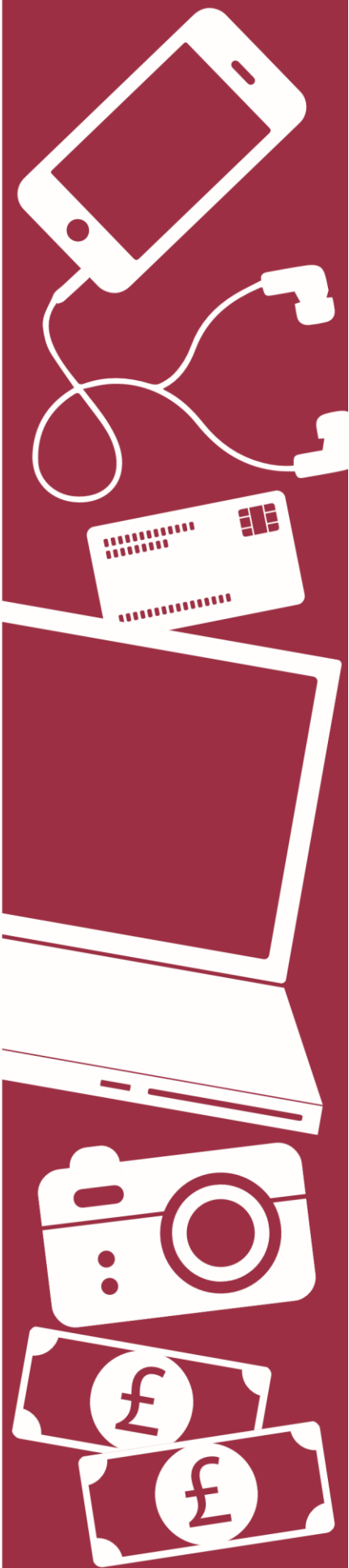


ARE YOU AN EASY TARGET?

Protect yourself from thieves stealing your personal belongings

- ➔ Are you valuables on show? Keep your smartphone, tablet, bank card out of sight
- ➔ Is your handbag closed? Consider over the shoulder bags with clasps facing inwards
- ➔ Is your jewellery covered? It may be wise to cover with a scarf or clothing
- ➔ Be aware of your surroundings? If you feel unsafe change your direction
- ➔ Use well lit, busy streets and a route you are familiar with
- ➔ It may be a good idea to scan the area around ATM's before you use them



Contact/Advice

Contact your local Crime Prevention Team for expert advice:

<https://www.westyorkshire.police.uk/contact-us-3>



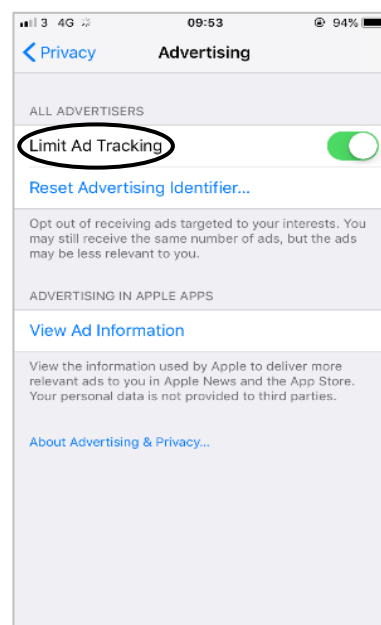
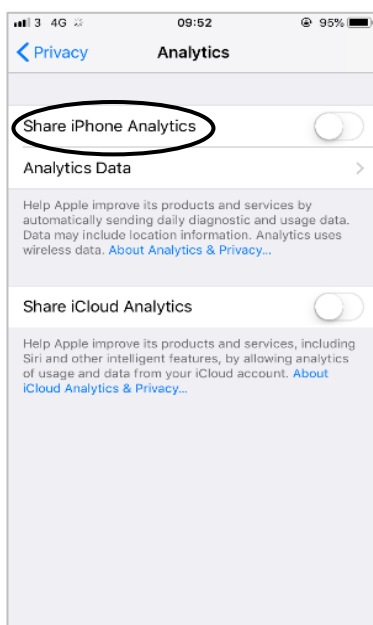
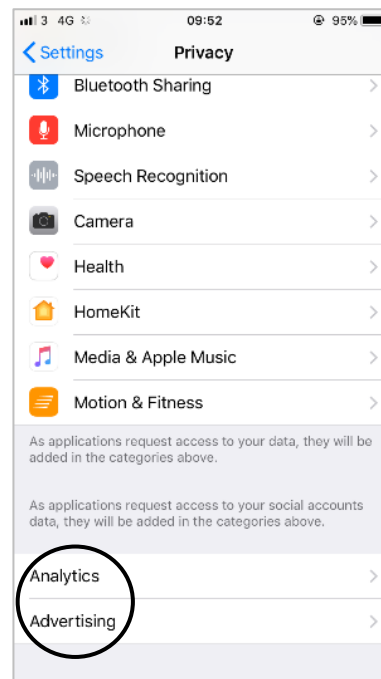
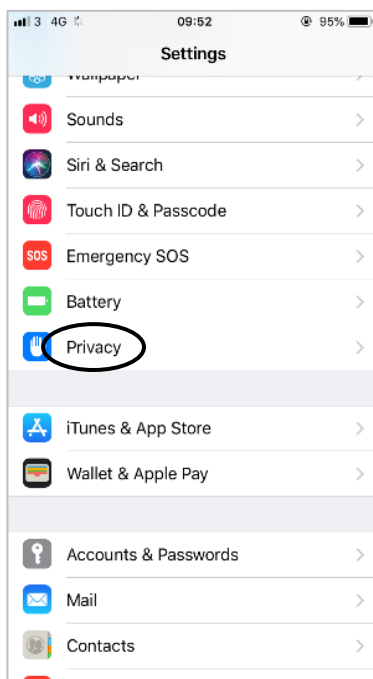
**WEST YORKSHIRE
POLICE**

Apple – Making your iPhone secure

Analytics and advertising - Turning off 'Analytics' means Apple won't get data on how your device performs (in a nutshell, you'll be handing over less data!).

Disabling the 'Advertising' means you won't get ads that are targeted to your interests.

1. Tap on **Settings**.
2. Then tap on **Privacy**.
3. Scroll to the bottom where it will show **Analytics** and **Advertising**.
4. Turn 'Share iPhone Analytics' off if you don't want to share analytic data from your phone to Apple.
5. To remove ads ensure 'Limit Ad Tracking' is turned **on**.

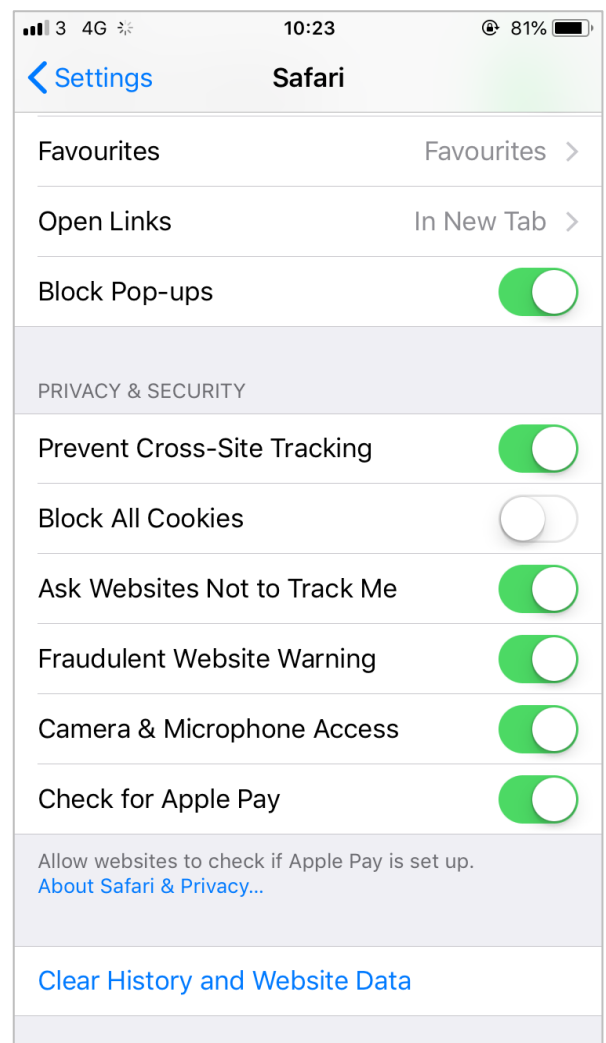
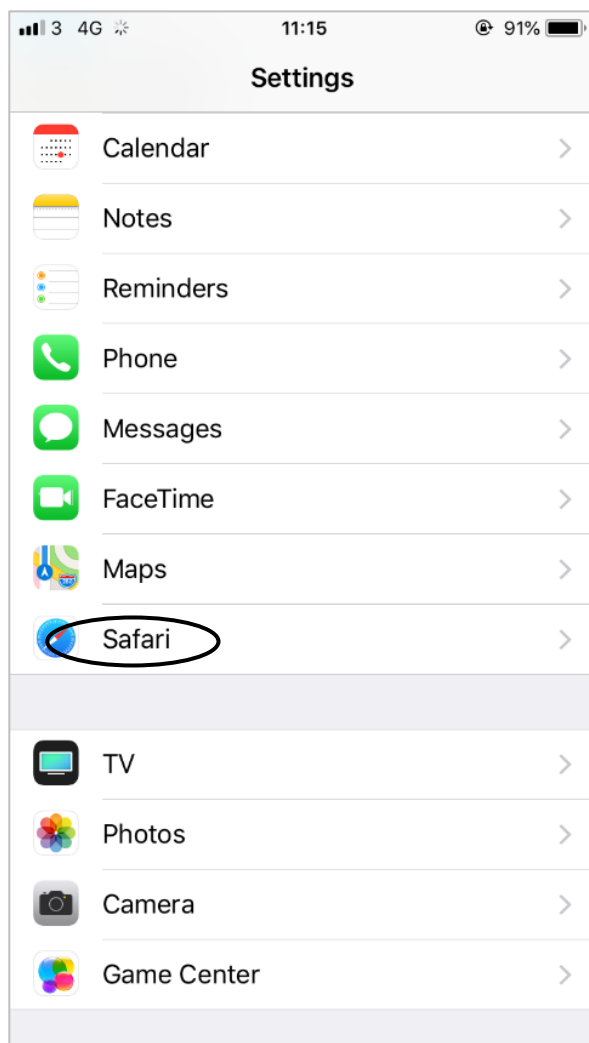


Safari - Settings can be changed to boost your privacy, by doing this you can prevent:

- ✓ **Cross-site tracking** - Some websites use third-party content providers. You can stop third-party content providers from tracking you across websites to advertise products and services.
- ✓ **Block all cookies** - A cookie is a piece of data that a site puts on your device, so it can remember you when you visit again. Turning this on may prevent some websites from working properly.
- ✓ **Ask websites not to track you** - You can also ask individual websites and others who provide those sites with content, including advertisers not to track you.
- ✓ **Get warnings for fraudulent websites** - Scammers use any means they can, fake emails, pop-up ads, text messages, even phone calls to try to trick you into sharing personal information, such as your Apple ID password or credit card information.

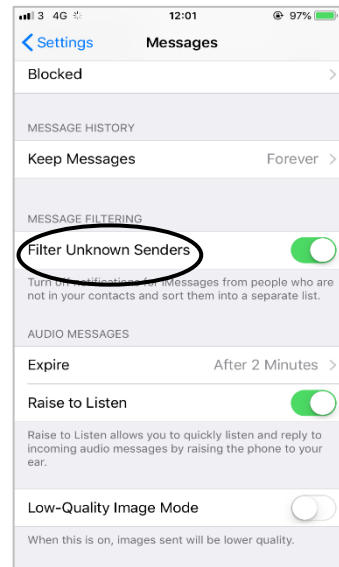
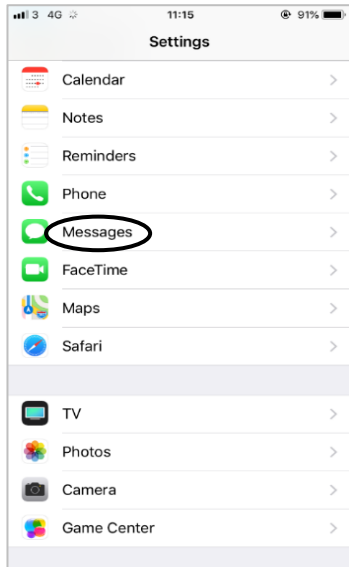
Settings can be changed by:

