Travel and Technology Landing Page

Travel and Technology Landing Page

On this page:

Overview

Traveling with your computer and smartphone can present special logistical and security challenges. Taking a few steps to prepare for your trip and think about what could go wrong can help save time recovering from issues encountered during travel. These tips are not exhaustive, and sometimes specific destinations may warrant additional (or fewer) preparations.

This article does not attempt to recreate the many excellent third-party resources that exist on this topic for academic professionals. It adds some MIT-specific details, but please review the Resources list below for details, how-to guides and international travel security advice collected by EDUCAUSE.

For more information, including travel to high risk areas, see: Secure Travel Recommendations

Before you travel

Contact tech support BEFORE you travel
We recommend contacting your local IT support provider to ask if a sanitized loaner computer and/or mobile device is available for use while traveling. Alternatively, you may be eligible for loaner equipment from IS&T. For more information, see: Secure Devices for International Travel.

Back up your laptop

- If you are using MIT's Crashplan service, verify that backups have run successfully. Use the Crashplan web interface to inspect backed

up files.
- If you are using another backup solution, such as Apple's TimeMachine, launch the client on your computer and run a backup before your trip begins.

Back up your mobile device

- You may want to synchronize your smartphone or tablet with your computer or verify that you are synchronizing it with iCloud (for iOS devices) or Google (for Android devices) before you leave. See the following knowledgebase articles on backup for [iOS] and [Android] devices.

Secure your computer...

- If you have not already done so, register your laptop with the MIT Police, and make a note of the STOP tag number.
- Make a note of the serial numbers of all your devices, and keep a copy of that information somewhere at MIT, so you or your colleagues can provide the information to law enforcement if your devices are stolen.
- For more tips, see How do I protect my laptop while traveling?

... and its data

⚠ Avoid taking sensitive data unless absolutely necessary.

- If you have sensitive data on your machine, make sure full disk encryption is enabled.
- Ensure your computer does not automatically log you in when it powers up, and ensure a screensaver/wake-from-sleep password is set before allowing you access to your machine.
- See Encryption at MIT for more information, as well as the international considerations section of this page.
- If traveling with a non-sanitized laptop, we recommend running a scan with Spirion to find any Personally Identifiable Information.

Test your software

- Ensure that your anti-virus and malware detection software is up to date. IS&T's recommended security suite is Sophos and Crowdstrike.
- Test your connection to the MIT Virtual Private Network (VPN). IS&T recommends the using the VPN client whenever you are connected to a public WiFi network (for example, in a hotel or coffee shop) as public wifi is not secure and poses a threat to your data and devices.
- If you will be using any other software or apps during your travels, take a moment to ensure they are up to date and working correctly.

Plan for connectivity

- Find out whether you will have wireless Internet connectivity at your destination. If you will only have wired Ethernet connectivity, make sure you bring an Ethernet cable and any adapters your computer may require.
- Verify whether or not you will have cellular voice and data service at your destination. Contact your cellular provider to determine what charges, if any, will be incurred for roaming or to determine whether a short-term international plan is available (See the international section of this page for more information).
- Use Eduroam. Eduroam wireless networks, providing the same level of security as MIT SECURE, are available at thousands of educational and research institutions in the U.S. and over 70 countries.
    - US locations
    - Global overview map
- Avoid any activities on public computers. If at all possible, is better to use either cellular data or a mobile hotspot. If absolutely necessary, use it as little as possible and ensure you don't save any passwords or other information locally. Log out of all accounts before leaving the device. Also, clear your browsing history and cache.

Check all necessary chargers and cables

- Make sure you have chargers and cables for all your devices.
- Are you giving a presentation? Bring the cables and adapters that connect your computer to a projector.
- If you're traveling internationally, make sure you have any necessary adapters. Even if your charger is dual-voltage, you will likely still need an adapter to connect to other power sockets.

