Facebook Privacy for Parents & Kids

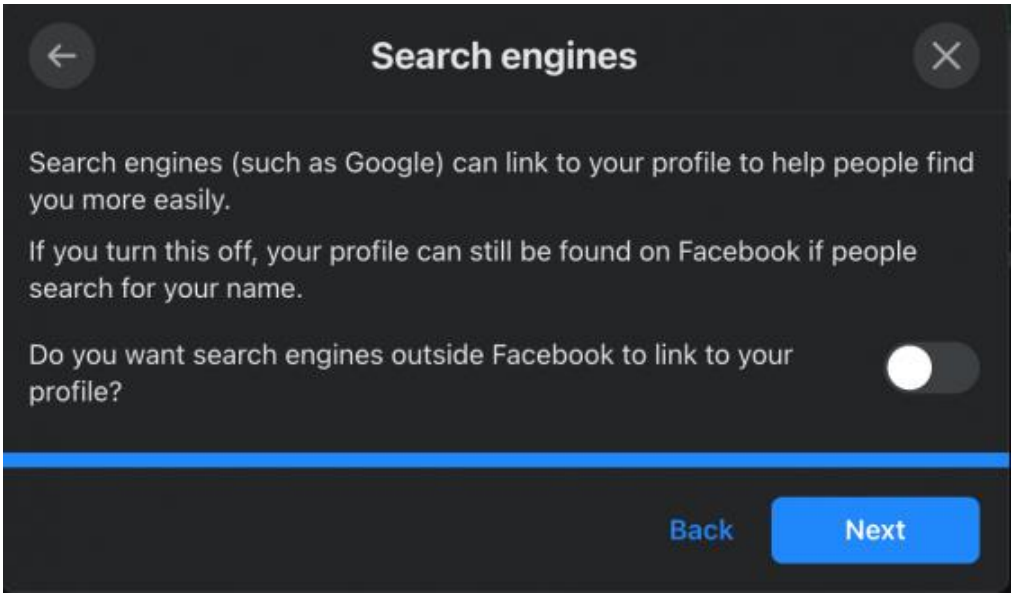
So your kid has setup a Facebook account, there are plenty of hidden dangers IRT privacy and security and this guide will go through some of the important tips to help you as parents & your kids to understand what these are and what they influence.

Account Search

Accounts generally can be searched by email, phone number, name and Google even has an integration setting where others can search on google websearch for a facebook email, name and it will appear if the setting is left on.

1. Select the top right of Facebook.
2. Select Settings & privacy
3. Choose Privacy
4. Choose who can find you on Facebook, this is good to have Phone Number as only me & Email Address as Only Friends.

It is also good to turn off the setting in Search Engines on how they can find you:



Web Data Tracking

Facebook often collects data from any website searched on your childs device & app used, this is often used to personalize the experience by providing targeted advertisements on Facebook based off what they have searched or used. To help stop this data collection the below steps will help:

1. Select the top right of Facebook.
2. Select Settings & privacy
3. Select Privacy Shortcuts
4. In Your Facebook Information, select View or Clear your off-Facebook activity
5. Select Clear History.
6. Turn off Manage Future Activity

Personal Information

There are settings to help limit what information such as DOB, phone number, posts and stories that can be seen on your childs Facebook. This can be found in Profile Information and can be set for each one as Only me, Friends or Everyone. Discuss with them the implications of this information public and even to friends where the information may not be required.

Location Data

Leaving location data on means Facebook can collect data about your location generally at any time when the app is running or not. This is often for targeted advertising services within the region your child may be in.

The best method to stop this from occurring is going in on the mobile phone device itself and within the relevant settings, privacy, location service and turning this setting to only while using the app or never/deny.

Facial Recognition

This is one of those often sneaky ones in the background left on, while Facebook claims not to sell any Facial recognition data and claim it is for helping identify fake accounts, tagging friends & the likes. The risk with biometric data may seem low however with advancements in technology it starts to gain risks while currently there is also no use for it to be left on.

This can be easily turned off by:

1. Select the top right of Facebook
2. Select Settings & privacy
3. Select Privacy Shortcuts
4. Under Privacy, select Control Face Recognition
5. Select Edit & choose No

Two Factor Authentication

This is to help ensure account security and provides another factor to prevent their account from being hacked into. When turned on this will send a code to your childs phone &/or authenticator app on phone each time they try to login to facebook. This can be easily done by:

1. Select at the top right of Facebook.
2. Select Settings & privacy
3. Select Security & Login
4. Select Set-up two-factor authentication and choose the method that works for your child.

There are also many applications out their which can help in monitoring usage, blocking content on the mobile and apps such as when it picks up pornography, illegal substances or content with aggressive elements such as hate speech. The right mix is to ensure your children know about all these cyber security practices, talk to them and help educate them and if further support is required such as apps that monitor usage and support to prevent content adopt this in however generally education and understanding how it can affect them, their family & friends if they don't practice correct cyber security is the best practice.