explain what a digital footprint is and how it can impact their future.

Materials Needed: Internet-connected device, reflection sheet

Activities:

- Google Yourself: Reflect on your digital footprint
- Class discussion: Who sees your digital trail?
- Real-world case studies: Explore social media consequences

Day 2: Privacy vs. Security

Objective: Students will differentiate between privacy and security and evaluate trade-offs in real-life scenarios.

Materials Needed: Case study printouts, debate guide

Activities:

- "Would You Rather" Privacy vs. Security Debate
- Case study card sort: Classify as privacy or security issue
- Role-play perspectives: hacker, government, tech company

Day 3: Cyber Threats & Protection

Objective: Students will identify and respond to common cyber threats.

Materials Needed: Escape room (Google Form), threat scenario cards

Activities:

- Cybersecurity Escape Room challenge
- Threat scenario group analysis
- Extension: Research a famous cyberattack and present takeaway

Days 4–6: Cybersecurity Poster or Board Game Project

Objective: Students will collaborate to create a project that promotes digital safety and cybersecurity best practices.

Materials Needed: Poster materials or digital design tools, rubric

Activities:

Day 4: Research & topic selection

Day 5: Design & development

Day 6: Presentations of posters or games

Day 7: Operating Systems & Security Settings

Objective: Students will explore and adjust digital security settings within an OS or device.

Materials Needed: Classroom devices or screenshots

Activities:

- Security Settings Scavenger Hunt
- Annotation of screenshots with improvement suggestions
- Adjusting app permissions and enabling 2FA

Day 8: Emerging Technologies & Ethical Concerns

Objective: Students will analyze the impact and ethical implications of AI and emerging tech.

Materials Needed: AI demo videos, articles, discussion prompts

Activities:

- AI and Ethics Discussion: Impacts on privacy and society
- Deepfake and facial recognition video analysis
- Mini-research: Students present one tech concern

Day 9: Post-Test & Jeopardy Review

Objective: Students will review and demonstrate understanding of cybersecurity concepts.

Materials Needed: Kahoot or Quizizz, buzz-in game, post-test

Activities:

- Jeopardy review game (use buzzin.live)
- Short post-test
- Exit reflection: How will you apply cybersecurity daily?

Unit Wrap-Up Objective

Students will be able to identify cybersecurity risks, use security tools to protect themselves online, and evaluate the broader impacts of emerging technologies on society.