

Cyber Elementary School

Elementary School Cyber Security, Online Safety & AI Safety Curriculum

Lesson 1: Creating Strong Passwords: Your Digital Lock and Key

Lesson Title: Creating Strong Passwords: Your Digital Lock and Key

Lesson Number: 1 of 36

Grade/Age: Elementary School (Grades 3–6)

Subject: Cyber Security and Safety

Duration: 30–40 Minutes

Learning Objectives

- Students will be able to explain, in their own words, why passwords protect their personal information and online accounts.
- Students will be able to identify the difference between a strong password and a weak password.
- Students will be able to create a strong, memorable password (or passphrase) that follows password best practices.
- Students will be able to describe at least one rule for keeping a password safe (e.g., never sharing it, not reusing it everywhere).

Skills

Digital literacy, critical thinking, pattern recognition, personal responsibility, creative problem-solving, basic cyber hygiene habits.

Warm-Up / Hook (5 minutes)

"Crack the Code" Guessing Game. Write four example passwords on the board, hidden at first, one at a time: 123456, password, Bella2016 (a sample "pet name + birth year"), and Tr@ff!c-Lemon42. Ask students to raise their hands and guess which ones a "digital burglar" (a hacker) could guess in under a second versus which ones would take a long time. Reveal that the first three could be guessed almost instantly by a computer program, while the last one could take years. Connect this to a physical analogy: a password is like a lock on your front door — a flimsy lock lets anyone walk in, but a strong lock keeps your house (your information) safe.

Recommended Teacher Talking Points (Introduction)

- Every day you use passwords — for a tablet, a game, an email account, or a school login. A password is like a key that only you should have.
- Just like you wouldn't give a stranger the key to your house, you shouldn't give your password to anyone except a trusted parent or guardian.
- Today we're going to learn what makes a password strong, what makes it weak, and how to build one that's hard for anyone else to guess but easy for YOU to remember.

Direct Instruction with Recommended Teacher Talking Points

Core Concept (All Grades):

- A strong password is long, uses a mix of different kinds of characters, and doesn't use information that's easy to find out about you — like your name, pet's name, or birthday.

- A weak password is short, common, or something everyone can guess — like 123456, password, or your own first name.
- Never share your password with friends, even best friends. The only people who should ever know it are you and your parent or guardian.
- Use a different password for different accounts. If one password gets stolen, you don't want a stranger to be able to unlock everything else, too.

Increased Learning — 4th Grade Level:

- Introduce the idea of "password length matters more than complexity tricks." Explain that adding just a few extra characters makes a password dramatically harder to crack.
- Introduce the concept of a passphrase — stringing together several random, unrelated words (e.g., PurpleTiger-Bicycle-7Clouds) — as an easier way to build a long, strong password.
- Talking point: "Computers that try to guess passwords work fast, but longer passwords take exponentially more time to guess. Four random words strung together can be both strong AND easy to remember."

Increased Learning — 5th Grade Level:

- Introduce password managers at a conceptual level: a secure digital "vault" that remembers strong passwords for you so you don't have to reuse the same one everywhere.
- Introduce the risk of credential reuse: if a website you use gets hacked and your password leaks, anyone can try that same password on your other accounts (email, games, school portal).
- Talking point: "Grown-ups often use password managers, which are like a locked notebook only you can open, so every account can have its own unique strong password without you needing to memorize all of them."

Increased Learning — 6th Grade Level:

- Introduce two-factor authentication (2FA) as a companion concept to passwords — a second layer of proof (like a code sent to a parent's phone) that keeps an account safe even if the password is somehow discovered.
- Introduce the idea of how attackers use "credential stuffing" and dictionary attacks at a basic conceptual level — automated programs that try common passwords and leaked password lists very quickly.
- Talking point: "Strong passwords are important, but they work best as part of a bigger toolkit — like adding a second lock or an alarm system on top of your front door lock."

Guided Practice by Grade Skill Level

(Skill activity to complement the learning objective)

3rd Grade: Weak or Strong Sort

- In pairs, students receive a set of 8 password cards (e.g., cat123, Sunshine!7Bridge, mydog, Q7#mPz2!). They sort each card into a "Weak" or "Strong" pile and explain one reason for each choice using a sentence starter: "This is weak/strong because ____."

4th Grade: Build-a-Passphrase

- Students are given three random word cards (e.g., "Turtle," "Rocket," "Umbrella") and combine them with a number and symbol to build a passphrase. They test their passphrase against a class checklist (length ≥ 12 , includes a number, includes a symbol, no personal info).

5th Grade: Password or Personal Info?

- Students review a short fictional social media profile (name, pet, favorite sports team, birth year all visible) and identify why passwords based on any of that visible information would be unsafe. They then write a strong password that avoids all of it.

6th Grade: *Layered Defense Diagram*

- In small groups, students label a simple diagram showing three layers of account protection: strong password → password manager → two-factor authentication. Each group explains in one sentence what would happen if only the first layer existed and it were guessed.

