CMSGu2011-03

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Social Networks

National Computer Board
Mauritius

Version 1.5

July 2011

Issue No. 3

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this document, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

Table of Contents

Table of Figures

1.0 Introduction

1.1 Purpose and Scope

This guideline offers an insight into the risks associated with the common social networking sites and gives details on the precautions to take by parents, children and the general public.

1.2 Audience

This document, while generic in nature, provides the background information to help readers understand the topics that are discussed. The intended audience for this document includes teenagers, students (primary, secondary and tertiary) and all those who make use of social networking sites.

1.3 Document Structure

This document is organised into the following sections:

Section 1 provides a brief overview of the document's content.

Section 2 gives a background on social networking sites.

Section 3 presents the impact of social networking sites, especially on young people.

Section 4 gives the safety measures that parents and children need to take regarding social networking sites

Section 5 concludes the document.

Section 6 contains a list of references used in drafting this document.

Appendix A includes a couple of snapshots taken from the Facebook website to help users set their privacy settings.

2.0 Background

In this age of globalisation, the world has shrunk due to the electronic media and portals. Communication has become effective as never before, thanks to the advent of Internet. The social networking sites have also played a crucial role in bridging boundaries and crossing the seas and bringing all people at a common platform where they can meet people or find old friends and communicate with them. It has become a potential mean to relation building and staying in touch with friends.

2.1 Basics of Social Networking

Social networking is the use of web-based tools to interact with other people through text, images, or sound. Some common social networking tools are Facebook, Twitter, Myspace and Linkedin. These tools can:

- Share media (text, photos, videos, audio)
- Carry on live discussions
- Send instant messages
- Share and edit documents

2.2 Common Social Networking Sites

2.2.1 Facebook

Facebook is a social networking service and website operated and privately owned by Facebook, Inc. Facebook users must register before using the site. Three of the most popular features of Facebook are the ability to add Friends, update your status and run applications such as games and quizzes. A *"friend"* is anyone on the Facebook network whom you allow to see various levels of personal information, such as job, birth date, photos, group membership, comments and list of other Friends. You can even play online games and keep others updated on your daily life. Friends can also see Friends of Friends, meaning individuals, whom you have officially befriended and may never have met, may have visibility into your personal information and whereabouts. Additionally, users may join common-interest user groups, organized by workplace, school or college, or other characteristics. Facebook allows any users who claim to be at least 13 years old to become registered users of the website. As per the statistics obtained from InSafe in February 2011, Facebook already had 500 million users registered.

2.2.2 Twitter

Twitter is a website, owned and operated by Twitter Inc., which offers a social networking and microblogging service, enabling its users to send and read messages called "*tweets*". Tweets are text-based posts of up to 140 characters displayed on the user's profile page. They are publicly visible by default; however, senders can restrict message delivery to just their followers. Users can tweet via the Twitter website, compatible external applications (such as for smartphones), or by Short Message Service (SMS) available in certain countries. While the service is free, accessing it through SMS may incur phone service provider fees. Users may subscribe to other users' tweets – this is known as *"following"* and subscribers are known as *"followers"* or *"tweeps"* (Twitter + peeps). Twitter also allows users to update their profile by using their mobile phone either by text messaging or by apps released for certain smartphones / tablets.

2.2.3 Myspace

Myspace drives social interaction by providing a highly personalised experience around entertainment and connecting people to the music, celebrities, TV, movies, and games that they love. These entertainment experiences are available through multiple platforms, including online, mobile devices, and offline events. It is also the home of Myspace Music, which offers an ever-growing catalogue of freely streamable audio and video content to users and provides major, independent, and unsigned artists alike with the tools to reach new audiences.

2.2.4 LinkedIn

Linkedin is a business-related social networking site, allowing registered users to maintain a list of contact details of people with whom they have some level of relationship, called "*Connections."* It also allows users to research companies with which they may be interested in working, and supports the creation of interest groups. Groups support a limited form of discussion area, moderated by the group owners and managers. Since groups offer the ability to reach a wide audience without so easily falling foul of anti-spam solutions, there is a constant stream of spam postings, and there now exist a range of firms who offer a spamming service for this very purpose. Groups may be private, accessible to members only or may be open to Internet users in general to read, though they must join in order to post messages.

3.0 The Abuse of the Internet and Social Networks

While the Internet is essentially a great place for children, there are some areas of cyberspace that are not appropriate, just as there are areas in almost every city that are inappropriate for children. Social networking sites, for instance, are gaining a lot of popularity these days with almost all of the educated youth using at least one of such sites. These have played a key role in bridging boundaries and crossing the seas and enabling them to communicate on a common platform. It has become a popular and a potential means for them to hook up with friends and to grow up their social circle. The question regarding Internet safety, privacy and the legal issues have been cropping up all this time. Through this guideline, we try to find out the impact of these networking sites on the personal and professional lives of people using them.

3.1 Privacy Issues

Although many people do not think of it, social networking web sites involve many dangerous elements and many people are concerned about some major problems that they contain. One such problem is privacy issues. With social networking web sites like Facebook and Myspace, it is almost too easy to retrieve personal information about someone and use it to harm them.

Phishing, which is the process in which attackers make use of social engineering techniques to fool users into divulging their confidential information, is a very common issue. It can often lead to the loss of personal information such as usernames, credit card numbers, and passwords. This in turn causes great privacy issues since that person can now access personal information and then sell it off to marketing companies for a profit. This selling of information to companies has led to the rise in spam e-mails that we all receive.

In a case with Myspace, the availability of being able to customize one's own site has allowed people to use phishing html code to create phishing profiles that allows that person to access anyone's profile who have visited the phishing profile.

3.2 Child Safety Issues

Another main issue of concern with social networking sites is that of child safety. According to researches, almost three out of every four teenagers who make use of social networking sites are at risk due to their lack of using online safety measures. Many websites do have an age requirement, but it is easily bypassed by lying about one's age. Even if they do not lie about their age, the average age requirement is around fifteen years old.

Even though a lot of the social networking web sites are trying to implement new ways of keeping children safe, Myspace included, predators are finding ways around these new implementations and kids are still naive to the fact that not everyone online is who they say they are.

Myspace has been specifically targeted for these child safety issues after a sixteen year old girl flew to Tel Aviv, Israel to meet and engage in sexual relations with a twenty year old male whom she had met through Myspace.

Paedophiles are increasingly using social networking sites to distribute distribute and sell nude images of children. The techniques used by criminals who buy, sell, share or collect child sexual abuse images are sophisticated and are diversifying. Over half of the material we deal with is related to commercial payment mechanisms confirming an ongoing demand for images of children being sexually abused. The scale of all child sexual abuse content online is difficult to measure because the methods of operation are changing, becoming quicker, cheaper and more opportunistic than ever before. The distributors are increasingly using legitimate internet services to make the images available, from free hosting platforms and image sharing websites to social networking areas and hacked websites.

According to "The Telegraph", half of all child abuse images may now be distributed via free sharing websites. It also warned child abuse rings and other perverts are hacking in to genuine websites to secretly store images which they then sell via spam emails.

3.3 Cyberbullying

Cyberbullying means pretty much what it sounds like. Cyberbullies are kids who act just like the bullies from past generations. They pick on other kids, trying to humiliate and intimidate them. Contrary to the traditional way, cyberbullies do their damages remotely via e-mails, instant messages, web posts and text messages. On social networking sites, cyberbullies can do damage very quickly by posting messages for all friends to see. These include receiving threatening messages; having their private emails or text messages forwarded without consent; having an embarrassing picture posted without permission; or having rumours about them spread online. When asked what form the cyberbullying took, the most common response was the sharing of private information (instant messages, e-mails, etc) rather than direct threats.

Teens who share their identities online are more vulnerable to cyberbullying. Cyberbullying, unlike bullying in general, can expose a victim to hundreds or even thousands through an e-mail, blog post or profile. Additionally, many cyberbullies use the web to embolden their actions, as they can hide behind their monitor.

3.4 Addiction

Social networking addiction is a mental illness centered on a dependency of online *"friends"* or online interaction on social networks. Social networking addicts are unable to control their tendency to be logged in and participating on social networking websites.

Some of the most common characteristics of social networking addiction are:

- A feeling that being online is the only way to be noticed by the world at large. The longing for another post, update, or chat session (otherwise known as *"sneaking"*) before they sleep. A strong anticipation to being logged onto their social network of choice and seeing what everyone in their network is doing.
- Episodes of logging onto their social network randomly while in the middle of something completely different.
- Attempts to control their addiction by changing social networks. For example jumping from Myspace to Facebook.
- Sneaking for long periods of time.

- Deleting wall posts so that others don’t notice their excessive amount of posts or updates.
- Binge sneaking and sleepless nights due to sneaking. Drowsiness the next day from long nights of sneaking.

According to “associatedcontent” from “Yahoo”, Facebook users have forgone their relationships and responsibilities, in favour of Facebook. Parents have reached out to school counselors, corporate HR departments have sought work performance psychologists, and couples have turned to marriage counselors to help their spouses overcome social media addictive behavior. In fact, “Facebook Detoxing” has been trending online as a top New Year's Resolutions for 2010.

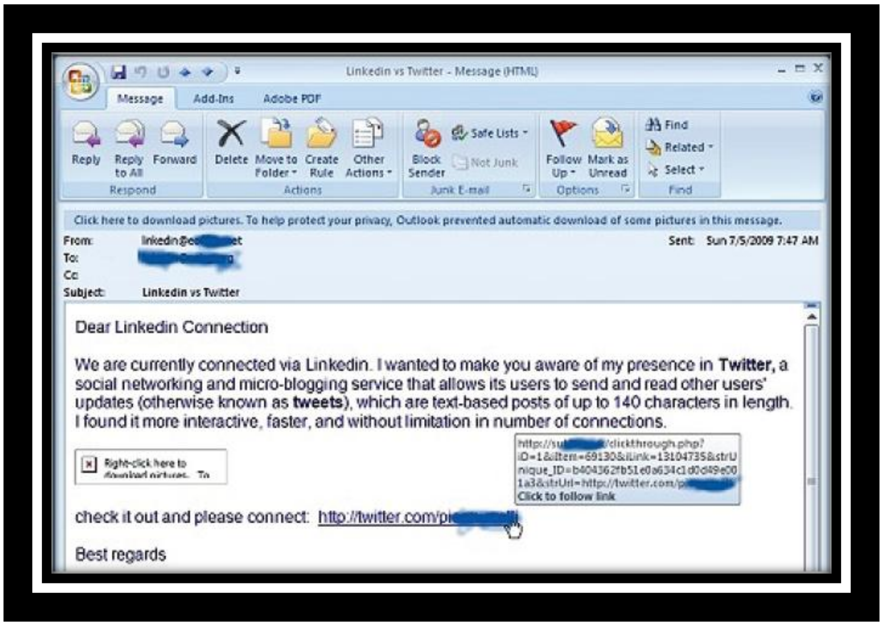
3.5 Harassment and Stalking

Social networking sites have been blamed to be a major source of harassment and stalking for teen users. For instance, peers may disregard one another or provide malicious advice. One possible consequence of younger groups' use of social networking sites derives from the rapid forming and dissolution of relationships. The dumpee (one who has been dumped) has the opportunity to abuse, defame or even reveal information, such as photos, about the dumper. A form of stalking behaviour is also possible, with the dumpee continuing to follow the person's activities. Although the dumper (the one who dumps the friend) has the opportunity to remove a person as a friend, the damage to self-esteem and reputation may already have been done by the time this occurs. If the dumpee has mutual friends on the social networking site they may still be able to maintain some forms of surveillance by exploring the sites of the friends of the ex-friend. Even where relationships have not broken up, friends may post materials or photos which are regarded as compromising, without seeking the permission of the persons featured. Similarly people who are disliked might seek to make friends, bringing unwanted attention.

