SAFE DEVICES, APPS & BROWSING · MODULE 2 · CHAPTER 5

Cloud vs Local Storage: Backup & Recovery

Cloud · Local · Access · Security · Reliability · Backup Strategy

55–65 min

GRADES 9–12

The Story So Far — Module 2 Recap

Ch 1: Rohan's laptop hit by ransomware — files encrypted, ₹8,000 demanded. Aryan said: "A backup would have made this powerless." **Ch 2:** Zara's laptop cryptojacked from a piracy site. **Ch 3:** Meera's laptop remotely accessed — skipped updates were the open door. **Ch 4:** Naman nearly made a UPI payment on an Evil Twin network. In every chapter, one word kept coming up: **backup.** Now in Chapter 5, we finally answer — what exactly is a backup, where should you keep it, and how do you design one that actually protects you?

MODULE 2 · Safe Devices, Apps & Browsing

Chapter 5 — Cloud vs Local Storage

Before We Begin — What Do YOU Actually Do With Your Data?

Be honest — tick what you *actually* do. We'll come back to this at the end of the chapter.

When it comes to saving and backing up my files, I...	✅ I do this	❌ I don't
...regularly save school notes and projects somewhere other than just my device	☐	☐
...know the difference between saving a file and backing it up	☐	☐
...use a cloud service (Google Drive, iCloud, OneDrive) for any of my files	☐	☐
...have ever lost a file, photo, or project because my device crashed or was reset	☐	☐
...know how much storage my phone or laptop has and how much is used	☐	☐
...could recover my school work today if my phone was stolen or destroyed	☐	☐

✅ I do this: ____ out of 6 ❌ I don't: ____ out of 6

In your notebook: If your phone was stolen right now, what would you lose permanently? List 3 things. We'll revisit this at the end.

Key Terms — Words You Will Need Today

Cloud Storage
Files stored on remote servers maintained by a company (Google, Apple, Microsoft). Accessible from any device with internet.

Local Storage
Files stored physically on your device or an external drive — hard disk, USB, SD card. No internet needed to access.

Backup
A **separate copy** of your data stored in a different location. If the original is lost or damaged, the backup lets you recover it.

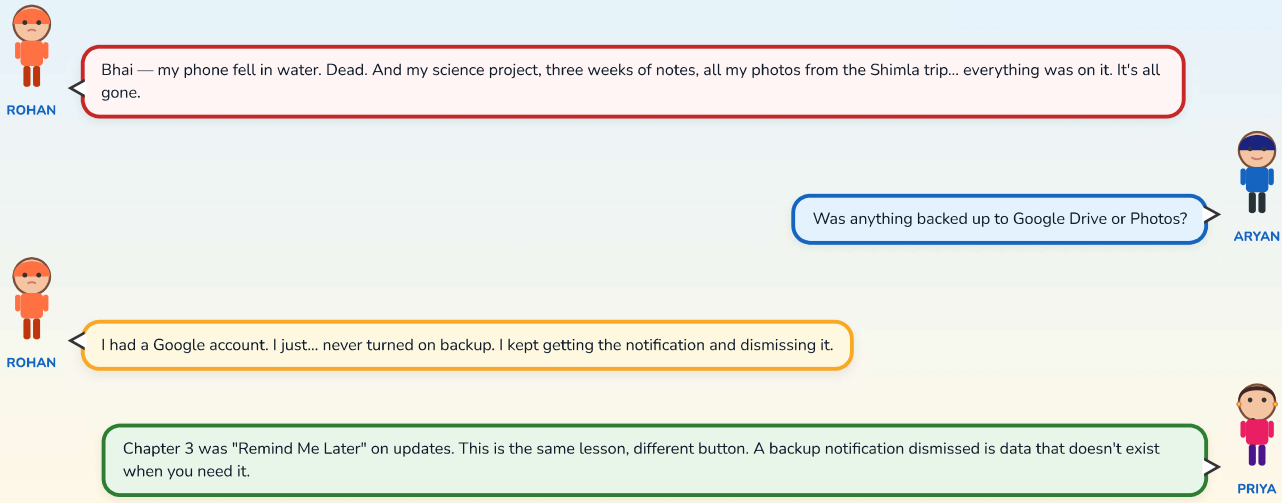
Recovery
The process of restoring lost, damaged, or encrypted data from a backup. Only possible if a backup exists.

