DIGITAL SELF & PERSONAL SAFETY · MODULE 1 · CHAPTER 2

Password Safety & Account Protection

Strong vs Weak · Never Share · 2-Step Verification (2FA / OTP)

⏱ 30–45 min

GRADE 6–8

⭐ Previously — What You Learned in Chapter 1

In Chapter 1, Monica posted her birthday invite publicly. It had her **home address** and **phone number**. Rohit and Sana helped her see the risk. Aryan almost shared his Aadhaar for a contest — Rohit stopped him in time. Monica learned to **think before you post.** Now in Chapter 2 — it is **Sana's** turn to make a mistake. Her Instagram gets **hacked.** Let's find out why.

🔑 Key Words

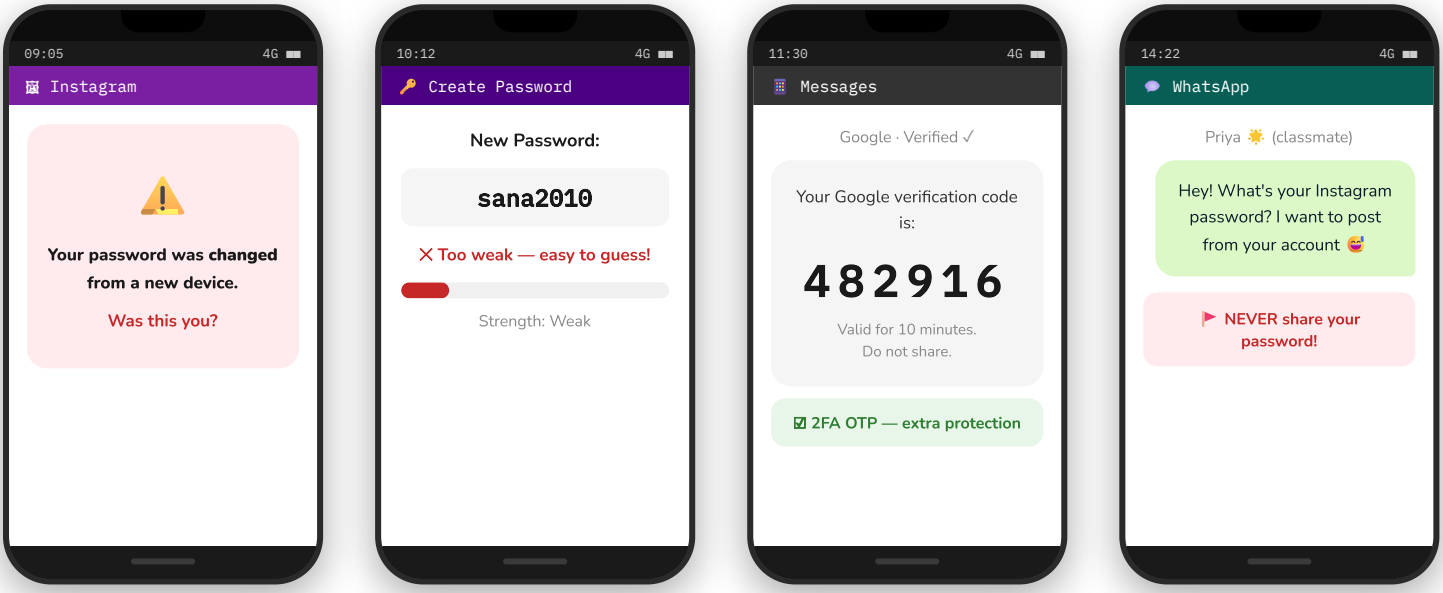
🔑
Password
A secret code. Only YOU should know it.

😟
Weak Password
Easy to guess — like your name or "123456".

💪
Strong Password
Letters + numbers + symbols. Hard to guess.

🔐
2FA / OTP
A second lock. A code sent to your phone.

📱 Have You Seen Any of These Screens?



Account hacked! 😱 | Weak password! 😰 | 2FA OTP! 🔒 | Friend asking! 😬

Activity — Match It!

Q1. Match each screen to what it shows — draw a line

Screen 1 — Account hacked 😱	(A) 2FA is protecting your account
Screen 2 — Weak password 😰	(B) What happens when a password is guessed
Screen 3 — OTP code 🔢	(C) Password with just name and year — weak!
Screen 4 — Friend asks 😬	(D) Sharing passwords — even with friends — is risky

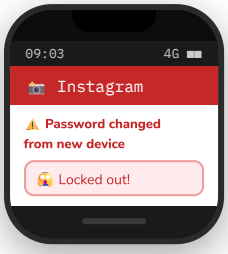
Pause & Think!

