These days, no matter where you're headed, being continuously connected is part of the travel plan. As you embark upon your next work trip, the National Cyber Security Alliance (NCSA) urges travelers to be cyber safe while away from the office by following some simple practices to help keep your devices safe and your travel plans from going awry.

**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 SYSTEM AND 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.

**OWN YOUR ONLINE PRESENCE**

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

**BACK IT UP**

If you haven't taken a moment to back up the information on your devices, do so before heading out. 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.

**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.

---

**REMEMBER**

Treat your boarding pass like it's a passport. Boarding passes contain information that, if accessed by a criminal, can reveal information like a traveler's frequent-flyer number. What could they do with this information? Access to your frequent flyer number could help a criminal steal earned miles or access any other sensitive information contained in an rewards account--particularly if you don’t have a strong passphrase and 2-factor authentication enabled on those accounts.

---

**GETTING READY TO GO**

*Before you head out on vacation, here’s a simple security checklist to add to your packing routine.*

**UPDATE YOUR SYSTEM AND 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.

**OWN YOUR ONLINE PRESENCE**

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

**BACK IT UP**

If you haven’t taken a moment to back up the information on your devices, do so before heading out. 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.

**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.
AUTO-REPLY WITH CAUTION
If you configure your email to auto-reply, letting business associates know you are unavailable for a specific period of time, try to be as vague as possible about the details of your travel. Simply “I’m currently unavailable and will get back to you as quickly as possible” is suitable.

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

SET UP THE “FIND MY PHONE” FEATURE ON YOUR DEVICES
This will allow you to find, remotely wipe data and/or disable the device if it gets into the wrong hands.

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:

IF YOU SHARE COMPUTERS, DON’T SHARE INFORMATION
Be extremely cautious on public computers in airports, hotel lobbies and internet cafes. Keep activities as generic and anonymous as possible. If you do log into accounts, such as email, always click “logout” when you are finished. Simply clicking the “x” does not log you out of accounts.

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.

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.
GET SAVVY ABOUT WI-FI HOTSPOTS
Do not transmit personal info or make purchases on unsecure networks. Instead, use a virtual private network (VPN) or your phone as a personal hotspot to surf more securely.

SHARE WITH CARE
Think twice before posting pictures that indicate you are away. Wait until you get home to share your travel photos.

PROTECT PHYSICAL DEVICES
Ensure your devices are with you at all times. Packing your devices? Store them in your carry on, not checked luggage.

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. Keep your devices with you at all times. The phrase “stranger danger” also applies to cybersecurity. Need to power up? Use your own battery charger when traveling. Public charging stations can be manipulated by criminals to steal your information.

AVOID SHOULDER SURFERS
Think critically about where you do your work, and who might be able to peer over your shoulder to see your screen or what you're typing. Consider using a screen guard and position yourself to limit how many people can come up behind you. When using ATMs or entering passcodes on devices, you should also try to cover your hand so others can’t see your codes.

ADDITIONAL RESOURCES

FCC: Cybersecurity Tips for International Travelers:
https://www.fcc.gov/consumers/guides/cybersecurity-tips-international-travelers

ID Theft Center: Travel Safe Blog:

Consumer Reports: What You Need to Know About Cyber Safety While Traveling: