Keeping your FB Account Safe

Disclaimer: This is NOT a perfect solution because”

A. FB keeps changing its settings
B. Hackers keep changing their methods

But, it will reduce the main risks.

The main problem with FB and other popular social websites is that they do not offer a paid subscription. As you know, you get what you paid for and thus there is no such thing as a free lunch. And, this means that for companies which own various social websites, they rely on ads from third parties.

This would not be so bad if said third parties were all squeaky clean and honest. But, alas, many of the ads on FB, for example, are spurious at best. At worst, they are decidedly dodgy.

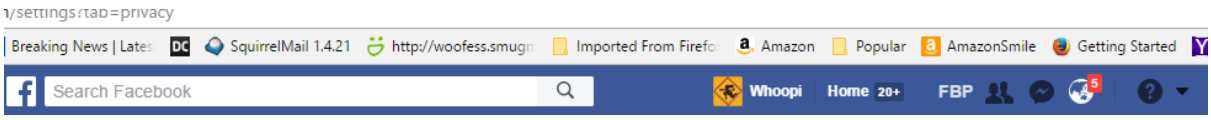
When you sign up for FB or similar and accept the default security/privacy settings, you are very exposed.

To ensure your personal security you need to delve deep into the settings of the software company. This is not easy and certainly not easy in the case of popular social media companies which rely on advertising revenue.

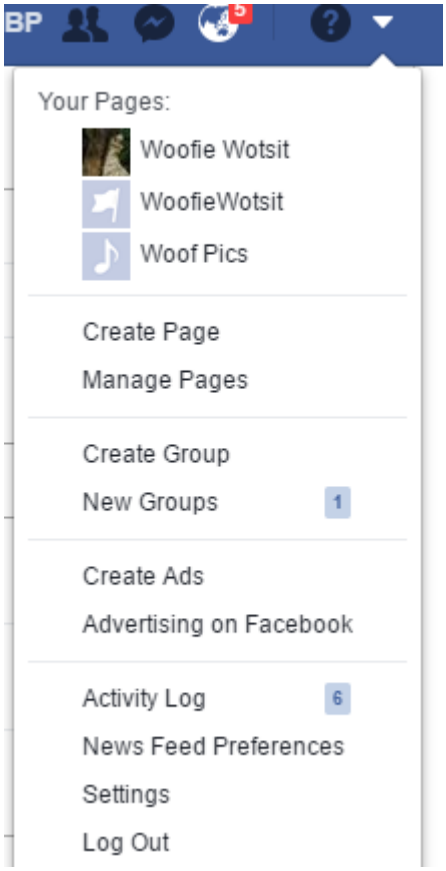
Currently, there are two sections in the FB settings that you need to address:

1. Privacy
2. Security

To access these you need to click on the downward pointing triangle on the far right of your FB screen:

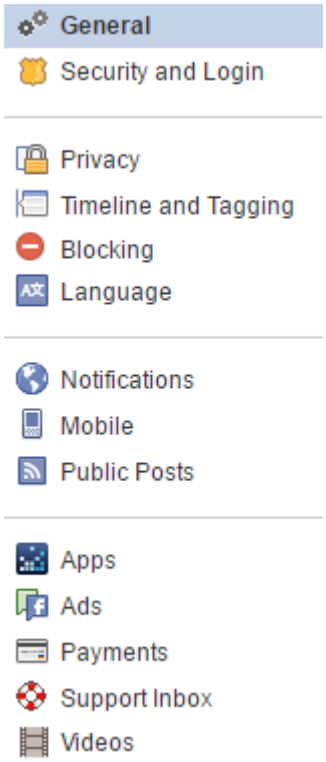


When you click on this, you will get this drop down menu:

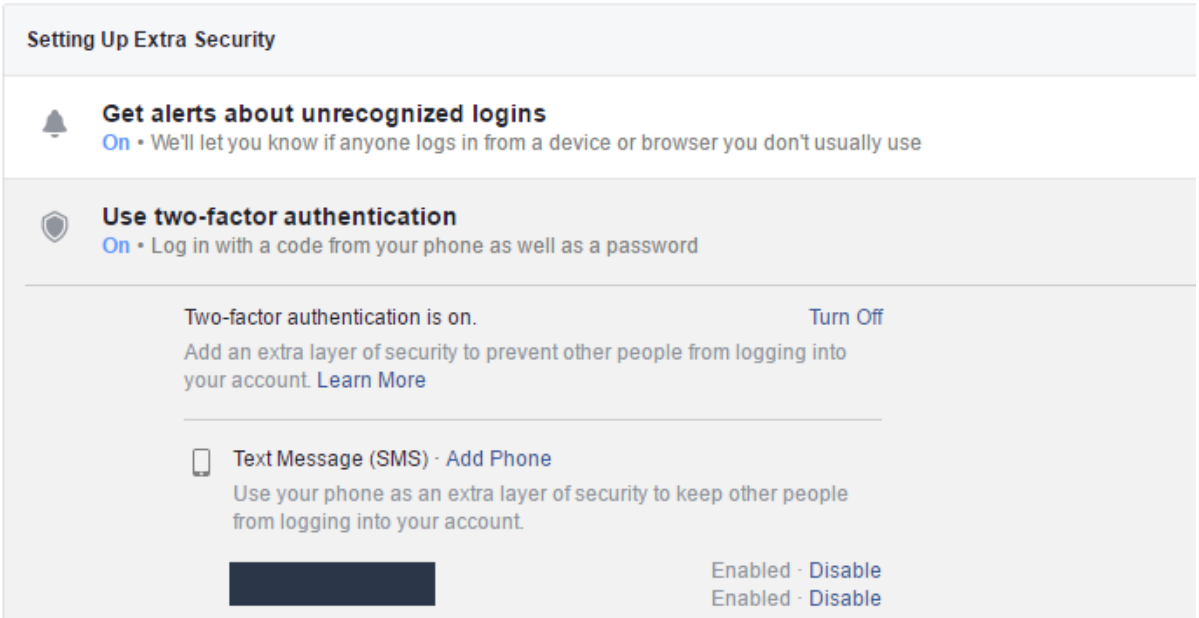


Click on SETTINGS

You will now be presented with the following menu (note that the menu you see may be different from this due to browser variations, but what you are looking for are the menus, SECURITY and PRIVACY.