Your password is like the **key to your house**. A weak key is easy to copy. A shared key can be lost. By the end of this chapter — you will know how to make a **strong key** and add a **second lock** on top!

Scene 1 — Sana's Instagram Gets Hacked!

Monday Morning · Sana wakes up to a nightmare

1



Sana: I can't log in! Someone changed my password! All my posts are gone!

2

Monica: Oh no, Sana! This happened to me too — almost! What was your password?

Sana: It was... *sana2010*. And I also told Priya my password once so she could post a photo for me.

3

Monica: Rohit! Come here. Sana's Instagram was hacked. *sana2010* — ring a bell? And she shared the password too!

Rohit: **Two mistakes, Sana.** The password was too weak. AND you shared it. I'll explain both. Don't worry — we can fix this.

4

Aryan: Wait — I use *aryan2012* as my password. Is that bad too?!

Rohit: **Yes, Aryan. Very bad.** You're next in line to learn. Let's all sit down.

After the Story

Understand Sana's Mistakes

Q2. Tick ALL the mistakes Sana made

- [ ] Used her own name in the password
- [ ] Used her birth year in the password
- [ ] Shared her password with Priya
- [ ] Had no 2-step verification on her account
- [ ] She had an Instagram account

Q3. MCQ — circle one

Why was "sana2010" a bad password?

- ○ (A) It was too long
- ○ (B) It used her name + birth year — easy to guess
- ○ (C) It had too many letters
- ○ (D) Passwords should never have numbers

Quick Fact

Hackers try **name + birth year first** — because millions of people use exactly this. It takes less than 1 second to guess.

Pause & Think!

Sana's password had her name and birth year — two things many people already know. **A hacker doesn't need to be clever. They just try your name + birthday first.** Your password should be something no one can guess — not even your best friend.

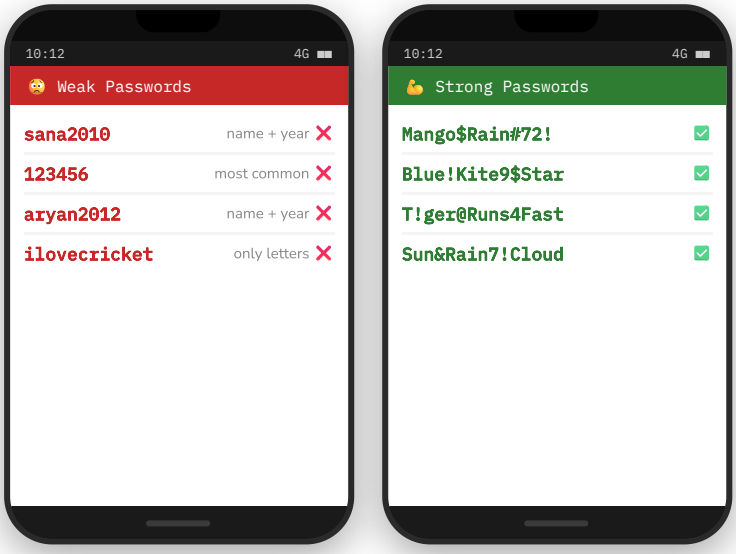
🎭 Scene 2 — Rohit Teaches: What Makes a Password Weak or Strong?

📍 **After School · Monica's House · Rohit explains to Sana, Monica, and Aryan**

Rohit: A strong password is like a **heavy lock**. A weak one is like a lock made of paper. Look at these examples on your phones.

Aryan: *aryan2012* is my password. Is that really that bad?

Rohit: A hacker can guess that in under one second, Aryan. Let me show you why.



Weak — easy to hack! Strong — hard to hack! ✅

🔍 Activity 1 — Strong or Weak?

Activity 1

Classify These Passwords

Q4. Write WEAK or STRONG in the box. Then write one reason

Password	Weak or Strong?	One reason why:
password123		
R0hit@School#1		
delhi2015		
Sun&Rain7!Cloud		

📖 Case Study — What Happened to Kabir?

Kabir, Class 7, uses **"kabir2012"** for his Gmail, Instagram, and gaming app — the **same weak password everywhere**. One day someone posts strange things from his Instagram. His Gmail also shows a login from an unknown city. His sister Neha says: *"You used your name and birthday — and the same password on every app!"*

Q5. Tick ALL the problems

- ☐ Used his own name
- ☐ Used his birth year
- ☐ Same password on every app
- ☐ No symbols or uppercase letters
- ☐ He told his sister about it

Q6. MCQ — circle one

Why is using the same password on every app dangerous?

- (A) It makes the password stronger
- (B) If one app is hacked — all apps are at risk
- (C) Apps share passwords with each other
- (D) It is easier to remember

Q7.