Independent Practice or Homework Handout by Grade Skill Level

3rd Grade Worksheet: *"Lock It Up!"*

- Circle the STRONG password in each pair (5 pairs provided, e.g., dog vs. Bl3u-Kite92).
- Draw a picture of a strong lock and a weak lock to match a strong and weak password.
- Write one rule about who you can share a password with.

4th Grade Worksheet: *"Build Your Own Passphrase"*

- Choose three words from the provided word bank and combine them into a passphrase.
- Add a number and a symbol to your passphrase.
- Explain in 1–2 sentences why a longer password is harder to guess.

5th Grade Worksheet: *"Password Detective"*

- Read a short profile of a fictional student and list 3 pieces of information a hacker could try to guess as a password.
- Create a strong password for that student that avoids all of that information.
- Short answer: Why is it risky to use the same password on more than one account?

6th Grade Worksheet: *"Layers of Protection"*

- Define password, password manager, and two-factor authentication in your own words.
- Explain how each layer helps if one layer fails.
- Scenario question: A classmate says they use their birthday as a password for every account because it's easy to remember. Write 2–3 sentences of advice you would give them.

Closure (5 minutes)

Bring the class back together and ask 2–3 volunteers to share one new password rule they learned. Reinforce the key takeaway: "A strong password is long, unique, and private — and it's one of the easiest ways to protect yourself online." Preview that the next lesson will build on this by discussing how to keep devices and software updated and even safer.

Assessment

3rd Grade Quiz (4 questions)

1. Which of these is the strongest password? a) 123456 b) mycat c) Gr33n-Fr0g!7 d) password
2. True or False: It's okay to tell your best friend your password.
3. A password is like a _____ for your information. a) window b) key c) sticker
4. Name one thing that makes a password weak.

Answer Key (Teacher Use) — 3rd Grade

1. c) Gr33n-Fr0g!7 — it's long and mixes letters, numbers, and a symbol.
2. False — passwords should only be shared with a parent/guardian, never friends.
3. b) key.
4. Open-ended — accept any reasonable answer (e.g., it's short, it's a common word, or it uses personal information like a name or birthday).

4th Grade Quiz (5 questions)

1. What is a passphrase?
2. Why is password length important?
3. Which is a stronger passphrase? a) Tiger-Cloud-9Bicycle b) tiger123
4. True or False: Adding a symbol and number to a passphrase makes it stronger.
5. Short answer: Write an example of a strong passphrase (not using your real information).

Answer Key (Teacher Use) — 4th Grade

1. A passphrase is a password made of several random, unrelated words strung together (e.g., PurpleTiger-Bicycle-7Clouds).
2. Longer passwords have many more possible combinations, so they take a computer much longer to guess.
3. a) Tiger-Cloud-9Bicycle.
4. True.
5. Open-ended — accept any passphrase of 3+ random words plus a number and symbol, with no personal info (e.g., Rocket-Umbrella-42!).

5th Grade Quiz (5 questions)

1. Why is it risky to reuse the same password on multiple accounts?
2. List two pieces of personal information you should NOT use in a password.
3. What is one benefit of a password manager?
4. True or False: A strong password should include personal details so you remember it.
5. Short answer: Explain, in 2–3 sentences, how a hacker might guess a weak password.

Answer Key (Teacher Use) — 5th Grade

1. If one account's password leaks, an attacker can try the same password on other accounts and get into all of them.
2. Accept any two: name, pet's name, birthday/birth year, favorite team, address, phone number.
3. It securely stores and can generate a unique strong password for every account, so a person doesn't have to reuse or memorize them all.
4. False — personal details make a password easier to guess and should be avoided.
5. Open-ended — accept explanations that mention trying common passwords, guessing personal information, or using an automated program to try many passwords quickly.

6th Grade Quiz (6 questions)

1. What is two-factor authentication, and why does it add protection beyond a password?
2. Define "credential stuffing" in simple terms.

3. Why do security experts recommend a unique password for every account?
4. True or False: A password manager stores passwords so a person does not have to memorize every unique password.
5. Scenario: A website you use had a data breach and passwords were leaked. What should you do, and why?
6. Short answer: Describe the three layers of account protection discussed in class (password, password manager, two-factor authentication).

Answer Key (Teacher Use) — 6th Grade

1. 2FA requires a second proof of identity (like a code sent to a trusted device) in addition to the password, so an account stays protected even if the password is guessed or stolen.
2. Credential stuffing is when an attacker takes leaked username/password pairs from one breached site and automatically tries them on other websites.
3. Because if one password is stolen, unique passwords on other accounts keep those accounts safe rather than all being compromised at once.
4. True.
5. Change the password right away (and on any other account using the same one), and consider turning on two-factor authentication if available.
6. Password = the first lock protecting an account; password manager = securely stores/generates a unique strong password for every account; two-factor authentication = a second layer of proof beyond the password.

Teacher Reflection / Notes

- What worked well in this lesson? _____
- Which grade level needed more scaffolding or support? _____
- Did students grasp the analogy of password-as-lock? _____
- Adjustments for next time: _____