1. Tap on **Settings**.
2. Scroll down to where it says **Safari**.
3. Swipe the ones that you think need turning on.



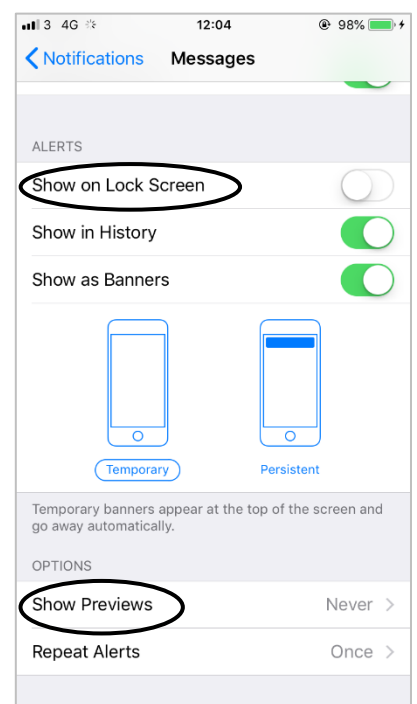
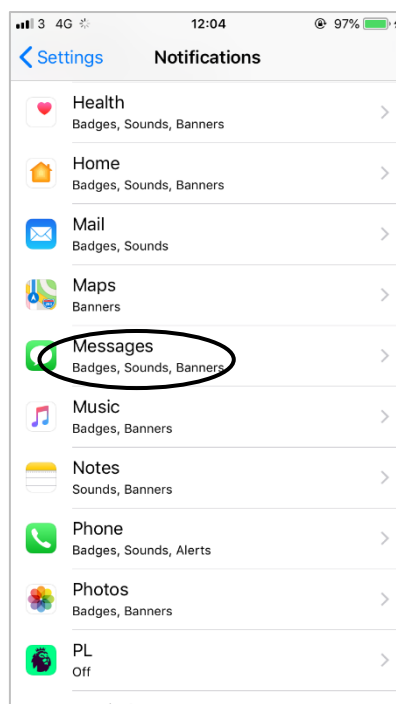
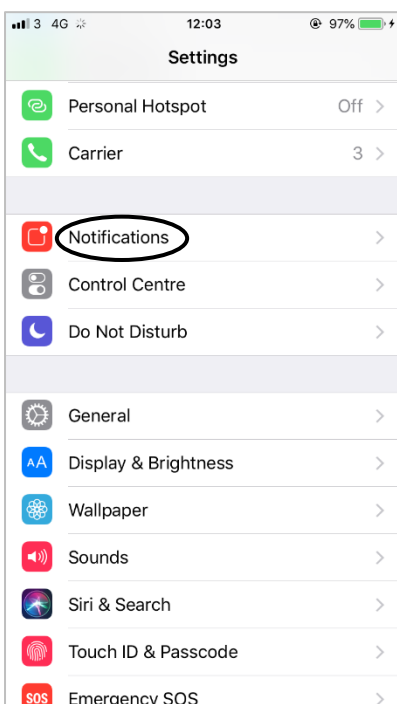
Notifications - Allows you to turn off iMessage notifications for anyone who isn't in your contacts.

