Password Strength Activity

Student Activity Audience: Students | Grades 8-12

Purpose

• Do not write, share, test, or submit a real password. Use only fictional examples created for class.

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 14.3.

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

Important Safety Rule

Do not write, share, test, or submit a real password. Use only fictional examples created for class.

Main Ideas

- Long passphrases are usually stronger and easier to remember than short complex passwords.
- Reusing the same password across accounts creates risk.
- Multi-factor authentication adds protection if a password is stolen.
- Password managers can help users store strong unique passwords safely.
- No one should ask for your password in a message, chat, or email.

Part 1: Evaluate the Examples

Fictional Example	Rating	Reason
tigers	Weak	Too short and easy to guess
Tigers2026!	Better but still risky	Uses a common pattern and school/team clue
Blue-River-Pizza-Cloud-77	Stronger	Longer passphrase with unrelated words
SamePasswordEverywhere!	Risky	Reuse across sites creates major risk

Part 2: Build a Safer Passphrase Pattern

Create a fictional passphrase pattern using unrelated words. Do not use personal information, pet names, birthdays, school names, sports teams, or anything you really use.

Fictional passphrase example:

_____

Why it is stronger: _____

Part 3: Account Protection Reflection

- Why is password reuse dangerous?
- How does multi-factor authentication help?
- Why should you avoid sharing passwords, verification codes, or recovery codes?
- What should you do if you think an account has been compromised?

Exit Ticket

One password habit I should avoid:

_____

One stronger account habit I can use:

_____

Detailed Tennessee Standards Connection

Tennessee Standards Connection

This activity supports standards when students connect account protection, access control, confidentiality, and safe security practices to everyday technology use.

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 14.3 - Security Practices: Students identify security practices for computer and network systems, including access control, encryption techniques, BIOS features, and malware response strategies.

Item	Details
Estimated Time	30-45 minutes
Purpose	Help students understand why strong passwords, passphrases, multi-factor authentication, and safe account habits matter.
Student Product	Password safety analysis, stronger passphrase example, and reflection.

Use guidance

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