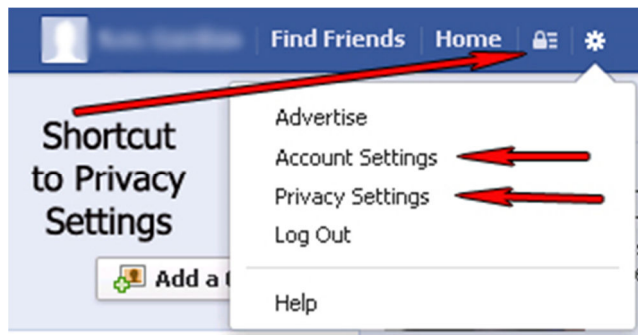


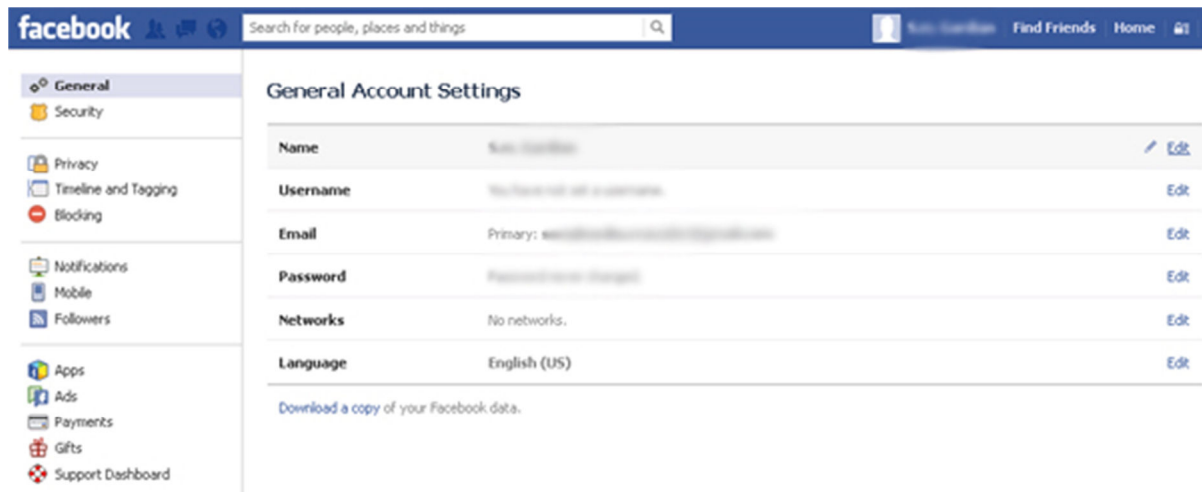
Maximum Privacy and Security for Your Facebook Account

Recent studies show that privacy concerns are very much on the minds of Facebook users. Part of being a responsible member of any online community is educating yourself and your loved ones on how to properly configure the privacy and security settings offered by the platform. The fact that Facebook has just over a billion members now, and some are out to hack, scam and victimize others makes the issue even more pressing.

This walk-through will show you how to configure your Facebook Account and Privacy Settings:

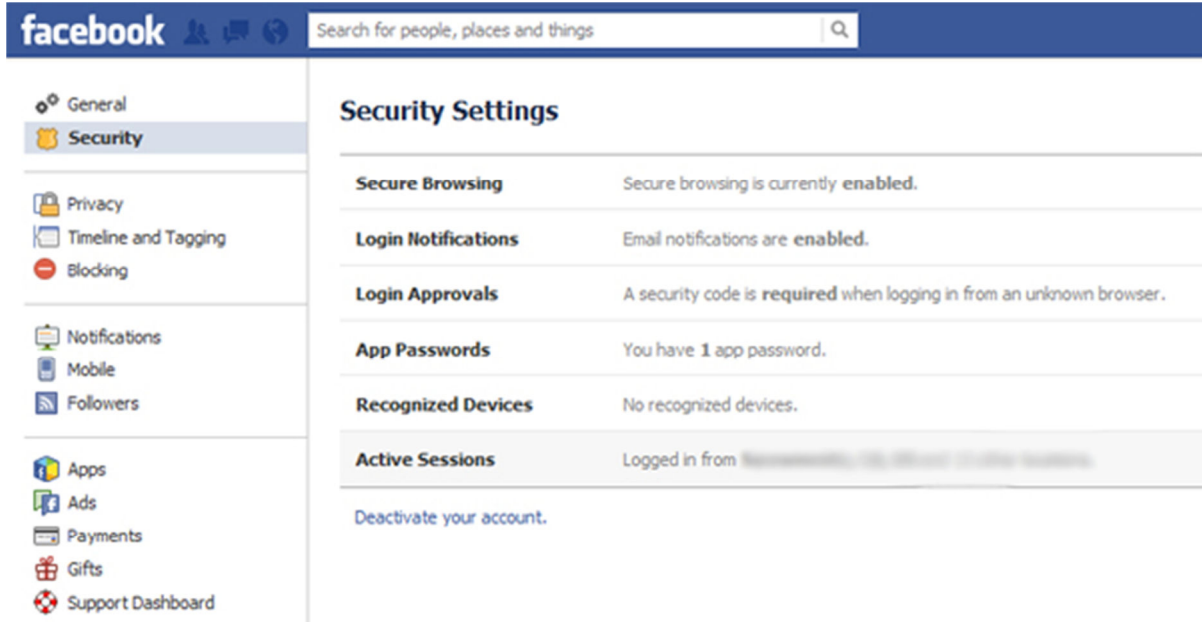


First we'll start out with the **Account Settings**. Click the gear icon shown above.



1. Use a dedicated email address for Facebook. If you use an email account that you also use for banking or other sensitive information, then you are opening yourself up to more opportunities for criminals if your Facebook account is ever hacked.
2. Create a strong, secure password. (*Don't use the same password for Facebook that you use to access other accounts*)

Security Settings – Click the ‘Security’ tab located in the left column:



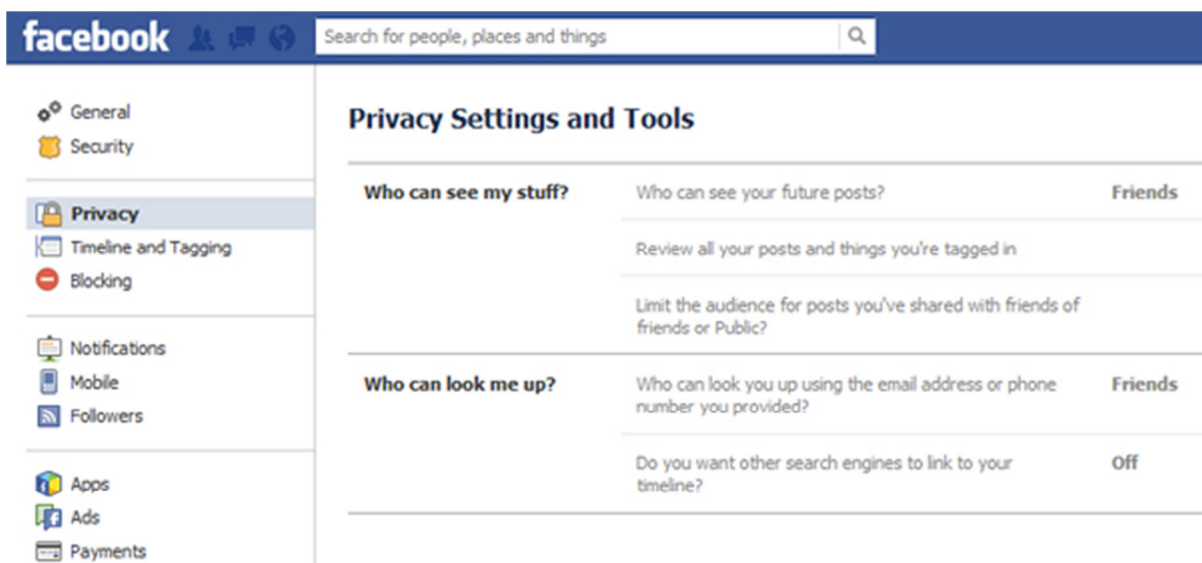
The screenshot shows the Facebook Security Settings page. The left sidebar contains navigation tabs: General, Security (selected), Privacy, Timeline and Tagging, Blocking, Notifications, Mobile, Followers, Apps, Ads, Payments, Gifts, and Support Dashboard. The main content area is titled 'Security Settings' and lists several settings:

Setting	Status
Secure Browsing	Secure browsing is currently enabled .
Login Notifications	Email notifications are enabled .
Login Approvals	A security code is required when logging in from an unknown browser.
App Passwords	You have 1 app password.
Recognized Devices	No recognized devices.
Active Sessions	Logged in from XXXXXXXXXX, US, iPhone 12 Pro Max

At the bottom of the main content area, there is a link: [Deactivate your account.](#)

1. Enable **Secure Browsing**
2. Enable **Login Notifications** – (this lets you know when your account has been accessed)
3. Require **Login Approvals** – (this will require you to enter a code sent to you via text message if Facebook doesn't recognize the device). This is a great way to prevent your account from being hacked
4. End any active sessions you don't recognize

Privacy - Click the ‘Privacy’ tab located in the left column:



The screenshot shows the Facebook Privacy Settings and Tools page. The left sidebar contains navigation tabs: General, Security, Privacy (selected), Timeline and Tagging, Blocking, Notifications, Mobile, Followers, Apps, Ads, and Payments. The main content area is titled 'Privacy Settings and Tools' and lists several settings:

Setting	Current Setting
Who can see my stuff?	Friends
Who can look me up?	Friends
Do you want other search engines to link to your timeline?	Off

1. Set default privacy to **Friends**
2. Use the Activity Log to review all your posts and things you're tagged in
3. Limit the audience for old posts on your Timeline
4. Set "Who can look me up?" to **Friends**
5. Don't allow search engines to link to your Timeline

Timeline and Tagging -Click the 'Timeline and Tagging' tab located in the left column:

Timeline and Tagging Settings		
Who can add things to my timeline?	Who can post on your timeline?	Friends
	Review posts friends tag you in before they appear on your timeline?	On
Who can see things on my timeline?	Review what other people see on your timeline	
	Who can see posts you've been tagged in on your timeline?	Friends except Acquaintances
	Who can see what others post on your timeline?	Friends except Acquaintances
How can I manage tags people add and tagging suggestions?	Review tags people add to your own posts before the tags appear on Facebook?	On
	When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	Custom
	Who sees tag suggestions when photos that look like you are uploaded?	No One

1. Under **Timeline and Tagging**, its recommend that you use the options shown above

Blocking – Click the 'Blocking' tab located in the left column:

The screenshot shows the Facebook 'Manage Blocking' settings page. On the left is a navigation menu with options: General, Security, Privacy, Timeline and Tagging, **Blocking**, Notifications, Mobile, Followers, Apps, Ads, Payments, Gifts, and Support Dashboard. The main content area is titled 'Manage Blocking' and contains the following sections:

- Restricted List:** When you add friends to your Restricted list they can only see the information and posts that you make public. Facebook does not notify your friends when you add them to your Restricted list.
- Block users:** Once you block someone, that person can no longer be your friend on Facebook or interact with you (except within apps and games you both use and groups you are both a member of). Below this is a form with a text input labeled 'Add name or email' and a 'Block' button.
- Block app invites:** Once you block app invites from someone, you'll automatically ignore future app requests from that friend. To block invites from a specific friend, click the "Ignore All Invites From This Friend" link under your latest request. Below this is a form with a text input labeled 'Type the name of a friend...'.
- Block event invites:** Once you block event invites from someone, you'll automatically ignore future event requests from that friend. Below this is a form with a text input labeled 'Type the name of a friend...'.
- Block apps:** Once you block an app, it can no longer contact you or get non-public information about you through Facebook. [Learn more.](#)

1. Here you can manage all of the people, applications and events that you have blocked on Facebook.

Mobile – Click the ‘Mobile’ tab located in the left column:

1. You will need to enter a mobile number here to enable **login approvals**. If Facebook doesn’t recognize your browser they will send you a code via text message that you must enter to complete the login.

