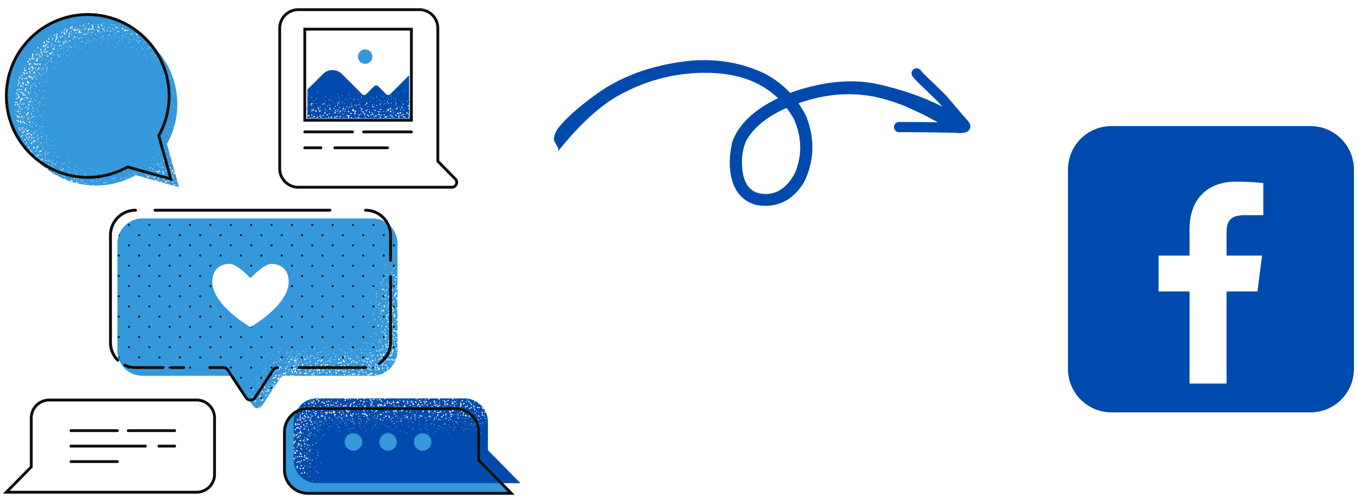
FOLLOW THESE STEPS TO BE CYBER-SAFE WITH FB

1. Clear your history using ‘Off-Facebook Activity’

Why?

Facebook is constantly keeping tabs on your activity, whether that is on or off its site.

Apps and websites automatically check if you’re still logged in and report what you’re doing online back to Facebook.



Adjust and even delete what the company knows through a menu called “Off-Facebook Activity.”

2 OPTIONS

Clear History Button

- The Clear History button will disconnect your profile data from your account, which stops Facebook from serving you targeted ads.
- It won’t completely prevent it from gathering analytics reports from other websites, though. You’ll have to log out first to stop that.

