SAFE DEVICES, APPS & BROWSING · MODULE 2 · CHAPTER 4

# Public Wi-Fi Risks & Secure Connectivity

Public Networks · Eavesdropping · Man-in-the-Middle · VPN · Safe Habits

55–65 min

GRADES 9–12

### The Story So Far — Module 2 Recap

**Ch 1:** Rohan's laptop was infected by a Trojan, worm, and ransomware — all from one "free game" download. **Ch 2:** Zara's laptop was cryptojacked from a piracy site. **Ch 3:** Meera's laptop was remotely accessed through an unpatched Windows vulnerability — because she kept clicking "Remind Me Later." Now in **Chapter 4**, the same group is at a café. They're all on the same public Wi-Fi — and someone else in that café is watching every packet of data they send.

MODULE 2 · Safe Devices, Apps & Browsing

Chapter 4 — Public Wi-Fi Risks

## Before We Begin — What Do YOU Actually Do?

Be honest — no marks here. Tick what you *actually* do. We'll revisit this at the end.

| When on public Wi-Fi, I... | ✅ I do this | ❌ I don't |
|---|---|---|
| ...check whether the network name looks legitimate before joining | ☐ | ☐ |
| ...avoid logging into bank accounts or UPI apps | ☐ | ☐ |
| ...use a VPN before connecting | ☐ | ☐ |
| ...avoid sending passwords or OTPs over public Wi-Fi | ☐ | ☐ |
| ...prefer using my mobile hotspot instead of public Wi-Fi | ☐ | ☐ |
| ...turn off Wi-Fi when not actively using it in a public place | ☐ | ☐ |

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

📓 Write in your notebook: which ❌ habit do you think creates the **biggest risk** — and why? We'll return to this at the end.

## Key Terms — Words You Will Need Today

**Public Wi-Fi**
An open wireless network accessible to anyone nearby — cafés, airports, malls. No password needed means **no encryption** between you and the router.

**Eavesdropping**
Intercepting unencrypted data flowing over a network — like reading someone's postcard. Anyone on the same Wi-Fi can do this with basic tools.

**Man-in-the-Middle**
An attack where someone silently intercepts and reads (or alters) data between you and the website — without either side knowing.

**Evil Twin Network**
A fake Wi-Fi hotspot with a convincing name (e.g. "Café_Free_WiFi") set up by an attacker to intercept all traffic from devices that connect.

**VPN**
Virtual Private Network — encrypts all your internet traffic, creating a secure "tunnel" even on an open public network. Makes eavesdropping useless.

**Mobile Hotspot**
Using your phone's mobile data connection shared as a private Wi-Fi. Only you control it — far safer than public networks for sensitive tasks.

## Story — "Free Wi-Fi!" — Naman's Near Miss at the Café

### Scene 1 — Café Connect, Khan Market · Saturday Afternoon · The Group is Studying

NAMAN: Finally — free Wi-Fi! "Café_Connect_Free" — perfect. I'll just quickly transfer ₹500 to Rohan for his share of the snacks.

ARYAN: Stop. Don't open your UPI app on that. Public Wi-Fi is unencrypted — anyone on this network can intercept your data.

PRIYA: Also — that network name. Look at the café's actual router. What does it say on the board?

NAMAN: The board says "CafeConnect_KM". I connected to "Café_Connect_Free". Those are... different names.

PRIYA: That's an **Evil Twin network**. Someone in this café set it up. Disconnect right now — everything you were about to send could have gone straight to them.

## How the Attack Works — The Unencrypted Highway

*"Let me show you exactly what happens when you use public Wi-Fi for something sensitive," says Aryan, drawing a diagram.*

### The Public Wi-Fi Attack Chain

**You**
Open banking app or type password

→

**Open Router**
Data travels unencrypted on this hop

→

**Attacker**
Intercepts & reads your data silently

→

**Website**
Receives your request (unaware)

With a VPN: all data is encrypted end-to-end — the attacker intercepts only gibberish they cannot read.

