Queensland Law Society

QLS Guide: Information security on the road

Some basic tips for legal professionals working away from the office

March 2019

What is the information security risk of working away from the office?

Remote working exposes legal professionals to an additional set of information security considerations. Out of the office we can be:

- dependant on an electronic stream of information, and less likely to verify email instructions;
- more likely to encounter insecure or fraudulent equipment such as Wi-Fi, chargers or printers;
- inclined to upload sensitive data to cloud storage or USB devices;
- tired, jetlagged and targeted by airport thieves;
- using smaller, personally owned or less secure equipment;
- unable to contact IT if something is odd or not working;
- exposed to more distractions, and possibly less careful than during standard work hours; and
- inadvertently sharing the contents of your screen with the person behind you.

What can we do to about it?

Like most information security strategies, risk minimisation for remote working is part focus, part preparation and part technology.

Policies need to be explained to and applied by everyone. Senior people are often the worst offenders for failing to follow IT policy, and of course are often the most valuable targets. If you are a sole practitioner you need self-discipline, and if you are a partnership, the partners collectively need to make sure that everyone knows and follows agreed procedures.

Phishing

Phishing attacks on phones via email and SMS are now a very common way for law firms to suffer a major data breach. This is not exclusive to being out of the office, but we are more vulnerable due to the smaller phone screen, and the fact that we often just quickly check messages while primarily focussed on other matters.

A Phisher's usual objective is getting someone to follow a link which either infects the device with malware, or asks you to enter your password to access a document.

Risk reduction for users:

- Don't follow links in messages or email, even if you think the sender is trustworthy. Navigate directly to the website or use an app.
- Fake website log on pages can look identical to the real thing. Check the URL carefully, and never enter passwords if prompted by a link.
- Ask your IT department / provider to walk you through what normal message / document retrieval looks like. Unless you understand "normal", you won't be able to spot "odd".
- Separate business from private email. Set up a "burner" email for use with online shopping and general web use, a secure personal email for more important communication and keep business for business.

Risk reduction for firms:

- Develop training and policies to support users in the above objectives.
- Train staff to spot Phishing attacks, but don't put total reliance on that as many attacks are almost undetectable.
- Consider mail screening services. Your email provider may offer this. If not, specialist providers can screen out some (but not all) fraudulent emails.
- Introduce two factor authentication for all email and document storage.[1]

[1] Multi factor authentication is one of the best value for money steps an organisation can take to protect confidential data. It can keep attackers at bay even if a user is successfully Phished.

Free Wi-Fi and phone chargers are dangerous

Avoid plugging your device into any equipment you don't own (such as a charging bar or printer) and avoid free Wi-Fi – especially in a public place such as an airport - but even your own hotel is a risk.

A fake Wi-Fi hotspot can be built for just a few dollars and placed in airports, conference centres, hotels or cafes. The log on screen looks the same as the real thing, and the Wi-Fi will work, but the attack device can copy everything (including passwords) accessed on it.

USB charging facilities can inject malware or copy data. Even legitimate hardware may be a threat from misconfiguration or if infected with malware.

Risk reduction for users:

- Don't use public Wi-Fi. Either avoid hotel Wi-Fi altogether or be very careful to ensure that you know exactly what the SSID (Wi-Fi name) should look like (eg: CosyHotel may be legitimate, but Cosyhotel may not). For more tips see here.[2]
- Consider buying a tablet or similar device for entertainment and video chat over insecure Wi-Fi and don't use this to access anything important.
- Don't use charging stations or USB charging in public places. Only use your own charger plugged directly into a power socket.
- Follow normal security procedures for mobile devices (see here).

Risk reduction for firms:

- Training and policy for staff and partners is essential.
- Use a VPN. These come in two types – a corporate VPN and domestic. For an explanation of the difference see here.[3]
- Supply a firm mobile dongle, and be generous with the data allowance. Generosity might not extend to Netflix on the road, but the less incentive staff have to use hotel Wi-Fi the better.
- Follow QLS guides for mobile device security (see here).

Accessing data

Remote access to a firm network can be achieved in a number of ways, some of which are extremely insecure. Configuring such access is best left to an IT professional. The IT-Pro should be requested to supply detailed written instructions on how to use and troubleshoot connection problems. This should be printed and kept available, but obviously with any passwords omitted.

Data in the cloud may be accessible irrespective of where the device is located (check prior to international travel. Blocking overseas access is a sound security practice in many cases, and you may need that feature temporarily disabled before you go).

Physical device security

A reminder that travellers can be tired, jetlagged and easy targets for thieves in airports and hotels. Phones and tablets put down for a second while we open a suitcase can disappear, and important information copied to USB for use out of the office can easily fall out of a briefcase.

Risk reduction for users and firms:

- Know and use the measures suggested in the QLS Guides for Android or Apple mobile devices, and the Data Storage Best Practice guides.
- At the very least, encrypt all data on a USB/storage drive and have a good password on your phone.
- Buy and use privacy screen-guards for laptops to make it harder for people behind you to read documents you are working on (the removable kind is best, as they do make screens slightly less readable for the user as well).

Enquiries: David Bowles
Direct line: 3842 5937

[2] <https://www.safervpn.com/blog/recognize-fake-public-wi-fi/>.
[3] <https://www.pcmag.com/article/363962/why-consumer-vpns-arent-business-grade>.