WSFC Tracking Number # 17-0179

Tracked By: HSEC-1, HSEC-7 and WSFC SIN-4

Designed to Print at 11 x 17 Inches

REFERENCE AID: INTELLIGENCE AND CYBER SECURITY THREATS TO CONSIDER DURING INTERNATIONAL TRAVEL

The following information is provided to help state and local government officials better understand the potential intelligence threats they may face when traveling overseas—especially when traveling with electronic devices—such as smartphones, laptops, and tablets—and steps they can take to mitigate those threats. While these devices can facilitate staying in contact with the home office, the risk for compromise and exploitation of electronic devices "greatly increases" during overseas travel. Travelers must assume that any electronic device will be compromised and should never assume they are too "insignificant" to be targeted. Travelers should always consider taking disposable smartphones and loaner laptops or tablets—wiped of any sensitive data. Information provided in this reference aid represent only some of the intelligence collection and cyber threats travelers may face. Travelers are encouraged to request a comprehensive travel security briefing prior to undertaking any international travel. To request a MyWATCH travel security briefing, please contact: Washington State Fusion Center at 1-877-843-9522, or E-mail: Intake@wsfc.wa.gov.

Overseas Airport

- Avoid using public Wi-Fi services—unless you use private VPN service for encryption
- Avoid discussing sensitive information, or business matters, while waiting for your flight
- Be wary of conversations initiated by strangers in airport lounge
- Keep your electronic devices and belongings with you at all times—even the restroom
- Assume you are under surveillance
- Closed-circuit TV cameras are widespread at most airports
- Protect your personal information and travel itinerary as much as possible
- Always use a baggage tag with a protective cover
- Never transport your electronic devices, or sensitive documents, in checked baggage; keep them on your person
- Baggage locks are not a deterrent against baggage handlers and airport security

On The Plane

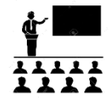
- Avoid using public Wi-Fi services—unless you use private VPN service for encryption
- Voice, data, SMS, Webmail, and other data may be susceptible to interception and collection when aircraft are above 10,000 feet
- Avoid discussing business matters during the flight
- Keep your electronic devices secure and ensure they are password protected
- If you plan to sleep, consider placing your electronic devices inside a locked bag under your feet
- Do not feel obligated to engage in conversations initiated by other passengers

Ground Transportation

- It is preferable to have a prearranged, vetted, private security service drive you
- Taxis are commonly employed by intelligence services and criminal organizations
- Reject any offer by taxi drivers to be your personal driver for duration of your trip
- Taxi drivers may understand English—even if they indicate otherwise
- Do not discuss sensitive information or business matters while in a taxi
- Most taxis are equipped with video and audio recording devices
- Avoid announcing the name of your hotel or destination loud enough to be overheard by anyone standing nearby
- Alternative taxi service apps have been known to collect user location data, even if the app is closed

Hotel

- Avoid using hotel computers and Wi-Fi services—unless you use private VPN service for encryption
- Hotels are prime locations for foreign intelligence services and business competitors to collect information from you
- Assume your room is under audio and video surveillance—especially in China and Russia
- Do not discuss sensitive information or business matters with hotel staff—or in hotel bars
- Do not give hotel staff your business card
- Do not leave your passport with hotel staff—if required, provide them with a photocopy of your identification page
- Do not allow hotel staff to take your baggage to your room—if they contain electronic devices or business documents
- Never assume your electronic devices are secure in a hotel room safe
- Never engage with strangers who show up unexpectedly at your door
- If approached by an attractive and flirtatious individual, assume you are being targeted



Conference-Trade Fair

- Avoid using public Wi-Fi services—unless you use private VPN service for encryption
- Intelligence services love international trade fairs and conventions—these types of events allow them to collect information and establish personal relationships for future elicitation and exploitation
- Understand the concept of elicitation and probing questions—avoid divulging sensitive or private information
- If a foreign contact gives you gifts, such as USB flash drives or DVDs, do not allow them to be installed on your electronic devices
- Keep your electronic devices secure and ensure they are password protected
- If approached by an attractive and flirtatious individual, assume you are being targeted

WARNING! Travelers should NEVER, under any circumstances, practice counter surveillance techniques. For example, travelers should NEVER search for hidden cameras or listening devices in their hotel room—or attempt to evade or confront a surveillance team. Use common sense and avoid doing anything that would arouse the suspicions of a foreign government.

