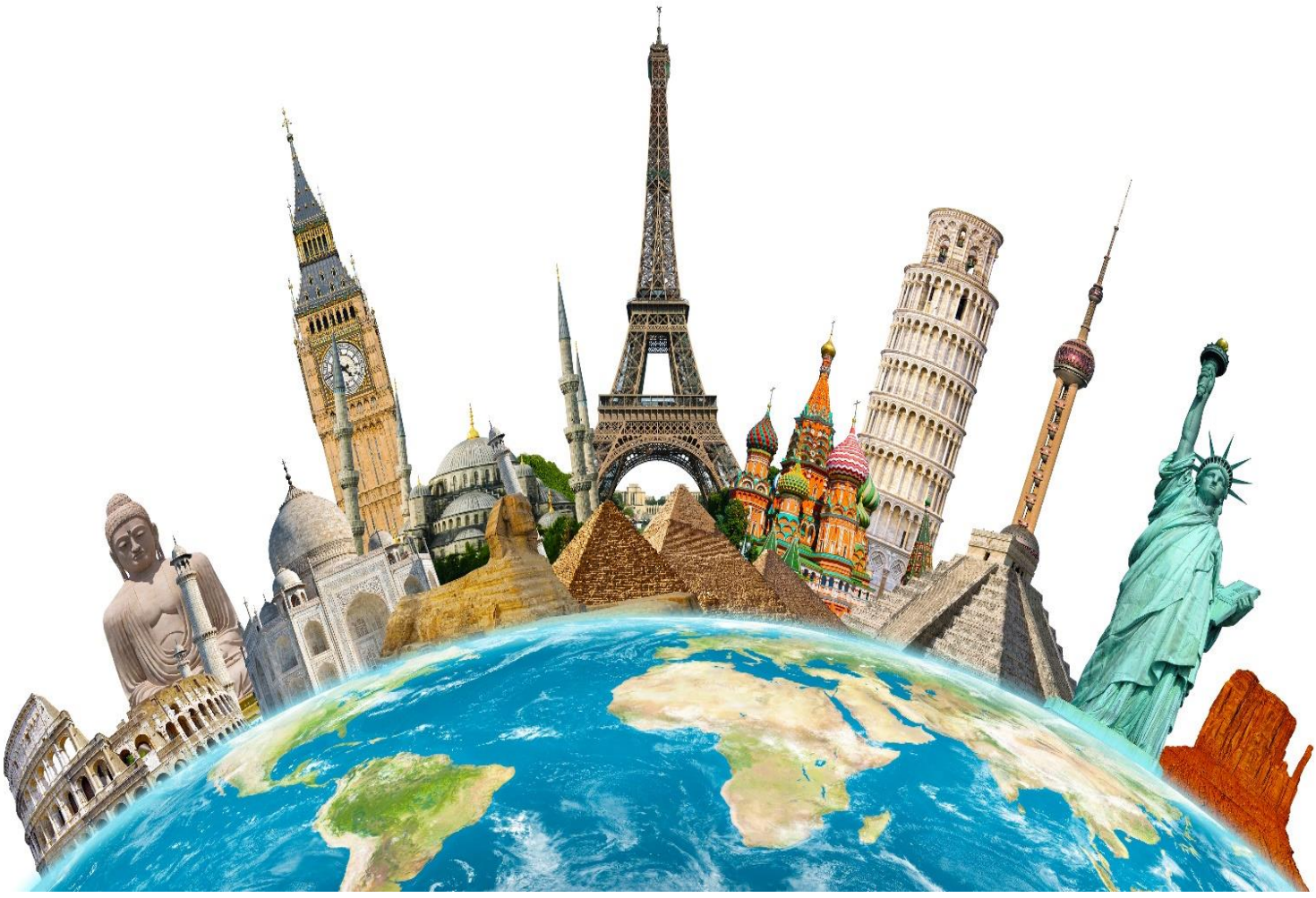
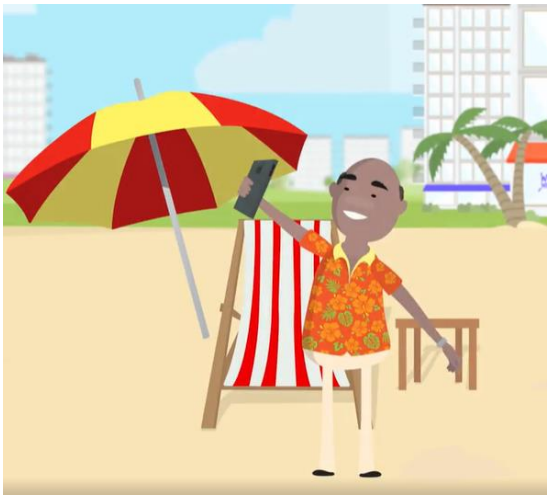
CSU COMPUTER SERVICES UNLIMITED

