CYBER SECURITY

IN OFFICE

Preventative and protective actions
- Change passwords regularly and avoid reusing passwords
- Back up your data regularly, and make sure your anti-virus software is always up-to-date

Adopt simple cautious behaviours
- Ensure devices are powered down or securely locked if left 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
- Be careful of what you plug in to your computer

CYBER SECURITY WHILE TRAVELLING

BEFORE TRAVELLING

- Research the potential cyber threats specific to the location.
- Minimise the number of devices you take with you and remove any unnecessary or highly sensitive data prior to your trip.
- 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 a cyber attack.
- Use the ‘forget network’ setting if you did connect to any public Wi-Fi networks.

WHILE TRAVELLING

- Avoid connecting to insecure Wi-Fi networks. When necessary, use a Virtual Private Network (VPN) to protect your data.
- Limit location tracking and turn off Wi-Fi and Bluetooth when not in use.
THE COST OF CYBER ATTACKS

**Data breach.** Theft of data due to limited security measures could lead to leaks of sensitive and reputation damaging information.

**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 two years due to its potential for privilege escalation and lateral movement.

**Financial fraud.** Usually delivered through phishing emails. Used to lure victims into making illegitimate payments or redirect legitimate payment details into criminal accounts.

**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.

**IPSOS MORI:** AROUND A THIRD (32%) of businesses report having cyber security breaches or attacks.

POINTS OF CYBER SECURITY VULNERABILITY FOR TRAVELLERS

- **Insecure Wi-Fi.** Public Wi-Fi networks in airports, hotels and other spaces are insecure, easily allowing access for cyber criminals.
- **Surveillance.** 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.

BUSINESS TRAVELLERS ARE MORE LIKELY to fall victim to a data breach than a mugging while abroad.

TYPES OF THREAT ACTOR

**Cyber Criminals:** The primary motivation is financial gain. Cyber criminals have grown in technical and operational sophistication, and are a pervasive threat to organisations holding large amounts of personally identifiable information or payment details. This information allows cyber criminals to profit from fraudulent activity or reselling data.

**Nation States:** Typically the most sophisticated of the cyber threat actors, professional government or government-backed groups use advanced tactics to gain a foothold on systems to obtain sensitive information from their victims or meet intelligence requirements from their ‘customers’. Victims can be foreign state institutions or private organisations.

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.
- **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 two years due to its potential for privilege escalation and lateral movement.
- **Financial fraud.** Usually delivered through phishing emails. Used to lure victims into making illegitimate payments or redirect legitimate payment details into criminal accounts.