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

Choosing Safe App Sources

Trusted stores · Sideloading risks · Fake apps · The 4-Point Check

Grade 6–8

⏱ 30–45 min

⭐ Previously — Chapter 1 & 2

You learned to spot **fake pop-ups, phishing messages**, and **unsafe links**. Monica, Rohit, and Sana now know: *"STOP. CHECK. ASK."* Today — a new question. There's an app they want. It's not on the Play Store. A classmate says he can get it free from a website. Should they?

⭐ NEW CHARACTER — Joins in Chapter 3

Dev

Monica's classmate. The class "tech expert" — knows how to find apps outside the Play Store and thinks that makes it safe. Chapter 3 is where he learns that **knowing how to do something ≠ knowing if it's safe.**

💥 3 Big MYTHS about App Downloads — and the TRUTH

❌ MYTH	❌ MYTH	❌ MYTH
"An APK file is just an app file — it can't hurt you."	*"Nothing bad happened yet — so it must be safe."*	*"The free APK is the same app — just without paying."*
✅ **TRUTH:** An APK can hide malware. Without official store vetting, **nobody has checked it** for safety.	✅ **TRUTH:** Malware can silently collect your data for **months before anything looks wrong.**	✅ **TRUTH:** Free cracked APKs are often **modified to include spyware or adware** — you pay with your data.

🔑 4 Key Words — Learn These First!

App Store
An official, trusted place to download apps — Google Play Store or Apple App Store.

Sideloading
Installing an app from outside the official store — risky because nobody has checked it.

Fake App
An app that *looks* real but hides malware, steals data, or shows endless ads.

App Vetting
The process where official stores check an app for safety before users can download it.

🎭 Scene 1 — Dev's Shortcut

Friday · School · Monica, Sana, and Dev

Monica

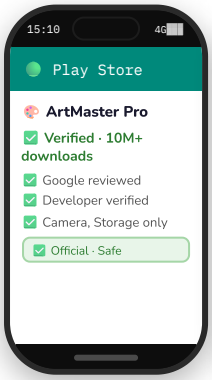
Dev, the art app we need costs ₹350 on Play Store. I can't afford it!

Easy! I know a site — apk-vault.net. You can get it free. I do this all the time, nothing bad ever happened!

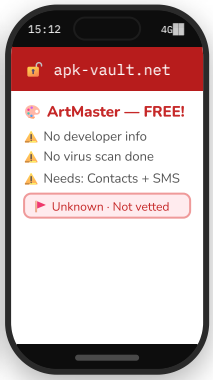
Dev 😍

Sana 🤔

Wait — remember Vikram? Didn't Rohit say downloading from random sites is dangerous? Let's call Rohit first.



Play Store ✅



Random Site ⚠️

🔍 4 Red Flags in Dev's "Free" Version:

- ⚠ **No padlock** — the site itself is not secure
- ⚠ **No developer name** — who actually made this version?
- ⚠ **Art app asking for Contacts & SMS** — it has no reason to need those
- ⚠ **Paid app offered free** — someone modified it. Why?

Scene 2 — Rohit Explains: What Does the Play Store Actually Do?

Same Evening · Monica's House

Rohit: Dev, before any app reaches the Play Store — Google checks it. A sideloaded APK skips ALL of that. You're taking a blind risk every time.

Dev: But I've done it 20 times with no problem. Doesn't that mean it's safe?

Rohit: No. Malware can collect your data silently for months. Nothing *looking* wrong doesn't mean nothing *is* wrong.

What Play Store Checks

- Scans for viruses and malware
- Verifies the developer's real identity
- Reviews if permissions are reasonable
- Checks for fraud or fake claims

What Sideloading Skips

- No virus scan on the file
- No check on who made it
- No permission review
- No ongoing safety monitoring

When you sideload — YOU are the only safety check. And you can't see inside the APK.

Activity 1 — Tick ALL the Warning Signs — Dev's Download

Read each option. Tick ✓ the ones that ARE warning signs. Leave the safe ones empty.

- ☐ Website has no 🔒 padlock in the URL
- ☐ Paid app offered completely free from unknown site
- ☐ No developer name or verified badge
- ☐ Art app asking for Contacts and SMS
- ☐ The same app is also on Google Play Store ✅
- ☐ No reviews from verified users

Q1. Dev says: "I've done it 20 times — nothing bad happened." Is this a good reason to keep doing it? Write YES or NO and why:

Q2. A paid app is free on a random site. What might someone have *added* to it in exchange for removing the price?

The Real Cost of "Free"

When a paid app is free on a random site — you are still paying. Not with money, but with your **photos, contacts, and data.** Someone removed the price and added spyware instead.

Scene 3 – Spot the Fake App!

Next Day · Dev shows Rohit two listings he found – even inside the Play Store

Dev: Rohit — there were *two* versions of the app on the Play Store itself. One looked a bit off. How do I tell which is real?

Rohit: Good question — fake apps exist even inside the store. You need to check 4 things: developer name, downloads, reviews, and permissions.

