

FACEBOOK



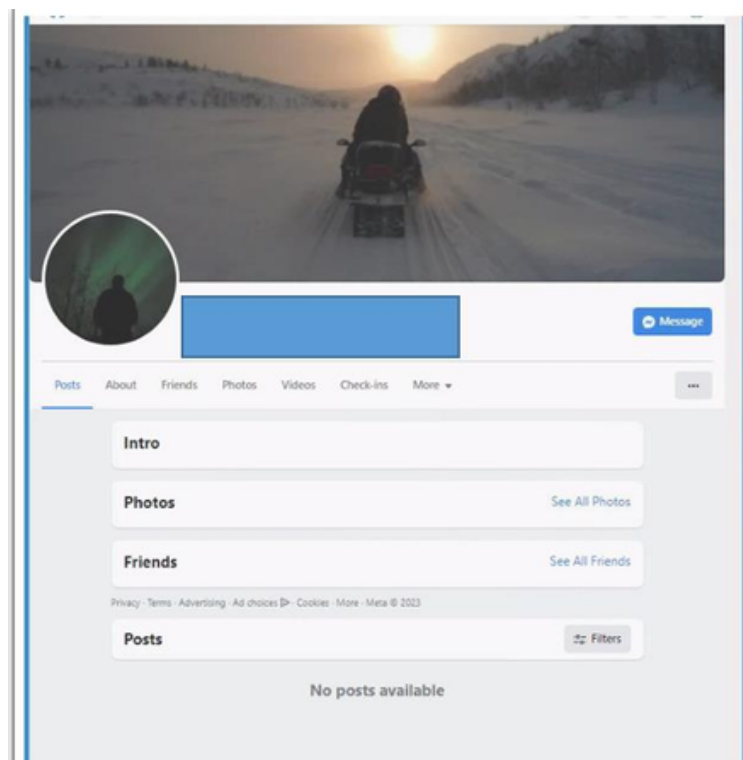
Facebook is first in this guidance for good reason. It is a **phenomenally invasive platform**, and the source of most online data leakage. Facebook's business model is to **sell every piece of data** it can obtain from the information you willingly provide.

If you do have security concerns about using Facebook, the best advice you can follow is to **delete your account**, or at least deactivate it for a relevant period. If you are unwilling to do so, **the following steps will assist in limiting the information you provide** to a select, pre-chosen audience.

Steps to tightening security and privacy on Facebook

1.

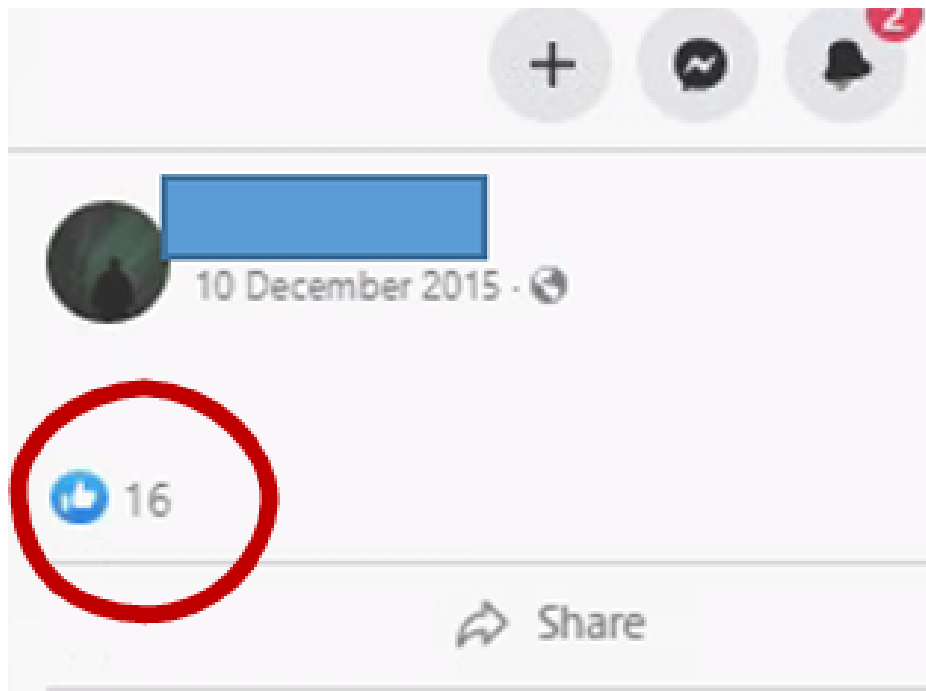
To begin, it is important that profile pictures **do not contain personal information** and do not give away anything about you, such as where you live, your family etc., for example:



FACEBOOK



...However, even this is **not perfect** because, upon clicking on the large banner image, someone can see **that 16 people have liked it**



Therefore, even though the account owner **has hidden their friends list**, 16 of the account holder's friends can still be **discovered indirectly**. If any have the same **surname**, they are potentially a **relative**, and if that **relative's privacy settings** are open, their profile may show images of the original account holder, their family, their home etc.