Travel Tips:

Safety and Security



Travel Safety and Security Tips



No matter how you get to your destination or where you choose to stay, you will still be connected when you're on vacation.

Many travelers rely on technology even more to enhance their experience. As you embark upon your next adventure, stay cyber-safe while away from home by following some simple practices to help keep your devices safe and your vacation plans from going awry.

GETTING READY TO GO

Before you head out on vacation, here are some security tips to add to your packing routine:

The Trip is Only Part of the Equation
Remember, your vacation starts (at least from a cyber criminal's perspective) from the day you book the trip through the weeks after you have returned.

Be Cautious When Booking Hotels and Travel

Book directly with a known online booking company and access by typing in their address rather than using a link in an email. Hackers are creating look-alike websites that can steal your information, including credit card numbers.

If a booking agent calls you out of the blue, they may be a scammer. Hang up and call the property directly.

Hotel and Airline points can be targeted by scammers who send random emails advising that you log in and reset your password. Go directly to your account and check your account. If 2-factor authentication is available, take advantage of the extra security.

Never pay by wire transfer, cryptocurrency or gift cards, which they often will not be able to get back. Don't fall for 'How can we offer such a good deal? It's because we don't have the overhead of traditional credit cards.'"

Don't sign or pay until you know the terms of the deal. Get a copy of the cancellation and refund policies before you pay. If you can't get those details, walk away. Say "no thanks" to anyone who tries to rush you without giving you time to consider the offer.

Make sure you are monitoring your accounts before, during, and long after your trip in order to watch out for suspicious activity.

Travel lightly

Limit the number of devices you take with you. The more you take with you, the more risk you open yourself up to.

Protect your credit, debit, identification, and money cards from electronic fraud

RFID (Radio-frequency identification uses electromagnetic fields to automatically identify and track tags attached to objects. An RFID system consists of a tiny radio transponder, a radio receiver, and a transmitter) devices can scam your pocket or purse to steal your card's information. RDIF-blocking sleeves and wallets are readily available.

(Resource: Nick MacDiarmid, Director, Cyber Incident Response, Marriott*)

Be cautious of clicking links in travel promotion emails; hover over links to be sure they are going where they say they are going. Use credit cards rather than debit cards because they offer better fraud protection. If it sounds too good to be true, it probably is! Confirm your reservations directly with the hotel or airline. (Resource: Liz Buser, Senior Advisor, Fraud Prevention Programs, AARP*)

When traveling to high-risk countries or limited consulate services, be sensitive to the environment where you will be traveling. The State Department recommends that you delete any sensitive comments or photos or other materials from your social media accounts, laptops, cameras and other electronic devices that could be considered controversial or provocative by the local groups to stay respectful.

When deleting photos, especially sensitive or compromising photos, be sure that they are also deleted from your cloud storage.

(Source: Lindsey Carraher, Interagency Liaison, Office of Cyber Threat and Investigations, Department of State*)

Check your settings

Set the privacy and security settings on web services and apps. Limiting how and with whom you share information (like location tracking) is okay, especially when you are away.

