

BeSafe in CyberSpace



**A Family
Guide to
CyberSafety**

By Mark Seguin

No part of this book may be reproduced or transmitted in any form or means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval systems, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher.

Requests to the Publisher for permission should be addressed to Permissions Department, TBG Solutions, Inc.

*PO Box 8421, Tyler, Texas 75711
(903) 533-9123, fax (903) 533-0088.*

TABLE OF CONTENTS

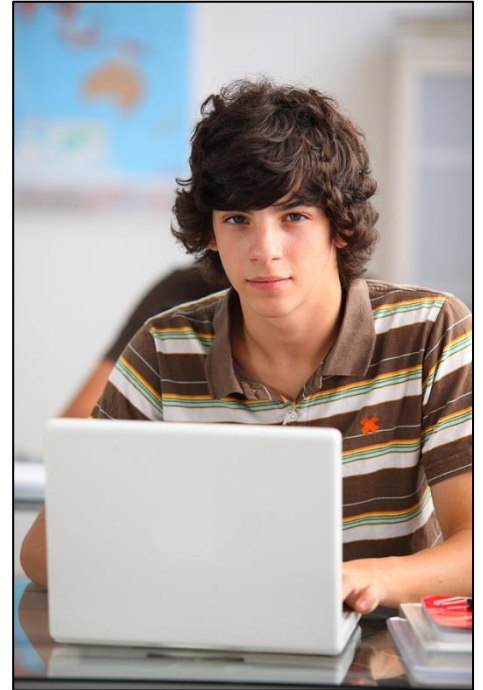
Safer Social Networking	2
Tips for Parents	3
Tips for Your Kids & Teens	4
Cyberbullying	6
Tips for Parents	7
Tips for Your Kids & Teens	8
Sexting/Texting	9
Tips for Parents	10
Tips for Your Kids & Teens	10
Passwords	11
Tips for Parents	11
Tips for Your Kids & Teens	12
Laptop/Computer/iPad/iPod Touch Safety	12
Tips for Parents	12
Tips for Your Kids & Teens	15
iTunes Content Restrictions	15
Advice for Parents	15
Smartphone Safety	18
Tips for Parents	18
Tips for Your Kids & Teens	19
Identity Theft	20
Learn the Lingo	23
Helpful "How To's"	24
How to Review Browsing History	24
How to Turn off Geo-Tagging	25
How to Set Up a Facebook Page - Safely	27
How To Report or Block Someone on Facebook	38
How to Unfriend Someone on Facebook	38
How to Secure an Existing Facebook Page	39
How to Deactivate or Delete your Facebook account (there IS a difference):	47
How to Register and Use Twitter	48
How to Use Instagram Safely	49
How to Safely Use Google+	59
How to Safely Use Other Social Media Platforms	64
Additional Resources & Websites	65
Resource Websites for the Family	65
Internet filtering software:	65
Family Alternative to Facebook/Google+:	65
Family Internet Contract	65
About the Author	67

Introduction

The internet has become an essential part of life; it is a powerful resource providing opportunity to people of all ages to communicate in new ways. For children, growing up with the internet is a necessary tool. Their entire lives have been surrounded by online technology, many starting to use the internet at a very young age.

However, there are risks in participating in internet activity. Harassment, stalking, identity theft and even blackmail and kidnapping are risks that could come from exposing too much information online. It is important to know how to use the internet safely in order to have a positive online experience. It is important for kids and parents to know how to apply these skills at home, at school and in public places such as the library, and internet hot spots such as coffee shops and restaurants.

The best way to protect kids online is to talk to them. This guide is to provide practical advice and information on safe internet use. In learning and applying safe internet skills, and sharing these with their children, parents can help to keep them safe, and ensure that the whole family enjoys positive internet experiences. Not all internet users will experience problems.



Limit of Liability/Disclaimer of Warranty: The area of internet safety and security is very broad and encompasses many aspects. Therefore, only key issues are covered in this guide. Users need to use their own judgment in how to protect their children and themselves and make their own inquiries about what is best for their family and situation. No warranties or guarantees of any kind, either express or implied, including the warranty of fitness for a particular purpose are made by this information. You should consult with a professional where appropriate. Neither the publisher nor the author shall be liable for any loss of profit or any other commercial damages including but not limited to special, incidental, consequential, or other damages.

Safer Social Networking

Children and teens use a variety of services to communicate online. These include social networking sites, chat rooms, blogs, forums, email, online games, virtual worlds and instant messaging. Internet users may be able to chat in real time, post opinions, send files, view others through webcams and publish and share personal information including photographs. These forums can be a great way to keep in touch with friends and family and basically just hang out and visit. Facebook alone is over the one billion mark of active users.

Social networking sites have different purposes, including:

- **Facebook, Google+, MySpace** – create communities of friends (for ages 13 and over)
- **Fanlala.com** for kids 12 and under to create groups of friends, post photos, to “hang out”
- **YouTube and Google Video** – create, download and upload video content
- **Facebook, Google+, Photo-**
- **bucket, Flickr and Instagram** – share still photos and video and comments
- **Pinterest** – create online bulletin boards of interesting ideas, websites, art and other interests



People often forget who they are communicating with and who might see the information they post. It is important for internet users of all ages to stop and think about how their posts or messages will affect others as well as themselves. It's often easier to say and do things online that they might not do in “real life”.

No matter how much someone knows about the internet, it is changing so fast that even experts are constantly in learning mode. Due to the frequency with which social networking changes, check your privacy settings often; weekly would be advantageous.

Social Media is increasingly being used as a background screening tool by:

Employers

Parents

Scholarship Committees

School Administrations

Colleges

Law Enforcement Agencies

and more...

This past school year in Texas, a high school senior received a full-ride scholarship, worth about \$150,000-\$200,000. The Scholarship Committee does a social media review of all applicants. Apparently, the young lady had been at a party where there were drugs and alcohol involved because she posted pictures of the participants on her Facebook page. Although she was not in any of the pictures, the Scholarship Committee deemed her guilty by association and she lost the full scholarship. What we put on Facebook and photos can have dire consequences on our lives.

In another instance, a young woman applied for a job at a local restaurant and the employer did a screening check on her Facebook profile. Apparently, her boyfriend had taken an inappropriate picture of her and it had gone viral. Due to her indiscretion, the restaurant was no longer interested in hiring her. Social Media is now the number one background screening tool used by employers

Tips for Parents

- **Realize** that you are not a customer. Social networking sites consider each user inventory. Data about interests, likes, location, activities, travels, birthdates, photographs, addresses and even pet's names are used to gather data about the user. This information is then sold to advertisers. This same information, however, is just as valuable to an identity thief or scam artist. All this information is neatly bundled in one location and all it takes is the scammer to become your "friend" to disclose your personal profile. Depending on how your settings are configured, your data may be available to everyone and not even require someone to be a "friend" to access your information.
- **Be aware** that social networking sites such as Facebook and Google+ require that a user must be 13 years of age or older. These sites have some specific safety measures in place for teens that will only be in effect if you are honest about your teen's birth year when registering for an account.
- **Look** into using a site such as Fanlala.com for children 12 years of age and younger as a social networking alternative to Facebook. They have extra security measures in place and are specifically geared for youth.
- **Check** privacy settings often on social networking sites such as Facebook and Google+. It is not uncommon for them to change without notice to you, so be proactive about protecting yourself and your family.
- **Read** the privacy policy and privacy help page for the social networking sites you and your child use.
- **Learn** how to delete and deactivate your social media pages and teach your child how to do the same.
- **Keep** your computer in a public or common area of your home. Set up an internet content filter or other security software and update it often.
- **Consider** creating your own social networking profile in sites such as Facebook and Google+ so you can "friend" or "circle" your child and see for yourself what they are doing. By being involved, you also help keep them safe.
- **Talk to your child** about unsuitable websites, pornography and digital disrespect. This way, they can be prepared and aware so if they are inadvertently exposed they will know what to do.

