SAFE DEVICES, APPS & BROWSING · MODULE 2 · CHAPTER 3

Safe Download & Update Practices

Software Vulnerabilities · Update Patches · Safe Installation · Download Hygiene

55–65 min

GRADES 9–12

The Story So Far — Module 2 Recap

Ch 1: Rohan's laptop was hit by malware — a Trojan, worm, and ransomware — all from one "free game" download. The group learned to identify the four malware types and Aryan's 7 prevention steps. **Ch 2:** Zara's laptop was cryptojacked from a piracy site she'd been using for three years. The group learned how piracy sites and cracked software carry hidden threats. **Now in Chapter 3**, a neighbour arrives with a device problem that has a different root cause — not a bad download, not a piracy site, but something almost everyone ignores: the **humble software update notification**.

MODULE 2 · Safe Devices, Apps & Browsing

Chapter 3 — Safe Download & Update Practices

Key Terms — Words You Will Need Today

Vulnerability
A weakness or flaw in software that an attacker can exploit to gain access — like a cracked wall in a house.

Security Patch
A fix released by the developer to close a known vulnerability. An update that contains a patch repairs the cracked wall.

Official Source
Play Store, App Store, or a developer's official website — the verified, safe place to download apps and software.

Fake Update Pop-up
A fraudulent browser alert pretending to be a system update — actually a trick to install malware on your device.

Warm-Up — What Do You Think Caused This?

Read Each Device Problem — Then Guess the Cause

Four students describe what happened to their devices. Write your best guess for what caused each problem in your notebook. No right or wrong — just think.

Meera's Laptop, Delhi

Meera's laptop kept showing "Update available" for 6 months. She always clicked "Remind me later." One morning, strangers were able to access her laptop remotely without any password. She hadn't downloaded anything unusual.

Tarun's Phone, Bhopal

Tarun downloaded a study app from a website his friend recommended — it wasn't in the Play Store. The app worked perfectly. Two weeks later, every contact in his phone received a strange link "from him" that he never sent.

Anjali's Laptop, Kolkata

Anjali saw a pop-up: "⚠ URGENT: Your Windows is out of date. Click here to update NOW." She clicked it and a programme installed. Her browser homepage changed and she started seeing ads she couldn't remove.

Rahul's Phone, Chandigarh

Rahul's bank app had been showing "Update available" for weeks. He ignored it. One Tuesday, he found three transactions he never made. The bank confirmed his app had a known security flaw that the update would have fixed.

Q1.

For each device problem above, write what you think caused it. One line per case is enough — you'll return to these at the end of the chapter.

Personal Device Audit — How Updated Are You Right Now?

Check Your Own Device — Be Honest

Think about your own phone or laptop. Circle your honest answer for each row. You'll return to this at the end of the chapter.

My phone's operating system (Android / iOS) is fully up to date	Yes ✅	No ❌	Not sure 🤔
My apps (WhatsApp, Instagram, banking, etc.) are all updated	Yes ✅	No ❌	Not sure 🤔
I have pending "Update available" notifications I haven't acted on	Yes ❌	No ✅	Not sure 🤔
I only download apps from official stores (Play Store / App Store)	Yes ✅	No ❌	Not sure 🤔
I check app reviews and permissions before installing something new	Yes ✅	No ❌	Not sure 🤔

Q2.

Count your ❌ or 🤔 answers. If you have 3 or more — your device may have gaps in protection right now. Does this surprise you? Write one honest sentence.

🎭 Meet the New Character — and the Problem Begins

Meera NEW CHARACTER

Class 10, Delhi — Aryan's neighbour, Rohan's friend. Smart and careful about most things. But every update notification gets the same response: *"Remind Me Later."* Her logic: *"Updates break things. My device works fine."* The weekend never comes — and her devices are months behind on security patches.

📍 Scene 1 — Aryan's Doorstep · Saturday Morning · Meera Arrives Panicking

MEERA: Aryan bhai — someone's controlling my laptop! The 🖱️ cursor is moving on its own. I didn't download anything, I didn't click anything weird!

ARYAN: Disconnect from Wi-Fi — now. Good. When did you last update Windows?

