SAFE DEVICES, APPS & BROWSING · MODULE 1 · CHAPTER 1

Passwords, Account Security & The Master Key

Unique Passwords · Email Security · 2FA · Password Managers

55–65 min

GRADES 9–12

🔑 Key Terms — Your Security Dictionary

Password Reuse
Using the **same password** across multiple accounts — the #1 cause of large-scale account hacks.

Password Manager
An app that **stores & generates** unique passwords for every account — you only need to remember one master password.

Email as Master Key
Your email lets you **reset passwords** for all other accounts — if someone hacks your email, they can access everything.

Strong Password
12+ characters with **uppercase, lowercase, numbers & symbols** — hard for computers to guess.

Two-Factor Auth (2FA)
A second verification step (OTP/app code) that **blocks attackers** even if they know your password.

Domino Effect
One leaked password triggers a chain reaction — attacker enters email, resets UPI, drains account. All from one breach.

Honest Check — Before We Begin

Do You Agree or Disagree? Circle Your Honest Answer

No right or wrong here. Just be honest — this is to wake up your thinking before the chapter.

1. "It's fine to use the same password for multiple accounts as long as it's a strong one." — Agree / Disagree / Not Sure
2. "If I don't have any money in my account, no one would bother hacking me." — Agree / Disagree / Not Sure
3. "A password manager is risky — if that app gets hacked, everything is gone." — Agree / Disagree / Not Sure
4. "Enabling 2FA on Gmail is unnecessary effort — a strong password is enough." — Agree / Disagree / Not Sure

Come back to these at the end of the chapter. You might be surprised how many answers change.

Quick Read — This Actually Happened

Read Carefully — Then Answer Q1 in Your Notebook

Aryan, a Class 10 student from South Delhi, woke up one Tuesday to find **₹14,000 missing** from his family's PhonePe account. He had used the same password — `Delhi@2024` — for his Instagram, Gmail, and PhonePe. A minor data breach on a gaming website had leaked his email and password. The attacker logged into his Gmail, found PhonePe notifications there, reset the PhonePe password using Gmail's "Forgot Password," and drained the account — **all within 40 minutes.**

"I didn't know my Gmail was like a master key," said Aryan. *"Once they were in my email, they could reset everything else."* His sister Priya — sitting beside him — had been warning him about reused passwords for months. *"I never thought it would actually happen to me,"* Aryan added.

Q1.
List THREE decisions Aryan made that led to the ₹14,000 loss. For each one, write what he should have done instead.

Answer in your notebook

Q2.
The attacker never needed to guess Aryan's PhonePe password. Why not? Explain the exact steps the attacker took — using only what is described above.

Answer in your notebook

🔑 Why Your Email is a Master Key

"I need to show you something," Priya says, pulling up a diagram on her phone. "This is how one leaked password from a gaming site took down everything."

🔑 The Email Master Key — One Hack, Four Disasters

Every major account you have is linked to your email. Here is what the chain reaction looked like for Aryan:

Gaming site leaks password → Attacker logs into Gmail (same password) → Resets PhonePe via Gmail OTP → ₹14,000 transferred — 40 min

↑ This entire chain starts with ONE reused password on a small gaming website ↑

📍 Scene 1 — Aryan's Room, Delhi · Tuesday Morning · The Aftermath

ARYAN: Priya — ₹14,000 gone from PhonePe! I got an SMS. I didn't do anything! How is this even possible?!

PRIYA: Aryan bhai — check your Gmail. I bet there's a sign-in alert from an unknown location. Your PhonePe password was reset using your Gmail. That FreeFire gaming site was hacked last week — and your Gmail password was the same one.

ARYAN: There's an alert — "New sign-in from Karachi, 2:37 AM." That's not me. Priya — this is your fault, you should have made me change my passwords earlier!!

PRIYA: I told you six times. Stop arguing — first, change your Gmail password right now. Then we fix PhonePe. Then every other account. This is exactly what a password manager would have prevented. Let me show you.

Q3a.

Was Aryan's blame of Priya fair? Circle one and write one sentence explaining your choice.