The knock-on effect **weakens the privacy settings** of the original account holder and reveals information they had intended on keeping private. It is scenarios like this that some **criminals will actively seek to exploit**.

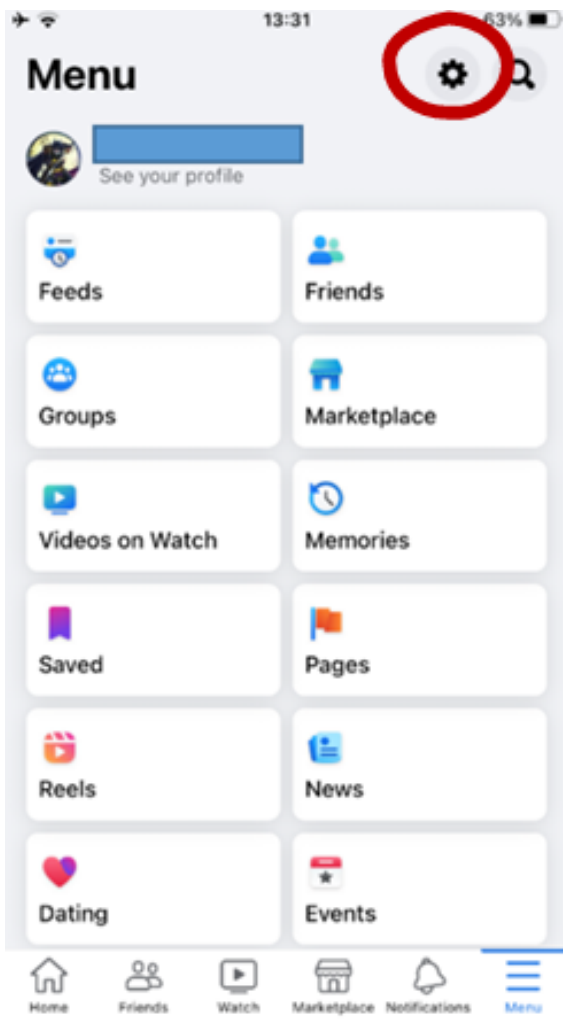
A security system is only as strong as the weakest link.

FACEBOOK

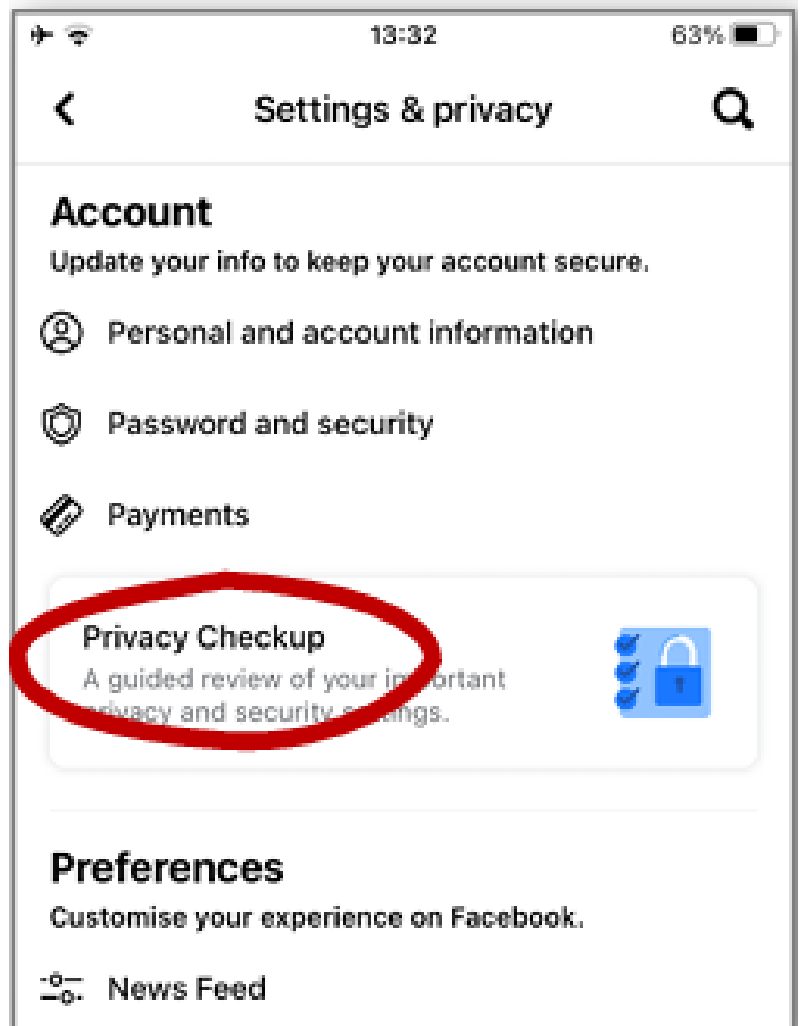


2.