Note: This product was coordinated with and reviewed by the U.S. Department of State – Overseas Security Advisory Council (OSAC), and the Federal Bureau of Investigation – Seattle Division.

UK Man Arrested After Refusing to Turn Over Passwords at Airport

A British human rights activist was recently arrested at Heathrow International Airport for refusing to provide police passwords to his encrypted cell phone and laptop computer. The man was charged with willfully obstructing or seeking to frustrate a search examination under schedule 7 of the Terrorism Act, which gives British border officials sweeping search powers. The Guardian

French Intelligence Used Air France to Spy on Business Travelers

Being stuck on a long, transoceanic, flight can be the perfect opportunity for a foreign intelligence collector to acquaint themselves with an unsuspecting target. According to Pierre Marion, former chief of the French General Directorate for External Security (DGSE), during the 1980s and 90s, French intelligence routinely spied on business travelers flying on Air France. The DGSE is believed to have bugged the first class sections of aircraft operated by Air France, and placed intelligence officers among passengers and flight crew members. New York Times | The Register

Beware of In-flight Social Networking Applications

A number of U.S. and international airlines have rolled out in-flight social networking applications for the purpose of allowing business travelers to connect and communicate with other business travelers during their flight. However, these social networking applications also provide an opportunity for foreign intelligence services, business competitors, and criminal organizations to target and build a profile on you. With some networking applications, they can even start doing this days before your flight. Forbes | CNBC | New York Times | The Economist

Popular Ride-hailing App Tracks Users' Locations, Meetings, and Appointments

A popular transportation company's smartphone app has been found to collect location data and track users of the app for up to 5 minutes after their ride is over—even if the app is closed. The app also integrates with a user's smartphone calendar, giving it access to all upcoming meetings and appointments. Hacker News | Quartz | Ubergizmo

DarkHotel: Sophisticated Hacking Attack Targeted High-profile Hotel Guests

For several years, the Wi-Fi networks of luxury hotels in Asia were compromised and used to download sophisticated malware on to laptop computers of hotel guests. Targets of these attacks included executives and officials associated with governments, NGOs, military organizations, the defense industry, energy sector, pharmaceutical companies, and large electronics and peripherals manufacturers. The Economist | Kaspersky | Wired

Hotels Have Become Prime Targets for Stealing Travelers' Credit Card Data

Over three months in 2016, more than 1,200 InterContinental Hotels worldwide were hacked by cyber thieves. A large number of major American hotel chains were also hit, allowing hackers to steal credit card and other personal information from thousands of hotel customers. Because many hotels are chains, one breached location allows hackers to break into the entire network. Even if travelers take precautions to protect their credit card information, it can still be stolen if a hotel chain's network has been compromised. KrebsonSecurity | CNET

Seoul Hotel Break-in Has Makings of a Spy Novel

In February 2011, members of South Korea's National Intelligence Service (NIS) were caught breaking into one of the hotel rooms of a visiting Indonesian government delegation in downtown Seoul—while attempting to access and steal information from a laptop computer. The 50-member Indonesian delegation was in Seoul to discuss trade and military deals with the government of South Korea. New York Times | BBC News

Hotel Chain Monitors Social Media to Spy on Guests

At least one major hotel chain has started monitoring news sites and social media in order to keep track of their guests' activities. From several command centers in the U.S., and overseas, they use geo-fencing technology to track their guests' activities, comments, and photos on Reddit[USPER], Instagram, Weibo, Facebook[USPER], and Twitter[USPER]. This hotel chain has over 4,400 of their properties geo-fenced worldwide, and track approximately 300,000 guest postings daily. CNBC | Quartz | Revinate | Net Affinity | ReviewPro