Yes — it was fair | No — it wasn't fair | Partly fair

📓 Circle + one reason in notebook

Q3b. — Match the Cause to the Consequence

Draw a line to match each cause (left) with its consequence (right) in your notebook.

Cause	Consequence
Reused same password on gaming site & Gmail	Attacker reset PhonePe password using Gmail OTP
No 2FA on Gmail	Attacker logged into Gmail once gaming site was breached
Gmail linked to PhonePe for password reset	Attacker could not be blocked even after entering Gmail

📓 Draw matching lines in notebook

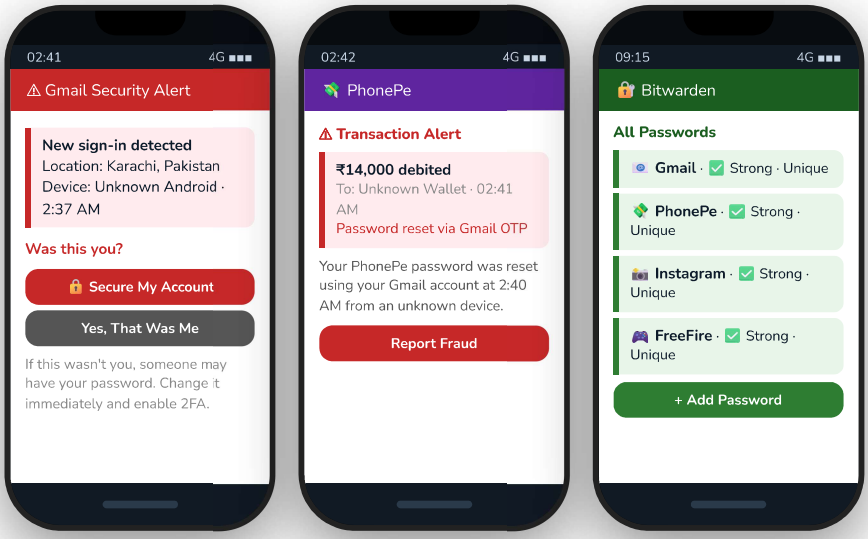
Q3c. — Odd One Out

Three of these four things make a password account MORE secure. One makes it LESS secure. Circle the odd one out.

Using a unique password per account | Enabling Google Authenticator 2FA | Reusing one strong password everywhere | Using Bitwarden to generate passwords

📓 Circle the odd one out in notebook + write one reason why

What These Screens Actually Looked Like on Aryan's Phone



Screen 1: Gmail Security Alert Aryan received this

Screen 2: PhonePe Transaction ₹14,000 gone

Screen 3: Bitwarden — after Priya helped fix everything

Password Strength Lab — Rate Aryan's Old Passwords

Priya pulls up Aryan's password history. "Let's go through these one by one."

#	Account	Password	Weak	Medium	Strong	What's the problem?
1	Gmail	`Delhi@2024`	☐	☐	☐	*Write in notebook...*
2	Instagram	`Delhi@2024`	☐	☐	☐	
3	PhonePe	`123456`	☐	☐	☐	
4	FreeFire	`aryan2007`	☐	☐	☐	
5	School Portal	`Xk#9mP@rT3!`	☐	☐	☐	

Password Strength Guide: Weak — common words, only numbers, under 8 chars | Medium — mix of letters & numbers but uses name/word | Strong — 12+ chars, uppercase + lowercase + numbers + symbols, no real words | **Never:** use your name, birth year, or reuse passwords

Q4.
Rewrite password #3 (123456) to make it Strong. Then explain in one sentence what makes your version stronger than the original.

Write new password + explanation in notebook

Q5.
Passwords 1 and 2 are identical — same password for Gmail and Instagram. Using the Master Key chain from Page 2, explain the specific danger of this combination.

Answer in your notebook

What Is a Password Manager? — Priya Explains

"Aryan, I'm going to solve your password problem permanently. One app. Free. Five minutes to set up. You will never have to remember more than one password again."