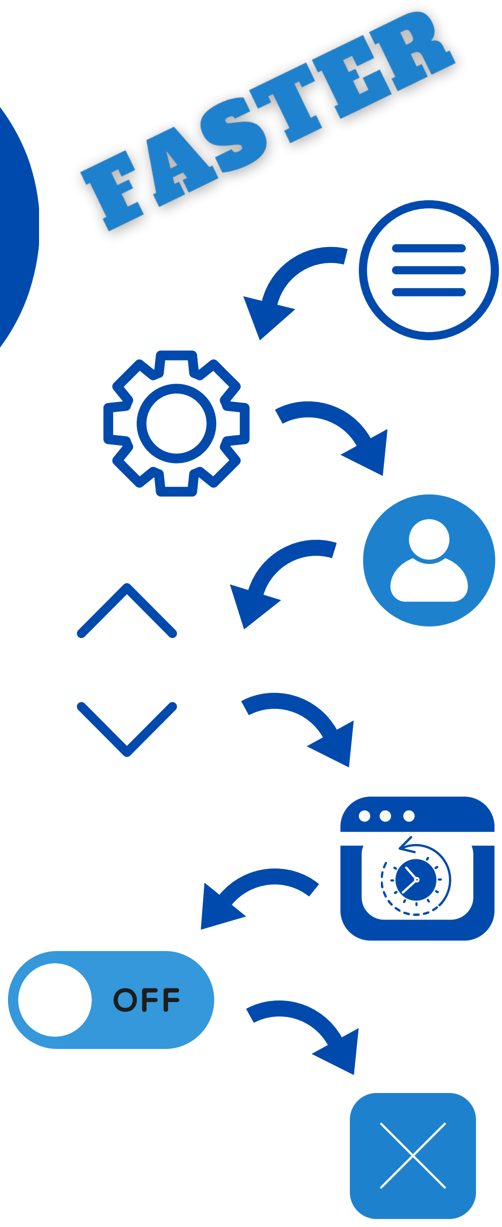
Manage Future Activity

- The Manage Future Activity tool acts as a more permanent version of Clear History.
- When you turn it off, it stops companies from sending Facebook ad-targeting data about you.
- Keep in mind that disabling Future Activity prevents you from signing into other apps and websites with Facebook.

Undertake the following steps

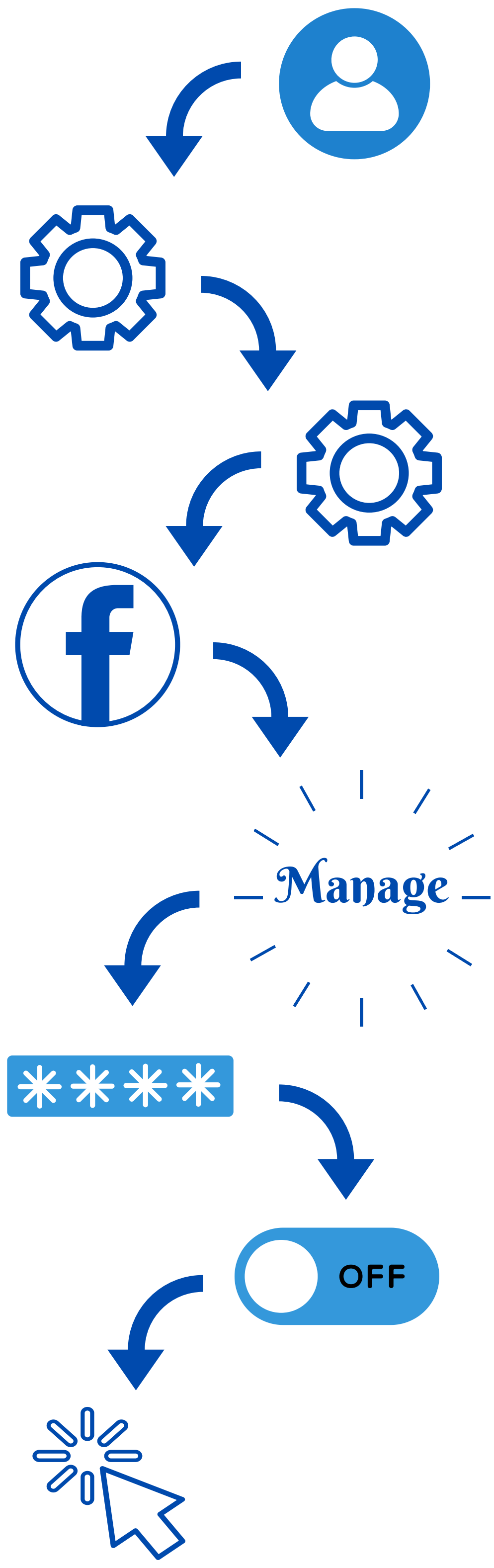
To clear your history on the mobile app:

- Tap the **three-line menu** in the bottom right of the Facebook app and click **Settings & Privacy**.
- Select **Settings**.
- Scroll down and select **Off-Facebook Activity**.
- Examine the apps that use your activity and make sure you want to remove the information.
- Tap **Clear History**.



