SOCIAL MEDIA: BEING SMART, STAYING SAFE!

Social media has been a powerful tool for all of our movements. Through social media we have been able to challenge the media blackout on many of our issues as well as rapidly mobilize collaborators across borders and issues. However, social media is not a neutral tool, social networks like Facebook, Twitter, and Instagram may operate like civic public spaces, but in fact these are private self-surveilling corporate platforms with various degrees of collaboration with government surveillance systems.

As a result, many of us are vulnerable because we are unaware how our posts, tweets, and pictures are being used to create an enormous data portfolio for these corporations to use, sell, and share with other corporations and governments. **This is why these platforms are not really free, because we pay for them with our data**.

The question of visibility is something we all have to make our own risk assessments by doing a thorough analysis of the areas of your life that may contain risks if exposed. Many of us began by creating personal accounts on social media, later realizing the political, professional, and personal implications such visibility could have on our lives. A few common sense safeguards will go a long way in avoiding unwanted leaks of personal information or embarrassing reveals that can affect you and the worlds that you may be a part of.

All actions online must be well considered. Filling out a “Profile” or “About me” may seem relatively harmless, it is in fact a moment where you have to decide what information you want to make available, and how that relates to, or affects the work you do. Say for instance, you reveal the city you live in, the broad unknown online public will have information they can use to figure out your physical location. If security settings on your account are not set tightly, you may have made yourself vulnerable. We recommend you make decisions with careful consideration based on what you feel most comfortable with.

Questions to ask yourself:

- Who can access the information I am putting online?
- Who controls and owns the information I put into a social networking site?
- What information about me are my contacts passing on to other people?
- Will my contacts mind if I share information about them with other people?
- Do I trust everyone with whom I am connected?

COMPARTMENTALISATION: PERSONAL VS PROFESSIONAL ACCOUNTS

A piece of sound advice is to maintain two accounts if you feel vulnerable. It's perfectly acceptable to develop separate accounts for personal and professional uses. Many folks open two accounts within the same social media site, one for each purpose. However, be aware that your colleagues could be connected to you via a professional account only but there is still a chance they could find and view your personal account.

Many activists today already maintain a professional and personal Facebook account. This helps the individual to express harder political points of view on Facebook, Instagram, and other platforms without worrying about how their views will affect their job searches and employment. So the first part of this section will speak to this compartmentalization.

PROFESSIONAL

- Links and Resources
- Positions on Academic/Industry Focus
- No Explicit political position

PERSONAL

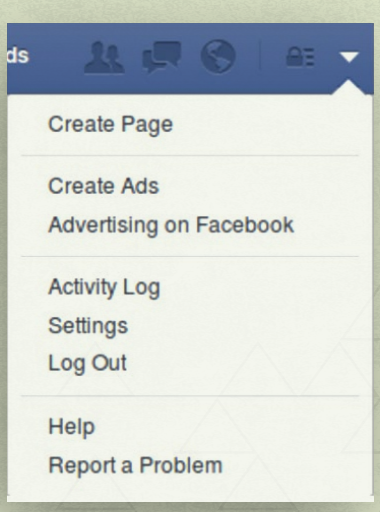
- More political
- More personal
- Understanding these are thoughts in process

FACEBOOK

Here are some ways we can assign settings that make our experiences on Facebook as private and safe as possible.

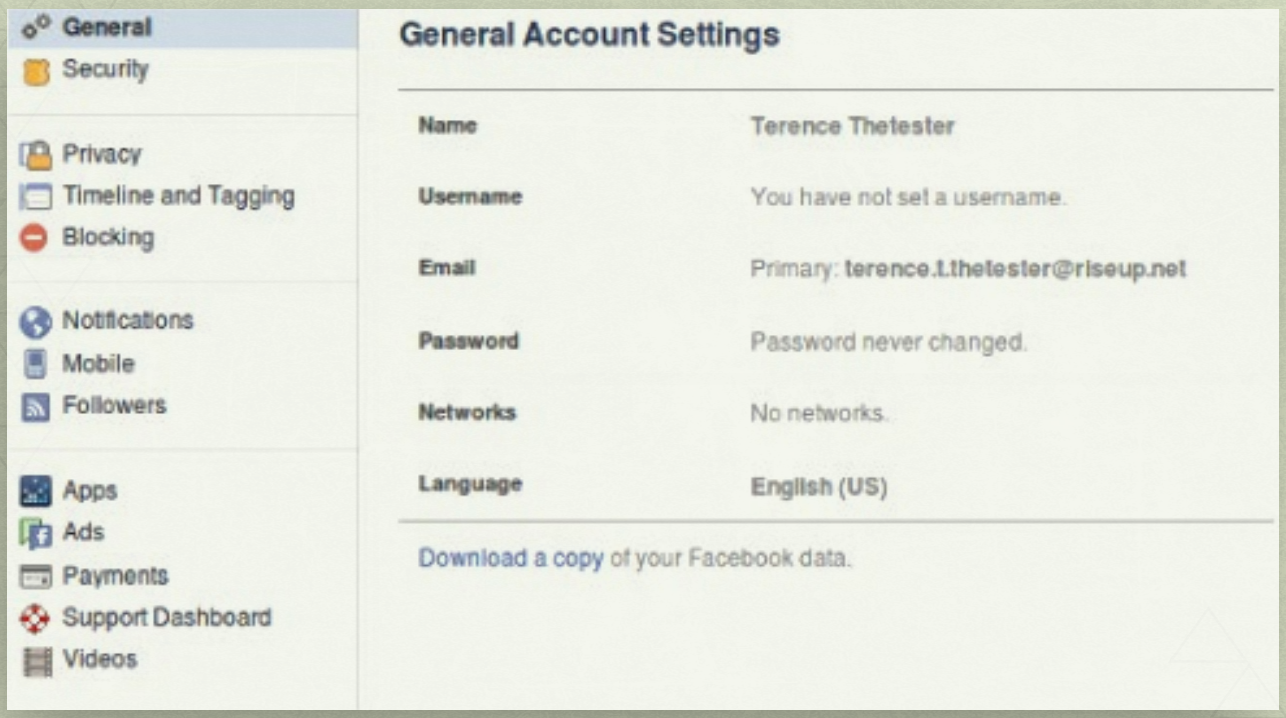
GENERAL SETTINGS AND TOOLS

From your Facebook Home page, click on the small arrow beside Home in the top right-hand corner and select **Settings**.



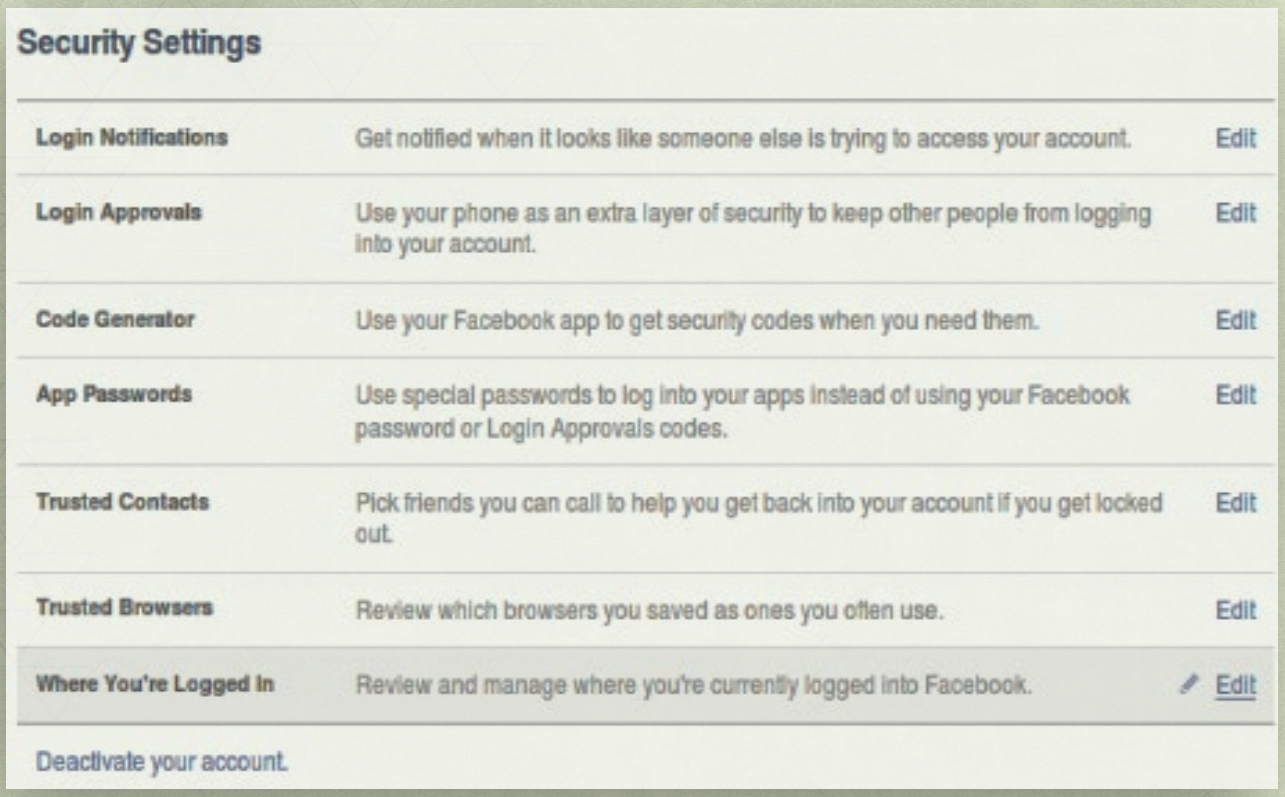
This will take you to the Settings menu. On the left-hand side, you can choose different categories of settings. The first tab is **General Account Settings**, where you can edit information about your name, username, email, password, networks, and language.

You should update your password regularly, preferably at least once every three months. Remember, it is extremely important that you choose a strong password to protect your account and your information.