Write ONE thing you would tell Kabir to do right now:

Pause & Think! Hackers try name + birthday first. If that does not work, they try simple patterns like 123456. **Your password should never be something people already know about you.**

🔑 Activity 2 — The 4 Rules of a Strong Password

Rule 1 — Mix Letters
Use UPPER and lower case letters together · **Example: Mango**

Rule 2 — Add Numbers
Include at least 2 numbers anywhere · **Example: 72**

Rule 3 — Add Symbols
Add ! @ # $ % — makes it much harder · **Example: $Rain#**

Rule 4 — Make It Long
At least 8 characters. 12+ is even better! · **Example: Mango$Rain#72!**

🖍️ Activity 3 — Build Your Own Strong Password!

Activity 3

Rohit's trick: *"Pick 2 random words. Add a number. Add a symbol. Put them together. Done!"* Do NOT use your real name or birthday.

Step 1 – Word 1	Step 2 – Word 2	Step 3 – Number	Step 4 – Symbol
_____	_____	_____	_____

🔐 **My password (combine all 4):** _____

✅ Activity 4 — True or False?

Activity 4

Q8. Tick T (True) or F (False) for each statement

- ☐ T ☐ F Your name + birthday makes a weak password.
- ☐ T ☐ F A password with symbols is harder to crack.
- ☐ T ☐ F "123456" is used by millions of people — it is very safe.
- ☐ T ☐ F A longer password is generally stronger than a short one.

💭 Think About Yourself

Q9. Tick one — be honest!

How strong do you think your current password is?

😬 Weak — like sana2010 | 🤔 Not sure | 💪 Strong — has all 4 rules!

Pause & Think!
A strong password does NOT need to make sense as a word. Random is better! Once you make one — keep it private. Do not write it on a sticky note. Do not save it in a chat. A password only works if only YOU know it.

🎭 Scene 3 — Never Share Your Password — Not Even with Friends!

📍 Monica's House — Sana argues with Rohit

Sana 😳

But Rohit — Priya is my *best friend*! I trust her completely. Sharing with her is okay, right?

Even your best friend can make a mistake, Sana. They might tell someone else. Their phone might get hacked. Or you two might have a fight one day.

Rohit 🛡

It's like giving someone the **key to your house**. Even if you trust them — what if they lose the key? What if someone takes it from them?

Monica 💡

Aryan 😊

I gave my YouTube password to my classmate Ravi once. He seemed fine about it. Why is that bad?

📖 Case Study — What Happened to Arjun?

Arjun gave his YouTube password to classmate Ravi so Ravi could watch a video. Two weeks later, Arjun and Ravi had a fight. The next morning — Arjun found that someone had **deleted all his saved videos** and changed his channel name to something embarrassing. Arjun never found proof — but he knew **only Ravi had his password.**

Q10. `MCQ — circle one`

What was Arjun's mistake?

- ○ (A) He used YouTube
- ○ (B) He shared his password with Ravi
- ○ (C) He saved too many videos
- ○ (D) He fought with Ravi

Q11.

What should Arjun have done instead? Write one thing:

🚫 NEVER Share Your Password With...

- 👫 Your best friend
- 👩‍🏫 A teacher or adult online
- 📱 Anyone in a message or form
- 📝 A sticky note or paper

💭 Think About Yourself

Q12. `Tick one — be honest!`

Have you ever shared your password with anyone?

😳 Yes | 😊 No | 🤔 Not sure

If you answered Yes — what will you do about it now?

🔐 Pause & Think!

Even your best friend is human — they can forget, make mistakes, or be tricked into giving your password to someone else. **A password shared is a password at risk.** If you think your password was shared — change it right away and tell a trusted adult.

🎭 Scene 4 — Rohit Explains the Second Lock: 2FA!

📍 Monica's House — Rohit shows Sana how 2FA works

Even with a strong password — someone clever might still crack it. So we add a **second lock**. It is called 2-Step Verification or 2FA. — Rohit 🔒

Sana 🤔 — How does it work? Does it send a code to my phone?

