

# Sentry — VPN Safety Checklist

Setup checks before you connect to any VPN — including server, protocol, and kill-switch verification.

## Before you leave

- Update OS, browser and key apps. Reboot.

*You don't want a 90-minute security update queued on hotel Wi-Fi.*

- Confirm full-disk encryption is enabled on every device you're taking.

*If a device is stolen, encryption is what stops it from being a data breach.*

- Take only the data you need. Move the rest to encrypted backup at home.

*Less on the device = less to lose. This is also helpful at borders.*

- Carry recovery codes for 2FA on a separate piece of paper, not on the same device.

*If your phone is lost or stolen, codes on it won't help you recover.*

- Tell your bank you're travelling, and add an alternate contact method.

*Locked-out-of-banking is the worst flavor of locked-out.*

## On the road

- Avoid logging into sensitive accounts from public computers.

*Hotel and business-center machines are the textbook keylogger scenario.*

- Treat all hotel and conference Wi-Fi as untrusted: use HTTPS-only mode and a reputable VPN.

*VPN moves the trust to your provider; pick one whose policies you've actually read.*

- Disable Wi-Fi auto-join for unknown networks and turn off Bluetooth when you're not using it.

*Auto-join networks named 'attwifi', 'xfinitywifi', etc. is a known phishing trick.*

- Use your phone's mobile hotspot instead of public Wi-Fi when feasible.

*Carrier networks aren't perfect, but they aren't 'whatever-was-named-Starbucks-in-the-airport'.*

- Lock your devices physically when leaving the hotel room (cable lock or hotel safe).

*Most hotel-room theft is opportunistic. A small barrier solves most of it.*

## At borders

- Know the data-handling laws in the country you're entering.

*Rules differ widely on whether you must unlock devices. Plan in advance.*

- Consider travelling with a clean device and accessing data only when needed.

*Common practice for journalists, lawyers, and anyone whose work touches sensitive sources.*

- Power devices off (not just sleep) before crossing a border.

*Cold-boot encryption is stronger than hot-state encryption on most platforms.*

## After you return

- Review account login history on email, password manager, banking and SSO.

*Catch unfamiliar locations or devices early.*

- Rotate any credentials you typed into a public or untrusted machine.

*Better to rotate proactively than wonder later.*

- Update and reboot devices again. Apply anything that landed while you were away.

*Closes any gaps that opened during the trip.*

Educational content from Sentrly (<https://www.sentrly.com>). Free to share with attribution. Verify time-sensitive details on the relevant vendor site.