

CLASSROOM LESSON · GRADES 3-5

Passphrase power

Build a password that is easy to remember and hard to guess

Students play a password guessing race to see why every extra word makes a password much harder to guess, learn the silly-sentence and random-word methods for building a passphrase, practice building one (practice only, never a real password), and agree never to reuse passwords or share them except with a trusted adult.



GRADE BAND 3-5	TIME 40 minutes	FORMAT Whole class + groups	PREP Print & cut, ~10 min
---------------------------------	----------------------------------	--	--

BIG IDEA



A long, silly, secret string of words protects your account better than a short word with tricky symbols. Use a different one for every account and share it only with a trusted adult.



Students will be able to

- ☐ Explain in their own words why a longer password is harder to guess than a short one with symbols
- ☐ Build a practice passphrase of four or more words using the silly-sentence or random-word method
- ☐ Explain why reusing one password on many accounts is risky
- ☐ Name the trusted adults who may help with a school password (a parent or guardian, the teacher or the school technology helper)



Materials

- Board or projector for the slides
- Worksheet: Passphrase builder (1 per student)
- Worksheet: Passphrase crossword (1 per student, for early finishers or a next-day review)
- Scenario cards (1 set per group of 4)
- One die per pair (optional; students can also close their eyes and point to the word bank)
- Sticky notes for the exit ticket
- Timer

Before class

- Print the builder and crossword worksheets and one set of scenario cards per group of four. Cut the cards apart.
- Write two word lists on the board for the guessing race. List A (animals): 1 cat, 2 dog, 3 frog, 4 bear, 5 duck, 6 fish. List B (colors): 1 red, 2 blue, 3 green, 4 pink, 5 gold, 6 gray.
- Write your secret race answers on a folded sticky note: Round 1 is one animal (for example frog); Round 2 is one color plus one animal (for example gold duck). Do not use anything that is a real password.
- Write on the board: Long. Silly. Secret. Different for every account.
- Write the name of your school's technology helper or help desk process on the board.



Vocabulary

- **Password** — A secret you type to prove an account is yours.
- **Passphrase** — A password made of several words in a row, like PurpleCatTacosMoon. It is long, so it is hard to guess, and silly, so it is easy to remember.
- **Authentication** — Proving you are really you when you log in, for example by typing your passphrase.
- **Reuse** — Using the same password on more than one account. If one account is broken into, all the others are in danger too.

Vocabulary (continued)

- **Random** — Picked by chance, like rolling a die, so nobody can predict it.
- **Trusted adult** — A grown-up who keeps you safe and may help with your password: a parent or guardian at home, or your teacher or school technology helper.

Standards alignment

- **ISTE Standards for Students 1.2.d** — Digital Citizen, Digital Privacy: students take steps to protect their privacy on devices and look after their personal information and account security when they are online.
- **CSTA PK-12 Computer Science Standards (2026) E4-SYS-SE-13** — Grade 4, Systems and Security: students tell the difference between proving who you are (authentication) and what you are allowed to do once you are in (authorization) when protecting devices and private information.
- **CSTA PK-12 Computer Science Standards (2026) E5-SYS-SE-13** — Grade 5, Systems and Security: students describe the three goals of keeping information safe (keeping it private, keeping it correct and keeping it available) and why each one matters.
- **CSTA K-12 Computer Science Standards (2017) 1B-NI-05** — Grades 3-5, Networks and the Internet: students talk about real cybersecurity problems and the ways people can protect personal information.

This lesson lines up with widely used digital citizenship and computer science frameworks; Georgia districts can map it to their state computer science and digital literacy expectations for grades 3-5.

Lesson sequence · 40 minutes

5' Warm-up

- 1 Ask students to write on a scrap paper (not to share): Which is harder to guess, cat or PurpleCatTacosMoon? Why?
- 2 Take a few answers. Listen for longer, more letters, weird, not a normal word.
- 3 Remind students: We will never say or write a real password today. Everything we make is practice.

