CYBER HYGIENE *for Business Travel*

DASHBOARD

BEFORE

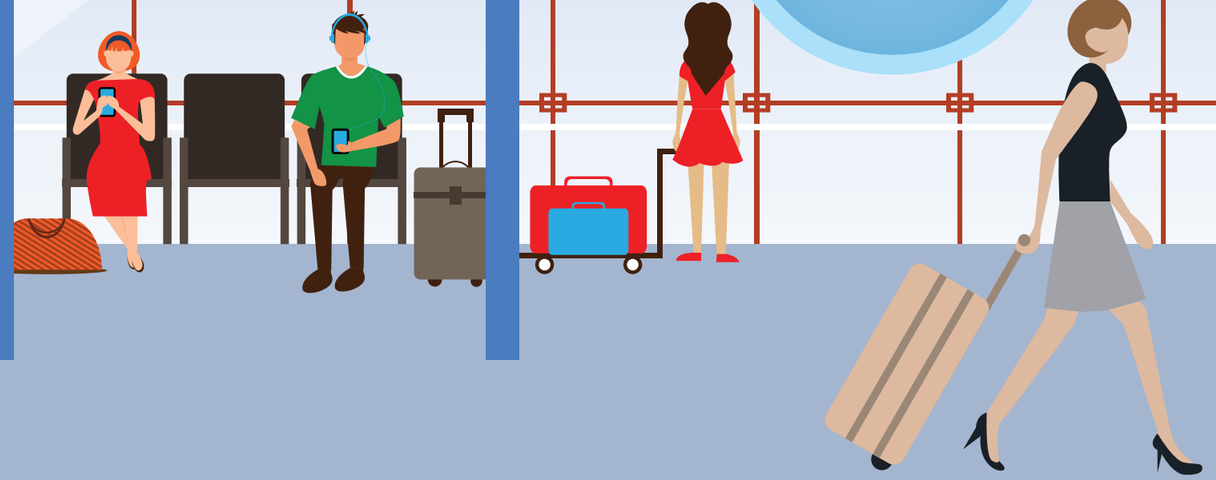
- Disable features such as Bluetooth and wireless headset capabilities.
- Remove unnecessary data.
- Only take the devices that are necessary to do the job.
- Change your passwords before you leave.
- Back-up your important data.

DURING

- Keep your device in your possession at all times.
- Power off devices while going through customs or other inspections points.
- Change your passwords at regular intervals on mobile devices and frequently used applications and websites.
- Empty your Trash and Recent folders after every use.
- Clear your browser after each use.
- Be aware of your surroundings and who might be able to view your screen or keyboard.
- Do not use the remember me feature on websites.
- Do not use public Wi-Fi networks.
- Do not store or communicate information above the approved classification of the device.
- PIN-to-PIN messaging is not suitable for exchanging sensitive information and is not protected by security settings.
- Do not open emails, attachments or click on links from unknown sources.
- Contact your IT Security department if your device is stolen, misplaced or if you suspect a security concern.

AFTER

- If your device was not in your possession for any reason or if you suspect a security concern, report this information to your IT Security department.
- Change the passwords on your devices and on any online services you accessed while abroad.



Sources: Canadian Centre for Cyber Security