State Privacy Office
March Privacy Tip

8 Tips to Keep Your Data Safe When Traveling Abroad

Almost all worker travelers rely on WiFi to do work while on the road, be it domestically or internationally. Most simply log on to a free network and then continue browsing web pages or writing emails where they left off without even thinking about how secure the network is. The trouble with doing that, of course, is you are potentially exposing your passwords and other confidential information to hackers around the world.

1. LOCK DEVICES DOWN

Most smart phones, laptops, and tablets come equipped with security settings that will enable you to lock the device using a PIN number or fingerprint ID. Do this on every available device. While traveling, change the PIN numbers you regularly use. In the event that any of your devices have been momentarily misplaced or forgotten, this will be the first line of defense against a security breach.

2. BE CAUTIOUS OF PUBLIC WIFI

Free WiFi access can be very appealing for business or leisure travelers but is also particularly vulnerable to security issues. Avoid unencrypted WiFi networks; ask your hotel about its security protocol before connecting to the Web. Be extra cautious using Internet cafes and free WiFi hotspots; if you must use them, avoid accessing personal accounts or sensitive data while connected to that network.

3. DISABLE AUTO-CONNECT

Most phones have a setting that allows a device to automatically connect to WiFi networks as you pass through them. While this is a nice feature when used at home, it's not something you should allow while traveling abroad. Before you travel, change this setting so that your smartphone and laptop must be manually connected each time you access the Web.

4. MINIMIZE LOCATION SHARING

It's very common for travelers to update social networking sites as they move about new counties or cities. The problem with this type of excessive sharing is that it creates a

security threat at home. By signaling your every location, you make it easy for a criminal to determine that you're not in your hotel room or at your home, leaving your personal belongings within these areas vulnerable to a physical intrusion.
Limit the information you post online about your specific whereabouts to limit these threats to your personal property.

5. INSTALL ANTI-VIRUS PROTECTION

Paid Anti-VIrus Protection Software is one of the easiest and most effective ways you can keep your personal information, as well as company information, secure while traveling. In addition to using a trusted brand of security, make sure that you regularly update this software as new versions become available.

6. UPDATE OPERATING SYSTEMS

Just like your antivirus software, you should keep your operating system as current as possible. This also goes for apps on your phone; take special care to update apps that you regularly use to conduct financial or personal business.

7. UPDATE PASSWORDS REGULARLY AND BEFORE TRAVEL

If you plan on traveling, change all of the passwords you regularly use. Similarly, if you must create a PIN for a safe or security box in a hotel room, make sure it's unique and not something you commonly use. Don't skimp on password creation either – a numerical sequence is not ideal. Take the time to create something that will keep a criminal out of your personal property. Once you return home, you can change all the passwords back.

8. DISABLE BLUETOOTH CONNECTIVITY

Just like your phone's automatic WiFi connectivity, Bluetooth connectivity can present problems. Bluetooth signals can come from anywhere. If your Bluetooth is left on, nearby assailants can connect to your phone and potentially hack into your device. Keep Bluetooth disabled as much as possible while abroad.

Copyright © 2024 FCM. All rights reserved.
Reprinted with permission.

Note: *Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.*