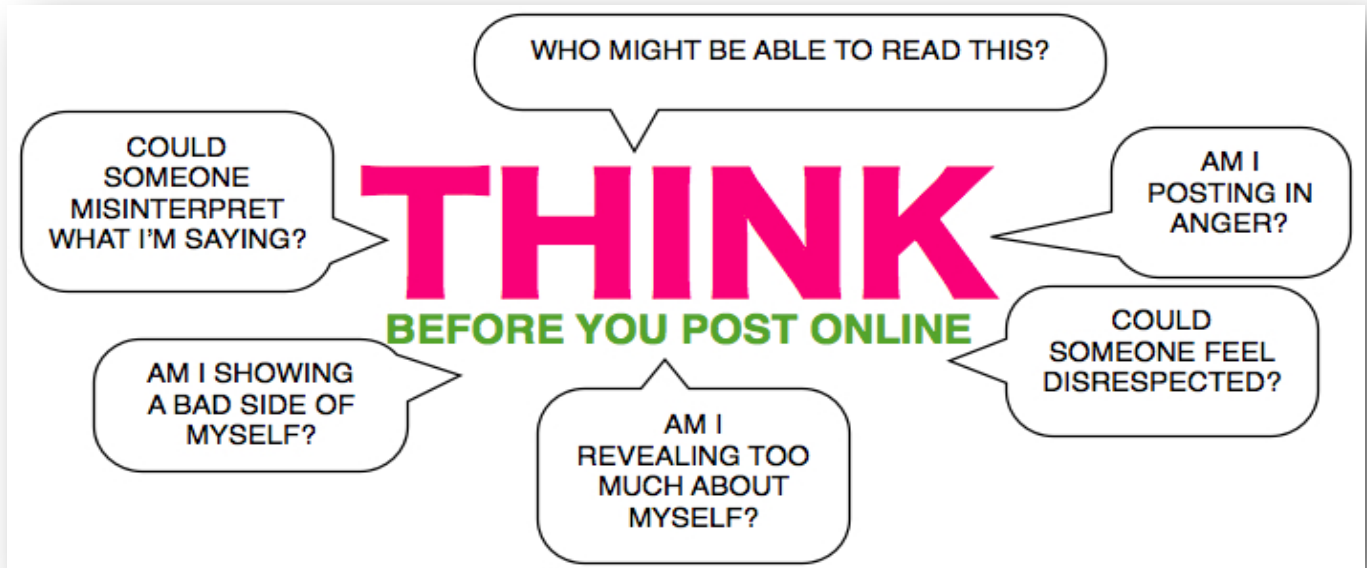
- **Stay educated** about your child's use of technology – ask them to show you how social networks work. Set up your own account, ask to join your child's "friends" list or "circle" and see for yourself what they are doing. By being involved, you also keep them safe.
- **Learn how** to turn off geotagging (see page ** for "How to".)
- **Set an example** by modeling appropriate use of technology by refraining from sending or forwarding offensive jokes and mean comments and by reporting hateful comments and harassment when it occurs.
- **Help your child** set up their profile to make sure that they don't put too much personal information online. Help them identify what is and isn't appropriate to post online.
- **Don't discuss** travel plans online made by you, your spouse or your family. This can alert others to your current whereabouts and activities of your personal life.
- **Check** the privacy settings for each service and find out how to block other users and report abuse. Hopefully you will never need to do this, but it's good to be prepared.
- **Talk to your child** about who they should make "friends" with or communicate with online.
- **Discuss** the amount of time your child can spend online and ensure they maintain an online and offline balance in their life. Remind them of their other responsibilities and encourage outside activities, hobbies and face-to-face time with friends.
- **Report** abuse or inappropriate content to the website administrator and show children how to do this as well.
- **Raise** your kids to be digitally respectful. Good manners and respect are vital online and offline.
- **Contact** police if you think a child is in immediate danger from any contact made online.
- **Learn** how to block people. Your kids may not want to see messages from a particular person or receive private messages from them.
- **Tell kids** not to open messages from people they don't know and to delete them right away.
- **Help them beware** of a stranger's "friend" request. They may be an adult posing as a kid to take advantage of your child. These predators are very skilled at luring kids with pornography.
- **Emphasize** the importance of keeping passwords secret: they are not to be shared with friends – no matter how close a "friend" they may be.

Tips for Your Kids & Teens

- **Think before you post.** (this term includes tweeting, blogging, commenting, writing on a wall, texting, etc.) Content posted online will likely be there forever. You can put it up, but can't always take it down.



- **Make sure** you don't put any key personal information on your profile or timeline. This includes phone number, personal email address, home address or the name of your school. Be careful, when you post photos that they don't include any of this information like geo-tags.
- **Keep in mind** you are not a "customer" of Facebook, search engines (i.e. Google and Bing) or any other social networking sites, nor are they free. You are inventory and the price you pay is privacy: your information such as Likes and activities is gathered and then sold.
- **Check with your parents** if you do decide to give out personal information or put it on your profile.
- **Use the privacy settings.** Learn how to make your profile or timeline private so only people you accept as friends can see what you are posting. Privacy settings options change often so it can be good to check that the controls are blocking information from outsiders effectively.
- **Don't** post information or photos that you wouldn't want everyone to see.
- **Remember** not everyone is who they claim to be. For example, an adult perpetrator could be posing as a 15-year old girl. Although it is great to have online friends, including them on your "friends" list allows people who do not know you to learn all about you. This information could be used for a scam, to steal your identity or worse.
- **Keep your online friends online.** Remember that online friends are really strangers no matter how long they have known you online. If you do want to meet someone that you haven't met so far in person, ask a parent or another trusted adult to go with you and always meet in a public place, preferably during the day.
- **Keep in mind** the best online friends are people we know offline.
- **Just Say No!** Free offers are usually too good to be true and can end up costing you a great deal.
- **Do not respond** if someone sends you unkind or inappropriate messages or asks you to do something that makes you feel uncomfortable or scared. Tell your parents or another adult you can trust immediately.
- **Do not share** passwords with friends – no matter how close you are with them. Passwords are private.
- **Stop and think** before you "check in" somewhere. Geo-locators tell strangers where you are and not everyone needs to know where U R.
- **Remember** some things were never meant to be shared.
- **Imagine** what you would think if you received the message you are planning to send.
- **Be considerate.** Post only comments you would be happy to receive yourself. Do not post photos of other people without their permission. Remember, when you post photos you might be compromising the privacy of your friends too. Photos may also be linked with geo-locators which can expose you or your friends' location.
- **Tone down** your speech. Using all caps, bold fonts and long rows of exclamation points online is the equivalent of yelling.
- **Limit contact.** Although it is flattering to have lots of friends, it also increases your exposure to deceitful practices by others. Only communicate with people you would be friends with in person.
- **Be suspicious** of online quizzes, games, apps and causes. Many of these interactive methods may be gathering your information to be sold to marketing companies or to profile you for identity theft.



Cyberbullying

Cyberbullying can result in the child or teen experiencing social, psychological and academic problems. Teens typically have their phones with them 24/7. This means they are susceptible to victimization (and able to act on mean intentions toward others) around the clock. Because of a measure of anonymity, it is also easier to be hateful using typed words rather than spoken words face-to-face.

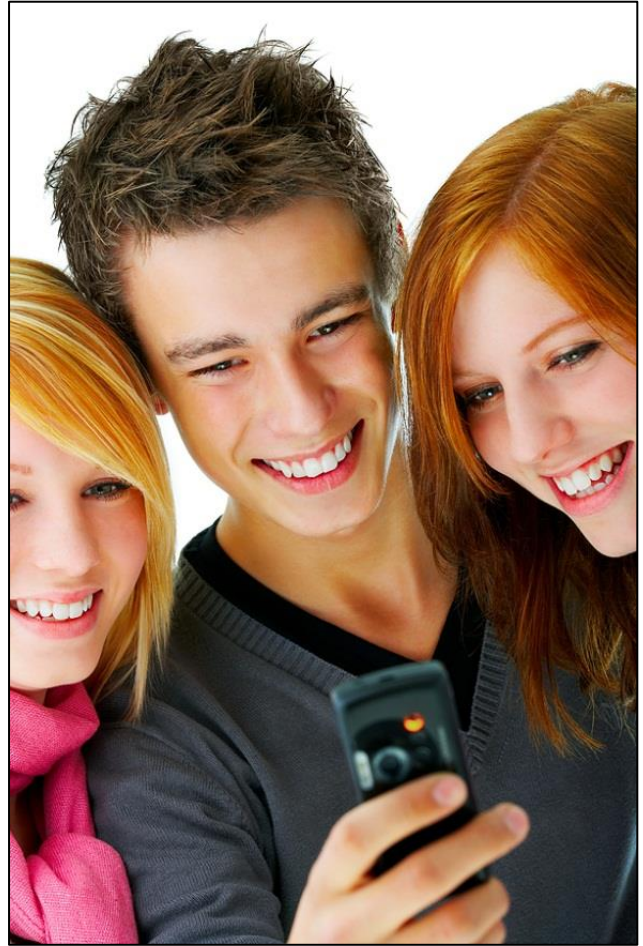
Cyberbullying (or digital disrespect) involves repeated harassment or behavior that threatens, humiliates or intimidates someone. This includes sending abusive texts or emails, excluding others from online communication or posting unkind messages or inappropriate images on social networking sites.

Cyberbullying can also be used as a dating violence tool. Pain and suffering may very well result from cyberbullying in romantic relationships. Technological devices allow abusers to feel constantly connected to (and within "reach" of) their dating partner, who often feels that he or she has no escape from the torment. Because teens constantly have their phones with them, this harassment is amplified. Harassment by excessive texting and inquiries ("where are you," "what are you doing," "who are you with") is digital disrespect.

Parents should look for signs that their child or teen might be a victim of cyberbullying, including having nightmares, avoiding school, acting sad or withdrawn, or suddenly showing disinterest in computers or rapidly switching screens. In addition, research has revealed a link between cyberbullying and low self-esteem, family problems, academic problems, school violence, and delinquent behavior. Finally, cyberbullied youth also report having suicidal thoughts. Not all children are equally at risk online, and the children who are most at risk online are those who are most at risk in “real life,” or offline.

Tips for Parents

- **Talk to your child** about cyberbullying before it happens. Make plans to address cyberbullying that you are both comfortable with, so your child knows what to expect if they do report their concerns to you.
- **Establish** one or two other trusted adults your child is comfortable to approach about their concerns.
- **Be aware** of what your child is doing online and explore it with them.
- **Keep** the computer in a shared or visible place in the home.
- **Work hard** to keep the lines of communication open so your child will be comfortable to talk to you if something is worrying them. Help your child to develop the necessary skills to interact safely and respectfully online.
- **Discuss** the kinds of sites that are okay to explore and those that are not, and have clear rules about online activities and the amount of time spent online.
- **Help your child** to block anyone who sends offensive content. Most social networking services allow users to block and report someone who is behaving badly.
- **Be attentive**— look for warning signs that a child in your care might be the target or perpetrator of cyberbullying. If you observe excessive technology use, fear or avoidance of technology, social withdrawal or other behaviors that concern you, talk with your child or seek professional help.



If you think your child is being cyberbullied:

- **Do not reply** to the cyberbullying and instruct your child or teen not to reply.

- **Identify the evidence** that exists (online conversations, text messages or images, emails, etc.), and do not destroy it! This evidence may be helpful in identifying the perpetrator and may be requested by law enforcement officials if criminal behavior was involved.
- **Block future cyberbullying attempts** if the bullying is coming through cell phone or email. Determine if there are features that enable you to block future contact with the perpetrator.
- **Discuss any changes** in mood or behavior with your child. If you are concerned, help your child to stay connected to friends and family that they trust.
- **Notify** the police immediately if you have serious concerns about your child's safety.
- **Inform** school administrators of the problem; they may be able to help you respond, can determine if the cyberbullying is occurring via school computers, and can take note of any bullying at the school where your child or teen is the target. Ask them to thoroughly explain their processes so that you can work towards achieving a positive outcome.
- **Cyberbullying won't stop if it's ignored.** – you can help by listening to your child and working with them to take control of the situation.

