BOARD OF REGENTS OF THE UNIVERSITY SYSTEM • OF GEORGIA •

UNIVERSITY SYSTEM
OF GEORGIA

Traveling with Mobile Devices: A USG IT Handbook Companion Guide

Version 1.0

5/24/2022

Public

Abstract: This companion guide is developed to aid USG organization’s cybersecurity professionals concerning mobile device management with a focus on traveling in both low and high-risk countries.

Revision & Sign-off

Change Record

Date	Author	Version	Change Reference
202207??	Todd Watson	1.0	Posted.

Document Properties

Item	Details
Document Title	Traveling with Mobile Devices: A USG IT Handbook Companion Guide
Document Type	Guideline (Internal Use Only)
Author	Todd Watson
Document Manager	Todd Watson
Creation Date	20220524
Last Updated	20220524
Document Classification	Public

Table of Contents

Recommendations for Travelers to Lower Risk Countries

USG Cybersecurity maintains a list of high-risk countries. By default, a country is considered low risk unless it appears on the high-risk list. When traveling to lower risk countries, special consideration and preparation is still required, although not necessarily to the extent as when traveling to high-risk countries. It is important to take a minimum complement of technology along to accomplish work while abroad. Consider following the Recommendations for Travelers to High-Risk Countries regardless of the risk level of your destination.

Computers

If you are taking a laptop computer, before you go you should:

- Verify that your computer software is current by having your computer reviewed by technical support. Make an appointment for a review in advance of your trip.
- Make sure your computer is fully backed up via the organization backup services and whole disk encryption is enabled.
- Test the VPN software to ensure you are familiar with how it operates.
- Remove any documents containing sensitive or confidential data.

Mobile phones

Consider a loaner phone borrowed in the country you plan to visit, an unlocked phone with a local SIM card, or a phone you buy or rent at the airport or hotel when you arrive. If you must use your own phone:

- Back it up before you leave.
- Secure it by ensuring the phone is enrolled in the organization's Mobile Device Management (MDM) program,
- Enroll in an international rate plan to avoid incurring exorbitant roaming charges, and
- Save your data, reset to factory defaults, and restore your backup when you return.

Planning will protect your privacy and USG data, while also saving money and frustration later.

Additional information

Before You Depart

- Turn on multifactor authentication. We recommend doing this a week or two before you go so that you get used to the procedure.
- Ensure your voicemail forwards to email. This eliminates the need to call your voicemail, potentially revealing your voicemail passcode and incurring international toll call charges.

While Abroad

- Do not plug your phone into charger kiosks. There may be a hostile computer on the other end of that innocent-looking wire.
- Be aware of your surroundings. Watch for those looking over your shoulder or potential thieves.
- Do not leave your devices unattended. Even hotel safes are not secure.

When You Return

- Change your institution password.
- If you checked your voicemail by calling in while traveling, change your voicemail passcode.

Recommendations for Traveling to High-Risk Countries

Travel to High-Risk Countries[1] requires special consideration and preparation regarding the technology accompanying you. It is important to take the minimum you need to get your work done while you are gone. The following options range from the most secure to the minimum required safeguards when traveling to high-risk locales.

Computers

Best: Travel light: We strongly recommend that you leave your current devices here and travel with an institution-provided Travel Loaner kit.[2] You can borrow a kit by requesting one.[3] Travel with the option of your choice instead of your laptop; Any of these choices enable you to manage email, view your calendar, run presentations, edit documents, and connect to institution websites. The devices are set up specifically for your use and wiped back to factory settings when you return. The loaners are enrolled in the institution Mobile Device Management (MDM) program to encrypt the device and provide you with a secure platform for the duration of your travel.

Good: Travel with less data: If you do not feel that you can travel without a full laptop, another option is to take a new or freshly rebuilt machine and load only the data you will need for this trip. You will need to make sure that the machine is encrypted before you go. Make an appointment with the IT help desk for assistance. Whenever possible, leave USB drives at home. These are easily lost and easily corrupted. If you must travel with a USB device, be sure that it is encrypted.