IF YOU DON'T HAVE THE APP

To clear your history on the Facebook website:



- Click on your profile picture in the top right of the screen of your Facebook and click **Settings & Privacy**.
- Select **Settings**.
- Tap **Your Facebook Information** in the left column.
- Click **Off-Facebook Activity** to review. From here, click **Manage Your Off-Facebook Activity**.
- You'll be asked to answer a few questions and to re-enter your password. Once you're verified, it will show you the apps and sites that have shared ads with your Facebook account.
- When you're ready to clear this information, click **Clear History**.

2. Hide your location

Why?

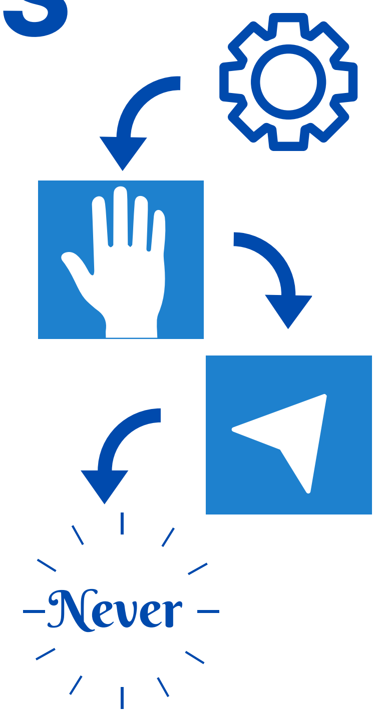
Facebook uses location data to serve you news or sell you things. If you disable location services, it won't use your precise location to target you with ads.

Unfortunately, Facebook still has access to your network location, so you'll need to disable the feature on both your phone and the app.

Undertake the following steps

To disable location services on an iPhone

- Go to the phone's **Settings** and tap **Privacy**.
- Tap **Location Services**, followed by Facebook.
- Tap **'Never'** to disable location services.



To disable location services on an Android phone

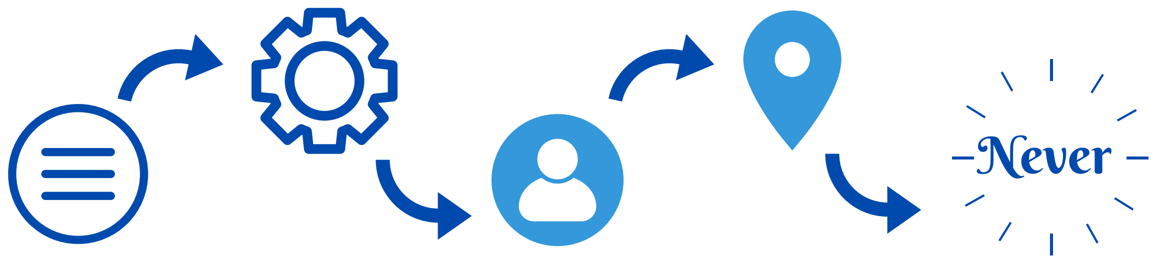
Premission manager
OFF

- Go to the phone's **Settings** and tap **Privacy**.
- Tap **Permissions Manager**, followed by **Location**. Choose **Facebook**.
- Tap **Deny** to disable location services.

To disable location tracking in the FB app

Once you're finished with adjusting your phone's permissions, follow these steps to disable location tracking in the app:

- Tap the icon with the **three lines** in the bottom right.
- Tap **Settings & Privacy**, followed by **Privacy Shortcuts**.
- Tap **Manage Your Location Settings**, followed by **Location Services**.
- Tap Location and select **Never**.



