Top 5 things to know about technology when traveling abroad

Jessica Murray
Information Security Officer
IS&T
December 11, 2023
1. Travel resources from IS&T

- Loaner Device Request
  [https://ist.mit.edu/secure-devices-travel](https://ist.mit.edu/secure-devices-travel)

- IS&T Knowledge Base kb.mit.edu
  - Travel and Technology Landing Page
    [https://kb.mit.edu/confluence/display/istcontrib/Travel+and+Technology+Landing+Page](https://kb.mit.edu/confluence/display/istcontrib/Travel+and+Technology+Landing+Page)

- Secure Travel (High Risk)
  [https://kb.mit.edu/confluence/display/istcontrib/Secure+Travel+Recommendations](https://kb.mit.edu/confluence/display/istcontrib/Secure+Travel+Recommendations)
2. What will you bring?

• A loaner device is recommended
  • especially for High Risk Travel
  • laptops, tablets, and phones available
• Will your cell phone work internationally?
• Do you have all your power cords?
• Consider a Yubikey for Duo authentication
• Test new devices or apps before you go
3. Protect your devices and data

• [https://infoprotect.mit.edu](https://infoprotect.mit.edu)
• Backup your devices before you go
• Bring only the data you need
  • If a loaner device is not available, after you back up the device you can wipe and reinstall a clean copy of the OS etc.
• Update your operating system and applications
• Encrypt your devices (laptop, phone, external drives)
• Install security applications (Crowdstrike, Sophos, VPN client)
4. While you are there

- Don’t leave your devices unattended
- Be mindful of your surroundings when entering passwords or accessing information
  - “Shoulder surfing,” reflective surfaces, or security cameras
- Utilize the MIT VPN (if not prohibited)
- Don’t use unknown USB drives
- If using a loaner or a wiped device, use outlook.com or owa.mit.edu for email, Dropbox on the web, etc. instead of installing clients that sync data
5. When you return

• If you traveled with a loaner or wiped your devices before traveling
  • Copy any data you’ve modified onto an external drive
  • Scan the data for viruses (Sophos)
• Wipe and reinstall, restore data from backup
• Reset out of office messages
• Reset passwords