App Listing A – REAL

ArtMaster Pro
Developer: PixelLab Studios

- ⭐ 4.8 · 2,40,000 real reviews
- 10 Million+ downloads
- Permissions: Camera, Storage
- Price: ₹350

Verified · High downloads · Sensible permissions

App Listing B – FAKE

ArtMaster Pro — FREE!
Developer: Pixel_Lab_Studois

- ⭐ 5.0 · only 12 reviews (all 5 ⭐!)
- 500 downloads
- Permissions: Camera, Storage, **Contacts, SMS, Location**
- Price: Free

Typo · Very few downloads · Excess permissions

Rohit's 4-Point Check – Use This for EVERY App

Developer	Downloads	Reviews	Permissions
Real company name? Any typos?	Popular apps have millions. Under 1,000 = be careful.	All 5 stars with no text? Only 12 reviews? Suspicious.	Does the app actually NEED what it's asking for?

Activity 2 – Apply the 4-Point Check – Fill the Table

Check	App A (Real)	App B (Fake)
Developer name — any typos?		
Download count — high or low?		
Reviews — do they look genuine?		
Permissions — make sense?		

Q3. What is the BIGGEST clue that App B is fake?

Q4. Why would an art app ever need your SMS and Location?

Even inside the Play Store – stay alert!
Official stores are much safer, but fake apps can still slip through. The 4-Point Check is your second line of defence. Developer · Downloads · Reviews · Permissions — check all four, every time.

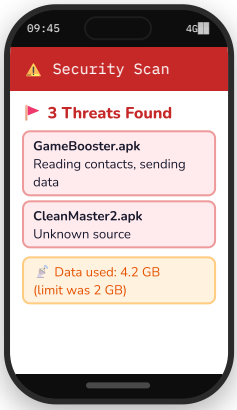
Scene 4 — Dev's Confession

A Week Later · Dev runs a security scan — and finds something he didn't expect

Dev: Rohit... the scan found 3 apps I don't remember installing. And my data went over the limit twice last month.

Rohit: Those unknown apps almost certainly came from the APKs you sideloaded. They installed silently. Tell your parents — let's clean this up together.

Dev: I thought I knew what I was doing. I was wrong. Knowing *how* to do something and knowing if it's *safe* are two different things.



Dev's scan result

Activity 3 — Safe Source or Not? — Sort Each App

Read each situation. Write its number in the correct zone.

1 Game from Play Store | 2 Study app APK on WhatsApp | 3 App from Apple App Store | 4 Torch app from .xyz website | 5 Dictionary · Play Store · 5M downloads | 6 "Free cracked" game from Telegram

Safe to Install

Write numbers here…

Do NOT Install

Write numbers here…

Q5. Dev admitted he was wrong. What does his experience teach us about "nothing bad has happened yet"?

Being Tech Smart ≠ Being Cyber Safe

Dev knew how to sideload an APK. But malware can run silently for months with zero visible signs. Tech skill without safety awareness leaves a door open. Official store, or don't install it — same rule for everyone.

The Only 3 Trusted App Sources

Google Play Store
- For Android phones
- Apps reviewed before listing
- Developer identity verified
- Automatic safety updates

Apple App Store
- For iPhone and iPad
- Strict review process
- Developer identity verified
- Privacy labels required

Anywhere Else
- Random APK websites
- WhatsApp / Telegram files
- Email attachments
- "Free cracked" sites

Epilogue — One Month Later

1

I presented the 4-Point Check at school assembly. Our whole class knows it now!

Dev — now a champion!

2

I bought the real ArtMaster Pro. ₹350 well spent — and no malware!

Monica — safe & creative!

3

Not from a store? Q1 says STOP — I didn't even need Q2!

Sana — always careful!

4

STORE · CHECK · ASK! Safe App Champions!

All four — together!

Quick Check — Test Yourself!

Q6. "Sideloading" means:

- ◯ (A) Loading apps faster using WiFi
- ◯ (B) Installing an app from outside the official store
- ◯ (C) Moving an app from one phone to another
- ◯ (D) Downloading from Google Play Store

Q7. True or False? — Tick T or F

- T F Play Store checks apps for malware before listing them.
- T F A sideloaded APK can collect data silently for months.
- T F "Nothing bad happened yet" means a sideloaded app is safe.
- T F Fake apps with very few downloads can still appear on the Play Store.

Q8. Dev says at assembly: *"Knowing how to do something doesn't mean it's safe to do it."* What does he mean? Write in your own words:

Use Only Official Stores
Play Store and App Store vet apps before you can download them. Anywhere else — no one has checked it.

Sideloading = Blind Risk
APKs from WhatsApp, Telegram, or random sites skip all safety checks. Malware can run silently for months.

Fake Apps Exist Everywhere
Even inside stores — check developer, downloads, reviews, and permissions before installing anything.

Tell a Trusted Adult
If you've installed something suspicious — don't hide it. Telling an adult early makes fixing it much easier.

Monica, Rohit, Sana & Dev's Golden Rule

"Before you install ANY app — **STORE · CHECK · ASK.**

Official store only · Real developer · Real reviews · Sensible permissions

Not sure? Close it. Tell a trusted adult. Your app, your data, your choice."