Followers – Click on the ‘Followers’ tab located in the left column:

1. If you enable followers, these people will be able to see all of your public posts.

Apps – Click the ‘Apps’ tab located in the left column:

Search for people, places and things

App Settings

On Facebook, your name, profile picture, cover photo, gender, networks, username, and user id are always publicly available, including to apps (Why). Apps also have access to your friends list and any information you choose to make public.

Apps you use	Use apps, plugins, games and websites on Facebook and elsewhere?	On
	B Bitdefender Safego	Only Me
Apps others use	People who can see your info can bring it with them when they use apps. Use this setting to control the categories of information people can bring with them.	
Instant personalization	Lets you see relevant information about your friends the moment you arrive on select partner websites.	Off
Old versions of Facebook for mobile	This setting controls the privacy of things you post using old Facebook mobile apps that do not have the inline audience selector, such as outdated versions of Facebook for BlackBerry.	Only Me

1. We recommend configuring your App settings as shown above.
2. Don't install questionable third party apps and remove anything suspicious.
3. If you don't use apps at all and have no desire to, then you can totally disable them in the **Apps you Use** settings:

App Settings

On Facebook, your name, profile picture, cover photo, gender, networks, username, and user id are always publicly available, including to apps (Learn Why). Apps also have access to your friends list and any information you choose to make public.

Apps you use

Platform is on.

If you turn Platform off you can't use the Facebook integrations on third party apps or websites. If you want to use these apps and websites with Facebook, turn Platform back on. Using Platform allows you to bring your Facebook experience to the other apps and websites you use on the web and to your mobile device and apps. It allows Facebook to receive information about your use of third party apps and websites to provide you with better and more customized experiences. [Learn more.](#)

If you turn off Platform apps:

- You will not be able to log into websites or applications using Facebook.
- Your friends won't be able to interact and share with you using apps and websites.
- Instant personalization will also be turned off.
- Apps you've previously installed may still have info you shared. Please contact these apps for details on removing this data.

←

B Bitdefender Safego Only Me

4. You'll also want to edit the **Apps others use** setting to keep the applications your friends use from accessing your data:

Apps others use

People on Facebook who can see your info can bring it with them when they use apps. This makes their experience better and more social. Use the settings below to control the categories of information that people can bring with them when they use apps, games and websites.

<input type="checkbox"/> Bio	<input type="checkbox"/> My videos
<input type="checkbox"/> Birthday	<input type="checkbox"/> My links
<input type="checkbox"/> Family and relationships	<input type="checkbox"/> My notes
<input type="checkbox"/> Interested in	<input type="checkbox"/> Hometown
<input type="checkbox"/> Religious and political views	<input type="checkbox"/> Current city
<input type="checkbox"/> My website	<input type="checkbox"/> Education and work
<input type="checkbox"/> If I'm online	<input type="checkbox"/> Activities, interests, things I like
<input type="checkbox"/> My status updates	<input type="checkbox"/> My app activity
<input type="checkbox"/> My photos	

If you don't want apps and websites to access other [categories of information](#) (like your friend list, gender or info you've made public), you can turn off all Platform apps. But remember, you will not be able to use any games or apps yourself.

[Save Changes](#) [Cancel](#)

Ads – Click the ‘Ads’ tab located in the left column and edit these settings to ‘**No one.**’

Facebook Ads

Third Party Sites

Facebook does not give third party applications or ad networks the right to use your name or picture in ads. If we allow this in the future, the setting you choose will determine how your information is used.