SECURITY SETTINGS

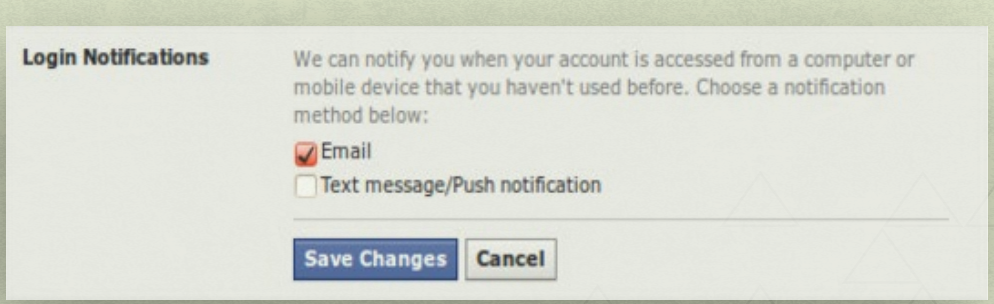
Click on Security in the menu on the left hand side. This will open the Security Settings page.



LOGIN APPROVALS

Click on **Login Notifications**. Here, you can choose to be notified if an attempt is made to log in to your Facebook page from a device which you have not used before. Choose whether to receive by **Email** or Text **Message/Push Notification**.

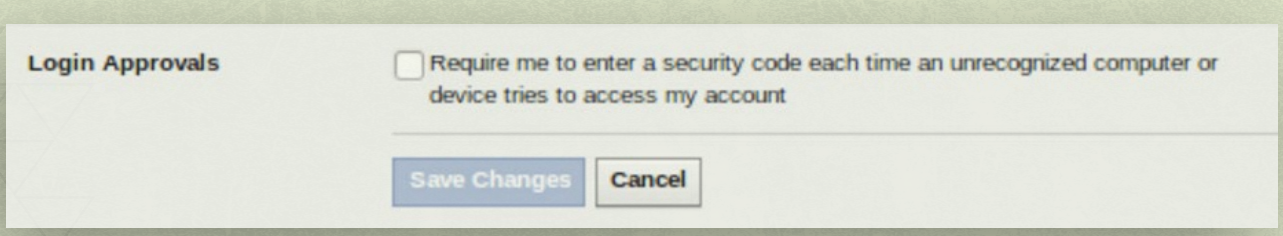
WARNING: If you choose to receive alerts via Text Message, this means you will link your mobile phone number to your Facebook account, making your activities on the site more easily identifiable.



LOGIN APPROVALS (TWO-FACTOR AUTHENTICATION)

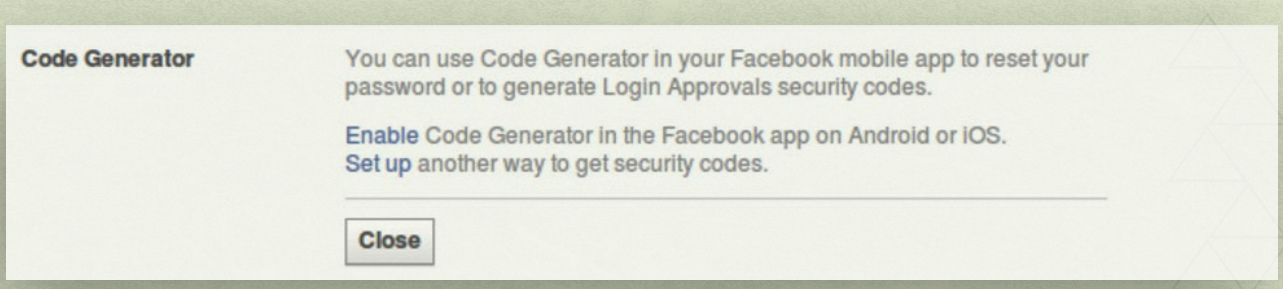
For added security, you can choose to enter a security code every time your account is accessed from a computer or device **Facebook** does not recognise. The security code will be sent as SMS to your mobile phone.

NOTE: Enabling this option will make it more difficult for someone else to access your account unless they also have access to your mobile phone. However, as mentioned above, it also involves associating your mobile phone number with your **Facebook** account. You should consider the pros and cons of this for your own situation and make the choice that you consider more secure for you.



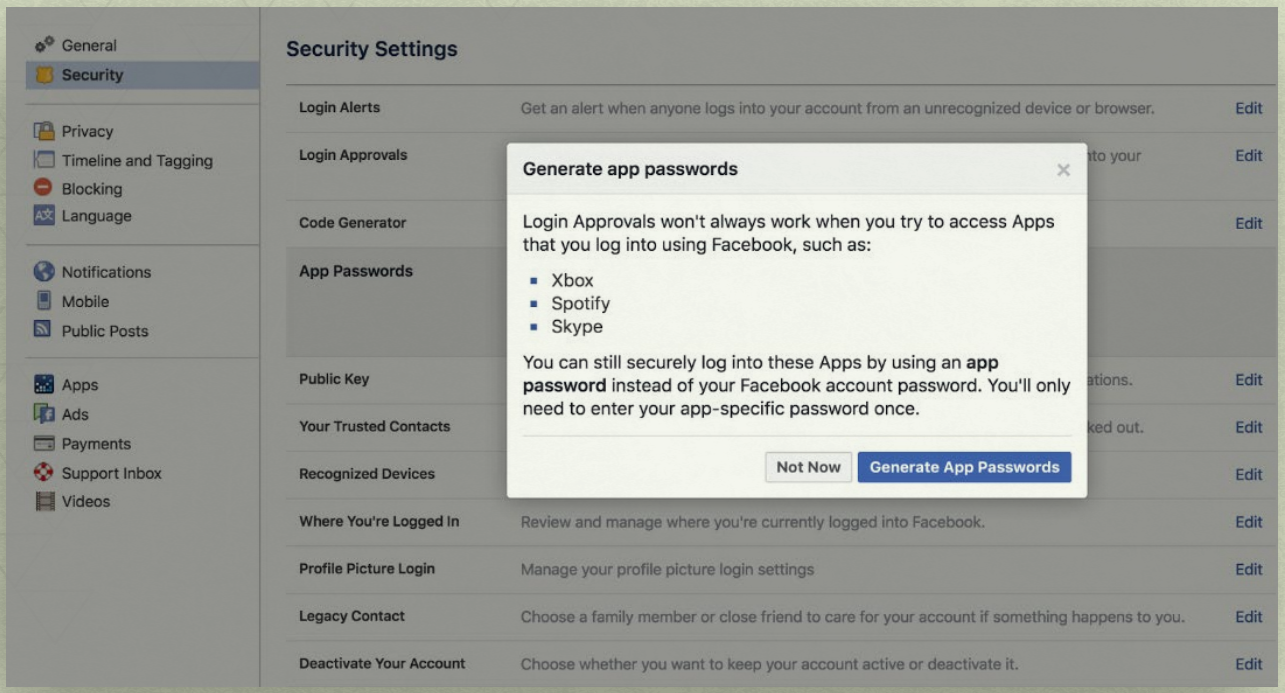
CODE GENERATOR

This setting allows you to use the **Facebook** mobile app on your smartphone in order to generate login codes or new passwords.



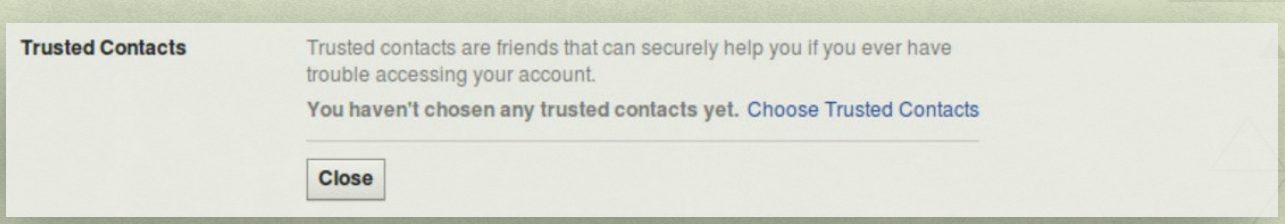
APPLICATION PASSWORDS

If you use applications on **Facebook**, this option allows you to generate individual passwords for them. Unless you have a specific need to do so. However, we recommend avoiding Facebook applications.



TRUSTED CONTACTS

This option allows you to select certain contacts from your **Facebook** friends who can help you to log-in to your account if for some reason you are otherwise unable to. This is done through sharing a secret code with your contact. If you decide to use this option, be sure to choose your trusted contacts carefully and establish a secure means of communication for sharing the code.

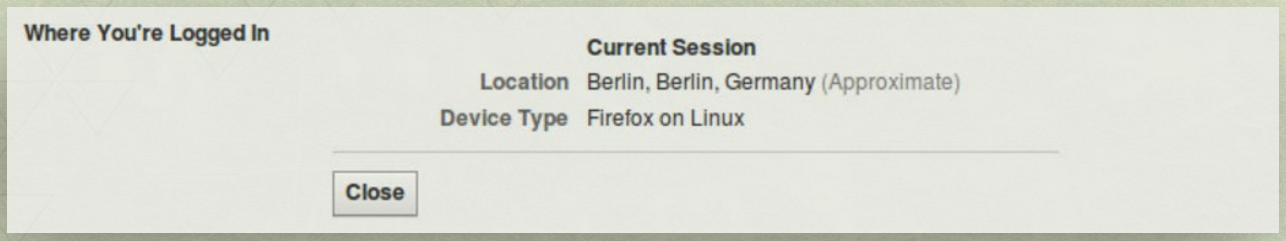


TRUSTED BROWSERS

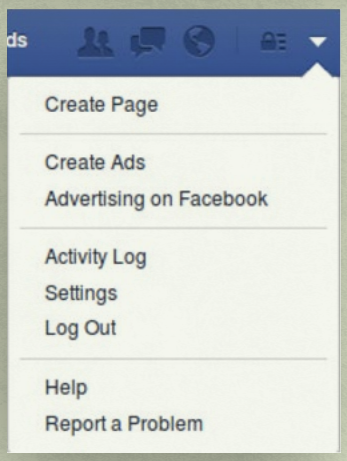
Here you can review the browsers most frequently used to access your Facebook account.

ACTIVE SESSIONS

This shows details of any Facebook session that you may have forgotten to logout of—for example in an internet café, or a friend's computer—and therefore is still active. The location is determined by the IP address.



