Info security

You are the key!

Social Media: Important things you (maybe) never knew but you need to consider

It’s hard to ignore Social Media; from Twitter to Facebook, via Snapchat, there are different types that all address a different need so this guide is intended to let you know the fundamentals and, hopefully, make you aware of things you can do, right now, to make you, and others, more secure.

1. Don’t post Yours or Your Family Member's Full Birth Dates

Getting a “happy birthday” from our friends on our Facebook wall makes us feel all special knowing that people remembered and cared enough to write us a short note on our special day. The problem is when you list your full birthday you are providing identity thieves with one of the 3 or 4 pieces of personal information that is needed to steal your identity. If you really must list it, at least leave out the year - your real friends should know this info anyway.

2. Your Relationship Status

Whether you are in a relationship or not, it may be best not to make it public knowledge. If you change your status to "single" it lets people know that you might be home alone since your significant other is no longer around.

The best thing to do? Just leave this blank on your profile unless you really need to announce it.

3. Your Current Location

There are a lot of people who love the location tagging feature on Facebook that allows them to let people know where they are 24/7. The problem is that you have just told everyone that you're on vacation (and not at your house). If you add how long your trip is then thieves know exactly how much time they have to rob you.

My advice is not to provide your location at all. You can always upload your holiday pictures when you get home or text your friends to let them know how jealous they should be that you're sipping an umbrella drink while they toil away at work.

4. The Fact That You Are Home Alone

It is extremely important that you never put the fact that you are home alone in their status; you wouldn't walk into a room of strangers and tell them you are going to be 'all alone at your house' so don't do it on Facebook either.

We may think that only our friends have access to our status, but we really have no idea who is reading it. Your friend may have had their account hacked or someone could be reading over their shoulder at the library.

The best rule of thumb is not to put anything in your profile or status that you wouldn't want a stranger to know. You may have the most stringent privacy settings possible, but ***if your friend's account gets compromised than those settings are meaningless.***

5. Pictures of Your Kids Tagged With Their Names

We love our kids. We would do anything to keep them safe, but most people post hundreds of tagged pictures and videos of their kids to Facebook without even giving it a second thought. We even go so far as to replace our profile pictures with that of our children.

9 out of 10 parents posted their child's full name, and exact date and time of birth while they were still in the hospital after delivery. We post pictures of our kids and tag them and their friends, siblings, and other relatives. This kind of information could be used by predators to lure your child. They could use your child's name and the names of their relatives and friends to build trust and convince them that they are not really a stranger because they know detailed information that allows them to build a rapport with your child.

If you must post pictures of your children then you should at least remove personally identifying information such as their full names and birth dates. Untag them in pictures. Your real friends know their names anyway.

Lastly, think twice before you tag pictures of the children of friends and relatives. They might not want you tagging their kids for the reasons mentioned above. You can send them a link to the pictures and they can tag themselves in place of their children if they want to.

6. Don't put any details about work or details of what you are working on

It's a personal profile for a reason; unless it's a WCC social media account (that has to contain details to communicate with the public) then try and refrain from posting anything that could have repercussions for both you and WCC. Examples include:

"Having a large glass of wine to de-stress after visiting nightmare family on Accaccia Avenue today"

“Getting quite down working on the WCC Widget Project – all those people affected”

As well as statements such as those, just remember the golden rule of social media interaction – whatever you write can be misinterpreted and words twisted to match someone else’s agenda so just don’t post about work.

7. Not all websites seem like social media – but they are!

Internet dating, as an example, used to be a fairly innocent process; you posted a pic and an honest profile and then looked for someone similar.

Not now – a lot of these sites are now open to fraud, phishing and scams as they have become akin to a social media service and there are a lot of pitfalls.

Scams where pics of the toned and beautiful (who aren’t real) are asking you to click here, join this, send money, fill in this short questionnaire, etc before I can send you a message or make contact are rife and you need to always be aware when using a site.

Remember this: if something is too good to be true, it usually is; that video of Beyonce in a car crash “Live footage!!!” is designed to make you click on things you shouldn’t.

Use your instinct, as it’s typically right!