1. Tap on **Settings**.
2. Scroll down to **Messages**.
3. Scroll down and tap **'Filter Unknown Senders'**.



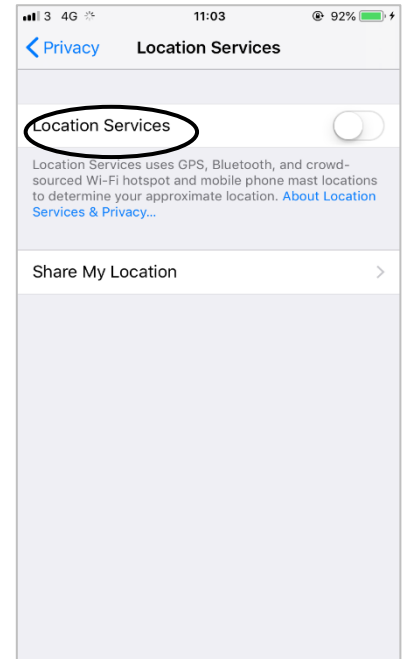
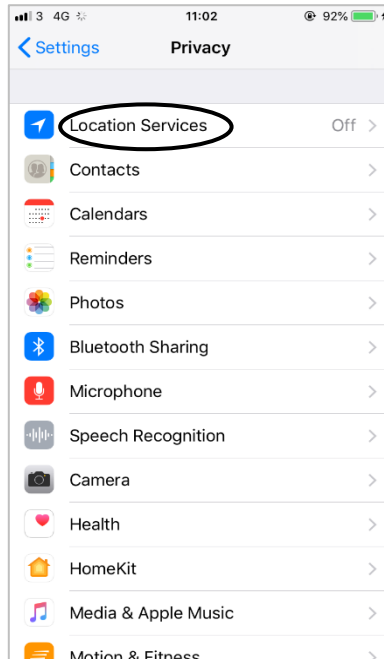
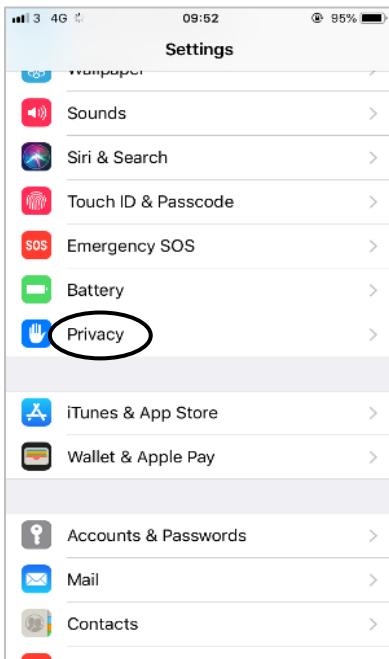
You can also turn off previews, this will stop anyone picking up your iPhone or iPad from having a glimpse at the most recent notifications – even when the device is locked.

1. Tap on **Settings**.
2. Tap on **Notifications**.
3. Tap on **Messages**.
4. Make sure **'Show on Lock Screen'** is **not** turned on.
5. At the bottom, tap on **'Show Previews'** and tap **'Never'**.



