

INTERNATIONAL TRAVEL SECURITY TIPS AND CHECKLIST

SECURE PASSPORT AND ALL TRAVEL DOCUMENTS

Keep your passport and visa with you at all times. To maximize your personal safety, remember to always travel with valid identification (i.e. international passport with valid visa). Maintain paper copies and photographs that you can access on your phone of the following: driver's license, passport, birth certificate, immunization record, credit card(s).

MINIMIZE THE CASH YOU CARRY

Determine the amount of cash you may need for emergency needs (transportation, food, etc.) and then use credit cards as much as possible. Notify your credit card company's fraud department of the countries you will be visiting and on what dates. Include those countries where you might have a layover.

DO NOT WALK/TRAVEL ALONE

Always walk with a partner or in groups to maximize your personal security while abroad.

USE EXTREME CAUTION WHEN USING CABS/CAR SERVICES

Where possible seek the assistance of your team, hotel or apartment staff to identify a driver or car service.

SOCIAL MEDIA: BE CAREFUL WHAT YOU TWEET, POST, ETC.

Limit status updates, geotags on pictures and other kinds of information you share on any social media platform while traveling. Be careful not to share too many details when describing your private life or travel plans. Note, however, that in an emergency, updating your status may be an effective way of communicating with family and friends.

RESPECT INTERNATIONAL LAW, CULTURES, AND CUSTOMS.

Most people traveling internationally expect differences. It is important to know the law of the country and to demonstrate respect for its culture when visiting.

DO NOT LEAVE ELECTRONIC DEVICES UNATTENDED

Never store valuables or electronics in your checked luggage. Report stolen devices to the US embassy or consulate.

ANTIVIRUS AND OTHER SOFTWARE UPDATES

Make sure your antivirus, security patches, and firewall are enabled and current. Updates should be done before you leave because you may receive a fake security update that ultimately seeks to install malware or spyware on your computer when connecting to a local network in a country overseas.

WI-FI / THE INTERNET: THERE ARE NO EXPECTATIONS OF PRIVACY

Many countries overseas do not have the same privacy protections for electronic communications. Be mindful that any cell phone conversation, email or internet browsing may be intercepted by local private or governmental entities. Avoid Wi-Fi if possible. Where possible use a VPN connection before you log into any websites or access sensitive data. Beware of “phishing” scams referencing local attractions and businesses.