Surveillance systems can track the locations of mobile phone users and spy on their calls, texts and data streams. The Washington Post has reported on such systems that are being turned against travellers around the world, according to security experts and U.S. officials. The summer season highlights the need to take extra precautions when travelling.

When travelling anywhere in the world, for business or pleasure, citizens need to be aware of and alert to looming physical and cybersecurity threats.

To elaborate on expert security tips, strategies and advice for traveling this summer, we presented several questions to The Chertoff Group, a global security advisory firm that enables clients to navigate changes in security risk, technology and policy. Chris Duvall, Senior Director at The
Chertoff Group, offers insights into cybersecurity concerns, physical security precautions, and recommends digital resources/apps for consumers while traveling.

Q: How are security risks – physical and digital – changing? Why are threats greater today than five years ago?

"The exponential number of headlines over the past few years is a strong indication that both physical and digital risks are evolving and increasing.

Duvall: The exponential number of headlines over the past few years is a strong indication that both physical and digital risks are evolving and increasing. The scope, severity and complexity of physical and cyber risks are increasing and becoming more dangerous and destructive. This is especially true for those travelling outside the U.S.

On the physical side, threat actors are actively seeking “soft targets” – public events, social settings, mass audience venues, etc. – to communicate their message, sow chaos and inflict catastrophic harm.

On the digital or cyber side, we have seen a shift from “thrill hacking,” to an increase of “hacking as a business” (through credential compromise and ransomware), to an increase in “hacking for harm” - with the rise of “nuke ware” and ransomware without a clear financial motivation.

Q. What specific precautions should a traveller take to protect their calls, texts and data streams from being spied on?

Duvall: When travelling abroad, we recommend to our clients that their personnel and executives should practice good internet and social media hygiene. Some best practices include:
Avoid using public Wi-Fi services—unless you use private VPN service for encryption
Increase the privacy setting on your technical devices
Disable location identifiers on apps
Create a new (unlinked) email for internet correspondence
Consider purchasing international MyFi devices to decrease the risk of getting your personal identification information (PII) or protected healthcare information (PHI) stolen
Use temporary (i.e. burner) phones to protect your data and your contacts

Q. What cybersecurity concerns are likely to impact travellers? Are the threats greater outside the United States or in any specific parts of the world?

Significant precautions should be taken to protect personal electronic devices (PEDs) and the data connected to PEDs

Duvall: The international cybersecurity landscape has grown increasingly dynamic, with threats posed by government authorities (in some countries), terrorists, insurgents, and criminals, requiring travelers to be proactive and vigilant. U.S. citizens, particularly executives of U.S.-based technology companies, must be aware that they are considered high-value targets for nation-state intelligence services and criminally-motivated bad actors. Many countries will go to great lengths and expense to acquire and exploit proprietary information from U.S.-based companies, and views U.S. executives visiting the country as “soft” targets of opportunity. As such, significant precautions should be taken to protect personal electronic devices (PEDs) and the data connected to PEDs. The tactics, techniques and procedures (TTPs) utilised by bad actors are often covert and nearly undetectable by the affected person.

Threat actors routinely access, monitor and utilise Wi-Fi networks at hotels and in public spaces to
compromise target devices. Other targeting methods include luggage searches, extensive questioning, and unnecessary inspection and downloading of information from personal electronic devices.

There are numerous, high-risk countries for which the U.S. Government warns travellers to be wary of mobile malware, mobile device privacy attacks and hot spots for mobile botnets. The U.S. Department of State has the most recent and up-to-date list. For example, the U.S. Government has investigated numerous incidents in which U.S. travellers’ PEDs (personal and company devices) have been compromised by Russian authorities while transiting Russian airports, left unattended in public spaces and in travellers’ hotel rooms.

Q: What physical security precautions should a traveller take?