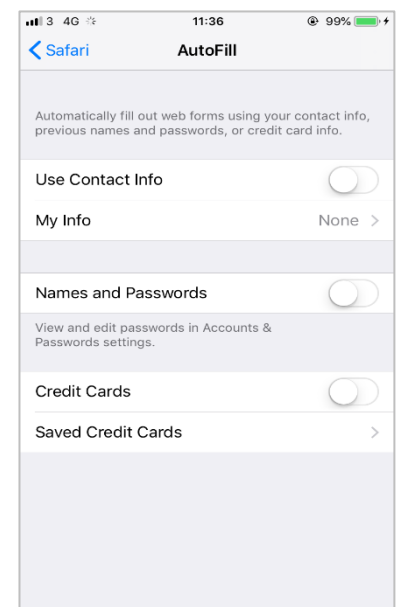
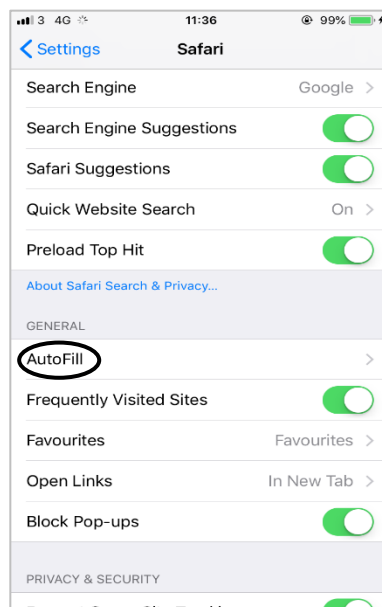
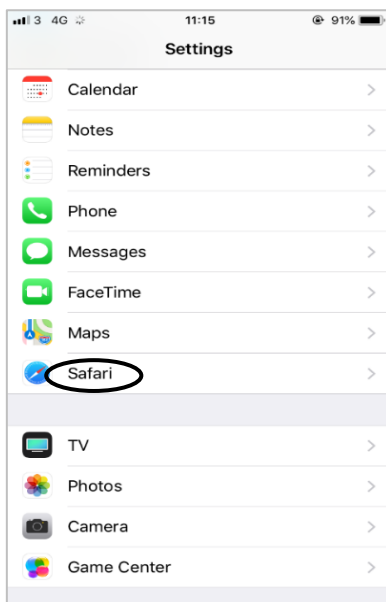
Location Services – Having ‘Location Services’ turned on means your phone, internet or apps can track where you are. You can disable this by turning your ‘Location Services’ off.

1. Tap on **Settings**.
2. Tap on **Privacy**
3. Tap on **Location Services** and ensure it is **off**.



Autofill – Your iPhone can store your personal information for AutoFill. AutoFill makes it easier when filling out forms or logging in to an account. It can also make it very easy for a thief to access your data and accounts if you phone gets stolen.

1. Tap on **Settings**.
2. Scroll down to where it says **Safari**.
3. Tap on **AutoFill** and turn **off** those settings that you think may protect your data.

