+44 345 094 0945
www.waterstons.com
Article

Stay secure while working away

Breadcrumb

1. Home /
2. Print /
3. Pdf /
4. Node /
5. Entity Print

Insight navigation

- Latest insights
- Latest news
- Articles
- Case studies

Download PDF

Jul 2023

Stay secure while working away

The summer holidays are almost upon us and its common for many to take the opportunity to take their remote working location further afield than a home office or the dining table. Working from anywhere gives immense perks for many employees, but it's important to make sure you and your team know the risks, restrictions and rights involved.

Categories Cyber Security Strategy

Jul 2023

Sean-Francis Brown

Senior Information Security Consultant

Email

sean.brown@waterstons.com

Here we share our top five pieces of advice when working away from your office or secure home network.

1. **Avoid prying eyes – and ears**

Thieves are always on the lookout for opportunities to steal data, and shoulder surfers use direct observation to do just that. It

could be anything from noticing what is written on a form to a PIN entered in a cash machine, looking over your shoulder in a crowded café or even using binoculars to read personal data on a laptop screen.

But it's not just your screen that could be compromised – 'shoulder' surfers also monitor phone conversations, listening in from the next seat on a train, walking behind someone in the street or even through thin hotel walls.

It may seem extreme, but if you work with confidential or legally protected information it could result in a significant data breach, loss of revenue or potentially costly ransom demands.

When choosing somewhere to work, be aware of your surroundings and ask yourself: can someone look over my shoulder or hear what I'm saying? If so, best to change location.

2. **Taking things with you**

Over 12,000 laptops are left in airports around the world each week, and we hear of enough left on trains by important people to know that it can make national headlines, but it's not only politicians and company leaders who need to be vigilant when it comes to transporting and storing devices.

Your work devices can often access significant data not only about your own company, but also your clients, so you could lost more than simply the last document you were working on.

Devices should never leave your possession when travelling; whether ordering a coffee, nipping to the loo or stretching your legs, you should have your device/s with you, or ensure they are in the care of a trusted colleague.

Mistakes happen, and flustered travellers can misplace items when running for trains or flights, so companies should always have procedures in place to clear, or lock down a device in the event of a breach or issue.

The risk of loss or compromise are only two of the issues to bear in mind when travelling with your device/s.

Many organisations require prior notification of where you will be taking your device for insurance and protection purposes. If you're usually at your home office in Reading, your IT team may become suspicious if all of a sudden you're logging in from Borneo.

The best way to protect your device is to ensure it is encrypted – but that can lead to challenges in its own right as many nations restrict, and often ban, the carriage of encrypted products without proper authorisation. Largely manifesting from the use of encrypted devices to launch acts of terrorism and cyberattacks, it's understandable that restrictions are in place, so always check before you travel.

3. **Accessing Wi-Fi**

We live in an age where Wi-Fi can be accessed almost everywhere – gone are the days of internet cafes or connecting to the cables in the library. However, with this upgrade in connectivity comes an increase of risk.

Due to widespread encryption, most public Wi-Fi networks are safe – which you can check by looking for a lock symbol or https at the start of the address bar. Best to do that before you work on anything!

When accessing a public network, it's common to be asked for personal details to do so. While this is a common data capture tool for marketing purposes, it can be used for nefarious purposes – so always read the fine print before giving away any personal details.

One of the best ways to avoid this risk is to use your personal device as a hotspot for internet connectivity. Just make sure you have a strong password – and sufficient data!

4. **Plugging into things**

While significantly more convenient due to not having to carry bulky chargers, it's wise to avoid plugging devices into hotel room, café, or bar USB ports. Why? Juice jacking. Yes, that's a thing.

Juice jacking is a type of cyberattack that hackers use to access data or install malware on your device to cause malfunctions, infiltrate data, and generally cause havoc.

5. **Plugging things in**

Similarly to plugging IN to things, you should always be careful about WHAT you're plugging into your device.

According to the Honeywell Industrial Cybersecurity USB Threat Report, 52% of threats were specifically designed to utilise removeable media. This means that anything you connect to your device – USB stick, camera, portable hard drive – could be designed purely to access your data.

Practice safe security – don't put anything in, or put your things into, anything you don't trust.

Thinking of working away and not sure what you need to consider? Or are your team planning to spend time abroad and not sure what's involved? Get in touch with our team on info@waterstons.com to find out more.