



Personal Device Hygiene Checklist

Updates · Security Scans · App Permissions · Backups · Safe Habits

55–65
minGRADES
9–12

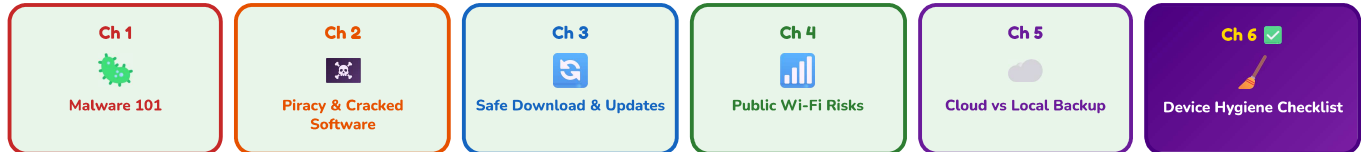
The Full Module 2 Journey – What You've Learned So Far

Ch 1: Rohan's laptop infected by a Trojan, worm & ransomware — from one "free game" download. **Ch 2:** Zara's laptop cryptojacked from a piracy site. **Ch 3:** Meera's laptop remotely accessed through an unpatched Windows vulnerability. **Ch 4:** Naman nearly leaked his UPI credentials on an Evil Twin network. **Ch 5:** Rohan lost all his phone data — no backup enabled. In every chapter, a preventable problem. In every chapter, a habit that could have stopped it. **Chapter 6 brings it all together** — into one personalised device hygiene checklist that works for your device, your life, and your risks.

MODULE 2 · Safe Devices, Apps & Browsing

Chapter 6 – Personal Device Hygiene

Module 2 – Your Journey So Far



Warm-Up – Rate Your Device Right Now

How Healthy Is Your Device? – Honest Self-Audit

Rate each area honestly: Done | Partial / Not Sure | Not done

Device health area	<input checked="" type="checkbox"/> Done	<input type="checkbox"/> Partial	<input type="checkbox"/> Not done
My OS and apps are fully updated	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I have antivirus installed and it was recently updated	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I have reviewed app permissions in the last month	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
My important files are backed up (cloud + local)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I do not connect to unknown public Wi-Fi for sensitive tasks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
I only download apps from official stores (Play Store / App Store)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

 Done: — Partial: — Not done: —

In your notebook: which **X** creates the biggest risk for your device specifically — and why? We'll revisit this at the end.

Personal Device Hygiene Checklist

 Story – "The Device Audit" – The Group Checks Each Other's Phones

 Scene 1 – Aryan's Study Group · End of Module · Everyone Has Their Devices Out


ARYAN

Six chapters. Six devices. Six problems that could have been prevented. Let's each check our own device — right now — and see if we'd actually pass our own checklist.



NAMAN

I just checked. Two apps on my phone still have "always on" microphone access. I never changed that after Chapter 2.



KAVYA

My last Windows update was last week — I'm clean there. But I haven't run a full antivirus scan in two months. That's a gap I didn't even notice until now.



MEERA

My Wi-Fi is set to auto-connect. I have 7 saved public networks — including three from malls. I didn't realise that was even a setting I should change.



PRIYA

That's exactly the point. Device hygiene isn't a one-time fix. It's a regular habit — like brushing your teeth. You don't do it once and declare yourself done.

 What Is Device Hygiene – and Why Does It Matter?

Device hygiene is the set of regular practices that keep your device secure, clean, and protected — the digital equivalent of washing your hands, maintaining your health, and not leaving doors unlocked. Just like physical hygiene prevents illness, device hygiene prevents infections — malware, unauthorised access, and data loss.

**Updates**

Patch known holes before attackers find them

**Security Scans**

Detect threats that slipped in despite precautions

**App Permissions**

Limit what apps can access — only what they need

**Backups**


Ensure data survives any failure or attack

**Safe Connectivity**

Manage Wi-Fi, Bluetooth, and network habits


Activity 1
 Story Analysis – Each Character Has a Gap
Q1a.

Each character in the story reveals a specific device hygiene gap. Match each character to their gap, the chapter it was first covered, and which hygiene pillar (Updates / Scans / Permissions / Backups / Connectivity) it belongs to.

 Draw a table in your notebook: Character | Gap | Chapter | Pillar

Q1b.

Priya says "Device hygiene isn't a one-time fix — it's a regular habit, like brushing your teeth." What does this analogy tell us about how we should think about device security? Why does doing it once and forgetting it not work?

