



International Division
UNIVERSITY OF WISCONSIN-MADISON

Cyber and Data Security Abroad

International Safety and Security
University of Wisconsin–Madison

Before You Go

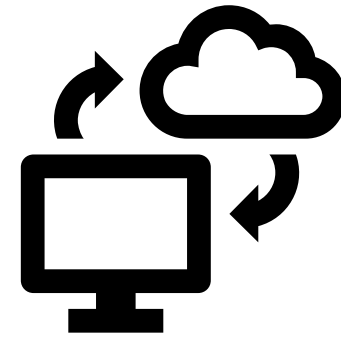
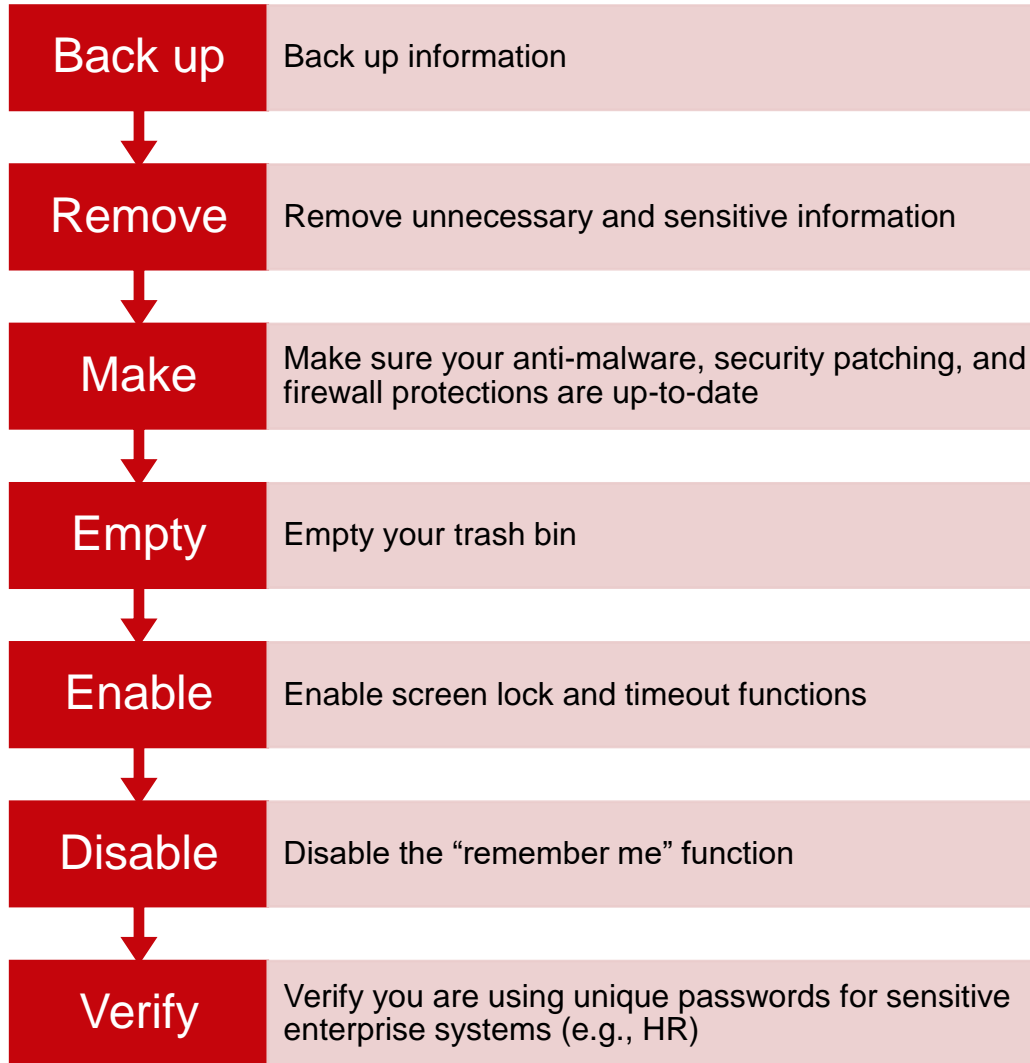
- Consider reserving a loaner laptop or cell phone from DoIT to limit the amount of data at risk
- Bring only “must-have” electronic devices with you, those that are really necessary for the trip’s purpose
- Familiarize yourself with local laws and security
 - See the U.S. Department of State’s country-specific webpage for your destination, and read the information under the expandable tabs:
<https://travel.state.gov/content/travel/en/international-travel/International-Travel-Country-Information-Pages.html>
- Enroll in the Smart Traveler Enrollment Program (STEP) to receive messages/alerts directly from the U.S. embassy at your destination



Enroll Now

<https://step.state.gov>

Sanitize Your Devices



Remember



You may be compelled to share access to any/all files on your devices while abroad, including a demand to decrypt protected files or drives.