A shooter, Seung-Hui Cho, allegedly used Facebook to locate and stalk female classmates. In July 2007, authorities in Lorager, Louisiana, arrested a 17-year old for stalking and cyberstalking another teenage boy. The alleged stalker's MySpace page featured a video of the accused pistol-whipping another boy posing as the victim.

3.6 Spam and Hoaxes

Whether you use Facebook, Twitter, LinkedIn or any online site for social networking, online banking or day-to-day purchases, you should be aware of e-mails that appear to be from these sites but are actually hoaxes and may contain malicious content. I have received numerous e-mails that allege to be from my bank, yet are actually sent by a spammer in the hopes of obtaining my online username and password. Similarly, e-mails claiming to be Twitter and Facebook invitations are now commonplace (See Figure 1). The messages may even contain an attached ZIP file that recipients are asked to open to see who invited them. The attachment actually contains a mass-mailing worm, which can cause damage to both your computer and your reputation.



From: linkedin@e[redacted]et

To: [redacted]

Cc:

Subject: Linkedin vs Twitter

Sent: Sun 7/5/2009 7:47 AM

Dear Linkedin Connection

We are currently connected via Linkedin. I wanted to make you aware of my presence in **Twitter,** a social networking and micro-blogging service that allows its users to send and read other users' updates (otherwise known as **tweets**), which are text-based posts of up to 140 characters in length. I found it more interactive, faster, and without limitation in number of connections.

http://su[redacted]/clickthrough.php?iD=1&iItem=69130&iLink=13104735&strUnique_ID=b404362fb51e0a634c1d0d49e001a3&strUrl=http://twitter.com/p[redacted]

check it out and please connect: http://twitter.com/pi[redacted]

Best regards

Figure 1 Hoax e-mail example

The message claims to be from a LinkedIn connection, inviting the recipient to also connect on Twitter. Yet, the sender and the recipient do not actually know each other, and their respective addresses and names were likely gleaned from a spam database. Placing the cursor over the link near the bottom of the message reveals the web address of the actual spam site; it also contains information that identifies the individual who received this message.

4.0 Safety Measures for Parents and Children

4.1 Basic Privacy Guidelines

The options for online communication and interaction are constantly evolving and changing. As a result, these guidelines have been established to assist individual users in making good decisions to protect themselves.

- **Check privacy policies & settings**

  All major social networking services have specific privacy guidelines and rules that are published on their websites. Make sure you understand them, even though they may be tedious to read, as they likely explain if your information is shared with other parties. Some services offer the ability to restrict your privacy settings for specific groups, such as allowing you to share pictures with your friends only and not everyone. Make good use of these settings.

- **Choose strong passwords**

  Use hard to guess passwords. (Your birth date or *"123456"* are not strong passwords.) If possible, the password should contain letters and numbers, as well as special characters. If you cannot remember complex passwords, either use a passphrase as hint or use any of the available password management utilities that can securely store them for you. Do not choose a password that can be guessed by the information that you have published on your account site. This includes friend's names, favoured movie stars, or pet names.

- **Keep your password secret**

  You should never share your password with others. This includes services that promise to help you get more friends or something similar. Do not lose control of your password. If you enter your password, ensure that you are on the real website and not a phishing scam page that just looks like the original site. Should you suspect that you have fallen for a phishing attack and your account has been compromised, use a clean computer to log into the original service and change your password.

- **Be on your guard**

  Social networks can be a useful source for business information, as well as for newsworthy updates from your friends. However they also contain a lot of useless information. You should treat anything you see online with a high degree of caution. Do not believe everything you read, whether it is financial advice, breaking news, or free tips, especially if it involves clicking a link or installing an application. If someone asks you for money in advance, it might be a scam.

  Besides, people on the Internet are not always who they claim to be. The celebrity who you are following might just be another fan, and the supposed co-worker from another office might just be someone doing reconnaissance on your enterprise. Not everyone that claims to be your friend is your friend.

- **Be considerate**

  Always think twice before posting something. Keep in mind that once you posted it, even to a close group of friends, you no longer have control over where it will be reposted and who might read it. These things can come back to haunt you when you search for a new position in the future. Consider if you really need to publish the full information. This includes posting too many personal details, such as phone numbers or work-related things. Furthermore refrain from forwarding virus hoax or exaggerated warning messages that will confuse more than help other users. Be nice and respectful to others and do not post hate messages about others, since you would not want to receive them yourself.

- **Keep yourself updated and protected**

  Always ensure that the software you use is up-to-date. Not only does this include the operating system and web browser, but also third-party plug-ins, such as PDF viewers. Install all the latest patches and hot fixes from the official site and automatically check for newer available versions through the software.

  Some of the newer attacks are very sophisticated and are sometimes hard to spot for an untrained eye. Use comprehensive security software to protect against these threats.

4.2 Photo Guidelines

Photos posted on social networking should be done so with the utmost care. Nothing posted online is private, and photos should be regarded as such. The following guidelines should be used when posting photos:

- Photos of children should not be posted without expressed consent from the parents. Even then such photos should be avoided.

- Care should be taken not to post photos of individuals who would object. This may involve obtaining the appropriate permissions.

- Photos posted on social networking sites must be appropriate. As a guideline, they should be photos that could be posted on a college's official Web site. Examples of photos that should be avoided include but are not limited to: photos involving alcohol, nudity, medical and hospital patients, and graphic scenes.

4.3 Chat and Instant Messaging Guidelines

Chat is a very popular activity for young people, especially teenagers, but it is also the area where they are most likely to get into trouble. When you are in a chat area, it is easy to forget that you are in a public *"place"* and that you do not necessarily know the true identity of anyone in the chat room. It is common to *"meet"* someone in a chat area who gains your confidence by being sympathetic and willing to *"listen"* to your problems.

- Children and especially teens need to be extremely careful in chat rooms.
- They should **NEVER** reveal their identity and they should never assume that someone is as he or she seems to be.
- They should **NEVER** agree to meet someone in person based on a friendly online chat without talking to their parents.
- If parents agree to the meeting, they or another adult should be present and it should be in a public place.

Instant messaging is like chat, except that it is usually a one-on-one experience instead of a group activity. In some ways that is safer if the person the child is messaging is a friend or relative. But it can be dangerous if it is a stranger. Unlike in some chat rooms, there is never anyone else there to monitor activity, so when your child is messaging another person it's as if the two of them are together in a private room.

Ways to avoid problems in chat rooms:

- Parents should not let their child chat in chat rooms that are not moderated. They should only allow him or her in rooms run by a reputable company or organization that monitors activity.
- As many spammers use names they can easily collect from a chat room, consider giving your child a chat screen name. This name would be one that is different than their e-mail address. This could help prevent unwanted Spam mail from coming to your child.
- Parents should instruct your child never to give out personal information in a chat room.
- Parents should also instruct their child never to agree to get together with anyone they meet in a chat room without first checking with them.
- Parents should talk with their children about the way some people behave in chat rooms and remind them that people are not always who they seem to be. They should also remind their children to be very careful about people who offer easy solutions to difficult problems or make offers that are "*too good to be true.*"
- Parents should consider using software to block sensitive personal information from being transmitted through their children's chat.

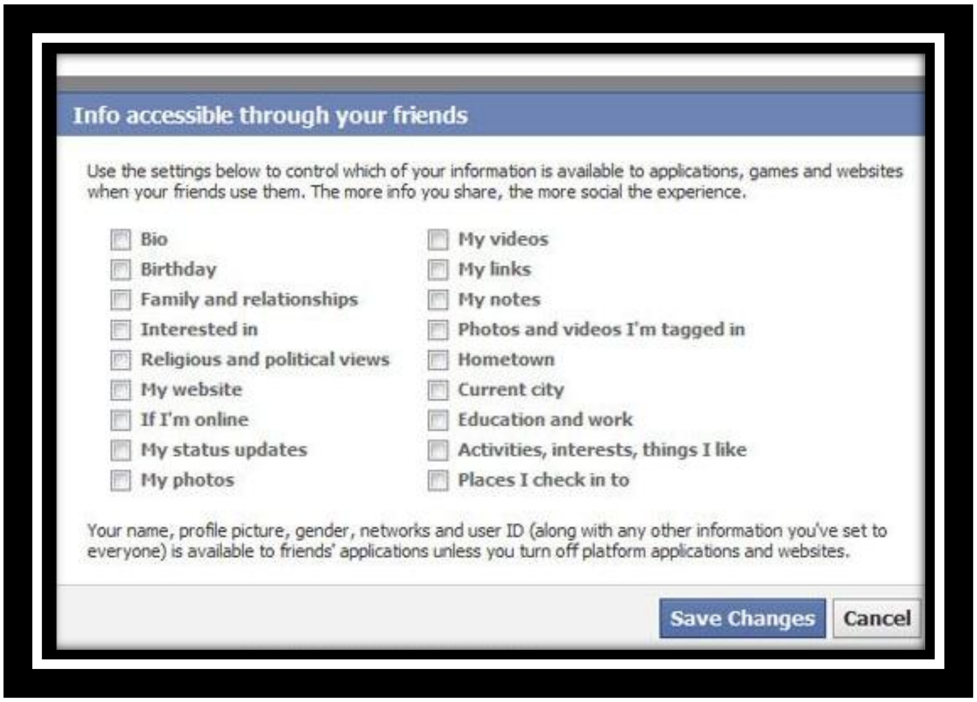
4.4 Facebook Security and Privacy

As Facebook is seen as the most popular social networking site that involves many security and privacy issues, we are going to have this section dedicated to its security and privacy.

4.4.1 Information your friends can share about you

When your Facebook friends use games and applications, those apps can request information about other friends, such as you, even if you do not use the app. This information may include your biography, your photos, your political views, and places where you check-in.

