A guide to Facebook security settings

Facebook, Social Media — By Matthew Tommasi on April 19, 2009 at 7:23 pm

ID fraudsters target Facebook and other social networking sites to harvest information about you. I recommend you set the following Facebook privacy options to protect against online identity theft.

Facebook walkthrough – adjust your privacy settings

This guide walks you through my privacy settings in Facebook, and shows you how to set more secure levels of privacy and reduce the chance of becoming a victim of online identity theft.

* Profile

Control who can see your profile and personal information.

* Search

Control who can search for you, and how you can be contacted.

* News feed and wall

Control what stories about you get published to your profile and to your friend’s News Feeds.

* Applications

Control what information is available to applications you use on Facebook.

General safety tips for Facebook

Adjust Facebook privacy settings to help protect your identity

Unlike some other social networking sites, Facebook has provided some powerful options to protect you online – but it’s up to you to use them!

Think carefully about who you allow to become your friend

Once you have accepted someone as your friend they will be able to access any information about you (including photographs) that you have marked as viewable by your friends. You can remove friends at any time should you change your mind about someone.

Show “limited friends” a cut-down version of your profile
You can choose to make people ‘limited friends’ who only have access to a cut-down version of your profile if you wish. This can be useful if you have associates who you do not wish to give full friend status to, or feel uncomfortable sharing personal information with.

Disable options, then open them one by one

Think about how you want to use Facebook. If it’s only to keep in touch with people and be able to contact them then maybe it’s better to turn off the bells and whistles. It makes a lot of sense to disable an option until you have decided you do want and need it, rather than start with everything accessible.

Profile privacy settings

Facebook has provided users with powerful controls to protect themselves online, and it is up to individuals to check and ensure that appropriate settings are in place. Sophos has published recommendations for how to configure the settings for each of these privacy areas of Facebook.

Profile

My recommended Profile settings:

Basic
Why:

Profile:

By default, Facebook allows all of your networks and all of your friends to be able to view your profile. As networks can contain hundreds of thousands of people (and you have no control over who else joins the network), you are instantly revealing personal information to potential identity thieves if you leave this option at its default setting.

It is sensible only to allow your profile to be viewed by your friends, so you should set this option to: “Only my friends”.

Basic Info:

Unless you want hundred’s of thousand of people seeing your basic information, then it is best to set this option to: “Only my friends”.

Personal Info:

Unless you want hundred’s of thousand of people seeing your personal information, then it is best to set this option to: “Only my friends”.

Status Updates:

As you may change your status to say “Going to hospital for surgery in three days”, or “On holiday down south until September 2!” (which may be useful information for criminals) it makes sense not to make your status available to anyone other than approved friends. You should not make it viewable by your networks. Non-friends do not need to know what you are doing minute-by-minute.

Photos Tagged of You:

Photos and videos should only be shared with friends, not with wider networks on Facebook. If photos and videos may be posted that you think may in the future be embarrassing to you, then tag this option to say only you can view them and ask yourself what can be done to prevent such material being uploaded onto the internet in future. If you are not comfortable with material appearing on your resume or job application then don’t post it online.

Videos Tagged of You:

Photos and videos should only be shared with friends, not with wider networks on Facebook. If photos and videos may be posted that you think may in the future be embarrassing to you, then tag this option to say only you can view them and ask yourself what can be done to prevent such material being uploaded onto the internet in future. If you are not comfortable with material appearing on your resume or job application then don’t post it online.

Friends:

Only your friends should be allowed to view who your other friends are. Giving unknown members of the Facebook community access to your friends list may provide them with additional data about you, which could assist them in identity fraud – especially if your friends have not been as careful as you in securing your privacy online.

Wall Posts:

Personal information can be published on your wall by yourself and others, therefore it is unwise for it to be viewable by the wider Facebook community. For this reason, you should not allow networks to view your wall.

Education Info:
Only your friends should be allowed to view your education information. Giving unknown members of the Facebook community access to your education info may provide them with additional data about you, which could assist them in identity fraud.

Work Info:

Only your friends should be allowed to view your work information. Giving unknown members of the Facebook community access to your work info may provide them with additional data about you, which could assist them in identity fraud.

Photo Album Privacy Settings:

Photos and videos should only be shared with friends, not with wider networks on Facebook. If photos and videos may be posted that you think may in the future be embarrassing to you, then tag this option to say only you can view them and ask yourself what can be done to prevent such material being uploaded onto the internet in future. If you are not comfortable with material appearing on your resume or job application then don’t post it online.

Contact Information
Why:
IM Screen Name / Mobile Phone / Other Phone / Current Address:

It is recommended that these privacy options are set to “No-one”. Users who are completing their profile on Facebook should ask themselves whether it is appropriate or necessary to tell other Facebook users their contact details. Facebook allows users to opt-out of entering this personal information, and as Facebook allows friends to contact each other via Facebook it is not necessary to know someone’s real address or phone number. If they really are a friend they should know where you live and what your phone number is! And if a friend really can’t remember they can always contact you via Facebook and ask you. It’s then up to the user to decide whether they feel comfortable sharing that information, and if their friend has a valid reason for asking.

Website:
The publishing of a personal website address is less of a privacy risk than revealing other contact information, providing other private information is not listed on the personal website itself.