Say: "Quick question. Which would take longer to guess: the word cat, or the words purple cat tacos moon all squished together? Think about it, then jot your answer. And one rule for today: we will never say or write a real password. Everything we build is practice, just for learning."

12' Mini-lesson

- 1 Password guessing race, Round 1 (2 minutes): Say your secret password is one word from List A. Call on students one at a time to guess. Tally guesses on the board. With only 6 choices, the class finds it in 6 guesses or fewer.
- 2 Round 2 (3 minutes): Now the secret is one color from List B plus one animal from List A. Teams take turns guessing for 2 minutes and you tally. Reveal the answer. Show the math: $6 \times 6 = 36$ possible two-word passwords.
- 3 Show slide 3. Keep multiplying: 3 words from 6-word lists = 216 choices, 4 words = 1,296. Real passphrases pick from thousands of words. With 1,000 words to choose from, 4 random words make 1,000,000,000,000 (one trillion) possible passwords. A 4-digit PIN has only 10,000.
- 4 Show slide 4: length beats tricky symbols. A short word like P@ssw0rd1 is easy for guessing programs, because people tend to make the same swaps (a to @, o to 0, add 1 at the end). Computers can guess much faster than people, so length is what slows them down. CISA, the U.S. cybersecurity agency, suggests at least 16 characters, and a passphrase of 4 to 7 unrelated words is one way to get there.
- 5 Show slide 5: two ways to build one. Silly-sentence method: picture a silly scene and use the whole words (PurpleCatTacosMoon). Random-word method: roll a die or close your eyes and point at a word bank, then string the words together. Avoid your name, birthday, pet, school, team or a famous quote.
- 6 Show slide 6: the two rules that protect you. Never reuse (a different passphrase for every account), and never share except with a trusted adult (a parent or guardian, your teacher or the school technology helper).

Say: "Round one: my secret password is one animal from List A. Who wants to guess? ... Found it fast, right? Only six choices. Round two: one color and one animal. Teams, you have two minutes. ... That was much harder, and I only added one word. Every word you add multiplies the choices. That's the power of a passphrase. Now here's a surprise: P@ssw0rd1 looks tricky, but guessing programs try those swaps first. Long beats tricky."

13' Activity

- 1 Hand out the Passphrase builder. Students choose a method and build a practice passphrase of at least four words. Remind them: this is practice only. Do not use it for a real account.
- 2 Students count the letters (aim for 16 or more), check for personal words and draw a memory picture.
- 3 Groups of four take turns reading a scenario card aloud and agreeing on an answer (5 minutes). Circulate and listen for reuse and sharing answers.
- 4 Early finishers start the Passphrase crossword.

5' Discussion

- 1 Ask two or three discussion questions. Call on groups to share their hardest scenario card.
- 2 Clear up any confusion: real passwords stay secret, school passwords are shared only with a trusted adult, and anyone who thinks a password got out should tell an adult so it can be changed.
- 3 Collect or send home the builder sheets. Ask students to cross out their practice passphrase if they plan to take the sheet home.

5' Exit ticket

- 1 Students answer the three exit ticket questions on a sticky note.
- 2 Sort the notes into got it and needs a check-in; follow up with students who chose the short tricky password or said it is fine to reuse.

Discussion questions

1. Why was Round 2 of the guessing race so much harder than Round 1?

Listen for: Adding a word multiplies the number of choices (6 became 36). More words means many more guesses.

2. Why might P@ssw0rd1 be weaker than PurpleCatTacosMoon even though it has symbols?

Listen for: It is short and uses common swaps that guessing programs try first; the passphrase is longer and not a common word.

3. Why should every account have its own passphrase?

Listen for: If one game or website leaks your password, someone could try it on your school or email account. Different passphrases keep the problem in one place.

4. Who may you share your school password with, and why only them?

Listen for: A parent or guardian, the teacher or the school technology helper. They help keep you safe and can reset it; friends and online players cannot.