You may see social context on third party sites, including in ads, through Facebook social plugins. Although social plugins enable you to have a social experience on a third party site, Facebook does not share your information with the third party sites hosting the social plugins. [Learn more about social plugins.](#)

Ads & Friends

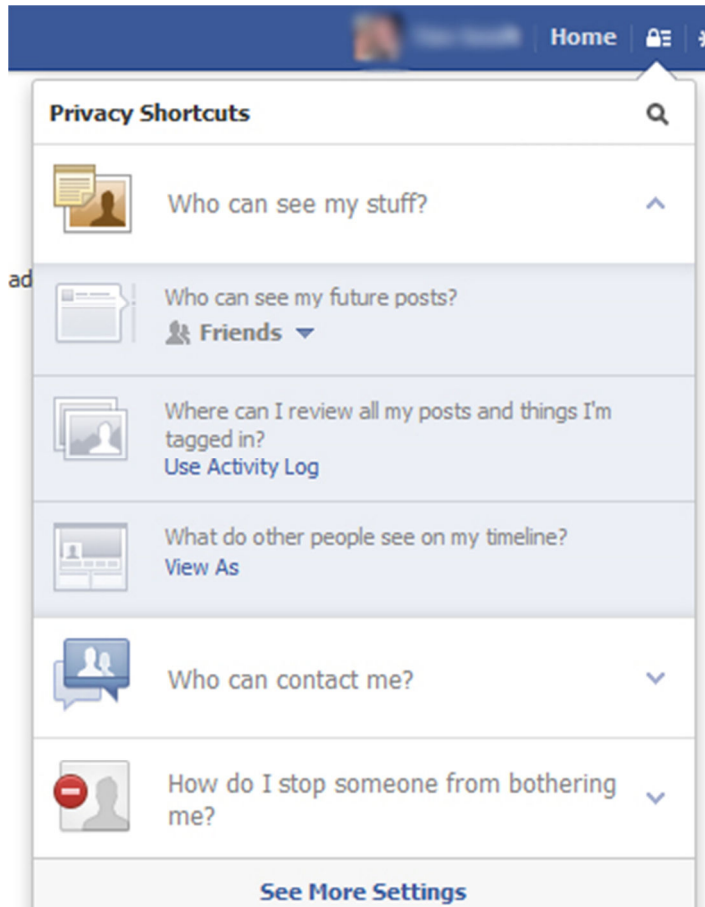
Everyone wants to know what their friends like. That's why we pair ads and friends—an easy way to find products and services you're interested in, based on what your friends share and like. [Learn more about social ads.](#)

Here are the facts:

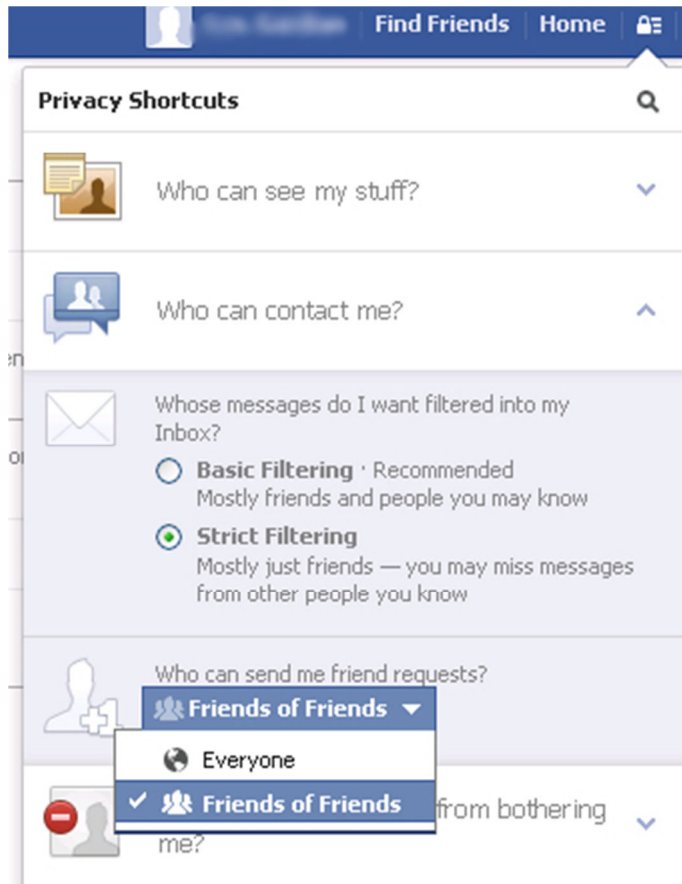
- Social ads show an advertiser's message alongside actions you have taken, such as liking a Page
- Your privacy settings apply to social ads
- We don't sell your information to advertisers
- Only confirmed friends can see your actions alongside an ad
- If a photo is used, it is your profile photo and not from your photo albums

Support Dashboard – This tab shows you the status of anything you have reported to Facebook.