Tips for Your Kids & Teens

- **Report** to an adult if you have received unkind or bullying messages or know other kids who have been cyberbullied. Report to your parents, a teacher or the police any messages or postings that are mean, embarrassing or threatening to yourself or other students – even if it is received from your dating partner.
- **Don't respond or retaliate to the sender** of these messages and block the person who is behaving badly.
- **Speak up** if you see or know about cyberbullying happening to a friend; it is important to support them and report the bullying.
- **Be considerate** - treat others as you would like to be treated. Don't forward on messages or photos that may hurt or upset someone.
- **If you are using** the internet to embarrass, threaten, harass or hurt others, chances are you will be caught. Be aware that the police can recover messages, pics and posts – even after they have been deleted.
- **Be aware** that many internet and cell phone providers have rules about behavior. If you break them, your account – and every account in your home – could be jeopardized. If you break the law, you may also be reported to the police.
- **Avoid** taking quizzes, adding unknown applications or joining unknown groups.

Sexting/Texting

Sexting refers to the sending of provocative or sexually explicit photos, messages or videos, generally using a smartphone. Sexting can also include posting this type of material online. While it may seem like innocent fun or flirting, sexting can have serious social and legal consequences. It may be difficult for kids to anticipate the potential outcome of sharing provocative images or messages, particularly when they trust the people they share them with.



Social implications of sexting

Once images and messages are sent, they often spread quickly. Once images are posted online or sent as a text, it can be almost impossible to remove them.

Sexting can cause embarrassment both now and in the future. **Family, friends, future partners, employers and college admissions may have access to sexting images** which can damage the teen's reputation. For example, a 14-year old girl takes a topless photo of herself and sends it to her boyfriend's smartphone. After they breakup, the boy posts the photo with unkind comments on a social networking site for friends to see.

Sexting images can be used by others for cyberbullying, cyberstalking or sexual harassment. Kids need to plan ahead and consider how they deal with their own, and others' messages and images. It can be easy for kids and teens to forget the potential impact of their actions in an online environment.

Legal implications of sexting

Under Texas State law, Senate Bill 407, kids are committing a crime when taking, receiving or forwarding sexual images of themselves or friends who are minors. This applies even if all participants are willing. These acts can represent the production or distribution of child pornography. Violators who send or possess explicit images face a class C to class A misdemeanor and parents may have to pay for and attend internet safety classes along with the child.

Tips for Parents

- **Remind** your child to think before they act – taking or sending sexual images, even of themselves, has social implications and may be illegal.
- **Warn your child** about the social and legal consequences of sexting.
- **Remind** your child to delete any sexual content they receive from others and to avoid forwarding this type of content and tell a trusted adult or parent.
- **Remind** your child to consider the feelings of others when distributing any content by smartphone or online.
- **Learn** how to use your child's smartphone and talk with them about what they can and cannot do with it. Some cell phone companies such as Verizon and AT&T offer classes on how to use your phone. Check with your local store to see if they when they are offered. For iPhones, you can also go to <http://ipod.about.com/od/introductiontotheiphone/tp/Things-To-Do-With-New-Iphone.htm> or <http://www.apple.com/support/iphone/basics/> for basic tutorials. For the Android, try UseMyDroid.com, and for the Blackberry check out <http://us.blackberry.com/support/blackberry-101.html>
- **If you are concerned** that a sexting incident may be a criminal matter, contact your local police.

Tips for Your Kids & Teens

- **Think before you post!** Content posted online will be there forever. You can put it up, but you can't take it down.
- **Ask yourself** – do you really want everyone to see that?
- **Keep in mind** that no message, text or email is completely private. Your school and adult family members may be watching online activity and the police can recover all messages – even if you deleted them.
- **Be considerate** – send only the kind of messages and photos you would be happy to receive.
- **Texting** in abbreviations or shorthand can lead to misunderstandings. Think about how your message may come across before you send it.
- **Remember** that sexting can be illegal, so never share naked images of yourself or forward images you have received to anyone.
- **Say no if someone asks you to do something** – like take or pass on a photo – that makes you feel uncomfortable.
- **Don't be embarrassed** – talk to a trusted adult if someone pressures you to do something that makes you feel uncomfortable or sends you content that worries you.
- **Stay aware** of what's going on around you and guard your privacy. Remember, if you can take pictures of everything and everyone with your phone, so can others...you may not want to be the subject of those photos!
- **If you have sent an image** or message that you regret, seek advice from a trusted adult.

Passwords

Passwords are one of the main keys to maintaining safety online. More and more we are required to have passwords for various aspects of our lives. They are often hard to remember and can be a hassle to use, but are nonetheless necessary. It is important to think through how we create and use our passwords. Hackers are becoming more successful at figuring out passwords and we need to stay one step ahead. Most people use mnemonic shortcuts substituting a number for a letter or vice-versa, such as F10w3r\$ for Flowers. This used to work but hackers are now on to that trick. Check out some of the tips below for creating stronger passwords.

Many websites are starting to use a two-factor identification system, and we will see more of this safety measure to come. This may mean when you try to login to a website, you may receive a text message that notifies you a log-in attempt is being made. This type of confirmation is a lot better than having to use your mother's maiden name.

In a recent study by Splashdata.com, passwords information from compromised accounts posted by hackers showed an interesting trend for the last two years. Following is a list of the top twenty most commonly used passwords, if you see yours in this list, it is time to choose a stronger password.

- | | |
|--------------|--------------|
| 1. Password | 11. iloveyou |
| 2. 123456 | 12. Trustno1 |
| 3. 12345678 | 13. 1234567 |
| 4. Abc123 | 14. Sunshine |
| 5. Qwerty | 15. Master |
| 6. Monkey | 16. 123123 |
| 7. Letmein | 17. Welcome |
| 8. Dragon | 18. Shadow |
| 9. 111111 | 19. Ashley |
| 10. Baseball | 20. Football |

Tips for Parents

- **Help your child** choose two to three word phrases for their passwords such as "YummyDonutHoles" or "SuperSpeedZone" or better yet, choose words that are unrelated such as "ElevenTroyZippersSnow". That is a 19-letter password – it would take millions of years for a computer to crack that combination – but Eleven boys named Troy closed their Zippers before going out in the Snow! If you can only use one word as a password, make it case sensitive and use a combination of numbers and symbols
- **Enable** the two-factor identification system if it is available on a website you use.
- **Stay trustworthy** with passwords your kids have entrusted to you.

- **Encourage** kids not to post their passwords out in plain site (such as taped to the monitor); set an example by not doing so yourself.
- **Use** long, different passwords for internet banking, social networking sites, online purchases and email.
- **Consider** having a “no big deal” password for sites that would not be a crisis if they were hacked such as Spotify or Pandora.

Tips for Your Kids & Teens

- **Never** share your password with anyone other than your parents or trusted adult. No matter how close a “friend” may be - passwords are private.
- **Change** your passwords about every six months – if you have chosen two to three word phrases. If you are only allowed one word, make it case sensitive and add numbers and symbols, such as L’s could be replaced by the number 1, E’s could be the number 3, A’s could be @. Be creative to keep yourself safe. If you are only allowed one word, make it a combination of words that normally do not go together such as “blackorange” or “willowball”.

Laptop/Computer/iPad/iPod Touch Safety

Personal computer, Macs and iPads are becoming more commonplace than ever. By using basic guidelines you can manage these devices and enjoy the benefits of new technology.

Tips for Parents

Talk to your kids about how to stay safe online.

Speak directly about your expectations and your family ethics regarding computer use.

Decide which parental control option suits your family

Use anti-malware software regularly on your computers

Check the age guidelines of any site or game in which your child might want to engage and consider whether you are comfortable with your child accessing the sites. What is the content like? Who can they contact? Who can contact your child or teen?

If you really want to be safe, avoid typing your credit card number or any other financial or otherwise sensitive information into any public computer.

Be careful with all those third party utilities out there such as uninstaller, diagnostics, and other programs. A lot of them are very intrusive on your system and cause more problems than they fix.

Set restrictions for iPads/iPod Touch/iPhone. You can enable and adjust Restrictions, or Parental Controls, on your device to prevent access to specific features or content on the device. Locate these settings by tapping **Settings > General > Restrictions**.



Using Restrictions

To Enable Restrictions, tap Enable Restrictions and enter a passcode. The passcode will be required to make changes to these settings or to disable restrictions.

- You can choose to restrict access to the following applications and features on the device:

Safari

Camera (also disables FaceTime)

FaceTime

iTunes

iBookstore3

Installing apps

Deleting apps

Siri

Explicit language for Siri

You can choose to prevent access to specific content types.

Ratings (select the country in the ratings section to automatically apply the appropriate content ratings for that region)

Music and podcasts

Movies

TV shows

Books3

Apps

In-app purchases

You can also adjust the time necessary before a password is required to purchase content.

You can choose to prevent changes to Privacy settings Location Services

Contacts

Calendars

Reminders

Photos

Bluetooth sharing

Twitter

Facebook

- You can choose to prevent changes to accounts. Accounts (disables changes to Mail, Contacts, Calendars, iCloud, and Twitter accounts)
- You can choose to restrict Volume limit.
- You can choose to restrict features within Game Center.



Remind your kids that if they are going to make online purchases or need to make sure a website is secure, that they must look for the “s” at the end of the https path in your web addresses. If there is not an “s”, the site is not safe for financial transactions of any kind.

