

A Complete Guide to Web, Facebook, Twitter, and Google Plus Privacy and Security!

TheEdublogger.com

A Complete Guide to Web, Facebook, Twitter, and Google Plus Privacy and Security!

The digital landscape has changed dramatically in the last few years. The *Web 2.0 revolution* brought with it the ability for everyone to create content on the web at rates I can't imagine anyone ever thought possible.

So what does all of this mean?

We all have a **digital footprint** - a permanent record of where we have been and what we have done on the interwebs.

It is a good idea to regularly do a health check of that digital footprint. So here is a list, as short as could be and still remain thorough, that should help ensure everything is on the up and up.

This is especially important for educators and other professionals that have others "googling" them to learn more about them.

Contents

Start With A Google Search	3
1. Name Search - "Your Name"	3
2. Email Address Search	3
3. Home Address Search	3
4. Phone Number Search	3
5. Set up Custom Alerts	3
Facebook Privacy Checks.....	4
6. Check Your Personal Profile	4
7. Check What Friends See.....	5
8. About Friend Lists.....	5
9. Review All Photos.....	5
10. Removing Old Apps.....	5
Twitter Needs Checking Too!.....	7
11. Review Profile Information.....	7
12. Double Check Private Tweets	7
13. Check DMs and Feed For SPAM	7
14. Clean Out Twitter Applications	8
Google and Google Plus	9
15. Check Public Profile	9
16. Review Privacy Settings	9
17. Review Photos.....	10
Miscellaneous Tasks.....	11
19. Blogs and Other Web Media	11
20. Browsers and Advertising.....	11
21. Passwords	11
Checklist	12
Keep In Touch.....	13

Start With A Google Search



Before digging into specific sites and applications, we'll turn to our favorite search engine (most likely Google but could be something like Bing).

If something comes up that you didn't know about, or want to remove, try looking for contact information on the site and put in a request.

If you really find something you don't like and can't find contact information for a site, try visiting whois.net to see who owns the domain name - often contact information is available there.

1. Name Search - "Your Name"

Do a search for your name. Put your name in quotation marks to avoid extra results that aren't really relevant.

Be sure to try different variations - including your full name, nicknames, etc.

2. Email Address Search

Search for each of your email addresses that you have used. Spam filters are getting better, but having your email address available on the web is a huge reason why your inbox might be filling up.

3. Home Address Search

If you own a home, it might be a local law that your contact information, name and home address is published online - along with your tax bill! You might not be able to remove everything here, but it is always good to know what personal information about yourself is out there and publicly available.

4. Phone Number Search

This will help make sure your phone number only appears where you might want it to.

5. Set up Custom Alerts

Be sure to set up [Google Custom Alerts](#) to get an email notification whenever your name, email address, phone number, or anything really is added to their searched sites.

Using quotation marks around the information when you put it in can help ensure you don't get email alerts when people that have your first name are mentioned with someone else that has your last, for example.

Facebook Privacy Checks



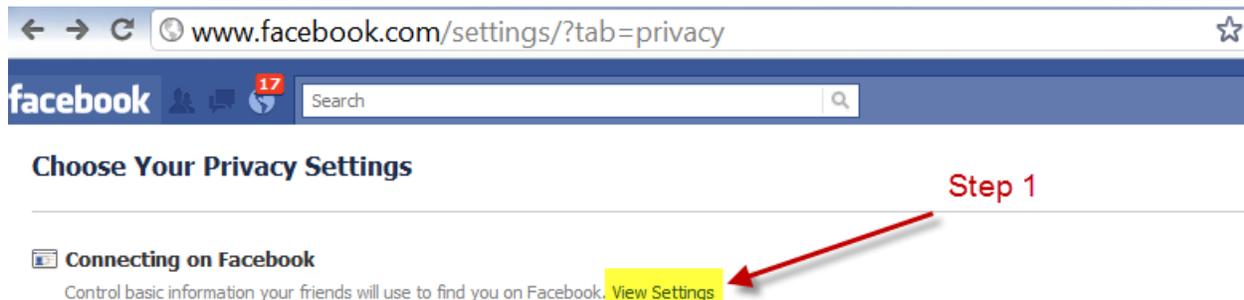
Assuming you have a Facebook account, it is a good idea to periodically review your settings to make sure they are how you like them.

For various reasons, some will want to have their profiles more open than others - the bottom line is *your privacy is a personal choice*. Understanding the settings and options available to you is critical.

