Remote Work & Travel Security

Scenario	Attack Vectors	Risks	Recommendations & Mitigations
Working from Home	🔥 Insecure home Wi-Fi 🔥 Shared network with household members and devices 🔥 Unpatched personal & IoT devices (Family malware downloads, Phishing emails) 🔥 Weak and breached passwords	⚠️ Lateral movement from infected home device to corporate device ⚠️ Data leakage ⚠️ Credential theft	✅ Change default router credentials ✅ Use WPA3 encryption for home Wi-Fi ✅ Disable wireless admin access and use direct ethernet connection ✅ Segment home network (separate networks for work and family) ✅ Use a company VPN for corporate access if available ✅ Educate household members on safe online behavior
Device Sharing	🔥 Unauthorized use of corporate device by family 🔥 Download of unapproved & risky software	⚠️ Accidental data exposure ⚠️ Malware infection ⚠️ Policy violation	✅ NEVER share your corporate device with anyone!
Traveling - Hotel/Airport/Cafe Wi-Fi	🔥 Man-in-the-middle (MitM) attacks 🔥 Fake hotspots 🔥 DNS spoofing 🔥 Credential theft	⚠️ Data interception/loss ⚠️ Session hijacking ⚠️ Compromise of corporate credentials	✅ Do not use open or public Wi-Fi ✅ Use a dedicated mobile hotspot or a mobile phone internet sharing via Wi-Fi (tethering) ✅ Use trusted VPN before browsing or connecting to services ✅ Verify network names with hotel/venue staff before connecting ✅ Turn off Wi-Fi and Bluetooth when not in use
Traveling - Public Charging Stations	🔥 Juice jacking (malicious USB ports) 🔥 Data transfer via USB	⚠️ Malware injection ⚠️ Data theft	✅ Avoid public USB ports for charging or use USB data blockers (charge-only cables) ✅ Prefer AC power outlets over USB

Lost, Stolen or baited Devices	🔥 Theft during travel 🔥 Pickpocketing 🔥 Lost or delayed in taxi/hotel/airplane 🔥 Baited USBs	⚠️ Unauthorized access to corporate data ⚠️ Identity theft ⚠️ infiltration and Endpoint compromise	✅ Encrypt hard drives ✅ Use biometric and strong password protection ✅ Enable tracking and remote wipe ✅ NEVER insert unauthorized removable devices ✅ Notify IT immediately upon loss
Phishing & Social Engineering	🔥 Spear phishing targeting traveling employees 🔥 Fake security alerts 🔥 Malicious QR codes (Quishing)	⚠️ Credential compromise ⚠️ Malware installation	✅ Stay informed and complete all company cybersecurity training ✅ Use only company approved browser plugins ✅ Inspect all emails and links ✅ Do not scan public QR codes
Weak Private Device Hygiene	🔥 Outdated, vulnerable, unpatched OS or software 🔥 Lack of endpoint protection (Antimalware)	⚠️ Malware infections ⚠️ Exploits and RCE attacks ⚠️ Credential compromise	✅ Use trusted and updated Antimalware solution ✅ Regularly/auto update all Software and Firmware ✅ Disable unnecessary services and ports

🔐 General Recommendations (Applies to All Scenarios)

✅ **Stay vigilant and informed** about cyber threats, safe remote practices, phishing detection, and secure travel tips

✅ **Keep Your Device's Operating System, Firmware and Applications Up to Date**

✅ **Use MFA and VPN** whenever available

✅ **Use Endpoint Protection and MDM** to manage threats, enforce policies and enable remote wipe

✅ **Use DNS and WEB filtering** to block malicious domains and websites

✅ **Use regular instead of admin account** for daily work

✅ **Report anything unusual to your IT/Information Security** (abnormal login and access behavior)

✅ **Back up data** regularly (use the 3-2-1 backup strategy)