Minimum: Travel encrypted: If you cannot travel with a tablet or a loaner computer and must take your own laptop, there are some additional steps you need to take before you go. Make an appointment with your IT service department to:

- Verify that your computer software is current.
- Make sure your computer is fully backed up and encrypted.
- Remove any documents containing Sensitive or Confidential data from your computer.
- Ensure your device does not contain proprietary encryption software.

When you return, transfer the documents you created while traveling to another device, completely wipe your computer, restore from the backup created before the travel, and transfer the new files.

Mobile Phones

Best: Go Without: The first thing to consider is whether you really need a mobile phone. Are you going to make calls? Can you get by with a Wi-Fi-only device like the iPad travel kit provided by the institution?

[1] https://www.usg.edu/cybersecurity/assets/cybersecurity/documents/High_Risk_Countries.pdf
[2] https://www.usg.edu/cybersecurity/assets/cybersecurity/documents/Sample_Travel_Loaner_Program.pdf
[3] https://www.usg.edu/cybersecurity/assets/cybersecurity/documents/Loaner_Requisition_Form.pdf

Can you manage without a phone during a short trip? We are more dependent on mobile phones these days, but perhaps you can go without.

Good: Get it There: The best thing to do is to use a device you will not use again. This can be a loaner phone borrowed in the country, an unlocked phone with a local SIM card, or a phone you buy or rent at the airport or hotel when you arrive.

Minimum: Have a Plan: If you must use your own phone:

- Back it up before you leave,
- Secure it by enrolling in the institution Mobile Device Management (MDM) program,
- Enroll it in an international rate plan to avoid incurring exorbitant roaming charges, and
- Save your data, reset to factory defaults, and restore your backup when you return.

Planning will protect your privacy and the University's sensitive data and save a lot of money and frustration later.

Additional information

Before You Go

- Submit a service center request to forward your voicemail to email. Listening to voicemail from email attachments saves you from having to dial into your voicemail account, eliminating international toll charges and potentially revealing your voicemail passcode.

While You Are Traveling

- Do not plug your phone into charger kiosks. There may be a hostile computer on the other end of that innocent-looking wire.
- Be aware of your surroundings. Watch for those looking over your shoulder or potential thieves.
- Do not leave your devices unattended. Even hotel safes are not secure.
- Report any incidents to your institution IT service center immediately, including lost or stolen equipment. When you report, ensure the service center knows you are traveling abroad.

When You Return

- Change your institution password.
- If you checked your voicemail while traveling, change your voicemail passcode.
- If you took your computer abroad, save any documents you created while away to an external drive and restore from your pre-departure backup.
- Return all loaner equipment promptly; communicate any problems or challenges you encountered while abroad.

High Risk Countries

The derives the list of high-risk countries from several sources, including countries that are the subject of Travel Warnings[4] by the U.S. Department of State, and those that are identified as high risk by other

[4] https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html/

U.S. Government sources such as the Department of the Treasury Office of Foreign Assets Control (OFAC)[5], the Federal Bureau of Investigation (FBI)[6], and the Office of the Director of National Intelligence (ODNI)[7].

This list is maintained by USG Cybersecurity and will be updated regularly.

* Any plans to travel on behalf a USG institution to Cuba, Iran, North Korea, Syria, or the Crimean region of the Ukraine must be reviewed and approved by senior leadership. Approval is required before availing of the Device Loaner program.

China: A special travel situation

Travelers to the People's Republic of China (PRC) report a range of issues.

- Access to services that we take for granted like Gmail and other Google apps, Wikipedia, and Yahoo Web Mail are often blocked altogether or filtered.
- China may not permit access to Google search and instead promotes the PRC-endorsed Baidu search.
- Skype and other conferencing software may be monitored by the government.
- When attempting to use VPN software, some have reported they are often cut off for hours at a time. Do not assume VPN software downloaded in PRC will be secure.
- Hotel staff and government officials can access hotel room safes. Do not assume a computer or mobile device left in a hotel safe will be secure.

Domestic Travel Mobile Phone Tips

For those who travel domestically, somewhat greater care must be exercised than when at home. A few commonsense practices will help safeguard your mobile phone, protect your property, and continue to safeguard information entrusted to you.