Sync
Automatic updating of files across devices or to the cloud. Syncing keeps files current — but **is not the same as a backup.**

3-2-1 Rule
3 copies of data · **2** different storage types · **1** copy offsite (cloud or external drive elsewhere). The gold standard of backup.

🎭 Story — "It Was All on My Phone" — Rohan's Second Crisis

📍 Scene 1 — Aryan's House · Three Weeks After the Malware Incident · Rohan Visits Again



☁️ Cloud vs 💾 Local — What's the Difference?

☁️ Cloud Storage

Examples: Google Drive, iCloud, OneDrive, Dropbox

- ✅ Access from **any device**, anywhere with internet
- ✅ Auto-sync — files update automatically across devices
- ✅ Safe from physical damage (fire, flood, theft of device)
- ✅ Easy sharing and collaboration
- ❌ Requires internet to access
- ❌ Company can be hacked or go down — your data is on their server
- ❌ Free storage limits (15 GB Google, 5 GB iCloud) — then you pay
- ⚠️ Privacy concern — provider can theoretically access your files

💾 Local Storage

Examples: Hard drive, USB drive, SD card, laptop SSD

- ✅ Works completely **offline** — no internet needed
- ✅ Full control — no third party can access your data
- ✅ Fast access — no upload/download delays
- ✅ One-time cost — buy a drive, no monthly fees
- ❌ Lost or damaged with the device in a fire, flood, or theft
- ❌ No auto-sync — you must manually update your backup
- ❌ Hardware failure — drives fail without warning
- ⚠️ Ransomware can encrypt local backups if the drive is connected

Activity 1

📖 Story & Comparison Analysis

Q1a.
Priya says: "Chapter 3 was 'Remind Me Later' on updates. This is the same lesson, different button." What does she mean? How are skipping updates and skipping backups similar in the risks they create?

Write in your notebook — 2–3 sentences

Q1b.
Rohan lost data when his phone fell in water. Would cloud storage have saved his files? Would a local USB backup? Explain what each would and would not have protected.

Write in your notebook

📊 Side-by-Side Comparison — Cloud vs Local on Three Dimensions

"Let's be precise," says Naman. "It's not just 'one is better.' It depends on what you're comparing — access, security, or reliability."

Dimension	☁️ Cloud Storage	💾 Local Storage	🏆 Verdict
Access	Any device, any location — as long as you have internet. Perfect for students working across phone, tablet, school PC.	Only from the device or drive you have with you. You must physically carry the storage.	☁️ **Cloud wins — unless you have no internet**
Security	Encrypted in transit and at rest. But: company data breach risk, account hacking risk, government/legal access possible. Weak password = your whole cloud exposed.	No internet = no remote attack. But: ransomware can reach connected drives. Physical theft exposes everything if unencrypted.	⚖️ **Tie — different threats, different contexts**
Reliability	Very high uptime (Google Drive 99.9%). But service outages happen. Company can change policies, close free tiers, or shut down.	Drives fail without warning — average HDD lifespan 3–5 years. Water, heat, and drops destroy local storage instantly.	☁️ **Cloud wins — physical drives are fragile**
Cost	Free tier (15 GB Google, 5 GB iCloud). Beyond free: ₹130–200/month for 100 GB+.	One-time cost: 1 TB external drive ~₹3,500–5,000. No recurring fees.	💾 **Local wins for large storage long-term**
Ransomware protection	Cloud often keeps version history — can restore files from before encryption. Google Drive keeps 30-day history.	If the drive is connected when ransomware hits, it gets encrypted too. An **offline** or disconnected drive is safe.	☁️ **Cloud wins — version history is key**
Privacy	Provider can access files (terms of service). Government can request data. Your files are on someone else's server.	Complete privacy — only you can access. No third party involved.	💾 **Local wins — full control**

💡 **Pause & Think!**

Notice the Ransomware row — Google Drive's version history is one of the most powerful protections against ransomware for individual users. When Rohan's laptop was encrypted in Chapter 1, if his files had been in Google Drive, he could have simply restored the previous day's version. **No ransom needed. No data lost.** This is exactly why Aryan said "a backup would have made this powerless" — and specifically why cloud backup with version history beats a local drive that's always connected.