Do NOT take any patentable, proprietary, or sensitive materials/files on your devices.

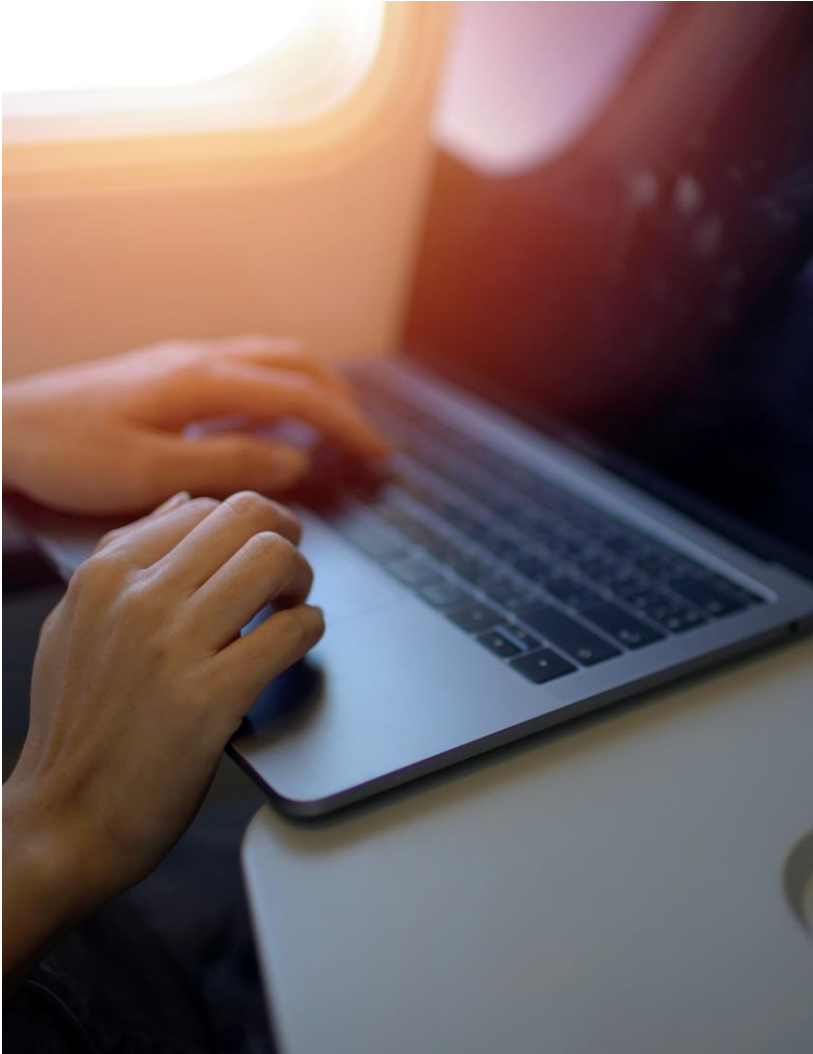


If presenting, try to review the presentation so that content is not so specific that it may allow others to exploit your professional work.



You may lose your work to those who do not care about US law, disciplinary standards, or professional propriety!

During Your Travel



- **Have no expectation of privacy**
- Keep all electronic devices and sensitive information in your possession
- Disable your devices' network capabilities (Bluetooth and Wi-Fi) when you are not using them
- Only visit secure websites
- Always manually enter your username and password
- Avoid accessing systems with sensitive or restricted information from abroad
- Use a VPN whenever possible, but remember use of VPN may be unlawful in some countries – *find out to be certain it is allowed!*

Upon Your Return

When you return to the United States, do not connect to a personal or business network until you run your antivirus and malware software or take your device to your organization's IT specialist to be scanned.

Do not forget to scan and/or clean any USB-connected thumb drives you may have used!

Return any loaner devices to DoIT for analysis and cleaning. Make sure to save any information you need in another location once the files are scanned.

As soon as your device is scanned and known to be clean, change all your passwords and PINs.

Report loss or theft of information or electronic devices to help@doit.wisc.edu.



International Safety and Security

UW-Madison International Division

Ronald Machoian, PhD
International Safety and Security Director

256 Bascom Hall

ronald.machoian@wisc.edu

608-890-2446

Website: <https://internationaltravel.wisc.edu/>



UW-Madison Information Technology

Connecting & Supporting Our Digital Campus

Information Technology – Get Help

Website: <https://it.wisc.edu/help/>