**Activity 1**

### Story Analysis — Naman's Near Miss

**Q1a.**
**Naman was about to make a UPI payment on public Wi-Fi. Using the attack chain above, describe step by step exactly what the attacker could have obtained if Naman had completed the transaction.**

*Write in your notebook*

**Q1b.**
**The Evil Twin network was called "Café_Connect_Free" while the real one was "CafeConnect_KM." How could Naman have spotted this earlier — what should he have done before connecting?**

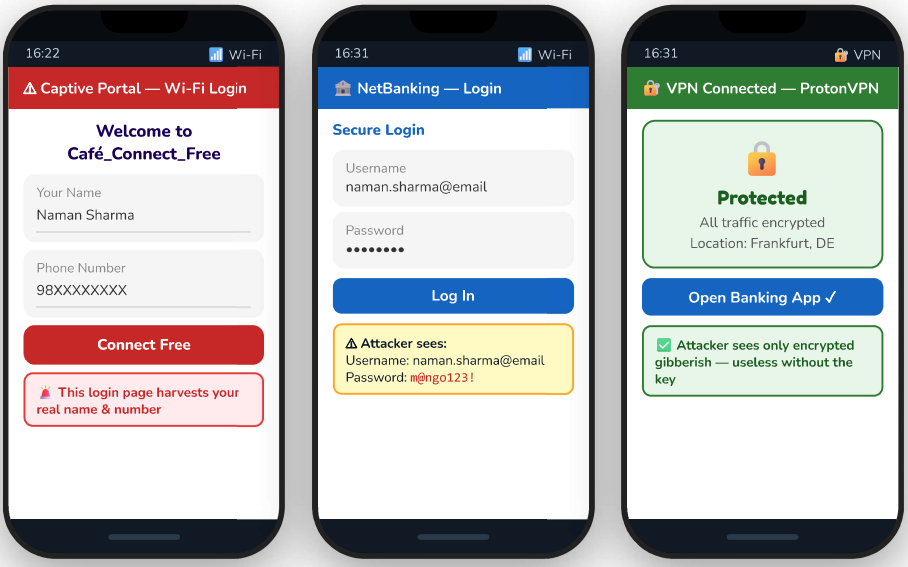
*Write in your notebook*

**Q1c.**
**Choose the correct option — An Evil Twin network is dangerous primarily because:**

- ○ It slows your internet connection significantly
- ○ All traffic you send passes through the attacker's device, giving them full visibility
- ○ It only works on Windows devices, not Android or iOS
- ○ It installs malware automatically when you connect

## What Public Wi-Fi Attacks Look Like on Your Device

*Rohan pulls out his phone — "I saw these kinds of screens during Aryan's demo. Here's what the three attacks look like in real life."*




Screen 1: Evil Twin Captive Portal (harvesting your details)

Screen 2: Credentials intercepted during bank login

Screen 3: VPN active — safe to use banking on public Wi-Fi

**Pause & Think!**

Screen 1 shows a captive portal — the login page many cafés, airports, and malls ask you to fill in before granting Wi-Fi. This page can be **fake** on an Evil Twin network, harvesting your real name and phone number. Screen 2: even a legitimate café network is unencrypted — your login data travels in plain text. Screen 3 is the only safe version: VPN encrypts everything so interception yields nothing useful. **The network doesn't have to be fake to be dangerous.**

## Risk by Network Type — What's Safe for What?

| Task | Public Wi-Fi (No VPN) | Public Wi-Fi + VPN | Mobile Hotspot | Home Wi-Fi |
|---|---|---|---|---|
| Browse news / social media | ⚠ Risky | ✅ Safe | ✅ Safe | ✅ Safe |
| Log into Gmail / email | 🚨 High Risk | ✅ Safe | ✅ Safe | ✅ Safe |
| UPI / banking / payment | 🚨 **Never** | ⚠ Use with caution | ✅ Safe | ✅ Safe |
| School work / Google Docs | ⚠ Risky | ✅ Safe | ✅ Safe | ✅ Safe |
| Streaming / watching videos | ⚠ Mildly risky | ✅ Safe | ✅ Safe | ✅ Safe |
| Sending OTP / passwords | 🚨 **Never** | ✅ Safe | ✅ Safe | ✅ Safe |

**Q2.**

**Look at the "UPI / banking / payment" row. Why is Public Wi-Fi + VPN marked "use with caution" rather than fully safe — even though the VPN encrypts your data?**

*Write in your notebook — hint: think about what happens if the VPN itself is compromised or drops mid-session.*

## 🎭 Story Continues — Scene 2 · "Actually, It Happens All the Time"

### 📍 Scene 2 — Same Café · Aryan Demonstrates What an Attacker Can See

I'll show you without using a real network. This is what a packet capture looks like on an unencrypted Wi-Fi — every device's traffic visible in plain text.

