CHEAT SHEET | FOR SENIOR LEADERS WHO TRAVEL

Cyber hygiene for executive travel

Ten habits before, during and after a trip.



Brief it before every trip

Send this to the traveller and their executive assistant before every overseas trip. Hotel Wi-Fi, public chargers, airport lounges and borrowed screens are all openings.

01 **Travel light on data**
Pack a device holding only what the trip needs. ☐

02 **Update before you leave**
Patch laptop and phone the day before you fly. ☐

03 **Use the corporate VPN**
Never join hotel or lounge Wi-Fi without it. ☐

04 **Carry your own charger**
Avoid public USB ports. Bring your own plug. ☐

05 **Keep devices with you**
Never leave them in a hotel room or a car. ☐

06 **Guard the screen**
Use a privacy filter in lounges and on flights. ☐

07 **Report loss immediately**
Save the security team’s number before you fly. ☐

08 **Check on return**
Hand travel devices to IT after high-risk trips. ☐

09 **Lock accounts with app MFA**
Set up an authenticator app before you leave. ☐

10 **Watch what you say in public**
Keep sensitive calls out of lounges and taxis. ☐

Red flags

Spot these early and act on them

01 A laptop packed with files the trip never needs.

02 Updates still pending at the departure gate.

03 Hotel Wi-Fi joined ‘just to check email’.

04 A phone charging from a kiosk USB port.

05 Devices left in a hotel room or car boot.

06 Board papers open on a busy flight.

07 A lost phone reported the next morning.

08 A travel device back on the network unchecked.

09 Login codes sent by text to a roaming SIM.

10 Deal talk in a taxi or a lounge queue.

40% of regular public Wi-Fi users say their data was compromised.

Source: Forbes Advisor and OnePoll survey

Get the full set of cheat sheets at scottz.com