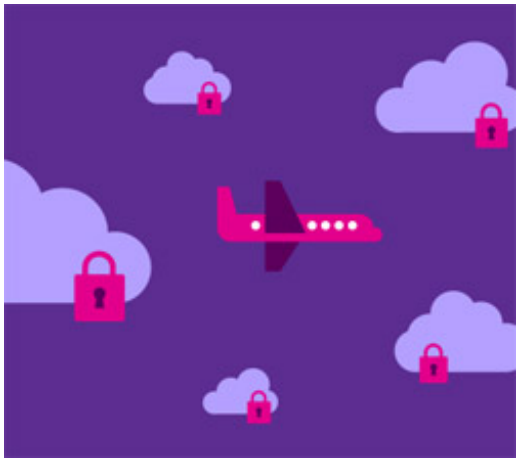
Managing Physical & Digital Security While Traveling

Posted At : August 30, 2015 11:16 AM | Posted By : Admin
Related Categories: Travel, Security

For a small community, Ithaca travels a lot all year long. Keeping your technology secure both physically and digitally ensures that your data stays with you during your trip and when you return.



Whether you're traveling for business or leisure this summer, chances are that as a small business owner or other professional, you'll be working on your trip. But with unsecured Wi-Fi hotspots and the potential for physical theft, among other risks, there are several steps you need to take to ensure security issues don't interrupt your productivity.

Use these tips to keep your devices and data safe on the road.

Before you go

- Back up your devices before you leave, and make sure current, updated security software is installed—including on your phone and tablet.
- Ensure your current data and documents are stored securely in the cloud so that you can access your files from a borrowed device or computer even if you lose your laptop or tablet.
- Set up features that enable remotely locking and wiping devices in case they're lost or stolen.
- Secure all your devices with a password or PIN. You may not use a password to log in to your laptop every day at work, but on the road this additional step adds a layer of protection.
- Encrypt your mobile devices (go to settings/security).
- Set up a virtual private network (VPN) at work that you can use on the road to connect to the Internet. The VPN encrypts everything you do online, protecting your data and devices.
- Bring only what you really need. You probably don't need both a laptop and a tablet. The more you bring, the greater your risk for physical and digital theft.

On the road

- Keep your eyes—or your hands—on your device at all times. It sounds paranoid, but physical theft is as big a risk as data theft. Never leave your laptop, phone, or tablet lying around, even for a moment. The cafés, coffeehouses, airports, and hotel lobbies that travelers frequent are home to pickpockets and thieves waiting for someone to get distracted. When leaving your hotel room, put electronics you're not taking in the in-room safe.
- Turn off Wi-Fi and Bluetooth when you're not using your devices to prevent them from accidentally connecting to a cybercrook's network.
- Stay off public computers. If you must, assume everything you do is being watched, so don't input any sensitive information or connect to your business network.
- Avoid public wireless hotspots. If you must use this type of network, never buy anything, connect

to your business network, or input passwords.

- If you don't have VPN, Use secure browsing, which you can set up within the "preferences" of your Internet browser. (You'll know you are browsing securely if the URL of the webpage you're on starts with HTTPS instead of HTTP.)
- Look under "settings" on your smartphone to see if your phone enables setting up a private mobile hotspot. Most newer phones offer this feature, which provides added security.

Take these precautions before it's too late—it's expensive and potentially damaging to business if you learn the lesson the hard way. Even if you can't take every one of these steps, each one you do take increases your chances of keeping your business information safer while you're on the road.