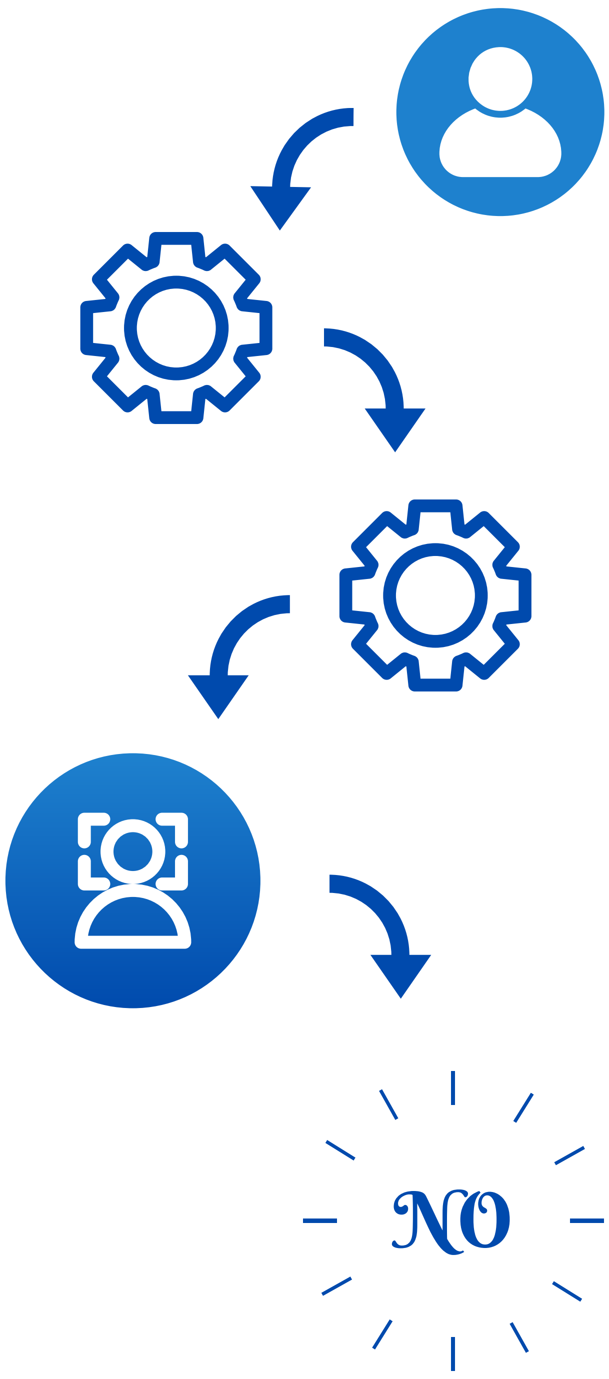
3. Disable Facial Recognition

Why?

You can disable facial recognition on the desktop version of Facebook.

Undertake the following steps

- Click on your profile picture in the top right of the screen.
- Select **Settings & Privacy**, followed by **Settings**.
- In the left column, click **Face Recognition**.
- Tap **"Do you want Facebook to be able to recognize you in photos and videos?"** Select **No** in the drop-down menu to disable the setting.



4. Get rid of apps that track you off Facebook

Why?

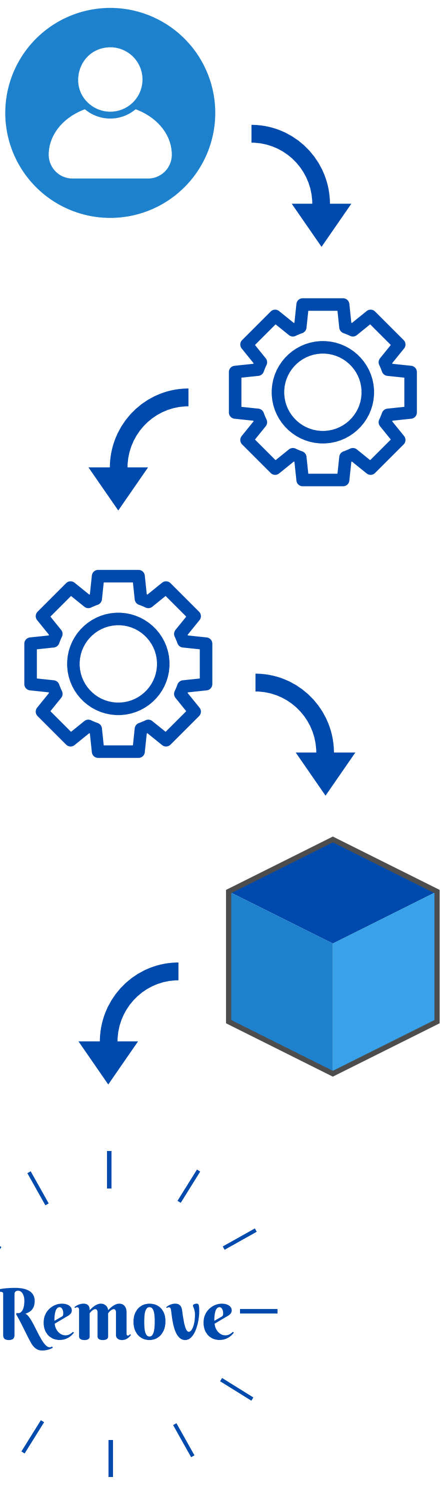
Logging into other platforms or websites with your Facebook username gives those companies access to your data and may permit them to share your activity with Facebook.

