Digital Security Guidelines for Travelers

ITS Information Security | Middlebury College

Revision 1.2, Apr 16, 2025

Overview

The following guidelines are intended to help you understand and manage cybersecurity and digital privacy risks associated with travel, with the following disclaimers:

- No device can be completely safeguarded against all types of digital threats, especially when traveling to high-risk areas.
- International border crossings present different complexities that are not addressed here.
- Always observe all local laws and regulations.

Recommendation	*Destination Risk Level*		
	Low	**Medium**	**High**
Apply the latest software updates to all devices	✓	✓	✓
Use Multi-Factor Authentication	✓	✓	✓
Use complex passwords	✓	✓	✓
Use device encryption	✓	✓	✓
Use secure Wi-Fi for sensitive tasks	✓	✓	✓
Do not use shared or public computers for sensitive work	✓	✓	✓
Be careful you are not observed when unlocking or using your device.	✓	✓	✓
Remove unnecessary data from devices		✓	✓
Shift necessary data to the cloud		✓	✓
Leave personal devices at home			✓
Leave Middlebury devices at home			✓
Use only burner devices			✓
Use a temporary email address			✓
Disable facial and fingerprint unlock of devices			✓

Digital Security Guidelines for Travelers

Low Risk Travel

- **Install all the latest security updates on your devices.**
- Do not reuse passwords. **Use unique passwords** for each of your important online services.
- Use **strong passwords** for your really important online services, including your Middlebury account.
- Protect your digital accounts with **Multi-Factor Authentication (MFA).**
- **Never leave your devices unattended.** Theft of phones, laptops, and tablets is common, even close to home.
- **Secure your phone or tablet with a PIN or passcode.** A passcode or PIN will encrypt your data and help protect your accounts and information from prying eyes if your device is lost or stolen. Modern phones and all Middlebury managed devices are encrypted by default.
- **Uses secure Wi-Fi networks or cellular data plans to perform sensitive tasks.** Use your phone's cellular data plan when necessary and/or consider a commercial VPN option (see below).
- **Pay close attention to web browser security warnings.** Warnings that your "connection is not secure" could indicate that someone is attempting to steal your password and data.
- **Do not use shared or public computers for sensitive work.**
- **Be careful you are not observed when unlocking or using your device**. A strong passcode can help protect your device, but watch out for "prying eyes" who may try to steal your passcode and device.
- **Report lost or stolen devices to ITS immediately:** 802-443-2200, helpdesk@middlebury.edu.

Medium Risk Travel

- **Remove unnecessary data from your device before traveling**. The less data on your device to begin with, the less you have to be concerned about should your device go missing.
- **Shift necessary data to the cloud**. "Travel light" by moving required data to Middlebury's OneDrive, Google Drive, or other approved storage location.

High Risk Travel

- Phones, computers, and tablets may be searched without your consent or knowledge.
    - **Any and all data stored on devices you travel with may be scanned and copied**.
    - Any **devices left unattended may be tampered with**, perhaps in undetectable ways.
- Do not bring your daily use phone, laptop, or tablet to a high risk location.
    - **Leave your personal devices at home.**
    - **Leave Middlebury devices at home.**
- Make use of "**burner"** devices, i.e. temporary use-only phones, laptops, and/or tablets.
- Create a **temporary email address** for use while you are travelling.
- Upon return, at a minimum, do a complete **"reset to factory defaults**" on any devices you travelled with, restoring your data and apps from your cloud services.
- **Reset passwords** for any technology services you accessed while away, including your Middlebury password.

Additional Resources

International Travel Guidance

- US FCC: Cybersecurity Tips for International Travelers
- Princeton Information Security Office: Travel Guidelines
- FBI Counterintelligence: Business Travel

High Risk Areas

- US Department of State: Travel Advisories
- US Department of State: US Students Abroad