Security when Traveling

NCSA Incident Response and Security Team

ILLINOIS
NCSA | National Center for Supercomputing Applications

General Travel Tips

- Read through various general travel tips at https://safetyabroad.illinois.edu/
  - There is considerable information on this site
  - Read through it several weeks/months ahead of time, particularly for international travel
- NCSA travel planning tool at https://internal.ncsa.illinois.edu/mis/travelplan/main.php

Consider what NOT to take

- Do you need your:
  - Computer
  - Tablet
  - Phone
  - 2FA token/Yubikey
  - data
- If you do not need it, do not bring it
- Consider purchasing a phone in your destination country
- Consider requesting a loaner laptop (particularly for international travel to “high risk” countries)
  - ITS can provide a loaner laptop (email at least 1 week ahead) help+its@ncsa.Illinois.edu
  - Unencrypted, clean laptop without any data on it

Backup Your Data

- Backup your devices before travel to ensure you have known good copies
  - include all devices: phone / tablet / laptop / USB flash drives / portable hard drives
- Record serial numbers, inventory tags, IMEI , property accounting PTAGs, MAC address
  - This information will be helpful to keep track of items if they are lost or stolen

Device Installs BEFORE Your Trip

Install, configure and be sure to actually TEST

- NCSA VPN software
  - https://wiki.ncsa.illinois.edu/display/cybersec/Virtual+Private+Network+%28VPN%29+Service
  - Understand the different connection profiles
  - This same software should work for the UIUC campus VPN too: https://answers.uillinois.edu/illinois/47199
  - VPN software can be installed on most smart phones and tablets too
- Lastpass (if needed)
  - NCSA Lastpass is restricted to specific countries: US, UK, CA, GB, CL, AU
  - You can use the NCSA VPN with the ncsa-vpn-tunnelall profile to access Lastpass
- Duo (if needed)
- ActiveSync Office365 device remote wipe capabilities for Illinois.edu email

Device Installs BEFORE Your Trip

Install, configure and be sure to actually TEST

- Anti-malware software – (Malwarebytes app for Android, Microsoft Defender)
  - Update and run a full scan before you leave town
- Disk Encryption (if not using loaner equipment)
  - Bitlocker on Windows – set a bootup PIN for added protection
  - Filevault on MacOS
  - Various encryption methods on other mobile devices
  - Consider additional per-file encryption (7zip files) if you need to take important data
- Consider using Google/Apple/Samsung Pay apps instead of credit cards

Device Installs BEFORE Your Trip

Install, configure and be sure to actually TEST

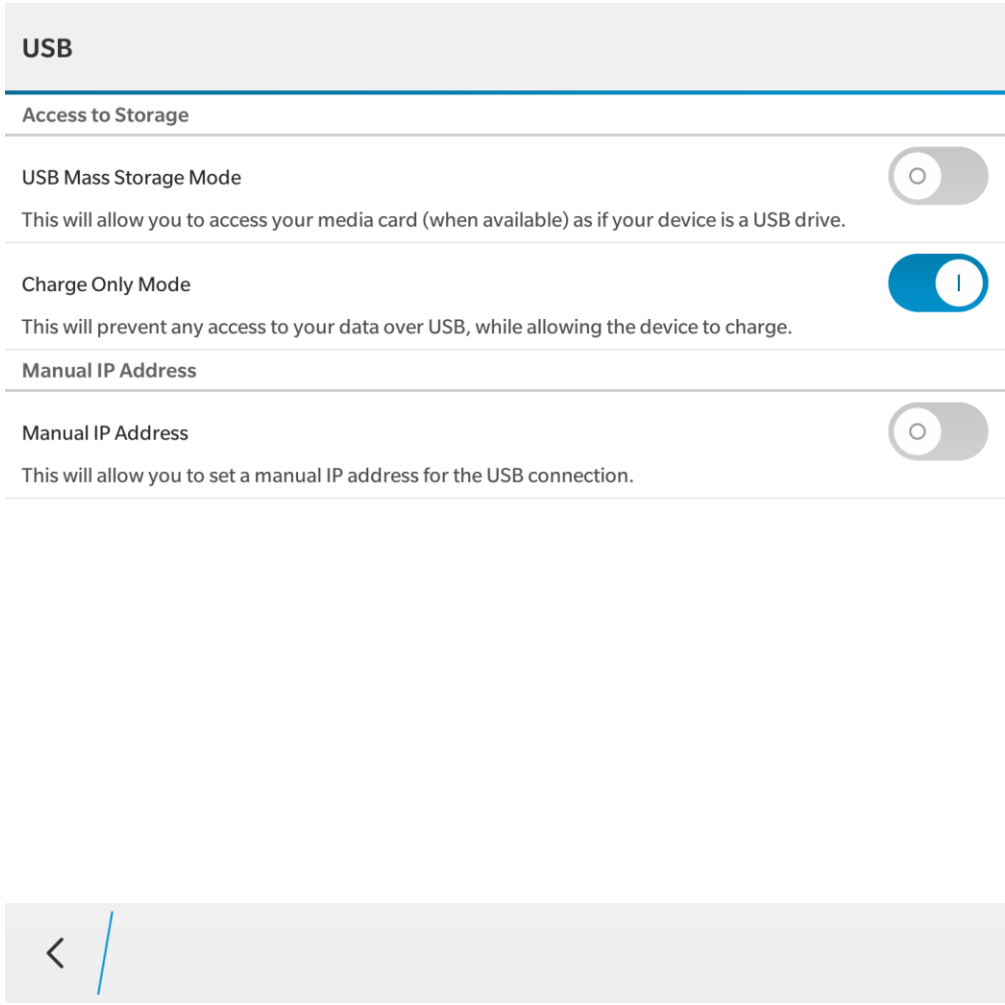
- anti-theft
  - https://play.google.com/store/apps/details?id=com.miragestacks.pocketsense
- Location Tracking / Remote Wipe
  - https://preyproject.com/ - free for up to 3 personal devices
  - ActiveSync devices can be remotely wiped via campus Office365
- Trip specific apps
  - Weather apps
  - Earthquake / Hurricane / Tsunami / Weather alert apps
  - Travel apps (airlines, etc.)
  - Maps (https://maps.me/ - has offline maps you can install and use even off network)