6. Check Your Personal Profile

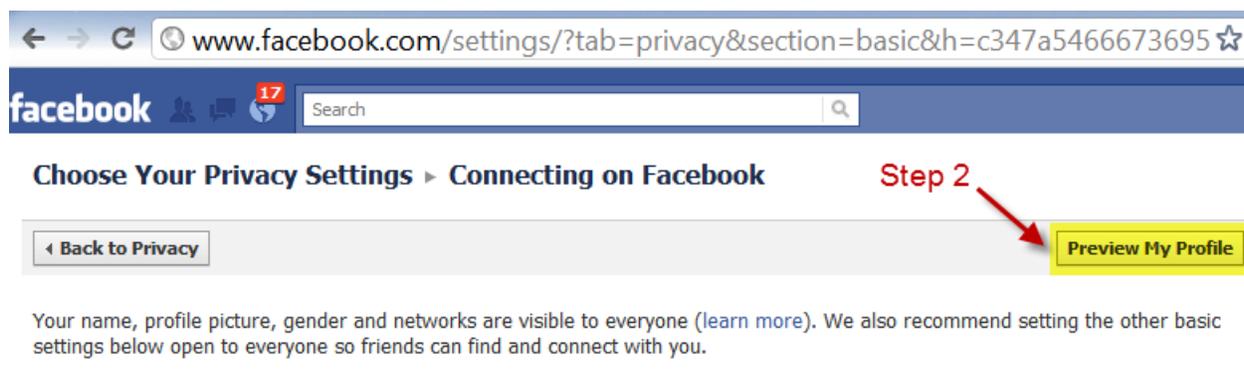
First, you will want to check your "Public Profile" on Facebook.

To do this, go here after logging into your Facebook account: <http://www.facebook.com/settings/?tab=privacy>



Then click on **View Settings** as shown in the image above.

From here, click on the **Preview My Profile** button.

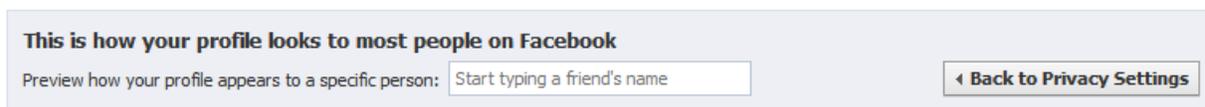


This is exactly what someone will see who is not currently your friend - make sure nothing is shared that you aren't comfortable with.

The most common settings here would be to only share your profile image, location, school information, and maybe work history. For anything else, especially photo albums and wall posts, you will most likely want friends only to see.

7. Check What Friends See

From the same screen, you can type in any of your friends' names, and see your profile exactly as they do.



This is particularly important if you use lists (which you probably should!) to organize your friends. Especially if you have lists for colleagues, family, students etc. and you don't want them all to have access to the same things.

8. About Friend Lists

Speaking of Friend Lists, if you currently use them, you should take this opportunity to double check that everyone is appropriately assigned.

I wrote much more about lists in [The Why and How of Using Facebook for Educators - No Need To Be Friends At All!](#)

If you aren't currently using lists, you should set aside time to set them up if you think they might be needed.

9. Review All Photos

You should also take this opportunity to review all of your photos - paying closest attention to photos you are tagged in.

Visit your **Profile**, click on **Photos** and look for **See All: Photos and Videos** about halfway down on the right.

Facebook has recently made this even easier for you by allowing you to scroll endlessly and quickly look over each and every photo. Untag yourself if there are any photos that you aren't comfortable with, and even delete them or contact the original poster of the photo and ask them to.

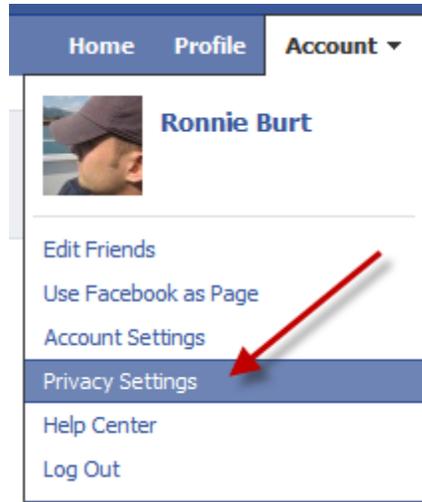
10. Removing Old Apps

This step is often forgotten about - but as you sign up for more and more websites, games, and other applications using your Facebook account, you are keeping open a link between you and that site.

You agreed to the connection at one point in time, but it is a good idea to regularly go through and delete applications you don't use any longer. By keeping your application list pruned, you will better be able to spot anything you don't like in the future as that list can grow rather lengthy in no time!

