Attachments & Safe Handling

What is Malware?

- Malware = **Mal**icious Soft**ware**
- It is a harmful program made to ***damage*, *steal***, or ***control*** your device.
- Hackers often use social engineering to trick people into installing malware themselves.

Common Malicious Attachment Types

Attachments are files sent with emails. Cybercriminals often hide viruses, malware, or harmful scripts inside these files.

- A “fee_receipt.pdf.exe” file pretending to be a receipt.
- A Word file asking you to “enable macros”
- A ZIP file with unknown documents inside

If you don’t expect it… don’t open it!

Common Dangerous File Types

1. **.exe** → Programs (most dangerous)
2. **.zip / .rar** → Can hide malware
3. **.docm / .xlsm** → Macros enabled = risky
4. **.pdf** → Can contain malicious scripts
5. **.html / .htm** → Can redirect you to fake login pages

Just because a file *looks* normal, doesn’t mean it’s safe!

Safe Handling Rules (Student-Friendly)

⚠️ Before You Click:

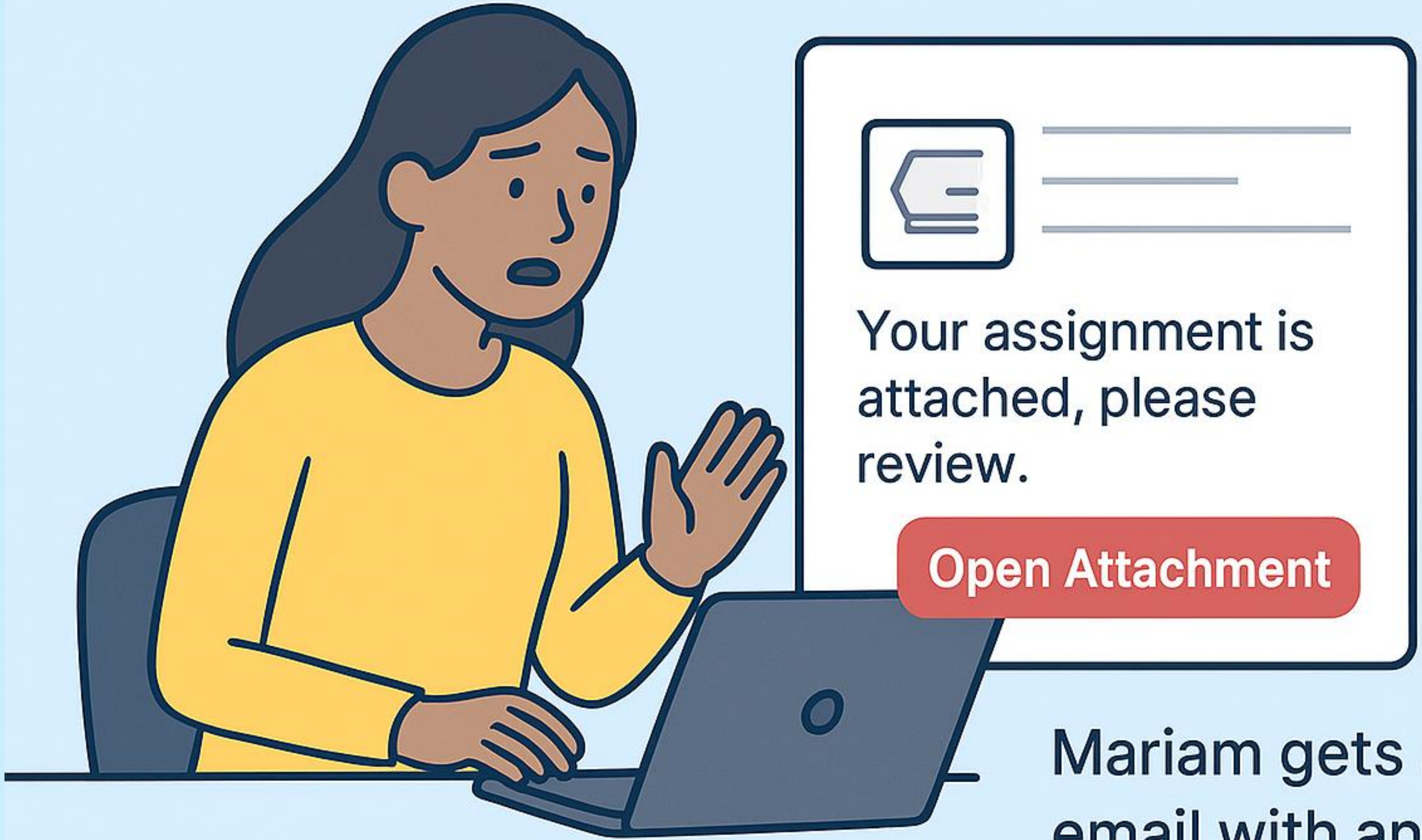
- Ask yourself: *“Was I expecting this file?”*
- Look at the name carefully
- Look for spelling mistakes in the email
- Check if sender’s email looks fake

