With warm weather right around the corner, you have most likely started to think about summer getaways. Whether you’re considering a relaxing family vacation, an exotic experiential excursion or a long-awaited high school reunion, chances are you will use an Internet-connected device to make your travel plans. According to USDM.net, in 2016 most digital travel bookers will use mobile devices to conduct research, with an overwhelming majority – 90 percent – using smartphones. Once on vacation, travelers will also use smartphones and other mobile devices to keep them “in the know” about local hotspots while navigating new cities and countries and sharing tales of their trips with family and friends back home.

With an increasing amount of our lives spent online, including those periods when we are away from home, it’s important to keep our devices safe and secure. With summer on the horizon, the National Cyber Security Alliance (NCSA) has provided some user-friendly STOP. THINK. CONNECT. travel tips to help vacationers protect themselves, their families and the extended online community while away. By following some smart practices, travelers can use the Internet with greater confidence during a summer escape.

**NCSA’s Top Tips before Hitting the Road**

**Keep a clean machine**
Before you hit the road, make sure all security and critical software is up to date on your Internet-connected devices, and keep devices and apps updated during travel. It is your best line of defense.

**Get two steps ahead**
Turn on two-step authentication (also known as multi-factor authentication) for an extra layer of security beyond the password that is available on most major email, social media and financial accounts.

**Make sure all devices are password protected**
Use a passcode or security feature (like a finger swipe) to lock your mobile device.

**Think before you app**
Review the privacy policy and understand what data (such as location and entry to your social networks) the app can access on your device before you download. Delete apps you are no longer using.

**Own your online presence**
Set the privacy and security settings on web services and devices. It is okay to limit how and with whom you share information – especially when you are away.
NCSA’s Top Tips While On the Go

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

Get savvy about WiFi hotspots
Do not transmit personal info or make purchases on unsecure networks. Instead, use a virtual private network (VPN) or your phone’s cellular connection as a personal hotspot to surf more securely.

Delete unused apps
Many people use apps that can be specific to a city or attraction. These apps should be deleted when no longer needed.

Turn off WiFi and Bluetooth when idle
When WiFi and Bluetooth are on, they connect and track your whereabouts. If you do not need them, switch them off.

Protect your $$$
Be sure to shop or bank only on secure sites. Web addresses with “https://” or “shttp://” mean the site takes extra security measures. However, an “http://” address is not secure.

Never use public computers to log in to any accounts
Be extremely cautious on public computers in airports, hotel lobbies and Internet cafes. Keep activities as generic and anonymous as possible.

Share with care
Think twice before posting pictures that would reveal you are not home or that you would not want certain people (like your parents or employer) to see.

Post only about others as you would have them post about you
The golden rule applies online, too.

Tips on protecting yourself, friends and family from ID theft & fraud:
https://staysafeonline.org/stay-safe-online/protect-your-personal-information/id-theft-and-fraud
#CyberAware tips for protecting your mobile devices on the go:
http://staysafeonline.org/stay-safe-online/resources/stay-cyberaware-while-on-the-go-safety-tips-for-mobile-devices