Go to the menu and find the '**Settings and Privacy**' section. This may be the cog that is top-right on the below image, or it may be a separate setting at the bottom of this page **depending on the version** of your phone:



Navigate to the **Settings & Privacy** menu and select **Privacy Check-up**

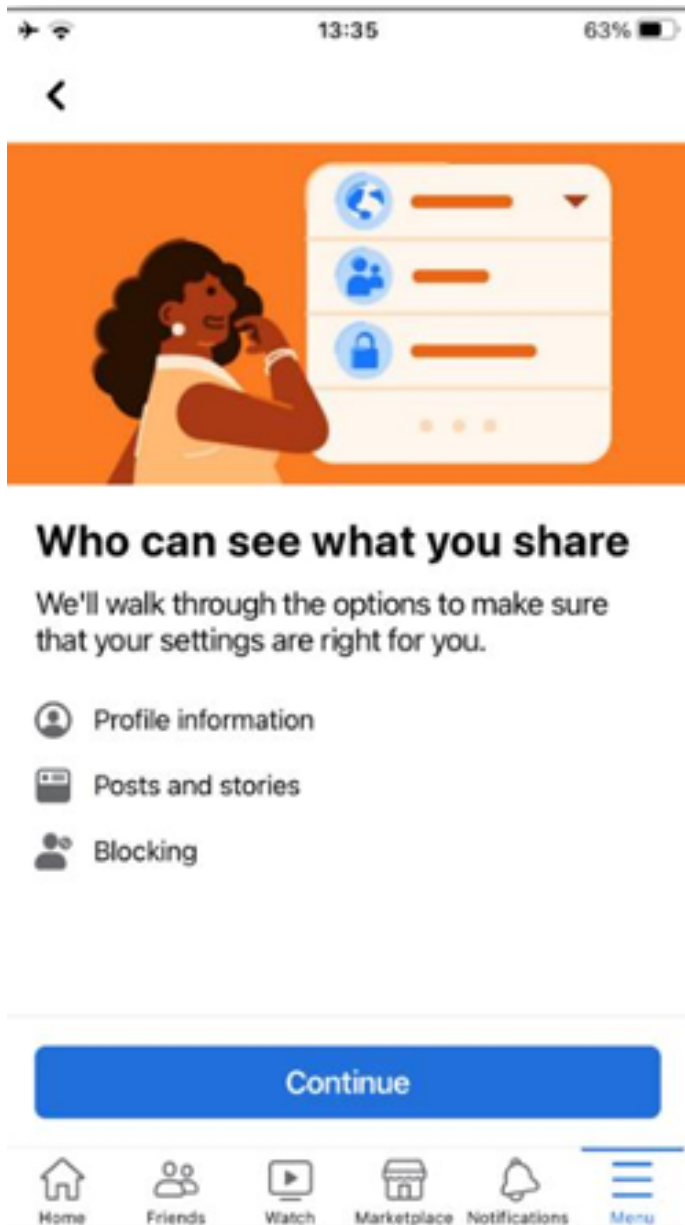


FACEBOOK

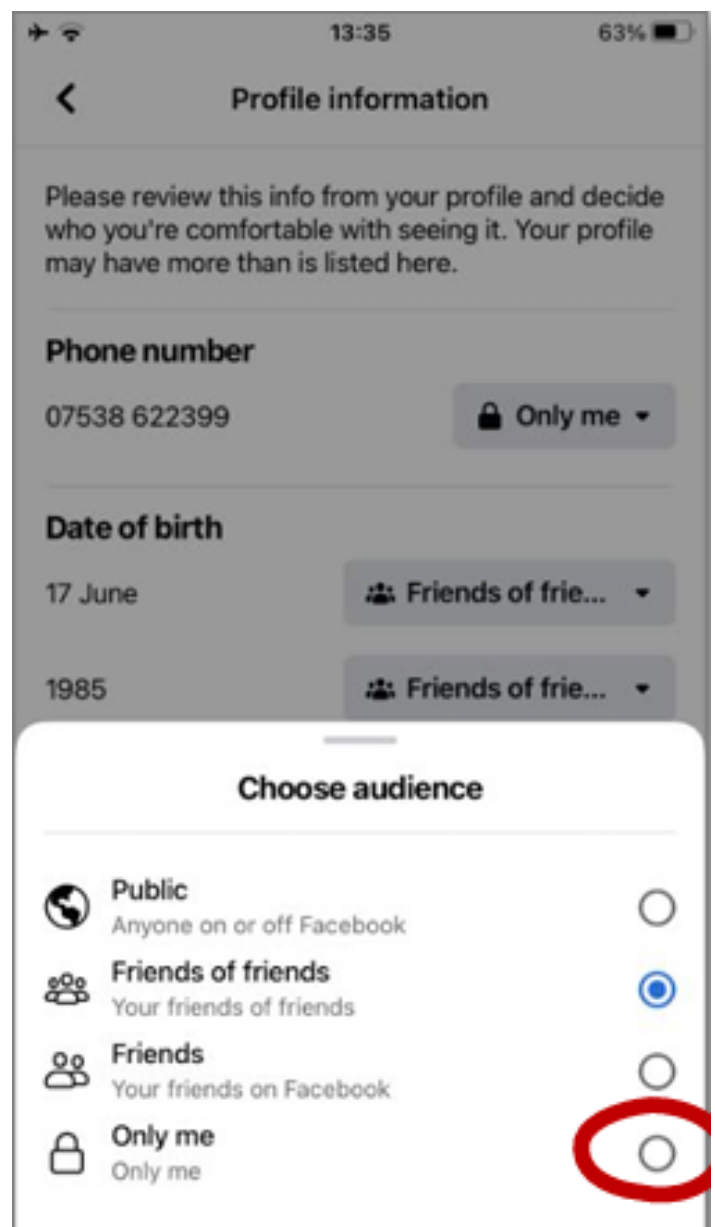


3.

Start with “Who can see what you share”



There are several options in here, and they determine **who can see your personal information** based on whether they are ‘friends’ or not.