1. Consider turning on the “Find my Phone” service if your device provides this feature.
2. Keep your phone, cables, chargers, and accessories organized. Take a quick inventory of what you brought along when moving from one place to another.
3. Do not leave your phone or accessories unattended.
4. Disable the “automatically connect to any available network” feature.
5. Take care when using wireless network (“Wi-Fi”) services. If you decide to use them, take caution, and only use legitimate and documented services. Check network names very carefully before connecting. Airlines, airports, and hotels offering Wi-Fi will document their name of their service. If you are unsure, ask an airline, airport, or hotel representative before connecting.
6. Ensure you are using a VPN to connect with your office if you are using your phone to access information systems.
7. Unlimited cellular data plans may be a good alternative to using Wi-Fi services, depending on the details of your trip. If your cellular plan has a data cap, use Wi-Fi services carefully.

[5] http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx
[6] https://www.fbi.gov/
[7] http://www.odni.gov/

8. A mobile “hotspot” uses a cellular network to connect to the internet, and typically shares that connection via Wi-Fi. Hotspots are a combination of hardware and services purchased from your cellular phone company and are useful when cellular service is available, but Wi-Fi is not. Hotspots access the internet from your laptop via your phone company’s cellular network by connecting the laptop to the hotspot. Hotspot may be
9. Turn on “Airplane Mode,” “Flight Mode,” or “Offline Mode” when traveling by air, if permitted by your airline. Using this mode helps reduce power consumption by disabling the phone from searching for cellular towers and enables use on in-flight services.
10. Avoid oversharing to social media while traveling. Sharing with social media informs your social circle that you are away from home, which increases the risk of a burglary. Share photos when you return home.
11. If a state-supplied device is lost or stolen while traveling, report it to your organization’s cybersecurity team as soon as possible.

International Travel Mobile Phone Tips

What to do when traveling abroad

1. Be aware that international service plans to mobile phones must be added prior to leaving the United States. We advise adding international service plans at least one week prior to departure. Plans often must be added during business hours.

2. Know what countries you are traveling to and the dates you will be in each country.
Note: International service is not available in all countries. Check with your service provider for details.

    - AT&T http://www.att.com/shop/en/wireless/international.html
    - T-Mobile https://www.t-mobile.com/travel-abroad-with-simple-global
    - Verizon http://www.verizonwireless.com/wcms/global.html

3. Know what devices you plan to take abroad (i.e., cellphone, tablet, data card) and the phone number associated with each.

4. Determine what service plans you will require for each device.

5. Submit a service ticket with all the information from above. This is a good time to set your voicemail passcode so that you can listen to voicemails while abroad. If you need help, please contact the service center at 706-583-2001.

6. Most international plans are automatically removed within 30 days. Please refer to your email confirmation to see if you need to call in and remove plans. Your organization is not responsible for any monthly charges incurred if the plan has not been removed. Please submit a service ticket or call 706-583-2001 to remove the international service plans if needed.

Be sure and turn phones/iPads on airplane mode while on airplanes and or cruise ships to avoid high overages. Even with an international plan, keeping your phone on airplane mode will minimize international calling tolls from inbound calls. Turn on Wi-Fi via settings.

Technical difficulties

If you have technical difficulties using your mobile device while traveling outside the U.S., try this simple step first: Turn off your phone for one minute, then restart it.

If the issue continues, contact your carrier directly.

- AT&T: 1-314-925-6925. *To access the plus sign (+) on most devices, press and hold the 0 key.*
- T-Mobile: 1-505-998-3793
- Verizon: Dial the exit code for the country you are in, then dial 1-908-559-4899

Reminder: Not having an international plan could result in loss of service and high charges (i.e., overages). Changing plans during non-business hours could result in additional added fees.

More travel tips and resources

- Travel Loaner Program

Calling from the U.S. to other countries requires an international calling plan. This plan reduces the per minute cost of calls to the countries being called. (Cost varies by country.) Please call 706-583-2001 or submit a service request[8] for support. Facetime Audio on Wi-Fi is free. The cost for Facetime not used on Wi-Fi is based on your data plan. To avoid high data overages, you must initiate the call using Facetime and not by establishing a standard voice call and then switching to Facetime. (Check the Apple website[9] for more information.)

[8] https://www.usg.edu/customer_services

[9] https://support.apple.com/guide/iphone/make-calls-using-wi-fi-iph78f4697ca/ios