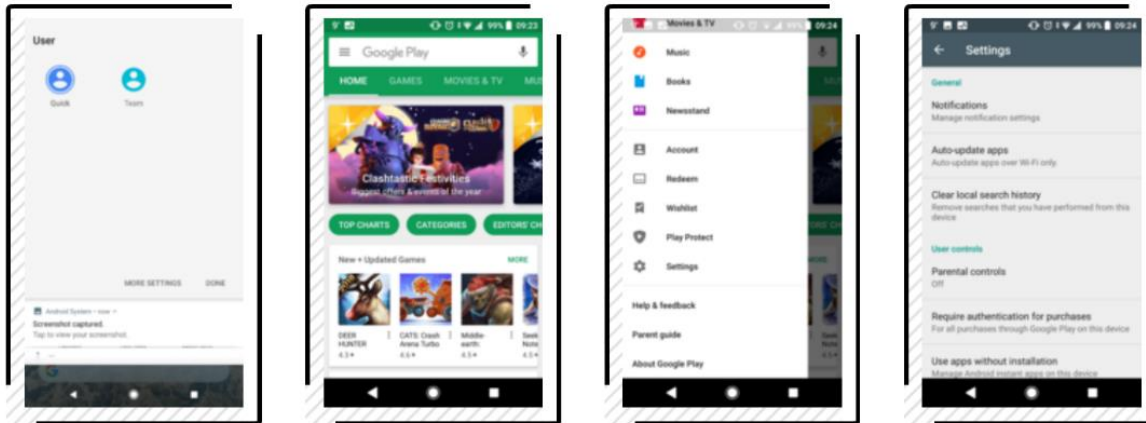


Android – Making your Android phone secure

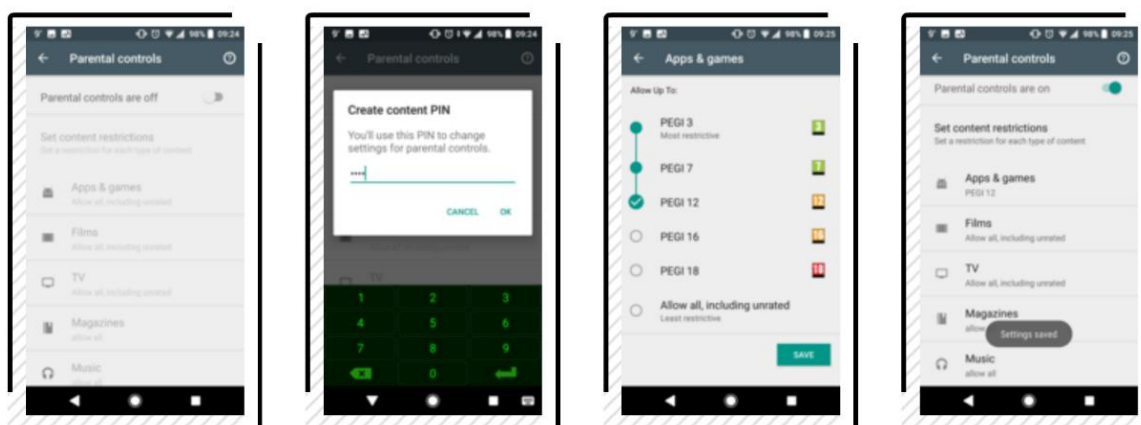
App Store - There are things you can do to make sure your App store is secure:

Filter content

Choose what content your child can download from the Play Store by setting up parental controls in their user account.



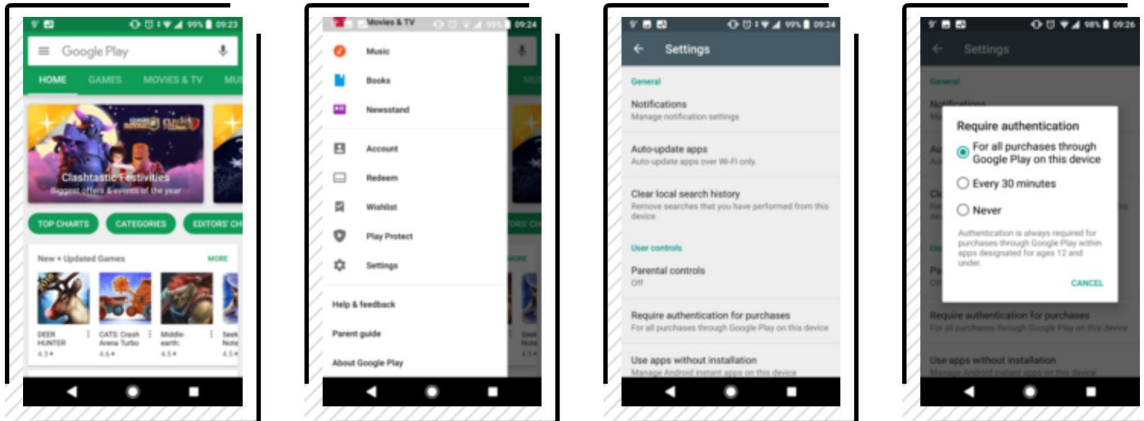
1. Swipe down from the top of the screen and tap **User**, then tap the child's account.
2. Open the **Play Store**.
3. Tap **Menu > Settings**.
4. Tap **Parental controls**.



5. Tap the switch to turn parental controls on.
6. Type a PIN then tap **OK**, type it again and tap **Continue**. That'll stop your settings from being changed, keeping the Play Store age-appropriate.
7. Tap a content type to set an age rating for it.
8. Some content types have a tick box to restrict what can be seen.