How a Password Manager Works — 5 Steps

1. You remember ONE Master Password
2. App stores UNIQUE passwords per site
3. Visit Gmail / PhonePe / any site
4. App auto-fills correct password
5. One site hacked? Others stay safe

Free options in India: Bitwarden (free) | Google Password Manager | Samsung Pass

WITHOUT a Password Manager

- ❌ Same password reused across 5+ accounts
- ❌ Password written in notes app or on paper
- ❌ One breach = ALL accounts compromised
- ❌ Uses guessable patterns — name + year
- ❌ Can't track which accounts are at risk

WITH a Password Manager

- ✅ Every account has a unique strong password
- ✅ Passwords encrypted — not stored as plain text
- ✅ One site hacked? All others stay safe
- ✅ Generates 20-char random passwords instantly
- ✅ Alerts you if password appears in a breach

Activity — Password Audit — Help Priya Fix Aryan's Accounts

Fill in the Missing Columns in Your Notebook

After the hack, Priya lists all of Aryan's accounts. Draw this table in your notebook and complete it.

Account	Current Password	Same as another? Y/N	Risk Level	Action needed
Gmail (Recovery email)	`Delhi@2024`	Y	CRITICAL	Change FIRST — it's the master key!
PhonePe / UPI	`Delhi@2024`	☐	☐	*Write in notebook...*
Instagram	`Delhi@2024`	☐	☐	
Gaming site (FreeFire)	`aryan2007`	☐	☐	
School Portal (CBSE)	`Aryan_Class10`	☐	☐	

Draw and fill this table in your notebook

Q6.
Why should Aryan change his Gmail password FIRST before changing any other account? Explain in 2 sentences using the Master Key idea.

Answer in your notebook

Q7.
Aryan says: "A password manager is risky — if it gets hacked, everything is gone!" Is this concern valid? How do password managers actually protect against this? Write 2–3 sentences.

Answer in your notebook

🔒 Securing Your Gmail — Priya's 5-Step Protection Plan

"Changing your password is step one, Aryan. But there are four more things you have to do right now."

🛡️ Priya's Gmail Security Plan — Do These in Order

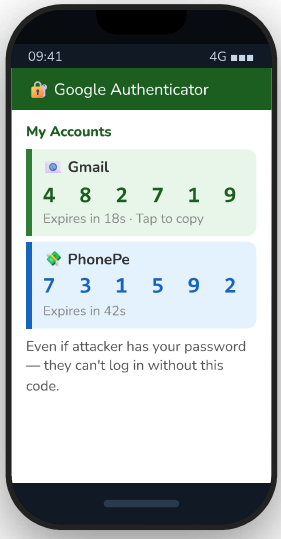
1 **Use a unique passphrase for Gmail ONLY**
Never use this password on any other website. Create a passphrase: 4 unrelated words + numbers + symbols. Example: `Blue!Rain#Train7Cup` — easy to remember, impossible to guess.

2 **Enable 2FA immediately using an Authenticator App**
Go to: myaccount.google.com → Security → 2-Step Verification. Use Google Authenticator (not just SMS — SMS can be intercepted via SIM swap fraud).

3 **Add a Recovery Phone Number & Backup Email**
Settings → Security → Recovery. Use a parent's trusted phone number. This lets you regain access if you're ever locked out.

4 **Review Third-Party App Permissions every 3 months**
myaccount.google.com → Security → Third-party apps. Remove any apps you don't recognise or no longer use — they may have Gmail access.

5 **Set Up Security Alerts on a trusted device**
If someone logs into your account from a new device, Google sends an alert instantly. Act immediately — change password and review all linked accounts.



Google Authenticator generates 6-digit codes that expire every 30s

🔒 How 2FA Blocks Attackers

Even if an attacker steals your Gmail password in a data breach — to log in they also need the 6-digit code from your phone. That code changes every 30 seconds. Without your physical phone, they are completely locked out. **Password + 2FA together = two separate locks on the same door.**

⚠ Why NOT SMS-based 2FA?

SMS OTPs can be intercepted through **SIM swap fraud** — attackers contact your telecom provider pretending to be you, get your SIM transferred to their device, and receive your OTPs. Authenticator apps are not vulnerable to this. Use an app, not SMS.

Q8.
Aryan argues: "A strong passphrase for Gmail is enough — I don't need 2FA as well." Priya disagrees. Using the 2FA explanation above, write why Priya is correct in 2–3 sentences.

