Travel Cybersecurity Checklist

Checklist · Before, During, And After Your Trip.

Travel turns your devices into high-value targets. Hotel Wi-Fi, airport networks, public computers, lost luggage — this checklist covers the realistic risks at each stage.

Before You Leave (15 Min)

- Operating systems updated on every device you're taking.
- Backups completed for each device (so a loss is recoverable, not catastrophic).
- Find My / Find My Device confirmed working.
- VPN installed and tested before departure.
- Set Up bank/card travel notifications (so legitimate transactions abroad don't get blocked).
- Photocopy or photograph passport/ID — store securely (encrypted cloud, not in 'Downloads').
- Reduce the wallet to essentials — leave Social Security card, secondary cards at home.
- Set out-of-office on email if the hijack window matters for your work.

Devices To Bring (Or Not)

- Travel laptop ideally has minimal data — clone of necessary work, not full archive.
- Don't bring devices you can afford to lose: drop count = 4× normal during travel.
- Travel adapters bought from reputable brands (cheap ones can damage devices).
- Power bank charged and tested.
- Cables checked for fraying / tampering.

Public Wi-Fi Rules

- VPN ON before connecting to any unfamiliar network.
- Verify network names with venue staff — beware impostor 'Free_Hotel_WiFi.'
- Auto-join unknown networks DISABLED (Settings → Wi-Fi → Auto-Join Hotspot off).
- Sensitive activities (banking, password changes) deferred to trusted networks or cellular.
- Public charging cables — use a 'USB data blocker' or your own cable into a wall adapter.

In Hotels

- Use the room safe for passports, backup phone, sensitive documents.
- Don't leave laptops or tablets visible when you're out.
- Door peepholes / privacy seal apps on laptops to prevent shoulder surfing.
- Cover laptop webcam when not in use.
- Know how to remote-wipe each device in case it's stolen.

Crossing Borders

- Devices powered OFF before crossing (forces full cold-boot, harder to forensic).
- Long passcodes preferred over biometrics at borders (some jurisdictions can compel biometrics, not memorised passcodes).
- Sensitive documents stored encrypted offsite — accessible from a clean travel device.
- If high-risk: travel with burner phone and burner laptop, restore at destination.

After You Return

- Change passwords used on travel devices (especially if used on questionable Wi-Fi).
- Run malware scans on all travel devices.
- Review bank and card statements for the full trip.
- Reset travel notifications on cards.
- Restore from backup if any device showed unusual behaviour.