

Smartphone Security

**BUSINESS CRIME
REDUCTION
CENTRE** ↓



As mobile devices become more sophisticated, they lend themselves to the same types security risks that PCs have done in the past, this makes them a very appealing prospect to cyber criminals and a real threat to your personal and sensitive data.

The Business Crime Reduction Centre has produced this fact sheet to raise awareness of these risks.

How is my Smartphone's security at risk?

Businesses are careful to dispose of any paperwork that can give away personal information to criminals, but your smartphone probably contains just as much sensitive data as anything you keep in a file at the office.

Smartphones can be used to access your email accounts and any information inside them, follow your social network activity, and track what you search for on the internet, as well as the websites you visit.

If you use popular travel applications such as Google Maps criminals could see what locations you've visited and perhaps work out where you live.

This vast amount of personal information can potentially be retrieved either by malware or by the theft of your handset.

Another growing risk to Smartphone's is 'silent activation'. This is where malware gets onto your phone and calls a premium number set up by a hacker. These calls can rack up huge bills without your knowledge.

How can I keep my smartphone safe?

The good news is its not difficult or even expensive to protect your devices and the information they contain.

Update your software regularly

Making sure your software is up-to-date is the first line of defence.

Every software patch released addresses a number of security vulnerabilities, which is essential in keeping your device's in-built security up-to-date. A good rule is to check your manufacturer's website every couple of weeks to see if any software or firmware updates are available. If so download and install it, closely following the manufacturers instructions.

Watch your apps! Use approved suppliers and developers

Apps are great fun, and many are offered for free, so it can be very tempting to download them without checking the source, this can provide an easy route into your device for cyber criminals. Be particularly wary of the Android app market, as this tends to be very open, without the strict developer guidelines found in Apple's App Store. For any app you download make sure you trust the developer and have checked on other users reviews and feedback.





Security Settings - Don't mess around

Most security settings in Android, iPhone and Blackberry devices are fairly secure out of the box. Do not change these without checking with your manufacturer or service provider.

Avoid unencrypted public wireless networks

Public wireless networks sometimes do not require a password to login, which means anyone can access them, including criminals. If you are connecting to these networks be cautious about the sorts of things you do e.g. Online banking or shopping which may be visible to the criminals. A good rule is to turn off your Wi-Fi functionality when you're not using it. This will prevent your device automatically connecting to networks.

Turn off cookies and form autofill

If your device is set to automatically enter passwords and login information into websites you frequently visit, turn this setting off. It might seem convenient but it carries a privacy threat. This information might fall into the hands of a criminal.

Locks and Passwords

Lock your device with a pin code or password. Use a combination of letters, numbers and special characters. Never use things like your favorite song or football team as this information can be obtained from social networking sites you may have used.

Back up and encryption

Back up your data. Either through a product that offers this functionality, or simply by copying your documents, pictures and other information to your computer. When you are accessing a website e.g. banking from your device, make sure you are using HTTPS. The S means you are connected to a secure encrypted site.

Consider using an anti-virus package

There are some mobile anti-virus packages available on the market which can help to protect your phone, always check with the phone manufacturer before buying and installing any software for the handset.

If your phone goes missing

There are also a number of remote wipe apps available which means that if your phone is lost or stolen, you can remotely clear all of your data, including e-mail, contacts, texts, and documents from the handset, thus keeping sensitive information away from criminals.

Which Smartphone's are most at risk?

Each type of smartphone operating system has its own separate risks when it comes to hackers or malicious software.

The iPhone, for example, has a 'sandbox' configuration, which stops applications communicating with the phone, in theory making the Operating System more secure. But recent advances in multitasking technology means the iPhone may be more at risk than previously thought.

Android phones are more closely related to PC operating system structures and therefore potentially provide a relatively easy target for cyber criminals to explore.

One of the biggest problems for the Android operating system is that its apps market is built on an open model, with very few quality controls, making it easier for malicious apps to find their way onto your phone.

BlackBerry devices are thought to be more secure than others, as they employ encryption software to protect data - one of the reasons they are so popular amongst business users.

Be Smart to Stay Safe