CENTER FOR INTERNET SECURITY®

How to Secure Your facebook Account

Shehzad Mirza
Director, Security Operations Center
Multi-State Information Sharing and Analysis Center
Center for Internet Security

www.cisecurity.org
@CISecurity

How to Secure Your facebook Account

Social media sites are growing in numbers. These sites provide a great way to collect and share information. These sites are used mainly for keeping in touch with your friends or for networking and building business relationships. Due to the rapid growth of these sites, many hackers are using these sites to their advantage.

Facebook is one of many widely used social media sites. As of January 20, 2013, Facebook reports that there are over one billion users on Facebook, and approximately seven billion people in the world. This means there are one out of seven people in the world on Facebook.

So, what are hackers trying to get? The main goals primarily are to steal financial information, identity theft, or take over your account. The financial motivations are pretty straight forward, but why would they want to take over your account? The idea behind that, by taking advantage of trust you have with your friends, they are able to hijack your account and utilize it for their own purposes.

Facebook provides a great help center that can guide you through many of the above items, as well has the latest security threats seen on Facebook and how to recover a hacked account. Facebook Help has great resources for managing your Facebook account and the various setting that are included with it. This site can be accessed using the following link https://www.facebook.com/help/security.

The intent of this paper is to help end users implement the security features available through Facebook. The purpose of this guide is to provide you with steps that can be taken to not only secure your account, but also maintain some privacy for your account and those with whom you communicate. This document will give a few tips on securing your account by using strong passwords, as well as additional steps for preventing unauthorized access to your account.

Strong Passwords

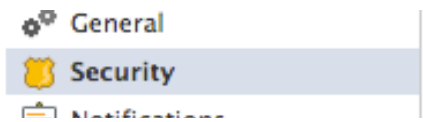
The easiest method of securing your Facebook account (or any account for that matter) is to use a strong password. Exploiting weak passwords are one of the first (and possibly easiest) methods a hacker will take to compromise your Facebook profile. Unfortunately, many users have easy-to-guess passwords, such as 12345, their birthday, favorite sport team, or a pet name. Making sure you have a strong password will help to deter attackers.

Users should consider using the following guidelines:

- A password of 9 or more characters
- Use a complex password consisting of:
  - Numbers
  - Letters – a combination of uppercase and lowercase
  - Special characters
- A password that could not be guessed based on information that someone may know about you
- Change passwords every 60-90 days

Once you have created a strong password, do not use it anywhere else. Also do not share it with anyone.

Facebook Security Settings



Using a strong password is only one line of defense you must use. Given time, any password can eventually be cracked or stolen. This is why you should utilize the security settings in Facebook.

These security settings can be found by clicking on the button that looks like a gear  (found in the top right corner of Facebook) and then clicking on Account Settings.

Here you will be presented with many features. Those features are:

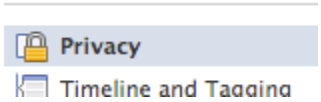
1. **Secure Browsing** – this will force Facebook to use HTTPS. The benefit of utilizing this is to make sure that all traffic to and from Facebook for your account is encrypted. **Recommendation:** Enable this.
2. **Login Notifications** – this will allow Facebook to notify you when your account is accessed from a computer or mobile device that you haven't used before. This is done via email and/or text message (standard text messaging rates apply.) This way you know if someone other than yourself is accessing your account.
   Recommendation: Enable this.
3. **Login Approval** – this will require a security code to access your account from unknown browsers, thus preventing anyone but you from accessing your account. The security code will be sent as a text message to your phone.
   Recommendation: Enable this.
   a. If you cannot receive text messages, then there is an option to set up Code Generator. This will only work if you have the Facebook app on an Android phone or an iPhone.
4. **App Passwords** – this allows you to connect apps to Facebook by using a randomly generated password rather than your Facebook password.

Recommendation: Enable on a case-by-case basis.

5. **Recognized Devices** – this is the list of approved devices that are allowed to access your Facebook account. You won't get notified or have to confirm your identity when logging in from these devices.
   Recommendation: Check this area as often as possible and remove any devices which have a date one week or longer from the current date.
6. **Active Sessions** – this section will provide you with a list of all the devices that are currently or have connected to your Facebook account. The information provided to you is the date last accessed, location of session, the device used, and device type.
   Recommendation: If you notice any unfamiliar devices or locations, click 'End Activity' to end the session.

Privacy

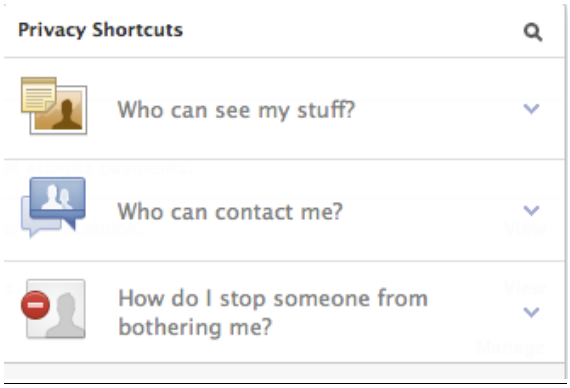
This section allows the user to define some of the privacy settings for your Facebook account.



