TitanFile

Protecting your data while travelling

Regardless of what industry you are in, you probably frequently find yourself travelling – often with a lot of confidential client data in tow.

With all of these devices and documents on the move, there are increased risks of security breaches. If you're crossing international boundaries, your electronic devices may be searched and subsequently copied by border guards. Aside from the potential for a border search, unsecured networks, easy to lose USB memory sticks and theft all add up to potential data loss while traveling.

Take these 10 steps to protect your confidential information on your next trip:

□ 1. Remove sensitive data from your devices

Before you depart on your next business trip consider what's stored on your computer. Do you need those privileged client files? Remove anything that isn't entirely necessary for this trip, saving it to an encrypted external device, or a secure cloud application. Consult with your IT department; they may have computers that are to be used specifically for business travel.

□ 2. Seek out SSL protection

SSL (Secure Socket Layer) encrypts your information before it is sent over the Internet. This prevents hackers and malicious parties from eavesdropping on your communication. Most professional services, including Google Apps, LinkedIn and Exchange Servers, have SSL sites you can access by using https:// instead of http:// when typing in the site's URL.

□ 3. Connect to your own hotspot whenever possible

Hackers can use busy spots such as airports or coffee shops to set-up monitored or fake wireless (WiFi) networks, filtering content for passwords and other sensitive data. Avoid these traps by using a personal hotspot. Most cell phone providers offer 3G and LTE USB modems that allow secure connections to the Internet over a cellular network.

□ 4. Store confidential information in a secure cloud

Worried about someone accessing documents on your stolen or confiscated device? Storing files in the cloud provides you with an alternative that not only protects your information, but also negates the need to have files stored on your computer. Cloud computing is also beneficial for travellers, giving you the freedom to access your data regardless of location.

□ 5. If you must use a storage device, choose an external hard drive

If, due to organizational regulations or poor Internet connectivity, storing your data in the cloud is not an option, consider external hard drives. As they are generally larger than USB keys, they're not as easy to misplace. If choosing this option, it's important that all files stored on the drive are encrypted – adding an extra layer of security in case of loss or theft.

□

6. Avoid public computers

Many airports and libraries have computers available for public use. Never use these computers to check your email or access confidential information. If you have no other option, always check for the presence of keyloggers – small, cheap devices that log everything you type.

□

7. Use a device tracking system

With their many devices; travelers are often targets for thieves. Oftentimes when a device goes missing, it's not the loss of the hardware that's the issue – it's the loss of its contents. Immediately download tracking software on your device. Many solutions allow you to track the location of your hardware, remotely pull and delete files and take screenshots and camera images to monitor anyone using the device.

□

8. Avoid using local storage for email

If you use Microsoft Outlook, Mozilla Thunderbird or one of the other desktop based email clients, chances are that the viewed email messages will be stored locally. It is better practice to opt-in for web-based access to email, including Gmail via Google Apps, or WebMail for Microsoft Outlook. If you have to store your email messages locally due to corporate policies or low Internet connectivity, always encrypt your email database file.

□

9. Invest in a privacy screen

The majority of modern laptops pride themselves on having a wide viewing angle. While this is a great feature if you're watching a movie with a friend, it's not as impressive when you're reviewing confidential financial reports. Protect yourself while flying or sitting in close quarters with a privacy screen. Privacy screens are cheap and accommodate all sizes of Macs and PCs.

□

10. Keep your laptop inconspicuous

Storing your laptop in your checked baggage or using any other method for concealment could spell disaster. Overly guarded or hidden laptops attract the attention of border guards who could become suspicious of your secrecy, as well as thieves who immediately place a higher value on protected items.

Interested in learning about how TitanFile can help you travel with ease? Contact us today to learn more.