Duvall: Here are some useful precautions:

- When traveling to an unfamiliar place, research your destination to understand the local roads and transportation, geography, local roads, culture, etiquette and laws.
- Protect your personal information and travel itinerary as much as possible.
- Limit the amount of jewelry worn, cash, credit cards and electronic devices carried while traveling.
- Avoid staying on the ground floor of a hotel. Consider choosing a room on the 2nd through 7th floors as these rooms may be more difficult to break into than those on the ground level, but still able to be accessed by fire/emergency response equipment.
- Never answer your hotel room door for anyone until you’ve determined who they are, why they are at your door, and if it is necessary for you to open the door to interact with them.
- Carry a rubber door stop/wedge with you to install on the room side of the door before you go to bed.
Vary your patterns and routines when venturing out into a new location, do not become predictable.

Politely decline offers of food or drink from strangers (If you do accept beverages, ensure that they are in sealed containers and that there is no evidence of tampering).

Never discuss your itinerary, personal, business or other sensitive information where others can hear you.

Q: How can companies be proactive in protecting their business travellers?

Companies should educate their employees on the importance of maintaining good internet hygiene while travelling abroad

Duvall: When travelling on business, companies should provide their employees with clean computers and cell phones before departure. Upon return, the company should immediately wipe the computer clean to prevent any malicious threats from penetrating the company’s internal, cyber-infrastructure. Additionally, companies should educate their employees on the importance of maintaining good internet hygiene and recommend their employees disconnect from social media platforms while travelling abroad. Some general tips to recommend to your employees when travelling abroad include:

- Register in the Smart Traveler Enrollment Program (https://step.state.gov/step/)
- Visit Travel.State.Gov to view travel related information specific to the country or countries you’re visiting, including local US Embassy or Consulate contact information, as well as current travel advisories and alerts.
- Always leave a copy of your transportation and hotel itinerary and driver’s license (or passport if travelling internationally) with a family member or trusted friend.
Always use a baggage tag with a protective cover
Avoid using public Wi-Fi services

Q: What digital resources and/or apps might a traveller benefit from (and how)?

Duvall: The Chertoff Group recommends researching the below travel-related apps before departing on a trip:

- **TravWell**: This app provides destination-specific vaccine recommendations, a checklist of what you need to do to prepare for travel, and a customisable healthy travel packing list. The app can store travel documents, keep records of medications and immunisations, and set reminders to get vaccine booster doses or take medicines.

- **My TSA**: This app provides real-time updates on airport delays. It includes how long security lines are at various airports; information about what you can and cannot bring onto an airplane; and a frequently-asked question list, including new advanced imaging technology.

- **Border Wait Time**: The app provides estimated wait times and open-lane status at land ports of entry, which may be particularly helpful when in an area with multiple crossings.

- **Mobile Pass**: The Mobile Passport app speeds you through U.S. Customs and Border Protection at (1) cruise port and (24) airports

Q: As a security expert, what’s your best advice for travellers?

Duvall: At the end of the day, travel security is not rocket science. Simply put, travellers need to:

- Be aware and situationally alert at all times.
Be aware and situationally alert to the location of your luggage and carry-ons at all times.

Don’t access unknown, unsecured or public Wi-Fi if at all possible.

Turn off “auto connect” features and institute stringent privacy controls as much as possible.

Try to “blend in” – you don’t have to try to look like a local but travellers should avoid gaudy and expensive attire wherever possible.

Use your common sense – if an offer, invitation or opportunity seems to good to be true... it probably is.
You may also be interested in...

Body search and airport security – maximising safety and dignity for t...

A US Department of Homeland Security investigation showed that undercover agents defeated airport screening in 95 percen...

TSA security checks under the scanner: Are ineffective airport screeni...

I suspect that many people – especially travellers – associate the idea of “security” with what they see at the airp...

Facial recognition technology to enhance travel and banking in 2018

2018 will start to see facial recognition and other biometrics used in a combination of ways, but I’d like to look even further into t...

How to tackle the Zika virus impact on employee security, companies an...

Many companies are considering carefully the possible risks of business travel to the areas most impacted by the Zika virus, and others may...
High-speed visitor screening systems will improve soft target security

Several recent terrorist and mass violence attacks have been directed at soft targets, or relatively unprotected locations where people gath...