GENERAL TRAVEL TIPS

Before You Go:

- Apply any updates for your mobile and/or laptop computer operating systems.
- Backup any important information, contacts, photos, videos and other mobile or laptop device data with another device or cloud service.
- Set up multi-factor authentication for your accounts for an additional layer of security.

  Haas faculty, staff and employees are required to be enrolled in CalNet 2-Step, and travel with backup passcodes, as an alternate authentication mechanism.
- Secure or request access for the services you need during your trip, like international mobile roaming services and VPN access.

  Learn more about mobile roaming in the Haas Telecom Services Policy page.
  Learn more about Campus VPN access at the Campus Technology page.
- Keep your devices locked/password-protected when not in use.

During Your Trip:

- Protect your personal items (like your passport), data, and devices, and never leave them unattended.
- Do not use unfamiliar devices to log into Haas- and University-owned resources.
- Always use the Campus VPN to access Haas- or University-owned resources when traveling.
- Public locations and networks (internet cafes, hotels etc.) may not offer enough security or privacy. Keep this in mind when sharing or sending data across unknown or unfamiliar networks and Wifi services.
- Do not connect your phone or laptops to unknown storage devices, as these can install malware or even copy your data.

Upon your return:

- Check your devices and email accounts for any suspicious material or unusual items/activity.
- You may consider changing your passwords for all devices and accounts used during the trip.
- If you are uncertain about the status of your devices, you may contact Haas Help Desk and ask a technician to help scan your devices for you.

See more travel tips on this U.C. Berkeley Information Security and Policy page.