ARYAN

NAMAN

Wait — you can see usernames and passwords? Just like that? No hacking needed?

On HTTP sites — yes, instantly. On HTTPS sites — harder, but a Man-in-the-Middle attack can still intercept session tokens, which lets attackers *stay logged in as you* even without your password.

PRIYA

## 🔒 Wait — Does HTTPS Protect Me on Public Wi-Fi?

### ✅ HTTPS — What It Protects

- ✅ Encrypts **content** of your messages, passwords, and data between your the device and the website
- ✅ Prevents basic eavesdropping on page content
- ✅ Verifies the website is who it claims to be (certificate)

### ❌ HTTPS — What It Does NOT Protect

- ❌ Does NOT hide **which websites** you're visiting (DNS is visible)
- ❌ Does NOT protect against **session hijacking** via stolen cookies
- ❌ Does NOT protect you from a **fake certificate** on an Evil Twin network
- ❌ Does NOT encrypt your full connection — only the HTTPS portion

### 📊 Let's Assume — What the Data Might Show

*Illustrative figures to help you think about the scale of the risk.*

**~1 in 4**
public Wi-Fi users may have had data intercepted or accounts compromised while on an open network

**68%**
of students surveyed connected to public Wi-Fi at cafés or malls without checking the network name

**Airport & Mall**
Wi-Fi networks are the most targeted locations for Evil Twin attacks — high footfall, low awareness

**Only 12%**
of Indian mobile users in a study regularly used a VPN when connecting to public Wi-Fi

**Q3a.**
**The "68%" figure and the "Only 12%" figure together tell a story. What gap do they reveal — and why is this dangerous?**
*Write in your notebook*

**Q3b.**
**Why are airports and malls particularly high-risk locations for Evil Twin attacks? Think about the type of person using the network and what they might be doing.**
*Write in your notebook*

### 🔍 Go & Find — Explore Beyond This Page

The figures above are illustrative — but real incidents happen all the time. Your task: **go search, read, and bring back something real.**

**🔎 Search & Read**
Search: *"public Wi-Fi hack India"* or *"Evil Twin attack café India"*. Find one real news article or report. Write in your notebook: What happened? Where? How did the attacker get in?

**📊 Find the Real Data**
The figures on this page are illustrative. Search: *"public Wi-Fi risk statistics India"* or *"CERT-In Wi-Fi advisory"*. Find one real statistic — write the source, the number, and what it means.

**💬 Share & Compare**
Share what you found with one classmate. Did you find the same story or different ones? Write: one thing your classmate found that surprised you — and why.

📓 **In your notebook, write:** Article/source you found · The key fact · One sentence on how it connects to what Naman almost did in this chapter.

## What You Can Do — Safer Alternatives & Protective Habits

*"So what do we actually do at a café?" asks Meera. Aryan pulls up his checklist.*

### Aryan's Public Wi-Fi Safety Rules

1. **Verify the network name before connecting**
   Ask staff for the exact Wi-Fi name. Never guess or pick the strongest signal.
2. **Never do banking or UPI on public Wi-Fi**
   Use mobile data or your hotspot for payments. No exceptions, even on HTTPS.
3. **Use a VPN for everything else**
   Free options: Proton VPN (no data cap), Windscribe. Turn it on before connecting. All traffic encrypted.
4. **Use your hotspot for sensitive tasks**
   Your phone's hotspot is private — only you control it. Switch to hotspot for logins, email, or anything sensitive.
5. **Turn off Wi-Fi when not using it**
   Your device auto-connects to known networks — even fake ones with matching names. Off = no risk.
6. **Enable "Forget Network" after use**
   Stop your device from auto-reconnecting to public networks next time. Settings → Wi-Fi → Forget.