First, click on **Account** > **Privacy Settings** in the top right from just about anywhere on Facebook.

A Complete Guide to Web, Facebook, Twitter, and Google Plus Privacy and Security!

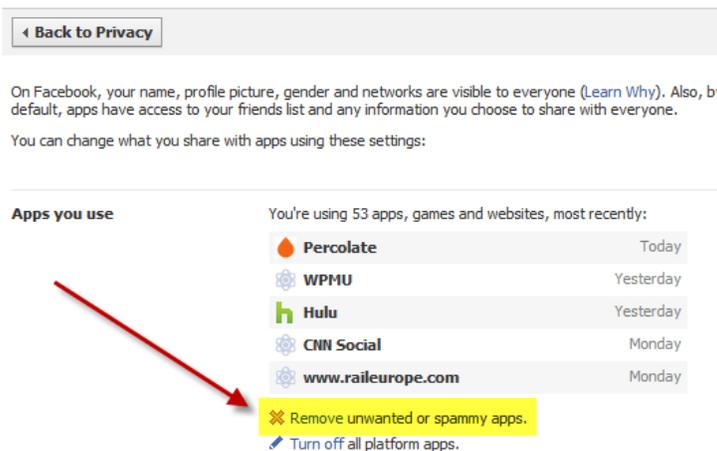


Then look for **Edit Your Settings** in the bottom left corner under **Apps and Websites**.



From here, click on **Remove unwanted or spammy apps** and go through the list removing what you no longer use.

Choose Your Privacy Settings > Apps, Games and Websites



Remember that you can always add back these apps later and you will most likely want to keep some of them! Judging by the 53 number above, it is time for a good cleaning of my own account as well :)

Twitter Needs Checking Too!



By design, Twitter is built around the idea of open sharing and making connections with those you may not have previously.

But that doesn't mean there aren't a few things to check privacy-wise as well.

Of course, if you don't (yet) tweet, skip on to #14 below. And if you are looking to get started, [check out our complete twitter guide here!](#)

11. Review Profile Information

Go to your main Twitter page - a place that if you use your mobile app and tweetdeck or another twitter service you may hardly ever visit.

For example, my main Twitter page is <http://twitter.com/ronnieburt>

Does everything look ok? Are you sharing a location or personal contact information that you may not wish to?

Make sure to visit this page when not logged into Twitter to see what others will see as well.

12. Double Check Private Tweets

Some twitter users might decide to have their tweets only visible to those that follow them. If you set it so that you must approve all followers, this effectively makes sure only those you approve see your tweets.



A reminder that if you choose to go this route, you won't be able to participate in hashtag chats or have your tweets re-tweeted which can really stifle the effects Twitter can have on building blog readership, for example.

13. Check DMs and Feed For SPAM

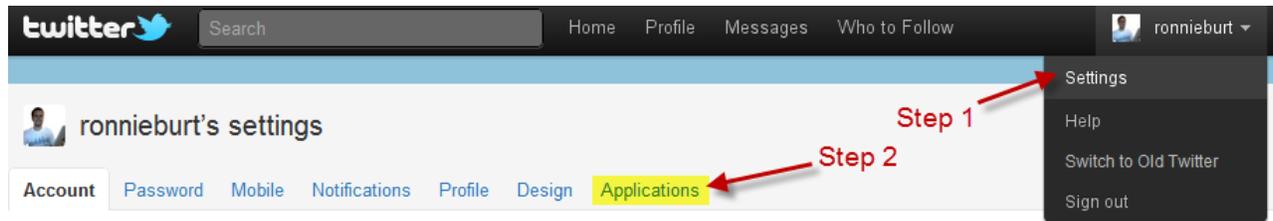
Over the past few weeks, twitter users have been noticing more and more spam and malicious tweets coming through. If a tweet sounds weird or suspicious, **don't open the link!**

It is best to send a message to the person who sent it to you (by email or another means besides Twitter if possible) to double check that they actually sent it.

I have noticed that several of the direct messages that I received with bad links lately have since disappeared, so it sounds like Twitter is helping to fight and control this growing problem.

14. Clean Out Twitter Applications

Just like with Facebook, you might have accumulated a number of associated applications with your Twitter account as well.



Click on **Settings** in the top right and then the **Applications** tab.

From here you can quickly **Revoke Access** to anything you no longer use or which to have associated with your Twitter account.

Google and Google Plus



Even if you aren't yet on Google Plus, you more than likely have a Google Profile of some sort.

