How to stay safe in your mobile office

Ten years ago, your staff would never have considered taking their office computer home with them at night. They certainly wouldn't have taken it up to their bedroom or on holiday. But that's exactly what many of them do now, because their smartphone is one of their office computers.

New research from Oftel shows that more people access the internet from their smartphone than from laptop computers. Mobiles don't just go everywhere with people; they're also becoming the main route onto the internet, for work and pleasure.

Given their popularity, it's no surprise that criminals are increasingly targeting smartphones, both for their intrinsic value and the data they give access to. Information shared via mobiles can effectively bypass many of the security systems operated by companies, leaving firms exposed in ways they may not anticipate.

We've put together some recommendations for keeping your smartphone safe. The same principles also apply to laptops, tablets and any other form of mobile computing device.

Tips for keeping your data safe on a smartphone

1. Don't lose it. This might seem obvious, but 300,000 phones are reported lost in the UK every year, with the real number that go missing probably being much, much higher. It's amazing how we seem happy to leave a device worth several hundreds of pounds on café tables, in the back of taxis or on trains. To a cybercriminal, a lost or stolen phone can provide a goldmine of information, worth much more than the phone itself.

A simple way to reduce the risk of loss is whenever you leave anywhere, always look back to see what you may have left behind.

2. Activate device tracking and keep a note of serial numbers. If you do lose your smartphone, there's a chance you may be able to get it back. Device tracking systems are becoming increasingly sophisticated, allowing your phone to broadcast its location. Keeping a record of serial numbers and its IMEI number will also help identify it and can allow mobile operators to shut it down.

It's a good idea to adopt a policy of recording key information whenever you get a new phone or other device, and understanding the tracking options.

3. Keep the screen locked. But don't rely on this keeping out someone who knows what they're doing. While a simple PIN or unlock pattern can deter a casual user, such as a family member, from using your device and inadvertently accessing commercial data, it won't stop an experienced attacker.

If you don't currently lock your screen, take a few moments to activate this feature, and when it comes to choosing a PIN, avoid the obvious combinations, such as a birthday.

4. Take care on what you click. The fastest route for a cyberattacker to reach your smartphone is by installing malware on it. This is achieved most easily by persuading you to click on something that delivers the code. The attempts to make you click are becoming increasingly sophisticated, as cybercriminals learn how to turn human behaviour to their advantage.

A good habit to develop is to pause before clicking or sharing anything and to perform a quick sense check as to whether it might be a threat in disguise.

5. Only install apps that you trust. No matter how cool an app might be, if you can't be entirely sure of the source, it may be wise to give it a miss.

One way to be certain that the app is available from an official app store is not to follow a link from a website or social post, but to find it yourself through the store app.

6. Avoid insecure or public wifi. Almost everywhere seems to offer wireless internet these days, but the levels of security vary widely. It's easy for a cyberattacker to connect with an insecure wifi network, such as in a busy café, and then monitor what users are up to.

It's unwise to access commercial or financial data and systems using wifi that may not be secure. If in doubt, don't do it.

7. Security software. Antivirus apps, common on desktops and laptops for years, are also available for smartphones. While they're always one step behind the most sophisticated cyberattackers, they provide another layer of protection. This layer is strengthened when the app is part of a company-wide network that's configured correctly.

A good business IT security solution will now encompass every device that touches the network, including employee-owned devices used to access business systems, data and email.

How we can help you with mobile security

Clients using our mobile device management service enjoy a number of benefits including:

- Set-up of authorised configurations, managed centrally and remotely.
- Control over which apps are installed and how they are set up.
- The capability to remotely lock or wipe a phone or other device that's no longer controlled by the business.
- Monitoring of password complexity.
- Advanced location tracking.

If you're concerned about the risks of mobile data use in your organisation, we'd be pleased to have a no-obligation conversation about the options open to you.

To find out more, give us a call on 0808 168 9135 or email enquiries@itsupport365.co.uk.

Mobile data security is a new, complex area that cybercriminals are moving fast to exploit. Take action now to minimise the risk of your business becoming an easy target.