Set up the "find my phone" feature

This will allow you to find, remotely wipe data and/or disable the device if it gets into the wrong hands.

Password protect your devices

Make sure you require the use of a passcode or extra security feature (like a fingerprint) to unlock your phone or mobile device in case either is misplaced or stolen.

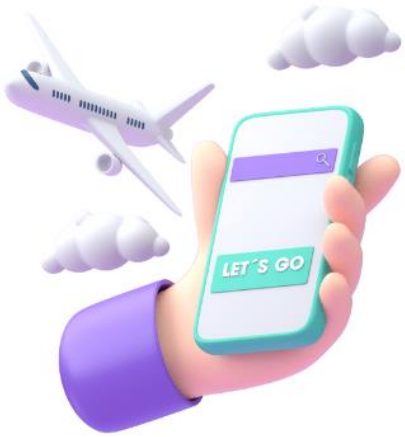
Update your software

Before you hit the road, make sure all security and critical software is up-to-date on your connected devices and keep them updated during travel. Turn on "automatic updates" on your devices if you're prone to forgetting.

Back up files

If you haven't taken a moment to back up the information, including files and photos, on your devices, do so before heading out for vacation. If something unfortunate does happen and you lose your device or access to it, you'll at least be able to recover the information you backed up.

ON THE GO



Now that your devices are updated, password protected, and backed up, there are a few steps you can take to improve your security while on the go:

Actively manage location services

Location tools come in handy while planning navigating a new place, but they can also expose your location – even through photos. Turn off location services when not in use.

Use secure Wi-Fi

Do not transmit personal info or make purchases on unsecure or public Wi-Fi networks. Instead, use a virtual private network (VPN) or your phone as a personal hotspot to surf more securely.

When Wi-Fi is turned on, your device is constantly looking for a network to connect to, even without you knowing. Consider turning off the Wi-Fi on your device when not in use. This will prevent your device from automatically trying to connect to unknown Wi-Fi networks.

Joining a Wi-Fi network is all about trust. Before connecting, you should ask yourself, "Do I really know who owns this network?" and "Who else may have access to this network?"

Private Connections

When in doubt, use your mobile phone or a personal hotspot for a private Internet connection. This is a safer approach to accessing wireless Internet when compared to a public Wi-Fi network

Remember, "free Wi-Fi" doesn't mean "safe Wi-Fi."

Think before you post

Think twice before posting pictures that indicate you are away. Wait until you get home to share your magical memories.

Protect physical devices

Ensure your devices are with you at all times. If you are staying in a hotel, the best thing to do is lock them in a safe. If a safe is not available, lock them in your luggage. Don't leave devices unattended with strangers. Using your device at an airport or cafe? Don't leave it unattended with a stranger while you get up to use the restroom or order another latte.

Stop auto connecting

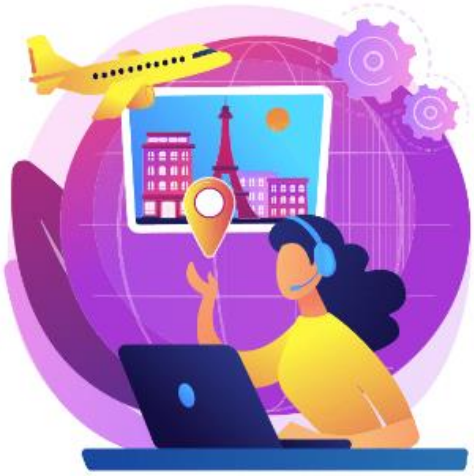
Disable remote connectivity and Bluetooth. Some devices will automatically seek and connect to available wireless networks. And Bluetooth enables your device to connect wirelessly with other devices, such as headphones or automobile infotainment systems. Disable these features so that you only connect to wireless and Bluetooth networks when you want to. If you do not need them, switch them off.

If you share computers, don't share information

Avoid public computers in hotel lobbies and internet cafes. If you must use a public computer, keep activities as generic and anonymous as possible. Don't log into accounts or access sensitive information. If you do log into accounts, such as email, always click "logout" when you are finished. Simply clicking the "x" on your browser does not log you out of accounts.