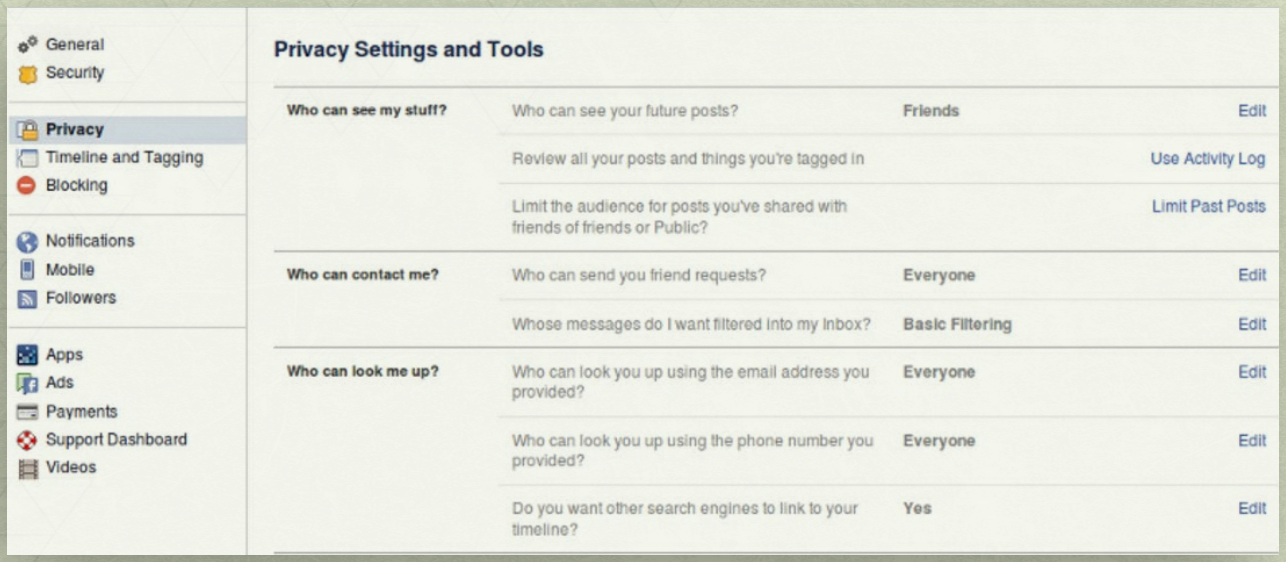
It is very important to close these sessions in order to prevent anyone else accessing your Facebook account, especially if you note any devices in the list which are not yours or you do not recognisze.



SPECIFIC PRIVACY SETTINGS AND TOOLS

To edit your **Facebook** Privacy Settings, **click** on the small arrow beside Home in the top right-hand corner and select Settings.

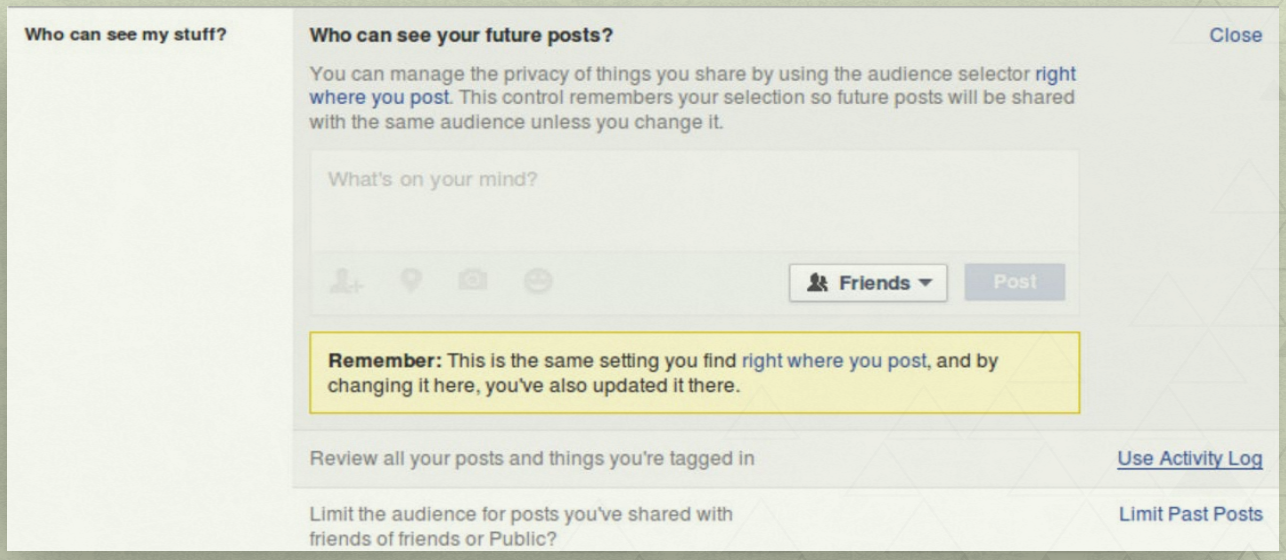
This will take you to the Settings menu. On the left-hand side, **choose Privacy**.



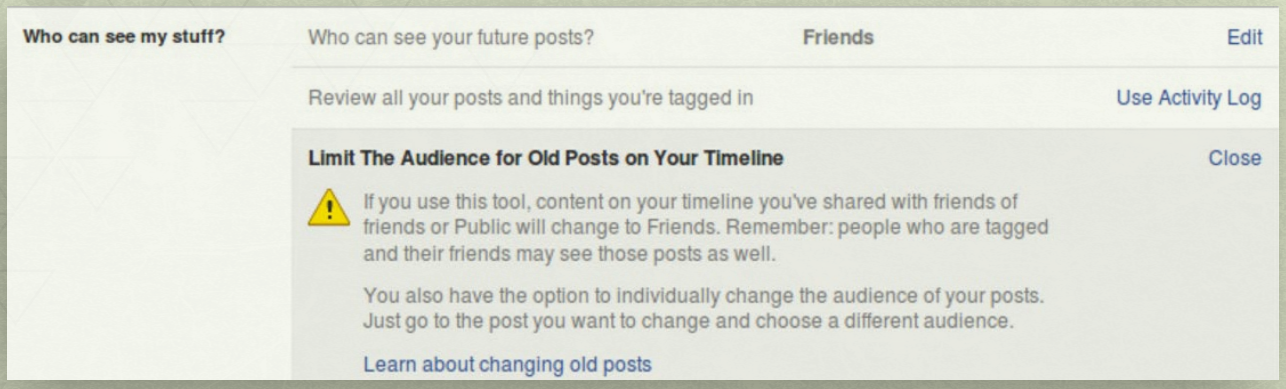
WHO CAN SEE MY STUFF?

The first option here creates a default rule for your future status updates: Who can see your future posts? Here, you can **choose** between making them available to the entire public, your **Facebook** friends, yourself only, or a custom group which you can determine. Note that you can also change this for individual status updates, so that you can decide which ones are public, which ones are for friends or which ones are for a specific group. It's also worth noting, though, **that everything you post is recorded by Facebook (including when you select Only Me) and can be handed over by them to third parties**.

The second option allows you to **review** the posts which other **Facebook** users have tagged you in. To see this, **click** on Use **Activity Log**.



The third option allows you to **restrict** access to previous status updates of yours which may have been public.

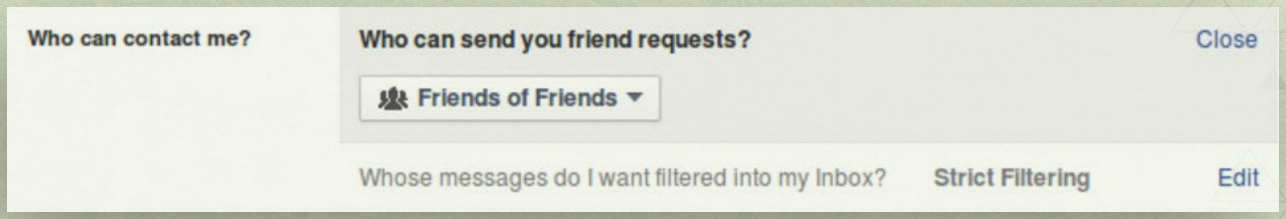


NOTE: However, the limitation that individuals you tagged and their friends will still be able to see this content.

WHO CAN CONTACT ME?

In this section, you can decide who is able to send you a friend request. This is not particularly important in terms of information security, since in the end, it is still you who decides who to accept as a friend, and you should always exercise caution and **avoid adding people who are unknown or untrusted**. If you want to change this setting, **click** Edit.

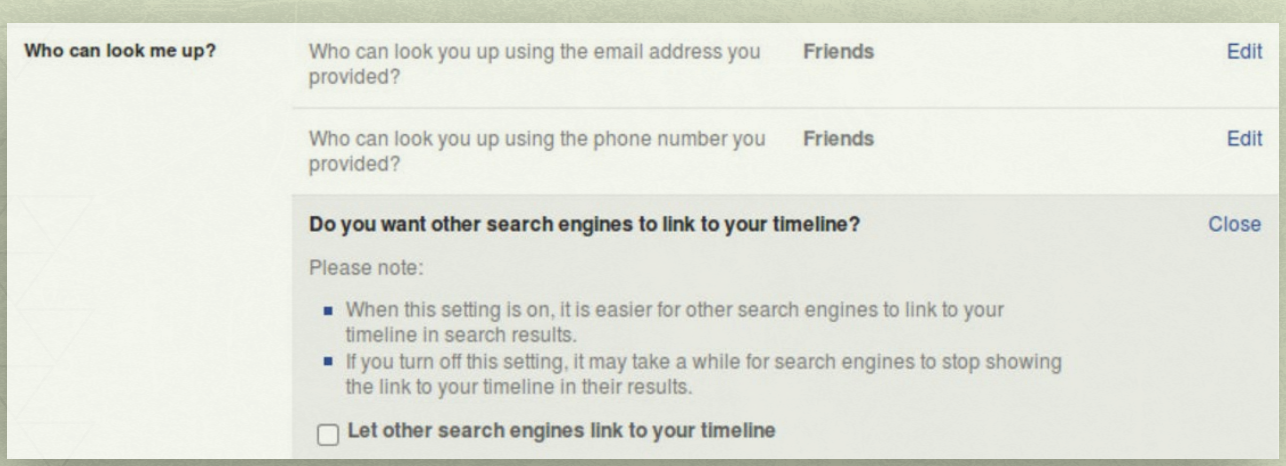
Whose messages do I want filtered into my inbox?: **Facebook** allows you to filter the messages you receive into two folders: **Inbox** and **Other**. Here you can **choose** between **Basic Filtering**, which is more permissive of messages from people who are not on your friend list, and **Strict Filtering**, which is less permissive.