To prevent this, go to Account -> Privacy Settings -> Apps -> Websites. Click "*Edit Setting"s* next to "*Info accessible through your friends"*, and uncheck any necessary boxes, as shown in Figure 2.



Info accessible through your friends

Use the settings below to control which of your information is available to applications, games and websites when your friends use them. The more info you share, the more social the experience.

□ Bio
□ Birthday
□ Family and relationships
□ Interested in
□ Religious and political views
□ My website
□ If I'm online
□ My status updates
□ My photos
□ My videos
□ My links
□ My notes
□ Photos and videos I'm tagged in
□ Hometown
□ Current city
□ Education and work
□ Activities, interests, things I like
□ Places I check in to

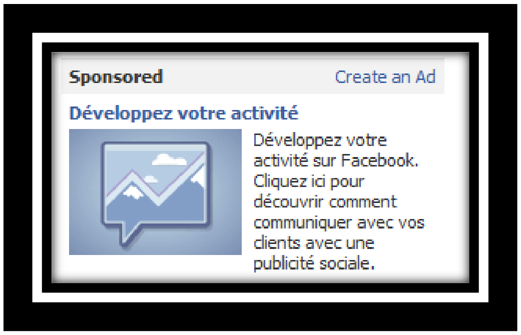
Your name, profile picture, gender, networks and user ID (along with any other information you've set to everyone) is available to friends' applications unless you turn off platform applications and websites.

Figure 2 Facebook shared information settings

4.4.2 Social ads

You have probably noticed ads in the margins of your Facebook profile and elsewhere on the site. A "social ad" pairs an advertisement with an action that a friend has taken, such as *"liking a page"*.

To opt-out and ensure that your Facebook actions will not be associated with an ad, open your Account Settings and click the "*Facebook Ads"* tab. From the drop-down menu, choose either "*No on e"* or "*Only my friends"*, depending on your preference.



Sponsored Create an Ad

Développez votre activité

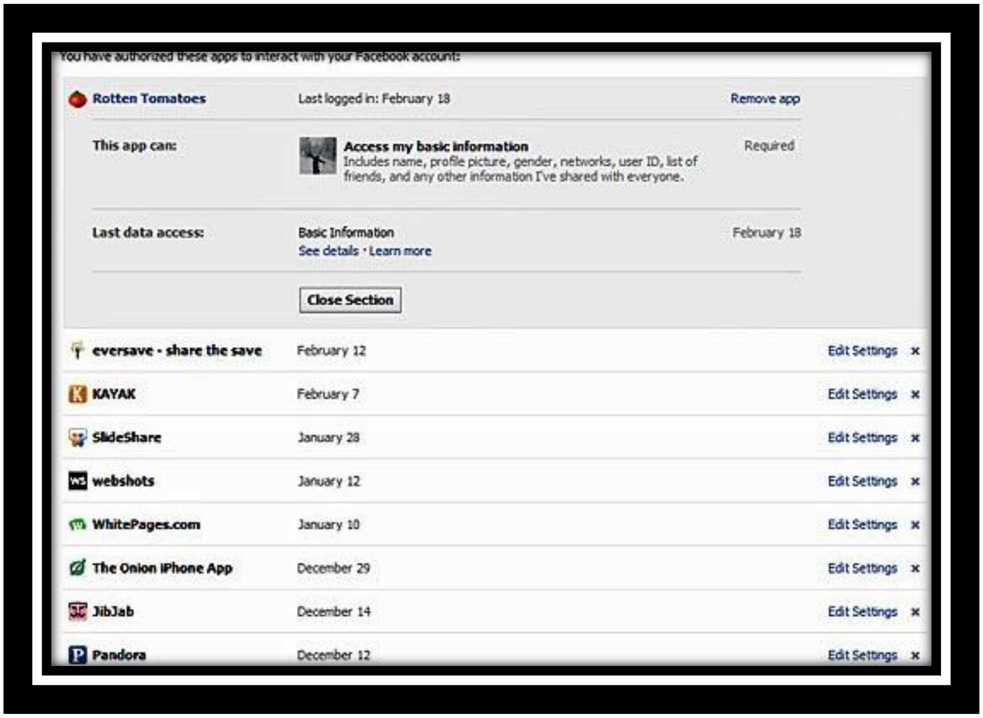
Développez votre activité sur Facebook. Cliquez ici pour découvrir comment communiquer avec vos clients avec une publicité sociale.

Figure 3 Facebook social ad example

4.4.3 Application settings

The *"Applications You Use"* dashboard gives you a detailed overview of which applications you're using and what information those apps can access.

To view the settings, choose Account -> Privacy Settings -> Applications -> Websites. Then, next to *"Apps you use"* choose *"Edit Settings"*. Here, you can see which applications you have authorized to interact with your account and when you authorized them, and you can edit the settings or delete the application entirely.



You have authorized these apps to interact with your Facebook account:

Rotten Tomatoes — Last logged in: February 18 — Remove app

This app can: Access my basic information — Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've shared with everyone. — Required

Last data access: Basic Information — See details · Learn more — February 18

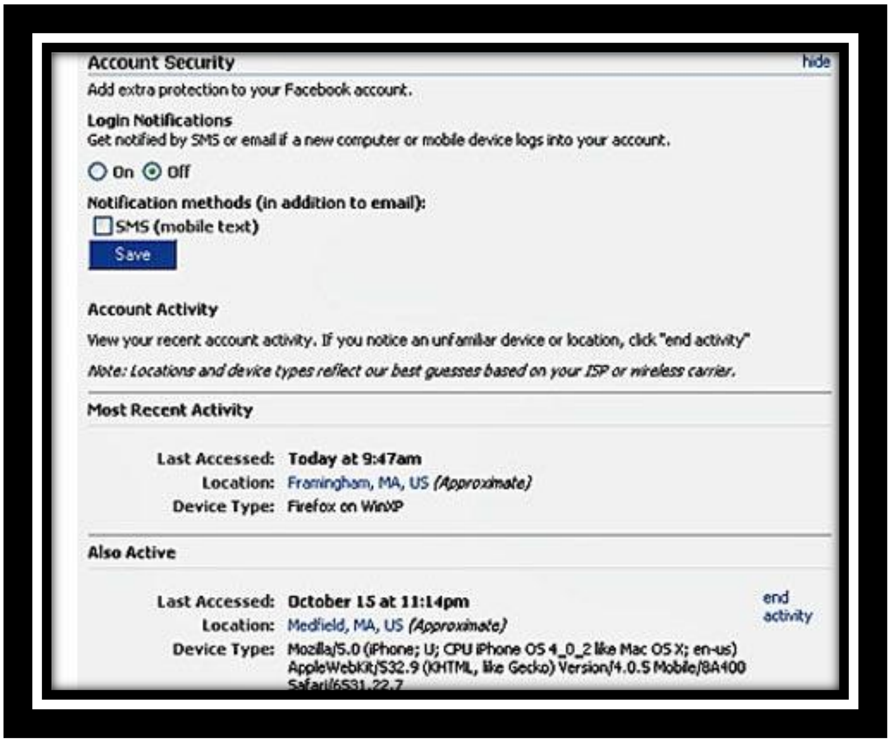
eversave - share the save	February 12	Edit Settings	×
KAYAK	February 7	Edit Settings	×
SlideShare	January 28	Edit Settings	×
webshots	January 12	Edit Settings	×
WhitePages.com	January 10	Edit Settings	×
The Onion iPhone App	December 29	Edit Settings	×
JibJab	December 14	Edit Settings	×
Pandora	December 12	Edit Settings	×

Figure 4 Facebook application settings

4.4.4 Remote sign-out

If you forget to log out of Facebook at the office or elsewhere, you can do so remotely. From Account, choose Account Settings ->Account Security. Here, you can choose to receive notifications via SMS or e-mail when a new computer or mobile device logs into your account.

You can also view details of the latest activity: the time, location, and device that accessed your account. If these locations seem suspicious, you can choose “*end activity”* to log out of the location.



Account Security

Add extra protection to your Facebook account.

Login Notifications
Get notified by SMS or email if a new computer or mobile device logs into your account.

○ On ● Off

Notification methods (in addition to email):
□ SMS (mobile text)

Account Activity

View your recent account activity. If you notice an unfamiliar device or location, click "end activity"

Note: Locations and device types reflect our best guesses based on your ISP or wireless carrier.

Most Recent Activity

Last Accessed: **Today at 9:47am**
Location: Framingham, MA, US *(Approximate)*
Device Type: Firefox on WinXP

Also Active

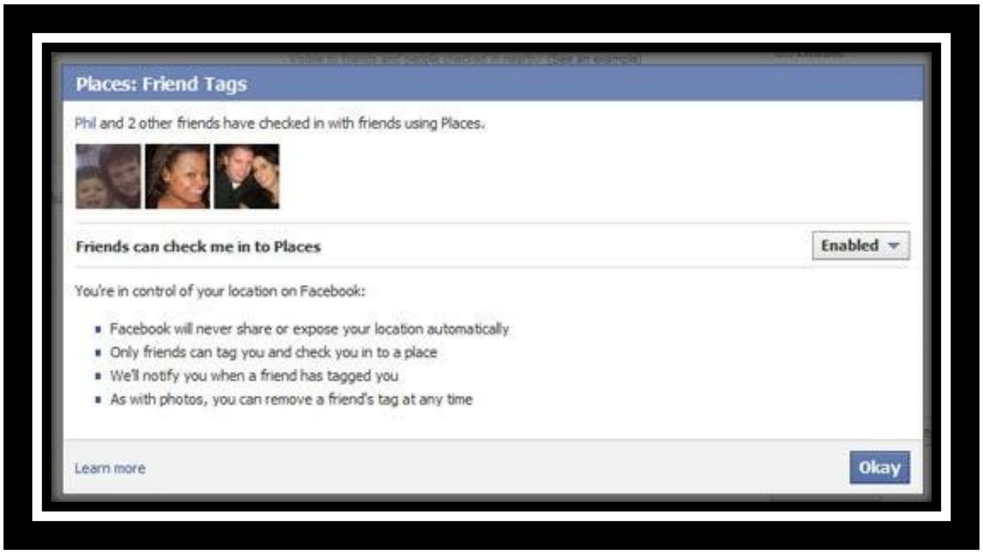
Last Accessed: **October 15 at 11:14pm**
Location: Medfield, MA, US *(Approximate)*
Device Type: Mozilla/5.0 (iPhone; U; CPU iPhone OS 4_0_2 like Mac OS X; en-us) AppleWebKit/532.9 (KHTML, like Gecko) Version/4.0.5 Mobile/8A400 Safari/6531.22.7

Figure 5 Facebook account settings

4.4.5 Facebook check-ins

If you have this feature enabled, your Facebook friends can tag you and *“check you in”* to a place. You receive a notification when you're tagged, and an update is posted on your wall telling your friends where you are and who you're with. You can remove the tag at any time.

