

A light gray world map is visible in the background, centered on the Atlantic Ocean. The continents are shown in a darker gray shade against the white background.

Device Security and Loaner Program

Kyle Filipe

Director of IT Support Services

IS&T

Secure Data Travel Recommendations – Highlights

Before Travel:

- Backup your data. IS&T makes [CrashPlan](#) available for free to the community
- If don't have currently: [encrypt](#) your devices; install security applications ([Crowdstrike](#), [Sophos](#), [VPN client](#))
- Bring the least amount of information and data on the fewest devices possible. Store potentially sensitive material on an encrypted flash drive
- Consider new loaner device program (more to come)

During Travel:

- Use [MIT's VPN](#) (if not prohibited) to create a more secure connection between your devices and the resources you need to access
- Do not use unknown USB drives
- Avoid downloading and using apps that sync data, and instead use outlook.com or owa.mit.edu for email, Dropbox on the web, etc.

After Travel:

- If you traveled with a loaner device, or wiped your devices before traveling:
 - Copy any data you've modified onto an external drive
 - Scan the data for viruses. IS&T makes [Sophos](#) anti-virus software available for free for the community
- Reset passwords

FREE Loaner Device Program

Why should I borrow loaner devices?

- Using loaner device is more straightforward than the complex process of configuring your personal device
- Devices are already configured with settings to achieve a more secure computing experience
- Less risk with loss/theft or confiscation. IS&T can lock or wipe the devices to protect the data they contain under certain scenarios

What devices are being offered?

- Travelers may request up to one laptop, one tablet, and one phone (free cellular data plans available if needed)
- A base suite of apps are currently installed on all issued devices. Additional apps may be added to devices upon request; we are flexible and will review all app requests to ensure the devices are able to support your work

Who can borrow devices?

- Faculty, staff, and students

When should I borrow devices?

- Can borrow anytime you are traveling abroad (business or personal) and encourage this
- MIT **strongly recommends** borrowing devices when traveling to any destination with a **Level 3 or higher** travel advisory [designated by the U.S. Department of State](#)

How do I submit a request?

- Visit IS&T's [Secure Devices for International Travel](#) website to learn more and submit your request

Additional IT Guidance

- [Travel and Technology guidance](#) in the Knowledge Base
- [Secure Travel Recommendations](#) for “High Risk” destinations
- [Secure Devices for International Travel](#) IS&T loaner program
- [Protecting Information at MIT](#)

Questions? Email ist-loaners@mit.edu

KB The Knowledge Base

[Home](#) [Edit](#) [View](#) [Watch](#) [Comment](#) [History](#)

Travel and Technology Landing Page

On this page:

- Overview
 - Before you travel
 - ✓ Back up your laptop
 - ✓ Back up your mobile device
 - ✓ Secure your computer...
 - ✓ ... and its data
 - ✓ Test your software
 - ✓ Plan for connectivity
 - ✓ Check all necessary chargers and cables
 - ✓ Update voicemail greetings and e-mail auto-responders
 - ✓ Have a "Plan B"
 - While traveling
 - ✓ Never leave your device unattended
 - ✓ Whenever possible use the MIT VPN client
 - ✓ Check your mobile device settings
 - After you travel
 - ✓ Perform a full virus-scan of your computer
 - ✓ Reset any e-mail automatic replies or voicemail greetings
 - International travel considerations
 - Resources
 - See also