Security Tips for Traveling at Home and Abroad

CYBER SECURITY MARCH 2017

We all like to travel with our mobile devices (smartphones, laptops, or tablets) — whether it's to the coffee shop around the corner or to a café in Paris. These devices make it easy for us to stay connected while on the go, but they can also store a lot of information — including contacts, photos, videos, location, and other personal and financial data — about ourselves and our friends and family. Following are some ways to protect yourself and others.

Before you go

- If possible, do not take your work or personal devices with you on international trips. If you do, remove or encrypt any confidential data.
- For international travel, consider using temporary devices, such as an inexpensive laptop and a prepaid cell phone purchased specifically for travel. (For business travel, your employer may have specific policies about device use and traveling abroad.)
- Install a device finder or manager on your mobile device in case it is lost or stolen. Make sure it has remote wipe capabilities and that you know how to do a remote wipe.
- Ensure that any device with an operating system and software is fully patched and up-to-date with security software.
- Makes copies of your travel documents and any credit cards you're taking with you. Leave the copies with a trusted friend, in case the items are lost or stolen.
- Keep prying eyes out! Use strong passwords, passcodes, or smartphone touch ID to lock and protect your devices.
- Avoid posting social media announcements about your travel plans; such announcements make you an easy target for thieves. Wait until you're home to post your photos or share details about your trip.

While you're there

- Physically protect yourself, your devices, and any identification documents (especially your passport).
- Don't use an ATM unless you have no other option; instead, work with a teller inside the bank. If you must use an ATM, only do so during daylight hours and ask a friend to watch your back. Also check the ATM for any skimming devices, and use your hand to cover the number pad as you enter your PIN.
- It's hard to resist sharing photos or telling friends and family about your adventures, but it's best to wait to post about your trip on social media until you return home.
- Never use the computers available in public areas, hotel business centers, or cyber cafés since they may be loaded with keyloggers and malware. If you use a device belonging to other travelers, colleagues, or friends, do not log in to e-mail or any sensitive accounts.
- Be careful when using public wireless networks or Wi-Fi hotspots; they're not secure, so anyone could potentially see what you're doing on your computer or mobile device while you're connected.
- Disable Wi-Fi and Bluetooth when not in use. Some stores and other locations search for devices with Wi-Fi or Bluetooth enabled to track your movements when you're within range.
- Keep your devices with you at all times during your travels. Do not assume they will be safe in your hotel room or in a hotel safe.

When you return

- Change any and all passwords you may have used abroad.
- Run full antivirus scans on your devices.
- If you used a credit card while traveling, check your monthly statements for any discrepancies for at least one year after you return.
- If you downloaded any apps specifically for your trip and no longer need them, be sure to delete those apps and the associated data.
- Post all of your photos on social media and enjoy reliving the experience!