

| Key Threats Associated With Travel

- **Social Engineering:** When a threat actor attempts to manipulate a target into compromising personal or enterprise security through techniques such as phishing.
- **Unsecure Hotspots:** Threat actors can often host bogus Wi-Fi hotspots or attempt to hack legitimate but poorly secured public networks to collect data or deliver malware.
- **Juice Jacking:** A security exploit in which an infected USB charging station is used to compromise connected devices.
- **Keylogging:** A type of malware or hardware used to capture someone's activity on a device, often public, without the permission or knowledge of the user.
- **ATM Skimming:** When devices are illegally installed on ATMs and point-of-sale terminals to capture data or record cardholders' PINs.
- **Shoulder Surfing:** A physical risk to privacy whereby a threat actor can view the device screen and keypad to obtain personal information.

| Recommendations for Travel

BEFORE

- ➔ Update software and apps on all devices, including antivirus programs and internet browsers.
- ➔ Backup all data and sanitize devices; travel only with essential information.
- ➔ Consider applying privacy screen filters to devices to prevent shoulder surfing.
- ➔ Enable multi-factor authentication, ensuring methods do not require an SMS message as the second factor; alternatives include authenticator apps, hardware tokens, and biometric checks.

DURING

- ➔ Consider traveling with a sanitized burner phone, particularly if intending to purchase a local SIM card.
- ➔ Use a trusted VPN connection, encrypted messaging, and private browsing modes; check encryption laws before traveling.
- ➔ Disable auto-connect features, Bluetooth, GPS, and Near Field Communication when not in use.
- ➔ Limit social media use while business traveling, particularly the sharing of locations.
- ➔ Do not use public machines or wireless networks when accessing sensitive data.
- ➔ Use personal charging equipment plugged into standard power outlets and charging points.
- ➔ Do not interact with any suspicious links, and delete emails and SMS messages from unknown sources.
- ➔ Never leave devices unattended, including in luggage, storage, or hotel safes.
- ➔ Exercise caution when using third-party devices gifted during events or conferences, such as USB sticks.

UPON RETURN

- ➔ Scan for viruses, update software, and change passwords on all devices and accounts used while traveling.
- ➔ Report unusual device performance issues or any suspected security concerns immediately to IT security at your organization.

| High-Risk Travel Areas

Countries or territories that are identified as high-risk are often the subject of official travel advisories. ZeroFox Intelligence recommends that travelers consult their own respective government advisories for the latest travel updates for high-risk areas. Nevertheless, there are additional precautions that should be considered when traveling to such locations:

- ➔ Travel only with sanitized burner or loaner devices; do not take personal devices containing sensitive data.
- ➔ Understand that devices can be confiscated through arbitrary enforcement of laws within certain high-risk travel areas.
- ➔ Exercise extra caution with online activities; many high-risk travel areas enforce strict censorship measures, and access to certain services might also be disrupted or blocked entirely.
- ➔ Assume that all online activity and communications are monitored; state surveillance is commonplace within many high-risk travel areas—particularly for business and high-profile travelers.