Locking down your Facebook Profile

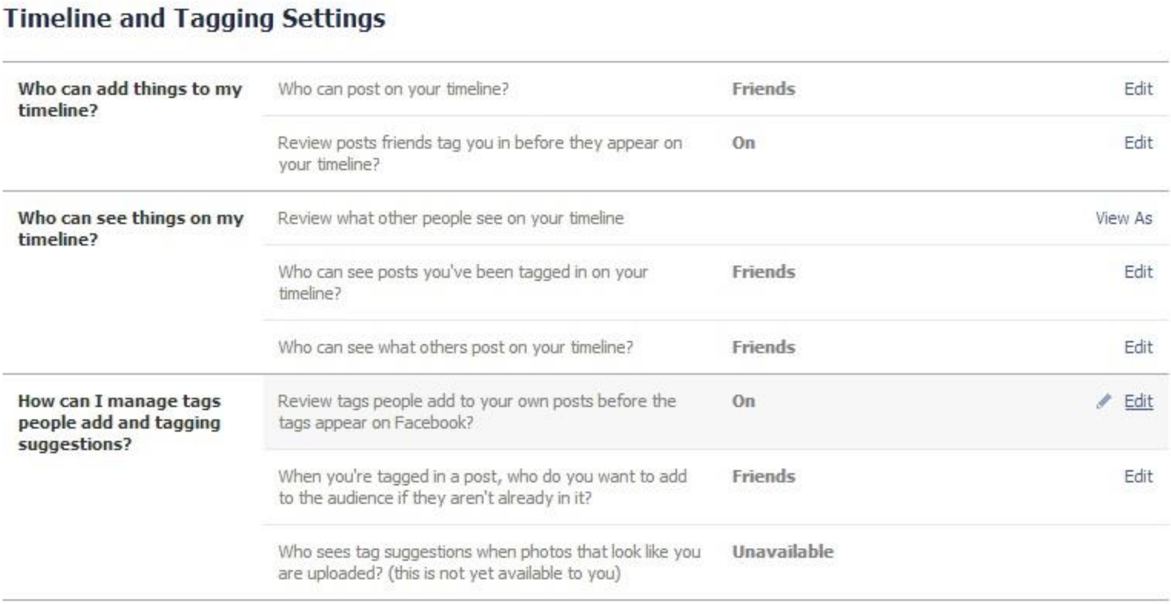
Tagging

Ah, isn’t that sweet – a relative has just posted (and tagged) a picture of you on Facebook from when you were young wearing that rather loud Xmas jumper. All your Facebook friends can see it..how embarrassing…

Now, imagine if I replace the photo with a one where you were slumped over in the kebab shop after a particularly heavy night..still just embarrassing? Or if that photo gets sent to everyone, is there anyone on your Friends list that it might offend? A work colleague? A manager?

How about a series of photos like that? Fun at the time but you don’t want it causing you issues now or in the future.

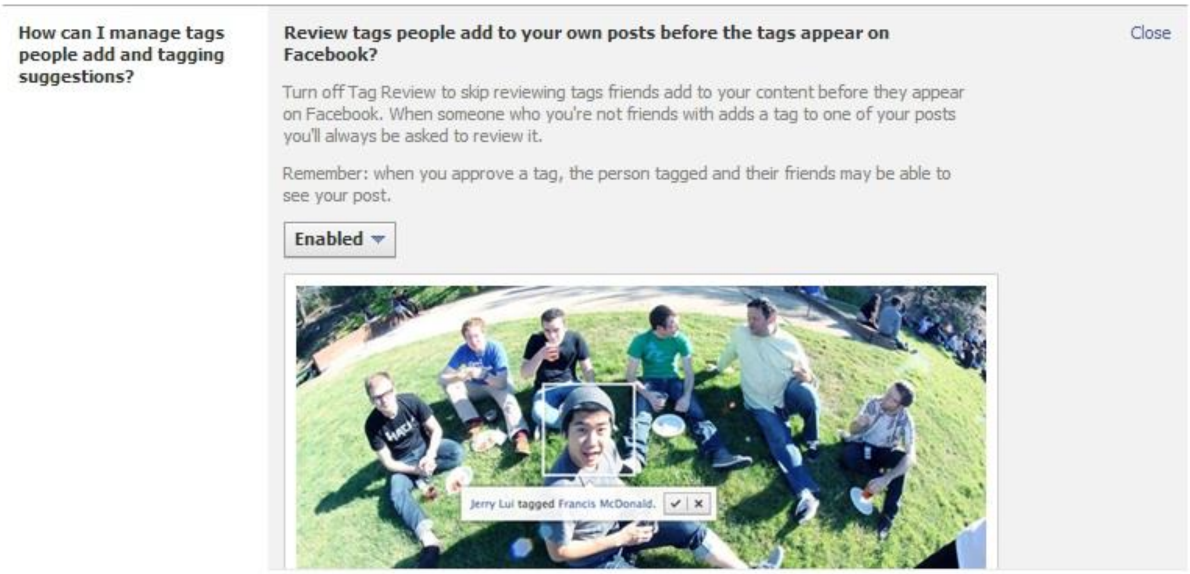
Well, in Facebook, there’s a way of reviewing any tagged photos; in the Privacy Settings, there is an entry called ‘How Can I manage tags people add and tagging suggestions’