5. What should you do if you think someone saw your password?

Listen for: Tell a trusted adult right away and change it together. You are not in trouble.

Exit ticket

On your sticky note, answer all three. Do not write any real password.

1. Circle the stronger one: Tiger7! or tuba-pickle-rainbow-sled. Why? → **tuba-pickle-rainbow-sled. It is longer and made of random words, so there are far more possible guesses.**
2. Your game and your school account have the same password. Is that OK? What should you do? → **No. Make a different passphrase for each account, with a trusted adult's help.**
3. Name one person you may share a school password with. → **A parent or guardian, the teacher or the school technology helper.**



Support

- Give a ready-made word bank (on the builder sheet) and let students build a 3-word passphrase first, then add a fourth word.
- Pair students for the guessing race and the builder so one can roll and one can write.
- Provide a letter-counting strip or let students count with a partner.
- Use only scenario cards 1, 2, 4 and 6 for groups that need a shorter set.



Extend

- Students calculate how many choices there are for 5 words from a 6-word list ($6 \times 6 \times 6 \times 6 \times 6 = 7,776$) and explain what happens with a bigger list.
- Students compare two passphrases with the same letter count and explain which is better and why (random words beat a famous phrase).
- Students write a short note for younger students explaining why passwords are secret.
- Introduce password managers: a program that creates and remembers strong passwords so a person only needs to remember one strong passphrase. Adults set these up, not students.



Multilingual learners

- Let students build a practice passphrase with words from their home language or mix languages; mixing is perfectly fine and can make it harder to guess.
- Pre-teach vocabulary with icons: passphrase (key), reuse (two arrows), secret (finger to lips).
- Spanish connections: contraseña (password), frase de contraseña (passphrase), secreto (secret), no reutilizar (do not reuse).
- Provide sentence frames: "A longer password is stronger because ____." "I share my school password only with ____."



Accessibility

- Fine-motor needs: students can say their practice passphrase to an adult scribe, type it in a shared document that is deleted afterward, or point to words in the word bank. They do not need to roll a die; a partner rolls.
- Visual needs: enlarge the builder and crossword to 150 percent; read the scenario cards aloud in each group; provide a large-print word bank. Students who use screen readers can build the passphrase orally.
- Offer a word-list version of the crossword (words with clues to match) for students who find grids hard to track.
- Students who struggle with spelling can choose short, easy words; length comes from the number of words, not spelling.



Family extension

Passphrase power: a family page. Today your child learned that a long passphrase of four or more random words is easier to remember and harder to guess than a short password with symbols. We also learned two rules: use a different passphrase for every account, and share a school password only with a parent, guardian or teacher.

Send home the family sheet (English and Spanish) included in this lesson pack.



Follow-up: free 2-minute lesson

k12cyberforward.com/learn/passphrase-power

Project it for a quick review or share the link with families.
Related Cyber Academy course: academy-students-3-5.

Sources and further reading.

- CISA Secure Our World: Use strong passwords (at least 16 characters; passphrase of 4-7 unrelated words; unique per account; password managers): <https://www.cisa.gov/secure-our-world/use-strong-passwords>
- NIST SP 800-63B-4: Authentication and Authenticator Management (length as a primary factor; no composition rules; predictable user substitutions): <https://pages.nist.gov/800-63-4/sp800-63b.html>
- FTC Consumer Advice: Heads Up, Stop. Think. Connect. (don't share passwords; different password for each account): <https://consumer.ftc.gov/articles/heads-up>
- FTC Consumer Advice: Use two-factor authentication to protect your accounts: <https://consumer.ftc.gov/articles/use-two-factor-authentication-protect-your-accounts>
- ISTE Standards for Students: <https://iste.org/standards/for-students>
- CSTA 2026 PK-12 Computer Science Standards: <https://csteachers.org/pk12standards/>
- CSTA K-12 Computer Science Standards (2017), condensed: <https://csteachers.org/wp-content/uploads/2025/03/csta-k-12-computer-science-standards-revised.pdf>