Update voicemail greetings and e-mail auto-responders

- You may wish to set an Out-of-Office reply for email that informs people you will have limited e-mail access and/or directs people to contact your assistant or colleague.
- Update your Zoom Phone Service voicemail greeting to let callers know you're away.
- For safety reasons, consider limiting what details you include in these messages. See What should I put in my Out of Office message? for more information.

Have a "Plan B"

- Make sure you have another way to access your data or give a presentation if your laptop breaks.
- If you are traveling internationally, obtain the customer service phone number for your mobile provider in your destination country.
- If your laptop is currently covered by a warranty, you may also wish to find out how to obtain repair service while traveling internationally. For example, is there an Apple Store near your destination? What is the telephone number for hardware/software service in your destination country?

While traveling

Never leave your device unattended

- Never leave your laptop or mobile device unattended, especially in public locations such as airports or cafés. If you must leave your laptop in your hotel room, make use of an in-room safe, or use a cable lock.

Whenever possible use the MIT VPN client

- Whenever possible, start a connection to the MIT VPN when using public network connections, however...
- **Some countries may restrict types of traffic, certain internet destinations, and technologies you can legally use, including connecting via a VPN. When traveling to such destinations always inform yourself of applicable laws and restrictions, and obey them. For more information about specific destinations:**
    - Consult the U.S. State Department's country database
    - Consider enrolling in MIT's International S.O.S. Program managed through MIT's Office of Insurance
        - Information about MIT's International S.O.S. membership
        - International S.O.S. MIT Program Portal
        - International S.O.S. provides important emergency services while you travel, and also maintains a help line for detailed advice on specific countries, local customs and laws, and restrictions you might encounter.

Check your mobile device settings

- If you're traveling internationally, consider disabling the International Data feature in your smartphone or tablet, as roaming charges can accumulate quickly.
- Turn off all location services/sharing except when actively using services that require it, such as maps, as this can result in unintended data exposure.

Mind Your Social Media Presence

- Take care when sharing travel updates. Delaying posts can protect you from broadcasting your location or absence to attackers who may take advantage of knowing where travelers are staying or homes/offices are unattended. If you do want to posy real time updates, adjust your privacy settings to restrict who can view your content to known safe associates. Never post a photo of your boarding pass, ID, passport, hotel, room number, address, license plates, or other travel-related documents and identifying information.

Be Aware of Physical security

- Be mindful of shoulder surfers who may be trying to catch a glimpse of your screen, travel documents, map locations, or accommodation information.
- Take care when speaking on your cell phone that you do not divulge information about your accommodations, travel plans or locations. Bad actors can use this information to attempt to access your home or travel locations when you're not there or to intecept you in a vulnerable location while you're in transit.
- Safeguard your physical devices and use personal chargers to reduce the risk of compromised charging stations.
- Use the hotel safe for passports, other important travel documents, cash, and valuables.
- Keep your phone with you at all times and use a passcode to keep it locked. Be sure to your pockets before you get up from a seat in public to ensure your phone, wallet, hotel key and other valuables are with you before you leave any location. Report them lost or stolen immediately if they are not and take measures to have them wiped and/or deactivated.

After you travel

Perform a full virus-scan of your computer

- Upon your return, perform a full virus-scan of your computer, particularly before exporting any data from your laptop.

Reset any e-mail automatic replies or voicemail greetings

- If you previously set an "Out of Office" automatic reply, remember to disable it once you're regularly checking e-mail again.

- If you previously set an "alternative greeting" on your voicemail box, remember to disable it or switch to your default greeting once you're regularly checking voicemail again.

International travel considerations

- Contact your cellular provider to determine whether your voice and data service will be available in your destination country, and what charges will be incurred for international roaming. Alternatively, you can arrange for a loaner or pre-paid cellular phone when you arrive at your destination.
    - Your mobile device may allow you to switch SIM cards. You can often buy a pre-paid SIM card in your destination country, which may be more cost-effective than paying roaming charges. Your mobile device must be "unlocked" in order to switch SIM cards. Contact your cellular provider for more information.

