Juice Jacking - What it is, why public USB is risky, and how to charge safely

Gridinsoft Help Center

What it is

Juice jacking is when a public USB charging port is used to steal data or install malware on your phone or tablet. The same cable that carries power can carry data - a tampered port or cable abuses that to poke your device.

How it works - quick tour

- A malicious kiosk or cable offers power but also exposes a data connection.

- Your device trusts the port and may mount storage or accept commands.

- Attackers can grab files, scrape tokens, or drop spyware in seconds.

What you may notice

- A prompt asking to trust this computer when you only wanted to charge

- File transfer mode turning on by itself

- Odd behavior after charging - new profiles, rapid battery drain, unknown apps

Prevent it

- Use your own wall charger or a USB data-blocker (charge-only adapter).

- Carry a power bank for airports, hotels, and conferences.

- If you must use public USB, deny trust prompts and keep the screen locked.

- On Android, set default USB to Charge only. On iOS, enable Lockdown Mode if appropriate and keep the device locked while charging.

- Keep your OS updated and avoid sideloading from unknown sources.

If you already plugged in

- Unplug immediately if a trust prompt appears.

- Reboot your device and run a mobile security scan.

- Review installed apps, device admin, accessibility, VPN, and MDM profiles - remove anything unknown.

- Change passwords from a clean device and revoke suspicious sessions.

- Watch accounts for unusual logins or 2FA prompts.