This section contains two parts:

1. **Who can see my stuff?** – This defines who is allowed to see your wall post by default. **Recommendation:** Restrict to just people you know.
2. **Who can look me up?** – This area allows you to set who is able to see your phone number, email address, and find your timeline by name. This also allows you to define which search engines can link to your timeline.
   Recommendation: Restrict to just your friends and disable search engine links.

This section can be accessed by clicking on the lock icon found on the top right hand corner next to the gear icon. By clicking on this icon, the following will appear:



These are the same options available if you go under account settings or privacy settings.

Timeline and Tagging settings

This section gives you more control on who can add or tag items in your timeline, as well as manages those tags and added items. The sections available here are:

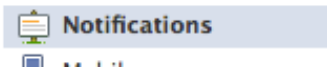
1. **Who can add things to my timeline?** – This section allows you to control which of your friends can add posts or pictures to your timeline.
   Recommendation: Enable the ability to review what is being posted to your timeline by friends. This way you have control on what is being displayed in case your friend's accounts have been compromised.
2. **Who can see things on my timeline?** - This area allows you to test some of your privacy settings. It gives you the ability to view your profile as one of your friends. This area also gives you the ability to define who is able to see posts you have been tagged in and who is able to see what others post on your timeline.
   Recommendation: Visit this capability once every 60 or 90 days, in order to confirm that your security configuration is still in place as you intended.
3. **How can I manage tags people add and tagging suggestions?** – Gives you the ability to review who is able to add tags to your posts.
   Recommendation: Enable this
   This area also lets the user define if photos that are similar or look like you are tagged automatically
   Recommendation: Set this to 'no one'

Blocking

This section allows you to setup a restricted list, which only allows friends to see public information, and to define blocks on users, app invitations, event invitations, and apps.

Recommendation: Add friends to the Restricted list as needed. If you are receiving unwanted messages or constantly receive uninvited requests, block those users or applications.

Notifications

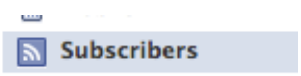


This section defines how notifications are to be sent to you. It is best to receive all notifications on Facebook, but restrict those notifications to email and push notifications on your mobile phone. You do have the option for text messages, but there is a chance you can get overloaded with text messages and go over your plan's limit.

The second part of this section is especially important. Here is where you define what notifications you want to receive.

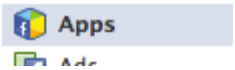
Recommendation: Turn on notifications for any activity that involves you, tags of you, and app requests and activity.

Subscribers



This section will define whether or not you want subscribers to your Facebook posts. Subscribers will only have access to information what is set as public, and not be Facebook friends.
Recommendation: Disable this.

Apps



The Apps sections will display what third party applications have access to your Facebook profiles. Many apps can post on your behalf, or access some of your personal information. There are four sections in this area.

1. **Apps you use** - If you click on 'Edit', it will tell you what the applications are capable of doing with your Facebook profile. This part also provides an option called 'Platform' to allow applications or websites to use your Facebook account to login. If you turn Platform off you can't use the Facebook integrations on third party apps or websites.
   Recommendation: Check this section often, and make sure that only apps you have allowed are accessing your Facebook profile. If there are applications that you are not sure of or have not been used for more than a month, remove them from the list by clicking on the 'x' at the end of the column.
2. **Apps others use** – This part defines what information people on Facebook can see about your profile and can bring it with them when they use apps.
   Recommendation: Do not allow any information to be used.
3. **Instant personalization** – This will personalize your experience with certain websites if you allow your Facebook account to be used for login, such as immediately playing the music you like or displaying friends' reviews.
   Recommendation: Keep this turned off.
4. **Old version 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.
   Recommendation: Set to "Friends Only".

Ads

This is the most important section for privacy in Facebook. Here is where you can define how Facebook will use your profile with Third Party sites, Advertisements, and Friends.

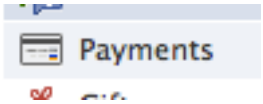
The following disclaimer is found under Third Party Sites:

> 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.

However, you still need to set how Facebook should handle the above in case anything changes in the future, and how Facebook should show your information. **Recommendation:** Set to "No One."

Payments

The Payments section under account settings will show you all the Facebook credits you may have earned via games or other applications. This is also the section that may have your credit card information.



Recommendation: Do not store your credit card information on Facebook, even if you are not making any purchases. If you have in the past, it is recommended that you remove it.