Set every option to **Only Me, or Friends at worst**. Complete this and press the **Next** button.

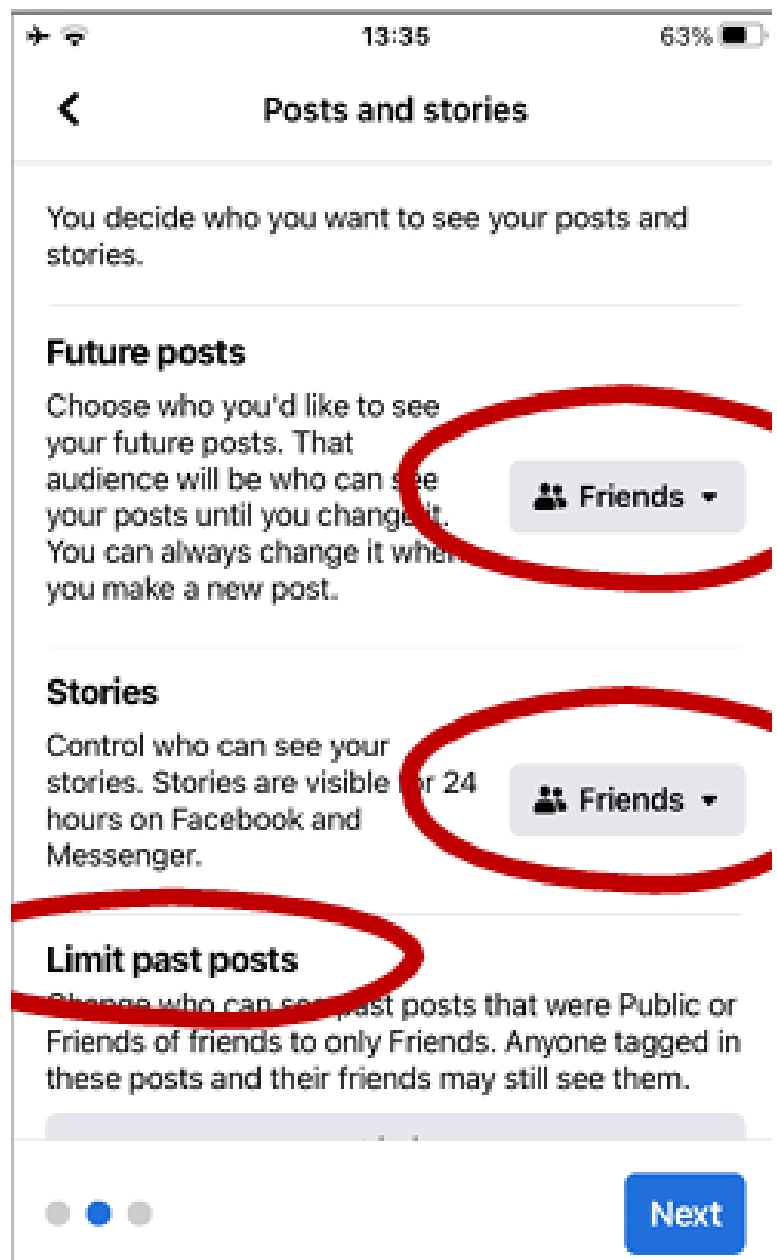
FACEBOOK



These settings are very important as it **closes your timeline from future posts** and can remove **historic unwanted** posts.

Ensure these are set to **Friends only**. At the bottom of the screen (just off the above screenshot) you'll see an option to **limit past posts**. Ignore any warnings from Facebook and **complete this**.

Then press the Next button. The final option is to **block people**, should this be required.