Timeline and Tagging Settings

Who can add things to my timeline?	Who can post on your timeline?	Friends	Edit
	Review posts friends tag you in before they appear on your timeline?	On	Edit
Who can see things on my timeline?	Review what other people see on your timeline		View As
	Who can see posts you've been tagged in on your timeline?	Friends	Edit
	Who can see what others post on your timeline?	Friends	Edit
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	Edit
	When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	Friends	Edit
	Who sees tag suggestions when photos that look like you are uploaded? (this is not yet available to you)	Unavailable	

And then you click on '**Review tags people add to your own posts before the tags appear on Facebook**' and make sure it is set to '**Enabled**'.



How can I manage tags people add and tagging suggestions?

Review tags people add to your own posts before the tags appear on Facebook?

Turn off Tag Review to skip reviewing tags friends add to your content before they appear on Facebook. When someone who you're not friends with adds a tag to one of your posts you'll always be asked to review it.

Remember: when you approve a tag, the person tagged and their friends may be able to see your post.

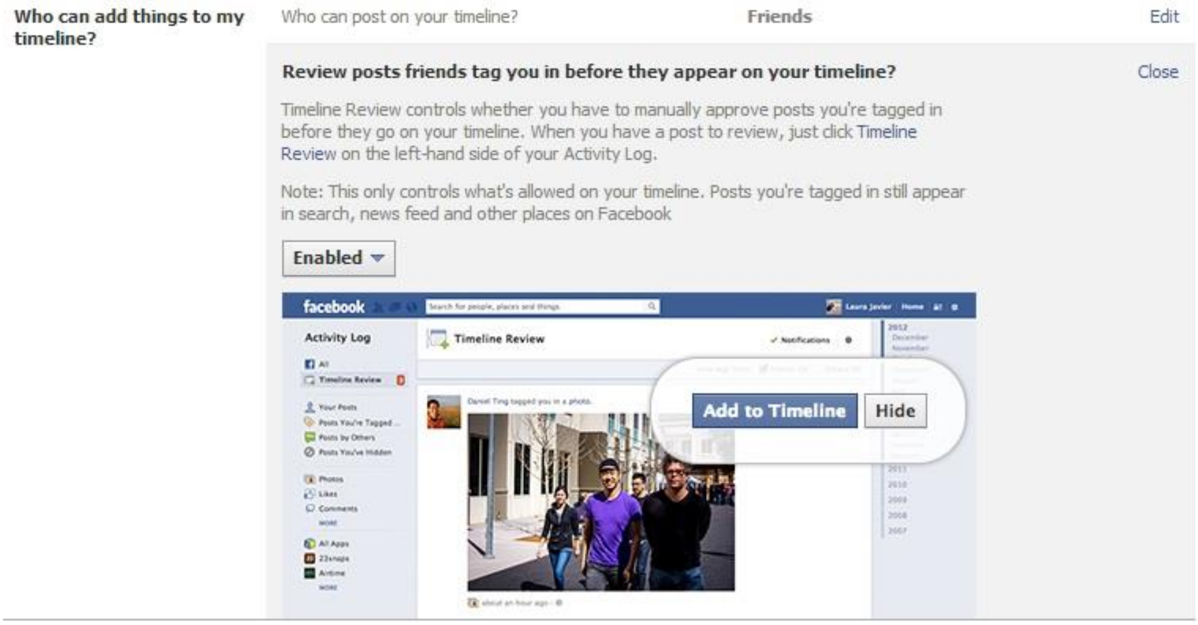
But what about tagging your name?

