Risk Insights

Advice for you and your business

Data Protection on Business Trips

As a business traveller, you are most concerned about bringing your passport, exchanging currency and packing your luggage efficiently and you may forget an important security measure – backing up and securing your work data.

While the Internet has made it a lot easier to attend virtual meetings with global offices, or communicate with off-shore vendors, there are still instances when you'll be required to travel for business. And if you are like most business travellers, your laptop and smartphone will always be close at hand.

Here are a few things you can do to help protect your data while you are travelling for business.

◉ Backup before you leave

- If you are like most of us, you keep "everything" on your laptop. So if you have not backed up your data in a while, you may want to do so before you leave on your trip. Your business automatically backs up server files? That's great – but keep in mind that the files you have on your desktop may not be included. You can upload them to the server before you go or store them on an external drive and lock it in your desk drawer.

◉ Consider ensuring your laptop has a virtual private network (VPN) installed

- A VPN creates a secure connection between your local computer and a remote computer (i.e. your company's network) via the Internet. Any information that is sent while you are using a VPN connection is encrypted, so even if an outsider intercepts information, it cannot be read.

◉ Ensure sensitive information is protected with adequate encryption

- Many enterprises will not provide employees with a laptop without **full disk encryption** today. Full disk encryption ensures that, if the laptop is stolen, the thief only gets to have the hardware and not the data stored on it. If you do not have full disk encryption, you can still use commercial and open source tools to encrypt files or folders that are most sensitive to you, your company and your clients.

> *Many **enterprises will not provide employees** with a **laptop without full disk encryption today.** This ensures that, if the laptop is stolen, the thief only gets to have the hardware and not the data stored on it.*

Data Protection on Business Trips *(continued)*

Ensure anti-virus and firewall software is installed and up-to-date

- This applies to both your laptop computer as well as your smartphone. There are a number of good mobile security and anti-virus apps available for mobile devices. Where possible, ensure you have enabled your **local firewall** in the operating system on your computer. This is another layer of defence to help resist attackers from connecting to your computer.

Never leave your laptop or mobile device unattended

- Not even if you're setting it down "just for a second." Thousands of laptops and mobile devices are lost or stolen at airports alone each year – do not let yours be one of them. If you're staying at a hotel and you are heading out for dinner, **store your laptop out of sight** in your hotel room or in your room safe if you can fit it.

Use password protection during inactivity time-outs

- Whether you are working on a PC, Mac or Linux computer, you can set a **screen saver password**, which locks your computer whenever you are using the screen saver. Be sure to enable **password protection on your mobile** devices as well.

Make sure your passwords are extra strong

- While you should already be using **strong passwords**, the fact that you are travelling is a good reason to update them. A strong password should be at least eight characters long, should not contain your name or company name (in fact, avoid using any complete words in your password altogether). Make sure it is completely different from your previous password. And finally, **use a mix of upper and lower case letters, numbers and symbols**. If you have a 4-digit password for your mobile phone, do not use easy combinations like 1234 or 1111.

Do not use public Internet connections to do your online banking or shopping

- While it might be tempting to take advantage of a coffee shop's or airport's free Wi-Fi to catch up on your online banking or to make a quick purchase, these Internet access points are not always trustworthy and may not even be provided by a legitimate business.

> *A **strong password** should be at least **eight characters long** and should **not contain** your **name** or **company name***

Data Protection on Business Trips *(continued)*

Switch off your wireless connection when not in use

- Your computer will seek out Wi-Fi access points, broadcast all the ones it knows and try to associate with them. Do not make it easier for anyone around you to gather that information. Prevent illicit access to your mobile devices by disabling Wi-Fi and Bluetooth when they are not in use. You can put your phone on airplane mode to disable connectivity altogether.

Be aware of your surroundings

- Situational awareness is always important for your own safety when travelling. Watch out for that ‘shoulder surfer’ trying to see your smartphone PIN or password. Don’t reveal your company or personal information on your screen if possible by using a privacy screen. Avoid carrying your laptop in dangerous areas or where others aren’t already doing the same. Do not stand out as a target!

Research the destination before you go

- Should you even be bringing those high tech valuables with you? Consider looking for a means to send the data ahead securely so that it is at your destination when you arrive without risking losing it along the way.

Federated Insurance

We believe that knowing your business matters. With industry-specific expertise and decades of experience, we can provide valuable insights, consulting and training to help keep your business safe.

- We specialize in your market and work with you directly
- 100% Canadian-owned
- Insuring companies for almost a century
- Member of the Fairfax family
- Endorsed by more than 50 trade associations

www.federated.ca | 1.844.628.6800

| Risk Insights is a trademark of Northbridge Financial Corporation, licensed by **Federated Insurance Company of Canada** (insurer of Federated Insurance policies). This Risk Insight is provided for information only and is not a substitute for professional advice. We make no representations or warranties regarding the accuracy or completeness of the information and will not be responsible for any loss arising out of reliance on the information.