Information Security
MURRAY STATE UNIVERSITY

Safe Computing Tips for Traveling Abroad

BEFORE YOU GO

- If you don't need it, don't bring it! Decide ahead of time what device(s) and data you will actually need, and do your best to limit what you take.
- Make an inventory of all data you do take. In case your device is lost or stolen you will need to know what has been lost.
- Backup your computer. If your device is stolen while traveling, a backup will ensure you don't lose everything. **Do not take the backup with you.*
- Consider requesting a loaner device from the MSU Library instead of your primary device and only load the data and applications *you absolutely need.*
- Change the password for any Internet services you use such as MyGate, Gmail, or Facebook. Enable 2factor authentication on any critical websites you use. Turn on Google's 2step verification to protect your Gmail accounts.
- If possible, encrypt your laptop, tablet, or other smart device. If the device is lost or stolen, your data is inaccessible. Windows 7-10 PCs can use built-in BitLocker encryption while Apple computers have FileVault. iOS devices are encrypted by default and many Android devices have an option to encrypt the device and any MicroSD card in use.
- Update all software immediately before travel, **especially antivirus**. (If software updates are necessary while abroad, download the updates directly from the software vendor's website).
- Consider using a VPN service on your devices to secure your Internet traffic, especially when using Wifi in public places or hotels. Most VPN providers have a monthly subscription option.
- If you need a cell phone while traveling, consider purchasing a disposable phone with international calling, such as an International PayGo or GoPhone, and leave your smartphone at home. If you absolutely must take your own phone, make sure to contact your provider *before you leave* to determine if your phone is international capable and purchase an international calling plan.

WHILE YOU ARE TRAVELING

- When checking web sites such as Gmail, Facebook, or your bank account, make sure you log in from a trusted computer using a secure web page. Secure web pages have addresses beginning with **https**. Do **not** use an untrusted computer, such as in a cybercafe or hotel business center to check email, Facebook, or your bank account.
- Be cautious when clicking on update pop-ups, especially while using untrusted hotel Internet connections. Some pop-ups are actually scams designed to trick people into installing malicious software. Update your software by going directly to the vendor's website to avoid this type of scam.
- If you believe your MyGate or RacerMail password has been compromised, you can reset it yourself on MyGate within the "Account Services" section of the "Home" tab. If you need additional help, contact the MSU Helpdesk at 270-809-2346.
- **For American citizens who feel endangered while traveling, contact the U.S. State Department Overseas Citizens Services:**

From within the U.S. **1-888-407-4747** From outside the U.S. **1-202-501-4444**

WHEN YOU RETURN

- When you return to the U.S., you should reset your passwords. If passwords *were* compromised while you were abroad, even if you aren't yet aware of it, changing them upon your return will render the stolen ones useless.
- If possible, erase and reload any devices taken with you. If malware was installed on your machine while traveling, this will aid in preventing further harm.

For more security tips on traveling abroad, visit
https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/hot-topics/security-tips-for-traveling-abroad