

Travel Wi-Fi Safety Checklist

Stay safe on public and hotel Wi-Fi — a quick pre-trip checklist for remote workers and travelers.

From the TechODash Remote Work Security series. Run through this before every trip.

BEFORE YOU LEAVE

- **VPN app is installed and tested on every device you're bringing**
Confirm it actually connects before you're relying on it from an airport or hotel room.
- **Two-factor authentication is active on accounts you'll access while traveling**
Prefer an authenticator app or hardware key — it works even without cell signal.
- **Important files are backed up before departure**
A lost or stolen device while traveling shouldn't also mean lost work.

WHILE CONNECTED

- **VPN is active before doing anything sensitive on public Wi-Fi**
Hotel and airport networks are shared and easy to eavesdrop on without one.
- **Network name is verified with staff before connecting**
A fake hotspot with a similar name is a common trick — ask at the front desk if you're unsure.
- **Auto-connect to open Wi-Fi networks is turned off**
Prevents your device from silently joining an unfamiliar or spoofed network on its own.

DEVICE HYGIENE

- **Full-disk encryption and a screen lock are both active**
Protects your data specifically in the scenario travel makes more likely: a lost or stolen device.
- **Public USB charging ports are avoided in favor of your own charger**
A compromised public charging port can potentially access data on a connected device.

WANT TO GO DEEPER?

The SOHO 2026 Guide covers the full picture: network architecture, device segmentation, remote work security, and AI scam defense — with checklists and templates for home offices and small businesses.

soho2026.gumroad.com//soho-2026