WHO CAN LOOK ME UP?

Here, you can limit the ease with which people can look you up by knowing your phone number or e-mail address (although this is still technically possible), as well as limiting people's ability to find your **Facebook** page via search engines. FB's default settings make it as easy for individuals to find you this way, including possible adversaries.

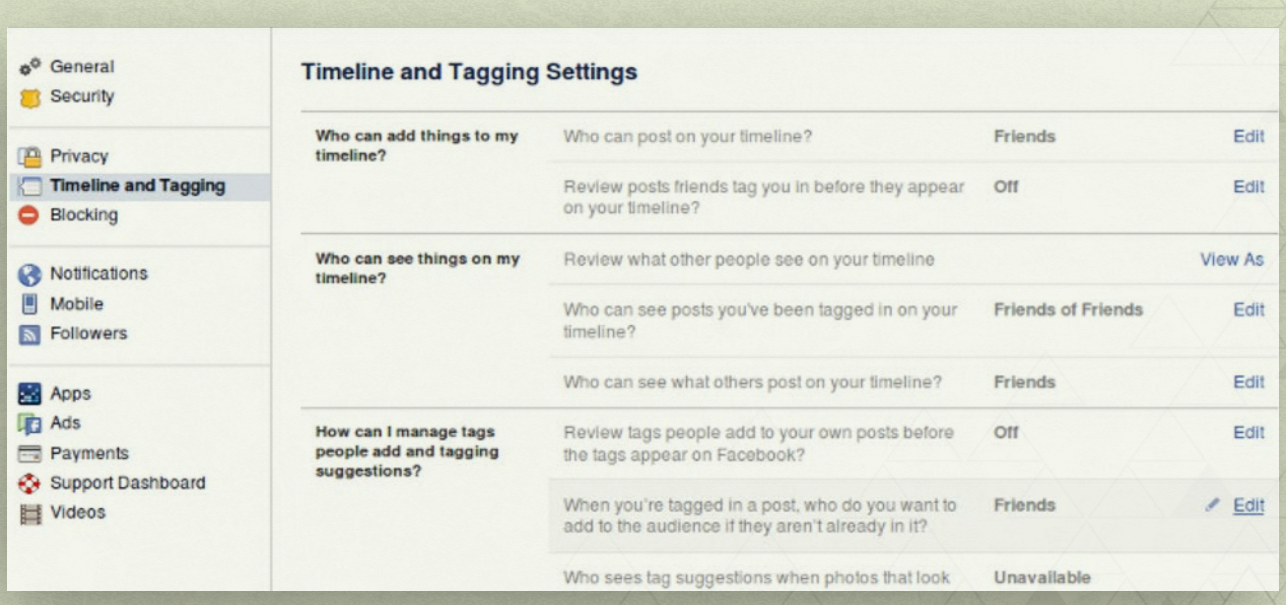
- ✓ Click Edit on the first two options and ensure that only Friends can search for you by your email address and phone number. For the third option, **click Edit** and **uncheck** the box which says Let other search engines link to your timeline.



TIMELINE AND TAGGING

As we have mentioned before, your information security on **Facebook** has a lot to do with the behavior of your friends. In the **Timeline and Tagging** menu, you can determine what happens when friends tag you or your posts and what happens when they post on your timeline.

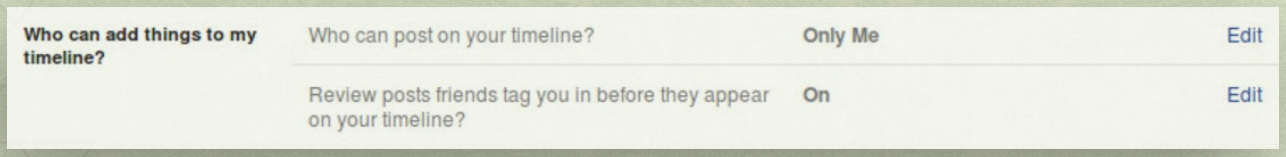
- ✓ In the left-hand sidebar, **click** on the Timeline and Tagging menu.



If you want your timeline to be truly yours, it's advisable to **disallow** posts on your timeline from anyone but yourself. To do this, click edit beside **Who can post on your timeline** and select **Only Me**.

Here, you can decide what happens when other friends tag you in their posts and photographs.

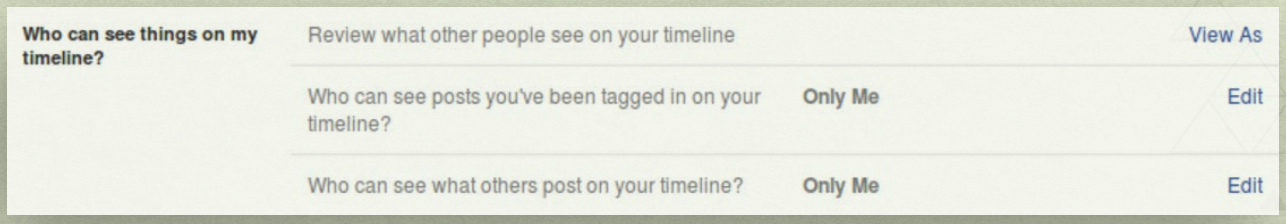
- It is advisable that you **click edit** and **enable** the **Review posts that friends tag you in** option so that you can prevent any irresponsible tagging appearing on your timeline. However, this will not prevent their posts (including your tag) from being visible to their friends, or perhaps even the public, depending on their settings.



Who can see things on my timeline? This item is associated with the previous options. Previously, we've decided who gets to publish material to your timeline, and here, you get to decide who can read them.

- If you **click Edit**, you can change these settings so that either everyone, friends of friends, a custom group of people, or only yourself can see posts you've been tagged in, or things others post on your timeline.

The first option, **View As**, is an interesting way to see what certain individuals can see on your timeline.



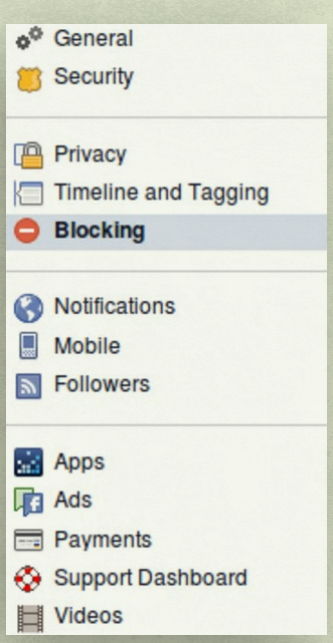
WARNING: When you see the warning sign, take note. These are important side notes that are meant to stress to avoid actions that could make you vulnerable or include actions that could keep you safer.

How can I manage tags people add and tagging suggestions? This refers to tags of you by other users of **Facebook**. It's best if you **switch on** the Review tags people add to your own posts before the tags appear on Facebook option, and limit the audience for the second option to Only Me. **Facebook** has begun using a form of **facial recognition** technology which allows it to identify

photographs that look like you among your friends and contacts photos. Facebook will even notify them to tag you. Naturally, for rights advocates, this could be particularly sensitive.

- It's strongly recommended that you **deactivate** this option if it is available to you.

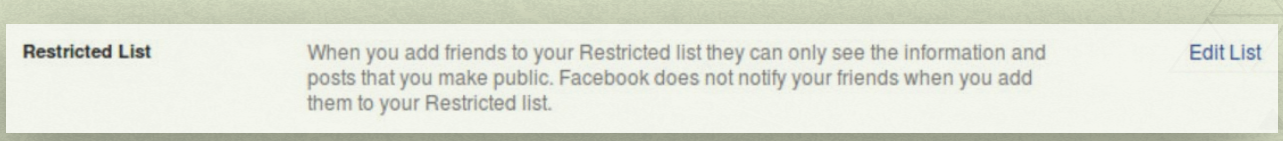
- **BLOCKING USERS AND APPS**
  In the menu on the left, **select Blocking**. Here, **Facebook** offers ample opportunities for blocking unwanted, intrusive, and sometimes potentially dangerous information.



RESTRICTED LIST

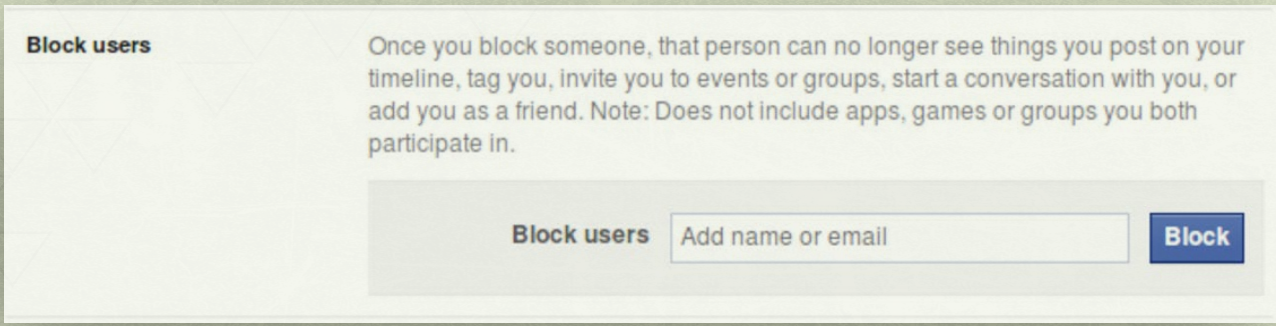
Here, you can discreetly add **Facebook** friends to a list which will limit them to only being able to view information you share publicly on your timeline (per the settings we explored above). To add friends to the list,

- **click Edit List**.



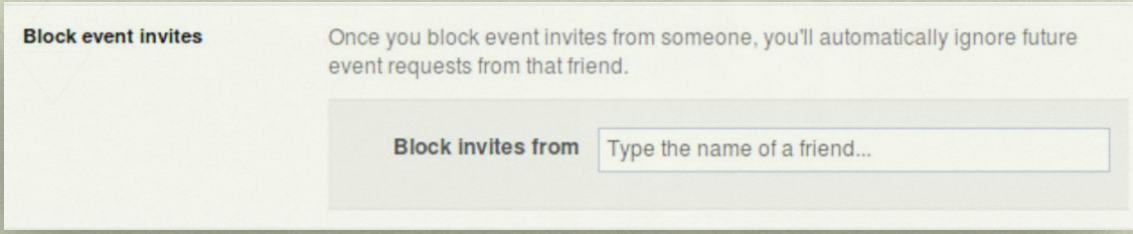
BLOCK USERS

Here you can block a user from accessing your **Facebook** page, any of your content, or adding you as a friend.



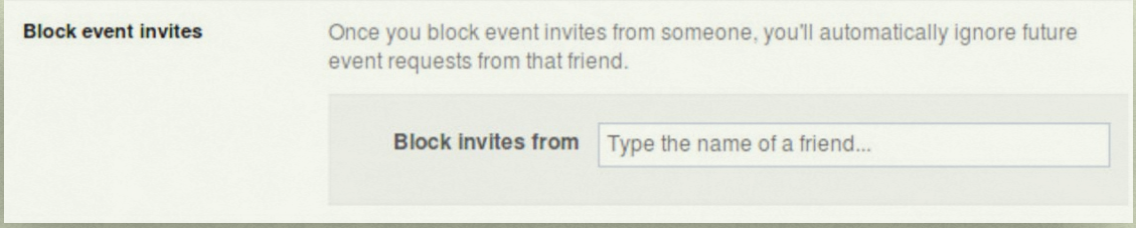
BLOCK APP INVITES

Often, we will have **Facebook** friends who are enthusiastic about a particular application, often a game, and they will continuously send us invites to join this game. Here, you can block application invites from such friends.



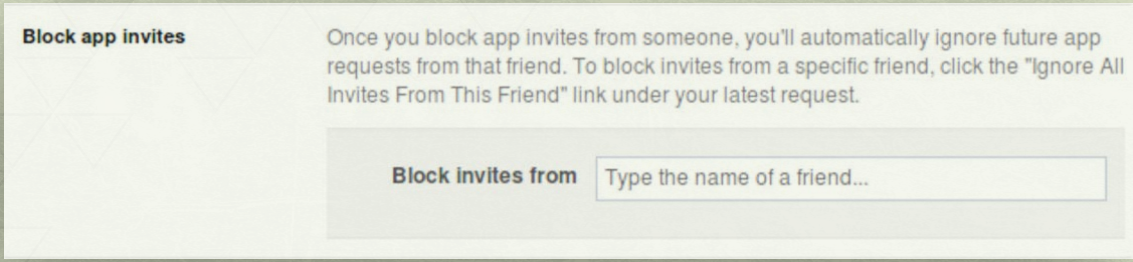
BLOCK EVENT INVITES

Similarly, here you can block invitations to events from certain **Facebook** friends.



BLOCK APPLICATION

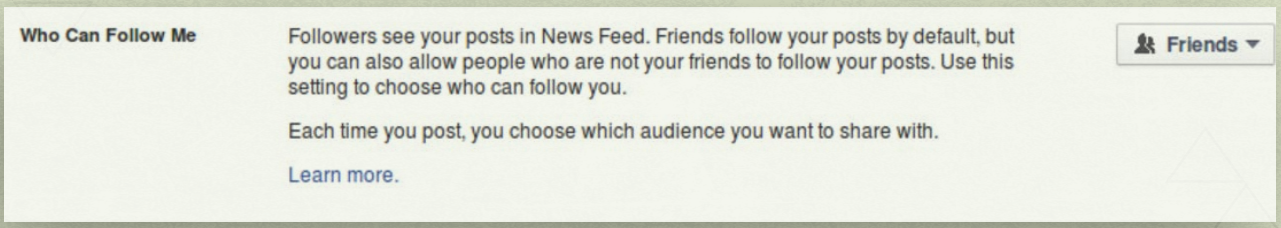
As the name suggests, here you can prevent an application from accessing all but your public information.



FOLLOWERS

Facebook gives you the option of allowing people to subscribe to your news feed, without being friends. Be aware however, that if you allow others to subscribe to your news feed, then some of your data is available for them and others in their network to see. The safest option is not to allow people to subscribe to your news feed.

Click on Followers from the menu on the left. Ensure that Friends is **selected**.

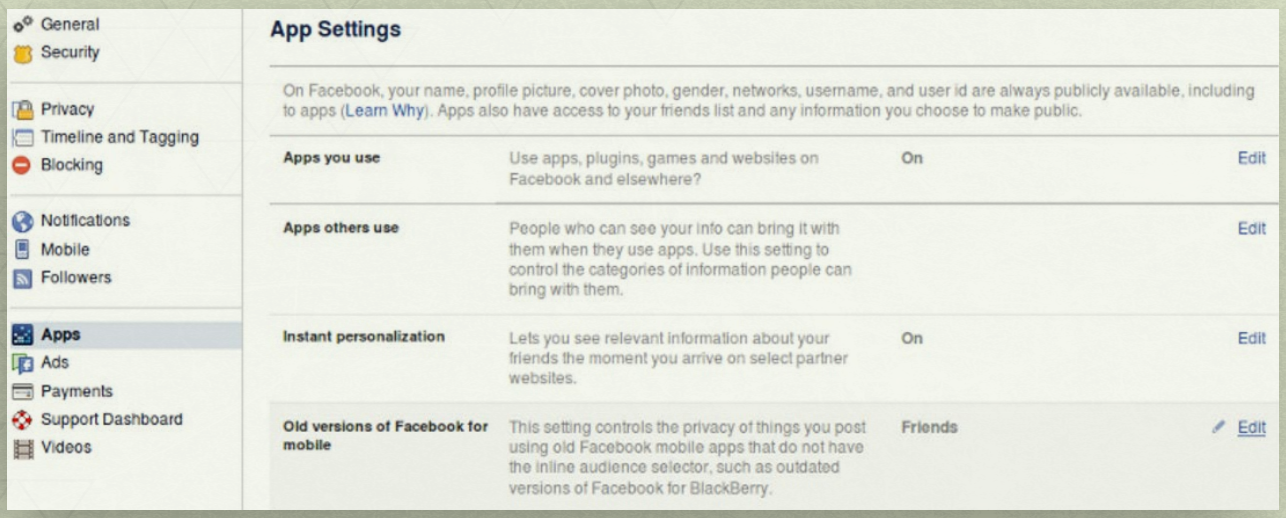


FOLLOWER SETTINGS

Applications

Many Facebook users love and actively add third party applications in order to play games, enhance communications, and more. But keep in mind each application is associated with your Facebook account, and the basic data of your Facebook account will be available to any application (such as your name, gender, public pictures and network). Also, when installing a new application, it may ask for your permission to have access to information about you and your friends. This includes a variety of data, such as age, place of residence, education, circle of friends and contacts. Thus, the application can gather and share information such as what country you come from and where you currently are, information you may consider sensitive. Therefore, for safety reasons, we recommend not to use Facebook applications unless you really need to.

- Click on **Apps** in the menu on the left.

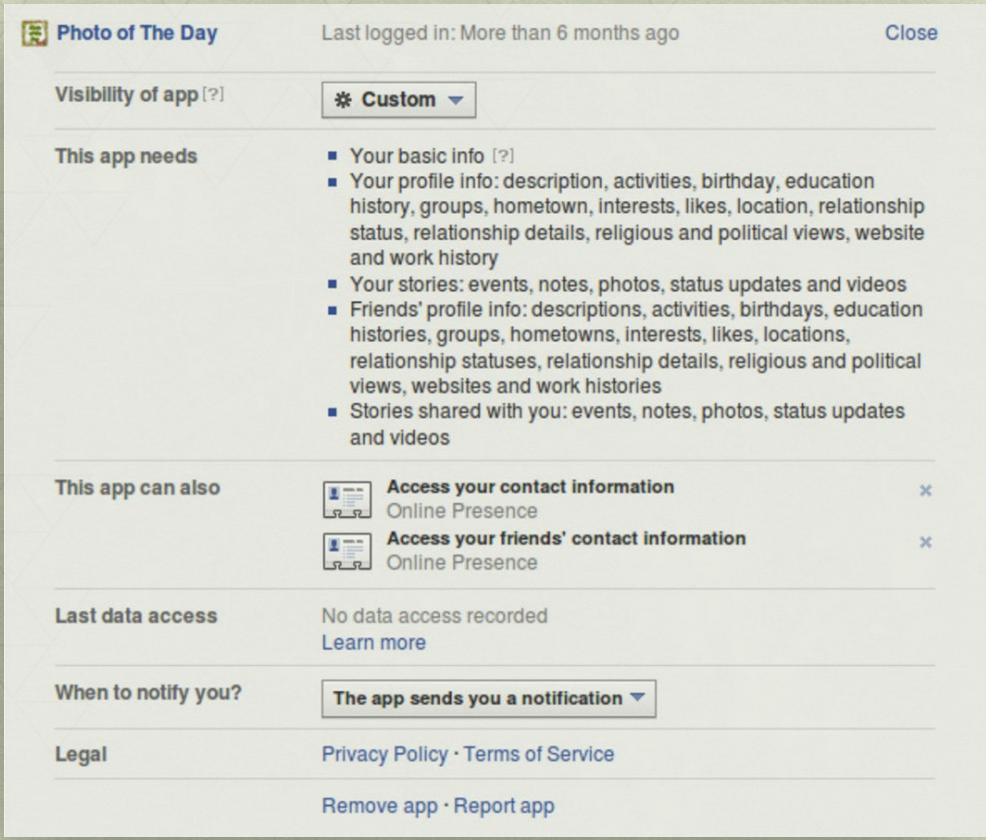


APPS YOU USE

Here, you can enable or disable the so-called "Facebook Platform" which allows you to quickly register and sign in on other sites using your **Facebook** account. This option is enabled by default. On the one hand, it's convenient: no need to spend time on registration forms, filling in fields. On the other hand, comments on news storys, or signed petitions can link to your **Facebook** account, where it's recorded and possibly shared.