Thankfully, Facebook has changed its stance on third-party applications and lets users disable all that tracking.

Undertake the following steps

Disable third-party app tracking from your desktop:

- Click on your profile picture in the top right of the screen.
- Select **Settings & Privacy**, followed by **Settings**.
- Tap **Apps and Websites** on the left menu.
- Select **Active**.
- Click on the box next to the app's name to stop tracking you and click **Remove**. This will disable it from tracking you.



5. Enable two-factor authentication to lock out hackers

Why?

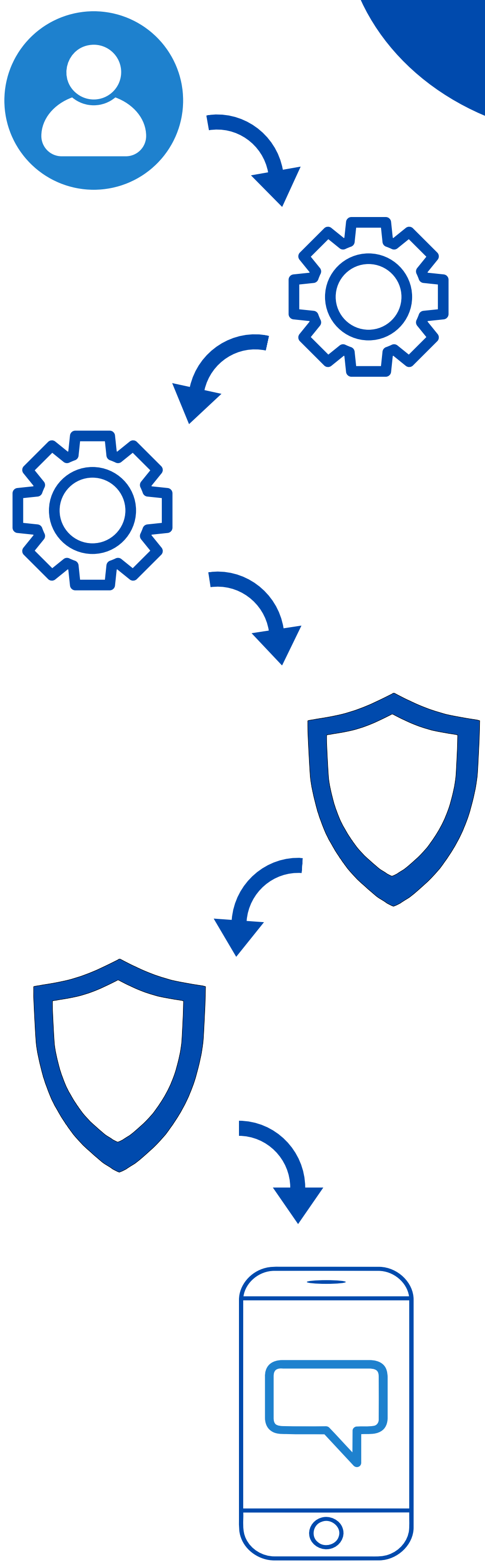
Two-factor authentication is one of the most robust ways to secure your profile from unwanted logins.

When someone tries to break into an account with 2FA enabled, they can't get in without a text-message code.

