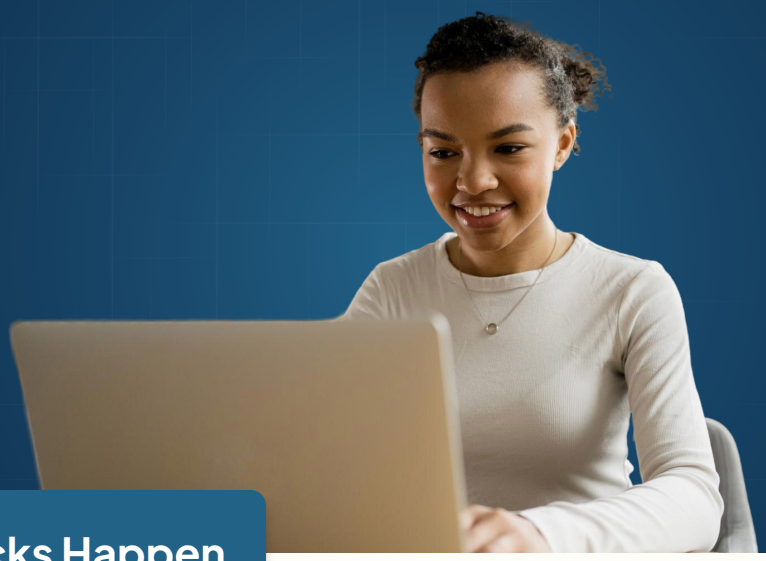
USB & Removable Media Risks

USB sticks and other removable media are convenient tools for transferring files, but they also pose serious security risks if misused. Attackers often exploit curiosity or convenience, turning these small devices into powerful entry points for malware.



How Attacks Happen

Infected USB Drops

Cybercriminals sometimes leave infected USB sticks in offices, car parks/parking lots, or public places. When someone plugs one in out of curiosity, malware can install automatically and give attackers access to the company network.

Tip: *Never plug in an unknown or "found" USB device.*

Unapproved Devices

Using personal or unencrypted USB drives for work data can expose sensitive information if the device is lost, stolen, or compromised.

Tip: *Only use encrypted, company-approved removable devices for storing or transferring files and an approved method for deleting the sensitive data after use.*

Auto-Run Exploits

Some malware takes advantage of auto-run settings, launching as soon as the USB is connected. This can infect machines instantly, often without the user realising it.

Tip: *Disable auto-run features on your computers.*

Suspicious Devices

Even a USB device that looks legitimate could be tampered with or compromised. One careless connection could put an entire network at risk.

Tip: *Report any suspicious or unexpected USB devices immediately.*