Frostburg State University

CyberSecurity Procedures for International Travel

1.0 Overview

For members of the campus community, a trip to a foreign country presents unique data security challenges. The nature of international travel requires you to use your device (laptop, tablet or smartphone) in various unfamiliar places that may expose your data and device to malicious people and software.

2.0 Purpose

Below is a list of data security safeguards you should add to your travel checklist before, during, and after your trip. In addition to data security safeguards, international travelers also need to consider US export control laws and import restrictions imposed by the destination countries.

3.0 User Responsibilities

YOU SHOULD KNOW

For general travel alerts and information, see the Department of State Site. http://travel.state.gov/content/passports/en/alertswarnings.html.

- In most countries you have no expectation of privacy in hotels, offices, or public places. Hotel business centers and phone networks are regularly monitored in many countries. In some countries, hotel rooms are often searched.
- All information you send electronically – by smartphone, tablet, or computer – can be intercepted. Wireless devices are especially vulnerable.
- Security services and criminals can track your movements using your mobile device and can turn on the microphone in your device even when you think it is off. To prevent this, remove the battery or power off the device.
- Security services and criminals can insert malicious software into your device through any connection they control. They can also do it wirelessly if your device is enabled for wireless. If you connect to your home server, the “malware” can migrate to your business, agency, or home system, can inventory your system, and can send information back to the security service or potential malicious actor.
- Malware can also be transferred to your device through thumb drives (USB sticks), smart cards, and other “gifts.”
- Transmitting sensitive government, personal, or proprietary information from abroad therefore carries a high degree of risk.
- Never assume you’re too insignificant to be targeted.

- Foreign security services and criminals are adept at “phishing” – that is, pretending to be someone you trust in order to obtain personal or sensitive information.
- If a customs official demands to examine your device or if your hotel room is searched while the device is in the room and you’re not, you should assume the device’s hard drive has been copied.

BEFORE YOU TRAVEL

- If you can do without the device, don’t take it.
- Don’t take information you don’t need, including sensitive contact information. Consider the consequences if your information were stolen by a foreign government or competitor.
- Back up all information you take; leave the backed-up data at home.
- If feasible, use a different mobile device from your usual one and remove the battery when not in use. In any case, have the device examined for malware and malicious activity when you return.
- Seek official cyber security alerts from: www.onguardonline.gov and www.us-cert.gov/cas/tips
- Complete a Travel Notice to inform IT that you may be accessing University technology resources such as Email, PAWS, or Canvas while traveling. Click the Security offerings on the Office of Information Technology home page, or visit the link directly at: https://portal.frostburg.edu/?app=travel&page=travelnotice

Prepare your device:

- Create a strong password (numbers, upper and lower case letters, special characters – at least 8 characters long). Never store passwords, phone numbers, or sign-on sequences on any device or in its case.
- Change passwords at regular intervals (and as soon as you return).
- Make sure you are using current, up-to-date antivirus protection, spyware protection, OS security patches, and a firewall.
- Encrypt all sensitive information on the device. (But be warned: In some countries, customs officials may not permit you to enter with encrypted information.)
- Update your web browser with strict security settings.
- Disable ports and features you don’t need.

WHILE YOU'RE AWAY

- Avoid transporting devices in checked baggage.
- Set up and use a virtual private network (VPN) to ensure all the traffic you send and receive is secure and encrypted. Frostburg State University provides a free VPN for faculty and staff use – https://www.frostburg.edu/information-technology/_files/pdf/help-desk/vpn-global-protect.pdf. However, be aware that some countries may use firewalls to prevent the use of security tools like VPN, You may find you cannot visit certain websites or conduct business as usual until you return home.
- Do not leave electronic devices unattended. If you have to stow them, remove the battery and SIM card and keep them with you.
- Don't use thumb drives given to you – they may be compromised. Don't use your own thumb drive in a foreign computer for the same reason. If you have no other option, assume you've been compromised; have your device cleaned as soon as you can.
- Shield passwords from view. Do not use the "remember me" feature on websites; re type the password every time.
- Be aware of who is looking at your screen, especially in public areas.
- Terminate connections when you're not using them.
- Clear your browser after each use: delete history files, caches, cookies, URL, and temporary internet files.
- Do not open emails or attachments from unknown sources. Do not click on links in emails. Empty your "trash" and "recent" folders after every use.
- Avoid Wi-Fi networks if you can. In some countries they're controlled by security services; in all cases they're insecure.
- If your device or information is stolen, report it immediately to your home organization and the local US embassy or consulate.

HOW TO USE PUBLIC COMPUTERS SAFELY

- Using the internet on public machines, in internet cafés, or hotel lobbies can be very convenient, and even essential if you don't have your own device with you. However, an insecure machine could be riddled with malicious software ready to record your every move. As a general rule:
    - Do not trust public computers when handling confidential information.
    - Change passwords the next time you log in from a machine you trust.
    - Never save any details (particularly passwords) on machines you don't trust.

  - Always log out properly at the end of your session and close the browser after clearing the cache.

WHEN YOU RETURN

- Change your password immediately.
- Have your device examined for the presence of malicious software.

ADDITIONAL CONSIDERATIONS FOR COUNTRIES WITH HEIGHTENED RISK

Prior to your trip, please visit https://travel.state.gov/content/travel/en/traveladvisories/traveladvisories.html and input your destination country to determine its level. For countries at **Travel Advisory Levels 2 or higher** from the U.S. Department of State these additional precautions are necessary.

- If possible, avoid traveling to countries with Travel Advisory Levels of 3 or 4.
- If you must travel to one of these countries, leave all electronic devices in the U.S. and inform colleagues that you will be “off the air” for the duration of your travel. Minimize the length of your stay in those countries. If you are travelling without your own laptop, you may be tempted to use a computer in a cyber cafe or hotel business center; however, those systems have a very high probability of being infected with malware (which may capture anything you type, including your username, password, credit card information, etc.), or of being routinely and actively monitored by national authorities. Therefore, never use shared computers in cyber cafes or hotel business centers, or systems belonging to other travelers, colleagues, or friends.
- If you are absolutely unable to be offline for the duration of your travel, do not take your normal day-to-day devices with you. Use a new temporary device, such as an inexpensive new laptop, a loaner laptop from FSU, and/or a disposable prepaid cell phone purchased just for that trip, instead (used electronics, including cell phones, are recyclable). Be sure that any such new system is fully patched, and has all institutionally recommended security software installed, but otherwise minimize what it contains, and while abroad, minimize your use of that system. Ensure it requires a long/complex password for access and keep it completely off (not just sleeping or hibernating) when you’re not actively using it, and keep it in your physical possession at all times. Assume anything you do on that system, particularly over the Internet, will be intercepted (in some cases, encrypted network traffic may be decrypted).
- Do **NOT** under any circumstances store any institutional data classified as Confidential (in accordance with the Frostburg State University Data Classification Policy) on devices you will be traveling with.

- Upon return to the U.S., immediately discontinue all use of that temporary system and have it reviewed for indications that it may have been compromised abroad. The system should then be sanitized and/or disposed of. Change any/all passwords you may have used abroad.

Revision History

Version Number	***Date***	***Author***	***Description***
1.0	*April 2023*	*Lori Bennett*	*Initial Document*
1.1	*May 2023*	*Lori Bennett*	*Updated URLs*