- If using Apps is not important to you or your work, we recommended that you **click Turn Off Platform** in order to better protect your privacy. If you do decide to leave the option enabled, then pay attention to the list of applications already installed at this point. Do you really need them all?

By **clicking** on an app you can see what information it has access to.

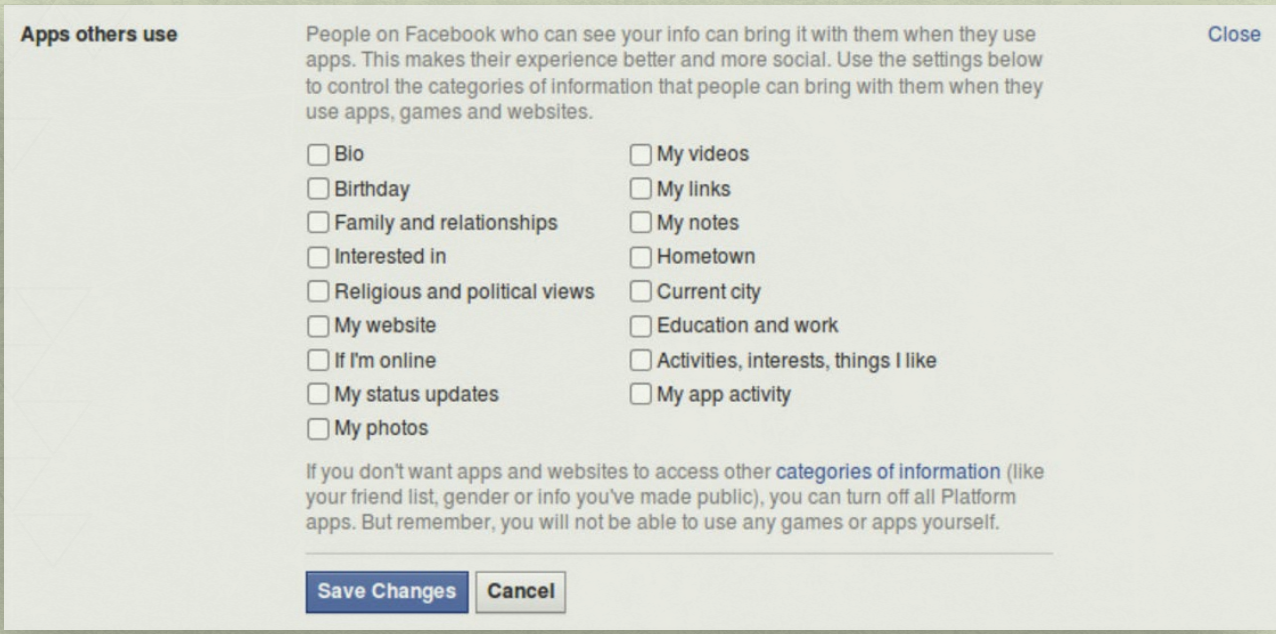


To remove an application, **click on the 'x'** beside the app in the list, and then **click Remove** in the warning window which pops up.

APPS OTHERS USE

We also have to consider that some of our Facebook friends bring our information into the apps that they use.

- By clicking on **Apps others use**, you can uncheck the boxes beside categories of your information which you do not want to share with your friend's applications.



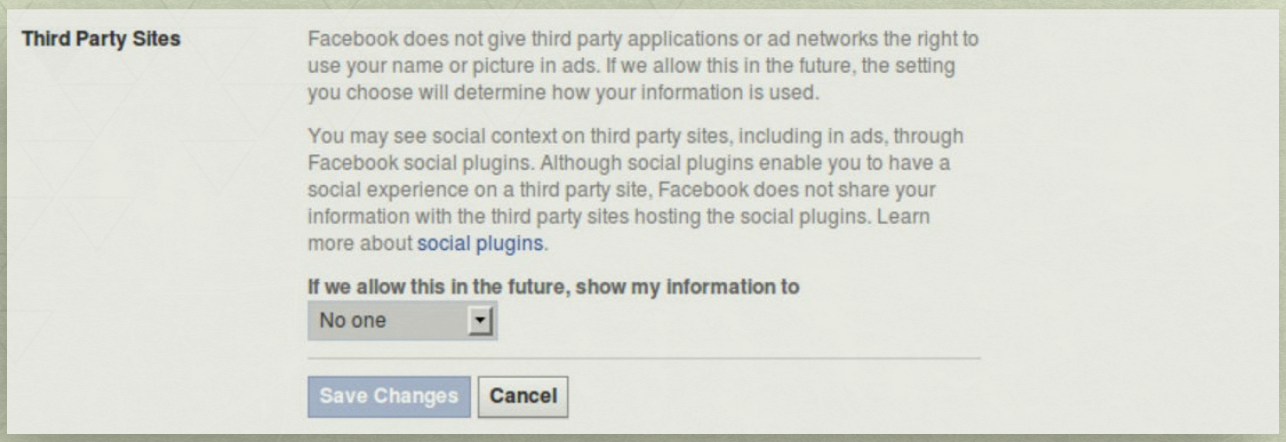
ADVERTISING SETTINGS

Advertising is fundamentally important to social networking companies because it's how they make their money. There will always be advertisements on social networking sites such as Facebook, though we can make them less personal, which is the right move in terms of information security and privacy.

- In the column on the left, select Ads.

Facebook currently promises not to associate your name or picture with third-party advertisements, although they leave space for this to be possible in the future. It's a good idea to change these settings so that your details still remain private in case advertising rules change in the future.

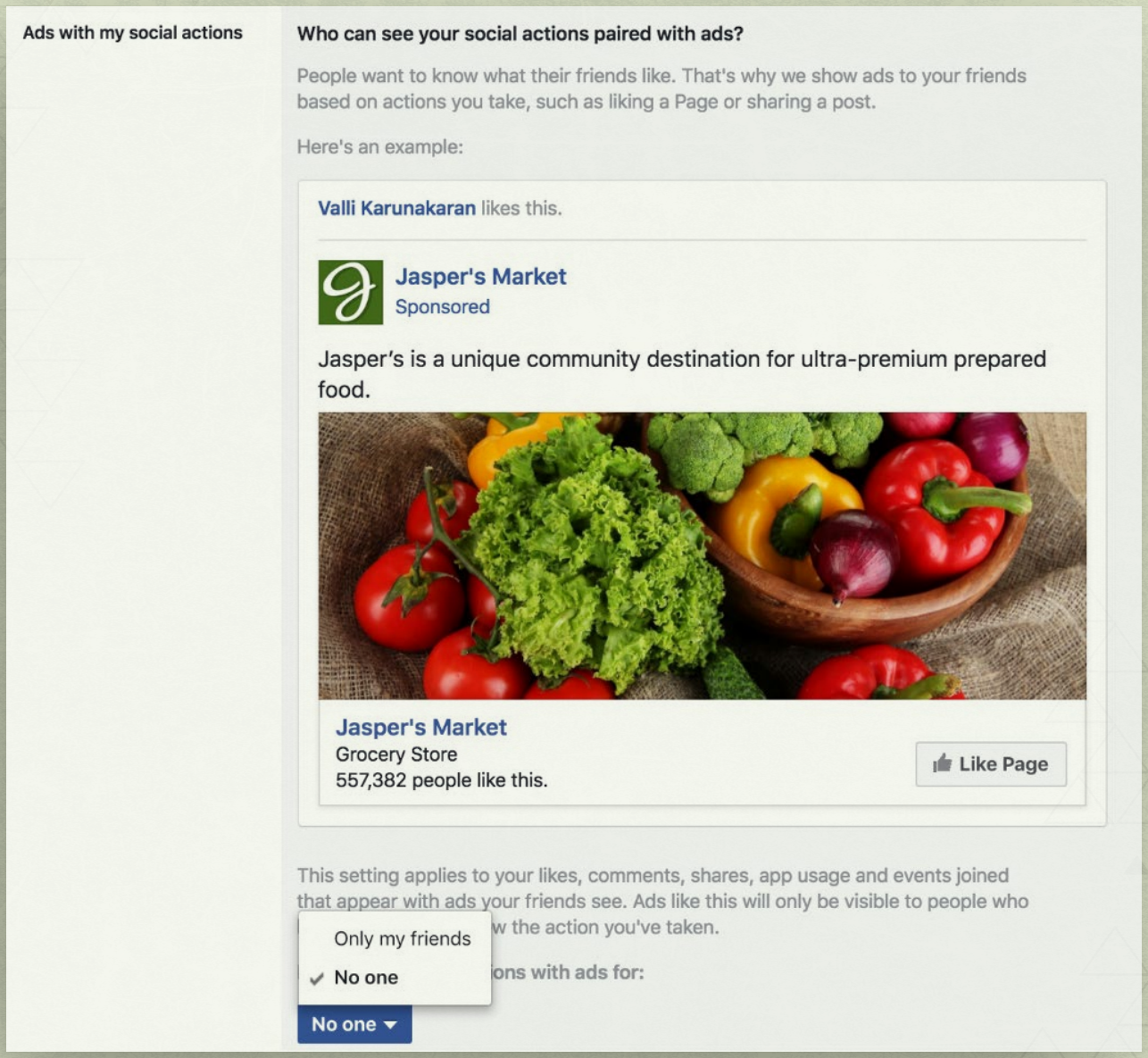
✓ Click Edit beside Third Party Sites. Select No-one and select Save Changes.



