OFFICE OF THE
CHIEF INFORMATION OFFICER
DEPARTMENT OF HEALTH AND HUMAN SERVICES

June CyberCare Excursion

Recognizing and Avoiding Cyber Traveling Risks

Do your summer plans involve domestic or international travel? Before you embark on any travel, be sure you understand the HHS guidelines that are in place to help you explore the world and stay cyber S.A.F.E.

Do you think you become an easier target for a cyber-attack while on travel? According to the 2019 IBM X-Force Threat Intelligence Index, the transportation industry has become a priority target for cybercriminals as the second-most attacked industry. In the past three years, over 500 million sensitive records have been leaked or compromised when traveling.

S Stay alert to your surroundings
A Always keep your government equipment with you
Are you traveling SAFE?
F Forget public Wi-Fi with no password
E Ensure devices are powered off

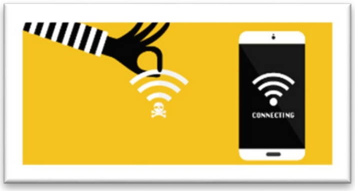
Below is a list of the most prevalent cyber risks that may occur when traveling domestically or internationally. To help you avoid these common traveling cyber risks, we've highlighted best practice tips and HHS policies to ensure you travel S.A.F.E.

Common Cyber Risks When Traveling

THAT SEEMS RISKY...
I have 5 minutes to board, so I'm just going to leave my government laptop while I run to the restroom.
Wait a second...
That seems risky.
Read CyberCARE's new article to learn how to protect all your government equipment while traveling.

Charging Station Risk: Beware of using device charging stations because they could have the ability to download data stored on your device and send malware to your phone.

Best Practice: Purchase a portable charging unit to charge on the go or plug your own charging cord directly into an electrical outlet. If you must recharge via Universal Serial Bus (USB) at a public kiosk, power off the device before plugging it into the charging station.



Hotspot Risk: Beware of free Wi-Fi hotspots. Cybercriminals can create an identical copy of a legitimate Wi-Fi network to trick you into connecting with their network. Hackers set up *Evil Twin* access points in areas serviced by public Wi-Fi, such as airports, hotels, and shops. Once connected to an *Evil Twin*, an attacker can easily hijack the device's communications. The attacker can monitor traffic, steal credentials or redirect you to malicious websites to either download malware or capture online credentials.

Best Practice: If a password-enabled hotspot is not available, consider tethering to your personal phone's hotspot to gain Internet access. Before you connect to any public Wi-Fi, be sure to verify its official name. Also, be sure to disable the "auto connect" or "auto join" functions for all of your wireless devices.

HHS Policy: Use a dedicated cellular or wireless connection that requires a password along with the HHS Virtual Private Network (VPN) access to conduct all HHS-related business.

Hotel Risk: Leaving your sensitive Personally Identifiable Information (PII) or Government Furnished Equipment (GFE) out in the open when leaving your hotel room increases the odds of these items being stolen. The hotel safe isn't impenetrable, either. Hotel safes can be cracked if you use an easy-to-guess password like the room number.

Best Practice: Place all PII and GFE devices in your hotel room safe and secure it with a strong password/combination that only you know. If items won't fit in the hotel safe, lock them in your luggage.

Special Notice on Foreign Travel

If you choose to travel internationally be sure to read up on the latest HHS policies and guidelines including Foreign Travel Checklist, Foreign Intelligence Entities for Foreign Travel Security Awareness, and Memorandum - Use of Government Furnished Equipment (GFE) During Foreign Travel. Ensure you depart with a foreign travel contact list, just in case you need additional support. Some important contacts to include are:

- ❖ HHS Travel Security Team - travelsecurityteam@hhs.gov
- ❖ Office of Overseas Citizen Services at 202-501-4444 (they are available 24/7)
- ❖ Office of National Security - International@hhs.gov

In addition to the aforementioned risks, the following risks can happen anywhere, yet are more heightened during foreign travel.

Social Engineering Risk: Beware if an unknown host country national approaches you and requests sensitive or classified information during casual conversations. This could either be social engineering or espionage.

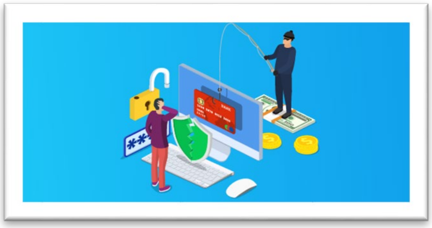
Best Practice: Always be aware of your surroundings when discussing HHS-related or personal business.

HHS Policy: Do not discuss sensitive matters where they could be overheard, and review the reporting requirements for Foreign Intelligence Entities for Foreign Travel Security Awareness policy for steps to follow if approached by a foreign national.

Cloning Risk: Cybercriminals use Near Field Communication (NFC) technology to capture and clone the footprint from a traveler's mobile device or computer hard drive.

Best Practice: Disable NFC connections on mobile devices. Do not leave your GFE mobile devices unattended. Lastly, keep GFE and other loaner devices powered off when not in use.

HHS Policy: Permanently issued GFE devices are prohibited during foreign travel. Only loaner GFE (including mobile computing, phone and storage devices) may be used during official foreign travel. GFE loaner devices must remain powered off during travel to and from the foreign country.



Spoofing Risk: Foreign travelers can become the victim of email spoofing. Email spoofing is a technique used in spam and phishing attacks to trick users into thinking a message came from a person or entity they either know or can trust. In spoofing attacks, the sender forges email headers so that client software displays the fraudulent sender address. If you click the malicious links, or open malware attachments, you could give a cybercriminal the ability to steal your user IDs, activate your camera, and/or monitor your emails.

Best Practice: Brush up on best practices to stay vigilant against phishing attacks. Be sure to verify the sender's email address, and the destination of any link you're asked to click.

HHS Policy: According to the HHS policy on Use of Government Furnished Equipment (GFE) During Foreign Travel, Outlook Web Access (OWA) is not authorized for usage while on official foreign travel.