Cybersecurity Checklist for Traveling Employees

Before You Travel

- Back up important files and store them securely.
- Update all devices (laptops, phones, tablets) with the latest security patches.
- Enable device encryption on laptops and mobile devices.
- Set strong PINs/passwords and enable biometric login where possible.
- Pack only the devices you truly need for work.
- Ensure Multi-Factor Authentication (MFA) is enabled on all work accounts.
- Alert IT about your travel plans in case support is needed.

While Traveling

- Avoid public Wi-Fi (use a VPN if you must connect).
- Never charge devices at public USB charging stations—use your own charger.
- Keep devices physically with you (don't leave them unattended in hotel rooms or cars).
- Be alert to shoulder surfing in airports, cafes, or conferences.
- Disable Bluetooth and Wi-Fi when not in use.
- Don't share sensitive work conversations in public areas.
- Lock your screen every time you step away.

After Returning

- Run a full antivirus/malware scan on all devices.
- Change any passwords you used while traveling, especially if connected to public Wi-Fi.
- Upload all work files to secure company storage—avoid keeping them on your device.
- Report any lost/stolen devices immediately to IT.
- Check accounts for unusual login activity.

Reminder: Traveling increases cyber risk. Treat your devices like your passport — always secure, never shared, and monitored closely.

1218 Amber Drive • 345-2900 • 1-800-465-3933 • sales@teleco.ca • Teleco.ca

TELECO
Integrating Technologies