 Write in your notebook — 2–3 sentences

Personal Device Hygiene Checklist

✓ The Master Device Hygiene Checklist – Organised by Pillar

Aryan has compiled everything from Module 2 into one master checklist — organised by the five pillars and colour-coded by frequency. Use this as your reference.



Updates & Patching

→ Ch 3

- | | | | |
|--------------------------|---|---|--------|
| <input type="checkbox"/> | OS and system updates installed
Check Settings → Windows Update / Software Update (iOS) | Patches known vulnerabilities attackers exploit | Weekly |
| <input type="checkbox"/> | All apps updated to latest version
Play Store / App Store → Updates pending: 0 | Old app versions have known security holes | Weekly |
| <input type="checkbox"/> | Automatic updates enabled
Settings → turn on auto-update for both OS and apps | Removes human delay from the patch cycle | Once |
| <input type="checkbox"/> | Browser is up to date
Chrome/Firefox/Safari — check for updates in settings | Browsers are frequent targets for exploits | Weekly |



Security Scans & Antivirus

→ Ch 1

- | | | | |
|--------------------------|--|--|---------|
| <input type="checkbox"/> | Antivirus installed and updated
Windows Defender (built-in), Avast, or AVG — check last update date | Old antivirus can't detect new malware | Weekly |
| <input type="checkbox"/> | Full device scan run
Open antivirus → Run Full Scan (not Quick Scan) | Catches threats that slipped through earlier | Monthly |
| <input type="checkbox"/> | No unknown processes running
Task Manager (Ctrl+Shift+Esc) → check for unfamiliar background processes | Malware often runs hidden in background | Monthly |
| <input type="checkbox"/> | Browser extensions reviewed
Check browser extensions — remove any you don't recognise or no longer use | Malicious extensions steal data silently | Monthly |



App Permissions & Privacy

→ Ch 2

- | | | | |
|--------------------------|---|---|---------|
| <input type="checkbox"/> | Microphone permissions reviewed
Settings → Privacy → Microphone — remove "always on" from any app that doesn't need it | Prevents silent audio surveillance | Monthly |
| <input type="checkbox"/> | Location permissions reviewed
Settings → Privacy → Location — switch non-essential apps to "Only while using" | Stops constant location tracking | Monthly |
| <input type="checkbox"/> | Camera permissions reviewed
Remove camera access from apps that have no reason to use it (e.g. weather apps, calculators) | Camera access = potential remote spying | Monthly |
| <input type="checkbox"/> | Unused apps deleted
Remove apps you haven't used in 3+ months — they still hold permissions and may not be updated | Unused apps are forgotten attack surfaces | Monthly |



Backups & Data Protection

→ Ch 5

- | | | | |
|--------------------------|---|---|---------|
| <input type="checkbox"/> | Cloud backup enabled and current
Google Drive / iCloud / OneDrive — check last sync date and available storage | Protects against device loss and ransomware | Weekly |
| <input type="checkbox"/> | Local backup completed and disconnected
Copy important files to USB / external drive → eject and store separately | Disconnected drive survives ransomware | Weekly |
| <input type="checkbox"/> | Backup recovery tested
Open one backed-up file from your backup source — confirm it actually opens | Untested backups sometimes fail silently | Monthly |



Safe Connectivity

→ Ch 4

- | | | | |
|--------------------------|---|--|---------|
| <input type="checkbox"/> | Saved public Wi-Fi networks cleared
Settings → Wi-Fi → Saved Networks — delete any public/unknown networks | Prevents auto-connecting to Evil Twin fakes | Monthly |
| <input type="checkbox"/> | Wi-Fi set to "Ask to Join Networks"
Settings → Wi-Fi → Auto-Join: Off / Ask to join | Stops silent connections to unknown networks | Once |
| <input type="checkbox"/> | Bluetooth off when not in use
Turn off Bluetooth when not actively pairing — reduces discovery risk in public | Open Bluetooth is an attack surface | Daily |

Personal Device Hygiene Checklist

★ Myth vs Fact – Device Hygiene Edition

"The hardest part isn't learning the habits — it's unlearning the excuses," says Priya.