Tips for Your Kids & Teens

- **Do not save** your logon information. Always log out of websites by clicking "log out" on the site. It is not enough to simply close the browser window or type in another address. Many programs (especially social networking websites, web mail, and instant messenger programs) include automatic login features that will save your user name and password. Disable this option so no one can log in as you.
- **Do not leave** the computer unattended with sensitive information on the screen. If you have to leave the public computer, log out of all programs and close all windows that might display sensitive information.
- **If using Internet Explorer, disable** the feature that "remembers" your passwords.
 - In Internet Explorer, click **Tools** , and then click **Internet Options**.
 - Click the **Content** tab, and then click **Settings**, next to **AutoComplete**.
 - Click to clear the check box for **User names on passwords and forms**.
- **Watch for over-the-shoulder snoops**
- **Don't enter** sensitive information into a public computer. Keep in mind that an industrious thief might have installed sophisticated software on the public computer that records every keystroke and then emails that information back to the thief.
- **Do not open** emails from someone you don't know.
- **Do not respond** to any emails stating you have won a contest, requesting money (even if its for a "friend") or asking for personal information – for any reason. Scammers work hard to get your info by making emails look very friendly.

iTunes Content Restrictions

Take advantage of iTunes and their parental control options in iTunes Preferences that allow you to set content restrictions. For example, you can restrict explicit content from displaying in the iTunes Store. You can also disable podcasts, radio content, the iTunes Store, and shared music so that these items do not appear on the left side of the iTunes window.

Advice for Parents

To set parental controls on your computer, follow these steps:

- In iTunes, open iTunes preferences.
 - Mac users: From the iTunes menu, choose Preferences.

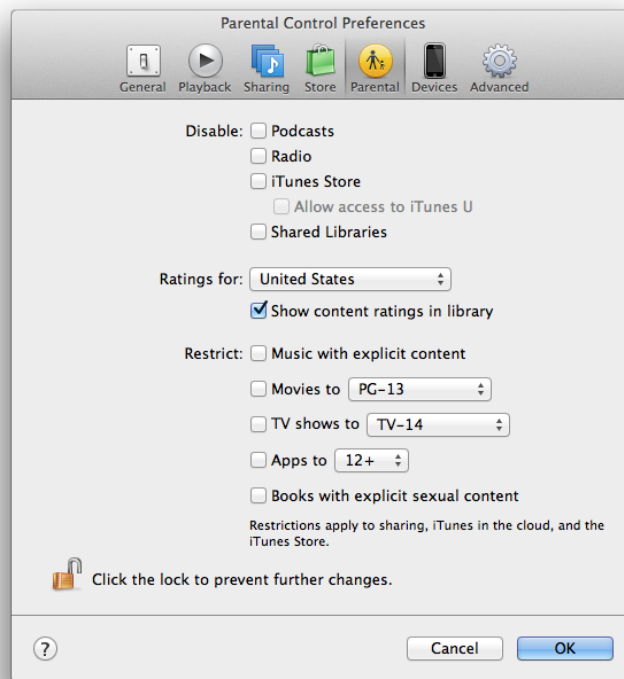
- Windows users: On the Edit menu, click Preferences.
- Click the Parental tab.
- Select the checkbox next to any item you wish to disable or restrict.
- To change a rating level of TV Shows, Movies, and Games choose a rating level from the pop-up menu.
- Click the lock icon to prevent users from making changes.

Step 1: Type your administrator password in the resulting dialog, then click OK (You'll need to know the administrator's account name and password).

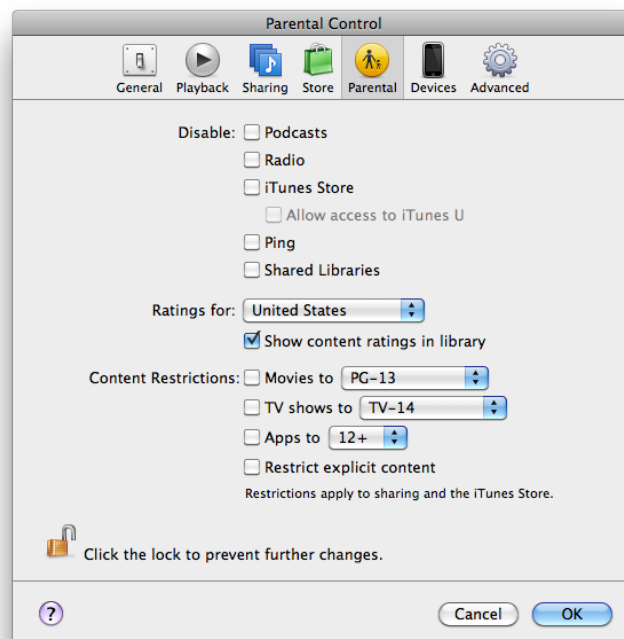
Step 2: Click OK to close iTunes preferences and have your changes take effect.

Step 3: If you want to make changes to your restrictions, open iTunes preferences, click the Parental tab, click the lock icon, and enter your administrator password in the resulting dialog to unlock the parental controls. You can then make any desired changes.

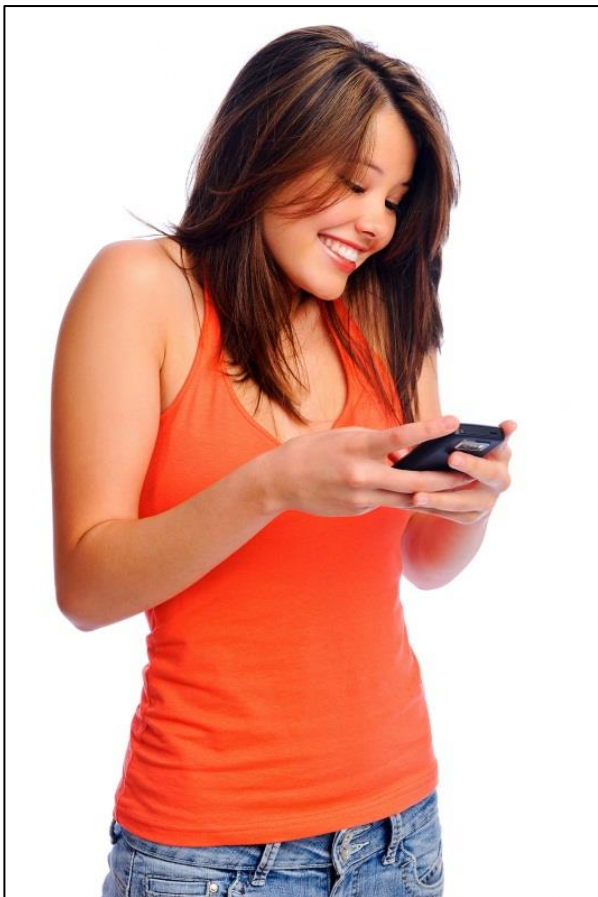
iTunes 11 Parental Controls:



iTunes 10 Parental Controls:



Smartphone Safety



Smartphones are a great way for children to stay in touch with their parents, family and friends. Smartphones also allow users to make calls, take photos, play games, send texts and images, and access the internet. Smartphones are a standard feature in teenagers' lives and are progressively being used by younger children.

Smartphones provide immediate communication and can be fun to use, but the fact that they can be on 24/7 and you cannot always be there to supervise, means there are potential risks. These include:

- High phone bills
- Scams and cons
- Cyberbullying and unwelcome calls
- Sexting/excessive texting
- Access to inappropriate content
- Reckless driving

Smartphones now have GPS technology installed which can be helpful in an emergency. Increase your child's safety and security by helping them block unwanted calls from specific numbers or disabling internet access. Contact your smartphone provider to find out how to do this.

Parents can manually lock most smartphones with a password or PIN number so no one (except you and your child) can make calls or access details. This is also very helpful if your child's phone is lost or stolen. The first step is not sharing too much personal information online.

Tips for Parents

- **Stay up-to-date** with your child's use of new technologies. Be bold and ask your child to show you how their phone works and what they are using it for.
- **Impress** upon them the importance of not texting when driving. Encourage them to pull over and stop before they read or send texts. (See a suggestion for a Parent-Teen Driving Contract at IDShepherd.com.)
- **Model** the same rules and behavior you expect of them.
- **Help your child** to understand that their phone is like a wallet and every text message, phone call or download service costs money and its contents are not for everyone to see.

- **Encourage** your child to be extra careful when downloading apps – some apps are set up to gather their usage and other data. Apps should come from a reputable source.
- **Read** the permissions section of any apps that your child would like to download and encourage them to do the same.
- **Remind your child** that they should not let anyone borrow their phone.
- **Talk with your child** about their experiences with their smartphone. Let them know it is okay to tell you if they come across something that worries them.
- **h your child** that there are ways they can deal with disturbing material – they should not respond if they receive something inappropriate and they should immediately hang up if they feel uncomfortable or worried.
- **Turn off** web access or turn on filtering if you are concerned about what your child or teen may find on the internet.
- **Do not** use banking apps – Never do any banking from your phone
- **Make sure** to turn off location settings on camera and apps like Facebook
- **Use** security software, and tracking and wiping software on all smartphones.
- **Review** the permissions section of your phone and make sure it reflects your family's choices.
- **Avoid** texting or talking on a smartphone in inappropriate places and demonstrate to your child or teen that you “walk the talk” when it comes to safe and responsible technology use.



Tips for Your Kids & Teens

- **If you receive** a text message from an unknown source, do not reply. The message could contain a virus or be an attempt to sign you up for an expensive service or subscription.
- **Never post** your number or other personal details on the internet or share it with anybody you don't know. The more private your number is, the less likely you are to be contacted by strangers or be the victim of identity theft.

- **Be cautious** about anyone who asks to borrow your phone in public – even if they claim it's for an emergency. If it is a genuine emergency, dial 911 for them and pass on the phone. Do not leave your phone with a stranger.
- **Don't accept** any offers that seem too good to be true, like a free smartphone. Check with your parents or guardian first.
- **Stay alert** of what's going on around you and guard your privacy. Remember, if you can take pictures of everything and everyone with your phone – so can they!
- **Always** pull over and stop driving before you read or send texts.
- **Be considerate** – only send the kinds of message and photos you would be happy to receive.
- **Remember: stop and think** before you check in. Geo-locators can tell strangers where you are.
- **Learn how to** pass code lock your phone

Identity Theft

Are you confident that your identity is secure? There is a direct correlation between your cyberspace identity and identity theft. Identity theft is one of the fastest growing crimes in America today. According to the Federal Trade Commission it has been the #1 rated complaint for 12 years.

