

What security impacts do mobile devices have on your business?

Companies of all shapes and sizes should be re-evaluating how they protect business-critical data and manage IT equipment use.

Too few companies have policies governing how employees use smartphones and tablets.

It's time to recognise the security threats posed by these mobile devices and put in place the technology, procedures and policies to deal with them.

As a small business owner or employee, you and your fellow staff members are probably keen to get your hands on the latest smartphones, tablets and portable laptop computers, to assist with your daily routine in and out of the office. Indeed, you may already have one!

The popularity of such mobile devices has seen staff in rapidly growing numbers bringing their own devices to work and using them for business purposes.

Workers are connecting to their company's Wi-Fi network, which provides access to the Internet and allows them to synchronise the devices with company computers. This often occurs without any additional layers of security control.

DOES LOTS OF POWER POSE POSSIBLE THREATS?

Today's sophisticated mobile devices mirror their desktop computer equivalents in almost every sense – they are packed with immense storage and computing power. The famous quote, "With great power comes great responsibility", comes to mind.

The vulnerability of mobile devices used in business is a very real threat. It is evident that employee devices are now as much a part of business IT resources as servers or databases where client records are kept. This means the apps and files on employee's devices (for both business and personal use) now start to form a solid element of risk.

Confidential business information can be compromised, as people can easily lose or mislay their mobile device. There is a lot of malicious web-based content specifically designed to attack mobile computing users.

Laptops and tablets can also be hacked over shared Wi-Fi networks in public places and smartphones can be subject to 'rooting' or 'jailbreaking', where the unit's security settings are disabled by a cyber criminal seeking a host to embed malware.

For these reasons, it is essential that all mobile devices are password protected and have security software installed on them.

THIS IS NOT PLUG-AND-PLAY COMPUTING

While mobile devices can significantly boost employee productivity when used conscientiously, small business owners need to realise that this is not plug-and-play computing.

There is a need to consider whether to allow employees to use mobile devices for both business and personal use. If they are going to be used for both purposes, employers should find out what kind of devices and apps are being used specifically, and also enforce company security policies to protect the business.

AVG (AU/NZ) recommends business owners put together a policy document spelling out security requirements and permissible usage. The **AVG Online Security Audit** can be used to assist with this process. It asks how employees use company and personal equipment – from computers and laptops, to smartphones and USB sticks – and what policies are in place for the use of business and private hardware, plus access to social networking and other Internet usage. A personalised audit report is then produced for the business, identifying where problems lie and recommended actions. The **AVG Online Security Audit** is available at <http://audit.avg.com.au>.

AVG (AU/NZ) provides security software to protect both small business and individuals – including **AVG Mobilation** for Android™ based smartphones and tablets and **AVG Internet Security Business Edition** for laptops and notebooks on the move (especially when using Wi-Fi networks), as well as workstations and servers back in the office.

Secure your devices and confidential business information with an AVG solution today!