International Travel Guidelines

GUIDE TO MOBILE DEVICE SECURITY ABROAD

GW Information Technology | 202-994-4948 | ithelp@gwu.edu | https//it.gwu.edu

THE GEORGE WASHINGTON UNIVERSITY
WASHINGTON, DC

International travel increases the likelihood that personal and university-owned devices and data will be compromised. As a result, George Washington University (GW) Information Technology (IT) has prepared the following security guidelines and tips for mobile devices to support GW community members traveling abroad on university business.

Please note that many of these guidelines are also useful and recommended for domestic travel.

In these guidelines, the term "mobile devices" includes smartphones, tablets, and laptops. Each mobile device may require a slightly different technical approach for securing the device prior to travel. For information regarding specific devices, please contact your local support partner or the IT Support Center before you travel.

Before You Go

1) Whenever possible, arrange to use temporary (loaner) laptops and loaner handheld devices while traveling. This is perhaps the most effective solution you can implement to protect your data on an international trip.
- Taking a loaner device drastically reduces the likelihood that theft or compromise will expose historical or archived data, which isn't needed while you travel. It also means that upon your return, after backing up relevant data from your travels, the device can be wiped clean (erased), helping mitigate the risks of importing threats back into your home equipment.
- Check with your local support partner or the IT Support Center for more information on loaner devices.

2) Limit the amount of data that you take with you on your trip.
- Travel only with data needed for your trip. This will reduce the risks associated with a system compromise or device theft while you are traveling.
- To the extent possible, keep data in GWU-approved cloud storage, such as GW Box, rather than on your local device. Data that is never stored on the device is at much lower risk of loss or compromise.

3) We strongly recommend all mobile devices be encrypted. Check to see if the country you're traveling to has any encryption import restrictions.
- Some countries, such as China, Israel, and Russia have restrictions on the import and use of encryption tools.
- If any of the countries you are traveling to have restrictions, GW IT strongly recommends that you consider taking a loaner device for the trip.
- If encryption cannot be used it is recommended that no regulated or restricted data be stored on mobile devices.

4) Do not store passwords or other credentials on the device.
- If you are not travelling with a clean loaner laptop, clear all of your browser history, cached passwords, filled forms, and any other local browsing data prior to travel. Contact the IT Support Center if you need assistance with this.
- Do not store any passwords on the device outside of password management applications designed to securely store and handle login credentials (username/password combinations). Be sure to configure your web browser(s) to not save passwords. This prevents login credentials from being saved in the browser cache. Your local support partner or the GW IT can provide recommendations for safe password storage options.

5) Make sure all applications and operating systems are updated before leaving.
- If you are not using a loaner computer, uninstall unused and unnecessary applications and turn off unneeded services on your computer. Leaving them installed and/or running only serves to provide additional, possibly "unlocked" doors for intruders to use to attack your device.
- If a software update is necessary, only accept updates from Windows Update, Apple Software Update, or the Adobe or Java websites. Do not download and install any supposed updates or patches sent via email or via unknown web links.

6) Make sure you are running in the lowest possible privilege level.
- While traveling, do not use an administrator account as your primary user account. Running as a non-administrative user on your system will defeat a significant number of malware and browser attacks.
- Refrain from installing third-party applications, especially on mobile devices that run the Android operating system. If you must install third-party applications, only do so from trusted, verifiable sources.

7) Connect securely.
- Plan ahead. Install GW's Virtual Private Network (VPN) before you go and use it when you connect to the Internet via public or shared wireless connections. This can help to secure your communications and improve privacy when using untrustworthy networks. Test your ability to get to your data using VPN from an off-campus location before leaving.
- For more information on how to obtain and install VPN on your mobile device, please contact the IT Support Center.

While You Are Away

1) On all of your mobile devices, turn off "join wireless networks automatically."
- Always manually select the specific network you want to join after confirming its name and origin with the provider.
- Turn off wireless and Bluetooth when these features are not being used.

2) Only connect your own external media to your devices.
- While USB drives and other forms of external media offer convenience in sharing and transferring files, they can also be vehicles for exploits and malware. While travelling be wary of plugging in any untrusted external media into your devices.

When You Return

1) Using a trusted computer, change passwords for all services you accessed while away.
- Whether you sign into personal or GW accounts while traveling, keep track of the services you've accessed. GW IT strongly recommends that at a minimum you change these passwords when you return. If you're on an extended trip, change them periodically. Do not use the same password for multiple services.
- When changing passwords for services you accessed while away, remember to pick strong, complex passwords, and do not reuse the same password for multiple services. For tips on how to create a strong password, see: http://it.gwu.edu/choosing-strong-passwords.

2) Have the devices you brought on the trip assessed by your local support partner or GW IT for signs of intrusion, especially if your job requires you to regularly access regulated or restricted data.

3) Return all of the devices you brought with you to their pre-travel configuration.
- Before connecting to GW resources, turn off any services that you enabled specifically to facilitate your work while traveling, update and apply any patches that were released while you were away, and scan any data you brought back for malware. If you need assistance with this, please contact your local support partner or the IT Support Center.

For assistance with any of these steps, contact the IT Support Center at 202-994-4948 or ITHelp@gwu.edu.