Using apps safely and securely on your mobile

In association with: PhonepayPlus, ico. Information Commissioner's Office, CMA Competition & Markets Authority, FCA Financial Conduct Authority

Apps are becoming an increasingly important way to communicate and access the internet through our phones, tablets and TVs.

We use them to play games, send messages, check the news and weather and use maps and navigation services. Increasingly we are also using them to do our banking. While apps provide a simple and easy means of accessing great content and services, it's important to be aware of how to use them safely and securely.

Here are some tips to help you make the most of your smart device and apps and how to use them with confidence. This guide has been produced by Ofcom in association with the Information Commissioner's Office, the Competition and Markets Authority, PhonepayPlus and the Financial Conduct Authority.

1. Install apps from recognised app stores

It is possible for some apps to exploit your mobile device once installed. This possibility increases if you install an app from a less reputable (or unknown) source. For example, someone could take a popular paid-for app, add their own illegitimate elements and then offer it for free on 'bulletin boards' or 'peer-to-peer' networks. Once the rogue app has been installed to your phone, the hacker could potentially take control of the handset, make calls, incur charges via premium SMS without your permission, or send and intercept SMS and voicemail messages. 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. Above all, exercise caution - research the app and check reviews before downloading it.

Ofcom

2. Consider content ratings

Apps in some popular app stores provide content ratings. The ratings may help you judge whether an app is appropriate for children.

Typically the ratings will give guidance on the content and intensity of themes such as violence, offensive language, sexual content, or drug references. You should be aware that each app store has its own content rating policy. This means that ratings will differ from app store to app store.

The table below outlines the different content rating systems used in some of the major apps stores:

Apple's app store

4+	Contains no objectionable material*
9+	May contain mild/ infrequent violence, or mature, horror-themed or suggestive content
12+	May contain frequent or intense violence or mature content
17+	May contain all of the above, plus strong sexual, alcohol- or drug-related content

*there is also a Kids' category, which curates age-appropriate apps

Google Play

Everyone	No objectionable, social or user-generated material*
Low maturity	May include mild violence. Some social material allowed.
Medium maturity	May contain sexual or mature references, social and UGC
High maturity	Frequent sexual/ suggestive/adult content

Windows Store

3+	Minimal comic violence, no shock content, and no nudity
7+	May include frightening content and partial nudity
12+	May contain nudity, partial violence/ profanity
16+	May contain violence and some sexual/adult activity
18+	May contain intense, gross or specific violence
Adult	Can't be listed or sold unless the app is a game and is rated by a third-party ratings board

Blackberry World

General	Items suitable for all ages
Teen (13+)	Suitable for young teens and above
Mature (17+)	Suitable for older teens and above
Adult (18+)	Suitable for adults only

Please note these ratings relate to the content in the app itself. If you use apps that allow you or your child to connect to the internet and access content outside the app, you may want to consider further device-level or network-level protections, filters or safe search options. More detail on these can be found at http://www.internetmatters.org/technologies/parental-controls.html

3. Be aware of what permissions you are granting

When you download an app, it will often ask whether it can access certain systems or data on your device. This is known as a 'permission request' or a 'permission'. For example, navigation apps may ask for permission to use your "current location" in order to provide accurate directions and location information. Photo editing apps may ask to gain access to your photos so that you can edit photos you take on your handset through the app.

It is generally agreed that developers should only request data and features directly necessary for the app to run. Some apps, however, may request additional permissions beyond what is strictly necessary for the particular app being accessed to function.

In order to protect your personal information, carefully read permission requests upon download or when prompted and ensure you are comfortable with the information you are authorising the app to use.

If you are not comfortable with the requested permissions you should deny the request or search for an alternative app.

4. Treat your phone as your wallet

Using a smart phone to manage your money is growing in popularity. Last year, customers of UK's biggest banks made more than 18 million mobile transactions every single week. There are some clear advantages to mobile banking: apps offer a simpler and more convenient way to bank on the move, and also save you time and money. But, inevitably, there are risks too. You need to remember some basic housekeeping e.g. it's important to log out of your banking app; only download from official app stores; not to change the factory security settings on your phone; and password protect your phone.

5. Be aware of costs, especially for roaming and in-app purchases

Apps typically consume data which may use up more of your mobile data allowance. If you're not careful about monitoring your data usage, you could end up going over your inclusive data allowance and incurring extra charges. Most mobile providers now offer online monitoring tools or apps to allow you to check your usage easily.

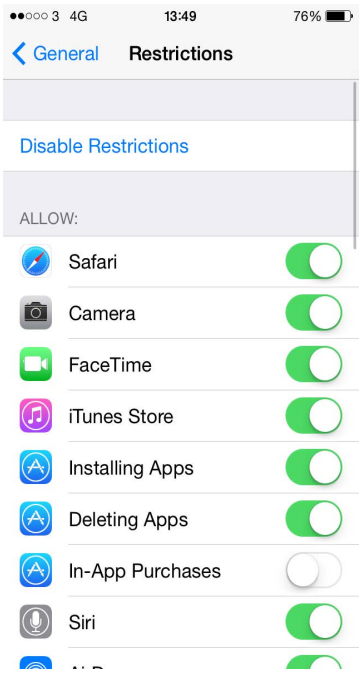
In addition, using apps abroad can lead to higher bills. Consider switching off mobile data roaming while you are away to help avoid a bill shock. Check out Ofcom's video guides which show you how to do this on some popular handsets. For further details on how to use apps abroad safely see Ofcom's guide to mobile roaming.