'Out for a nice walk – with Joe Bloggs '

..seems perfectly innocent but what if you were supposed to be somewhere else? Did you provide an excuse to someone who can now see on Facebook you wanted to go for a walk instead?

How about ' Tequila drinking completion – 11 in and Joe Bloggs is on fire!'

Do you really want all your Facebook friends to see what you're up to? Maybe you do but, if you care about your privacy and being able to control who sees what, then you also need to review who can tag your name:



Who can add things to my timeline? Who can post on your timeline? **Friends** Edit

Review posts friends tag you in before they appear on your timeline? Close

Timeline Review controls whether you have to manually approve posts you're tagged in before they go on your timeline. When you have a post to review, just click Timeline Review on the left-hand side of your Activity Log.

Note: This only controls what's allowed on your timeline. Posts you're tagged in still appear in search, news feed and other places on Facebook

Enabled ▾

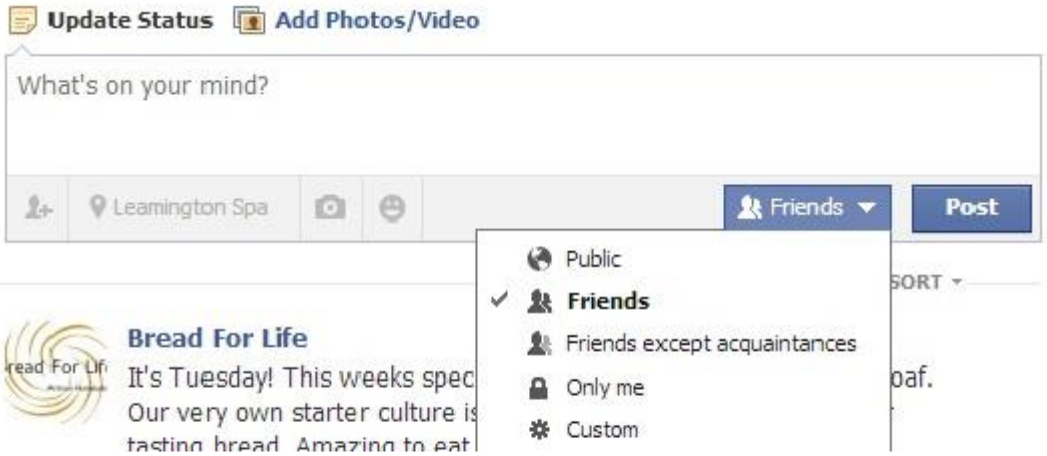
Why is this important?

Ideally, you want to be able to trust your friends; but with the average user having 229 Facebook 'Friends', you'd have to ask how many of them you could actually trust. Having the ability to review what is being said and posted, using your name, provides you with reassurance that you have a chance to look at it before everyone else does.

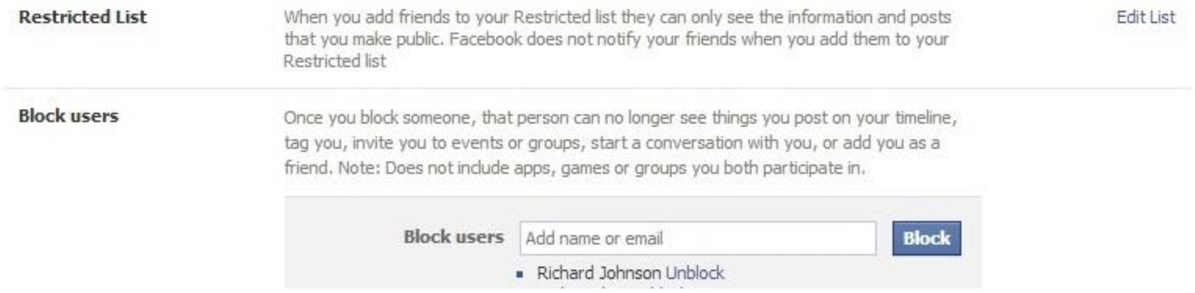
Some untrustworthy individual could cause you problems with everyone else you know on Facebook – just be careful.

Posting on Facebook

Take a look at that status update you're about to write:



See that list there when you click on the button next to 'Post'? It gives you a chance to limit who can see it so that it's not available to the whole world. It doesn't take away the risk that someone could 'share' but it certainly provides a good start.



