LIVERPOOL JOHN MOORES UNIVERSITY

Protect your smartphone

Date created: September 2016

Smartphone Security

Smartphones are revolutionising how millions of us go online each day, but they also carry some risks. Should your smartphone fall into the wrong hands, it is a potential treasure trove of information. If you download a rogue application, it's even possible for hackers to hijack your phone without it leaving your side.

In collaboration with Ofcom, the Office of Fair Trading and PhonepayPlus, the Information Commissioner has released the following guidance on how you can protect the information held on your smartphone.

1. Guard your phone, and set PINs and passwords

Treat your phone as carefully as you would your bank cards. Take care when using your phone in public, and don't let it out of your possession. Thieves can quickly rack up huge bills on stolen phones, and you may be liable for all charges run up on your phone before you have reported it lost or stolen to your provider.

To help prevent this happening, protect your phone against unauthorised use by setting up a PIN, swipe pattern or password for your home screen. You can usually do this through the Settings feature on your phone.

2. Take precautions in case your phone is lost or stolen

Make a record of your phone's IMEI number, as well as the make and model number. The IMEI is a unique 15-digit serial number which you will need to give to your mobile operator to have your phone blocked. You can check your IMEI number by keying *#06# into your handset or by looking behind your phone battery.

Consider making your phone less useful to potential thieves by barring calls to international numbers and premium rate lines, if you never use them.

Some mobile insurance policies, or any other policies that may cover the mobile phone, could provide limited cover for unauthorised use. So it is worth checking the terms and conditions of your existing policy, and when considering a new policy.

The national Mobile Phone Crime Unit's "Immobilise" database is a free registration service that assists the police in reuniting owners with their stolen smartphones.

For further details and contacts for different operators, see Ofcom's Lost or Stolen Phone Guide

3. Don't override your smartphone's security settings

It is not advisable to attempt to 'crack', 'jailbreak' or 'root' your smartphone or tablet. This is a process people use to remove restrictions placed on their device's operating system by the phone manufacturer. Doing so carries considerable risks; it compromises the security of your device, and may leave you more vulnerable to malicious software. It is also likely to invalidate your manufacturer's warranty.

4. Back up and secure your data

Many smartphones come with a software package to back up your data to a personal computer, so that you don't lose it if your phone goes astray. Check for information on how to do this in the phone's manual. There are also some third-party applications ('apps') that can do this for you, creating a copy of information such as contacts, photographs and other data.

5. Install apps from trusted sources

Apps are the easiest way for someone to hack into your phone. Sometimes hackers will take a popular paid-for app, add their own illegitimate elements and then offer it for free on 'bulletin boards', 'peer-to-peer' networks or through fake online stores. Once the rogue app has been downloaded to your phone, the hacker can potentially take control of the handset, incur charges via premium SMS without your permission, make calls, send and intercept SMS and voicemail messages, browse and download online content. You may not be aware anything is wrong until it's too late.

So avoid apps from unauthorised sources, such as ‘bulletin boards’ or ‘peer-to-peer’ networks. Instead, download your apps from official stores, such as the Apple App Store, Blackberry World or Google Play – and exercise care: for example, research the app and check reviews.

6. Use antivirus software

It’s not just rogue apps which pose a threat to your smartphone. Viruses and spyware can also be downloaded from websites, or by connecting your device to an infected computer. Some phone may be more vulnerable than others, but you can check for antivirus software in a reputable app store such as Google Play.

Also, before connecting your device to a computer, ensure it has the latest antivirus/antispyware and firewall installed and running. To find out more, visit Get Safe Online, the UK’s national internet security initiative.

7. Use software to find or erase your phone if it goes missing

Consider installing a reputable security app that enables you to track your phone’s location if it goes missing, or to wipe data from the phone remotely if you’re not able to recover the handset. Some manufacturers provide such an app themselves: for example, Apple’s Find My iPhone, the Android Device Manager or Windows Find My Phone. Third-party apps are also available to perform a similar function.

8. Clear your phone before you dispense with it

If you decide to donate, resell or recycle your smartphone, remember to erase any data on it first. Remove and erase any media cards and perform a full or ‘factory’ reset by going into the Settings menu.

9. Accept updates and patches

Occasionally, your smartphone manufacturer may send you a message proposing an update to your operating system – the software that runs your device. App developers may also propose updates to their app. It is advisable to accept these updates as they become available. As well as typically offering new features and improving your phone’s performance, they can also fix security vulnerabilities.

Mobile apps

Top tips for keeping your personal information secure when using apps:

 Only download apps from official and trusted app stores. Be extremely careful of using untrusted sources.

 Read the information available about an app in the app store before you download it. Check you are happy about the personal information it will be using.

 Have a regular clear-out. Many of us have downloaded an app and only used it once. If you no longer use the app, uninstall it.

 Consider downloading mobile security software to help keep your device secure.

 Make sure you erase any apps from the phone before you donate, resell or recycle an old device, as these may have access to your personal information. You should be able to find a ‘factory reset’ option in the device settings.