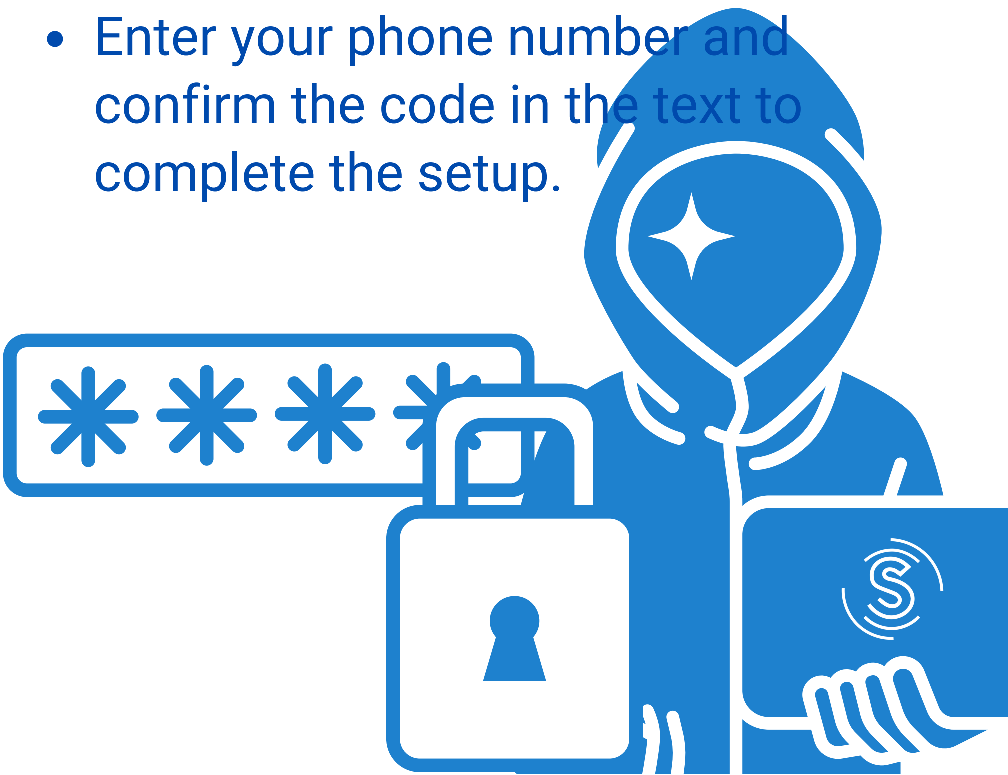
Since the code goes to your phone, only you will be able to log in.

Undertake the following steps

Activate 2FA from your desktop



- Click on your profile picture in the top right of the screen.
- Tap **Settings & Privacy**, followed by **Settings**.
- Select **Security and Login**.
- Scroll down to **Two-Factor Authentication** and tap **Use two-factor authentication**.
- Enter your phone number and confirm the code in the text to complete the setup.



6. Stop Google from showing your Facebook account

Did you know your Facebook profile is indexed on Google?

That means anyone looking up your name will be able to find your social media account, along with all the publicly visible data.

If you're not comfortable with this, we don't blame you. Google and people-search engines have a nasty way of making your private life public.

With Facebook, at least, you can keep your profile out of searches.

Why?