Many apps, both free and paid for, offer optional extras at a cost. These are known as in-app purchases. For example, you may have to make an in-app purchase to continue to play a game after a certain level, or to speed up gameplay.

In-app purchasing can be of particular concern to parents because children using the mobile device may run up high charges on an account without their parents' knowledge. Those wanting to control unwanted in-app purchasing can do so using a number of tools that are available across the recognised app stores. For instance, some operating systems allow you to require a passcode for each download or purchase.

IoS

The restrictions menu in iOS allows you to require a password for every purchase made on your iOS device.



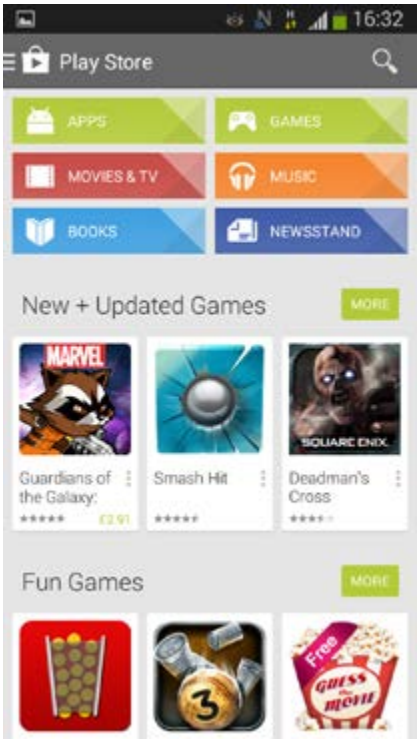
1. Tap Settings -> General -> Restrictions

2. Tap Enable Restrictions

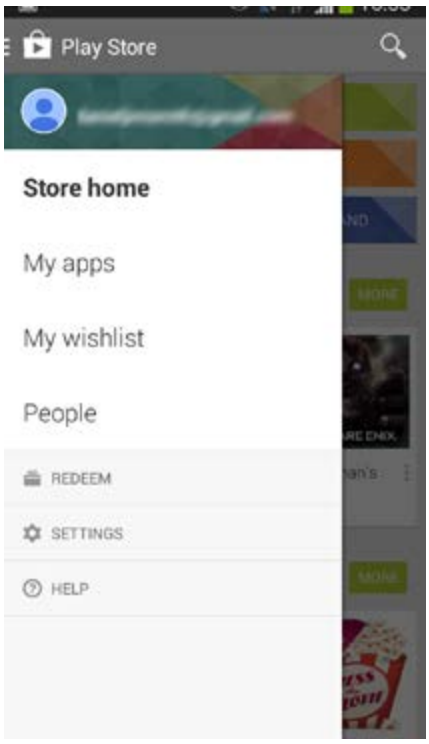
3. Choose a restrictions passcode that you will remember and confirm your passcode. We recommend choosing a passcode different from the passcode you use to unlock

Android

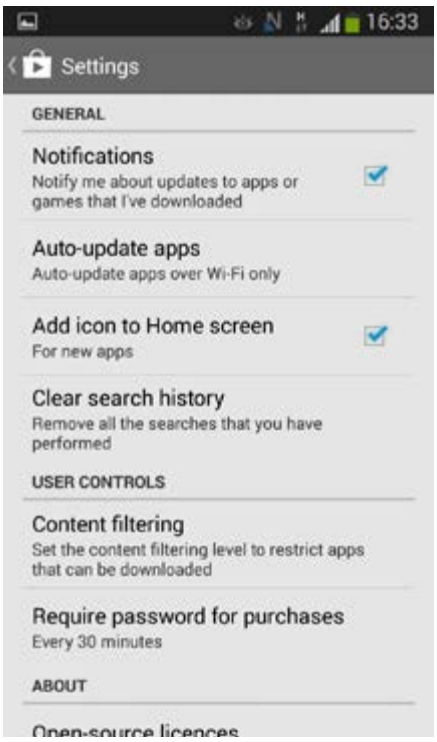
The settings in Google Play allow you to require a password for every purchase made in the Google Play store.



1. Go into the Google Play Store. Tap on the menu icon. Here it is located on the top left of the home page



2. Tap on Settings



3. Tap Require Password for purchases and then tap For all purchases through Google Play on this device.

Some mobile handsets allow you to disable in-app purchases altogether. Ofcom's video guides show you how to do this.

The screenshots are indicative as the settings may vary depending on the handset and version of the OS they have installed.

6. Regularly clear out the apps you don't use

How many apps have you got on your device – and how many of these do you actually use? Ofcom research found that almost half of apps downloaded are not regularly used.

Filling your device with dozens of redundant apps can affect its performance. Not only do they take up space but some apps constantly run in the background which can slow down your device and drain your battery. Go through your apps and remove any that you don't use anymore.

For apps that you regularly use, consider keeping them up to date as this may fix app performance or security issues.

7. 'Clean' your phone

If you decide to donate, resell or recycle an old mobile phone or tablet, make sure you erase all data and apps first as otherwise these may be accessed by whoever your device is passed to. You should also be able to find a 'factory reset' option in your device settings although this option may not delete all your personal information from the devices.