<p>✗ MYTH</p> <p>"My device is fine — it's fast and nothing seems wrong. I don't need to do a security scan."</p>	<p>✗ MYTH</p> <p>"I have antivirus. I don't need to update my OS — that's different software."</p>	<p>✗ MYTH</p> <p>"I only use my phone for social media and YouTube. There's nothing valuable to steal."</p>
<p>✓ FACT</p> <p>Malware is specifically designed to hide. Rohan's laptop was infected for hours before he noticed — the Trojan ran silently while the game worked perfectly. No visible symptoms ≠ no infection.</p>	<p>✓ FACT</p> <p>Antivirus catches known malware. OS updates patch the underlying vulnerabilities that malware uses to enter. WannaCry bypassed antivirus entirely — it used a Windows hole that an update had already fixed. Both are essential.</p>	<p>✓ FACT</p> <p>Your phone holds your contacts, photos, saved passwords, UPI app, WhatsApp messages, and location history. Attackers don't need bank documents — they need access. Your phone is the key to your entire digital life.</p>
<p>✗ MYTH</p> <p>"App permissions don't matter — I have nothing to hide."</p>	<p>✗ MYTH</p> <p>"I save everything in Google Drive, so I'm backed up and secure."</p>	<p>✗ MYTH</p> <p>"Public Wi-Fi is safe if the website uses HTTPS — I can see the padlock."</p>
<p>✓ FACT</p> <p>Privacy isn't about hiding — it's about control. An app with "always on" microphone access can record your conversations. "Nothing to hide" means nothing until those recordings are sold, leaked, or used against you.</p>	<p>✓ FACT</p> <p>Sync ≠ backup. If you delete a file or ransomware encrypts it, Google Drive reflects that change. A real backup is a separate, protected copy. You need both cloud AND a local backup that is disconnected after use.</p>	<p>✓ FACT</p> <p>HTTPS encrypts content — but not your DNS queries, session tokens, or identity on the network. Evil Twin networks can intercept session cookies even on HTTPS sites. Use a VPN or hotspot for sensitive tasks.</p>

Activity 2 – Sort the Myths

🔍 Which Myth Does Each Chapter Bust?

Match each of the 6 myths above to the chapter of Module 2 that directly contradicts it. Write the Myth number and Chapter number in your notebook — then write one sentence explaining the connection.

Myth 1

Ch. _____

Myth 2

Ch. _____

Myth 3

Ch. _____

Myth 4

Ch. _____

Myth 5

Ch. _____

Myth 6

Ch. _____

Q2.

Choose the myth you personally believed before this module. Write: (a) which myth it was, (b) what made you believe it, and (c) what specific moment from a chapter changed your thinking.

Write in your notebook — be honest, there are no wrong answers here

Personal Device Hygiene Checklist



"A generic checklist is a starting point," says Aryan. "A personalised one is what you'll actually use."



Step 1 – Identify Your Device(s)

In your notebook, write: (a) What devices do you use regularly? (phone, laptop, tablet) (b) What OS does each run? (Android, iOS, Windows, Mac) (c) Which device holds your most important data?

Step 2 – Identify Your Biggest Risks

Look back at your warm-up audit on Page 1. Which area had the most **X** marks? That is your highest priority. Write your top 3 personal risk areas in order of urgency.

Step 3 – Choose Your Frequency

For each checklist item — decide: Daily, Weekly, or Monthly? Be realistic. A daily checklist you ignore is worse than a weekly one you actually follow.


Step 4 – Add Personal Items

The master checklist covers common items — but you may have unique ones. Shared family laptop? School computer you use? A game account? Add items specific to your situation.

My Personal Device Hygiene Checklist

Name: _____ | Device(s): _____

✓ What I will do	How often	Why it matters
DAILY		
<input type="checkbox"/> _____	Daily	_____
<input type="checkbox"/> _____	Daily	_____
WEEKLY		
<input type="checkbox"/> _____	Weekly	_____
<input type="checkbox"/> _____	Weekly	_____
<input type="checkbox"/> _____	Weekly	_____
MONTHLY		
<input type="checkbox"/> _____	Monthly	_____
<input type="checkbox"/> _____	Monthly	_____
<input type="checkbox"/> _____	Monthly	_____
<input type="checkbox"/> _____	Monthly	_____
MY OWN ADDITIONS		
<input type="checkbox"/> _____		
<input type="checkbox"/> _____		

 Use the master checklist on Page 3 to fill in the items. Choose what's relevant to your device and your habits — add your own rows in the personal section.

Personal Device Hygiene Checklist

 Read the Situations – Apply the Full Module

Each situation below has a device hygiene failure. Write in your notebook: (a) Which pillar was neglected? (b) Which chapter covered this? (c) What should the person do immediately and going forward?

Situation 1 – Kavya, Shimla

Let's assume Kavya's laptop has been slowing down for three weeks. She hasn't run a scan — her antivirus subscription lapsed and she hasn't renewed it. She's been clicking "will you remind me tomorrow" on the antivirus renewal notice every day. Yesterday, she noticed her camera light flickered on for a second while she was typing notes — and no app was open.