**Activity 2 — Habit Sort**

### Safe or Risky? Sort These Behaviours

Sort each behaviour into the correct zone — then answer Q4.

1. Check Wi-Fi name with café staff before connecting
2. Use your bank app on airport Wi-Fi — it's HTTPS, so it's fine
3. Turn on ProtonVPN then connect to café Wi-Fi
4. Click "Connect" on "FreeWiFi_Mall" without asking anyone
5. Switch to mobile hotspot to send your UPI payment
6. Leave Wi-Fi on when walking through a market
7. Forget the public network from Settings after leaving the café
8. Enter your school login password on unprotected café Wi-Fi

**Safe Habit**

*Write numbers here...*

**Risky Habit**

*Write numbers here...*

**Q4.**

**Habit 2 says "It's HTTPS, so it's fine." Using what you learned on page 4 about what HTTPS does NOT protect, explain specifically why this is still risky on public Wi-Fi.**

*Write in your notebook*

## ⚖️ Read the Situations — What Would You Do?

Read each situation. Write in your notebook: (a) Safe ✅ or Risky ⚠️ · (b) What is the specific danger? · (c) What should the person do instead?

**Situation 1 — Naman, Metro Station**

Naman is at a Delhi Metro station and needs to check his marks on the school portal. He sees "DelhiMetro_FreeWiFi" with full signal. He quickly logs in with his school username and password to download his report card.

**Situation 2 — Kavya, Airport**

Kavya is at Delhi airport waiting for a flight. She needs to pay ₹2,400 for a hostel booking. She connects to "IndiGo_Lounge_Free" (she flew IndiGo) and opens her UPI app. The payment fails twice and she retries, entering her PIN both times.

**Situation 3 — Meera, Library**

Meera is at the public library. She needs to access her email for a teacher's assignment. She turns on ProtonVPN first, then connects to "Library_Public_WiFi" (verified at the front desk), opens her email, downloads the attachment, then disconnects and forgets the network.

**Situation 4 — Rohan, Shopping Mall**

Rohan is at a mall. He needs to send a file to his teacher on WhatsApp. His data is almost finished. He sees two networks: "Mall_WiFi_Official" and "MallFreeWiFi" — both with similar signal strength. He connects to "MallFreeWiFi" because it's slightly stronger.

**Activity 3 — Quick Questions**

### ✏️ Choose the Correct Option

**Q5a.**
**Which of the following is the SAFEST way to make a UPI payment when you're away from home?**

- ◯ Use café Wi-Fi — it's HTTPS so it's encrypted
- ◯ Use airport Wi-Fi — it's a large official network
- ◯ Use your phone's mobile hotspot or mobile data directly
- ◯ Use any Wi-Fi as long as you turn on Aeroplane Mode first

**Q5b.**
**Your device auto-connects to "Café_Free" when you walk past a café. This is dangerous because:**

- ◯ It uses up your battery faster
- ◯ An attacker could have set up a network with that same name to intercept your auto-connection
- ◯ Public Wi-Fi always contains viruses that install automatically
- ◯ The café can see your WhatsApp messages

**Q5c.**
**A VPN protects you on public Wi-Fi primarily by:**

- ◯ Blocking the public Wi-Fi from seeing your device
- ◯ Encrypting all your traffic so anyone intercepting it sees only unreadable data
- ◯ Detecting Evil Twin networks before you connect
- ◯ Making your connection faster and more stable

**Q5d.**
**Which of the following is the BEST indicator that a Wi-Fi network is safe to use?**

- ◯ It has a strong signal and fast speed
- ◯ It requires a password to connect
- ◯ The name was verified with staff and you're using a VPN
- ◯ It shows a padlock icon next to the name

## 🧠 Deep Analysis — Complex Case

### 📋 The Coffee Shop Incident

Let's assume: Preethi, a Class 12 student in Chennai, was studying at a café for 3 hours using the café's free Wi-Fi. She had a busy session — logged into her school portal, downloaded a PDF, checked Gmail twice, browsed YouTube, and quickly transferred ₹500 to a friend using PhonePe. She didn't notice anything wrong. Two days later, she got a notification: someone had logged into her school account from Hyderabad and changed her assignment submissions. Her Gmail also showed a login from an unknown device. Her PhonePe was untouched. She told her parents: "I didn't click anything suspicious — I was just using the Wi-Fi."

