

Facebook Safety and Potential Privacy Exposures

Brian Cragun

4/12/2009

An open letter to Youth, Parents, and Seniors on Facebook safety.

This short paper warns about safe practices and privacy exposures on Facebook. It is written for youth, parents and seniors concerned about staying safe on the Facebook. I am not an expert about Facebook, nor can I guarantee that following these guidelines will guarantee your safety on the Internet. There are many deceptive businesses on the Internet, and I believe some parts of Facebook may be deceptive and potentially unsafe. With this information in hand, I hope you will understand some of the risks and make informed decisions about your use of Facebook.

The Internet has always been compared to the wild west – an exciting new frontier with excitement to be found and dangerous villains to avoid. This has been true of email, websites, and online purchases; it is also true of social networking sites like Facebook. On the web, you can gain knowledge and conduct business, yet you risk exposure of personal information that may put you in personal danger; this is also true of Facebook.

Facebook has succeeded, in part, because it allows each user control over who sees their personal data. Users limit who sees their personal data by controlling their Facebook “friends”. With a limited number of viewers, users become a little braver about what they say and how much personal information they put on Facebook. Parents are more comfortable allowing their minor children on Facebook, because friends must be allowed by personal consent.

In general, I think Facebook lives up to its promise of a safer social web site. However, there is a dark side -- there are some activities on Facebook which I believe are not to be trusted, or at least of much higher risk than other Facebook activities.

There are three things you should do to increase your safety:

1. Only accept people you know as your Face *friends*.
2. Never put confidential information on Facebook.
3. Only use Facebook applications that are worthy of your trust. Decide this based on business reputation and privacy policy.

Only accept people you know as your friends

Everyone knows the adage, don't speak to strangers. In Facebook, you increase your safety by only allowing people you know to be your Facebook *friends*. When you allow someone as a *friend* in Facebook, they can see your personal data. They can see your name, your school, your likes, dislikes, and interests. They can see photos of you. They can see who your friends are.

Predators and scam artists like to obtain personal information and use it to convince you they are legitimate, gain your trust, and then take advantage of you. For example, if they know a hobby, they may try to convince you they have an interest in the same hobby. If they know the name of a

friend, they may try to convince you they know the same friend. The consequences of trusting strangers can lead to financial loss or even personal danger. Allowing strangers to see personal information increases your risk of personal danger. Only allow those you already know as your Facebook friends.

Never put confidential information on Facebook

Confidential information should never be put on a website like Facebook because there is always risk that it can be compromised. Facebook has millions of users, and they are not always truthful about who they are. Anybody on the Internet may try to guess your password. Your friends may accidentally share your personal information with others.

The only way to make sure private information is never seen is to never put it on the web. Your social security number, bank account numbers, credit card numbers, passwords and similar confidential information have no place on Facebook. Nor will Facebook ever ask for such information. Be immediately suspicious of anyone who requests such private information.

Once it's put on the web, you may never be able to remove it. Content on the web can be copied, stored, and kept in archives for years. Information that is potentially embarrassing should be kept off the web.

In similar manner, don't write anything on Facebook or in any correspondence on Facebook unless you can live with it becoming public. Once something is entered into Facebook, it will be seen. The question is only how many people and when. Even though Facebook respects your privacy, other users may not. Your comments may be copied and sent to others. Always write as if the whole world will see it, and you will avoid humiliating yourself.

Only use Facebook applications that are worthy of trust

Facebook has many fun applications, but some should not be trusted. Only use applications that you are certain can be trusted. **The primary purpose of this paper is to warn you about risky Facebook applications and to teach you what to be suspicious of.** You must decide which ones you will trust.

Applications

An application is a program that runs in Facebook. It may ask you questions, or display an image or animation, or display a little image on your Facebook page. Applications have names like "interview invitation", "Lil Blue Cove", "birthday request", "water balloons", "pillow fight", "water gun fight", "lil green patch", "cause invitation", "emoticons", "compare friends", "lucky clover", "Robin Hood", and so on.

When use an application, you give it permission to look at your personal data. Therefore you should only use applications that you trust. I recommend you find out about the business that owns the application and read the applications privacy policy. **If the business is suspicious or the privacy policy isn't good or can't be found don't use the application.**

You would never give a stranger access to your private data, but **many people use applications**

without understanding that they are giving strangers access to their private data. Not all applications are bad, but many are suspicious. The rest of this article will explain how to recognize an application, how to find the privacy policy, and how to determine the reputation of the company.

Recognizing applications

Applications can be recognized in two ways.

1. Applications are identified as applications by a link next to them which says: *Block This Application*. See Figure 1.



Figure 1 – Sample Application. *Block This Application* link is shown.