MEERA: Updates? I always press "Remind Me Later"... it's been about... six months? Maybe more? But how does that matter — I didn't click anything!

PRIYA: That's how it happened. An unpatched Windows vulnerability was the open door — your outdated software gave attackers the key.

🪞 Before We Begin — What Do YOU Actually Do?

Be honest — no one is marking you on this. Tick the column that describes what you *actually* do, not what you think you should do. We'll come back to this at the end of the chapter.

Behaviour — What do you do when...	✅ I do this	❌ I don't / rarely do
...an update notification appears, I install it **the same day**	☐	☐
...I download apps, I **only use the official Play Store or App Store**	☐	☐
...a friend sends me an APK or .exe over WhatsApp, I **don't install it**	☐	☐
...I install an app, I **read what permissions it asks for** before accepting	☐	☐
...I see a browser pop-up saying "Update your device now!", I **close it and ignore it**	☐	☐
...I find paid software available "free" on a random site, I **don't download it**	☐	☐
...I plug in someone else's USB, I **scan it with antivirus before opening any file**	☐	☐
...an installer says "disable your antivirus first", I **stop and delete it immediately**	☐	☐

📊 Count your ticks

I ticked ✅ **I do this** for ____ out of 8 behaviours.
I ticked ❌ **I don't** for ____ out of 8 behaviours.

🤔 Quick Reflection

Look at your ❌ column. Pick the **one habit** you think creates the biggest risk. Write it in your notebook — we'll come back to it at the end of the chapter.

📓 Write in notebook — don't change your answers later!

🔗 Why Updates Matter — The Vulnerability-to-Attack Chain

"Let me show you exactly what happens when you keep clicking 'Remind Me Later,'" says Naman, pulling up a diagram.

Pause & Think!

Notice Step 3 — the developer released the patch, making the vulnerability **publicly known.** Attackers immediately scan for unpatched devices. The longer you delay, the easier you are to find. Meera's 6-month-old Windows had a known remote-access flaw that was already patched — the attacker didn't need to be clever, just patient.

📋 Read the Situations — When "Remind Me Later" Had Consequences

🏥 Hospitals, India — 2022

Government hospital networks hit by ransomware exploiting an unpatched Windows flaw. Patient records locked. The patch had been available for **3 months** — systems simply hadn't updated.

🏦 Android Banking Apps — 2023

A flaw in older Android allowed malware to read banking OTPs. Users who hadn't updated were vulnerable. The fix was in a patch released **6 weeks earlier** — skipped by millions of Indian users.

🌍 WannaCry Link, 2017

WannaCry (Ch 1) targeted unpatched Windows systems. Microsoft's fix was available **2 months before** the attack. Every infected machine — 48,000+ in India — had skipped the update.

🔄 What Is Actually Inside a Software Update?

🩹 Security Patches	🐛 Bug Fixes	⚡ Performance Fixes	✨ New Features
Fixes for vulnerabilities — the most important part of any update	Repairs for crashes, errors, and glitches	Improvements to battery, speed & stability — updates usually make devices faster, not slower	New capabilities — the least important part, but often the most noticed

💡 The part students ignore (security patches) is the most important. The part students fear (breaking things) is the least likely to happen.

Q4.

Look at the three real cases above. What single action — if taken — would have prevented all three attacks? Write it in one clear sentence. Then explain *why* that action works using the Vulnerability Chain diagram.

