Department of Information Technology

International Travel

General Guidelines

Assume everything you do on your devices is being intercepted

The information that you send over a network may be monitored, even when using a hotel or business connection. It is always best to assume you are being monitored so that you can adjust your actions accordingly. Rule of thumb - Agencies should not take mobile devices with them, unless necessary to accomplishing the mission requirements

Never use public WiFi, computers, or devices

Shared computers in cyber cafes, public areas, hotel business centers, and foreign institutions-as well as devices that belong to other travelers-should never be used to access the State network or personal systems that are protected by a username and password. Public, free WiFi connections cannot be trusted and may compromise your device if you attempt to connect to them.

Keep your device with you at all times

Do not let your devices leave your sight. Should customs or other airport officials take your devices out of your view, those devices should be considered compromised and should not be used. Even if you will not be using your device, it should not be left in a hotel room, conference center, or foreign office unattended. If unable to do so, remove all battery sources from the device(s).

Do not use unknown storage devices

USB keys can be used to install malicious software on your devices and allow unauthorized individuals to compromise your data and accounts. Only plug items into your devices that you have brought with you. Public charging stations at airports or hotels should also be avoided, as they can transmit harmful software to your devices.

Be aware of your surroundings

When entering your username and password into your devices, be aware of those around you. Someone may be closely watching your screen and keyboard in an attempt to steal your credentials.

All devices should be erased and rebuilt upon you return

All devices with which you traveled should be considered compromised upon your return. They could contain malicious software that you do not want to introduce to the State's network or your home network. The safest course of action is to have the device securely erased and rebuilt, either from an existing backup or through a new installation of the operating system.

Change your passwords

You must change your password for all services that you have accessed while abroad. This should be done for your State Account as well as any personal email, social, or financial sites that you accessed while traveling. By limiting the sites that you visit abroad, you reduce the number of passwords you need to change. If possible, request a temporary account is created and deleted upon return.

Laptops

Keep Your Operating System Updated

The laptop's operating system, whether it be Microsoft, Apple, or Linux, should have all of the latest security patches applied to it.

Uninstall applications that you do not need

Keep on the laptop only those applications that are necessary for your travel. Uninstall any applications that you do not need or do not use. For those applications that remain, ensure that they are up to date with the latest security patches. This is especially important for those applications that interact with the web, including web browsers, Adobe Acrobat and Flash, Silverlight, and Java. Be aware that U.S. Export control laws preclude bringing some software applications across the borders of many countries.

Update the settings on your web browsers

All web browsers should be set to automatically clear your browsing history and cache after each session. Contact the DIT Help Desk for assistance in applying these settings to your preferred web browser.

Verify your anti-virus software is up to date

Ensure the latest version of Endpoint Protection is installed on the laptop and use the LiveUpdate feature to confirm that the virus definitions are up to date.

Remove any sensitive or confidential data

Prior to your travels, remove any sensitive or confidential data from your laptop. This includes personally identifiable information (including financial information), and any other information that is not available in a public directory), proprietary information, Agency business or planning documents, and any other materials that should not be made public. Materials related to the travel arrangements, presentations, supporting materials, educational information, and any other public domain documents can reside on the laptop.

Cell Phones and Mobile Devices

Consider using a non-smartphone

Our phones have become mini-computers and generally contain all of our email, private communications, and contact lists. These are high-value targets for international cybercriminals. The safest course of action when traveling abroad is to procure a non-smartphone that will be used only for making calls.

Back up and reset your device

If you will be traveling with a smartphone or mobile device, you should back up the device and then reset it to its factory default setting. This will clear all personal information from the device and allow you to selectively copy certain information back on to the device. Upon return, your device can then be restored to its previous state.

Limit data contained on the device

Email and contact lists contained on cell phones are often filled with information that international cybercriminals covet. Email can contain non-sensitive but highly confidential information. When traveling, it is best to remove from your device any email accounts, including your State email account and personal accounts like Gmail. At a minimum, the contacts and amount of email synced to your devices should be limited.

Use strong passcodes

Use a strong passcode to protect cell phones and mobile devices. This will prevent others from picking up your device and gaining access to it.

Disable Bluetooth and WiFi

Unless you are actively using these features, you should disable them on your phone or other mobile devices, e.g. tablets, laptops etc.). Allowing these services to run provides potential attackers with a method for gaining access to your device.

DIT Helpdesk Assistance

Inventory Your Equipment

DIT helpdesk can inventory your equipment prior to your travels. This will allow us to assist you in reporting lost or stolen devices, should you need to do so while traveling. We can then also verify the state of your operating system and applications, and we can determine whether any sensitive data is present on the devices.

Inform the supporting desktop support when traveling to areas considered high risk for data exploitation. The Enterprise Security and Risk Management Office (ESRMO) working with local FBI and DHS liaisons can provide more details on these countries. When traveling to these high-risk countries and communication back into the network is required, users should request specially configured, “clean” devices, if available. These devices must not be added to the State network upon return

Users must also ensure that any loss, theft or compromise of these devices prior to, or during the travel, be reported immediately to ESRMO.

Monitor your accounts

When notified of your travel dates, Agency helpdesk should monitor the logins from your State Account to look for any anomalous behavior. Should we identify any suspicious behavior associated with your account, we will contact you immediately to change your password.