Vacation & Travel Cybersecurity Tips



Cybersecurity isn't just for the office—it's just as important when you're traveling on vacation. Consider these steps to protect your personal data and stay safe online while traveling.

Before You Go



- **Update your devices and apps**
  Install all system and app updates on your phone, tablet, and laptop. These updates often contain important security patches.
- **Lock your devices**
  Always lock your device when you are not using it. Set strong PINs, passwords, or biometric locks *(like fingerprint or facial recognition)* on all your devices.
- **Enable "Find My Device"**
  Activate remote tracking tools like Apple's Find My or Google's Find My Device. These can help locate lost devices and, if necessary, erase them to protect your information.
- **Adjust privacy settings**
  Review your app and social media privacy settings. Limit who can see your posts and disable location tracking for apps that don't need it.
- **Back up your information**
  Back up your contacts, photos, and other important files. If your device is lost or damaged, your data is still available to you.



While You Travel

- **Disable auto-connect features**
  Turn off automatic Wi-Fi and Bluetooth connections, especially in public places like airports and hotels. Auto-connect can expose a device to unsafe networks.
- **Manage location sharing**
  Only enable location services when necessary. Most apps don't need constant access to your location—only allow what's essential.
- **Avoid public Wi-Fi**
  Public Wi-Fi is convenient but risky. Confirm the Wi-Fi name with staff to ensure you're using the appropriate network. Avoid logging into sensitive accounts without using a VPN or your phone's hotspot for added security.
- **Be cautious using public computers**
  Public computers may not be secure. Avoid logging into personal accounts on these devices. These machines may be infected with malicious viruses or software. If you must use them, always log out of any accounts you have accessed rather than only closing the browser window.

Welcome Home



- **Check your account activity**
  Once home, review any accounts you used while traveling for any suspicious activity or login attempts. Report anything unusual right away.
- **Remove unused travel apps**
  Delete any apps you downloaded just for your trip, like ticketing or local guides. Unused apps may still access your data. You can always reinstall them later.

UNIVERSITY of HOUSTON SYSTEM
INFORMATION SECURITY

Staying cyber-safe while traveling doesn't have to be complicated. With just a few proactive steps, you can enjoy your adventures—and your tech—without worry.