What is interesting about identity theft and data breaches is that they have a common denominator. According to a Ponemon Institute study, 88% of all data breaches were caused by employee error not employee intent. It is interesting that human behavior has such a great impact on identity theft, data breaches, privacy breaches and the like. It is important to know what identity theft really is. In the illustration below you will see a list of some of the top categories of identity theft.

It is not just about Credit!



- Social Media
- Driver License
- Social Security
- Medical
- Criminal / Character
- Credit
- Debit, CC, Checks
- Child

- Cyber
- Cell Phone
- Charity
- Child Support
- Government Benefits
- Utilities
- Grants
- Insurance

- ID Cloning
- Email
- Seniors
- Mail
- Phishing
- Passport
- Rental
- Bankruptcy

ID Theft: No. 1 consumer complaint category for 13 years

Can identity theft or privacy breaches be prevented? The answer is no. However, risk can be reduced by increasing awareness. You will see in the illustration below that if we change thinking, it changes behavior, thus managing or reducing risk. It is just good privacy management. According to the Secret Service 85% of all data breaches could have been avoided without high-tech or expensive measures. Therefore, it always points back to changing thinking, changing behavior. Most adults and youth using social media do not have good privacy practices because they don't think like a thief. If you are a hard-working, trustworthy person you tend to be trusting of others and don't think about some of the risks associated with online activities. Hard copies of documents like medical information, billing statements, drivers license information or even credit reports can provide a thief with excellent data.

Can ID Theft or Privacy Breach be Prevented?

The answer is "NO" However, risk can be reduced!

By Increased awareness:

- ✓ Changes thinking
- ✓ Changes behavior
- ✓ And Managing Risk



Results in good privacy management!

85% of data breaches could have been avoided without "hi-tech" or expensive measures. Source: U.S. Secret Service.

We need to impact how someone thinks by reviewing privacy settings and examining some of the risks that can be caused by our online activity. It can change our behavior and how we navigate the internet. As a result, we will manage and reduce risk of a privacy breach resulting in identity theft.



Using social media sites such as Facebook, YouTube, LinkedIn, Twitter and others can lead to identity theft. A thief only needs two pieces of information to begin the process of stealing your identity. If a thief has your name and your birthdate, anything beyond that is a bonus. If you are sharing too much information on your Facebook page, you are at risk. Some people only list their birth day and month; however, if you have your school or college listed or your hometown or birthplace, the thief may be able to figure out the year. A savvy identity thief can use the information you post in your online profile, your interests, and activities against you. Your children's names, pet's names (common password reminders), addresses, and birthdates are all bundled in one location.

Guard your identity by checking your privacy settings often and limit how much information is exposed to the public. An example post is "Going on vacation next week" which may alert a thief that your home will be unoccupied for a period of time. Seemingly benign comments can be used to profile you and leave you at greater risk for identity theft. We need to take steps to reduce that risk.

It is not just about Credit!

26% of Consumer Complaints - Identity Theft

How a Victim's Information is Misused

- Loan Fraud 4%
- Bank Fraud 11%
- Utilities 13%
- Government Benefits Fraud 15%
- Employment 15%
- Credit Card 20%
- Misc. Mix 22%



Education, good judgment, and a healthy dose of skepticism are the best defenses against becoming a victim. There is no way to totally prevent identity theft or privacy breaches, but becoming familiar with the various types of identity theft will minimize your risk.

Learn the Lingo

It can often be difficult to communicate with your child or teen, but if they are speaking a cyber-language it can be more difficult to interpret. Learn some of the basic 3 to 4-letter acronyms your kids may be using. In addition to the small sample below, do a Google search – you may be surprised!

fomcl = falling off my chair laughing
t tyl = talk to you later
g2g = got to go
nvm = never mind
lvysm = love you so much
182 = I hate you
420 = marijuana
4COL = for crying out loud

9 = parent is watching
P911 = parents are listening or are in the room
53X = sex
A3 = anyplace, anywhere, any time
GNOC = get naked on cam
IDKY = I don't know you
JK = just kidding
LHU = let's hook up

Avatar: A graphic alter ego you create to use online; can be a 3D character or a simple icon, human or imaginative.

Clickjacking. In one common version of this scam, you're offered a chance to watch an enticing video. Click on the "Play" button and you're really clicking on an invisible "Like" button that's hidden behind it. You may now be taken to a page that announces you have to disclose personal information before you can watch the video. Provide it and still there's no video — you're taken instead to other pages to complete online surveys or be pitched suspicious products.

Your Like is then registered on your Facebook page, so your friends think you've watched the video and thought it was good. When they click "play" to try to check it out, the same sequence of events happens to them. The scammer, meanwhile, is collecting a commission from unscrupulous merchants for every "Like" referral that is generated. So the two-part goal is achieved: spread quickly and make money. This is an effective way of spreading "malware". You will know you've been targeted this way if a pop-up appears saying you need to install special software to watch a video. Don't do it.

Facebook Places – Facebook's new location sharing feature, Facebook Places, an application that lets users "check in" on their mobile phones so friends know where they're hanging out and what they're doing.

"Like"-baiting. Unlike clickjacking, this ploy gets you to knowingly click a "Like" button. The goal is the same: extracting personal information out of you to create commissions for scammers. Rather than a phony video, the incentive is usually free tickets or an entry into a drawing. Instead of stealing your click, they get you to provide it voluntarily by promising free gifts. The gifts, however, do not materialize.

Malware: Short for malicious software, it is software used or created by hackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Some malware is disguised as genuine software, and may come from an official company website.

Social Engineering: Obtaining confidential information by manipulating and/or deceiving people. This can be done by gaining someone's confidence and online trust, using their information to profile the victim and then steal their identity or hack into accounts. Information can be obtained through online quizzes, games and even when setting up legitimate accounts.

Helpful "How To's"

How to Review Browsing History

Find out where your kids have gone online.

If necessary, you can check your child's or teen's browser histories. If you don't know exactly what that means; it's simple, really, so simple your kids know how to do it.

Let's start with "What's a browser?" A browser is what you use to interface with the Internet. The popular browsers are Internet Explorer, Mozilla Firefox, Chrome and Safari. The most popular search engine is Google. To see where your kids have been online, simply open your browser and do the following, depending on the browser you are using:

- Mozilla Firefox: find the  , click on the small upside-down triangle; click on history

- Safari: find the  on the far right and choose “history”.
- Internet Explorer: click on the star on the right side of the screen 
- Google, find the  on the right side. Click on it and then choose “history”.

Some browsers will show you fewer destinations than others. In fact, some have huge histories.

Keep in mind:

- Kids sometimes use multiple browsers, so check them all.
- If you see no history, that means your kids have erased it. Covering their tracks probably means they've been somewhere they know they shouldn't go.
- It may be time for a really good conversation about what you think is appropriate in your house.

How to Turn off Geo-Tagging

One of the great benefits to having a smartphone or digital camera is that it makes taking pictures and posting them online a snap. Ask just about any smartphone user and they will have a collection of photographs they have uploaded to Facebook, Twitter or Instagram. What you may not know, however, is that you or your child's phone may have more information than you'd like and it isn't shy when it comes to passing it out. Some online users, although careful about sharing personal information online, may be unwittingly exposing information through a process called “geotagging.” Many celebrities reportedly have given away their home location without knowing it.

Wikipedia defines geotagging as *the process of adding geographical identification “metadata” to various media such as photographs, video, websites, SMS messages, or RSS feeds and is a form of geospatial metadata*. This information most often includes latitude and longitude coordinates which are derived from a global positioning system (GPS). While that sounds complex, it really is not. It simply means the marking of a video, photo, or other media with an embedded location of where it was taken. Smartphones and digital cameras featuring GPS have made this “tagging” possible.

Smartphones have some great benefits but also carry some very real risks. Smartphones contain data software that can track locations just like GPS systems. Using this feature, someone can find the actual location of your child's home, school, events and even play areas. Using the built-in GPS, phone camera applications can embed the latitude and longitude of a location in photos. Coordinates are not shown in your photo library, but if you post a geotagged pic online, someone with an evil motive can easily extract the photo's [EXIF](#) data and find out where you live, eat, or hang out. This is a big security risk, especially for parents who post photos of their children online.

For more information on geo-technology, watch the video at IDShepherd.com entitled “**Smartphone Photo Risks**”.

There are numerous brands and types of phones and each brand of smartphone has different directions for disabling geo-tracking. For instructions on how to turn off geo-tagging on your family's phones, contact your smartphone manufacturer.

iPhone (iOS 4.x) Apple has conveniently created a way to turn off location services on a per-application basis. To see your settings, go to **Settings, Location Services**. From there you can set which applications can access your GPS such as apps coordinates or disable it entirely. You may want to leave some of the applications connected with your GPS such as Siri, Google Earth for driving directions, Starbucks, or other food finder. Turn off anything that you don't absolutely need to have connected to the GPS locator.



Android Camera:

For turning off geotagging on your camera:

1. Open the Camera app
2. Select the Location icon
3. Select Off

BlackBerry Camera:

1. Open Camera
2. Select the Location icon and set it to Disabled

Previous versions will need to open Camera, press the Menu button and select Options. Then set Geotagging to Disabled.

Other Cameras/Geotags:

Operating Systems vary. Refer to your mobile device User Guide for detailed instructions.

How to Set Up a Facebook Page - Safely

Facebook is a wonderful tool for keeping in touch with friends and family, following favorite businesses, common interest groups, celebrities, or social causes. Currently there are over one billion users. Terms of the site do not allow users under the age of 13. Facebook has certain protections for 13-to-17-year-old users (such as how adults can contact them). So, it is important to be honest about your teen's birth year.