Prevent purchases

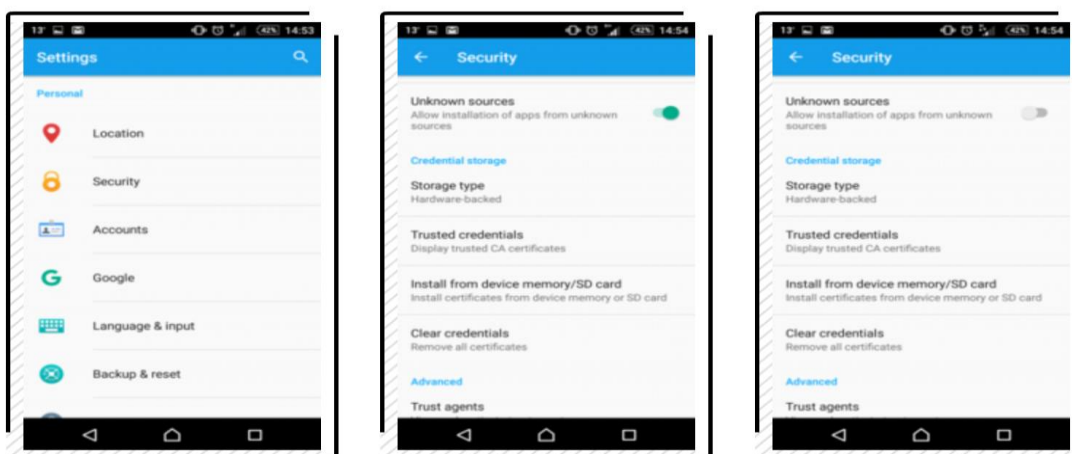
Change the Play Store security settings in your user account to stop users buying 'in-app' content or 'paid-for' apps.



1. Open the Play Store app.
2. Tap the **Menu** icon (three lines in the search box) then tap **Settings**.
3. Tap **Require authentication for purchases**.
4. Tap **For all purchases...** will instruct you to type your Google password every time you want to buy something.

Disable third-party apps

Apps can be downloaded from other places as well as the Play Store. This setting is off by default, but check to make sure.



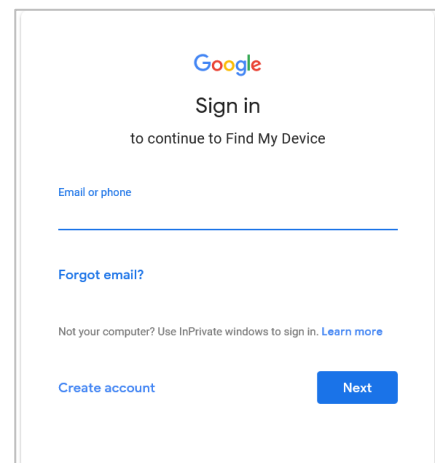
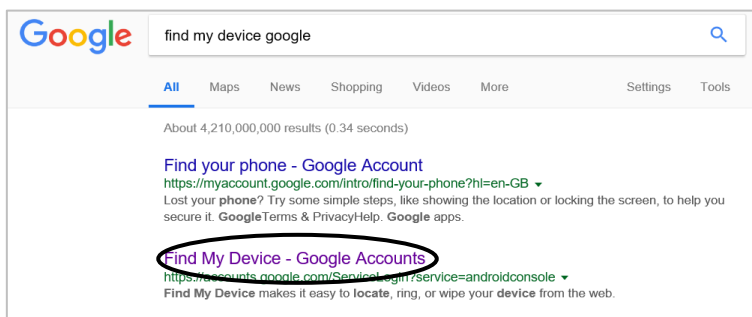
1. Tap **Apps > Settings**.
2. Tap **Security**.
3. The unknown sources switch will be blue if it's on. Tap to turn it off if you need to, then tap **Home**.

Change app permissions – How much of your personal information can any individual app access? You can check this by:

1. Open **Settings**.
2. Tap **Apps and Notifications**.
3. Pick an app you want to see or you can hit all to view full list.
4. To **edit** that app's access, tap **Permissions**.

Find your phone – Activating the Android's built in tracking system may help you recover your phone should you lose it.

1. Open **Settings**.
2. Tap **Security and Location**.
3. Tap **Find My Device**.
4. Should you misplace your phone, go on any device and search '**Find my device Google**' on any browser.
5. **Click** on the link highlighted below.
6. Thereafter you will need to log into you **Google account**. Once logged in you will be able to view your handset's location on a map.



Show emergency information – Should someone discover your phone if you've been in an accident, having your key medical information show up on the lock screen could save your life. You can provide details like emergency contacts, allergies and organ donor status.

1. Open **Settings**.
2. Tap **Users and Accounts**.
3. Tap **Emergency Information**.