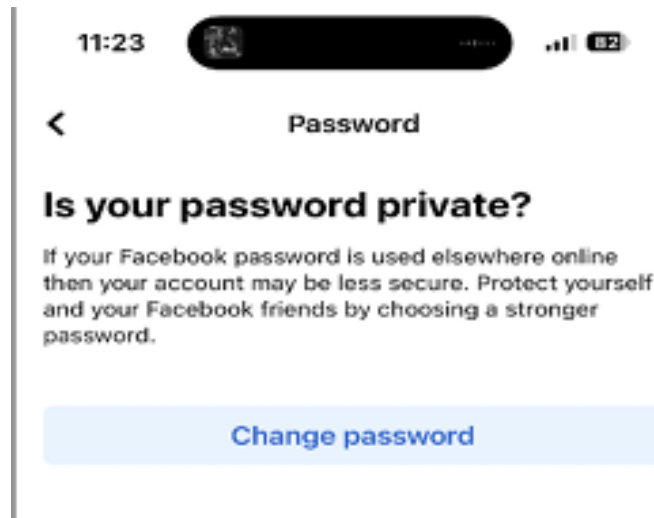
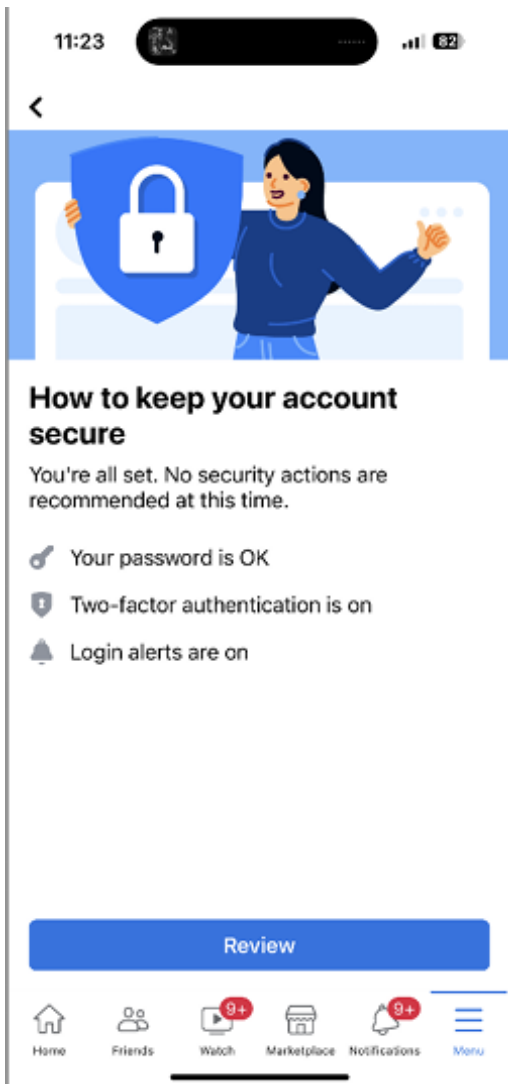
FACEBOOK



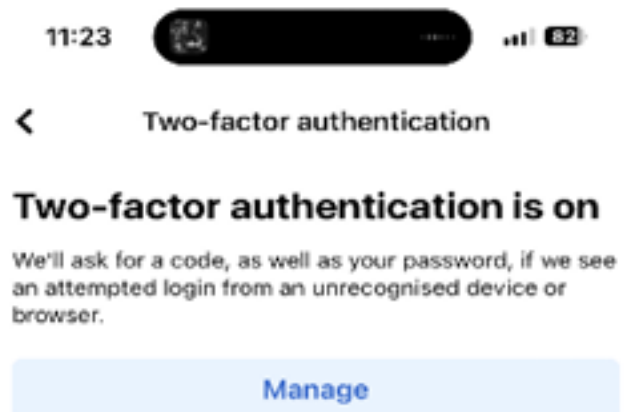
4

Now go to “How to keep your password secure”

Start with your password. **Make it unique** to Facebook only.

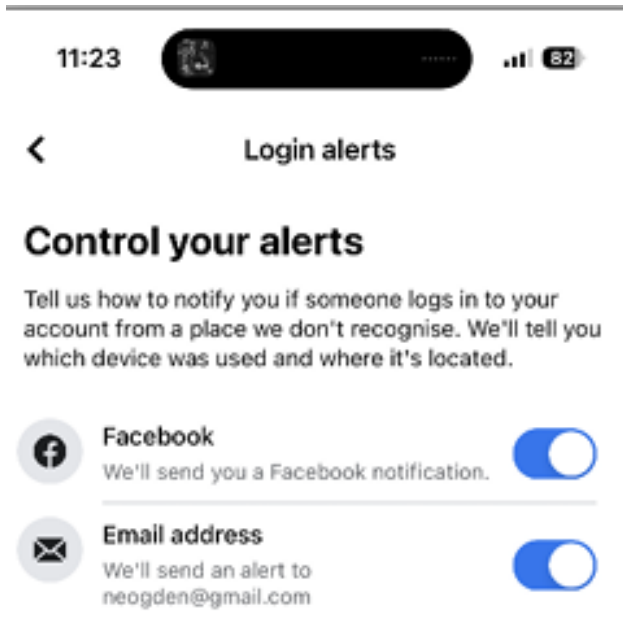


You should of course do this with every online **account you have** to limit the impact, should one company suffer a **data breach**; hackers cannot use your details on every site you use.



