International Travel Security

Using laptops and mobile devices while traveling helps us stay connected and productive. However, using these devices also increases the risk of compromised personal or institutional data.

Travel with the minimally necessary electronics. Password protect all devices. Biometric protections are optimal.

Remove any personal, proprietary, or unnecessary programs and data from devices. Consider having a travel-only device if traveling often.

Use a VPN to access data securely stored on the University servers. Configure VPN access before traveling.

Keep your electronics with you at all times. Do not assume hotel rooms or rental cars will be secure. Do not pack electronics in checked baggage.

Limit the sync period for past emails. Use WyoWeb to access older emails. Do not open email attachments unless you know they do not contain sensitive data.

Work with UW's IT department to install encryption software for devices containing necessary proprietary programs or data.

Log out of browsers and apps. Remove saved login credentials. Clear browser history.

Update your operating system and apps/software, including anti-virus before traveling.

Backup data. Data should be saved on University servers since they are backed up daily.

Unknown accessories (flash drives, charging stations, SD cards) can infect your device with malware designed to transfer data. Bring your own accessories, including power cords and only plug into an outlet.

Avoid the use of public Wi-Fi for sensitive data /transactions. Use your phone as a private hotspot when possible.

Never log onto a public computer to access sensitive information. These computers may contain keyloggers and malware.

Set up devices to ask before joining new wireless networks. Disable Wi-Fi, Bluetooth, and GPS when not in use.

Power off your devices while going through customs on both ends. This will help avoid a variety of common attacks.

EXPORT CONTROLS

Hand-carrying equipment, pictures, samples, or controlled data internationally is considered an export, even if no one else sees it.

Make sure you comply with Federal regulations. Contact export@uwyo.edu at least 4 weeks before leaving the U.S.

When returning to the U.S. all electronics are subject to search by Customs & Border Protection.

Be especially aware when traveling to "Countries of Concern" per the U.S. Department of State.

Register with the Smart Traveler Enrollment Program (STEP) before international travel.

QUESTIONS CAN BE ADDRESSED TO CARRIE HESCO, DIRECTOR OF RESEARCH SECURITY AND COI.