Device Updates BEFORE Your Trip

- Operating System updates
  - Follow your vendor's update procedures
- App/Software updates
  - https://patchmypc.com/home-updater-download can be used on Windows
- Driver/Firmware updates
  - These often contain important security fixes that protect your devices and data
  - Manufacturers provide updaters like Dell Command Update / Lenovo ThinkVantage
  - You can use https://www.iobit.com/en/driver-booster.php (can be installed from Patch My PC)
- Set passwords/PIN/screen locks on your devices
  - If your devices are lost or stolen, having the device locked should help protect your data

Disable Unused / Unneeded Functions

- Disable USB data to prevent “Juice jacking” attacks
  - Your device may have a setting for “charge only”
  - Can use a charge-only cable
  - Can purchase specific USB devices
  - https://portablepowersupplies.co.uk/
- Disable Bluetooth / NFC / WiFi
- Disable GPS / Location services
  - Note that some location tracking apps need this
- Disable file sharing apps/functions
- Disable auto-proxy discovery (WPAD)
  - Some networks might actually need this



Sanitize Devices/Data/Bags

- Remove SSH / x509 private keys from your devices
- Remove data
  - Export controlled data (hopefully is not on any mobile device)
  - NCSA/University data (unless needed for your trip)
  - Personal data – photos / tax returns / financial statements
- Clear browser history / caches
- Do you need your email cached on all of your devices or just one?
- Remove saved sites / favorites
- Remove phone contacts that you do not need for this trip

- A similar “sanitization” process can be done for laptop bags / wallets / purses

WiFi Worries

- Public WiFi in general (even when not traveling) should not be trusted
  - Use the NCSA or campus VPN with tunnelall profile
  - Connect to HTTPS sites
  - Do not ignore warnings about invalid security certificates on sites / services
  - Do not click on suspicious links
  - Turn off WiFi and disable autoconnect when not in use
- Phone hotspot
  - It might be better to create a WiFi hotspot on your phone and connect to it – be mindful of connection charges though
- eduroam
  - See if https://www.eduroam.org/where/ WiFi is available, especially if you are visiting a .EDU
  - Allows you to use your campus password to connect and you can setup and test Eduroam before you leave campus

While Traveling…

- Do NOT enter your credentials into public computers.
  - Clear your browsing history and close browsers when done
- Do NOT plug in untrusted accessories. Chargers/USB devices/ SD cards/etc
  - Use a charger you brought that plugs into an electrical outlet and do not use in-room USB ports
- Keep track of which passwords/sites you use while traveling for later on
- Be mindful of local laws when shopping online
  - Items legal to order in the US might be against local laws to order in other countries
- Turn Off and then reboot / power cycle device if taken out of sight at border
- Watch for “shoulder surfing” and obtain / use a privacy filter for your screens
- Do NOT leave your device unattended (in certain countries)
  - https://en.wikipedia.org/wiki/Evil_maid_attack

When You Return

- Use list of credentials / sites and change passwords from a trusted computer
- Return any borrowed equipment without connecting it to NCSA network
- Update anti-malware signatures and re-scan devices
- Consider wipe/reinstall of devices / restoring from the backup you made before traveling in case of compromise
  - Devices purchased abroad may have pre-loaded monitoring software
- Watch credit card / financial reports for odd activity and report it

Additional Resources

- https://safetyabroad.illinois.edu/
- https://research.illinois.edu/regulatory-compliance-safety/export-control
- https://www.ic3.gov/media/2012/120508.aspx
- https://www.us-cert.gov/ncas/current-activity/2019/05/24/Tips-Cyber-Safe-Vacation
- https://www.cyber.gov.au/publications/travelling-overseas-with-electronic-devices
- https://travel.state.gov/content/dam/NEWTravelAssets/pdfs/FBI%20business-travel-brochure%20(2).pdf
- https://www.cisecurity.org/wp-content/uploads/2017/03/Security-Primer-Traveling.pdf
- https://duo.com/decipher/a-traveler-s-guide-to-opsec

Contribute to Improving this Presentation

- https://go.ncsa.illinois.edu/traveltips
  - Add comments to this page with additional tips and we'll incorporate them into the page