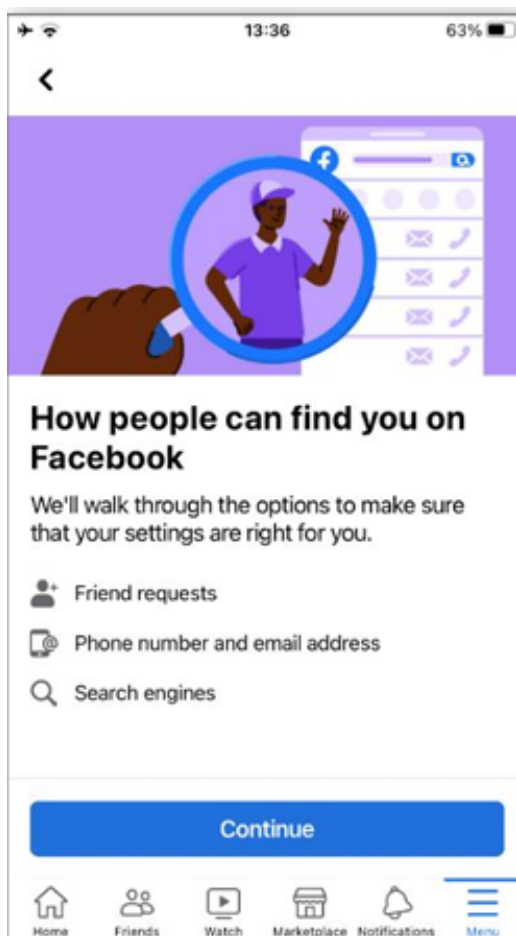
Next, turn on **two-factor authentication**. This means that no-one can access your account on a new device without **inputting a code** sent to your primary mobile. This isn't infallible as these texts can be faked, but it would have to be an extremely sophisticated attack to attempt this.

FACEBOOK



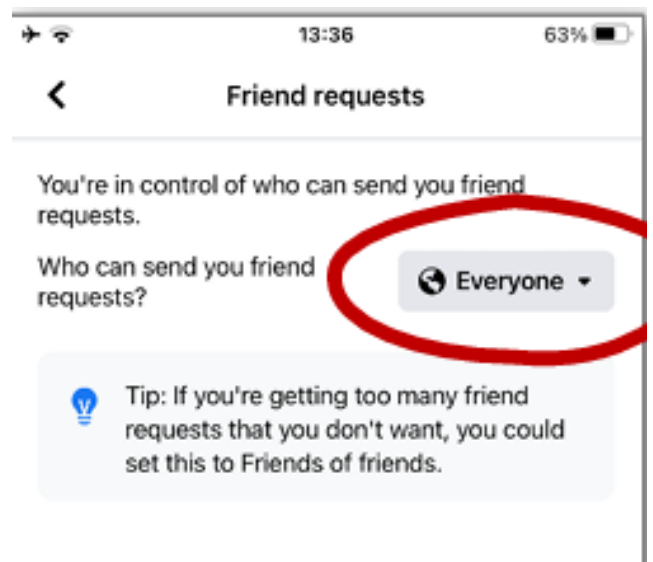
Finally, make sure you have alerts on, should **someone log-in from somewhere** that Facebook does not recognise.

5.



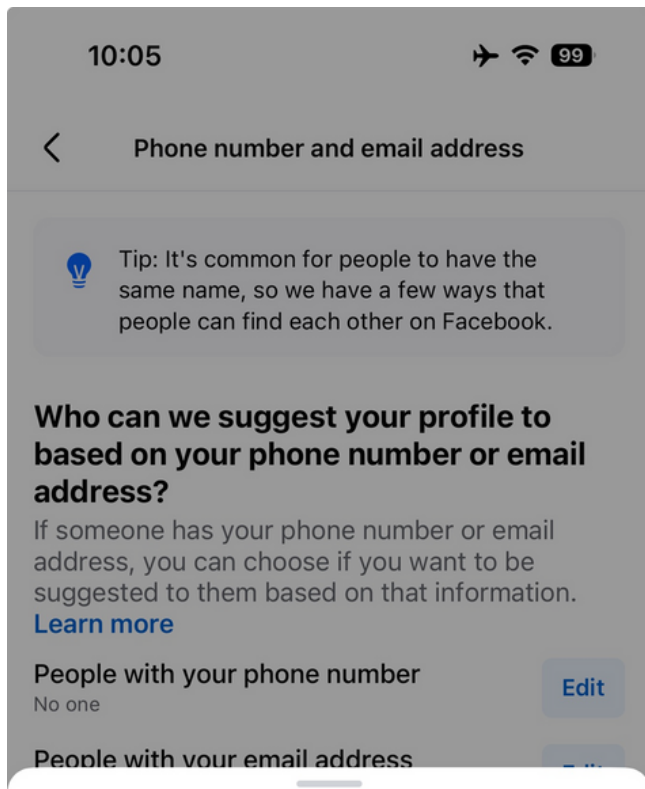
Next, we have “**how people can find you on Facebook**”

Your first option relates to who can send you friend requests; **change it to Friends of friends**, which will provide some protection.