2. An application must gain your permission before it can access your personal data. **When you start to use an application, you will receive a warning and you must agree to “Allow” the application to look at your personal data before you continue using it.** See Figure 2. **Only applications use the *Allow* dialog.**



Figure 2 – *Allow Access* dialog of a sample application. Note the permission you give to your profile information, your photos, your friends' info and more!

In the example of Figure 1, if you press the *Shoot Back!* Button you will be shown the Allow Access dialog, as shown in Figure 2. **Note that when you Allow an application access, it has permission to copy your profile information, your photos, and any information you can see about your friends!** Does this scare you? I think it should! Giving a strange business access to your data and your friend's information is a lot of private information just to pretend you are having a water fight.

Another thing that should worry you is: how many of your friends are using this application? **If a friend gives an application access, then the application has access to some of your data.**

Company Reputation

Before you trust a stranger with your private information and information about your friends, it would be a good idea to find out something about them. Most applications provide information about themselves. Usually this can be found by searching Facebook for the application, or by selecting a link that is often provided.




Figure 3 – Sample application search result. Note link to *View Application* in upper right. Note the number of users.

In the example, there is a link to *Water Gun Fight!* on both the invitation and the Allow dialog. *Water Gun Fight!* can also be found by searching from Facebook's search bar, as shown in Figure 3.

If you select *Water Gun Fight!* on the invitation, or *View Application* in the search result, you get an information page about the application. See Figure 4.

The sample application information page reveals more information about the application, including legal disclaimers. In the small type, Facebook makes no claims about the application, and distances itself from it, stating it was not developed by Facebook. Even more frightening is the **lack of a privacy policy**. The application claims to have over one million users. What is it doing with all the private data it has access to?

Water Gun Fight! ◀ Browse More Applications



Have lots of fun shooting **Water Guns** at your friends!
 Wide variety of **cool and amazing** weapons to choose from.
 Fill up your gun with water, milk, soda, urine, vomit and more!
 Plus **score points** based on where your shots land.
Don't miss out...come join the fun!

Facebook is providing links to these applications as a courtesy, and makes no representations regarding the applications or any information related to them. Any questions regarding an application should be directed to the developer.

[Go to Application](#)
 Become a Fan
 Block Application
 Share +


About this Application

Users:
 1,091,375 monthly active users,
 2 friends

Categories
 Gaming, Just for Fun

This application was **not** developed by Facebook.

Fans
 6 of 1,827 fans [See All](#)



[Friends Who Have Added this Application](#)
 2 friends have added this application [See All](#)

Contact Developer | Report Application Share +

Figure 4 – Sample application information page. Note Facebook disclaimer, clear identification that it was not developed by Facebook, and in this case total lack of a privacy policy.

What can developers do with private data?

Developers of an application are *supposed* to follow several conduct guidelines, including the [Facebook platform policy](#), the [Facebook Developer Guidelines](#), and the [Facebook Terms and Conditions](#).

The latter contains the following restrictions:

- You can't use Facebook Platform for anything that infringes on anyone's rights or intellectual property, generates spam, phishes, or is illegal.

- You must treat users' privacy with the same respect we do. If you directly collect personally identifiable information from users, you must post a privacy policy detailing what you'll do with that info.
- You must be honest and accurate about what your application does and how it uses information from Facebook users. Your application cannot falsely represent itself.

The terms state there **must be a privacy policy** if any data is collected. Do all applications adhere to that? Apparently not. I could not find any privacy policy for *Water Gun Fight!* or any indication of Facebook enforcement of this policy.

In a recent article in BBC news, a [BBC investigation found that Facebook private data is at risk](#). BBC created a sample application and tried to access data.

“[The] application was then added to four Facebook users' accounts. As a result, they could access details of those four people and all their friends on Facebook **even though many had chosen to hide those details on their public profile. This means that there is the potential for criminals to "skim" user data, via a rogue application.** Data can also be given away by a Facebook friend who innocently adds an application to his Facebook account. At the moment it appears the only completely sure and safe way to stop such data being shared is to remove all applications and not use them.”

As far as I can tell, the only enforcement of any of Facebook's policies is the revocation of the developer to have an application of Facebook.

In the end, it comes down to how much trust you place in the developers of these applications.

Privacy policy

If there is a privacy policy, it should be linked to the *Application Page* and the *Allow Application* page. Read the terms of the privacy policy to decide if you trust the application.

Use the application or not?

Your decision to use the application rests with you. You have to decide based on the reputation of the company and their privacy policy.

