AI + Cybersecurity Discussion Prompt

Student Tool Audience: Teachers, Students | Grades 8-12

Purpose

• AI can help people learn, create, summarize, detect patterns, and automate tasks. In cybersecurity, AI can support defenders, but it can also create new risks. This discussion helps students think critically about AI, privacy, data security, and responsible technology use in a safe classroom setting.

Student-safe note

• Use fictional examples. Do not use real passwords, real accounts, live suspicious links, or private information.

Standards summary

• This resource may support CSF 13.1, CSF 14.1, CSF 14.2, CSF 14.3.

• Detailed alignment depends on local district pacing, approved course placement, and teacher directions.

Purpose

AI can help people learn, create, summarize, detect patterns, and automate tasks. In cybersecurity, AI can support defenders, but it can also create new risks. This discussion helps students think critically about AI, privacy, data security, and responsible technology use in a safe classroom setting.

Student-Safe Guardrails

- Discuss defensive and ethical cybersecurity only.
- Do not ask for instructions to break into accounts or systems.
- Do not create malware, credential theft messages, or real attack plans.
- Do not use real school systems, real accounts, or real targets.
- Do not share passwords, API keys, verification codes, private student data, or personal information with AI tools.

Opening Prompt

AI can help cybersecurity defenders find patterns, explain alerts, summarize logs, and teach safer habits. It can also help attackers create more convincing scams or automate harmful tasks. How should schools teach students to use AI responsibly in cybersecurity?

Discussion Questions

- How might AI help a cybersecurity team defend an organization?
- How might AI make phishing or scams harder to recognize?
- Why is privacy important when using AI tools?
- What information should never be pasted into an AI tool?
- What is the difference between learning about security and attempting unauthorized access?
- What rules should students follow when AI and cybersecurity overlap?

Scenario Cards

Card	Situation	Discussion Focus
Scenario 1	A student wants AI to explain why a password should not be reused.	Acceptable if no real passwords are shared.
Scenario 2	A student asks AI to write a fake login page for a prank.	Not acceptable. It could enable credential theft.
Scenario 3	A student asks AI how to report a suspicious email safely.	Acceptable and defensive.
Scenario 4	A student pastes a private school email thread into AI for analysis.	Not acceptable without permission. Privacy risk.

Exit Reflection

One defensive use of AI in cybersecurity:

_____

One AI and cybersecurity risk:

_____

One rule students should follow:

_____

Detailed Tennessee Standards Connection

Tennessee Standards Connection

This discussion prompt supports standards when students evaluate AI-related security risks, privacy concerns, ethical responsibilities, and defensive cybersecurity uses.

Standards source: Tennessee Department of Education, Computer Science Foundations (C10H11), May 2023. Confirm final alignment against local district pacing, approved course placement, and teacher directions.

This resource may support the following Tennessee standards when used as part of cybersecurity, digital ethics, computer science, AI literacy, or career-connected technology instruction:

- CSF 13.1 - Social, Legal, and Ethical Issues: Students research social, legal, and ethical issues encountered by IT professionals and identify responsibilities when addressing technology problems.
- CSF 14.1 - Data Security: Students explain why data security is a priority and demonstrate understanding of confidentiality, availability, and integrity.
- CSF 14.2 - Security Breaches: Students demonstrate understanding of security breaches, enterprise-level security, encryption, protocols used to secure websites, and privacy considerations.
- CSF 14.3 - Security Practices: Students identify security practices for computer and network systems, including access control, encryption techniques, BIOS features, and malware response strategies.

Use guidance

- Confirm final alignment against local district pacing, approved course placement, and teacher directions.
- Keep instruction defensive, ethical, age-appropriate, and classroom-safe.