Being proactive about keeping your family safe includes learning how to set up and use Facebook. You need to be in control of your digital avatar – not allow someone else to do it for you. Keep in mind that Facebook does change its settings from time to time, but the basics are listed below and will get you going safely and knowledgeably.

Since Facebook changes its settings often, sometimes without notice, the best way to keep up on the latest changes is to go to MarkSeguin.com and select Facebook Updates and become familiar with two different areas of Facebook:

www.Facebook.com/Safety



Our Philosophy

Safety is an ongoing conversation among everyone who uses Facebook.



The Facebook Community

Each of us plays a role in creating a safe environment.



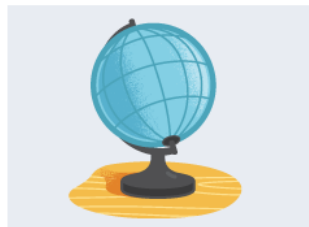
Tools & Resources

Learn about your account settings, safety best practices and more.



Parents

Help your teens play it safe on Facebook.



Teachers

Learn and teach about how to use social media wisely.



Teens

Be smart. Use good judgment whenever you're online.



Law Enforcement

Learn how Facebook works with your local law enforcement.

and:

www.Facebook.com/help

- Get Started on Facebook >
- Manage Your Account >
- Privacy >
- Security >
- Timeline >
- News Feed >
- Sharing >
- Messaging >
- Connecting >
- Facebook Mobile >
- Popular Features >
- Pages >
- Ads & Sponsored Stories >
- Apps, Games & Credits >
- Report Something >
- Community Forum



Discover Facebook Home



Learn About the New Design



Fill Out Your Timeline



Find Your Friends



Learn the Privacy Basics



Discover Games & Apps

Top Questions

- How do I get the new design?
- How do I reset my password?
- When I share something, how do I choose who can see it?
- How are Pages different from personal timelines?

More Help



Facebook Tips
Pro tips from Help Center writers



Facebook and Privacy
Privacy news and updates

To proceed with setting up your Facebook profile, start here:

SCREEN
SHOT #1:

facebook

Email Password [Log In](#)

☒ Keep me logged in [Forgot your password?](#)

Facebook helps you connect and share with the people in your life.

Sign Up
It's free and always will be.

First Name:

Last Name:

Your Email:

New Password:

Select Sex:

Birthday: Months: Day: Year:

Why do I need to provide my birthday?

By clicking Sign Up, you agree to our [Terms](#) and that you have read and understand our [Data Use Policy](#).

[Sign Up](#)

[Create a Page for a celebrity, band or business.](#)

- Do not use a work email address. Consider setting up a personal Email account (i.e. Yahoo or Gmail, etc.) just for social networking sites. You could call this your “Social Email Account”
- Do not use your actual DOB online EVER! Consider creating a “Digital DOB” to guard against identity theft (i.e. January 1, (year of birth)).
- For teens, be honest about the year of birth but create an online-only day and month so that all of Facebook’s security features for teens will be in place.

SCREEN
SHOT #2:

Step 1
Import your contacts

Step 2
Profile Information

Step 3
Profile Picture

Are your friends already on Facebook?
Many of your friends may already be here. Searching your email account is the fastest way to find your friends on Facebook.

Y! Yahoo!
Your Email: bubba@2100.co
[Find Friends](#)

Windows Live Hotmail [Find Friends](#)

AOL [Find Friends](#)

Other Email Service [Find Friends](#)

- Do not import all of your contacts at once
- Always select your friends one at a time
- Connect only with people you know and trust
- Create a very strong password. See the section on Passwords in this guide.

**SCREEN
SHOT #3:**

Step 1
Import your contacts

Step 2
Profile Information

Step 3
Profile Picture

Fill out your Profile info
This information will help you find your friends on Facebook.

Leave Blank

High School
College
Employer

Back Skip Save & Continue

**SCREEN
SHOT #4:**

Step 1
Import your contacts

Step 2
Profile Information

Step 3
Profile Picture

Set your profile picture

Upload a Photo
From your computer

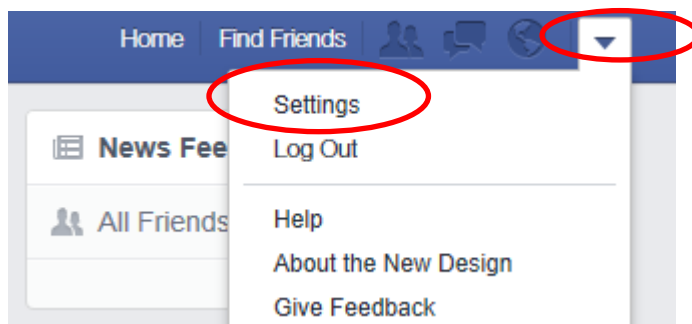
OR

Take a Photo
With your webcam

Back Skip Save & Continue

- Use a picture that you would not mind anyone seeing
- A picture from a social site may be available to search engines 30 to 50 years in the future even after its been deleted from your profile
- Encourage teens to choose a photo that reflects positively in case employers or colleges look into their Facebook page.
- A pop-up bar will appear at the top or bottom of your screen asking you to confirm the setup in your email.

**SCREEN
SHOT #5:**



- On the right-hand side of your main page you will see ads that appear. Notice they are customized to the DOB that you used, e.g. graduating class, etc.
- Notice most of the fields are left blank. (This is to guard against identity theft.) (Less is more in cyberspace!)
- Next, in the top right corner click the down arrow icon
- Then click "Settings"

**SCREEN
SHOT #6:**

- General Security - Privacy - Timeline and Tagging - Blocking - Notifications - Mobile - Followers - Apps - Ads - Payments - Support Dashboard	Security Settings <table border="1"> <tr> <td>Security Question</td> <td>Setting a security question will help us identify you.</td> </tr> <tr> <td>Secure Browsing</td> <td>Secure browsing is currently enabled.</td> </tr> <tr> <td>Login Notifications</td> <td>Login notifications are disabled.</td> </tr> <tr> <td>Login Approvals</td> <td>A security code is not required when logging in from an unknown browser.</td> </tr> <tr> <td>App Passwords</td> <td>You haven't created app passwords.</td> </tr> <tr> <td>Recognized Devices</td> <td>No recognized devices.</td> </tr> <tr> <td>Active Sessions</td> <td>Logged in from Frankston, TX, US.</td> </tr> </table> Deactivate your account.	Security Question	Setting a security question will help us identify you.	Secure Browsing	Secure browsing is currently enabled.	Login Notifications	Login notifications are disabled.	Login Approvals	A security code is not required when logging in from an unknown browser.	App Passwords	You haven't created app passwords.	Recognized Devices	No recognized devices.	Active Sessions	Logged in from Frankston, TX, US.
Security Question	Setting a security question will help us identify you.														
Secure Browsing	Secure browsing is currently enabled.														
Login Notifications	Login notifications are disabled.														
Login Approvals	A security code is not required when logging in from an unknown browser.														
App Passwords	You haven't created app passwords.														
Recognized Devices	No recognized devices.														
Active Sessions	Logged in from Frankston, TX, US.														

- On the left side, select “Security”
- Set up a security question for added protection
- Make sure secure browsing is enabled
- If desired, you may be notified by email or text that your account has been accessed on a different computer.

**SCREEN
SHOT #7:**

Privacy Settings and Tools

Who can see my stuff?	Who can see your future posts?	Friends
	Review all your posts and things you're tagged in	
	Limit the audience for posts you've shared with friends of friends or Public?	
Who can look me up?	Who can look you up using the email address or phone number you provided?	Everyone
	Do you want other search engines to link to your timeline?	Off

Under the “Privacy” area, select each option as shown above.

Timeline and Tagging Settings

Who can add things to my timeline?	Who can post on your timeline?	Friends	Edit
	Review posts friends tag you in before they appear on your timeline?	On	Edit
Who can see things on my timeline?	Review what other people see on your timeline		View As
	Who can see posts you've been tagged in on your timeline?	Friends	Edit
	Who can see what others post on your timeline?	Friends	Edit
How can I manage tags people add and tagging suggestions?	Review tags people add to your own posts before the tags appear on Facebook?	Off	Edit
	When you're tagged in a post, who do you want to add to the audience if they aren't already in it?	Friends	Edit
	Who sees tag suggestions when photos that look like you are uploaded?	Friends	Edit

Optional

Under the Timeline and Tagging Settings select each option as shown. Note this is also where you can view how others see your Facebook page.

**SCREEN
SHOT #8:**

Manage Blocking

Restricted List

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

Block users

Once you block someone, that person can no longer 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).

Block users:

Block

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:

Block event invites

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

Block invites from:

Block apps

Once you block an app, it can no longer contact you or get non-public information about you through Facebook. [Learn more.](#)

You have the option of blocking other users, invites or apps if you deem them inappropriate.

SCREEN
SHOT #9:

Notifications Settings

How You Get Notifications	 On Facebook	All notifications, sounds on
	 Email	Most notifications
	 Push notifications	Some notifications
	 Text message	Text notifications are turned off
What You Get Notified About	 Activity that involves you	On
	 Close Friends activity	On Facebook and Email
	 Tags	Anyone

SCREEN
SHOT
#10:

You have the option of being notified by email or text to your mobile phone whenever you receive a new message, if there is any activity that involves you or if you are tagged in a picture.

Mobile Settings

Activating allows Facebook Mobile to send text messages to your phone. You can receive notifications for friend requests, messages, Wall posts, and status updates from your friends.

You can also update your status, search for phone numbers, or upload photos and videos from your phone.

[+ Add a Phone](#)

Already received a confirmation code?

[Confirm](#)

[Learn more about using Facebook on your phone at Facebook Mobile.](#)

This is another area to authorize receiving notification of all activity sent to your mobile phone. This is optional.

SCREEN
SHOT
#11:

Follower Settings

Turn On Follow

☐ Followers will only see your public posts and will not be added as friends. You choose what posts to make public, and you can share personal updates with just friends. [Learn more.](#)

Want to know what followers can see? [View your public timeline.](#)

SCREEN
SHOT
#12:

Real through the Learn more area so you know the difference between Followers and Friends. Choose option accordingly.