📓 Answer in your notebook

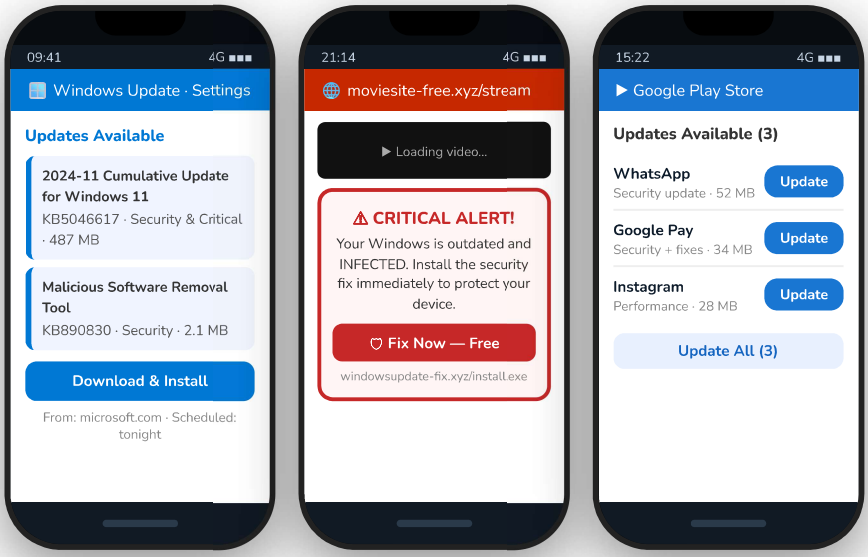
Q5.

Many students — like Meera — believe "updates break my device." The dark blue box above lists what updates actually contain. Which item in that list directly contradicts Meera's belief? Write one sentence explaining the contradiction.

📓 Answer in your notebook

Real vs Fake — What Update Screens Actually Look Like

"Here's the thing," says Zara — now helping the group after her own Ch2 lesson. "Some people skip real updates and click fake ones. Both are dangerous in opposite ways."



Screen 1:
✅ **Real Windows Update**
(from Settings menu)

Screen 2:
❌ **Fake Update Pop-up**
(on a piracy website)

Screen 3:
✅ **Real Play Store App Updates**

How to Tell Real Updates from Fake Ones

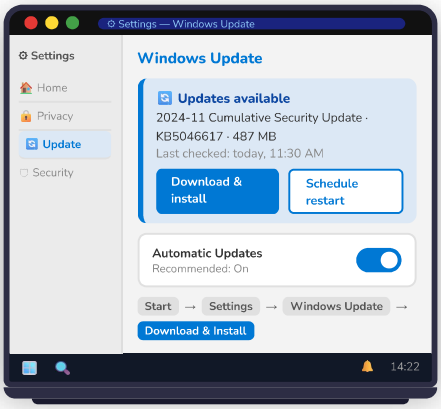
Feature	✅ Real Update	❌ Fake Update Pop-up
Where it appears	Inside Settings / Play Store / App Store — never in a browser tab	As a pop-up in a browser window while visiting a website
URL / source	microsoft.com · apple.com · play.google.com — verified	Random domain: `windowsfix.xyz` , `update-now.in`
Language used	Calm, technical, no urgency — "Updates available"	**URGENT! CRITICAL! INFECTED!** — designed to panic you
What it asks you to do	Click "Download & Install" — within the official app	Download an .exe or .apk file from an unknown website
What happens after	Device becomes more secure	Malware installs — device becomes less secure

Q6.

Anjali (from Page 1's Scenario 3) clicked a pop-up saying "⚠ URGENT: Your Windows is out of date. Click here to update NOW." Using the table above, identify THREE specific features of that pop-up that should have told Anjali it was fake.

📓 Answer in your notebook

Where to Find Real Updates on a Windows Laptop



✅ **This is where real updates live:**
Start → Settings → Windows Update

Q6b.

Look at the Windows Update settings screen on the left. Notice three things: the source path (Start → Settings → Windows Update), the update details (KB number, file size, type), and the Automatic Updates toggle set to On.

(a) Why does a real update screen show a KB number and file size, while a fake pop-up usually doesn't? What purpose do these details serve?

(b) The screen shows "Automatic Updates: On." Why is turning this on considered the single most effective update habit — even more than manually checking every week?

(c) Meera's laptop was on the *January version* of Windows in *July*. Open your own laptop or phone. Check Settings → Windows Update (or Software Update on iOS/Android). How many updates are pending right now? Write the number honestly.