Undertake the following steps

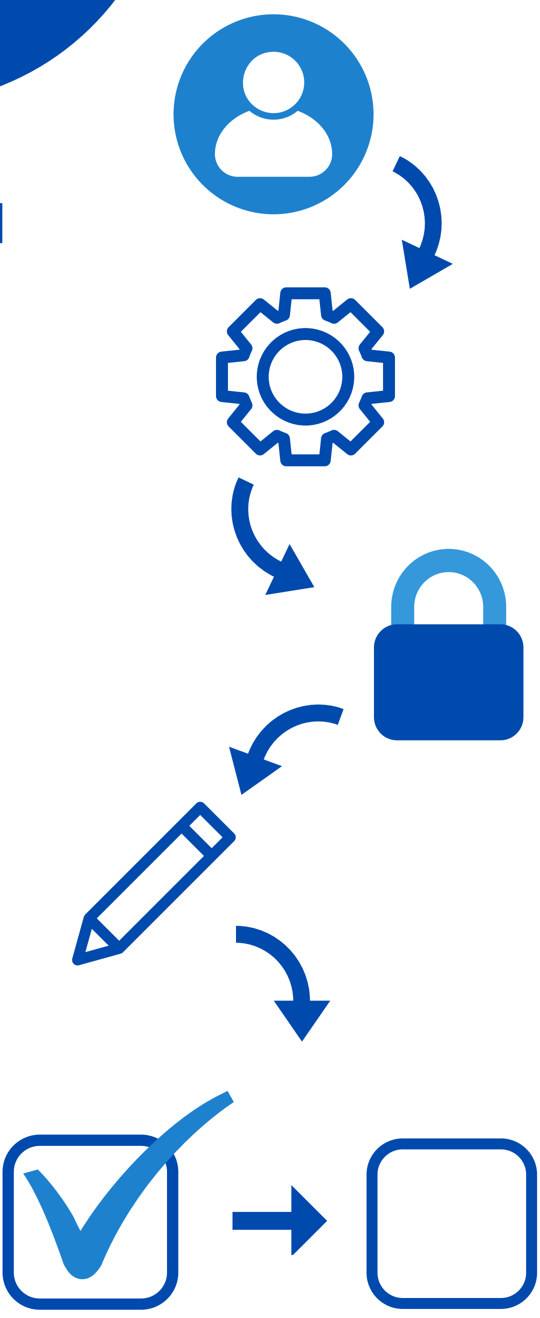
Disable google from showing your Facebook account from your desktop:

- On your computer, open Facebook and Click on your profile picture in the top right of the screen.

- Tap **Settings & Privacy,** then Settings followed by **Privacy**.

- Under **"Do You Want Search Engines Outside of Facebook to Link to Your Profile?"** click **Edit.**

- Click the **checkbox** on the bottom to turn off the setting.



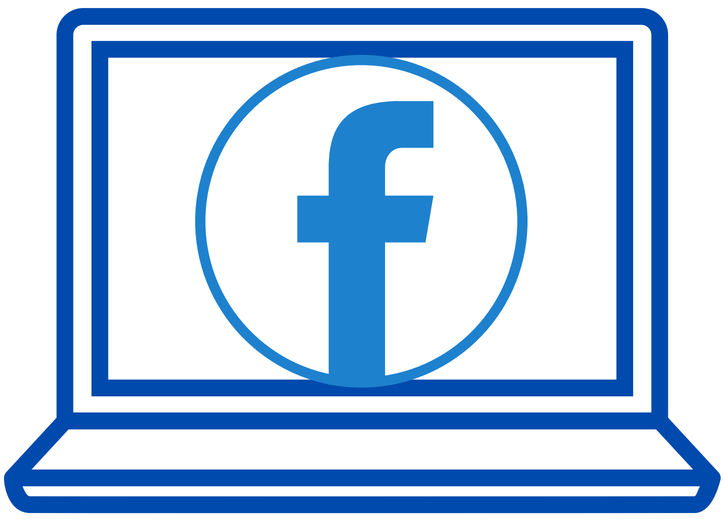
7. Limit the audience for your personal posts

Why?

People accidentally share all kinds of personal facts and information without realizing it.