- International cellular service may impact the behavior of Duo two-factor authentication. See Duo for International Travelers.

- If your trip involves a border crossing, special rules and considerations may apply. These can vary widely by destination. In general, be aware that when crossing a border your laptop and electronic devices may be searched and handled by individuals other than yourself.
    - You may be asked to provide passwords to your devices by local authorities. If you frequently access remote resources such as cloud storage services or web services on MIT campus, make sure passwords for those are **not** stored on your laptop or in your browser.
    - For some destinations you may want to consider bringing a laptop or mobile device borrowed and provisioned especially for your trip, which only contains the data and software you will need while abroad. This device should then be wiped of all content upon your return.

- Certain travel destinations are reputed to conduct routine surveillance of electronic transactions, including email correspondence, web browsing history, financial transactions and phone conversations.
    - When traveling to areas with a reputation for monitoring communications, consider setting up a temporary email account used for the duration of the trip and known only to a few individuals.
    - If you are using your regular email address, set an account password which will be used only for the duration of the trip. Limit communications by email and phone to those who understand that conversations may be monitored, and should not contain sensitive data or information. Advise those trying to reach you (see Update voicemail greetings and e-mail auto-responders) that you'll have unreliable communications while traveling, and direct them to an alternate email address or phone number which will be staffed by an individual at your home location

- Certain types of technical data and software fall under additional restrictions. See Export Controls for Travelers

For an exhaustive list of security, data protection, and privacy information with specific details for particular destinations please take a look at the **Security Tips for Traveling Abroad** pages maintained by EDUCAUSE, linked in the Resources section below.

Resources

- **MIT's Information Protection**
  MIT's Written Information Security Program (WISP). This program is based on classifying Institute research data and administrative information according to the risk posed by the loss of confidentiality, integrity, or availability of the information. For each level there are associated tasks to appropriately secure the information at that level, along with links to instructions for how to complete each task.

- **Internet2 Security Tips for Traveling Abroad**
  This collection of guides and resources contains the best how-to and advice pages from higher education institutions and the US Government.

- **How do I protect my laptop while traveling?**
  This article in the Knowledge Base goes into detail on how to protect your laptop during your trip, and resources such as insurance you can use to recover from issues.

- **Mobile Devices**
  This collection of services and resources outline how to protect your phone or tablet, secure the data contained on these devices, and what to do if your device is lost or stolen.

- **MIT's Travel Policy** and **Travel Resources** pages
  These resources are maintained by the Office of the Vice President of Finance (VPF) as part of the VPF Travel Site at http://vpf.mit.edu/travel

- **MIT Information Protection and Sensitive Data**
  This site talks about MIT's sensitive data policies (not specific to travel) and resources you can use to protect data on your computer.

- **Export Controls for Travelers**
  Regulations affecting members of the MIT community provided by the Office of Sponsored Programs.

- **SLIDES (pdf): Jan 2014 ICC presentation**
    - **Technology Tips for Travelers**, Jonathan Reed (IS&T), David Quimby (OSP)

    - **Safety: ISOS, High-Risk Travel**, Sandy Mitchell, Sarah Voigt (Insurance)
    - **Travel Clinic: Health Considerations**, Dr. Howard Heller (Medical)
    - **EHS Concerns**, Lou DiBerardinis (EHS)
    - **Travel Policies and Money Matters**, Kara Byrne Sechrist (VPF)
- **VIDEO: Jan 2014 ICC presentation (50 min)**

- Traveling Securely: A Comprehensive Guide to Protecting Your Digital Footprint While on the Move
- A great Trip Advisor article on cell phones in Japan
- How to Pick a Cellphone Plan for Traveling Abroad from the *New York Times*, June 16, 2015.
- How Tech Can Ease Your Summer Travel from the *New York Times*, August 2, 2017.

See also

- Secure Travel Recommendations