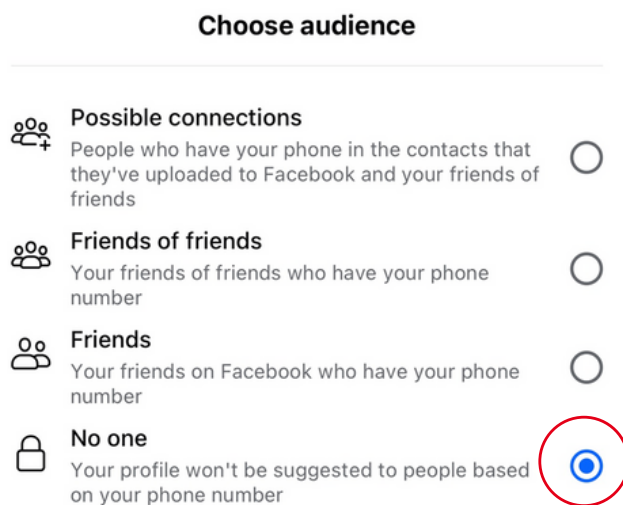
Complete this and press the **Next button**

FACEBOOK

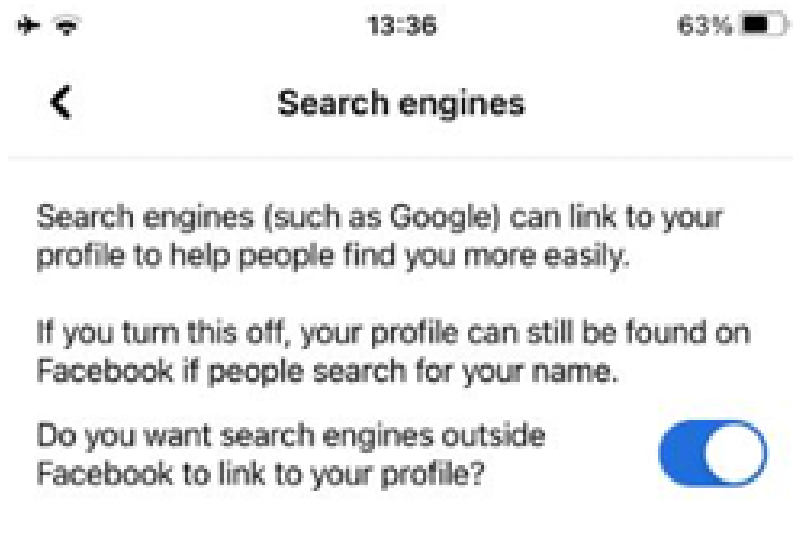


The next option potentially lets someone **identify your account via your email address and / or phone number**. Change this to Only me.

Complete this and press the **Next button**.



Turn off the search engine capability.

