DATA PROTECTION IN OFFICE

Preventive and protective actions

- Practice good password management
- Back up your data regularly, and make sure your anti-virus software is always up to date

Adopt simple cautious behaviours

- Never leave your devices unattended
- Constantly monitor your accounts for any suspicious activity and do not hesitate to report something suspicious
- Always be careful when clicking on attachments or links in email
- Sensitive browsing only on a device that belongs to you and on a network that you trust
- Be careful of what you plug in to your computer.

DISCLAIMER:
This pocket guide has been developed for educational purposes only. For more information, contact International SOS.

DATA PROTECTION WHILST TRAVELLING

BEFORE TRAVELLING

Research the **potential cyber threats** specific to the location.

Implement **adequate and effective security measures** to prevent issues whilst travelling.

Avoid advertising online the exact location/purpose of your business trip.

Ensure all software on your devices is **up-to-date.**

IN HIGH THREAT LOCATIONS

Maintain **continuous physical control** of your devices and sensitive information.

Keep your laptop with you as **carry-on luggage** and do not loan it to anyone while travelling.

When returning from a business trip or if you have witnessed suspicious activity on your devices, ask your **IT service desk to check for signs of cyber attack.**

Do not connect your devices to sensitive networks until they have been verified as safe.

WHILST TRAVELLING

Avoid connecting to **non-secure networks** (public WiFi hotspots).

Disable any WiFi and Bluetooth capabilities if possible.

CYBER SECURITY

Keeping your own and company information and devices safe and secure.

INTERNATIONAL SOS

Control Risks

THE COST OF CYBER ATTACKS

LLOYD'S: Global total cost of data breaches for businesses in 2015 was **$400 BILLION** and is expected to reach **$2.1 TRILLION** in 2019.

CONTROL RISKS' CYBER THREAT LANDSCAPE REVIEW 2017: In 2017, the relatively new method of deploying **MALICIOUS UPDATES TO SOFTWARE** already installed on organisations' computers has become one of the most dangerous methods used by cyber threat groups.

CONTROL RISKS' CYBER THREAT LANDSCAPE REVIEW 2017
264 SIGNIFICANT CYBER ATTACKS have been recorded between 1st January and 30th September 2017. In the same period, **75 COUNTRIES** have been impacted by cyber attacks.

Control Risks

CYBER SECURITY LANDSCAPE REPORT 2017

46% OF RESPONDENTS believe their organisation's board-level executives do not take cyber security as seriously as they should.

43% OF ALL RESPONDENTS reported a compromise or data breach in 2016.

37% OF I.T. AND BUSINESS professionals globally said employee education and awareness was their biggest cyber security challenge.

POINTS OF CYBER SECURITY VULNERABILITY FOR TRAVELLERS

- **Rogue Wi-Fi.** Wi-Fi hotspots in airport, hotel and other public places can be subject to packet sniffing attacks. These put at risk the confidentiality of communications being sent over that network. This may lead to credential theft and network breaches.
- **Eavesdropping.** Snooping, whether in person or through video, can lead to credential theft or sensitive data disclosures.
- **Theft of devices.** Opportunistic or organised theft of devices can lead to data breaches and sensitive data leaks. This may be carried out both by criminals and more advanced groups.
- **USB chargers.** These are supplied at public places for convenience but can be used to download and execute malware onto your devices.

TYPICAL CYBER ATTACK TECHNIQUES USED AGAINST TRAVELLERS

- **Data breach.** Theft of data due to limited security measures could lead to leaks of sensitive and reputation damaging information.
- **DDoS.** The use of a large number of infected devices that lead to slow or unresponsive web-facing devices and applications.
- **Ransomware.** Malware which encrypts data until a ransom is paid. Increasingly used as a smokescreen for deeper network intrusions.
- **Malicious updates.** Malicious requests for software or application updates. Hard to detect as installed malware runs in the background.
- **Phishing.** SMS and emails impersonating legitimate actors, usually involving malicious links or attachments used to install malware.
- **Unauthorised access.** Using stolen credentials or using brute force attacks (guessing username and passwords) to gain access to a network or device. Has been the highest threat score in the past 2 years due to its potential for privilege escalation and lateral movement.
- **Financial fraud.** Usually delivered through pishing emails. Used to lure victims into making illegitimate payments or redirect legitimate payment details into criminal accounts.