Answer in your notebook

Q9.
Design a passphrase for Aryan's Gmail account — 4 unrelated words + numbers + symbols. Write it in your notebook. Then explain in one sentence why it is stronger than his old password `Delhi@2024` .

Answer in your notebook

Activity 1 – Situation Analysis

⚖️ What Would You Do? – Real Scenarios from India

For each situation — write in your notebook: (a) Safe ✅ or Risky ⚠️ · (b) What should the person do instead?

Situation 1 – Priya's Call

Priya gets a call from someone claiming to be "Google Support." They say her account has been compromised and ask for the OTP that just arrived on her phone to "verify her identity."

Situation 2 – Aryan's Shortcut

Aryan sets his Bitwarden Master Password as `aryan123`. He thinks: "It's just one password to remember, and I know it well." He doesn't want to forget a complicated one.

Situation 3 – Naman's Gmail

Naman enables 2FA on Gmail using SMS OTP because "it's simpler than downloading another app." His friend mentions SIM swap fraud. Naman replies: "That only happens to celebrities."

Situation 4 – Kavya's Device

Kavya logs into her Gmail on a school computer to access her notes. After finishing, she closes the browser tab but doesn't sign out of her Google account. She is in a hurry for the next class.

📓 For each: Safe ✅ or Risky ⚠️ · What they should do instead

Activity 2 – True, False, or Fix It!

✏️ Write T / F / P – Then Correct Every F or P

Write T (True), F (False), or P (Partially True). For every F or P — rewrite the corrected version of the statement in your notebook.

1. A strong password alone is enough to protect your Gmail account completely.
2. If a gaming website is hacked, your Gmail could also be at risk if you used the same password.
3. Using SMS for 2FA is as secure as using an Authenticator App.
4. A password manager stores all your passwords — and if it is hacked, all your passwords are immediately exposed.
5. Aryan's PhonePe account could only be accessed if the attacker also knew his PhonePe password.
6. Your email account is the most important account to protect because it can be used to reset all other passwords.

📓 Write T / F / P and corrected statements in your notebook

❌ MYTH — what many students believe	✅ FACT — what actually protects you
Myth 1 **"I have nothing important on my accounts — no one would bother hacking me."**	**Reality** Attackers don't target *you* — they run automated scripts targeting thousands of accounts at once. Your Gmail gives access to your family's UPI, your school portal, and your personal messages. Aryan thought the same thing — until ₹14,000 vanished.
Myth 2 **"A password manager is dangerous — one app holds all my passwords. If it gets hacked, I lose everything."**	**Reality** Password managers encrypt your vault with your Master Password — even if the company is hacked, they only get scrambled data they can't read. The alternative — reusing one password everywhere — means a single small breach unlocks every account you own.
Myth 3 **"2FA is too much effort — I'll have to enter an extra code every time I log in. It's not worth it."**	**Reality** Most devices remember your login — you only enter the 2FA code on a new or untrusted device, perhaps 3–4 times a year. In exchange, even if an attacker steals your password, they still cannot log in without your phone. 5 seconds of effort, near-total protection.

Think & Connect

Your Doubts Are Valid – Let's Name Them Honestly

These are the most common worries students have about cybersecurity. Read each one and notice if you recognise yourself.

😰 **"What if I forget my Master Password?"**

😟 **"Setting up 2FA feels complicated and scary."**

Set it up as a passphrase you'll remember. Write it once on paper, store it safely at home — not digitally.

It takes 4 minutes. myaccount.google.com → Security → 2-Step Verification. Priya helped Aryan in one lunch break.

😬 **"I'm worried I might already be hacked."**

Go to haveibeenpwned.com and type your email. It shows if you've appeared in a known breach. Knowing is always better.

😳 **"I feel embarrassed — I've been doing this wrong."**

So had Aryan. You're learning this now, before something serious happens. Starting from this chapter is enough.

Q10a.

Which of the four fears above do you relate to most — or have felt before? Describe it honestly in 2 sentences. You don't have to share this with anyone.

📓 Notebook

Q10b.

What is ONE concrete thing you will change about your password habits this week? Name it specifically — not "I'll be more careful."

