1. USB DROP ATTACKS

Attackers leave infected USB drives in places like parking lots, elevators, or office hallways, making them look lost or important. Out of curiosity or an attempt to return it, employees plug the USB into a work computer. Once connected, the USB automatically installs malware or opens a backdoor, giving attackers access to the system.

WHAT IS A USB DROP ATTACK?

Attackers leave infected USB drives in parking lots, elevators, or office areas

Curiosity or helpfulness leads employees to plug them into work devices

Scenario: Hassan Finds a USB in the Parking Lot

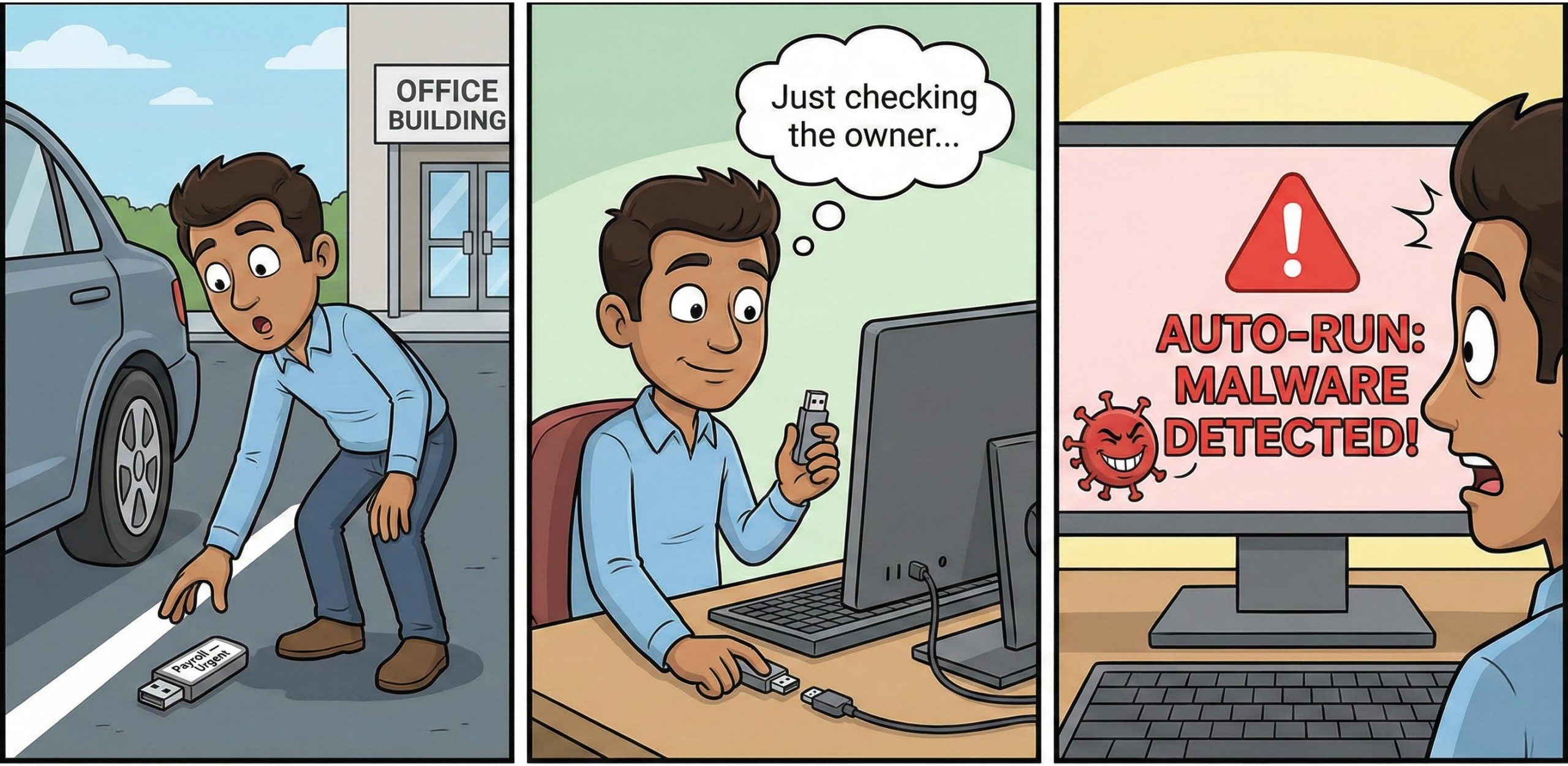
Hassan sees a USB labelled “PAYROLL Urgent” lying near the office entrance.

He plugs it into his workstation to “check who it belongs to.”

The USB auto-runs malware instantly, giving the attacker access to files and internal systems.

The label was intentionally designed to trigger urgency and curiosity.

Lesson: Never plug unknown USBs into work devices. Report found devices to IT so they can be checked safely.



USB Drop Attack: A Cautionary Tale

How USB Drops Trick Employees?

- Curiosity
- Desire to help return lost items
- Professional labels (Payroll, HR, Confidential)
- USB appears harmless

Red Flags Hassan Should Notice

- Unfamiliar USB device
- No reason for sensitive labels
- Device behaves oddly when connected
- Unexpected pop-ups

Prevention Tips

- Never plug unknown USBs into work devices
- Hand found devices to IT/security
- Disable auto-run on corporate systems
- Use hardware restrictions on USB ports