SOCIAL ADS

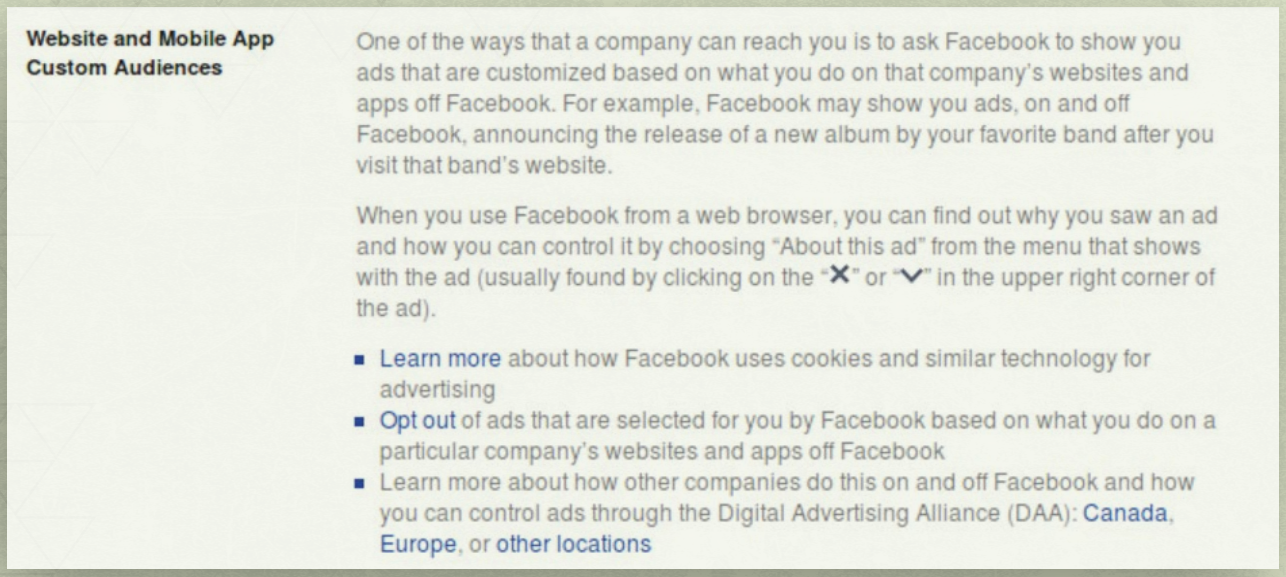
Here, **Facebook** encourages users to become ambassadors for products or pages they have 'liked'. This means that you could be used to advertise a page or product to your friends. If this makes you uncomfortable, it's recommended that you disable it.

✔ Under Ads and friends, **click Edit** and **select No-One** from the drop-down menu.



By default **Facebook** tries to display targeted advertising on your tastes and interests.

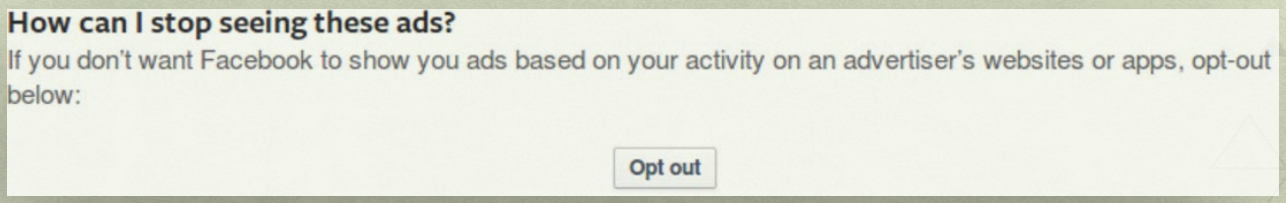
✓ To get rid of this, you need to **click** on the **Opt Out** link in this paragraph.



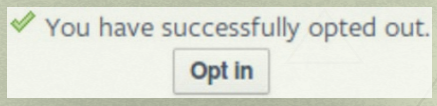
This will open a page titled **Custom Audiences** from your **Website and Mobile App**, where Facebook gives more information about its advertising policy.

✓ In the middle of the text is the Opt Out button for you to confirm.

WARNING: Changes made to this setting are not recorded by Facebook, but rather are stored in your browser. Unfortunately, you must repeat this process for every contact, call, and device you use to connect to Facebook.



After a request for confirmation, you will see the result:



TWITTER

Twitter[35] has become a valuable platform where activists around the world break their stories and ideas. It's become a place for, real on the ground news updates on movements and protest, where the oppressd have a voice and are able to connect with people in a real and powerful way.

Twitter states in its terms of service: "*This license is you authorizing us to make your Tweets available to the rest of the world and to let others do the same. But what's yours is yours—you own your content.*" While this may be the case, Twitter reserves the right to hand over your information to governments should a request be made.

Keep in mind, **Twitter is actively monitored by numerous governments**, including the United States. Moreover, Twitter's Terms of Service state that they **will share your information in response to legal requests including governmental investigations**. For more information, see Twitter's Privacy Policy and its Transparency Report.

Although it's a website, many people interact with and manage Twitter via desktop and smartphone applications that are known as Twitter clients. If you use a client you should make sure it is connecting to the site securely, over an encrypted connection.

Like Facebook, many people use Twitter in conjunction with numerous other websites and applications in order to share status updates, photos, locations, links, and so forth. Using these applications pose many potential additional security vulnerabilities, and it is very important that the privacy settings on all other applications are made as secure as possible.

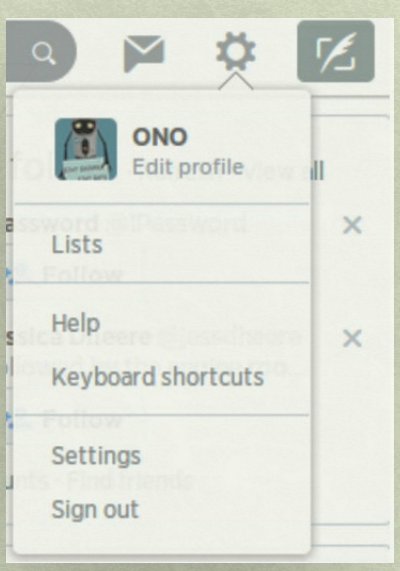
Read on to understand how better to secure your Twitter!

BASIC ACCOUNT SETTINGS ON TWITTER

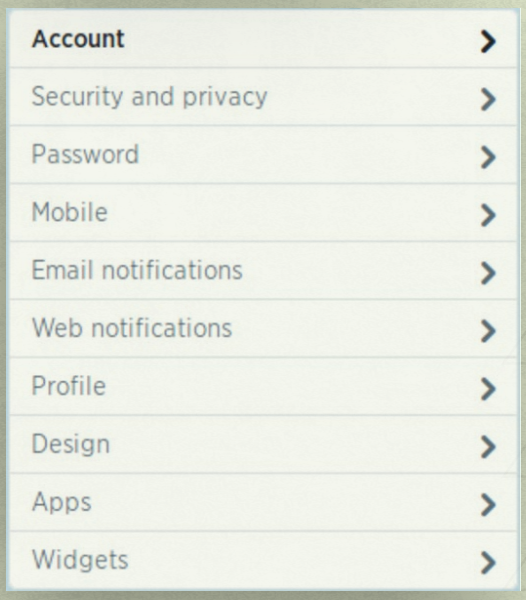
Twitter's Basic Account Settings allow you to control how people can find your profile, what information you share and the level of security your account requires when you are using the web-browser based version of **Twitter** (that is to say, not a client, smartphone app, or GSM phone).

[35] https://securityinabox.org/ru/twitter_main

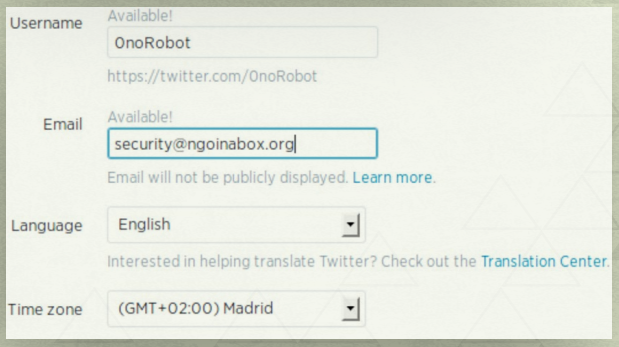
In order to access your account settings, log in to your account using your browser and click on the ⚙ icon at the top right of the screen to open the **Options** menu



In the drop-down menu, choose **Settings**. This will open the settings page. You will find a list of pages on the left-hand side where you can click between various categories of settings.



At the top of the Account Settings list, you will find the username and e-mail settings. **Choose carefully whether you want to use your real name or a pseudonym as your username**, and which email address you wish to associate with your profile. It may be best to set up a new e-mail address using the Tor Browser and connect to **Twitter** only using **Tor** if you wish to protect your **identity**.



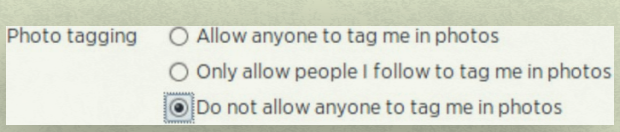
SECURITY AND PRIVACY SETTINGS ON TWITTER

Click on **Security and privacy** in the left-hand sidebar in order to access the Security and Privacy settings page.

Twitter gives you the option of sending a message to your mobile phone or smartphone any time your account is accessed. This is recommendable if you are also using the Twitter application on your smartphone. In this case, choose the **Send login verifications to the Twitter app** option.

WARNING: While this may be useful in alerting you to an unauthorized attempt to access your account, associating your mobile phone to your Twitter account makes your account more easily identifiable and is not advisable if you want to use Twitter anonymously or with a pseudonym.

In the photo-tagging section, Twitter allows you to control who, if anyone, can tag you in photos they upload. Since there is no option to approve or disapprove tagging in photos, it's advised that you choose the option **Do not allow anyone to tag me in photos. This is particularly important in cases where you may be photographed during protests, for example, which could later be used as evidence.**



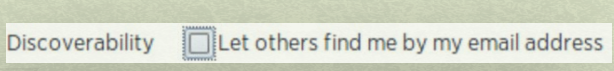
Twitter allows you to control who can see your tweets: the public in general, or only individuals who you allow to follow you.

Go to **Tweet Privacy settings**. Choose the **Protect My Tweets** option.

WARNING: Even if you choose the **Protect my Tweets** option, they are still accessible to Twitter and therefore can still be recorded and handed over to third parties.