App Settings

On Facebook, your name, profile picture, cover photo, gender, networks, username, and user id are always publicly available, including to apps ([Learn Why](#)). Apps also have access to your friends list and any information you choose to make public.

Apps you use	Use apps, plugins, games and websites on Facebook and elsewhere?	On	Edit
Apps others use	People who can see your info can bring it with them when they use apps. Use this setting to control the categories of information people can bring with them.		Edit
Instant personalization	Lets you see relevant information about your friends the moment you arrive on select partner websites.	Off	Edit
Old versions of Facebook for mobile	This setting controls the privacy of things you post using old Facebook mobile apps that do not have the inline audience selector, such as outdated versions of Facebook for BlackBerry.	Public	Edit

For the highest security available turn this option off.

SCREEN
SHOT
#13:

**SCREEN
SHOT
#14:**

Facebook Ads

Third Party Sites	Facebook does not give third party applications or ad networks the right to use your name or picture in ads. If we allow this in the future, the setting you choose will determine how your information is used. You may see social context on third party sites, including in ads, through Facebook social plugins. Although social plugins enable you to have a social experience on a third party site, Facebook does not share your information with the third party sites hosting the social plugins. Learn more about social plugins.	Edit
Ads & Friends	Everyone wants to know what their friends like. That's why we pair ads and friends—an easy way to find products and services you're interested in, based on what your friends share and like. Learn more about social ads. Here are the facts: ▪ Social ads show an advertiser's message alongside actions you have taken, such as liking a Page ▪ Your privacy settings apply to social ads ▪ We don't sell your information to advertisers ▪ Only confirmed friends can see your actions alongside an ad ▪ If a photo is used, it is your profile photo and not from your photo albums	Edit

Under Ads, first select to allow your information to be given to “No One”. Then select “No One” in the Ads and Friends area.

**SCREEN
SHOT
#15:**

Welcome to Your Profile [Start Tour >](#)

This is your place to collect photos, interests, and life events that tell your story on Facebook.



Mark Seguin

[+ Add Profile Picture](#)

[Update Info](#) [Activity Log](#) [*](#)

[Timeline](#) [About](#) [Friends](#) [Photos](#) [More ▾](#)

About

Where do you work?

Where did you go to high school?

Which city do you live in?

Where did you grow up?

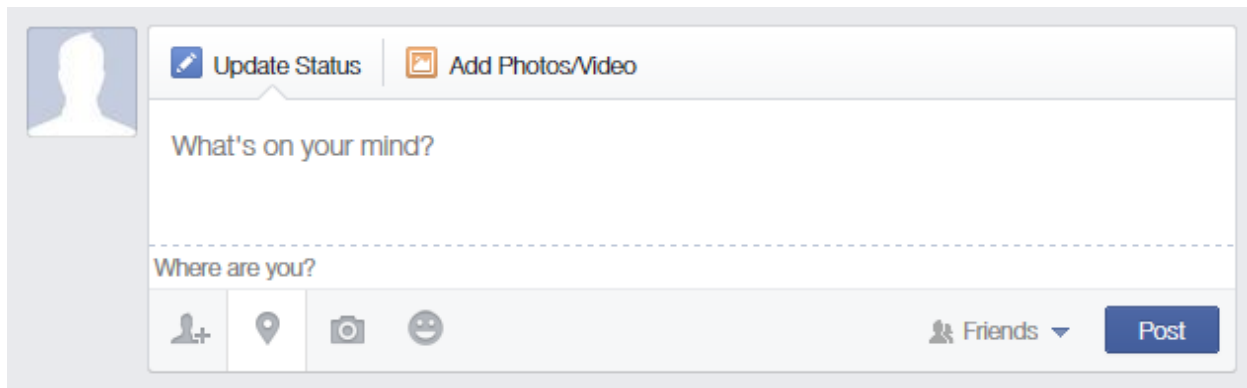
What is your relationship status? ▾

[Status](#) [Photo](#) [Place](#) [Life Event](#)

What's on your mind?

Once set up, you can view your profile by clicking on your name in the upper left-hand corner. For highest security, leave fields blank. To update, click Update Info.

**SCREEN
SHOT
#16:**



Before you post a comment, make sure that your location is not disclosed. Click on the location pin to turn this setting off. Notice that you can also select who sees your posts, so select carefully.

How To Report or Block Someone on Facebook

Report inappropriate content or abuse right where it occurs on Facebook, using the **Report** link near the content. The account responsible for the abusive content will not be notified of the identity of the person who made the report.

To block someone:

1. Click the account menu  at the top of any Facebook page and choose **Settings**.
2. Scroll to the **Blocking** section and click **Block Users**.
3. Enter the name or email address of the person you want to block. People will **not** be notified when you block them.
4. If you can't find someone using this method, try going to the person's profile (Timeline) and selecting **Report/Block This Person** from the dropdown.

How to Unfriend Someone on Facebook

To unfriend or delete a friend:

1. Go to that person's profile (Timeline)
2. Click the down arrow next to the gear symbol and choose **Unfriend**

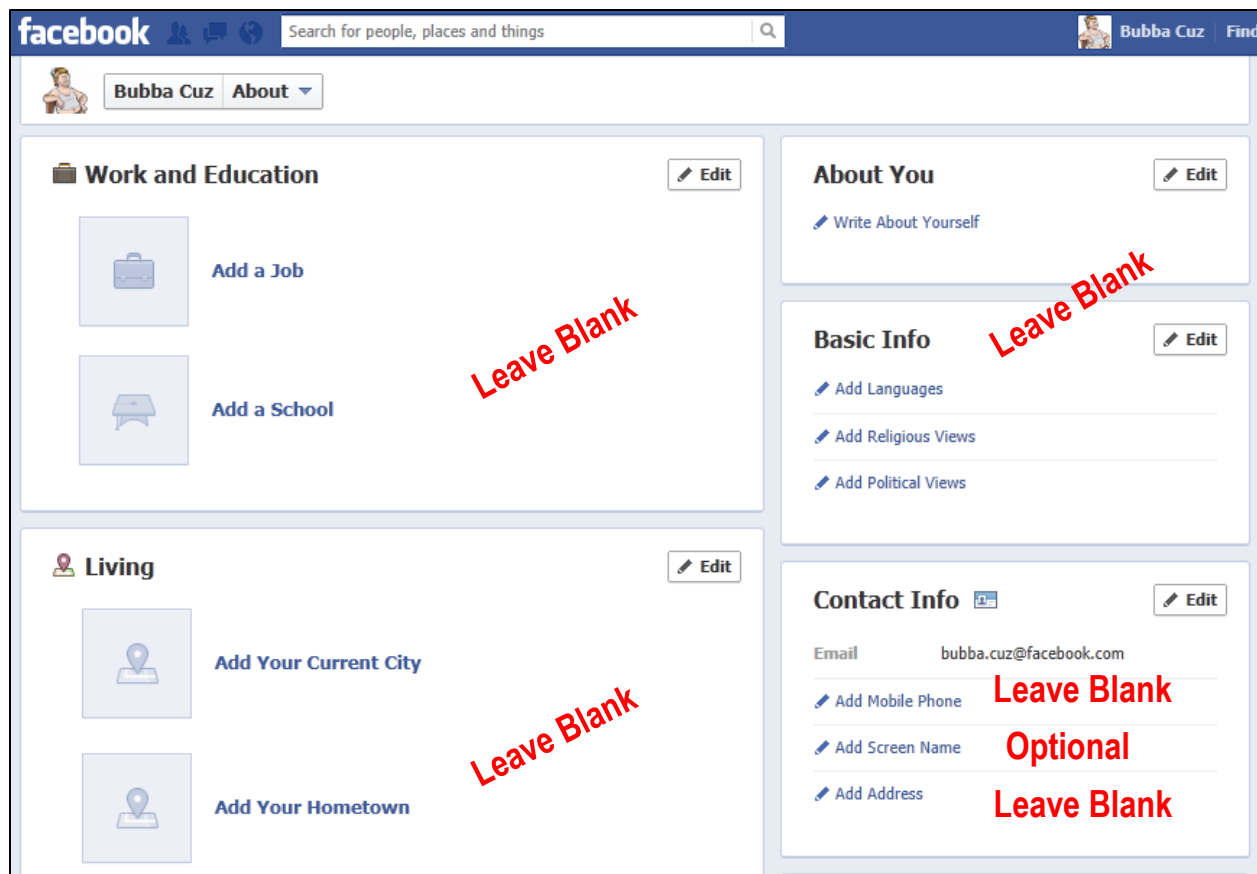
If you choose to unfriend someone, you will be removed from that person's friends list as well. If you want to be friends with this person again, you will need to send a new friend request.

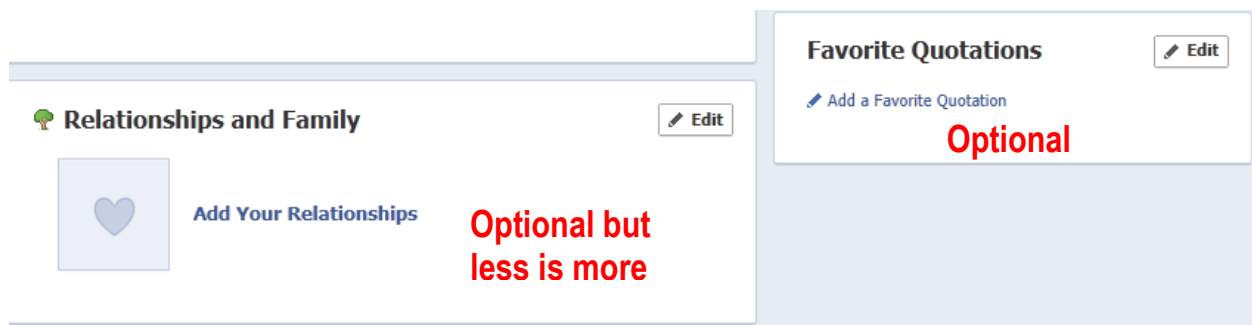
How to Secure an Existing Facebook Page

Facebook's features have changed dramatically as it has gained popularity. The changes, however, are not announced anywhere nor is the user advised of any updates. The user, therefore, is responsible for making sure that the most recent changes have been reviewed and that proper security features are selected. This can be an arduous task to keep up with the latest updates. Following are key points to "locking down" your Facebook as much as possible as of August 2012. Changes will be made on a quarterly basis, as needed.