📓 Answer all three parts in your notebook

🛡️ Safe Download Practices — What to Check Before You Install Anything

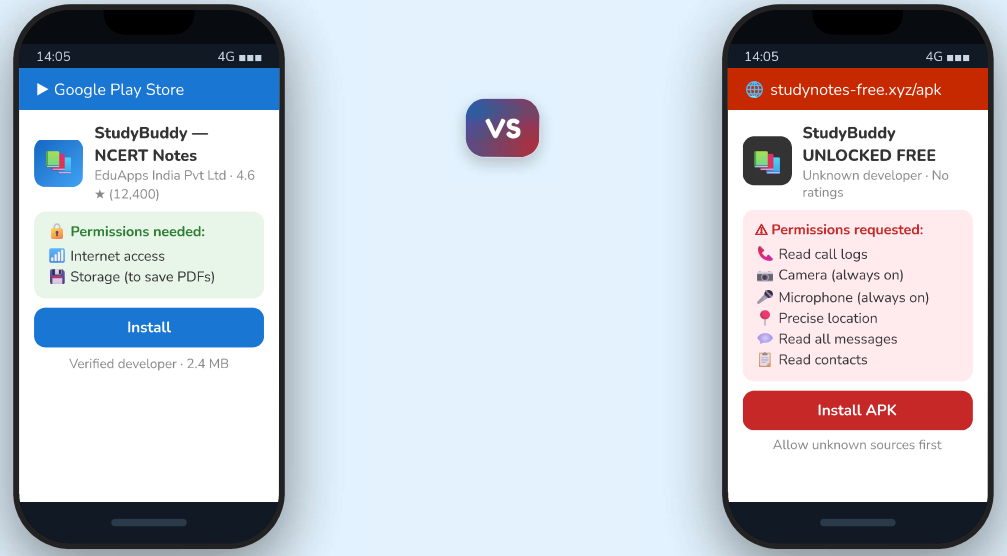
Naman has built a checklist. "Every time you install anything — app, software, file — run through this. It takes 60 seconds."

What to Check	What Safe Looks Like ✅	What Risky Looks Like ⚠️
Source / Store	Play Store, App Store, or official developer site	Random website, Telegram, WhatsApp forward, torrent site
App / File Reviews	Many reviews, high rating, verified developer name	No reviews, brand-new listing, misspelled developer name
Permissions requested	Only what's needed — camera for camera app, location for maps	Torch app wants contacts; game wants microphone "always on"
File type (for PC)	`.exe` from official site, or via official store	`crack.exe`, `keygen.exe`, `.apk` from unknown source
Install instructions	Just open and install normally	Says "disable antivirus first" or "allow unknown sources"
Price vs expectation	Free apps in official stores are free; paid software costs money	Paid software offered "free" outside official channels

🏫 Case Study — Read, Look & Analyse

Tarun Installs a New Study App — Two Very Different Stories

Tarun is installing a study app. Look at the two phone screens below — one is from the Play Store (official), one from a third-party website. Study them carefully, then answer Q7a and Q7b.



Screen A: ✅ Play Store Install (Official Source)

Screen B: ❌ Third-Party APK (Unofficial Source)

Q7a.
Look at Screen B. The app claims to be a study notes app. List THREE permissions it requests that a study app has absolutely no reason to need — and explain why each one is suspicious.

📓 Write in notebook

Q7b.
Tarun installed the Screen B APK. Two weeks later, his contacts started receiving strange links from his number. Using Screen B as evidence — which specific permission allowed this to happen, and how?

📓 Write in notebook

Activity 1 – Safe or Risky Habit?

Sort These 8 Student Habits

Naman surveyed students about their download and update habits. Sort each numbered habit into the correct zone. Write the numbers in your notebook.

1. "I always click Remind Me Later on updates"
2. Auto-update is enabled for all apps
3. Downloads APKs from Telegram groups
4. Only installs apps from Play Store
5. Clicked a browser pop-up saying "Update Windows now"
6. Checks app reviews before installing
7. Updates OS every time notification appears
8. Grants "All Permissions" without reading

✅ Safe Habit	⚠️ Risky Habit
Write numbers here...	*Write numbers here...*

Q8.

Look at the habits you marked as Risky. How many of them apply to you personally, right now? Write an honest sentence — and name one habit you will change this week.

📓 Answer in your notebook

Activity 2 – What Should They Do?

Help Each Character Decide

For each situation — write in your notebook: (a) Safe ✅ or Risky ⚠️ · (b) What specific mistake is being made? · (c) What should they do instead?

