You can travel but you can't hide

Trouble on your business trip is only a click away, says THOMAS PARENTY

Keeping sensitive information safe during business travel used to be simple. Handcuff a briefcase to your wrist, wear a dark suit and sunglasses, and have a healthy supply of exploding pens and invisible ink.

Today, with cybersecurity top of mind, the savvy business traveler is advised to carry a burner phone, use a loaner laptop, avoid email or Wi-Fi, and not carry a mobile phone into meetings.

The advice could very well include saving money on the plane ticket and not going at all. Yes, the risks are real and significant, but should you wish to do anything remotely productive while traveling, they are also unavoidable.

All a cyber attack does is exploit known risks – risks for which there are known countermeasures. If you go out in a rainstorm without a coat or umbrella you'll get wet. However, with a few simple tools you can go outside without looking like a drenched cat. The same principle applies to cybersecurity.

The first lesson is that you can't trust the network. All email and web browsing can be intercepted by anyone in the vicinity of an airport lounge or café where you use Wi-Fi. Your hotel can access any communication channeled through its network, and anything you've sent or downloaded on a local data plan is equally accessible. Your emails back to HQ might not be of as much interest as a world leader's, but still, you have some pretty valuable secrets, right?

Use a virtual private network (VPN). This can be either a business VPN tied to your corporate network or a personal one that connects to a server in the country of your choice. Added bonus: you can bypass any local bans of sites such as Facebook, YouTube and Netflix.

Similarly, every phone call and text that you send will go through networks that can be monitored. Encryption may provide the answer. FaceTime and WhatsApp are encrypted by default. Alternatives include Silent Circle and Open Whisper Systems.

For those who are gifted at leaving phones on airplanes or laptops in hotels, talk to your IT department about enabling whole-disk encryption on your hardware. It will render your information gibberish should someone copy it. For the increasingly paranoid, ask them to set a "BIOS" password – this will bolster the security of your operating system.

Think a nation state might be after you? Use a laptop with a bad maintenance rating. The harder it is to fix, the harder it is to put an evil chip into it.

In addition to having anti-virus software, update your software before your trip and don't install any updates while you're on the road. They can make you vulnerable.

Another threat is malicious software. Once on your device it can do whatever it likes, stealing or destroying your information, or surreptitiously turning on the camera and microphone. As a last resort, don't do anything in front of your devices you wouldn't want a cyber attacker to witness. It's probably best to leave the handcuffs at home, or at the very least, on the briefcase.

"OK, go ahead. I'm on a private network."

CARTOON: KAAMRAN HAFEEZ

A veteran of the US National Security Agency, **THOMAS PARENTY** runs a consultancy advising global businesses on information security.