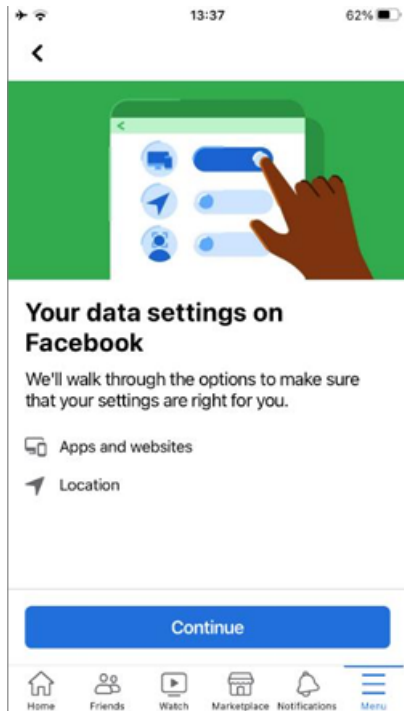


FACEBOOK

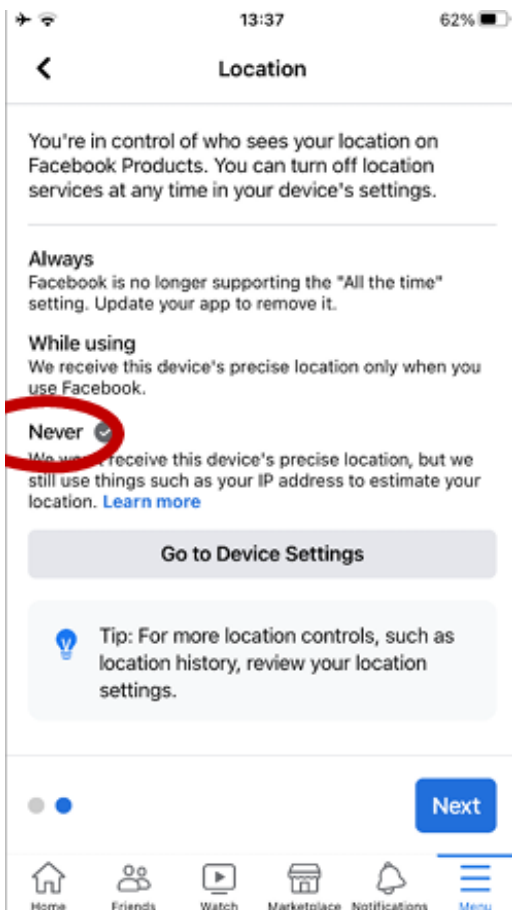
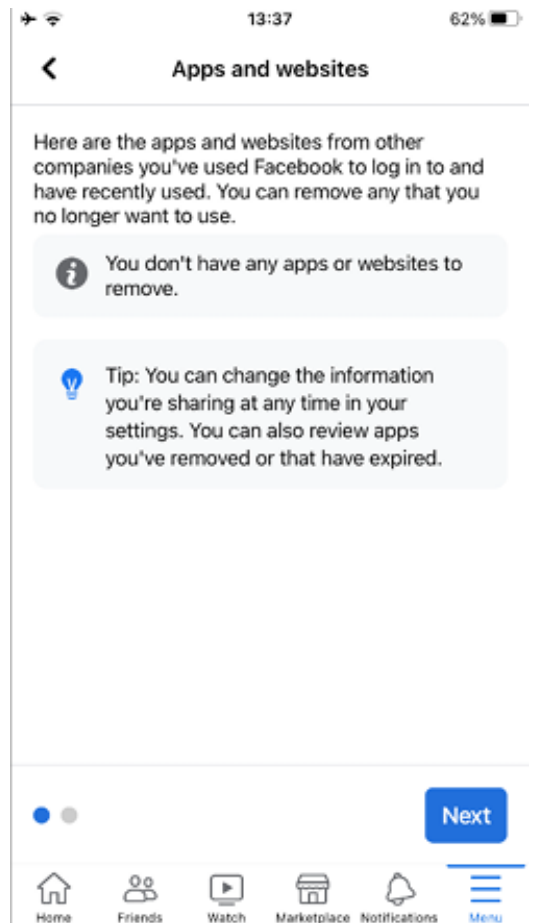


6.

Next, we have “Your data settings on Facebook”



Remove any app that **can access your data via Facebook**. Your screen should look like the below when you are done:

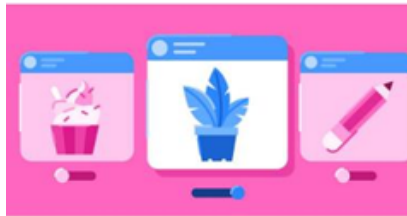


Next, **turn off allowing Facebook to use your location**. This should be set to **Never** but note that this only removes Facebook’s ability to know your **precise location**. It will still have a very good idea of where you are even if you turn this off, **as it can access your IP address**, which is a bit like a virtual postcode.

FACEBOOK



1. Next, we have “Your ad preferences on Facebook”:



Your ad preferences on Facebook

We'll walk you through the options to make sure that your preferences are right for you.

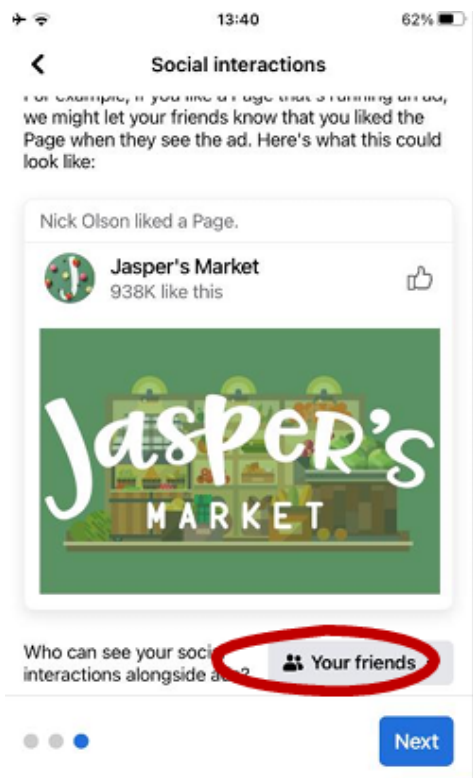
- Learn about ads
- Profile information
- Social interactions

Continue



Turn off every bit of data that Facebook currently shares with other companies, e.g., “Relationship status”, “Employer”, etc.

Finally, change who can see your social interactions alongside ads to only me.



About ads on Facebook

The ads you see on Facebook are personalised based on what we think you're interested in. This is because we want to show you ads that are relevant and useful to you.



For example, if we think that you're interested in sport, we might show you an ad about sport equipment.

To help us figure out which ads you would most likely be interested in, we use information such as what you do on Facebook and other Facebook Company Products, such as Instagram.

We may also consider what you do off Facebook, such as on non-Facebook websites or apps.

Relationship status

Unspecified



Next

Employer



Job title



Education