Thanks to StaySafeOnline.org for these tips
https://staysafeonline.org/resources/vacation-and-travel-security-tips/

For International Travelers



When traveling internationally, remember that your mobile phone and other personal communications devices transmit and store your personal information, which is as valuable as the contents of your suitcase, and possibly more so.

Scams from 3rd party sites

Be extra careful when using your mobile phone because you aren't able to mouse over the links to check their validity. TFA Pre-check and COVID testing phishing emails are rampant so think before you click and give them your information

Before you go

Take proactive steps to secure your devices and your personally identifiable information (such as your name, address, date of birth and Social Security Number) before you travel. Leave at home any electronic equipment you don't need during your travel. And, if you take it, protect it. Be sure to:

- Back up your electronic files.
- Remove sensitive data.
- Install strong passwords.
- Confirm antivirus software is up-to-date.
- Put all your social media on private

Many countries have tight restrictions on the use of cryptography (encryption). Among the more restrictive are laws in Belarus, Kazakhstan, Mongolia, Pakistan, Singapore, Tunisia, and Vietnam. For more information **https://www.gp-digital.org/world-map-of-encryption/** Clicking on a specific country provides an in-depth breakdown and analysis—including an expanded assessment, and details on the relevant laws and policies.

If you need a tourist VISA to travel to a specific country, get it from the country itself, don't go through a third party, even if they advertise an expidited time. They are probably looking for your sensitive information, your money, and you probably won't get it. (AARP)

To see if you need a Visa to travel: **https://www.atlys.com/post/countries-where-us-citizens-need-a-visa**

Visa Requirements for US Citizens

- A valid passport.

- At least two blank pages in your valid passport.
- Flight itinerary.
- Proof of sufficient funds (bank statements).
- Hotel itinerary.
- Travel insurance.
- Two passport-size photos.
- A completed application form.

These are just the general required documents. You might need to give any other relevant travel documents depending on the country you are applying for.
Resource: https://www.atlys.com/post/countries-where-us-citizens-need-a-visa#travel-to-bolivia-from-the-us

While traveling

Be vigilant about your surroundings and where and how you use your devices. Make sure to:

- Keep your devices secure in public places such as airports, hotels and restaurants.
- Take care that nobody is trying to steal information from you by spying on your device screen while it's in use.
- Consider using a privacy screen on your laptop to restrict visibility.

Be cautious while using public Wi-Fi

Some threats – device theft, for example – are obvious. Others, though, will be invisible, such as data thieves trying to pick off passwords to compromise your personally identifiable information or access your accounts. You may be especially vulnerable in locations with public Wi-Fi, including internet cafes, coffee shops, bookstores, travel agencies, clinics, libraries, airports and hotels. Some helpful tips:

- Do not use the same passwords or PIN numbers abroad that you use in the United States.
- Do not use the public Wi-Fi to make online purchases or access bank accounts.
- When logging into any public network, shut off your phone's auto-join function.
- While using a pubic Wi-Fi network, periodically adjust your phone settings to disconnect from the network, then log back in again.
- Try purposely logging onto the public Wi-Fi using the wrong password. If you can get on anyway, that's a sign that the network is not secure.

Remember also to avoid using public equipment – such as phones, computers and fax machines – for sensitive communications.

When you get home

Electronics and devices used or obtained abroad can be compromised. Your mobile phone and other electronic devices may be vulnerable to malware if you connect with local networks abroad. Update your security software and change your passwords on all devices on your return home.

Thanks to the FCC for the above tips!
https://www.fcc.gov/consumers/guides/cybersecurity-tips-international-travelers

Additional Resources:

For more tips, check the U.S. Department of Homeland Security's Computer Emergency Readiness Team webpage. (https://www.cisa.gov/uscert/ncas/tips)

Laws and policies regarding online security and privacy differ in other countries. While in a foreign country, you are subject to local laws. The State Department website has travel safety information. (https://travel.state.gov/content/travel/en/international-travel/International-Travel-Country-Information-Pages.htm) for every country in the world.