If you want to disable the feature, go to Account -> Privacy Settings -> Customize Settings; scroll to the middle section *"things others share"* and click Edit settings next to *"Friends can check me in"* to *"Places"* to disable it.



Places: Friend Tags

Phil and 2 other friends have checked in with friends using Places.

Friends can check me in to Places Enabled

You're in control of your location on Facebook:

- Facebook will never share or expose your location automatically
- Only friends can tag you and check you in to a place
- We'll notify you when a friend has tagged you
- As with photos, you can remove a friend's tag at any time

Figure 6 Facebook places settings

4.4.6 Inclusion in "People Here Now"

Another important Facebook privacy issue if you use *"Places*" is whether you want to be included in a 'People Here Now' list once you check in to a location.

By default, your name and Facebook profile picture appear in the list, which is visible to anyone--friend or not--who checks in to the same location. To disable this setting, visit Account -> Privacy Settings -> Customize Settings, and uncheck the box at the bottom of the first section that reads *"Include me in People Here Now after I check in*".

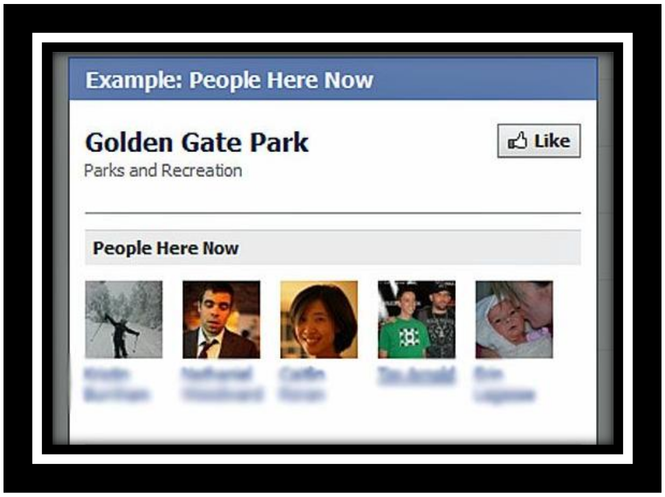
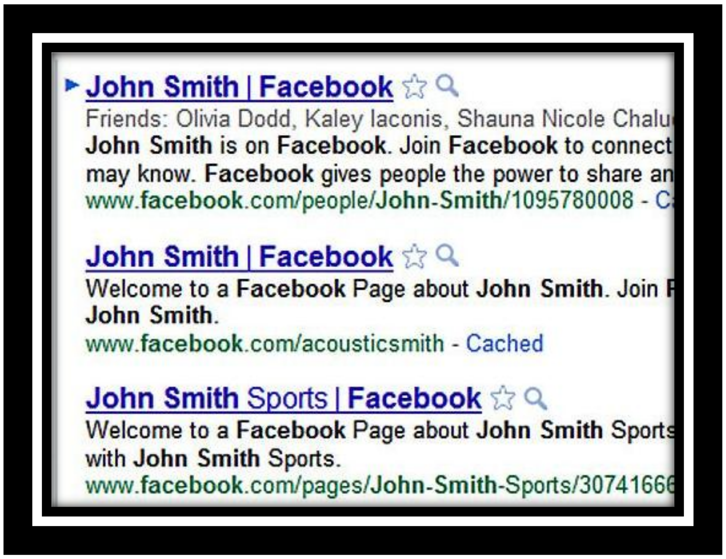


Figure 7 Facebook "People Here Now" settings

4.4.7 Appearing in search results

If someone *"googles"* your name, the search results may include your Facebook profile, your profile picture, and any other information you have made public.

To turn off this preference, go to Account -> Privacy Settings, and choose "*Edit your settings"* under Apps and Websites. Click "*Edit Settings"* next to the last option, "*Public search"*, and uncheck the box to disable it.



John Smith | Facebook
Friends: Olivia Dodd, Kaley Iaconis, Shauna Nicole Chalu
John Smith is on **Facebook**. Join **Facebook** to connect
may know. **Facebook** gives people the power to share an
www.**facebook**.com/people/**John**-**Smith**/1095780008 - C

John Smith | Facebook
Welcome to a **Facebook** Page about **John Smith**. Join F
John Smith.
www.**facebook**.com/acousticsmith - Cached

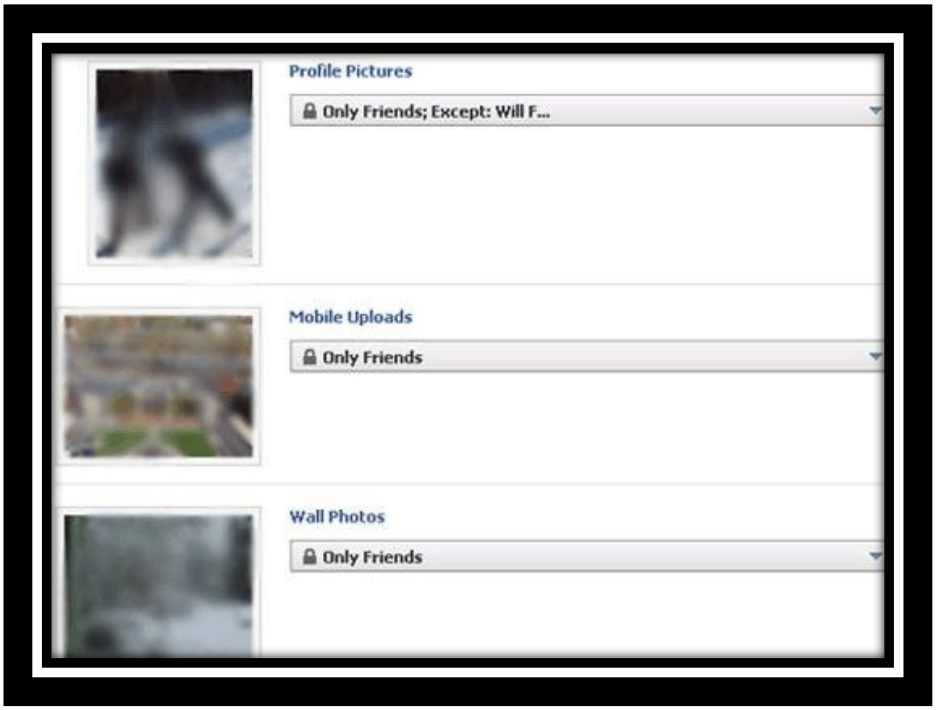
John Smith Sports | Facebook
Welcome to a **Facebook** Page about **John Smith** Sports
with **John Smith** Sports.
www.**facebook**.com/pages/**John**-**Smith**-Sports/30741666

Figure 8 Facebook public search settings

4.4.8 Photo albums

You may have set photos of you to be private, but what about your photo albums? You may not realize that the albums titled *"Profile Pictures"*, *"Mobile Uploads"*, and *"Wall Photos"* are usually visible by everyone, unless you edit your privacy settings.

Open your Privacy Settings page and choose "*Customize settings"*. At the bottom of the first section, click "*Edit album privacy"*. Here you will see every one of your photo albums, and the assigned privacy settings for each.



Profile Pictures

Only Friends; Except: Will F...

Mobile Uploads

Only Friends

Wall Photos

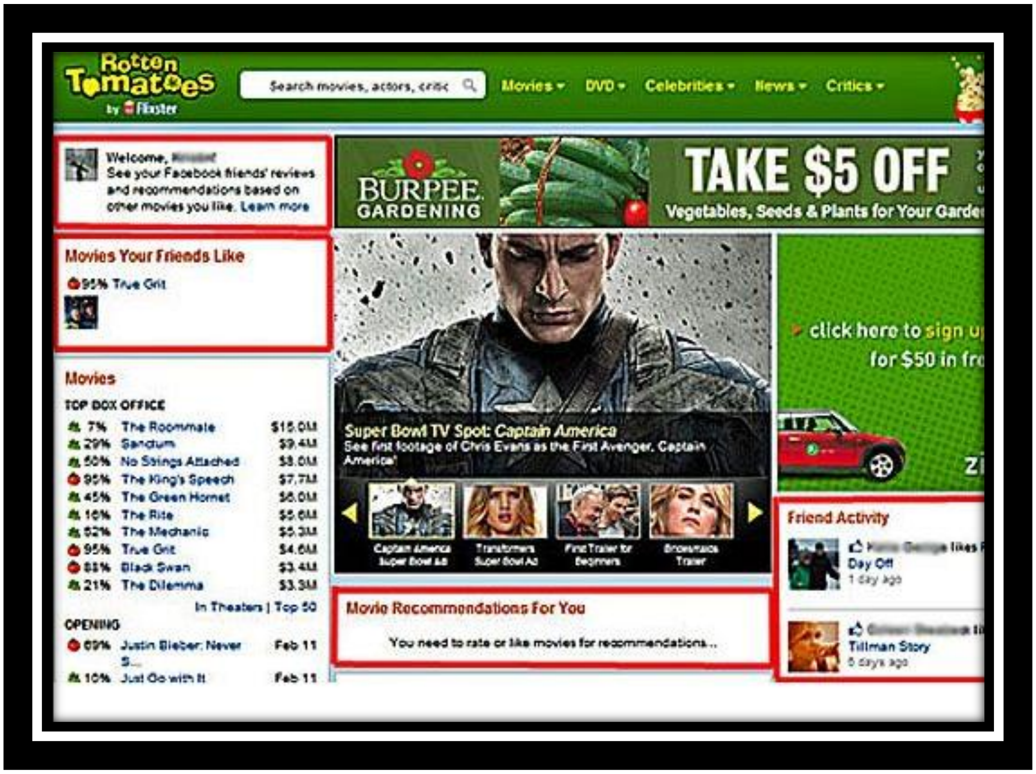
Only Friends

Figure 9 Facebook album privacy settings

4.4.9 Instant Personalisation

If you visit a site that supports Instant Personalization - Bing, Pandora, Yelp, or any of a number of others, you will see which of your friends have *"liked"* certain artists or news stories and be able to browse reviews that they have posted. Instant Personalization uses information that you made public on your Facebook profile to make recommendations.

Scroll to the bottom, click "*Edit Settings"* next to "*Instant personalization"*, and uncheck the box on the next page.



Rotten Tomatoes
by Flixster
Search movies, actors, critic
Movies ▾
DVD ▾
Celebrities ▾
News ▾
Critics ▾

Welcome, [redacted]
See your Facebook friends' reviews and recommendations based on other movies you like. Learn more

BURPEE.
GARDENING
TAKE $5 OFF
Vegetables, Seeds & Plants for Your Garde

Movies Your Friends Like

95% True Grit

Super Bowl TV Spot: Captain America
See first footage of Chris Evans as the First Avenger, Captain America!