📓 Notebook

Story — Aryan Becomes the Expert

Scene 2 — School Assembly Hall · One Month Later · Aryan Presents

I lost ₹14,000 because I used one password everywhere. My Gmail was my master key — and I left it unlocked for anyone to use. Now I use Bitwarden. Every account has a unique password. My Gmail has a passphrase and Google Authenticator 2FA. No more shortcuts.

ARYAN

PRIYA

And even if a gaming site leaks your password tomorrow — your Gmail stays safe because it has a DIFFERENT password. The domino chain is broken. That's what one password manager does: it turns a chain of dominoes into independent bricks.

Activity 3 — Quick Check — Circle in Notebook

MCQ — One Correct Answer for Each

Q11a.
Which action would have PREVENTED Aryan's ₹14,000 loss entirely?

- ○ Using a stronger password on the gaming site
- ○ Using a unique password for Gmail not used elsewhere
- ○ Deleting his PhonePe account
- ○ Not playing online games

Circle answer in notebook

Q11b.
Why is Google Authenticator better than SMS for 2FA?

- ○ It generates longer codes that are harder to guess
- ○ SMS OTPs can be intercepted via SIM swap fraud; the app cannot
- ○ It works without internet, which is more convenient
- ○ Google Authenticator stores your passwords as well

Circle answer in notebook

Going Deeper — Think Harder

The Bigger Questions

Q12a.
The attack on Aryan originated from a small gaming website breach — not from Gmail or PhonePe. What does this tell you about the weakest link in your security chain? Which of your accounts — that you consider unimportant — might be your real weak point?

Answer in your notebook

Q12b.
Design a "Personal Account Security Policy" for a Class 9–12 student — at least 5 specific rules covering passwords, email, and what to do if hacked. Write it as clear rules, not general advice.

Answer in your notebook

Aryan & Priya's Security Rules — The 6-Point Plan

1. **Never reuse passwords across accounts**
   Every account — no matter how small — must have its own unique password. The gaming site is the entry point to your bank.
2. **Protect your Gmail above all other accounts**
   Your email is the master key. It must have a unique passphrase + Google Authenticator 2FA + a trusted recovery number.
3. **Use a password manager (Bitwarden — free)**
   You only need to remember one strong Master Password. The app handles everything else. No more compromises for convenience.
4. **Use an Authenticator App — not SMS — for 2FA**
   Google Authenticator or Authy cannot be intercepted by SIM swap fraud. SMS can. The extra 2 seconds to open the app is worth it.
5. **Always sign out on shared devices**
   School computers, cyber cafés, a friend's laptop — always sign out of Gmail and any other accounts. Closing the tab is not the same as signing out.
6. **Never share an OTP with anyone — ever**
   No bank, Google, or telecom company will ever ask you for your OTP. Anyone who does is an attacker. Hang up immediately.

Return to Page 1 — Your Final Answers

Have Your Answers Changed? Compare Then vs Now.

Go back to the 4 statements on Page 1. In your notebook write: Statement number | Original answer | New answer | What changed your thinking?

Q13.
Which of the 4 statements surprised you most — where your thinking changed the most? In 2–3 sentences, explain what you now understand that you didn't at the start.

Answer in your notebook

Key Takeaways — What You Learned Today

- **Never Reuse Passwords**
  One leaked password from any website can expose all your accounts. Every account needs its own unique password — no exceptions.
- **Gmail = Master Key**
  Your email controls password resets for everything — PhonePe, Instagram, school portals. Protect it first, with a passphrase + 2FA.
- **Use a Password Manager**
  Bitwarden is free. It handles unique, strong passwords for every account. You need to remember exactly one Master Password.
- **Use Authenticator App 2FA**
  Google Authenticator blocks attackers even when they have your password. SMS 2FA is vulnerable to SIM swap. Use the app.

Aryan & Priya's Golden Rule for Chapter 1

"Unique password for every account. Passphrase + Authenticator App 2FA for Gmail. Password manager for everything else."

Safe Devices, Apps & Browsing · Module 1 · Chapter 1 → Next: Chapter 2 — Advanced Privacy & Tracking