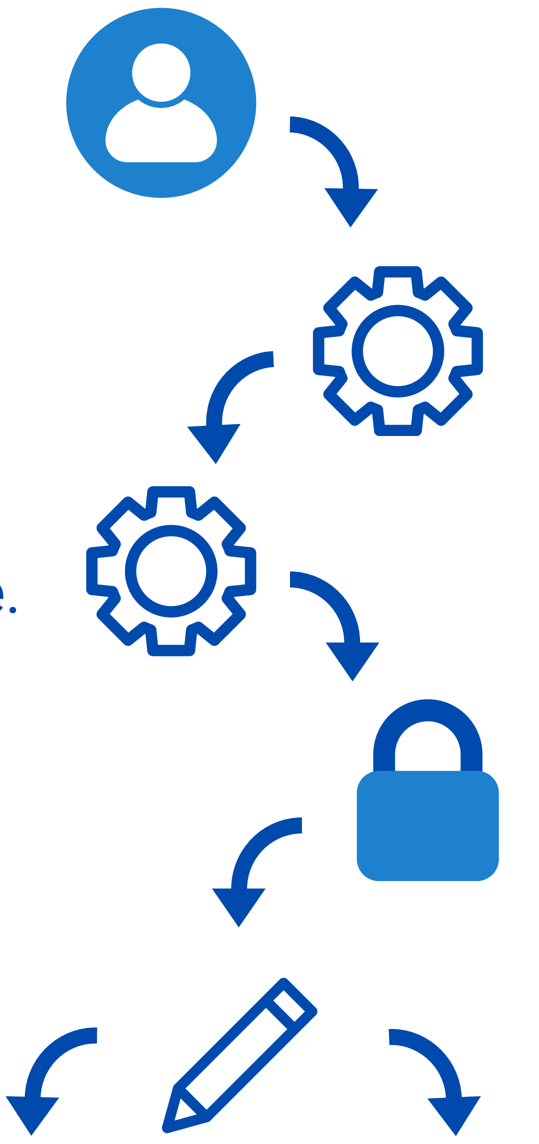
Changing this setting can protect you from getting phished or stop a hacker from correctly guessing one of your security questions.

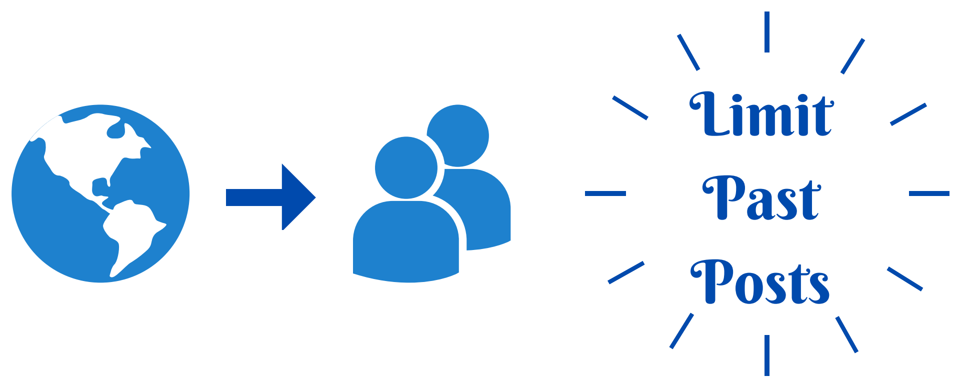
Undertake the following steps



From your Desktop

- Open **Settings & Privacy** again, then **Settings** and click on **Privacy**.
- Scroll down to (your activities) **Who can see your future posts?** and click **Edit**. You can adjust the settings for specific audiences here.
- Scroll down to **Limit Past Posts** to change who can access your previous content.





8. Stop your activity from being advertised (literally)

Why?

Ever seen an advertisement that tells you which of your friends Liked it?

That's because Facebook automatically uses these endorsements to target ads to you and your friends. And if you Like something, your friends will see the same kind of ads.

Of course, they're not asking your permission. But you can disable the setting to keep your interests and Likes more private.

Undertake the following steps

Disable from your desktop:

- Under **Settings & Privacy**, select **Settings**, then click **Ads**, followed by **Ad Settings**.
- Click **Social Interactions** and select **Only Me**.

HOW TO BE SAFE WITH FACEBOOK RECAP

8 STEPS TO MAKE YOUR ACCOUNT CYBERSAFE

1) CLEAR YOUR HISTORY USING 'OFF-FACEBOOK ACTIVITY'

2) HIDE YOUR LOCATION

3) DISABLE FACIAL RECOGNITION

4) GET RID OF APPS THAT TRACK YOU OFF FACEBOOK

5) ENABLE TWO-FACTOR AUTHENTICATION TO LOCK OUT HACKERS

6) STOP GOOGLE FROM SHOWING YOUR FACEBOOK ACCOUNT

7) LIMIT THE AUDIENCE FOR YOUR PERSONAL POSTS

8) STOP YOUR ACTIVITY FROM BEING ADVERTISED (LITERALLY)

RESOURCES USED: