BIZCOMMUNITY

7 tips to stay cybersafe on business trips

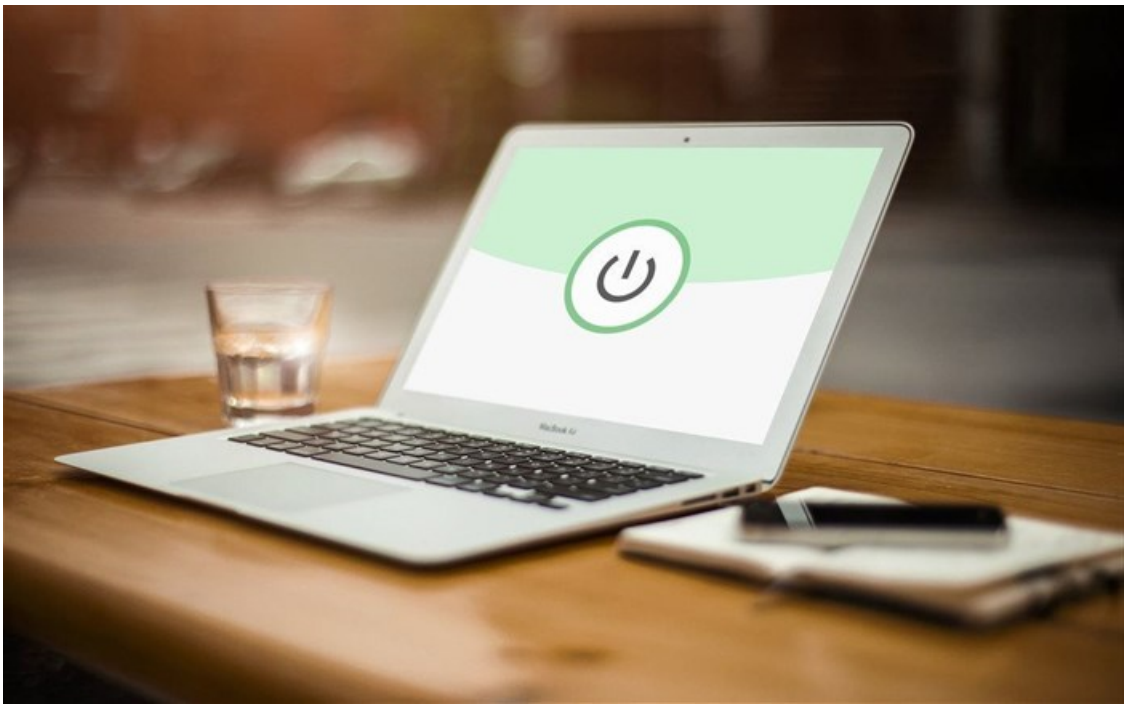
By Bonnie Smith

23 Sep 2022

Imagine the scenario: You're waiting for a flight and using a public Wi-Fi when suddenly your phone is flooded with notifications. According to a study by NordVPN, 1 in 4 travellers has experienced this exact security breach on a mobile device.

And it's not just leisure travellers who let their guard down. A study by IBM Security found that people on business trips are more likely to engage in risky behaviours, such as connecting to public Wi-Fi, than those on holiday trips.

Only 13% of respondents said they'd never used public Wi-Fi while travelling.



Source: Arthur Bowers via Pixabay

The stakes are high in a cybersecurity attack. At best, stolen passwords can lead to embarrassing conversations among friends, colleagues and customers. At worst, hackers can install ransomware that can cost you or your business a fortune.

It’s a reality. No matter where you are in the world, tech-savvy criminals are looking for ways to exploit email addresses, social media profiles, passwords, financial data, and stored files.

When business travellers are on the road, they face unique cybersecurity risks that may be different from what they're used to at home or in the office. These include having a laptop or other device stolen or thieves breaking into the system in search of sensitive information.

To stay safe, it's important for business travellers to be aware of these risks and take steps to protect themselves when away from home.

Here are 7 tips for better cybersecurity for business travellers:

1. Avoid using public wireless networks

Hackers can easily set up malicious hotspots in public places and steal people's personal data, say NordVPN security experts. This is a big problem because it puts everyone who uses public Wi-Fi at risk. It's a good idea to disable your devices' auto-connect and Bluetooth features so they only connect when you want them to. This way, you can avoid accidentally connecting to an insecure Wi-Fi network.

2. Hook yourself up with a VPN

A virtual private network (VPN) is one of the most effective ways for businesses to reduce the risk of cyberattacks. A VPN hides your IP address and encrypts your online activity, making it impossible for hackers to monitor your activity, even if you're using a public hotspot, and gives you a secure way to access company data from afar.

3. Be more streetwise

As travellers, we're often careless about safety once we reach our destination. It's important to remember that thieves targeting travellers know precisely when to strike, such as during meal times when laptops are left unattended in hotel rooms. Extra caution is needed at conferences and trade shows, as thieves know there will be a wide selection of devices with sensitive data around and they have more opportunities to gain access to guest rooms during published conference session times. The best way to protect your devices is to lock them in the hotel safe when you leave your room.

4. Reconsider your out-of-office message

If you're going to be away from your desk for an extended period, you should protect your email account from attack. One way to do this is to not include too much information in your out-of-office message. If you give criminals details about your absence, you make it easier for them to impersonate you in a scam.

5. Keep your software up to date

It can be tedious, especially if you're trying to get through those last few tasks before a trip. But it's worth it. Outdated software can leave you vulnerable to attack, and many security issues are fixed with the latest update. If you're travelling for work, be sure to update your software on all your devices, including your antivirus package.

6. Provide your own power source

Cybercriminals can use USB connections to download data from mobile devices or install malware without your knowledge. To protect your devices from data syphoning while you charge them in a public place, carry your own battery to charge them, choose a traditional power outlet instead of a USB port, or use juice outlet protection.

7. Change your passwords

Your passwords are like the keys to your house. You wouldn't use the same key for your front door, back door and garage. So why would you use the same password for all your accounts? If a cybercriminal gets their hands on one of your

passwords, they could try to use it to access others. That's why you must use a different password for each online account.

With a password manager app, you can keep track of all your individual passwords. Use a strong password for your password manager account. When you get home, you can reset your passwords to whatever you like. Just not your favourite pet’s name or your birthday!

ABOUT THE AUTHOR

Bonnie Smith, General Manager, FCM.