Twitter also gives you the option of adding a location to your tweets under the **Tweet Location** option. This option is disabled by default. If sharing your location widely is appropriate in order to stay safe, then this option may be useful. However, it is generally **recommended that you leave this feature disabled** as your location information can also be very useful to your adversaries.

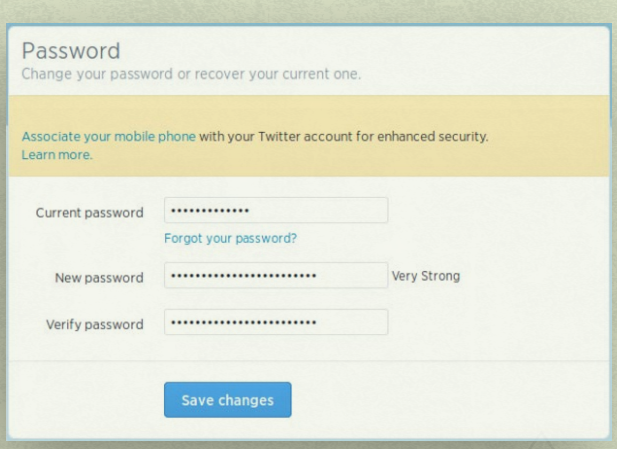
Discoverability gives you the option of allowing people to find your Twitter account if they already have your e-mail address. If you wish to maintain more privacy for your Twitter account, it's recommended that you disable this option.



In the **Personalization and Promotion** section, Twitter gives you the option of allowing them to monitor your behavior on their site and other websites. This allows them to tailor the content and ads they show you, which are selected based on you interests. It also helps them know which third parties might be interested in buying information related to your consumer behaviors and hobbies. It is recommended that you uncheck these boxes for more privacy.

PASSWORD SETTINGS ON TWITTER

Here, Twitter allows you to change your password. It's recommended that you select a strong, memorable password and update it regularly. For more, see section on "How to create and maintain strong passwords." Page 71



NOTE: The pencil sign denotes important details that often will provide important background to comprehending the section at hand.

MOBILE SETTINGS ON TWITTER

You can open Twitter's mobile settings by clicking on Mobile in the menu on the left-hand side. Here, Twitter encourages you to download the smartphone app and also gives you the option of activating Twitter text messaging, which allows you to tweet directly from your mobile phone. **As noted above, it is not advisable to associate your Twitter account to your mobile phone if you wish to maintain a degree of privacy or anonymity while tweeting.** Also, remember that **text messages sent over the GSM network are not encrypted and are easily interceptable and traceable to their authors.**

GENERAL GUIDELINES ON CLIENTS AND APPS

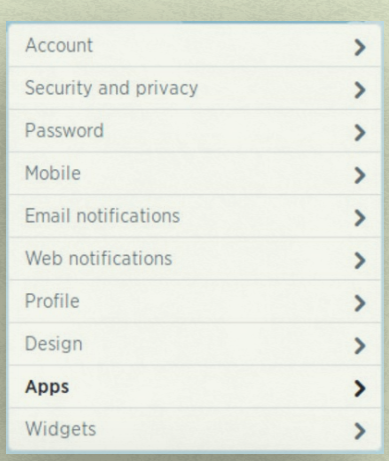
Twitter users can allow various third-party applications, including other social networking and photo-sharing sites to interact with their **Twitter** accounts, for example in order to share photos uploaded via websites such as **Instagram**, or **TwitPic.**[36] However, data when using social networking sites you must be careful when integrating your profiles on different social networking

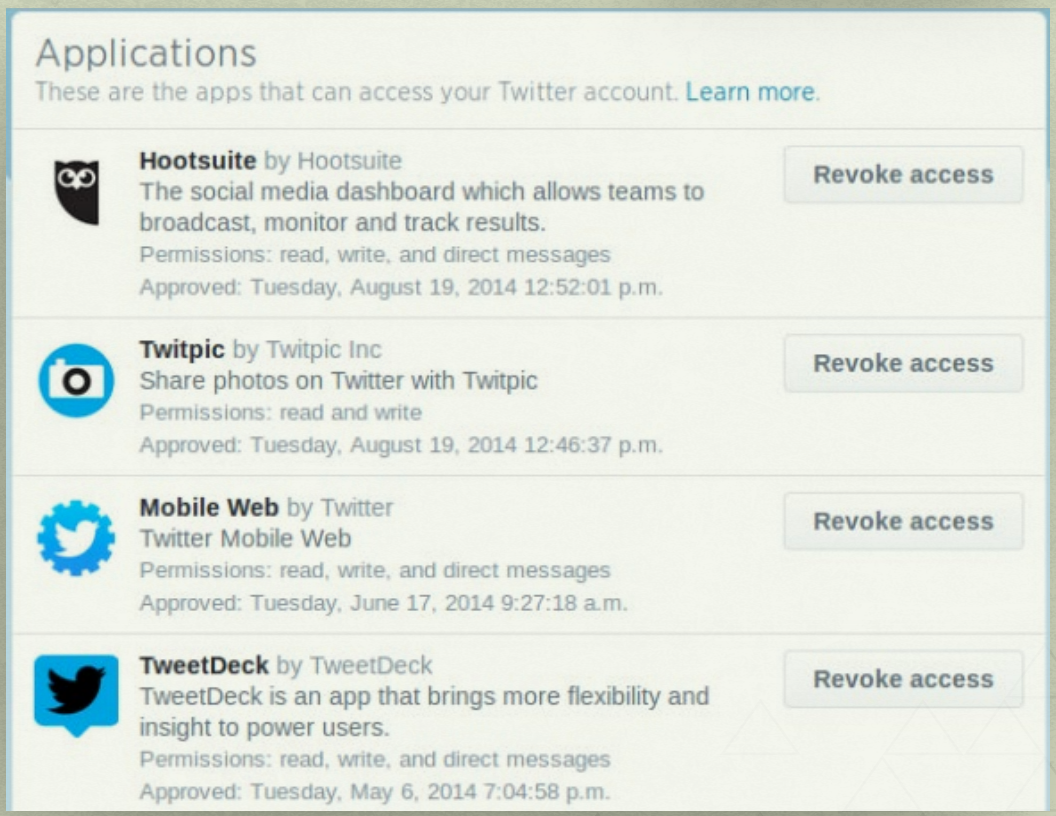
[36] https://securityinabox.org/ru/twitter_clients#2.0

sites. These third-party sites have their own terms of use, privacy policies and privacy settings which are not necessarily the same as Twitter's. Even if your **Twitter** account is relatively secure, your profiles on a third-party app/website may be completely exposed. Using the same username for multiple sites and accounts can make it easier for you to be tracked, using different names decreases that risk. The number of third-party sites and apps are vast, and only a few are explored in this guide. However, it is vital that you research and update your security settings on all third-party apps linked to your **Twitter** page. If you do not consider them secure enough, delete your profile and revoke its access to your **Twitter** account.

- Should you wish to revoke the access of an application to your Twitter profile, go to **Settings** of your account and click the **Apps** tab on the left-hand side.

  Having opened the list of apps connected to your Twitter account, select the app to which you wish to revoke access, click Revoke access





INSTAGRAM

Instagram[37] is a popular image-sharing smartphone application which belongs to **Facebook** and is often used in conjunction with **Twitter**. Since it is primarily a mobile application that is also owned by Facebook, using Instagram with Twitter and Facebook associates your account to your mobile device, which can mean a lot of information and metadata on your phone can be shared between these platforms all of whom can then share them with the state. It is not recommended that you use Instagram if you are concerned about sharing your location and other personal details.

By default, anyone can view your profile and posts on Instagram, you can make both private which grands access to followers that you have approved or that were following you before you made your accout private. If your posts are set to private, only your approved followers will be able to see them in the Photos tab of **Search & Explore** or on hashtag or location pages.

To set your posts to private from the Instagram app:

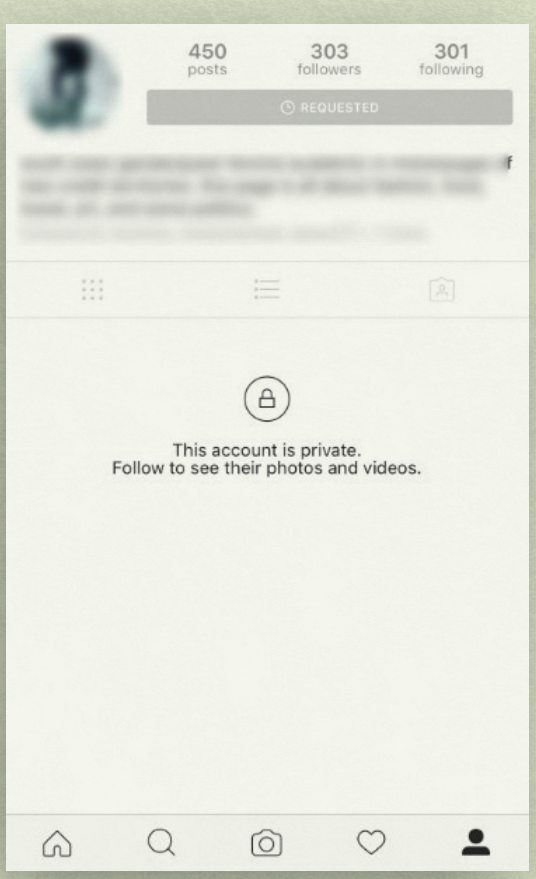
- **IPHONE OR WINDOWS PHONE**

  Go to your profile by tapping
  Tap
  Turn on the **Private Account** setting

[37] https://help.instagram.com/116024195217477/

ANDROID

Go to your profile by tapping
Tap ⋮
Turn on the **Private Account** setting



Things to keep in mind about private posts:

- Private posts you share to social networks may be visible to the public depending on your privacy settings for those networks. For example, a post you share to Twitter that was set to private on Instagram may be visible to the people who can see your Twitter posts.
- Once you make your posts private, people will have to send you a follow request if they want to see your posts, your followers list or your following list. Follow requests then appear in **Activity**, where you can approve or ignore them.
- If someone was already following before you set your posts to private and you do not want them to see your posts, you can block them.
- People can send a photo or video directly to you even if they're not following you.

- Under settings in instagram, go to **Linked Accounts** and de-link any other accounts associated.