# Protecting Privacy and Security While Traveling

Rebecca Herold, Privacy & Security Brainiacs
2023

Before going on a vacation, business trip, or any other type of longer travel, besides doing all your other regular trip preparation, include doing privacy and security actions before you leave. Then, stay privacy aware and cybersecurity smart during your trip.

**<u>Before Traveling</u>**:

☐ Take along and use some important security and privacy protection tools that are small and easy to travel with.

- ✓ Invest in comparatively low-cost USB data blockers, also commonly called juice jack blockers, to use yourself, and to provide to all your family, friends, and employees who work remotely. They are small and easy to carry in your pocket, phone case, etc. They look similar to this:

  They are also inexpensive. We've found them for as low as two for USD $7.89. They also typically cost less when buying them in bulk.

- ✓ Invest in some personal portable charging devices for situations where a power source is needed, but there are none to be found, such as while hiking, or spending the day with a client in an environment with few-to-no usable electrical outlets. We carry two; one a flat credit-card size, and another the size of lipstick, that can each be put into different pockets, or storage belts. The charging devices look similar to these:

- ✓ Carry a charging-only cable to use in public USB ports. This will prevent data from being transmitted through the USB connection similar to how juice-jack blockers work (but, yes, are larger and bulkier to carry). Cables that charge and provide data transfer have four. Charge only cables only have two wires, usually making them thinner.

- ✓ Bring an electric outlet-to-USB adapter with you when traveling. These are inexpensive (usually less than USD $10) and small. Most of these have two USB ports within them and look similar to this:

# Protecting Privacy and Security While Traveling

Rebecca Herold, Privacy & Security Brainiacs
2023

- ☐ You can lose access to your phone not only when your battery dies, but also when you are in extreme hot or cold temperatures. Phone manufacturers recommend keeping the devices between 32-95 degrees Fahrenheit (0 to 35 degrees Celsius) at all times. Invest in fairly inexpensive cellphone temperature protection, padded, waterproof cases/covers to protect your phone and devices from such temperature extremes and other environmental threats. While you're at it, get a case that also protects your phone from nearby wireless access via blue-tooth and RFID transmissions. These typically cost between USD $8.00 to $50.00

- ☐ Put your driver's license, passport, credit cards, and other RFID-embedded items into an RF-shielded travel belt, small storage bag, etc.; often called a "Faraday bag." This prevents those nearby from accessing the data stored on the RFID chips; commonly called RFID skimming.
- ☐ Always use a privacy screen on your laptop, tablet, and smartphone to keep others nearby from seeing, and easily recording or taking photos of, confidential information (financial data, passwords, phone numbers, etc.) on the device screen. This includes those who may be above you on balconies, in windows, drones, etc.
- ☐ Attach a physical alarm, or a software app alarm, that will go off if someone takes your computing devices.
- ☐ Attach digital trackers to your computing devices and within your luggage, backpacks, etc. to be able to find stolen or misplaced items.
- ☐ Invest in a travel laptop with the minimum necessary applications and data on the device to allow you to accomplish necessary tasks, without bringing all your data with you that is typically stored on regularly used computers.
- ☐ Take a telecommunications company (e.g., Verizon) wireless mobile router. They are small and easy to take in a carry-on or pocket. If you don't want to invest in paying for one within an annual plan, most telecommunications services have them for rent for such travel purposes.
- ☐ Install a VPN on your personal device to encrypt internet transmissions from computing devices.
- ☐ Invest in travel cyber insurance to cover lost or stolen phones, laptops, and other computing and digital storage devices.
- ☐ Do not use an email auto-reply that says something like, "I am traveling to XYZ, and will be there until ABC." Instead, use an auto-reply similar to, "I am unavailable to answer email. I will reply when I am once more available."

# Protecting Privacy and Security While Traveling

Rebecca Herold, Privacy & Security Brainiacs
2023

- ☐ Provide an itinerary to one or a few trusted family members and/or friends. Include phone numbers of the places where you are staying and/or the owners of those places.
- ☐ Keep up-to-date with all the details about your life, health and travel insurance policies, bank accounts, credit card accounts, other accounts, etc. Keep all this information in a secure location. For instance, bank deposit box, locked home safe, your personal lawyer, etc. Let your trusted family members and/or friends know where they can find this information if needed, such as if an accident or illness occurs while traveling.
- ☐ If you have a home security system, do a test before you leave to ensure you can access information the system is collecting from your home, ensure that the data is not publicly available, etc.
- ☐ Either put a hold on your deliveries and mail while you are gone or ask a trusted neighbor, friend, and/or family member to pick up such items daily while you are gone.

**<u>While Traveling</u>**:

- ☐ Use all the tech and tactics listed previously.
- ☐ Check for digital trackers that may have been planted on your vehicle, in your bags, luggage, pockets, or other locations that you don't normally check that often. If you have a reason to believe you are being tracked, invest in a digital tracker detector. There are many kinds. Ones similar to those shown below are typically available in the USD $40 - $50 range, and work well. Professional strength detector devices are available in the USD $150 - $250 range.

- ☐ Before using ATM machines, self-pay gas pumps, or other type of credit/debit card readers, grab the device and see if it jiggles. Check also for broken tape on the device, etc. If either of these, it could very well be a card skimmer. Use a different pump or different device to pay.
- ☐ After verifying a credit card reader is likely safe, punch in the PIN numbers with one hand while covering the keypad and card with the other hand, to protect against hidden cameras that could be recording your card number and associated PIN.

# Protecting Privacy and Security While Traveling

Rebecca Herold, Privacy & Security Brainiacs
2023

- ☐ Think twice before making publicly available posts to social media sites about your traveling and exactly where you are at any point in time. This is especially important when traveling alone. This communicates to others who are malicious that you may be a vulnerable target in locations where you do not live, and it also lets them know your home may be empty and an easy target for theft. Wait until after you are back to talk about your trip.
- ☐ Practice security and privacy in your hotel room, such as keeping doors double-locked, leaving valuables in safes, and checking for surveillance devices in your room or within the vicinity wherever you are.
- ☐ Do not use public USB chargers, unless you are using a USB data blocker, a charge-only cable, and/or an electric outlet-to-USB adapter.
- ☐ When taking videos and photos on your smartphone, encrypt and then e-mail them home or to a trusted source immediately. This allows the recipients to see the photos and videos right away, without having the transmissions being copied without your knowledge. This also reduces the possibility of losing all the memories within the phone if it is lost. If saving to an online cloud service, make sure the cloud storage encrypts all the photos and videos in storage and during transmission, and use access controls to restrict who gets to them.
- ☐ Use your VPN to encrypt the transmissions from the computing devices through the internet.
- ☐ Avoid using unsecured hotel, airport and any other public Wi-Fi networks. Instead, use your wireless mobile router.
- ☐ While out and about sightseeing or attending meetings, don't carry anything with personal information if you can help it. Be sure to securely lock away items like passports, driver's licenses and credit cards at the hotel in the room safe, or similarly secured area. Carry only a small amount of cash and/or travelers checks. We recommend an RF-shielded money belt, or something similar, with additional money and possibly even your passport and/or driver's license and a credit card, to wear unseen, to protect you from pick-pockets.
- ☐ Do not subject your computing devices or phones to extreme temperatures. For example, do NOT leave your computing devices or phones on vehicle dashboards, or other locations where they will have direct or filtered sunlight in warm to hot climates, or in freezing temperatures.
- ☐ Do NOT charge your phone in a pile of other electronic devices, within phone cases, or under blankets, coats or other types of items where there is no ventilation.
- ☐ Protect phones and computing devices from physical damage by using padded or hard sided cases.
- ☐ Charge computing devices and phones on hard, flat surfaces that are as uncluttered as much as possible.
- ☐ Don't leave computing devices or phones unattended in vehicles or packed in checked luggage.

# Protecting Privacy and Security While Traveling

Rebecca Herold, Privacy & Security Brainiacs
2023

**For Businesses:**

At a minimum, update your security and privacy policies and associated procedures to include travel security and privacy directives similar to the following, that are most applicable to your organization's work environments. Add other requirements from the previous pages, as applicable to your workers' travel activities.

- ☐ When not within secured environments (e.g., within the business facilities, or within your home office areas), connect a USB juice jack blocker to your computing device, then connect the blocker to the USB charging port.
- ☐ If, when plugging a device into a USB charging port, a prompt appears asking you to select "share data" or "trust this computer" or "charge only," always select, "charge only."
- ☐ If you're in public and need to charge a device, use the outlet-to-USB adapter in an electric plug-in outlet to prevent data transfer.
- ☐ Do not connect phones or computing devices to an unknown charging station without using one of the juice jack blocking tools previously described.
- ☐ Do not use public charging cables and power banks that seem to be left behind, or not provided by the facilities you are within. Cyber crooks set up these types of malicious devices in public areas to lure their victims to them.
- ☐ Carry one or two portable chargers while traveling in areas with scarce electric plug-in outlets, to have available when needed and no power source is available.
- ☐ Always use privacy screens on computing devices when traveling.
- ☐ Never leave computing devices unattended in areas where others are in the vicinity; e.g., restaurants, boarding gates, hotel meeting rooms and lobbies, etc.
- ☐ Digitally lock your phone or other type of computing device when charging. This minimizes the risk of malicious access from pairing with your connected device.
- ☐ Do not use public Wi-Fi networks. Instead, use mobile Wi-Fi routers that you take with you on your trip.
- ☐ If you must use a public Wi-Fi network, make sure you use a personal VPN loaded on your computer at the same time.
- ☐ Activate cyber insurance for traveling prior to the trip.

# Protecting Privacy and Security While Traveling

Rebecca Herold, Privacy & Security Brainiacs
2023

## For Facilities Providing Public USB Chargers:

It is becoming more important for facilities to take actions to ensure the USB chargers they are providing are not being used by juice jackers. Here are some ways in which such cybercrooks can be thwarted, or the risks at least minimized, in public locations, and in other types of locations where many different people are using the USB chargers, such as in hotel rooms and office-sharing spaces.

- ☐ Establish policies and supporting procedures for facilities security, the physical safety department, the digital security department, IT, or whatever team is most appropriate at your organization, to regularly (daily or more often, depending on the type of venue) check all public charging stations and look for changes, changed cables, hardware that has been tampered with, new charging devices put by those provided by the facilities, and other suspicious alterations. Report any changes or possible concerns to the most appropriate team in your organization to investigate.
- ☐ Consider installing CCTV cameras in locations with public charging stations, with view of the full station, USB ports, all cables, and any other related equipment. Often such CCTVs/etc. are best to mount on the ceiling immediately above the charging stations, to prevent individuals from being able to block the view as easily.
- ☐ Provide charge-only cables; those that do not have data transmission capabilities. Not only will this keep data from being skimmed, and to keep unauthorized access into devices, networks, and systems from occurring, it will also support having those using the stations not able to linger longer than necessary while working on the devices while they are charging, and to disconnect them after they have been sufficiently charged, allowing others to charge their devices more quickly.
- ☐ In addition to, or instead of, the previous option, use USB ports/sockets that have had the data signal/transmission leads removed, and only have the ground and power leads left to allow for charging.
- ☐ Post signs by each of the charging stations that say something similar to, “If you see something, say something! If you notice USB charging stations being tampered with, or suspect they have been tampered with, please call 999-999-9999.”
- ☐ In hotel rooms, residence halls, and other locations where there are temporary short-term guests, remove all charging cables, USB ports, and other types of charging hardware after each customer has vacated the space.