BLACKCLOAK™

Cybersecurity Travel Tips

BEFORE, DURING AND AFTER

Whenever you travel, and abroad particularly, the more cyber threats you face. Your personal and business devices carry sensitive information that is highly valued by cybercriminals. Therefore, it is important to stay mindful of cybersecurity best practices as you travel. Here are some simple tips to follow to ensure you have a safe and hassle-free trip!

Important Websites

Review the State Department's website

https://travel.state.gov/content/travel/en/international-travel.html

for cybersecurity laws and regulations and any travel advisories specific to the country you will be visiting

Enroll in the Smart Traveler Enrollment Program (STEP)

https://step.state.gov/step/

to receive alerts for the country you plan to visit and establish contact methods while your abroad

Review the Overseas Security Advisory Council (OSAC) website

https://www.osac.gov/Country

for the specific country you are visiting for security alerts, travel advisories, and embassy information

Before Departing on Your Trip

- ✓ Ensure device operating systems and apps are up-to-date to protect against malware/viruses.
- ✓ Backup your data in case you lose your device (or it is stolen) while traveling.
- ✓ Remove sensitive data from your devices and clear browsing/cookie history.
- ✓ Store passwords you use regularly in a password vault.
- ✓ Enable locking of your devices through auto-lock, Touch ID/Face ID, Pin/Password. An unlocked device is an open door for an attacker.
- ✓ Disable auto-connect to Wi-Fi and Bluetooth, and minimize location sharing so you connect only to wireless and Bluetooth networks when you want to.
- ✓ Install a device finder and/or enable the Find My Device feature on your devices.
- ✓ Consider taking a "burner" phone or laptop with you and leave your personal devices at home so you are not bringing sensitive information with you. You can toss and/or wipe the device when you return.

While Traveling

- Use BlackCloak's RFID Passport and Credit Card Holders. (if you don't have one or need more, just email us!)
- Do not leave devices unattended and do not check them with your luggage in the belly of the plane. You may never see them again.
- Consider using a privacy screen for your laptop.
- Be cautious of public Wi-Fi as they are vulnerable to security issues and cybercriminals love them. Instead, use our trusted VPN solutions when conducting sensitive/financial matters.
- Avoid using publicly accessible equipment – such as phones, computers and fax machines. They are likely to be less secure and potentially infected with malware.
- Please use the hotel safe and when you do, use a different pin than you use at home.
- Don't directly connect your devices to public charging kiosks. If you need to charge your device, first connect your device's USB cable to the BlackCloak USB Protector and then into the kiosk.
- Don't click links or email attachments you are unsure of. Phishing attacks can happen anywhere!

Upon Return from Your Trip

Update your devices and software again

Change your passwords on all devices

Perform a backup of your trip and remove apps used while traveling that are no longer needed

Check your financial and credit card statements for any suspicious charges incurred while traveling

Rest assured that BlackCloak will be continuously monitoring your devices for malware and viruses while you're away and when you return. If we identify an issue we will notify you!

QUESTIONS?

The BlackCloak Team is here to help you! If you have questions or concerns regarding your travel, contact the BlackCloak Concierge team.

To learn more, please visit: **blackcloak.io**