U.S. Businesswoman Arrested and Charged with Spying

In March 2015, a U.S. businesswoman was detained and arrested during a trade mission to China. The U.S. businesswoman, who was also president of the Houston-Shenzhen Sister City Association[USPER], was part of a delegation from Houston—which included Houston's Mayor Pro-Tem. Six months later she was officially charged with spying and stealing state secrets. After being convicted and sentenced to three and a half years in prison, she was deported back to the U.S. in April 2017. NBC News | New York Times

U.S. Defense Contractor Met Suspected Chinese Spy at Defense Conference

In March 2013, a 59-year-old defense contractor at the U.S. Pacific Command was charged with giving away classified information to his 27-year-old Chinese girlfriend, who was living in the U.S. as a student on a J-1 visa. The defense contractor and the Chinese woman initially met at an international defense conference in Hawaii and had maintained an intimate and romantic relationship since June 2011. Investigators say the contractor provided the woman with details of U.S. strategic nuclear systems and early warning radar systems in the Pacific Rim. CBS News | Christian Science Monitor

International Conferences and Trade Fairs Targeted by Spies

International conferences, high-tech trade fairs, air shows, and major sporting events attract large numbers of businesses, contractors, subject matter experts, scientists, engineers, military personnel, and government officials. As such, they can be key venues for economic espionage. Collection methods include elicitation of information during innocuous conversations, eavesdropping on phone conversations, breaking into hotel rooms to steal information, and downloading files from electronic devices. Washington Times | The Intercept | Information

U.S. Companies and Technologies Focus of Targeted Collection at UAV Conference

During a 2013 Unmanned Aerial Vehicle (UAV) conference in Washington, D.C., a three-page document was found on the convention floor. The document was written in a Middle Eastern language and was titled, "Information Collection during the Conference and Exhibition." The document tasked three individuals to collect very specific and detailed information on prioritized U.S. companies and technologies at the conference. FBI

Cyber-espionage Malware Taps Into Skype Calls

In 2016, security researchers discovered an unusually complex malware attack that taps into Skype communications. The Trojan horse, called T9000, has been detected in malicious E-mail attachments. Once activated, the Trojan exploits vulnerabilities in Windows to install a back door. It then downloads additional components that allow it to listen in on Skype conversations, take screenshots, and capture encrypted data. This malware is the latest in a line that has previously been linked to cyber-spies. CSO Online | Silicon

Spy Tech Firms Help Governments See Everything on a Smartphone

A rapidly expanding industry of spy tech companies have been developing and selling sophisticated surveillance tools that allow governments, intelligence agencies, law enforcement, and anyone willing to pay, the ability to remotely and covertly collect data from a targeted individual's smartphone. These tools can track everything a target does on a smartphone. One tracking tool, known as Pegasus, has been used to target a range of smartphones, including iPhones, Android, BlackBerry, and Symbian without leaving a trace. New York Times | The Intercept | Forbes | The Guardian

Israeli Firm Can Steal Phone Data in a Matter of Seconds

One Israeli company is recognized around the world for its technology that can unlock smartphones and extract data. With contracts in more than 115 countries, many with government agencies, Israeli firm Cellebrite was reportedly hired by the FBI to break into the iPhone of one of the San Bernardino, California terrorists. While iPhones present the biggest challenge, Cellebrite claims there is no phone operating system on the market that is impossible to unlock and compromise. Forbes | ZDNet

Welcome Back From Your Trip—Now Hand Over That Bugged Phone

For years, the FBI has warned government and corporate executives NOT to use hotel Wi-Fi connections, because of reports that travelers were unknowingly downloading spyware. Officials at the departments of Justice and Homeland Security typically expect their employees' smartphones will be compromised when they travel overseas. To contain the damage, employees are given loaner phones and tablets to use during their trip. When they return, those devices are quarantined and checked for any malicious software. Harvard Business Review | Defense One