Restricted List

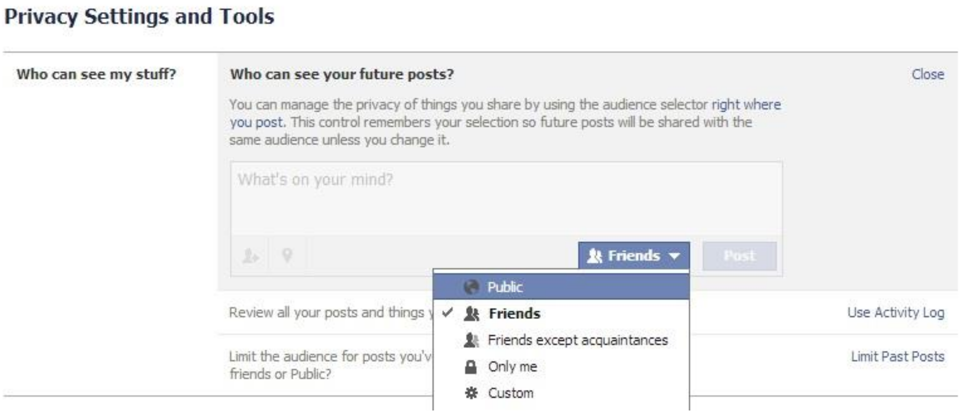
When you add friends to your Restricted list they can only see the information and posts that you make public. Facebook does not notify your friends when you add them to your Restricted list

Block users

Once you block someone, that person can no longer see things you post on your timeline, tag you, invite you to events or groups, start a conversation with you, or add you as a friend. Note: Does not include apps, games or groups you both participate in.

Also, if you do have 236 Facebook Friends, decide who your 'core' friends are that you can really trust and then consider adding people you're not totally sure about to a restricted list; people in this list can only see what you make public.

You can also change these default settings in the Privacy area.



Privacy Settings and Tools

Who can see my stuff?

Who can see your future posts?

You can manage the privacy of things you share by using the audience selector right where you post. This control remembers your selection so future posts will be shared with the same audience unless you change it.

Review all your posts and things y

Limit the audience for posts you'v friends or Public?

Geotagging

Would you go out and leave your front door open?

No? Why not? Is it because you want some sort of security and privacy that people can't peer in and see if you've got anything worth stealing?

How about standing up in a public area and telling everyone your address and saying you won't be home for the next 3 hours and there's no-one home?

If you don't do these things, why on earth would you do it online?

On every status update is the ability to tell people exactly where you are; what about our example where the person isn't going to home for another few hours?

How about this one?

'Off on sunshine holiday for 2 weeks – cat with friend..starting with a lovely meal! – Tagged at Gordon Ramsey's Restaurant at Terminal 5'

Blimey! Some nice bragging there; unfortunately, with you listing personal details on Facebook and not securing them, you've just told the whole audience that you're not there for 2 weeks. Potential burglars can now schedule when they are available to rob your house – thank you for that!

Turn it off and turn off other users' ability to geo-tag you with your name; remember, you need to control what other people do too.

Electoral Register (formerly the Electoral Roll) & other Internet Information Providers

Sorry for this next bit – it's a bit dry but it's very important.

The law makes it compulsory to provide information to an electoral registration officer for inclusion in the full register. The details you are likely to have to provide are your name, address, national insurance number, nationality and age.

The full register is published once a year and is updated every month. It is used by electoral registration officers and returning officers across the country for purposes related to elections and referendums. Political parties, MPs and public libraries also have the full register.

Opting out

Some people may already be opted out of the open register - if you had opted out at the point of the last household electoral registration your preference will have been noted and carried forward with the introduction of individual electoral registration.

If you are not already opted out but want to prevent your personal details on the electoral register from being made more widely available, you can make a request at any time to your local electoral registration officer for your details to be removed. Your request needs to contain your full name and address and can be in writing, via email or phone.

Other information lookup websites

Sites such as 192.com, can provide services to look up and you can also apply to them to have your details removed but be aware:

- Sites like these get your details from your telephone, mobile providers and others so the most important thing to remember is:

WHENEVER APPLYING FOR ANYTHING, ONLINE OR PAPER BASED, ALWAYS READ WHAT THEY PLAN TO DO WITH YOUR INFORMATION AND ALWAYS OPT-OUT (IF POSSIBLE) IF YOU ARE WORRIED OR CONCERNED.

The question you need to ask: *Who do you trust with your data?*