Captain America Super Bowl Ad
Transformers Super Bowl Ad
First Trailer for Beginners
Brownsville Trailer
click here to sign u
for $50 in fr
Zi

Movies

TOP BOX OFFICE

7%	The Roommate	$15.0M
29%	Sanctum	$9.4M
50%	No Strings Attached	$8.0M
95%	The King's Speech	$7.7M
45%	The Green Hornet	$6.0M
16%	The Rite	$5.6M
52%	The Mechanic	$5.3M
95%	True Grit	$4.6M
88%	Black Swan	$3.4M
21%	The Dilemma	$3.3M

In Theaters | Top 50

OPENING

69%	Justin Bieber: Never S...	Feb 11
10%	Just Go with It	Feb 11

Movie Recommendations For You

You need to rate or like movies for recommendations...

Friend Activity

[redacted] likes F
Day Off
1 day ago

[redacted] li
Tillman Story
5 days ago

Figure 10 Instant personalization settings

4.5 General Parental Guidance

Just as adults need to help kids stay safe, they also need to learn not to overreact when they find out a child or teenager has been exposed to inappropriate material or strayed from a rule. Whatever you do, don't blame or punish your child if he tells you about an uncomfortable online encounter. Your best strategy is to work with him, so you both can learn from what happened and figure out how to keep it from happening again.

The challenges posed by the Internet can be positive. Learning to make good choices on the Internet can serve young people well by helping them to think critically about the choices they will face. Today it's the Internet; tomorrow it may be deciding whether it's safe to get into the car of someone a teen meets at a party. Later it will be deciding whether a commercial offer really is *"too good to be true"* or whether it really makes sense to vote for a certain candidate or follow a spiritual guru. Learning how to make good choices is a skill that will last a lifetime.

4.5.1 Tips for helping your kids use social networking sites safely

Here are some tips that you can practice at home as a parent:

- **Help your kids understand what information should be private**

  Tell them why it is important to keep some things about themselves, family members and friends to themselves. Information like their full name, Social Security number, street address, phone number, and family financial information like bank or credit card account numbers is private and should stay that way. Tell them not to choose a screen name that gives away too much personal information.

- **Use privacy settings to restrict who can access and post on your child's website**

  Some social networking sites have strong privacy settings. Show your child how to use these settings to limit who can view their online profile, and explain to them why this is important.

- **Explain that kids should post only information that you, and they, are comfortable with others seeing**

  Even if privacy settings are turned on, some, or even all of your child's profile may be seen by a broader audience than you're comfortable with. Encourage your child to think about the language used in a blog, and to think before posting pictures and videos. Employers, college admissions officers, team coaches, and teachers may view your child's postings. Even a kid's screen name could make a difference. Encourage teens to think about the impression that screen names could make.

- **Remind your kids that once they post information online, they cannot take it back**

  Even if they delete the information from a site, older versions may exist on other people's computers and be circulated online.

- **Know how your kids are getting online**

  More and more, kids are accessing the internet through their cell phones. Find out about what limits you can place on your child's cell phone. Some cellular companies have plans that limit downloads, internet access, and texting; other plans allow kids to use those features only at certain times of day.

- **Talk to your kids about bullying**

  Online bullying can take many forms, from spreading rumors online and posting or forwarding private messages without the sender's acknowledgement, to sending threatening messages. Tell your kids that the words they type and the images they post can have real-world consequences. They can make the target of the bullying feel bad, make the sender look bad and, sometimes, can bring on punishment from the authorities. Encourage your kids to talk to you if they feel targeted by a bully.

- **Tell your kids to trust their gut if they have suspicions**

  If they feel threatened by someone or uncomfortable because of something online, encourage them to tell you. You can then help them report concerns to the police and to the social networking site. Most sites have links where users can immediately report abusive, suspicious, or inappropriate online behavior.

- **Read sites' privacy policies**

  Spend some time with a site's privacy policy, Frequently Asked Questions (FAQs), and parent sections to understand its features and privacy controls. The site should spell out your rights as a parent to review and delete your child's profile if your child is younger than 13.

4.5.2 A few more tips to protect pre-teens

Many of the tips above apply for pre-teens, but parents of younger children also can:

- **Take extra steps to protect younger kids**

  Keep the computer in an open area like the kitchen or family room, so you can keep an eye on what your kids are doing online. Use the internet with them to help develop safe surfing habits. Consider taking advantage of parental control features on some operating systems that let you manage your kids' computer use, including what sites they can visit, whether they can download items, or what time of day they can be online.

- **Go where your kids go online**

  Sign up for and use the social networking spaces that your kids visit. Let them know that you're there, and help teach them how to act as they socialize online.

- **Review your child's friends list**

  You may want to limit your child's online “friends” to people your child actually knows and is friendly with in real life.

- **Understand sites' privacy policies**

  Sites should spell out your rights as a parent to review and delete your child's profile if your child is younger than 13.

5.0 Conclusion

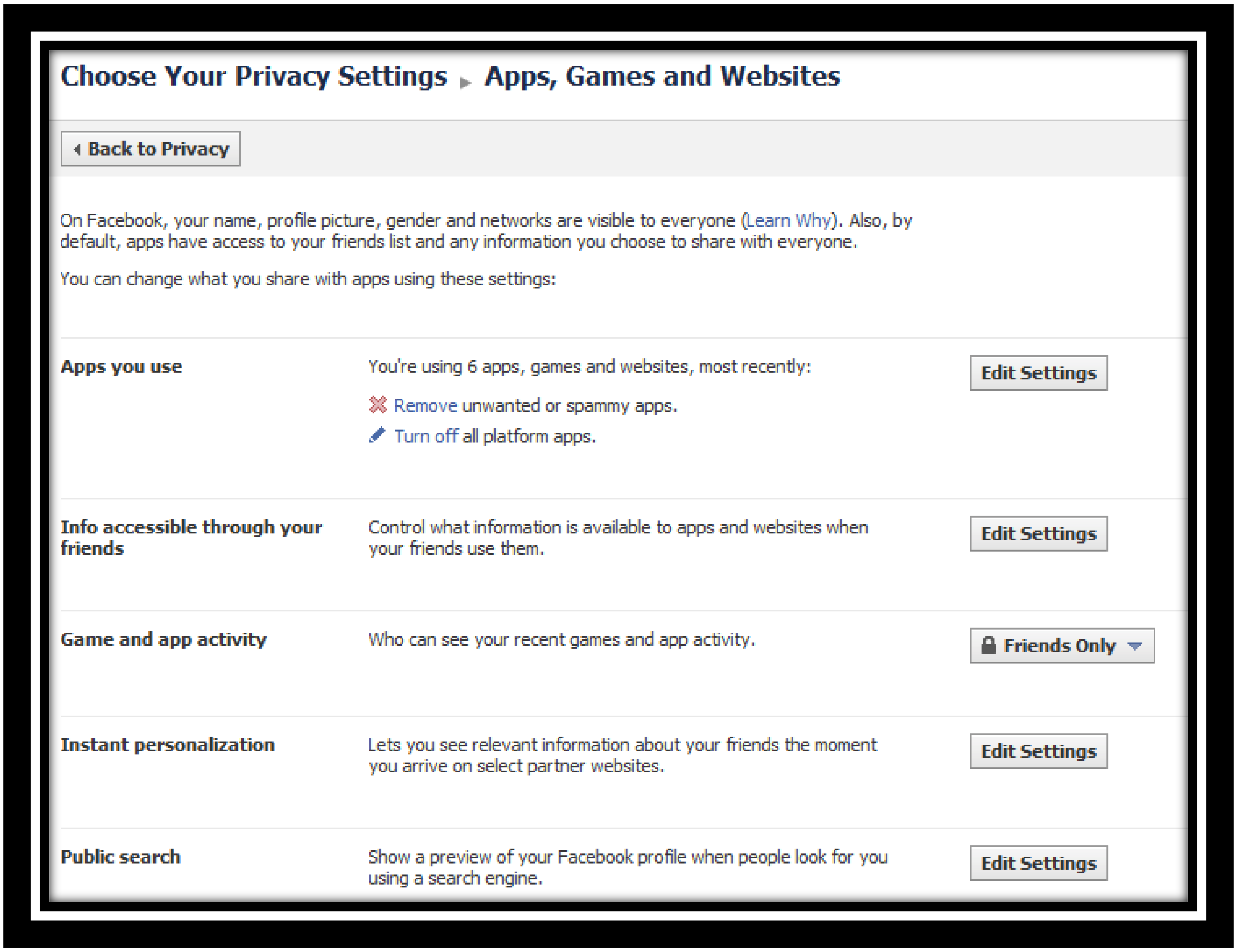
Social networking communities are an inherent part of today's Internet. People love using them to stay in contact with friends, exchange pictures, or just to pass the time when bored. With user groups with hundreds of millions of members, there are always some black sheep with malicious intent. There are a lot of cases of privacy breach, however many users do not even set the privacy settings provided by the web site itself and are unaware of the risks that come with sharing too much personal information. Sometimes they even post sensitive information like their own password for everyone to see. Social networks definitely can be entertaining, but users need to be aware of the risks involved and not trust everything they come across.

