

facebook

FB Website/Apps Partners and how they connect to you through Facebook

Have you played a game on Facebook? Maybe you've used an app like JibJab or a Birthday Card or calendar app. Did you know that the DEFAULT SETTING for almost all apps you can get through FB requires you to share your information? Unless you carefully control your settings, "Big Brother is watching."

- Go to **Account — Privacy Settings** — and then click on **Edit your settings** under **Apps and Websites (bottom left)**
- To prevent people from easily finding your FB account with Google, scroll down to **Public Search** and click on **Edit Settings**. Simply uncheck the check box next to "Enable public search".
- Next to **Apps you Use**, click on **Edit Settings**. Go on to edit settings for each app, and remove any app you no longer use. You will be amazed at the access that is required by most apps.

Avoid having your account hijacked or hacked. Enable https.
Here's how: Go to **Account — Account Settings—Account Security**. Click on **Change**, and click on **both boxes** to select "Secure Browsing," and notification if a new computer or mobile device logs in to this account. Click **Save**.

Riverside Brookfield High School

Facebook Privacy Settings for Students

Protections for you now . . . and for your future



Internet Safety Day 2011

Make Your Contact Info Private

Avoid Those Dangerous Photo/Video Tags

WHY?

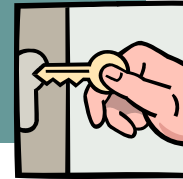
Your Reputation

- Future college admissions, scholarship awards, and employment can be derailed by inappropriate images on FB.
- Even if you've done nothing wrong, your links to your Friends' profiles may reveal information you don't wish to share.

Your Safety and Privacy

- If your settings are "wide open," predators, criminals, or anyone else could find out where you are—or are *not*.
- Your location can be tracked via GPS if you have FB loaded on a mobile phone.
- When you click "Like" on a community page to become a fan of that site, other fans of that page can access your private information.
- You may be solicited by businesses.
- You may be too-easily found by anyone doing a Google search.
- Your information may be shared through your friends' access to apps and their lack of privacy settings.

If you lock the front door to your house but leave the back door open, you're allowing thieves free access to your belongings. Similarly, if you don't carefully control your Facebook settings, you're allowing perfect strangers access to your information — it's like giving them a key.



HOW?

- Go to **Account — Privacy Settings**.
- The first section is **Connecting on Facebook**. Click on **View Settings**.
- This is where you choose who can VIEW information about you—your name, interests, school, your Friends list, gender, etc. We recommend changing most of them to either **Friends Only**, or **Friends of Friends**.
- Click **Back to Privacy**, and then under **Sharing on Facebook**, click on **Customize Settings**.
- There are 3 sections: **Things I Share**, **Things Others Share**, and **Contact Information**. This is the section that controls who can see all the content you

post regularly, such as status updates, photos, and videos. We recommend changing everything to **Friends Only**.

- For *some* items, you may wish to choose "**Friends of Friends**," but remember that you won't have any control over who those extended friends might be.
- Under **Things Others Share**, scroll down to where it says "Friends can check me in to Places" and click on "**Edit Settings**." You'll then see a window named Places: Friend Tags. Click on the box on the right and select "**Disabled**."