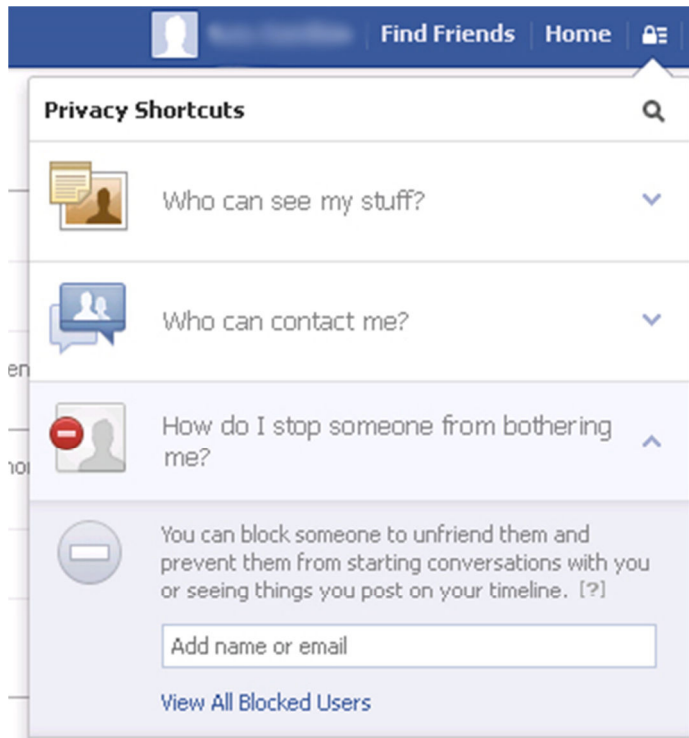
Privacy Shortcuts – Click the Padlock icon in the top right corner for quick access to these settings:



1. Set **Who can see my future posts** to **'Friends.'**
2. Use the **Activity Log** to review items you've been tagged in.
3. If you are ever curious to see how your Timeline appears to others, you can use the **What do other people see on my timeline?** feature.

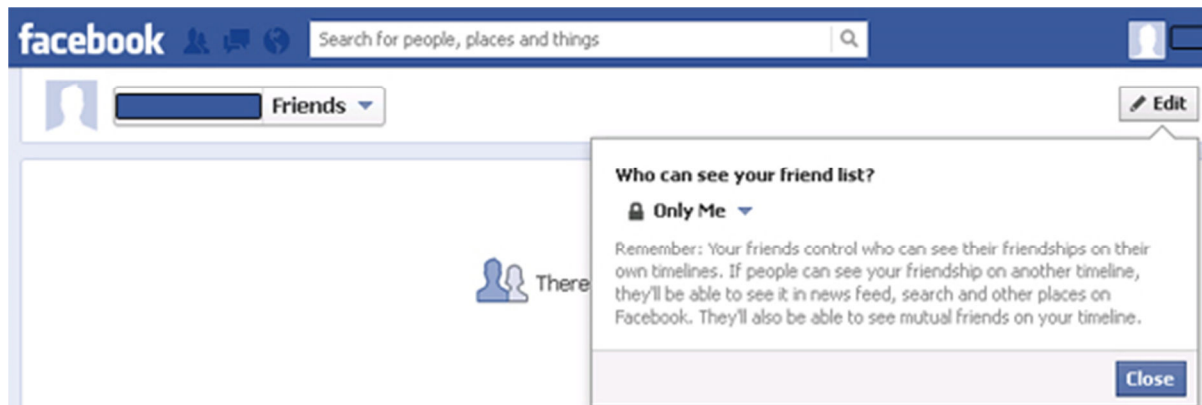


1. Use **Strict Filtering** to limit the amount of spam you receive in your Facebook Messages folder.
2. Determine who you want to be able to send you friend requests – **Friends of Friends** or **Everyone**.



