KSU Research International Travel Best Practices Checklist

Pre-Travel

Electronics

- Use a loaner device(s) – phone and laptop – if college/dept offer them
    - Load only essential data that will be needed while traveling
    - Strictly follow KSU policies regarding the device(s)
- Keep software updated – updated software is the best defense against malware
- Ensure antivirus/malware software is up-to-date
- Use a strong password – this protects info, especially if/when device is lost or stolen
    - At least 8 characters
    - Combines letters, numbers, and symbols
    - Not found in a dictionary and isn't a name
    - Changed regularly
- Download apps only from trusted sources, and make sure you understand what info it accesses (location, contacts, etc)

General

- **Review KSU Export Control policy** at http://www.k-state.edu/comply/ecp/travel/index.html **!!!**
    - This site is for your benefit in order to maintain your compliance with US Law
- Don't travel with classified or sensitive information, even if encrypted
- Leave any electronic equipment at home that you won't need during your travel
- Familiarize yourself with the country(ies) to which you're traveling. First off, contact your FSO about any concerns. Secondly, study the State Department's website, www.state.gov/travel, for any warnings, advisories, and nation-specific information.
- Enroll in US State Dept Smart Traveler Enrollment Program to get notices and info
- Above all, keep in mind that the laws and practices of foreign nations regarding online privacy and security will likely differ from the US.

Travel

Electronics

- Encrypt and/or password protect everything you can
- Switch off Wi-Fi and Bluetooth connections when not in use – automatic log-ins create vulnerabilities; some systems look for these connections to track your movements when within range, and in many nations, the Wi-Fi connections are controlled by the security service
- Avoid using shared computers – they're vulnerable to keylogging.
- Enable two-step authentication when offered
- Change passwords to any account you accessed while on an unfamiliar network
- When using public connection, avoid using sites that require personal info, like log-ins
- Use the KSU VPN protocol when you log on to any network, especially a public or non-secure one
- Be aware of your surroundings and whether others are looking at your device

    - Strongly consider a privacy screen on your computer
- Don't use the same password or PIN that you use in the US
- Clear Internet browser after use
- Don't allow foreign electronic storage devices to be connected to your phone/laptop

General

- Do not leave any electronic device unattended. Ever. This includes hotel rooms and safes.
- Be vigilant everywhere
    - Laptop theft is common in airports – keep closely held and secure
    - Do not place electronic devices in checked baggage
- Immediately report loss or theft of any electronic devices to the local US Embassy or Consulate and then KSU IT. Don't wait upon your return to report it.
- Beware of new acquaintances who probe for information
    - Especially if they propose something that seems awfully impulsive or spur-of-the-moment. You could end up in a potentially compromising situation.
- Beware that your conversations may not be private or secure
    - No other country has a Fourth Amendment, and most other countries don't have restrictions against technical and personal surveillance
    - In most countries, you have no expectation of privacy. Assume any information you send/receive is being intercepted.

Post-Travel

Electronics

- Work with IT to safely remove all data from your loaner devices, and return them promptly
- Change your passwords on any device or application/program you accessed while traveling
- Sanitize your remaining devices, by requesting IT analyze them for any potential harm
- Delete all previously downloaded apps that are no longer useful. This is especially valuable with apps/programs you used to plan the trip.

General

- If you have any suspicions about personal contacts abroad or upon your return, contact the FSO
    - Many, if not most, are innocent – they can help start the process to confirm