Contact Email Address:

It is not necessary to know a friend’s real email address via Facebook as it is possible to send a message to friends via the system itself.

Search

My recommended Search settings:

Privacy > Search

Search Discovery
Use this setting below to control who on Facebook can find you through search. Your friends will always be able to find you.

Search Visibility
Friends of Friends

Search Result Content
Use these checkboxes to control what people can see about you, and how people can contact you after finding you in search.

People who can see me in search can see:

- My profile picture
- My friend list
- A link to add me as a friend
- A link to send me a message
- Pages I am a fan of

In addition to the people selected above, allow the following people to find you in search results:

- People in college networks
- People in high school networks
- People in company networks
- People in regional networks
- People with no networks

Save Changes  Cancel

Why:

Search Visibility:
Be careful with this setting. If you are a member of a network and select this option then you are opening your profile up to potentially thousands of people.

My Profile Picture:

You will probably want to post a picture of yourself so people can tell you apart from the 190,000 other “John Smith”s online. However, be sure to choose a picture that you would not be embarrassed for a future employer to see. If it’s not a picture you would be comfortable to share – don’t use it online!

My Friend List:

Be careful with this setting. By selecting this option you are allowing the public to view your friend’s list.

Add you as a friend:

If you want people to connect to you (rather than you with them) then you will need to leave this option enabled. However, always exercise great caution before accepting somebody’s friend request.

Send you a message:

If you respond to a message sent to you by someone that you have not set up to be your friend then you are allowing them to view your profile information for a period of time. The more security conscious, therefore, would be wise to only allow their friends to send them a message them.

News Feed and Wall

My recommended News Feed and Wall settings:
Why:

News Feed and Wall:

It is recommended users leave all of these options disabled unless it is important to share the information with your friends.

Users can choose here what information gets shared via feeds with their friends. Users who do not wish their friends to see what they have posted on discussion boards, or as comments on other people’s photos and videos, may wish to disable the relevant options.

Social Ads:

It is recommended to disable this option as it may lead to potential identity theft. There is no real need to be appearing in social ads.
Applications

My recommended Applications settings:

![Applications Settings](image)

**What Other Users Can See via the Facebook Platform**

When a friend of yours allows an application to access their information, that application may also access any information about you that your friend can already see. Learn more.

You can use the controls on this page to limit what types of information your friends can see about you through applications. Please note that this is only for applications that do not use Facebook IDs.

- **Share my name, networks, and list of friends, as well as the following information:**
  - Profile picture
  - Bio, info, and notes
  - Personal info, activities, interests, etc.
  - Current location (what city I'm in)
  - Education history
  - Work history
  - Profile status
  - Wall
  - Notes
  - Groups I belong to

- **Do not share any information about me through the Facebook API.**

**Applications Authorized to Access Your Information**

When you authorize an application, it can access any information associated with your account that it requires to work. Contact Information is never shared through Platform. You can view a full list of applications you have authorized on the Applications page.

**Facebook Connect Applications**

Facebook Connect is a way to use applications outside of Facebook. You can take your Facebook profile information all over the Internet, and send interesting information back to your Facebook account.

When your friend connects a Facebook account with an application outside of Facebook, they will be able to compare their Facebook Friend List with information from that website in order to invite more friends to connect.

- **Don't allow friends to view my memberships on other websites through Facebook Connect.**

**Beacon Websites**

- **Don't allow Beacon websites to post stories to my profile.**

**Blocked Applications**

You've blocked the following applications. These may have access to any information you or your friends allow, but they may not appear on your friends' profiles. If you want to restore the block for any of these applications, click remove.

- **You have not blocked any applications.**

**Friends Application Invites**

You can ignore all application invites from specific friends. This option is available from the Requests page. You can remove people from this list at any time using the link next to their name.

- **You have not restricted any users.**

**Why:**

Facebook allows you to add extra third party applications to your profile. These have a wide array of uses including giving you a weather forecast, allowing you to doodle graffiti on another person’s wall, or telling people who your top friends are.

Users should exercise care over which applications they add to their profile as information can be shared with the application’s author. Facebook has published terms of service to inform developers of what is and is not acceptable behavior, but there is always the danger that people will abuse the ability.
Two commonly used applications supplied by Facebook are the facilities for sharing photos and notes with friends:

Privacy settings for Photos:

With these options you can choose which of your photo albums you want to share with which users. As a minimum, it is recommended that photo albums are only shared with friends. Always consider that material you post on the internet may end up in someone else’s hands – if the material is likely to embarrass you later think twice about posting it online!

Privacy settings for Notes:

Facebook users can post Notes on their page. You can allow everybody on Facebook to read your Notes, but it is recommended that as a minimum you limit visibility of your Notes to just your friends.

Syndication allows other Facebook members to subscribe to an RSS feed containing your Notes. Most users probably do not need to enable such an option, and it can be left disabled.

I hope this guide has been of some use, enjoy!

Tags: configure, configuring, facebook, guide, how, instructions, security, settings, setup

- Tweet This
- Digg This
- Save to delicious
- Stumble it
- RSS Feed

Add New Comment

You are commenting as a Guest. You may select one to log into:
This is a bit paranoid. I'd suggest using friend lists for more fine-tuned privacy control. For example, it makes sense to share your contact info to 'trusted' friends as more mobile devices can sync to your facebook account and get all your contact info.