Situation A – Meera (evolved)

After fixing her remote-access problem, Meera gets an update notification on her phone: "Security patch available — 124 MB." She's on mobile data and thinks "I'll wait for Wi-Fi — it's just an update, not urgent."

Situation B – Rohan (Jaipur)

Rohan wants a free PDF editor for school. He searches Google, finds "PDF Editor Pro Free Download" on a website, and downloads the .exe. The site looks professional. The installer asks him to "disable Windows Defender for smooth installation."

Situation C – Zara

Zara's Play Store shows 6 pending app updates. She clicks "Update All." One app asks for a new permission: "Access to call logs." She pauses and reads the update notes — it doesn't explain why call logs are needed. She doesn't update that one app.

Situation D – Naman

A WhatsApp message says: "⚠ Important: New WhatsApp update required — your old version will stop working. Download here: bit.ly/wa-update-new2024." Naman checks the Play Store and finds WhatsApp is already up to date. He ignores the WhatsApp message.

📓 For each situation: Safe ✅ or Risky ⚠️ · What mistake is being made · What should they do

Activity 3 – Quick Questions

Choose the Correct Option

Q9a.

A security patch is released by a developer. How quickly should you install it?

- ○ As soon as possible — within 24–48 hours
- ○ When the device slows down noticeably
- ○ After waiting 1 month to see if it causes problems
- ○ Only if a friend tells you their device got hacked

📓 Write answer in notebook

Q9b.

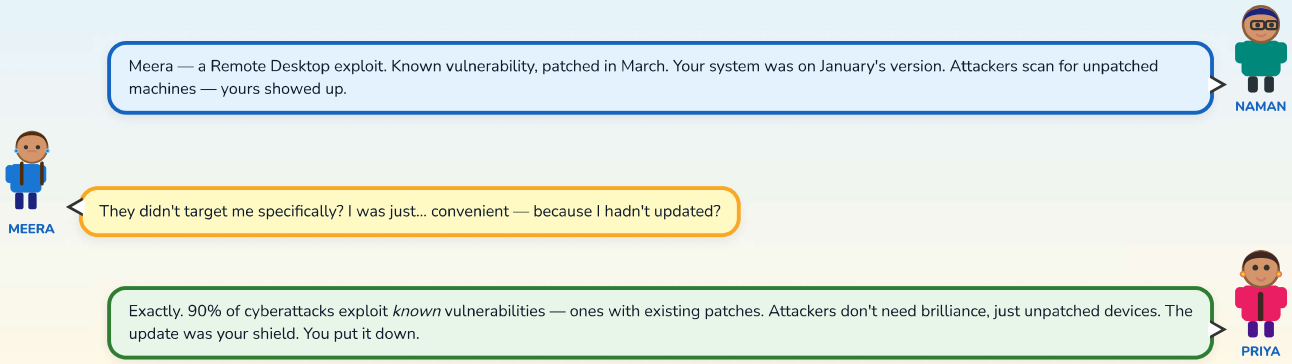
You see a browser pop-up: "⚠ Windows update required! Your PC is at risk." The most correct response is:

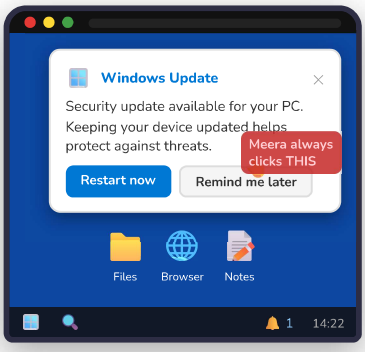
- ○ Click the "Fix Now" button — it's genuinely helpful
- ○ Close the pop-up and go to Settings → Windows Update
- ○ Download the file it recommends — it's faster
- ○ Ignore all updates — pop-ups are always fake

📓 Write answer in notebook

Story – Meera Understands What Happened

Scene 2 – Aryan's Room · 2 Hours Later · Meera's Laptop is Disconnected and Scanned





Meera's laptop – this notification appeared for 6 months straight

Quick Check – What Do You Think?

