MakingSenseofSecurity.com

Travel Cyber Security

==========

There are many precautions to take when traveling whether locally or distant to protect yourself and your data. When we travel, even just to the store, there are times that people may not take measures to protect themselves or their devices while they are away from home.

One thing to keep in mind also, is **these precautions can apply to tight apartment and townhome communities**. The more Wi-Fi signals you pick up on your device, the more protection you need.

Regardless of how long nor how far you may be from home, there are measures to implement to ensure safety for yourself, family, data and devices.

Write your name on a visible or accessible part of your device. For example, set up a screen saver that lists your name and a local address such as **your post office box or local police department** so that the device can be returned to you if someone finds it. **NEVER** put your home address on devices. If it is found while you are traveling, and you live in another state, the finder could be a bad guy and get into your device AND your home.

Ensure you have a mobile version of Anti-Virus protection on your device. Make sure it is updated continuously throughout the day. Hourly at minimum. One can use Kaspersky products and they will update often within the hour.

Ensure the Operating System (OS) on your device is up-to-date. Check for updates first before traveling. Just because you are on vacation does not mean security should be.

Disable Bluetooth (BT) unless absolutely needed. When possible, select headphones when traveling that require plugging into the charging port or a jack. Attackers can connect to your phone and potentially hack into your device.

Public Wi-Fi- Do not use it unless you need to. If you do, ensure you are signed out of all apps and websites. Further, ensure there are no tabs or internet windows open unless you are briefly using it. Do NOT go to any sites on public Wi-Fi involving banking, financial transactions or personally identifiable information (PII) that is sensitive.

Also disable wi-fi auto-connect to any open wi-fi.

Tip: Increase your data plan to unlimited for the time you are traveling. Then you can use your cell phone as a Hotspot to provide service, so you may avoid using public Wi-Fi, such as in an airport or a hotel.

Delete all saved Wi-Fi's saved in your connection list. Should your device be lost or stolen, the culprits will not be able to determine places your frequent.

Do not have passwords saved on your device(s) for accounts such as email. If your device is lost or stolen, the culprits will be able to get into your email and do various communications without your knowledge. Entering your temporary password is best. Why, because it is not a keylogger

you are worried about. It is about the transmission of your password being intercepted. (These measures together will help prevent that).

Change your Passwords temporarily when traveling. Ensure it is a hard one to remember and that you would not normally use. Change it before traveling and then change it after traveling. Keep a list of sites and apps accessed. Changes these passwords upon return. Should any other sites or apps you have accounts with appear compromised since, change those passwords also. Even if you are not sure.

Back up your files prior to traveling. This will ensure the ability to continue to work and all is not lost should your device(s) be lost or stolen.

BYOC- Bring your own chargers! Avoid charging your phone on computers or devices that you do not control, such as hotel docking stations. Malicious software could be stored on devices that have USB ports and could transfer malicious software when your device is connected. Use your personal computer or a direct-to-wall-socket charging port to charge your phone.

Turn OFF location. Do not use location sharing. Hackers are getting more sophisticated getting into devices without your knowledge. Then can see who you are and where you are. Within just feet of where you may be. Your safety is important.

Above all, DO NOT share your location live or at anytime while you are traveling. It is for one, no one's business. And two not safe for your home or personal safety while traveling. Attackers, stalkers, unknown strangers, workers, passer-by's, neighbors, ex's, friends of friends, etc., can all use your location and activities to their benefit. There is a time and a place to show off that you are on vacation in the Caribbean. Share it after you have arrived safely in your home or even later. An unoccupied home can be burglarized while away. Further, sharing posts that can be shared and shared and shared and also viewed through location tagging brings assailants looking to cause you harm.

DO everything you can to prevent yourself from being a victim. Use this knowledge to protect yourself and protect those you love.

Know the International laws and regulations when traveling. Use this resource when traveling internationally:

Learn About Your Destination

U.S. Passports & International Travel

https://travel.state.gov/content/passports/en/country.html

==========

(December 2018).