The same tools apply to both, for the most part, and should you join, keeping up with Privacy from the start is extremely important.

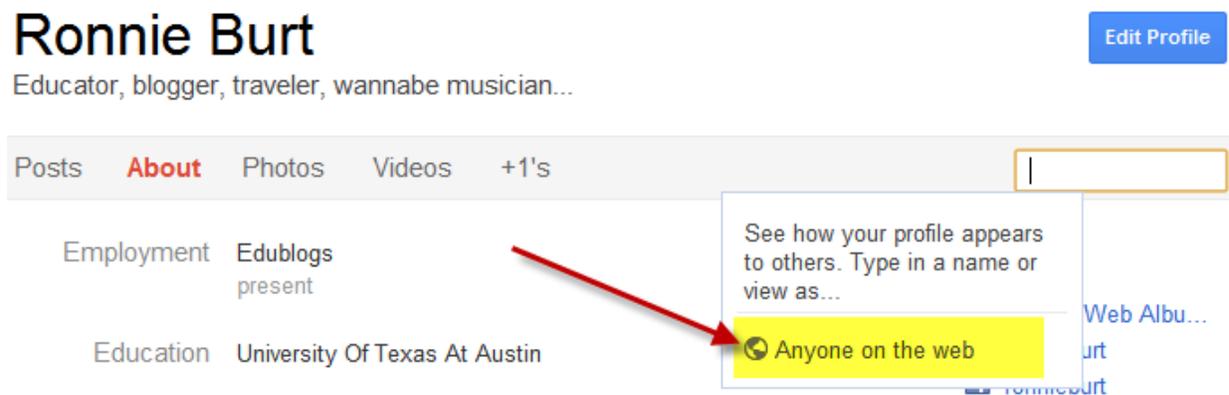
This is because once something is public, even for a few minutes, there is a good chance that it will live on forever, even after you remove it!

See [Google Cache](#) and the [Way Back Machine](#) as two reasons why.

15. Check Public Profile

Go to the [Google Dashboard](#) to see everything Google knows about you that is associated with your account.

In Google Plus, visit your **Profile** by click on your name after you login.



Click in the search box on the right and choose **Anyone on the web** to see what your public profile looks like.

Google Plus is a bit different from Facebook in that your profile is *always public*. You can limit what you post to select friends using **Circles**, but your **About** info is for everyone to see!

16. Review Privacy Settings

Click on your email address on the black admin bar in the upper right corner and choose **Privacy**.

Read through each setting and double check you understand and are happy with each selection.