Q9c.
Look at Meera's screen. She saw this notification for 6 months. Why do you think she kept clicking "Remind me later" instead of "Restart now"? Select the most likely reason AND write one sentence explaining your choice:

- ○ She didn't know updates were important for security
- ○ Restarting felt inconvenient — she was always in the middle of something
- ○ She was worried the update would break her device or delete her files
- ○ She didn't trust that it was a real Windows notification

Circle your answer & write one reason in notebook

Q9d.
The notification says "Keeping your device updated helps protect against threats." Meera read this every time. Yet she still didn't update. What does this suggest about the relationship between *knowing* something is dangerous and actually *changing behaviour*? Write 2 sentences.

Answer in your notebook

Pause & Reflect

The "Later" Trap – Why We Delay What We Know We Should Do

Meera knew updates existed. She saw the notifications. She just kept putting it off. This pattern — knowing something is important but delaying it anyway — is called **present bias**: the tendency to value small convenience right now over larger safety later. We all do it, in many areas of life. Ignoring an update feels harmless because *nothing bad happens immediately*. The consequence is invisible — until it isn't.

Q10a.
Think of another area in your own life where you regularly delay something you know is important — study revision, sleep, drinking water, etc. Why do you delay it? How is this similar to Meera's update habit?

Notebook

Q10b.
Priya says: "The update was your shield. You put it down." Is this a fair way to describe what Meera did? Or is it too harsh? Write your honest view in 2–3 sentences.

Notebook

Aryan's Safe Download & Update Rules

1. **Enable automatic updates — right now**
   Settings → Windows Update → "Automatic" / Play Store → "Auto-update apps." Set once, forget.
2. **Real updates never come from browser pop-ups**
   Close any pop-up claiming an urgent update. Go to Settings directly. Always.
3. **Download only from official sources**
   Play Store, App Store, or the developer's official site. Not there? Don't install it.
4. **Read permissions before accepting**
   When an update requests a new permission — pause. Does this app genuinely need it? If not, don't grant it.
5. **Any install asking you to "disable security" is malware**
   No legitimate software ever requires this. That instruction is always a red flag.
6. **Check your update status once a month**
   Settings → Windows Update / Check for Updates (iOS/Android). 5 minutes closes most known holes.

🔄 Return to Page 1 — Device Audit Revisited

Check Your Answers Again — What Will You Change?

Go back to your personal device audit on Page 1. Look at every ❌ or 😕 you ticked.

Q12.

Look at your device audit from Page 1. For every item you marked ❌ (No) or 😕 (Not Sure) — do the following in your notebook:

(a) **Name the risk** — what specific security problem does this gap create on your device?

(b) **Match the rule** — which of Aryan's 6 rules (above) directly fixes this gap? Write the rule number.

(c) **Set a deadline** — write exactly when you will fix it: *today / this weekend / by [date]*. Not "soon."

📓 Do this for every ❌ or 😕 — be honest and specific

Q13.

Go back to the four device scenarios on Page 1. Now that you've completed the chapter — write the correct cause for each one. Were your original guesses right? Which surprised you the most?

📓 Answer in your notebook — compare with your original Q1 answers

Key Takeaways

Updates Are Security Patches, Not Just Features
Every skipped update is a known vulnerability left open. Attackers scan for unpatched devices and exploit them automatically — no targeting needed.

Patches Must Be Installed Within 48 Hours
Once a patch is public, the vulnerability is public too. Attackers begin exploiting within 48 hours. "Later" means "during the attack window."

Real Updates Come From Settings, Not Pop-ups
Browser pop-ups saying "update now" are fake — designed to install malware. Legitimate updates are always inside the official settings menu.

Official Sources Only — Always
Play Store, App Store, official developer sites. If it asks you to "allow unknown sources" or "disable security" — it's malware, not software.

Meera, Aryan, Priya & Naman's Rule for Chapter 3

"An update notification is not an inconvenience. It is your device telling you: a hole has been found and a fix is ready. Click 'Remind Me Later' and you leave the hole open."

Safe Devices, Apps & Browsing · Module 2 · Chapter 3 → Next: Chapter 4 — Public Wi-Fi Risks & Secure Connectivity