**Q6a.**
**Preethi's school account and Gmail were compromised, but her PhonePe was not. Using what you know about HTTPS and session tokens, explain how both accounts could have been stolen without her password being visible — and why PhonePe may have been safer.**
*Write in your notebook — 3–4 sentences*

**Q6b.**
**Preethi said "I didn't click anything suspicious." Is this a valid defence? What does this chapter teach us about the relationship between user action and public Wi-Fi risk?**
*Write in your notebook — 2–3 sentences*

**Q6c.**
**Redesign Preethi's 3-hour café session so it is safe. List the exact steps she should have taken — before connecting, during her session, and after leaving — to prevent what happened.**
*Write in your notebook as a numbered checklist*

**Pause & Reflect**

### The Convenience Trap

Free Wi-Fi is one of the most tempting everyday shortcuts — and one of the easiest ways to create a serious security risk without realising it. Think about the last time you connected to public Wi-Fi. Did you verify the name? Did you check what you were doing on it? Most people don't — not because they're careless, but because the risk is **invisible**. No pop-up warns you. Nothing looks wrong. The danger is entirely silent.

In your notebook: Is "free" worth the risk — or is paying for extra mobile data a form of security spending? Write 2–3 honest sentences.

**Return to Page 1 — Revisit Your Habits**

### What Has Changed?

Go back to your tick table on Page 1. Look at your ❌ column.

**Q7.**
**For each ❌ you ticked on Page 1 — write in your notebook: (a) What specific risk does this habit create? (b) Which of Aryan's 6 rules fixes it? (c) Will you change this habit — and when?**
*Be honest — compare your first answers to what you know now*

## Epilogue — Back at the Café, 30 Minutes Later

**Naman**

"I disconnected, verified the real name with the staff, and used my hotspot for the payment. ₹500 transferred — safely."

**Aryan**

"I turned on ProtonVPN before connecting to any public network. It's two taps. The convenience-to-risk ratio is impossible to ignore."

**Priya**

"After this chapter, I've set my phone to 'Ask to Join Networks' instead of auto-connect. Small change, big difference."

**Meera**

"First I skipped updates. Now I've been connecting to any Wi-Fi I see. This module is a mirror I didn't enjoy looking in."

## Key Takeaways

**Public Wi-Fi Is an Unencrypted Highway**
Anyone on the same network can intercept unencrypted data. Open networks have no encryption between your device and the router.

**Evil Twin Networks Are Real and Easy to Set Up**
A fake Wi-Fi network with a convincing name routes all your traffic through an attacker's device. Always verify network names with staff.

**HTTPS Helps — But Doesn't Fully Protect You**
HTTPS encrypts content but not DNS, session tokens, or your identity. A VPN encrypts your entire connection — use it on public networks.

**Hotspot Is Safer Than Any Public Wi-Fi**
For banking, UPI, or logins — switch to your mobile hotspot. You control it, only you're on it, no one can intercept.

**VPN = Encryption on Any Network**
Free options like ProtonVPN encrypt all traffic. Turn it on before connecting to public Wi-Fi. Interception yields only unreadable data.

**Forget Networks & Disable Auto-Connect**
Your device auto-joins saved networks — including fake ones with the same name. Forget public networks after use. Set to "Ask to Join."

### Aryan, Priya, Naman & Meera's Rule for Chapter 4

*"Free Wi-Fi isn't free — you pay with your data, your passwords, and your accounts. Verify the name. Use a VPN. Use your hotspot for anything sensitive. If you can't do any of those — don't connect."*

Safe Devices, Apps & Browsing · Module 2 · Chapter 4 → Next: Chapter 5 — Backup, Recovery & Data Protection