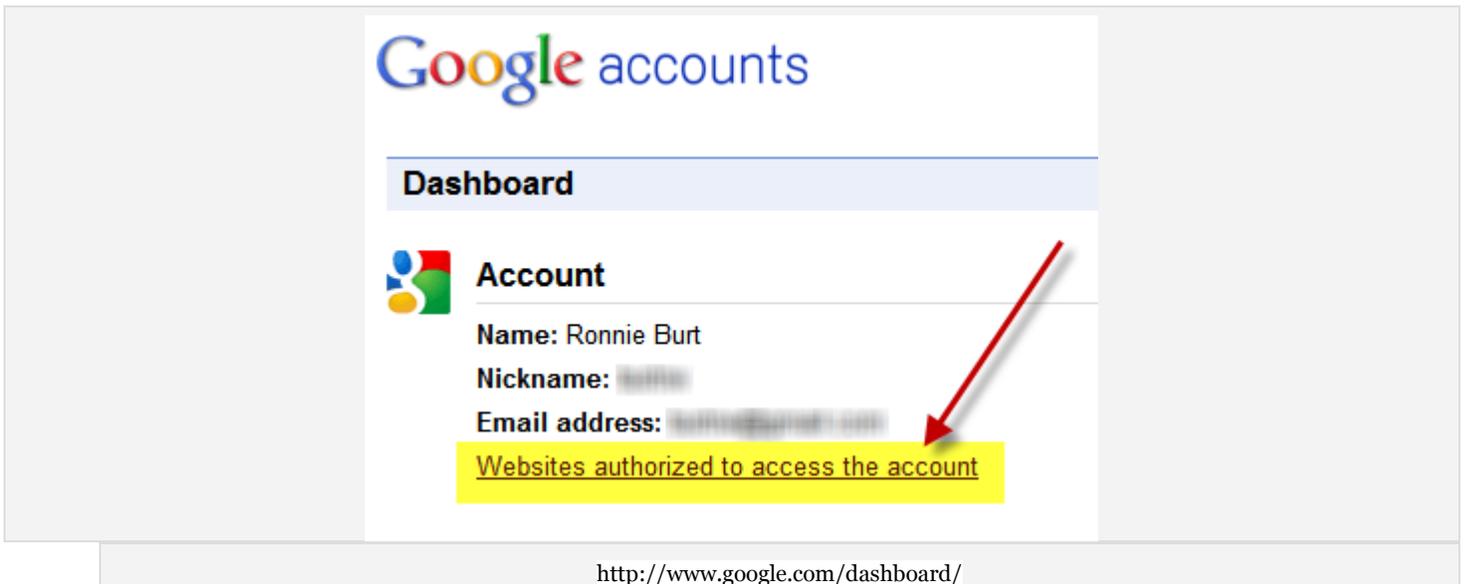
17. Review Photos

Just like with Facebook, you should check your **Picassa** (soon to be Google Photos) and Google Plus photos.

With Google Plus, you can limit your photos, or certain albums, to specific **circles** - so do make sure you are making use of those!

18. Clean Out Applications

From your [Google Dashboard](#), click on **Websites authorized to access accounts** near the very top left of the page.



Go through carefully and remove any sites you aren't currently visiting regularly - or others you would like to remove.

Miscellaneous Tasks

Beyond social networks, you might have even more of a web presence.

We'll also discuss everyday tools such as browsers and wifi settings to make sure you are as safe as possible while browsing the web.

19. Blogs and Other Web Media

Perhaps you have a blog, website, wiki, or other means of sharing information about yourself. Take some time to visit them all and look for contact and other personal information you may not still be comfortable sharing.

There are certain cases where it is definitely ok to share personal information online, this process is just to ensure everything that is out there is still how you want it to be.

One tip for blogs and websites is to use a contact form instead of sharing your email address and other contact information. This hides the info but allows people to still contact you.

20. Browsers and Advertising

So I looked online at one pair of Addidas running shoes for five seconds ONE TIME, and now, on just about any website I go to I see an advertisement for that exact pair of shoes!

Sound familiar?

If you want to learn more about the security and privacy options available, check out reputation.com for some sound advice.

21. Passwords

There are some interesting studies that show when applications or work requires you to change certain passwords regularly, they actually can become less safe.

Why? Because when you have to change a password, your first instinct is to write it down somewhere. Take a look around your desk or computer. If there are sticky notes around with a password on it, you are leaving your self open to someone finding out what it is!

The internet world really hasn't come up with a good solid way of managing the increasingly many number of passwords we all have. Especially for important accounts like for banks, work, email etc.

A good rule of thumb is to not use the same exact password everywhere that you can. I get around this by using a pretty standard password with something to do with the site it is for attached. I also like to put numbers at the end that I change periodically when I update passwords. This helps me to remember them all, but I inevitably do forget occasionally.

At the very least, don't continue to use passwords that are common and easy to predict!

A Complete Guide to Web, Facebook, Twitter, and Google Plus Privacy and Security!



SEARCH THE WEB

	1. NAME SEARCH – “YOUR NAME”
	2. EMAIL SEARCH – ALL EMAIL ADDRESSES
	3. ADDRESS SEARCH – “STREET ADDRESS” STATE
	4. PHONE NUMBER SEARCH
	5. SET UP ALERT NOTIFICATIONS



FACEBOOK

	6. CHECK PUBLIC PROFILE
	7. CHECK WHAT FRIENDS SEE
	8. CREATE AND USE FRIEND LISTS
	9. REVIEW ALL PHOTOS – YOUR ALBUMS AND PHOTOS TAGGED IN
	10. CLEAN OUT APPLICATIONS



TWITTER

	11. REVIEW PROFILE INFORMATION
	12. CONSIDER NEED FOR PRIVATE TWEETS
	13. CHECK DM'S AND FEED FOR SPAM
	14. CLEAN OUT APPLICATIONS



GOOGLE & GOOGLE PLUS

	15. CHECK PUBLIC PROFILES
	16. REVIEW GOOGLE PLUS PRIVACY SETTINGS
	17. REVIEW PHOTOS – FROM PHONE AND PICASSA
	18. CLEAN OUT APPLICATIONS



MISCELLANEOUS TASKS

	19. OTHER PROFILES – BLOGS, WEBSITES, ETC.
	20. BROWSERS AND ADVERTISING
	21. PASSWORDS

Keep In Touch

TheEdublogger.com

twitter.com/edublogs
facebook.com/edublogs

edublogs.org