Q2a.

Look at the Security row. The table says it's a "tie." But the *types* of threats are completely different. Describe one scenario where cloud storage is MORE at risk than local — and one where local is MORE at risk than cloud.

📓 *Write in your notebook*

Q2b.

A student argues: "I don't need a backup — I already save everything on Google Drive." Is this enough? What is the difference between saving on Google Drive and having a proper backup strategy? Use the table to support your answer.

📓 *Write in your notebook*

📐 The 3-2-1 Backup Rule — The Gold Standard

"There's a rule professionals use," says Aryan. "It's called 3-2-1. Once you understand it, you'll never think about backup the same way."

📐 The 3-2-1 Rule

3
Copies of your data
The original + 2 backups. If one is lost, you still have two more. Single copies are a single point of failure.

2
Different storage types
E.g. one on your laptop + one on a USB drive. Different media fails in different ways — don't put all copies on the same type.

1
Copy offsite / in the cloud
If your house floods or your room is robbed, on-site backups are gone too. Cloud or an external drive at a different location survives anything local.

💡 For most students: **Original on device** + **External USB drive (home)** + **Google Drive (cloud)** = perfect 3-2-1 implementation — free and simple.

🎯 Applying 3-2-1 — What Rohan Should Have Done

Copy 1

Original — Phone Storage
Science project, notes, photos — stored on the phone as you work. This is NOT a backup — it's the original.

❌ Rohan only had this

Copy 2

USB Drive — Home
Weekly copy of project files to a USB drive kept at home. Survives phone loss — fails in fire/theft of home.

✅ Should have had this

Copy 3

Google Drive — Cloud
Auto-backup to Google Photos + Drive. Survives any physical disaster. Free 15 GB — more than enough for school work.

✅ Should have had this

Activity 2

📐 Apply the 3-2-1 Rule

Q3a.
A student has all their files only on Google Drive. Do they satisfy the 3-2-1 rule? Identify which numbers (3, 2, 1) are missing and explain what additional steps they need to take.

Write in your notebook

Q3b.
Ransomware hits Rohan's laptop and encrypts everything — including the USB drive plugged in at the time. Under 3-2-1, is his data safe or lost? What rule does this situation highlight about how backups must be stored?

Write in your notebook

Q3c.
Choose the correct option — Which of the following best satisfies the 3-2-1 rule for a school student?

- ○ Files on laptop + one copy on the same laptop in a different folder
- ○ Files on laptop + Google Drive backup + USB drive kept at a friend's home
- ○ Two USB drives kept in the same school bag
- ○ Files only on iCloud — it has multiple servers so it counts as multiple copies

🎭 Story Continues — Scene 2 · Kavya's Laptop Disaster & the Version History Rescue

📍 Scene 2 — Same Day · Kavya Arrives with Her Laptop

KAVYA: I accidentally deleted my entire History essay — three days of work. It was in Google Docs. Can I get it back?

PRIYA: Google Docs keeps version history — every change, automatically. File → Version History → See version history. Find the version before you deleted it. Restore. Done.

KAVYA: It's all there. Three days of work — completely recovered in 30 seconds. This is the first time I've been grateful for cloud storage.

📊 Let's Assume — What the Data Might Show

Illustrative figures — not attributed to any specific source.