Under SECURITY AND LOGIN, the main option (in my opinion) is to opt for



And the easiest option for 2 factor authentication is to select the option for an SMS code to be sent to your mobile phone.

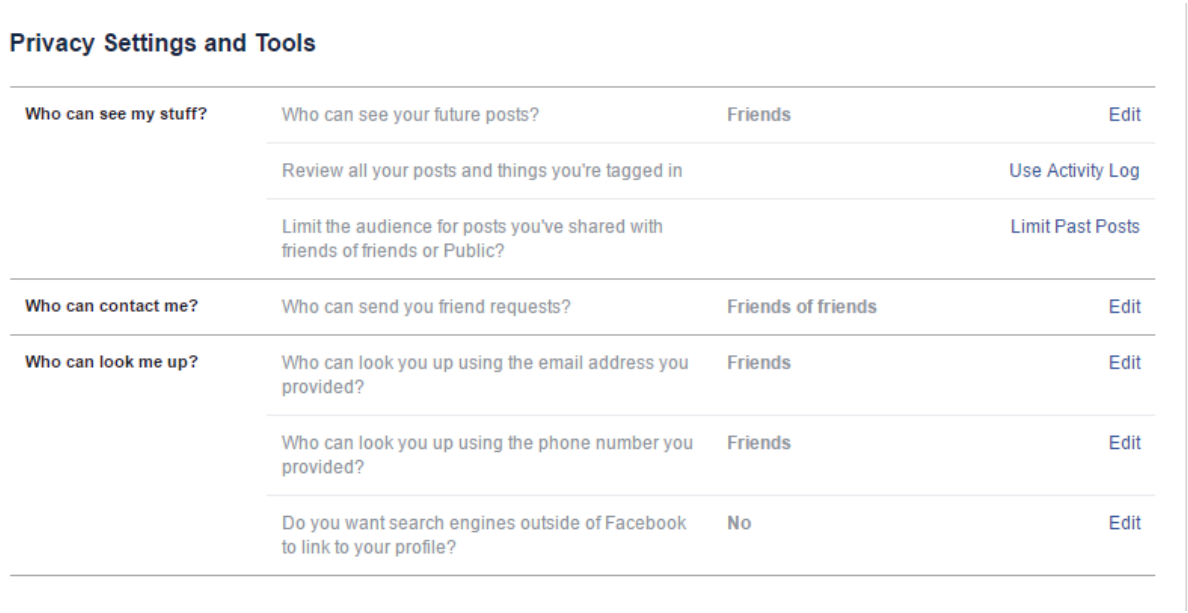
This means that when you create an FB account or modify an existing one (by changing the security sections as per above, or when logging onto your FB account via another browser, or device, you will get an SMS request with a code, which you need to enter into the device you are logged into. This will bugger up most of the scammers, particularly when they decipher your FB account password * see below re passwords.

PRIVACY

The DEFAULT SETTINGS for various social media apps such as LinkedIN, have been traditionally insecure. Often the default setting have been PUBLIC or similar. This means that anyone can see EVERYTHING you write. They also see every time you fart or pick your nose!

This was OK in the old days when the Internet was not commercial, but was, instead, run as an anarchy. But times have changed.

In the PRIVACY sub menu, select these settings:



Privacy Settings and Tools

Who can see my stuff?	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
Who can contact me?	Who can send you friend requests?	Friends of friends	Edit
Who can look me up?	Who can look you up using the email address you provided?	Friends	Edit
	Who can look you up using the phone number you provided?	Friends	Edit
	Do you want search engines outside of Facebook to link to your profile?	No	Edit

OBLITERATING THE CLICK BAIT and other dubious adds

There are browser add-ins for ads and other crap for browsers such as Firefox and Chrome – eg Ad Block. For Microsoft browsers such as EDGE, such plug-ins are not available. Your anti malware product will trap most nasties, but to really stop the FB ads, the best browser plug in is FB Purity.

You can get it here:

http://www.fbpurity.com/

Note that this means you need to access FB via a browser such as Chrome or Firefox and NOT via MS EDGE or the app for iPads etc.

And PLEASE don't be scumbags! Consider donating to them – hey – programmers work hard and should not be expected to work for free!

PASSWORDS

All passwords are hackable!

But here are some suggestions to reduce the risks:

1. NEVER use the SAME password for all your accounts!! Once the hacker has hacked your FB password he/she has the keys to your bank accounts etc etc etc!!!
2. Use COMPLEX passwords – 8 characters or more and a combination of upper case and lower case letters, numbers and special characters such as @ &! – note that what special characters you can use depend on the actual site or application.
3. To make it easier to remember different complex passwords, you can:
    a. Use a system which makes sense to you such as use the same main section of the password such as "I H@te D0gs" and add a different ending for each account, so that FB would be "I H@te D0gs FB" and for Twitter it would be "I H@te D0gs TW".
    b. Use a password manager such as Keepass - http://keepass.info/
    c. Use the password remembering option of browsers such as Firefox or Chrome, so that you only ever have to log into a site with one master password.

OK. Let me know if you need more information on anything.

Woofie ☺

Now to PRIVACY settings.