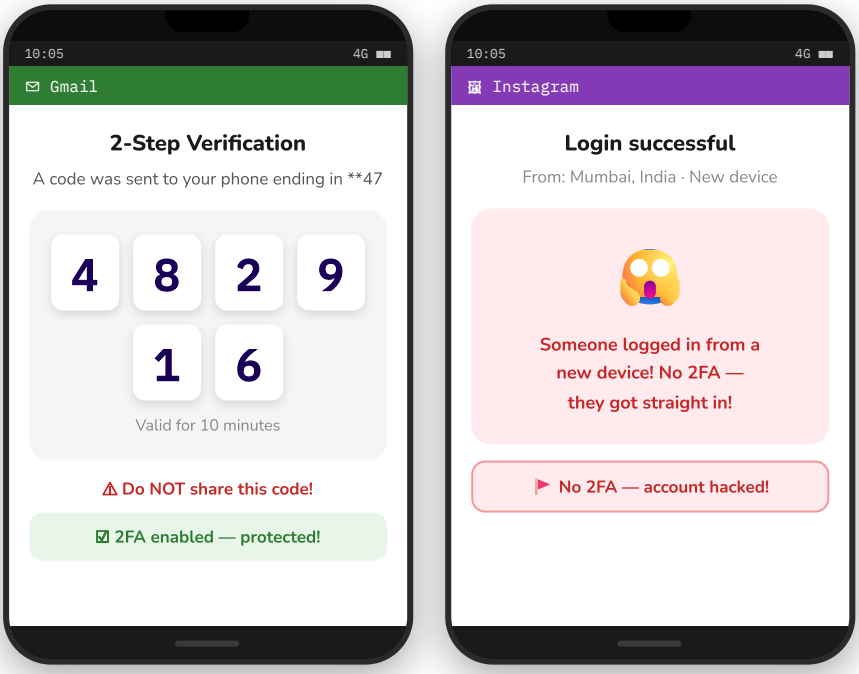
Exactly! First you enter your password. Then it sends an OTP — a one-time code — to your phone. You type that code. Only then does it let you in. **Two steps. Two locks. Double safety!** — Rohit 😊

It's like a door with TWO locks. A thief might pick one — but picking two is much harder! — Monica 💡

🔐 How 2FA Works — Step by Step

Step 1 Enter your password → **Step 2** OTP sent to your phone → **Step 3** Enter the OTP code → **Result** You're in! Account safe!

Hacker? No OTP = Can't get in!



With 2FA ✅ Hacker blocked!

Without 2FA ✗ Hacker got in!

Q13. MCQ — circle one

Sana's Instagram was hacked. If she had 2FA — what would have happened?

- (A) Hacker would still get in — 2FA doesn't help
- (B) Hacker needs the OTP on Sana's phone — which they don't have. Blocked! ✅
- (C) 2FA is only for Gmail — not Instagram
- (D) The OTP would be sent to the hacker

Q14. Tick one

Vikram turned off 2FA because it was "annoying." Two weeks later, his Gmail was hacked. Do you think 10 seconds to type an OTP is worth it?

☑ Yes — 100% worth it ☑ 😅 I get why Vikram did it

Write one reason for your answer:

Pause & Think!

Think of 2FA like this: your password is the **key to the door**. But 2FA is a **second lock** that only your phone can open. Even if someone steals your key — they still can't open the second lock. **Turn on 2FA on every account you have!**

Pause & Think!

Sana now has a **strong new password** AND **2FA on her Instagram**. She told the group: *"I will never share my password again — not even with my best friend."* Monica reminded everyone: *"You taught me to think before I post — now I'm teaching you to think before you share."* Now it's your turn to show what you know!

Quick Revision

Q15. MCQ — circle one

Which is the STRONGEST password?

- (A) rohit2012
- (B) 123456789
- (C) Tiger$Rain#92!
- (D) password

Q16. MCQ — circle one

What does 2FA do?

- (A) Makes your password longer
- (B) Adds an OTP so even if someone has your password, they can't log in ✓
- (C) Stops you from forgetting your password
- (D) Lets your friend log in for you

Q17. Match — draw a line to Safe ✅ or Unsafe ⚠

`sana2010`	
`Tiger$Rain#92!`	
Sharing password with best friend	
Turning on 2FA for your account	
Sharing your OTP with someone	
✅ Safe / Strong	⚠ Unsafe / Weak

Myth vs Fact

MYTH

"My password has numbers — my birthday. So it's strong."

✅ FACT: Birthdays are easy to guess. Use **random** numbers instead.

MYTH

"I can share my password with my best friend — I trust them."

✅ FACT: Even trusted friends can **accidentally** leak it. A password is for ONE person only.

MYTH

"2FA is annoying. Not needed if I have a good password."

✅ FACT: Even strong passwords can be cracked. 2FA is your **second lock**.

Key Takeaways

Weak Passwords Are Easy to Hack
Never use your name, birthday, or "123456". These are the first things hackers try.

Strong Passwords Have 4 Rules
UPPER + lower + numbers + symbols. At least 8 characters. Random is better!

Never Share Your Password
Not with friends, classmates, or anyone online. A password is for ONE person — you.

2FA Is Your Second Lock
Even if someone knows your password — 2FA sends an OTP to YOUR phone. They can't get in!

Sana, Monica, Rohit & Aryan's Golden Rule

"A strong password is your first lock. 2FA is your second lock.
Mix letters + numbers + symbols · Make it long · Make it random
NEVER share it — not even with your best friend.
Two locks. One account. Zero hackers."