~30%
of students may have permanently lost school work due to device failure, theft, or accidental deletion

1 in 2
phone users who experienced ransomware or device loss had no backup of any kind at the time

Google Drive
is the most used cloud storage by Indian students — but less than half enable auto-backup for photos and files

Only 9%
of ransomware victims who paid the ransom actually recovered all their files — a backup costs nothing and recovers everything

🔍 Go & Find — Explore Beyond This Page

The figures above are illustrative. Your task: **go search, read, and bring back something real.**

🔎 Search & Read

Search: *"data loss stories India students"* or *"phone lost all data no backup"*. Find one real incident. Write: what was lost, could a backup have helped, and how?

📊 Find the Real Data

Search: *"data backup statistics India"* or *"NASSCOM cloud storage report"*. Find one real statistic about backup habits — write the source and what it means for students.

🛠 Try It Yourself

At home, open Google Drive or iCloud on your phone. Is backup turned on? How much storage is used vs free? Write what you found — and one thing you will change.

📓 **In your notebook, write:** What you found (article or stat) · The key fact · One sentence on how it connects to Rohan's or Kavya's story in this chapter.

🛠️ Design Your Own Backup Strategy

"A backup strategy only works if you actually design it for your life," says Aryan. "Not for a corporation — for a Class 9–12 student in India."

Activity 3 — Design Challenge

🎨 Build YOUR Personal Backup Plan

Using what you've learned, design a backup strategy that fits your actual life. Answer each section below in your notebook.

📁 Step 1 — Identify What Matters

List the data you cannot afford to lose. Think about:

- 📚 School notes, assignments, projects
- 📸 Photos and videos you care about
- 🎨 Creative work — art, music, writing
- 📲 Contacts, messages, WhatsApp media

📓 Write your own list in your notebook — add anything specific to you.

☁️ Step 2 — Choose Your Cloud Option

Which cloud service will you use, and what will you back up there?

Service	Free storage	Best for
Google Drive	15 GB	Docs, school files, Android backup
Google Photos	15 GB shared	Photos & videos
iCloud	5 GB	iPhone/iPad backup
OneDrive	5 GB	Windows files

📓 Write: Which service, what you'll back up, and how often (daily auto-sync / weekly manual).

💾 Step 3 — Choose Your Local Option

What physical backup will you use — and where will you keep it?

- 🔌 USB drive — cheap, portable (~₹300 for 32 GB)
- 📦 External hard drive — large (~₹3,500 for 1 TB)
- 💻 Second device — old phone or tablet as backup store

⚠ **Remember: disconnect the drive after backup — or ransomware will encrypt it too.**

📓 Write: What you'll use, where you'll keep it, how often you'll update it.

📅 Step 4 — Set a Backup Schedule

A backup strategy only works if it's regular. Design a schedule that's realistic for you:

Frequency	What to back up	Where
Daily (auto)	Photos, new docs	Cloud (auto-sync)
Weekly (manual)	School project folder	USB drive
Before exams	Everything important	Both cloud + local

📓 Write your own schedule — be realistic about what you will actually do.

📋 Step 5 — Your Final Backup Strategy Statement

In your notebook, write a 3–4 sentence summary of your personal backup strategy using this structure:

"My most important data is _____. I will back it up to _____ (cloud) and _____ (local). I will update my backup _____. If my device is lost or damaged today, I will be able to recover _____ within _____ minutes."

⚖️ Read the Situations — What Would You Do?

Read each situation. Write in your notebook: (a) What went wrong with their backup strategy? (b) How could it have been avoided? (c) What should they do now?

Situation 1 — Meera, Exam Week

Let's assume Meera's laptop crashes two days before her board practical exam. She had saved all her practicals in a folder called "CBSE_2026" on her Desktop. She has no cloud backup. Her USB drive has a copy — but she updated it 6 weeks ago. She has 3 new practicals that don't exist anywhere else.

Situation 2 — Naman, Ransomware Hit

Let's assume Naman's laptop gets ransomware. His external hard drive was plugged in at the time — it's also encrypted. He has Google Drive — but he only backs up manually, and his last backup was 10 days ago. He's lost 10 days of school notes and two project drafts.

