THREATS LIBRARY

JULITH GmbH
Awareness-as-a-Service

Remote work & travel — when the office is everywhere

Home office, co-working spaces, airport lounges — every location brings its own risks. We provide concrete routines for travel, public Wi-Fi, meeting rooms, and home networks.

min read: 7 min **Updated:** 14 March 2026 **Risk:** Medium risk
Source: awareness-as-a-service.com/en/resources/threats/remote-travel

What do remote work and travel mean for security?

The spread of remote work has definitively dissolved the security perimeter. The corporate network no longer ends at the patch panel in the server room — it extends into every home, co-working space, and airport lounge chair. This creates attack surfaces that simply did not exist in classic office operations.

Three problems stand out: **insecure networks** (public Wi-Fi without encryption or with rogue hotspots), **physical exposure** (shoulder surfing, device loss), and **home network risks** (personal routers with outdated firmware, family members on the same network segment).

On travel, these risks compound: time pressure, unfamiliar environments, and the temptation to use available infrastructure (public USB charging stations, conference Wi-Fi) without checking lower alertness. Attackers know these patterns and deliberately target airports, hotels, and conferences.

At a glance

01

VPN is not optional

A consistently-used corporate VPN encrypts traffic even in insecure networks and prevents attackers on the same Wi-Fi from reading data in transit.

02

Juice jacking is real

USB charging cables at public stations can transfer data or install malware. USB data blockers (charge-only adapters) are a simple countermeasure.

03

Visibility is the biggest home-working risk

Shoulder surfers in trains or co-working spaces see confidential content not through technical compromise, but simply because the screen is readable from the side.

How to recognise remote and travel security risks

Unassigned Wi-Fi hotspots
"FreeAirportWifi" or "Hilton_Lobby" without a captive portal, not announced by any hotel or airport, could be an evil-twin hotspot.

Shoulder surfing
Someone nearby is persistently positioned at a favourable angle for your screen — or is pointing their phone in the direction of your display.

USB charging stations without a mains adapter
Stations that offer only USB cables (no power plug) may also transfer data. Use your own charger or a power bank instead.

Meeting rooms with pre-installed cables
HDMI or USB-C cables pre-installed at conference room displays could exfiltrate data (so-called O.MG cables).

Hotel Wi-Fi without a captive portal
A hotel Wi-Fi that connects immediately without any authentication may not be the legitimate hotel network.

A temporarily "misplaced" device
A laptop or phone briefly left unattended in a hotel or at a conference may have been compromised in the interim — an evil maid attack.

How to protect yourself

For employees

- **Keep VPN active at all times** in public or unknown networks — including for email, not just for file server access.
- **Privacy screen filter on your laptop** when travelling: a modest investment that prevents shoulder surfing on trains, planes, and in co-working spaces.
- **No USB from unknown sources:** Neither charge from unknown USB ports without a data blocker, nor connect unfamiliar USB drives to your own devices.
- **Be sceptical of conference cables:** Bring your own HDMI/USB-C cable for presentations.
- **Report device loss immediately** — not after you get home. Every hour matters for remote wipe and access revocation.

For administrators

- **Corporate-wide VPN with always-on configuration:** Employees should not have to decide when to activate it.
- **Mobile Device Management (MDM) with remote wipe** for all mobile devices holding corporate data.
- **Endpoint encryption (BitLocker, FileVault)** on all devices — mandatory, not optional.
- **Travel laptops for high-risk countries:** For travel to countries with elevated espionage risk, issue clean devices without sensitive data.
- **Understand split-tunnelling risks:** Split tunnelling (only corporate traffic over VPN) improves performance but leaves personal traffic unprotected.

Real cases

CASE 01 · CONSULTING FIRM · DE · Q3/2025

A consultant worked on a proposal in a train. A fellow passenger discreetly photographed the screen with their phone and could read pricing details and customer names. The material appeared in a competitor's conversation shortly afterwards.

Damage: competitive disadvantage, client relationship damaged · **Detection:** client notification · **Lesson:** A privacy screen costs CHF 30. Never work on a proposal or contract on an unprotected screen in public transport.

CASE 02 · TECHNOLOGY START-UP · CH · Q4/2025

A developer used the "Conference_Guest" Wi-Fi at a trade event — which an attacker was running as an evil-twin hotspot. TLS connections were terminated with a forged certificate (MITM). Credentials for a code repository were intercepted.

Damage: repository compromised, sensitive code exfiltrated · **Detection:** anomalous login alert from a foreign country the next day · **Lesson:** VPN would have encrypted the traffic before it reached the hotspot.

What to do if it happens?

THE FIRST 15 MINUTES

1. **Disconnect from the network** (disable Wi-Fi, turn off mobile data) if an attack is suspected.
2. **Inform IT immediately** — especially for device loss or suspected data compromise.
3. **Trigger remote wipe** for a lost or stolen device — via IT, not the employee themselves.
4. **Change credentials** that were stored on the device or used in the session.
5. **Document a timeline:** Which networks were used, when, and what was done?
6. **Have the device forensically checked** before returning to use if an evil maid attack cannot be ruled out.

Frequently asked questions

Isn't HTTPS enough protection on public Wi-Fi?

Usually — but not always. Certificate-pinning gaps, self-signed certificates users click through, and DNS hijacking are real attack methods against which HTTPS alone provides incomplete protection. VPN is an additional layer.

Is a hotspot from a company phone safer?

Significantly safer than public Wi-Fi. A mobile hotspot via a company phone is the recommended alternative to unknown Wi-Fi networks when travelling.

What exactly is juice jacking?

The attack exploits USB connections that simultaneously carry power and data. A compromised charging station can read data or install malware. USB data blockers (power pass-through only) are a simple and inexpensive countermeasure.

Related topics

Remote work and BYOD are closely linked — personal devices on corporate networks create similar risks to unsecured networks while travelling.

Passwords and MFA become more critical when access no longer comes from a controlled network.