Traveling?

Useful tips to protect yourself from cyber criminals

If you're planning some travel and taking your smartphone (who doesn't?), the following tips will prevent huge headaches. Your phone can help you get directions, find points of interest and take lots of selfies. But your phone presents big cyber-security risks for you and your money and data. Practicing good "cyber hygiene" before, during, and after your trip will help secure your devices and allow you to connect with confidence when you're away from home.

1. Update your devices. Updating devices can fix security flaws and help keep you protected from bots and spam. Whether it's a smartphone, computer or gaming device, be sure to update your operating system, applications, antivirus and malware software. Maybe you should consider turning on automatic updates.

2. Back up your devices. It's always a good idea to back up information such as contacts, financial data, photos, videos, and other data in case a device is compromised during travel and you have to reset it to factory settings. Worried you might forget to update on schedule? Make it automatic; some cloud services charge as little as $2-5 per month to back up your phone constantly.

3. Lock your device. Be sure to lock your device when you are not using it. Set your devices to lock after a period of time and use strong PINs and passwords.

4. Enable multi-factor authentication (MFA). Add an extra layer of protection so that the only person who has access to your account is you. For more information on MFA, see *https://www.cisa.gov/mfa.*

5. Guard your devices. Your devices are valuable, but your sensitive information is as well. Always keep your devices close at hand and secure in taxis, security checkpoints, airplanes, rentals homes, and hotel rooms. Make a habit to never lay your phone down (restaurant, taxi, hotel desk) but instead always slip it into your pocket or purse.

6. Recharge securely. Please don't plug your phone into a USB public charging station, such as those in the airport or in hotel room, lamp or clock radio inputs, as these cannot be trusted. Malicious individuals can hijack your session or install malware on your device through those public chargers. Always connect using your own power adapter connected to a power outlet.

7. Delete data from your rental car. If you connect your phone to a rental car for navigation or other purpose, be sure to securely remove the device so that other individuals do not have access to your address book, device name, text messages (hands free calling), or other sensitive information.

8. Avoid public Wi-Fi. While public networks are convenient, they are a security risk. Avoid connecting to public Wi-Fi unless absolutely necessary. Instead, consider using your phone carrier's internet connection or use your phone as a personal hotspot if your plan allows.

9. Control your connections. While auto-connect is enabled, devices will seek out and connect to available networks or Bluetooth devices. This could allow cyber criminals to access your device without you knowing it. Disable auto connect, Bluetooth connectivity and near field communication (NFC), like airdrop, so that you can select the network and you can control the connection.

10. Limit what you share. Limit the information you share on social media while on vacation. Consider posting updates about your trip after you return. When you reveal your travel plans, bad actors can rob your empty home. Scammers may even attempt to contact your family and friends with a variety of scam tactics. If your social media accounts are set to "public," please consider setting them to "allow friends only" to view. This limits your risk.

11. Avoid the use of public computers. Public computers such as hotel business centers and internet cafes are often poorly managed and provide minimal security protection for users. If you must use a public computer, do not enter any username or password on the computer and do not connect or transfer data via thumb drive/USB.

12. Shred your boarding pass and luggage tag. Scannable codes on boarding passes and luggage tags include full name, date of birth, and passenger name record. These can also contain sensitive data from your airline record, like passport number, phone number, email address, and other information that you wouldn't want to share publicly. For this same reason, never post boarding passes on social media.

13. Scan for virus and malware. It's best to update your security software when you return home and scan for virus and malware to be sure your device has not been compromised while you were away.

At The First National Bank & Trust Co., we care about your safety. In fact we offer a variety of tools to lower your risks against internet thieves. Just ask. Our bankers are equipped to answer your questions. As an example, did you know that you can use our free mobile phone app called SecurLOCK to turn your debit card on-and-off with a switch? It can stop criminals from using your lost debit card, no matter what time of day or night you realize it's gone. Ask for lots more ideas from your banker.

The First National Bank & Trust Co.
www.bankfnbt.com / 405-224-2200 / Serving Oklahoma since 1892