Situation 3 — Kavya, Theft

Let's assume Kavya's bag is stolen at a railway station. Her laptop, USB drive, and phone were all in the bag. She had Google Photos auto-backup on her phone and kept a copy of her most important documents in Google Drive. Her USB had a full backup made 3 days ago.

Situation 4 — Aryan, Cloud Outage

Let's assume Google Drive is down for 6 hours on the morning Aryan needs to submit his college application. All his documents are only in Google Drive — he never kept local copies. He has the correct files but cannot access them. The submission deadline passes.

Activity 4 — Quick Questions

✏️ Choose the Correct Option

Q4a.
What is the key difference between "syncing" a file to Google Drive and "backing it up"?

- ◯ Syncing is faster; backup is slower
- ◯ Syncing keeps one up-to-date copy; a backup keeps a separate copy that is protected from changes or deletion
- ◯ Backup works offline; syncing requires Wi-Fi
- ◯ There is no difference — they are the same thing

Q4b.
Why should you disconnect an external drive after completing a backup?

- ◯ To save electricity
- ◯ So ransomware cannot reach and encrypt the backup drive if your main device is infected
- ◯ Because drives overheat when left connected
- ◯ To prevent files from syncing automatically

💭 Pause & Reflect

The "I'll Do It Later" Problem

Backup is uniquely easy to postpone — because the consequence of not doing it is invisible until disaster strikes. Rohan dismissed a Google backup notification. Meera clicked "Remind Me Later" on updates. Naman's drive was connected when it shouldn't have been. None of them felt any danger before the moment of loss. **The cost of a backup is 5 minutes. The cost of not having one can be weeks of work.**

In your notebook: What is one thing — right now — you could lose if your device failed today? And what will you actually do about it this week?

Return to Page 1 — What Has Changed?

Revisit Your Opening Tick Table

Go back to your tick table on Page 1. Look at your ❌ column — and look at your notebook answer about what you would lose if your phone was stolen.

Q5.
For each ❌ you ticked on Page 1: (a) What specific data could you lose because of this gap? (b) Which part of your backup plan (from Activity 3) fixes it? (c) When will you do it — today or this weekend?

Be honest — compare your opening answers to what you now know

Epilogue — One Week Later

Rohan
"I turned on Google Photos backup immediately. And I bought a 32 GB USB for ₹280. Cheap insurance."

Aryan
"I already had cloud backup. But this chapter reminded me my USB drive was always plugged in. Disconnected it after backups now."

Kavya
"Version history saved my essay. Now I keep everything in Google Docs and check version history is on. And I have a USB at home."

Naman
"10 days of notes lost. Lesson learned. Auto-sync on Drive, USB unplugged after each weekly backup. Never again."

Key Takeaways

Cloud = Access + Auto-sync + Ransomware Recovery
Cloud storage is accessible from anywhere and version history makes it ransomware-resistant. But it needs internet and has free storage limits.

Local = Privacy + Offline Access + One-Time Cost
External drives are private, work offline, and have no recurring fees. But they fail physically and must be disconnected after backup to survive ransomware.

Use Both — The 3-2-1 Rule
3 copies · 2 storage types · 1 offsite. For students: device + USB drive at home + Google Drive. All three together protect against every failure mode.

Sync Is Not a Backup
Syncing to Google Drive keeps one copy up to date — but if you delete or overwrite a file, the sync reflects that change. Version history is your real safety net.

Backup Must Be Regular and Tested
A backup made 6 weeks ago protects 6-week-old data. Schedule regular backups — and occasionally test recovery to confirm the backup actually works.

5 Minutes Now vs Weeks of Work Lost
The cost of setting up a backup is one afternoon. The cost of not having one can be an entire project, a year of photos, or irreplaceable work — gone permanently.

Aryan, Priya, Kavya, Naman & Rohan's Rule for Chapter 5

"A file that exists in only one place doesn't really exist. Back up before you need to — not after you've lost something. Cloud for access, local for control, both for real protection."

Safe Devices, Apps & Browsing · Module 2 · Chapter 5 → Module 2 Complete