Situation 2 – Naman, Delhi

Let's assume Naman installed a "free study timer" app three months ago. He used it twice and forgot about it. The app still has "always on" microphone, camera, and location access. He hasn't checked his app permissions since installing his new phone 5 months ago. He has 23 apps — 9 of which he hasn't opened in more than 2 months.

Situation 3 – Meera, Delhi

Let's assume Meera's phone has been auto-connecting to Wi-Fi everywhere she goes. She's saved 12 networks — including "FreeWiFi_Station", "Airport_Open", and "CafeNET_Free" from various places. She connected to one of these automatically this morning at her building entrance without realising. Her UPI app was open at the time.

Situation 4 – Rohan, Jaipur

Let's assume Rohan has been diligently backing up to Google Drive every week since Chapter 5. His friend tells him "you should also test your backup — not just make it." Rohan has never actually tried to open a recovered file from Google Drive. He assumes the backup is working because it says "synced."

Activity 3 – Quick Questions
 Choose the Correct Option
Q3a.

Which of the following is the best reason to run a full antivirus scan even if your device seems to be working normally?

- To speed up your device
- Malware is designed to hide — no symptoms doesn't mean no infection
- Antivirus scans always find something to fix
- Full scans are required by law in India

Q3b.

An app you installed 4 months ago for a school project still has "always on" microphone access. The best action is:

- Keep it — you might need it again sometime
- Revoke the microphone permission and delete the app if you no longer use it
- Install a different antivirus to block the app's microphone
- Turn on Aeroplane Mode when not using the phone

Q3c.

Rohan has a backup — but has never tested it. Why is this a problem?

- Untested backups can fail silently — you may discover it's corrupted only when you need it most
- Backups expire after 30 days if not tested
- Testing uses up your cloud storage quota
- It only matters if the backup is on a USB drive, not cloud

Q3d.

Device hygiene is best described as:

- A one-time setup that protects you permanently once done
- A set of regular, repeated habits that keep your device secure over time
- Only necessary for people who use online banking
- The responsibility of the device manufacturer, not the user

Personal Device Hygiene Checklist

Deep Analysis – The Full Module in One Question

The Connected Failures – Rohan's Year of Device Problems

Let's assume: Over the course of one school year, Rohan experiences five separate device incidents. In January, his laptop is infected by a Trojan from a "free game" download — he loses 3 days of data. In March, he connects to an Evil Twin network at a mall and receives an OTP he didn't request — his Google account is accessed from an unknown location. In May, a security scan reveals a keylogger that had been running silently on his laptop since January — it was never fully removed. In August, his phone falls in water — no backup, 4 months of photos and school notes lost permanently. In October, a ransomware attack encrypts his laptop files — his only backup was a USB drive plugged in at the time, also encrypted.

Q4a.

Map each of Rohan's five incidents to a specific device hygiene failure — and to the checklist pillar (Updates / Scans / Permissions / Backups / Connectivity) that would have prevented it. Draw a table in your notebook.

📓 Notebook table: Incident | Failure | Pillar | Prevention

Q4b.

Notice that the January keylogger wasn't discovered until May — 4 months later. What does this tell us about the relationship between device hygiene and time? Why does neglecting it for months create compounding risks?

📓 Write in your notebook — 3–4 sentences

Q4c.

Design a simple monthly device hygiene routine for Rohan that — if followed from the start — would have prevented all five incidents. List each step in order of priority. Keep it realistic for a Class 9 student.

📓 Write in your notebook as a numbered monthly checklist — maximum 8 items

Pause & Reflect

Responsibility Without Blame

Every chapter in Module 2 featured a character who did something "wrong" — but none of them intended to cause themselves harm. Rohan wasn't careless; he was excited about a free game. Meera wasn't lazy; she was busy. Naman wasn't reckless; he just didn't know. Device hygiene isn't about being perfect or blaming yourself for past mistakes. It's about building habits that make the **safe choice the easy choice** — so you don't have to rely on perfect decision-making every time.

In your notebook: Which character from Module 2 do you relate to most — and what one habit from this chapter will you commit to starting this month?

Return to Page 1 – What Has Changed?

Revisit Your Device Health Audit

Go back to your audit on Page 1. Look at every **X** and **Δ** you marked.

Q5.