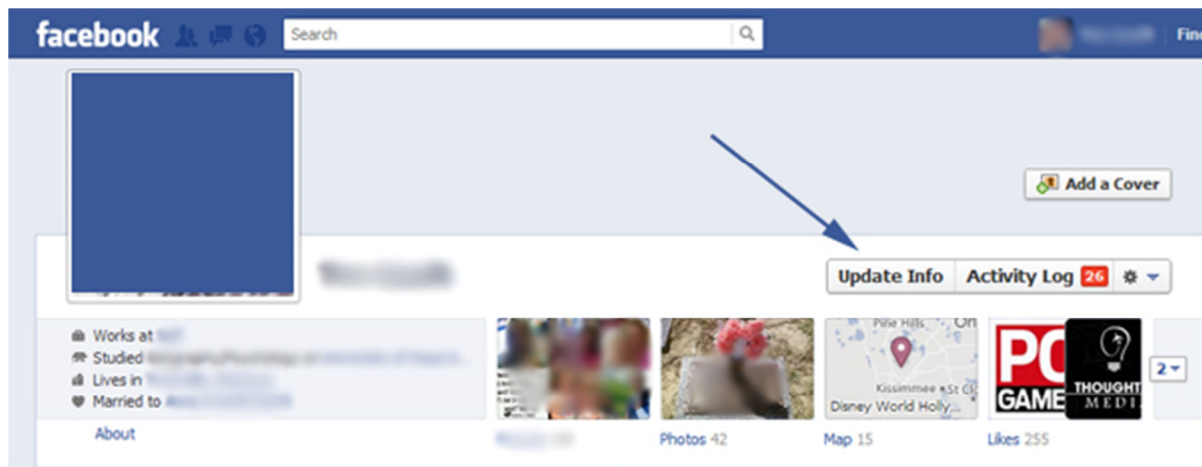
1. You can easily block people from contacting you by adding them here.

Another important setting that is often overlooked is limiting who can see your 'Friends List.' Navigate to your Timeline and click on your 'friends' box or link. Click the Edit button on this screen to access this setting.



1. It is best to set this to **Only Me**. If you have a friend that loses their account to a hacker, this can limit the damage they can do with fake Facebook profiles and the like. *(Always block or unfriend a compromised account until it is reclaimed by your friend.)*

The last section that needs attention is your Timeline profile information. Click on your name in the upper right corner to be taken to your Timeline. Click on the 'Update Info' link on the right side of the page.



1. Edit & Set Sharing Controls for all of the fields here to your sharing comfort level.
 - Only input information that you would be comfortable with the whole world seeing. Even if you set items to just “Friends,” what happens if a friend gets hacked? You don’t want a scammer having access to information that is typically reserved for just your friends.
 - We recommend the following settings
 - Only set items to be shared with ‘Friends’ or ‘Only Me.’ Don’t set anything to Public.
 - Show only the month and day of your birthday on your Timeline or a better option is to not display it at all.
 - Set your mobile phone visibility to “Only Me.”
 - Don’t enter your work or home phone numbers.
 - Do not enter your complete address – (only enter City & State or leave it totally blank)

Parting Thoughts

- **Public Pictures** – Your profile picture and cover photo are public by default, and this setting can’t be changed. If this concerns you, then don’t use a personal photograph. Also, be sure to use sharing controls for your photos and albums.
- **Be careful what you post** – once you post something online it can potentially come back to haunt you. Use the built in sharing controls for status updates and other posts to limit access to the intended audience.
- **Be careful what you click** – Even if all of your controls are set properly, clicking malicious links and installing malware can not only wreck your computer system, but it can affect your privacy and online safety as well.
- **Logout of Facebook** – Facebook has been known to track user activity on other websites, so logout when you are not using Facebook. Also, staying logged in can make it easier for your account to be hacked if you login from shared computers.
- **Anti-virus software** – install a reputable security software application and keep it updated.

Source: <http://facecrooks.com/internet-safety-privacy>