6.0 References

- University of Minnesota: http://www1.umn.edu
- Wikipedia: http://en.wikipedia.org
- Myspace: http://www.myspace.com
- Facebook: http://www.facebook.com
- Scribd: http://www.scribd.com
- OnGuard Online: http://www.onguardonline.gov
- Symantec: The Risks of Social Networking, Symantec, Security Response
- The telegraph: http://www.telegraph.co.uk
- AbsoluteSoftware: http://blog.absolute.com
- Anzmac: http://www.duplication.net.au
- Morehouse College, Guidelines for social networking: http://www.morehouse.edu
- Facebook Addition, The Brief Guide to Social Networking Addiction: http://www.thefacebookaddiction.com
- GFI Whitepaper, Social Networking and Security Risks: Social Networking and Security Risks: http://www.gfi.com
- PCWorld: http://www.pcworld.com
- The National Center For Victims of Crime: http://www.ncvc.org
- associatedcontent, Yahoo: http://www.associatedcontent.com

Appendix A

Facebook Privacy Settings



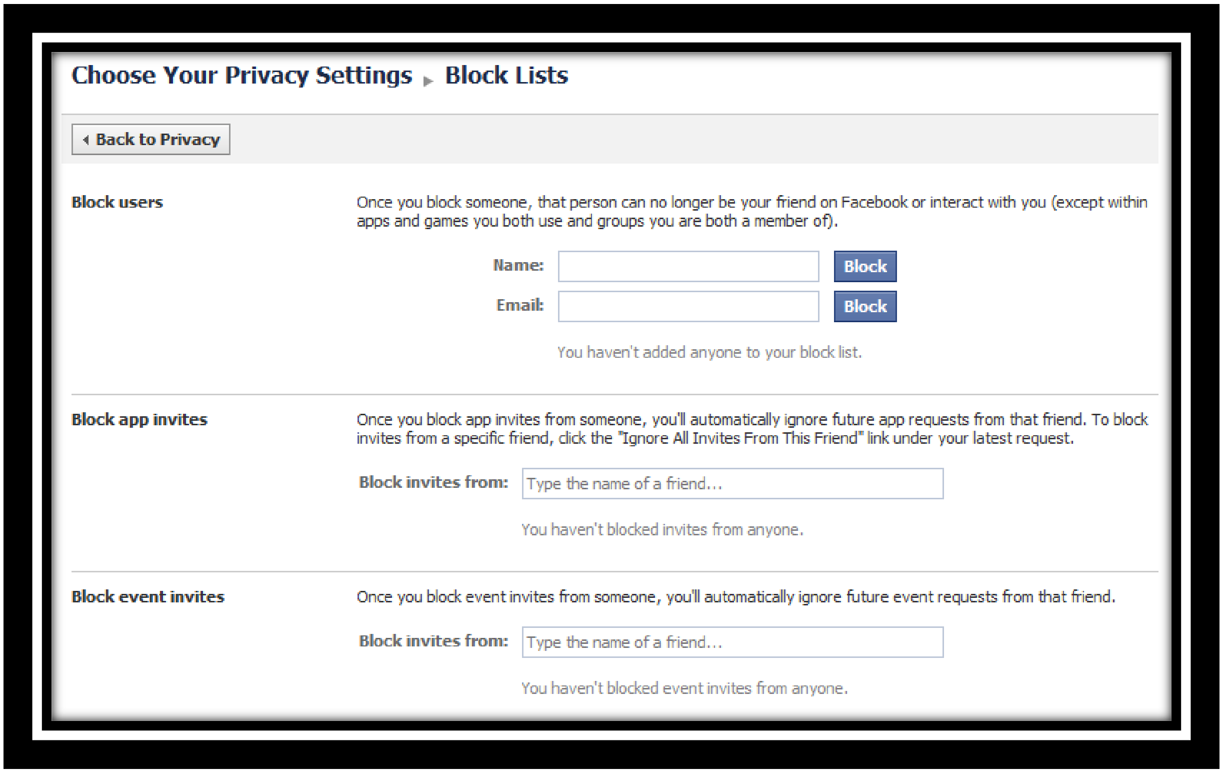
Choose Your Privacy Settings ▸ Apps, Games and Websites

On Facebook, your name, profile picture, gender and networks are visible to everyone (Learn Why). Also, by default, apps have access to your friends list and any information you choose to share with everyone.

You can change what you share with apps using these settings:

Apps you use	You're using 6 apps, games and websites, most recently: Remove unwanted or spammy apps. Turn off all platform apps.	Edit Settings
Info accessible through your friends	Control what information is available to apps and websites when your friends use them.	Edit Settings
Game and app activity	Who can see your recent games and app activity.	Friends Only ▾
Instant personalization	Lets you see relevant information about your friends the moment you arrive on select partner websites.	Edit Settings
Public search	Show a preview of your Facebook profile when people look for you using a search engine.	Edit Settings

Figure 11 Facebook apps, games and website settings



Choose Your Privacy Settings ▸ Block Lists

Block users

Once you block someone, that person can no longer be your friend on Facebook or interact with you (except within apps and games you both use and groups you are both a member of).

Name: Block

Email: Block

You haven't added anyone to your block list.

Block app invites

Once you block app invites from someone, you'll automatically ignore future app requests from that friend. To block invites from a specific friend, click the "Ignore All Invites From This Friend" link under your latest request.

Block invites from: Type the name of a friend...

You haven't blocked invites from anyone.

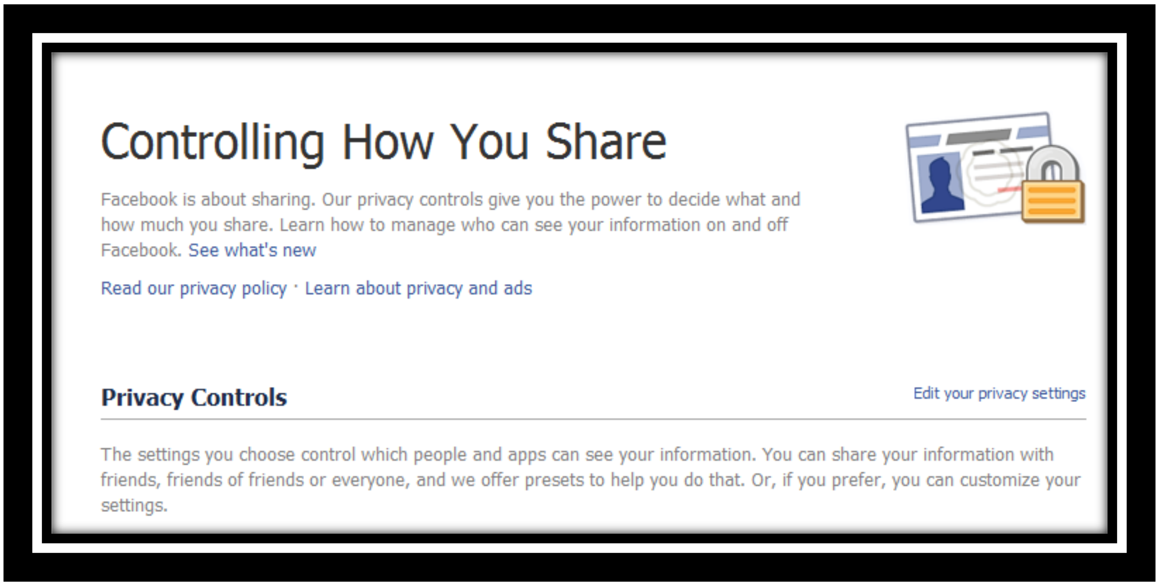
Block event invites

Once you block event invites from someone, you'll automatically ignore future event requests from that friend.

Block invites from: Type the name of a friend...

You haven't blocked event invites from anyone.

Figure 12 Facebook block lists settings



Controlling How You Share

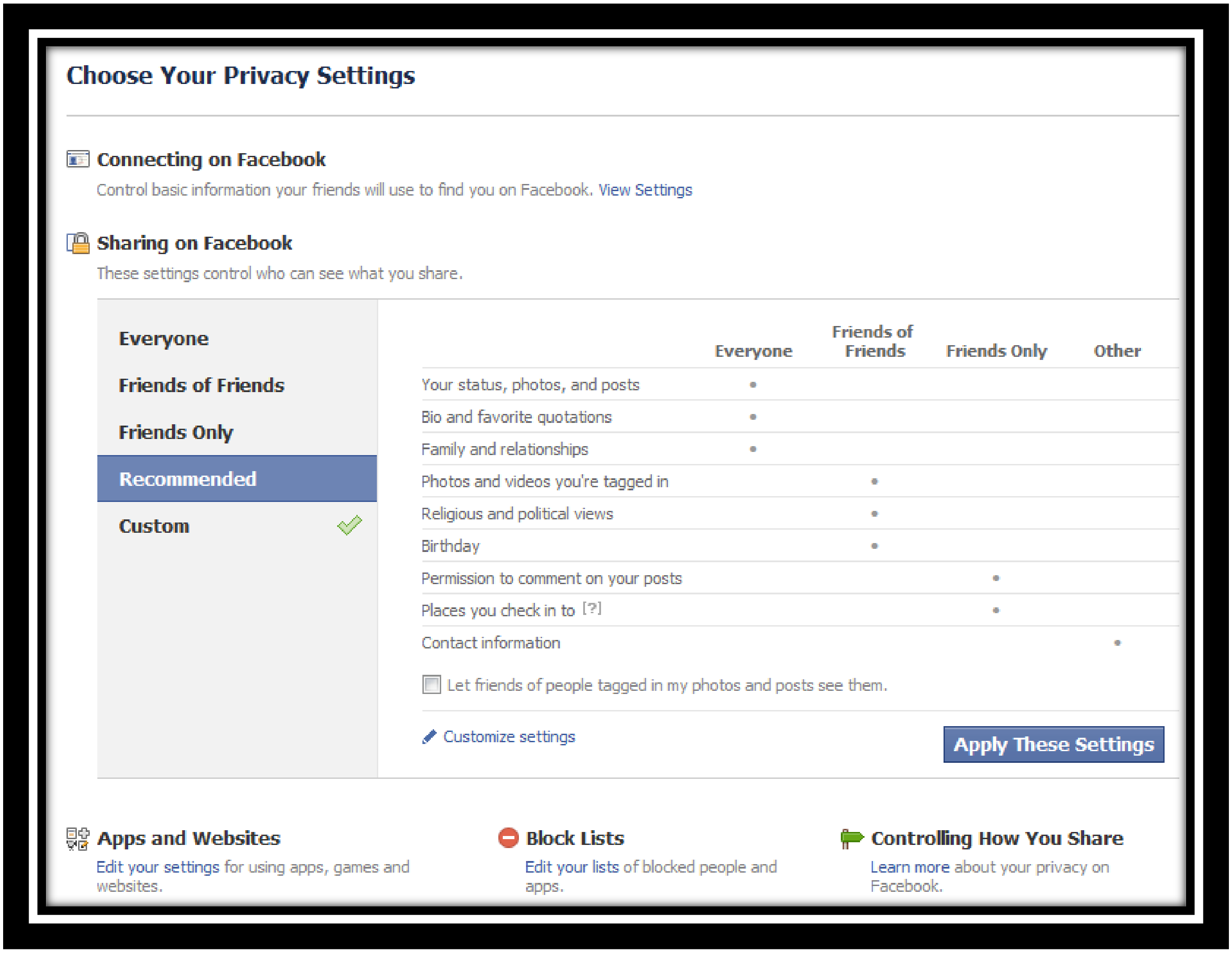
Facebook is about sharing. Our privacy controls give you the power to decide what and how much you share. Learn how to manage who can see your information on and off Facebook. See what's new

Read our privacy policy · Learn about privacy and ads

Privacy Controls

The settings you choose control which people and apps can see your information. You can share your information with friends, friends of friends or everyone, and we offer presets to help you do that. Or, if you prefer, you can customize your settings.

Figure 13 Facebook privacy controls



Choose Your Privacy Settings

Connecting on Facebook

Control basic information your friends will use to find you on Facebook. View Settings

Sharing on Facebook

These settings control who can see what you share.