🟢 Do This Instead:

- Preview file in online viewer if your system allows
- Upload suspicious files to **VirusTotal** (safe scanning)
- Delete if unsure — “Better safe than sorry”

Attachments & Safe Handling

How attackers use attachments — and how students can stay safe

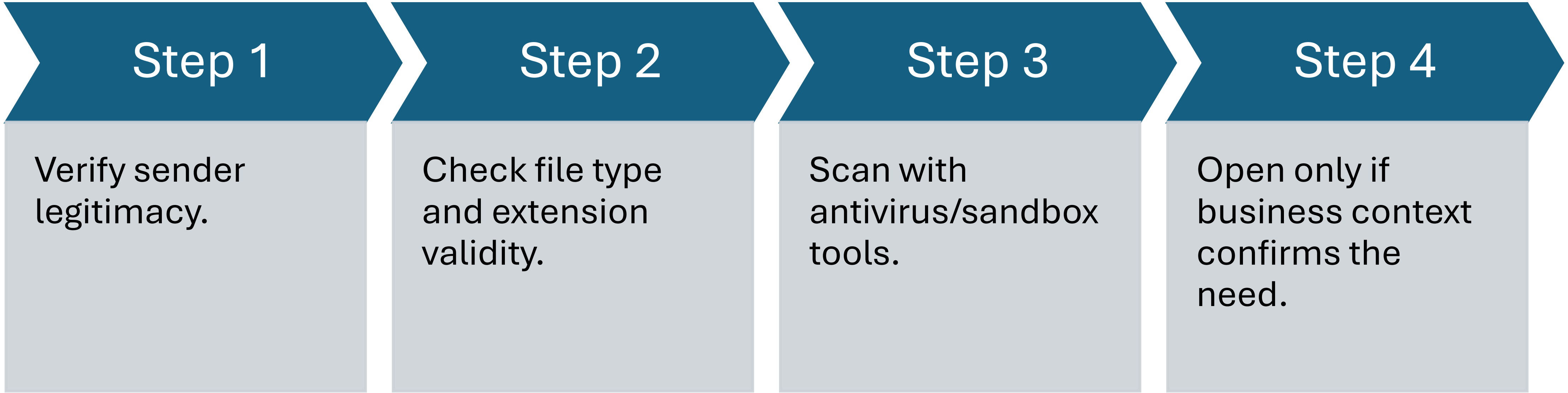


Your assignment is attached, please review.

If you don’t expect it... don’t open it.

Mariam gets an unexpected email with an attachment.

Attachment Handling Workflow



Step 1

Verify sender legitimacy.

Step 2

Check file type and extension validity.

Step 3

Scan with antivirus/sandbox tools.

Step 4

Open only if business context confirms the need.