For each **X** or **Δ** in your Page 1 audit: (a) Which checklist item from Page 3 addresses it? (b) What specific risk does your gap create? (c) Write it into your personalised checklist on Page 5 with a realistic frequency.

📓 Use your Page 1 audit as the input for your Page 5 personalised checklist — connect the two.

Personal Device Hygiene Checklist

🌟 Epilogue – Module 2 Complete · What Everyone Leaves With

Rohan

"Five incidents. Five preventable habits I didn't have. The checklist isn't extra work — it's the work I should have been doing all along."

Aryan

"I thought I was already doing well. This chapter found two gaps I didn't know I had. Auto-connect Wi-Fi and untested backup. Both fixed now."

Priya

"Device hygiene is like brushing your teeth. You feel fine whether you do it or not — until you don't. By then, it's a much bigger problem."

Naman

"9 apps with permissions I never reviewed. Deleted 7 of them. Revoked microphone from the other 2. It took 10 minutes. I feel different about my phone now."

Meera

"Deleted 12 saved public networks. Set Wi-Fi to Ask to Join. Enabled auto-updates. Three settings. Took 4 minutes. Should have done this in Chapter 3."

🔗 The Complete Module 2 Journey – What You Now Know

Ch 1 ✓



Spot & Prevent Malware

Ch 2 ✓



Avoid Piracy Risks

Ch 3 ✓



Update & Download Safety

Ch 4 ✓



Navigate Public Wi-Fi

Ch 5 ✓



Back Up Your Data

Ch 6 ✓



Own Your Device Hygiene

🌟 Key Takeaways



Device Hygiene Is a Habit, Not an Event

One-time fixes don't work. Regular, scheduled habits — updates weekly, scans monthly, permissions reviewed monthly — keep your device protected over time.



Updates Are the Single Most Impactful Habit

More attacks exploit unpatched software than any other vector. Enabling automatic updates is the highest-return single action in this entire checklist.



Permissions Are Forgotten Attack Surfaces

Apps accumulate permissions you forget about. A monthly review takes 10 minutes and significantly reduces your exposure to silent surveillance.



A Backup You Haven't Tested Might Not Work

Test your backup by recovering one file. Make sure the drive is disconnected after backup. Cloud + local + tested = real protection.



Connectivity Hygiene Is Invisible But Critical

Saved public networks, auto-connect Wi-Fi, and open Bluetooth are silent risks most students have never thought to check. Two settings changes fix most of it.



Personalise — Then Actually Do It

A checklist tailored to your device and your habits is far more useful than a generic one. The best security routine is the one you actually follow.

🏆 The Module 2 Rule – From Aryan, Priya, Naman, Kavya, Meera & Rohan

"Your device is only as secure as your last hygiene check. Update it. Scan it. Review its permissions. Back it up. Watch what it connects to. Do this regularly — and you won't need to learn these lessons the hard way."


Safe Devices, Apps & Browsing · Module 2 · Chapter 6 — Module 2 Complete ✓

Personal Device Hygiene Checklist

Comic Strip – "The Group Chat, Six Weeks Later"

The Group Chat – Six Weeks After the Device Audit

Panel 1 Rohan's Room

 **Device Hygiene Chat**


- ✓ Updates: done
- ✓ Scan: clean
- ✓ Backup: 2 days ago

ROHAN

Rohan sends his first-ever weekly hygiene report. On time. 📧


Panel 2 Naman's Phone

Guys I just found a fitness app had "always on" microphone since 8 months ago. How?! Deleted. Reviewed all 24 apps. Took 12 minutes 🙄

 NAMAN

Naman's permissions audit — 8 months late but finally done.

Panel 3 Meera's Laptop


 MEERA

Update notification appeared. I actually clicked "Install Now" for the first time in my life. It felt weird but good 😊

Meera's first voluntary update in recorded history.


Panel 4 Kavya's Desk, Shimla

Ran a full scan. **0 threats found.** Backed up to Google Drive + USB. Disconnected the drive after. Aryan would be proud 🙌

 KAVYA

Kavya's monthly hygiene routine — completed in 20 minutes.

Panel 5 Priya Replies


 PRIYA







This group chat has gone from "my laptop is dying" to everyone sharing hygiene reports. Six chapters. Zero excuses left. ☑️

Priya summarises the whole module in one message.

Panel 6 The Group – Final Word

Module 2: Complete. ✓
Devices: Hygiene-checked. ✍️
Next problem? Bring it. 🙌

 ARYAN

 Rohan  Aryan  Priya  Naman  Kavya  Meera

🗨️ The Cyber Safety Ambassadors – Module 2 Done!