Everyone

Friends of Friends

Friends Only

Recommended

Custom ✓

	Everyone	Friends of Friends	Friends Only	Other
Your status, photos, and posts	•			
Bio and favorite quotations	•			
Family and relationships	•			
Photos and videos you're tagged in		•		
Religious and political views		•		
Birthday		•		
Permission to comment on your posts			•	
Places you check in to [?]			•	
Contact information				•

□ Let friends of people tagged in my photos and posts see them.

Customize settings

Apps and Websites

Edit your settings for using apps, games and websites.

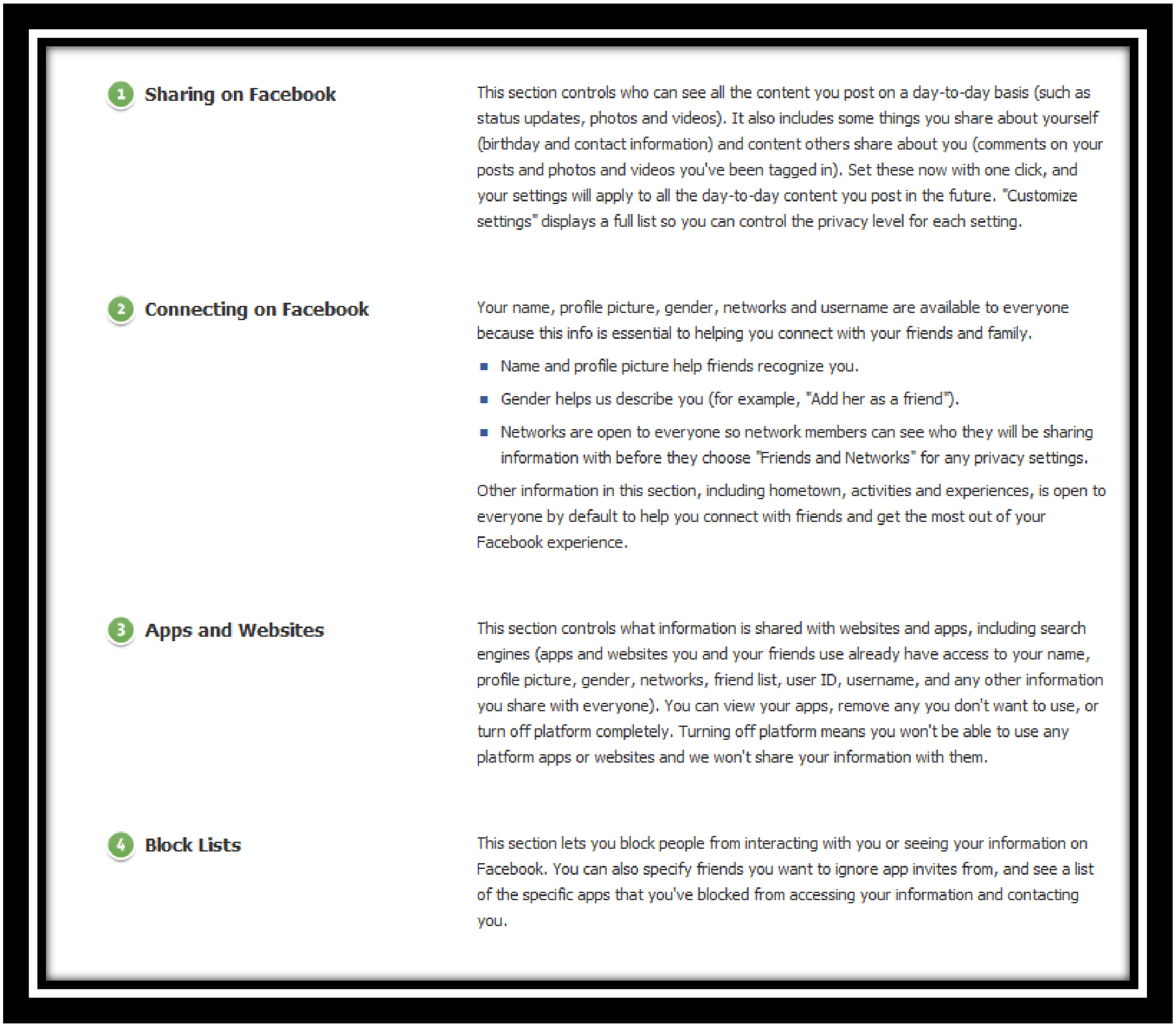
Block Lists

Edit your lists of blocked people and apps.

Controlling How You Share

Learn more about your privacy on Facebook.

Figure 14 Facebook recommended privacy settings



1 **Sharing on Facebook**

This section controls who can see all the content you post on a day-to-day basis (such as status updates, photos and videos). It also includes some things you share about yourself (birthday and contact information) and content others share about you (comments on your posts and photos and videos you've been tagged in). Set these now with one click, and your settings will apply to all the day-to-day content you post in the future. "Customize settings" displays a full list so you can control the privacy level for each setting.

2 **Connecting on Facebook**

Your name, profile picture, gender, networks and username are available to everyone because this info is essential to helping you connect with your friends and family.

- Name and profile picture help friends recognize you.
- Gender helps us describe you (for example, "Add her as a friend").
- Networks are open to everyone so network members can see who they will be sharing information with before they choose "Friends and Networks" for any privacy settings.

Other information in this section, including hometown, activities and experiences, is open to everyone by default to help you connect with friends and get the most out of your Facebook experience.

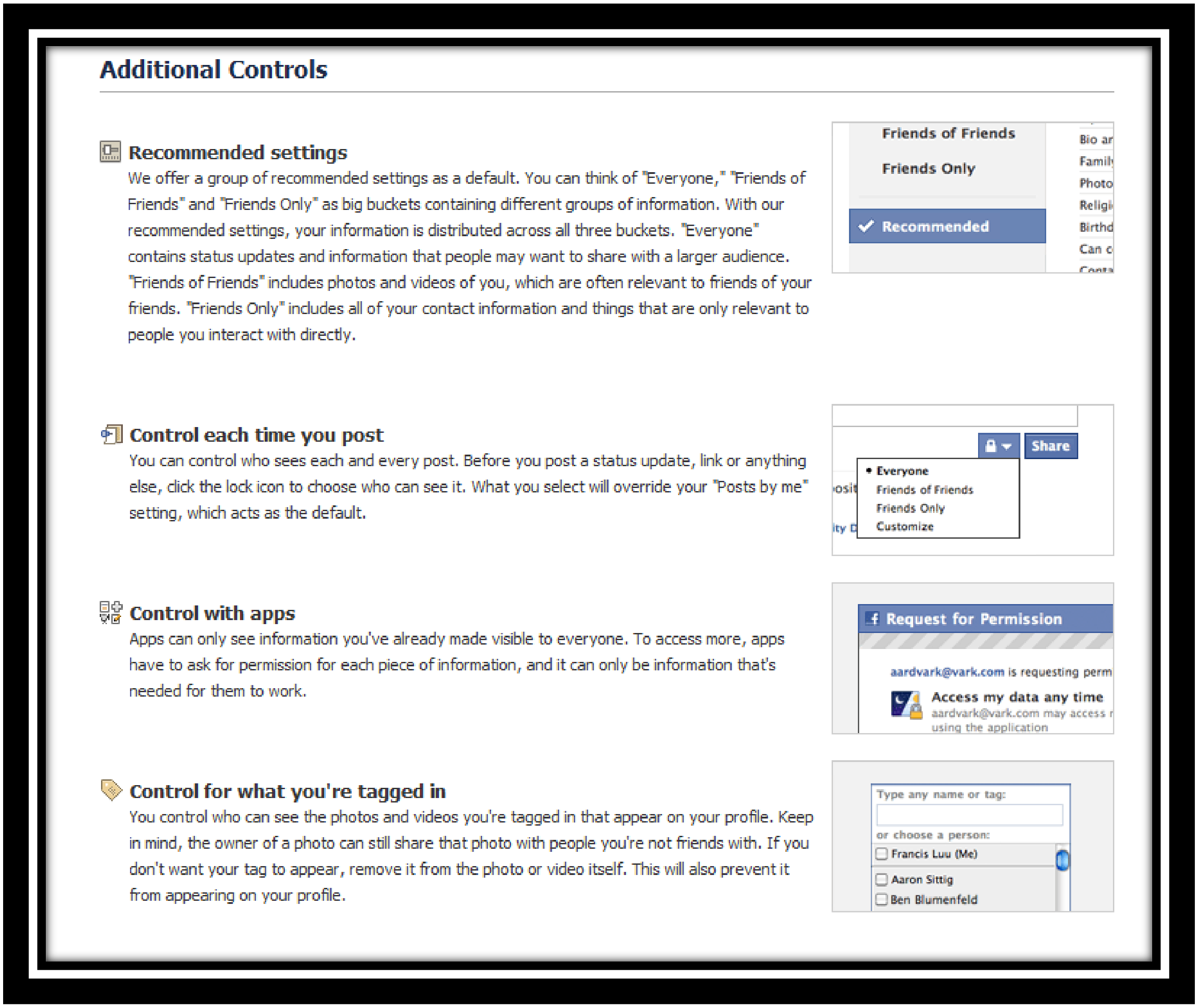
3 **Apps and Websites**

This section controls what information is shared with websites and apps, including search engines (apps and websites you and your friends use already have access to your name, profile picture, gender, networks, friend list, user ID, username, and any other information you share with everyone). You can view your apps, remove any you don't want to use, or turn off platform completely. Turning off platform means you won't be able to use any platform apps or websites and we won't share your information with them.

4 **Block Lists**

This section lets you block people from interacting with you or seeing your information on Facebook. You can also specify friends you want to ignore app invites from, and see a list of the specific apps that you've blocked from accessing your information and contacting you.

Figure 15 Facebook security control information



Additional Controls

Recommended settings

We offer a group of recommended settings as a default. You can think of "Everyone," "Friends of Friends" and "Friends Only" as big buckets containing different groups of information. With our recommended settings, your information is distributed across all three buckets. "Everyone" contains status updates and information that people may want to share with a larger audience. "Friends of Friends" includes photos and videos of you, which are often relevant to friends of your friends. "Friends Only" includes all of your contact information and things that are only relevant to people you interact with directly.

Control each time you post

You can control who sees each and every post. Before you post a status update, link or anything else, click the lock icon to choose who can see it. What you select will override your "Posts by me" setting, which acts as the default.