From the National Cybersecurity Alliance:

Planes, Trains, Automobiles... Staying Safe Online webinar
(https://www.youtube.com/watch?v=ck8c8PgGySU&t=143s)
* Lindsey Carraher, Interagency Liaison, Office of Cyber Threat and Investigations, Department of State
* Nick MacDiarmid, Director, Cyber Incident Response, Marriott
* Liz Buser, Senior Advisor, Fraud Prevention Programs, AARP
Jessica Willingham, Senior Analyst, Cybersecurity, Southwest
Moderator: Lisa Plaggemier, Executive Director, National Cybersecurity Alliance
We highly recommend this webinar which will provide practical tips for maintaining your amazing cybersecurity habits even when you are away from home! Learn about public wi-fi, when to use your device's location settings, and keeping your identity safe when traveling. It doesn't matter if you're headed across an ocean or down the street, this information will give you a better understanding of how to best protect yourself when you're on the go.

From The Identity Theft Resource Center:

(https://www.idtheftcenter.org/post/travel-safe-with-these-cybersecurity-protection-tips/)

Gear up for your next vacation with advice on how to travel safe when it comes to technology and cybersecurity.

Unfortunately, as too many travelers already know, heading out of town can be filled with pitfalls. Lost luggage, sudden cancellations, and unexpected illnesses are just the tip of the iceberg when it comes to potential problems. However, there is a far more serious danger lurking for the would-be traveler with consequences that take years to recover from – identity theft.

Cybercriminals do not take vacations, so you cannot let your guard down where your identity, financial data, and even your gadgets are concerned. In fact, in many ways, traveling brings a whole new kind of cybersecurity threat, specifically targeting people when they are away from home.

Once you have planned your getaway, there are a number of steps you must take to travel safe. Whether you are traveling within the country or abroad you should consider taking the below actions to protect your information.

Update and Backup all of Your Technology

If you are bringing any devices with you now is the time to **make sure they are updated** to the most recent operating system. The same is true of your apps. When you continue to use an outdated piece of software or an old app, you are leaving yourself wide open to a data breach; developers often issue updates specifically because they have uncovered a security hole. While you are at it, make sure you save all of your important files, documents, or photos to a secure source at home, just in case someone does attack your device.

Disable your Wi-Fi

A simple slide with your fingertip is all it takes to prevent your mobile device from automatically connecting to unknown networks. These are the kinds of free Wi-Fi connections found in coffee shops, hotels, restaurants, airports, and more. Turning off the Wi-Fi will not only save your battery, it will stop lurkers from infiltrating your device over unsecured networks. Do not worry, you can turn it back on whenever you are in range of a safe connection.

Power Up with Confidence

Avoid public charging stations if you can help it. Whether you use your own cord or use one that is provided, you cannot know where the cord's connection will lead. In **a scheme called "juicejacking**," criminals lure travelers into plugging in their devices for a quick charge, but the cord is actually connected to a hidden computer. The computer is downloading all of the files and information off the devices while you charge up, including usernames, passwords, account numbers, and more. If you can carry your own external charger battery or a "block" to plug into a regular power outlet, that would be much safer.

Passcodes, Passwords, and Pass it On

You might want to update your passcode lock on your mobile devices and your account passwords

on sensitive accounts before you leave. That way, you are not enjoying a day out on the waves—and away from a phone or computer—when a hacker steals a database of old usernames and passwords, or steals access to your online bank account and credit card. If you can leave these passwords with a trusted family member, they can help you out if something goes wrong while you are out of pocket.

The Trip is Only Part of the Equation

Remember, your vacation starts (at least from a cybercriminal's perspective) from the day you book the trip through the weeks after you have returned. Make sure you are booking your travels through a reputable company over a safe online connection and that you are monitoring your accounts before, during, and long after your trip in order to watch out for suspicious activity.