It would be unfair to characterize all applications as evil. There are certainly many that have a defined purpose and a good reputation. *We're Related* is an application written by [FamilyLink](#), a company that has a lot invested in user relations and their core business. They use the Facebook application as a link into their main site. I chose to allow *We're Related* because I was able to find a corporate page for FamilyLink. I had difficulty finding their privacy statement, but an email to their corporate email was quickly returned with a link to [FamilyLink's privacy statement](#).

Most applications are not so easy to evaluate. There is often no privacy policy to be found. You should ask yourself, why are the developers writing the application? It takes time and effort to write an application. Where are they making their money? Are they doing it out of the goodness of their heart? I doubt it. Facebook itself is different. They make their money from advertisements. Most applications, on the other hand, have no obvious source of income. Therefore, an application that has no privacy policy, written by a company that doesn't have a web page, and that has no source of income from its use, seems very suspicious to me.

Personally, I have chosen to ignore almost all applications because there is no disclosure on what they may be doing with the personal data they have access to. On the web, it is reasonable to be skeptical until a business has proven itself.

Other requests on Facebook

There are all kinds of requests on Facebook. Many requests are not applications. Here are a few of the other kinds of requests and my evaluation of their trustworthiness.

Friends

Friend suggestions and friend requests are just what they seem. Someone wants permission to see your profile and information and communicate with you. You will also be able to see their information. You can ignore people you don't want to be friends with or don't trust.

Once someone is your friend, they can post on your wall, an area that all your friends can see. If they post something that is embarrassing, you can remove it.

Keep in mind that when you comment on someone else's wall or photo, your comments are seen by everyone that has permission to see the wall or photo.

Generally, Facebook friends are safe as long as you select people you know and trust.

Groups

A group is a set of people that join together in a common interest. Groups have their own pages where information and photos can be posted. You must decide to join a group. Once you belong to a public group, everyone on Facebook can see that you belong to the group, and information about you that is part of the group. For example, anyone can see things you post on the group wall, or photos of you. However, someone must still ask to be your friend before they can see your personal data.

Generally belonging to a group is reasonably safe, but remember it is totally public. Anybody can join. Anybody can see the members. I would be suspicious of anyone you don't know making requests of you based on your membership in the group. Find out more about them, first.

Some groups are called secret groups. These groups are safer because you must receive an invitation from an administrator, and outsiders may not see who is part of the group. I personally feel much safer joining private groups.

Event invitations

An event invitation is like a group, but it also tracks whether you say you'll be coming or not. When someone sends you an event invitation, you will appear in a list on the event page that matches your reply. As far as I can tell, when someone sends you an invitation, you already appear in one list on the event page, and there is no way to totally disappear from the page.

Similar to groups, anything you post on the event page will be public to everyone who can see the event. If it is a public event, everyone can see the time and location of the event and whether you plan to be there.

If you create an event, select the *Closed* or *Secret* privacy option. This will prevent people you don't know from seeing the time, location, or other information that might make your event a potential target for strangers.

Generally, I think event invitations are reasonably safe. However if you get invitations to events you don't want to be associated with or that concern you, choose "Remove from My Events".

Recommendations for parents

Youth today are referred to as [digital natives](#); they have grown up with technology and the Internet. Most of them know there is danger on the Internet, but they don't have the life experience to consistently recognize potential dangers. When a friend sends an invitation to win a teddy bear icon or participate in a movie survey, the fun of the moment always seems to win out over prudent caution.

I think Facebook can be used in a safe way, if Facebook friends are selected deliberately, profile data is scrutinized and scrubbed, and applications are distrusted and avoided.

If you allow your child to have a Facebook account, I strongly recommend you get a Facebook account as well and insist that your child accept you as a Facebook friend. You can set up your profile to be notified of everything your child posts on Facebook. This has actually been fun to read the day to day posts of my children.

I recommend that parents also insist on having the password to their minor child's Facebook account and other email account(s) as well. Some parents and youth balk at this, but I believe it parallels the trust relationship a parent should have with a child and their room. I don't rummage through my child's dresser or read their diary. However, I reserve the right to do so should I ever have a concern. Trust with verification, if you want to call it that. I believe it is comforting to a child to know their parent cares and is watching out for them. The same is true of Internet usage. Setting boundaries and having content and interactions under a potential of scrutiny will help the youth do what they know they should.

Summary

Facebook users need to be careful what personal information they put in their profile, and be cautious in their use of Facebook applications. While theft of information has not been proven using Facebook applications, the ability to take private information has been shown to be possible. Facebook users should be selective in accepting Facebook friends.

About the author

Brian Cragun is a concerned parent and volunteers as a church leader. He has a Bachelors degree in Computer Science from Utah State University. Please send corrections to cragun@gmail.com.

Copyright © Brian J Cragun, 2009. All rights reserved.