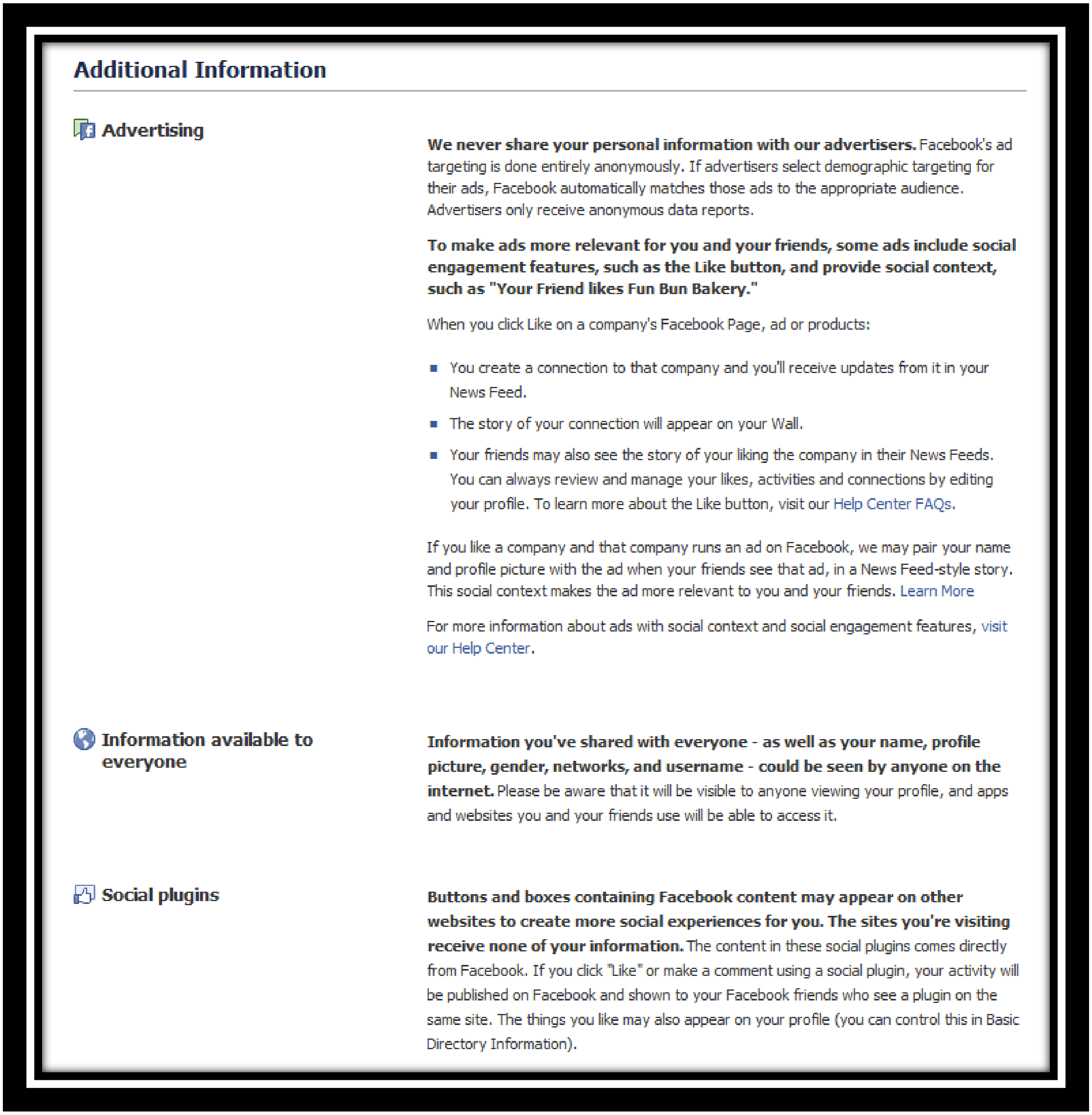
Control with apps

Apps can only see information you've already made visible to everyone. To access more, apps have to ask for permission for each piece of information, and it can only be information that's needed for them to work.

Control for what you're tagged in

You control who can see the photos and videos you're tagged in that appear on your profile. Keep in mind, the owner of a photo can still share that photo with people you're not friends with. If you don't want your tag to appear, remove it from the photo or video itself. This will also prevent it from appearing on your profile.

Figure 16 Facebook additional security controls



Additional Information

Advertising

We never share your personal information with our advertisers. Facebook's ad targeting is done entirely anonymously. If advertisers select demographic targeting for their ads, Facebook automatically matches those ads to the appropriate audience. Advertisers only receive anonymous data reports.

To make ads more relevant for you and your friends, some ads include social engagement features, such as the Like button, and provide social context, such as "Your Friend likes Fun Bun Bakery."

When you click Like on a company's Facebook Page, ad or products:

- You create a connection to that company and you'll receive updates from it in your News Feed.
- The story of your connection will appear on your Wall.
- Your friends may also see the story of your liking the company in their News Feeds. You can always review and manage your likes, activities and connections by editing your profile. To learn more about the Like button, visit our Help Center FAQs.

If you like a company and that company runs an ad on Facebook, we may pair your name and profile picture with the ad when your friends see that ad, in a News Feed-style story. This social context makes the ad more relevant to you and your friends. Learn More

For more information about ads with social context and social engagement features, visit our Help Center.

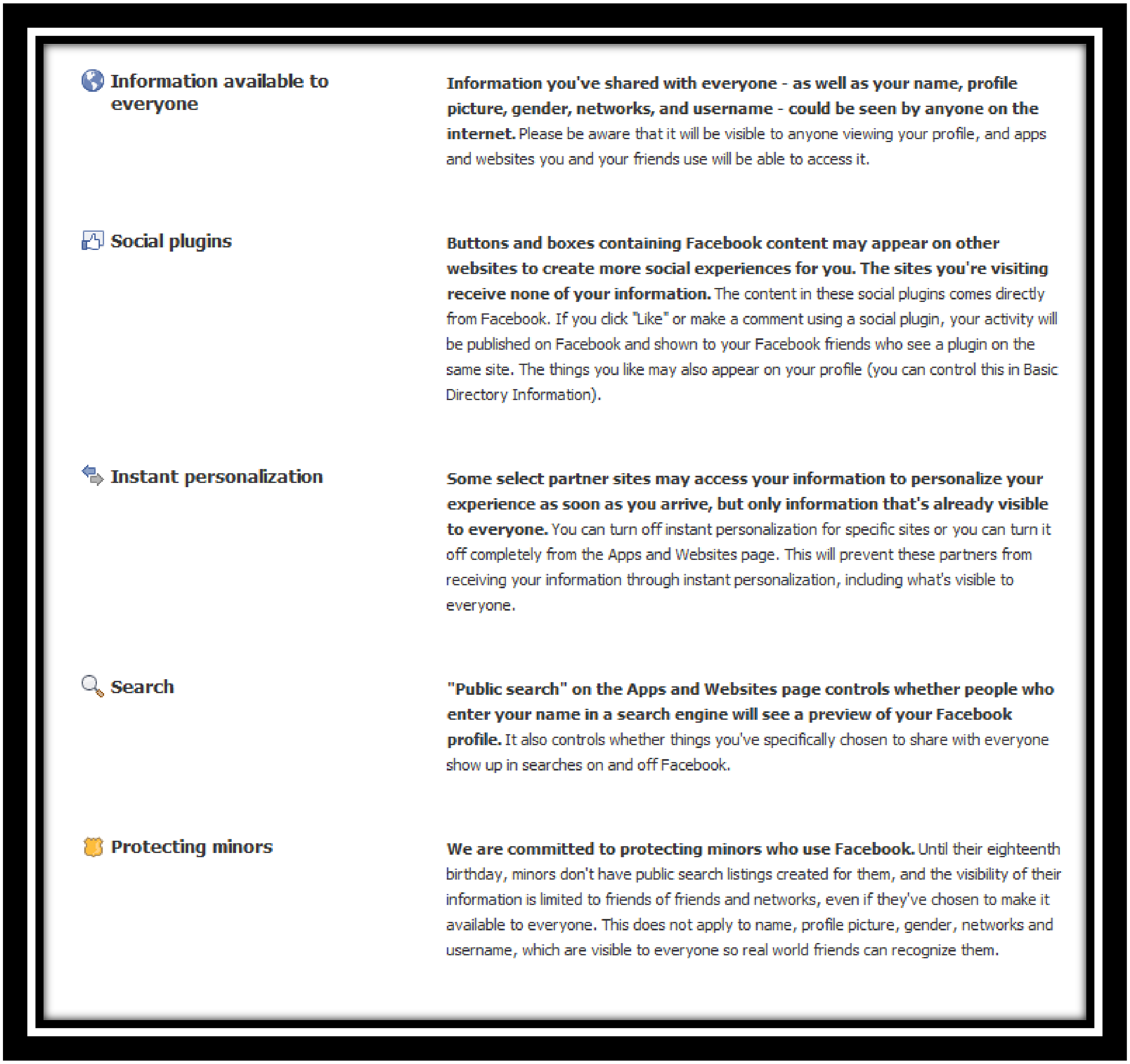
Information available to everyone

Information you've shared with everyone - as well as your name, profile picture, gender, networks, and username - could be seen by anyone on the internet. Please be aware that it will be visible to anyone viewing your profile, and apps and websites you and your friends use will be able to access it.

Social plugins

Buttons and boxes containing Facebook content may appear on other websites to create more social experiences for you. The sites you're visiting receive none of your information. The content in these social plugins comes directly from Facebook. If you click "Like" or make a comment using a social plugin, your activity will be published on Facebook and shown to your Facebook friends who see a plugin on the same site. The things you like may also appear on your profile (you can control this in Basic Directory Information).

Figure 17 Facebook additional security information (Part I)



Information available to everyone

Information you've shared with everyone - as well as your name, profile picture, gender, networks, and username - could be seen by anyone on the internet. Please be aware that it will be visible to anyone viewing your profile, and apps and websites you and your friends use will be able to access it.

Social plugins

Buttons and boxes containing Facebook content may appear on other websites to create more social experiences for you. The sites you're visiting receive none of your information. The content in these social plugins comes directly from Facebook. If you click "Like" or make a comment using a social plugin, your activity will be published on Facebook and shown to your Facebook friends who see a plugin on the same site. The things you like may also appear on your profile (you can control this in Basic Directory Information).

Instant personalization

Some select partner sites may access your information to personalize your experience as soon as you arrive, but only information that's already visible to everyone. You can turn off instant personalization for specific sites or you can turn it off completely from the Apps and Websites page. This will prevent these partners from receiving your information through instant personalization, including what's visible to everyone.

Search

"Public search" on the Apps and Websites page controls whether people who enter your name in a search engine will see a preview of your Facebook profile. It also controls whether things you've specifically chosen to share with everyone show up in searches on and off Facebook.

Protecting minors

We are committed to protecting minors who use Facebook. Until their eighteenth birthday, minors don't have public search listings created for them, and the visibility of their information is limited to friends of friends and networks, even if they've chosen to make it available to everyone. This does not apply to name, profile picture, gender, networks and username, which are visible to everyone so real world friends can recognize them.

Figure 18 Facebook additional security information (Part II)