Screen
shot #1

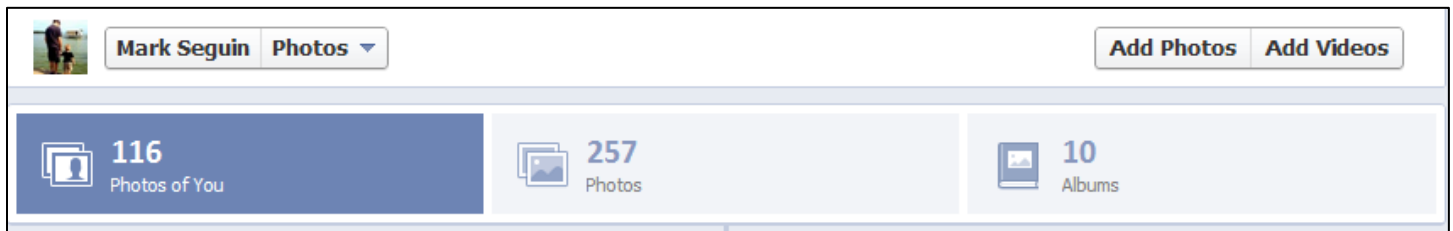
1. Login to Facebook and click on your name in the upper right corner.
2. On the left side of the page, just under your profile picture, select **About**.
3. One by one, Edit each section choosing information to be shared with either just Friends or Me Only (for greatest security).
4. Thoroughly review each section and consider who you really want to have access to your information.





Screen
shot #2

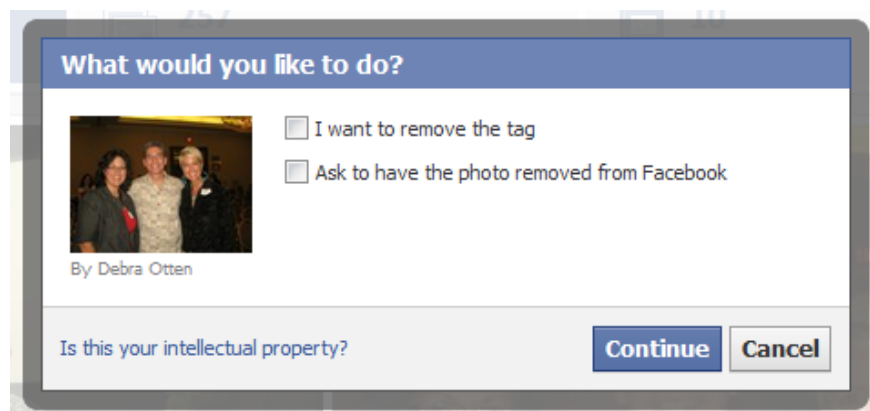
Next, click on your name again and choose **Pictures**.



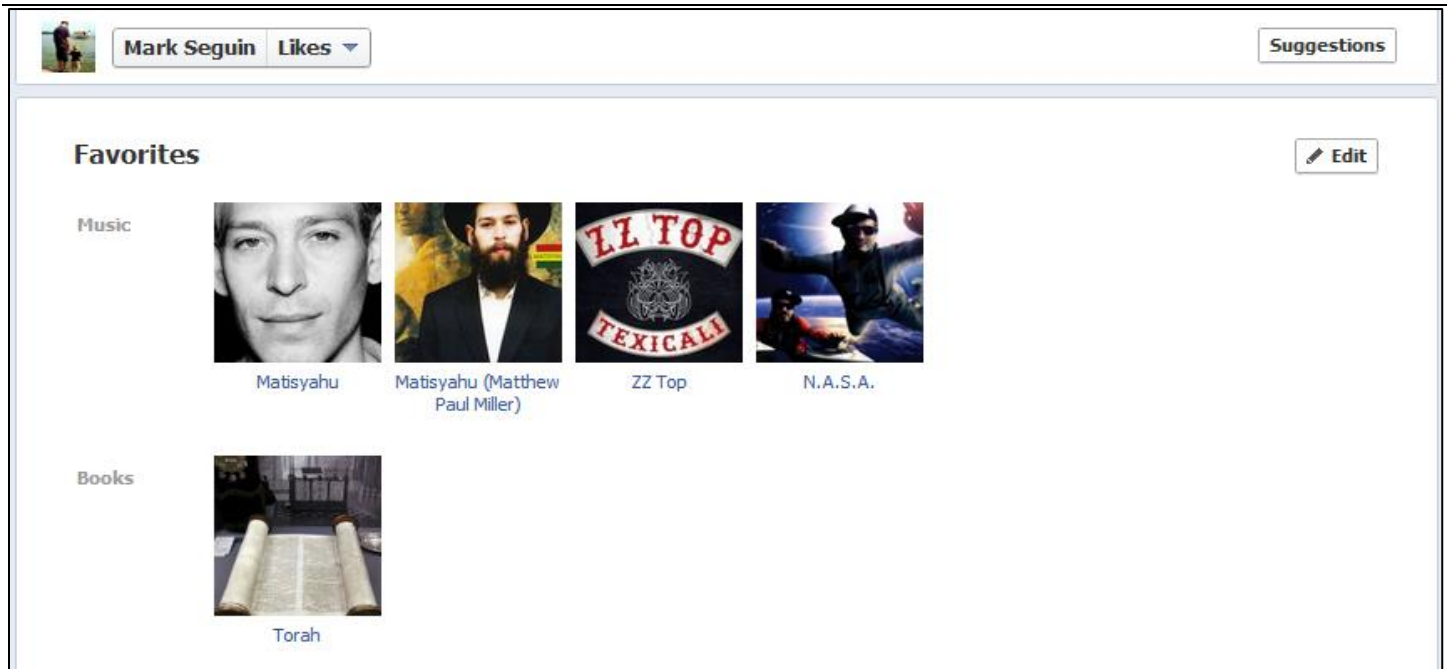
Photos of You are pictures others have taken of you and posted on their Facebook page. You can select one photo at a time and then:

- Add location
- Change date
- Download
- Make it your profile picture
- Remove tag (You can remove your tag which will only remove the picture from your timeline. The picture “belongs” to whoever posted it and it will stay in their album.)
- Report photo to Facebook to have it removed.

Screen
shot #3



In **Albums**, you can select either the  symbol or the  symbol to edit who can see your pictures. The gear symbol allows fewer choices than the drop down arrow.

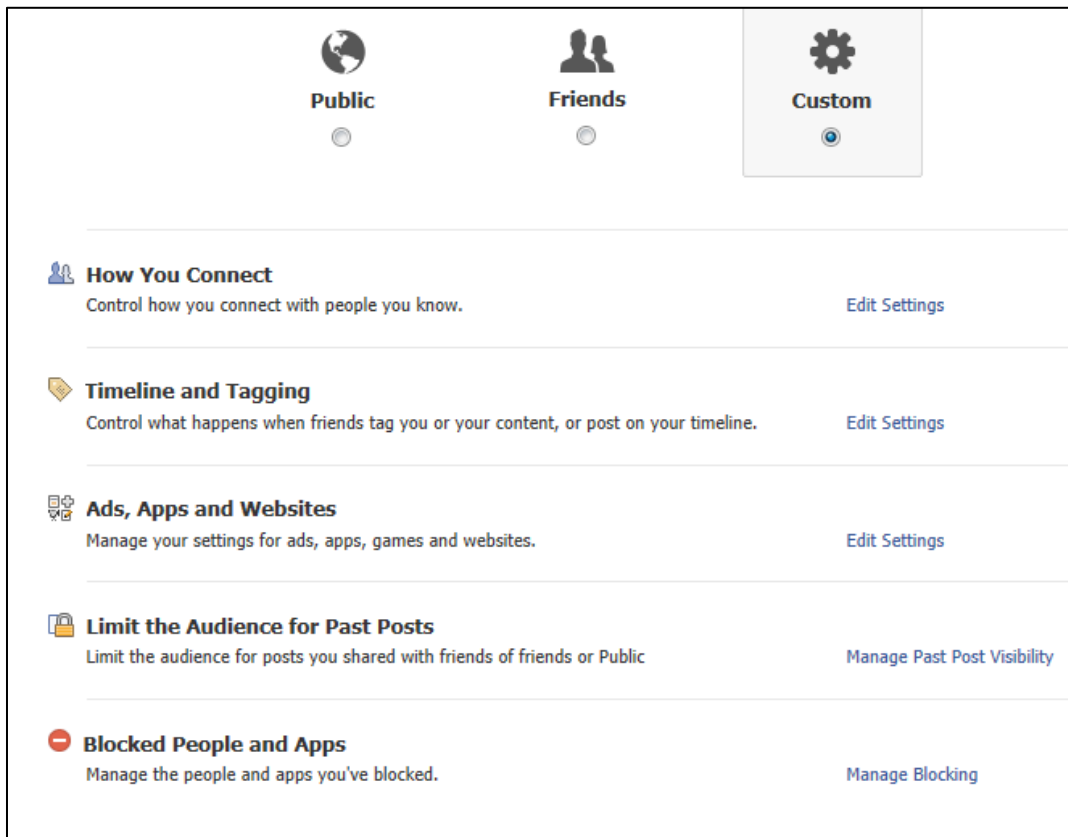


Screen
shot #4

- Edit and choose your **Likes** carefully, refraining from choosing anything that may be used for social engineering purposes.
- You can control who sees your Likes
- You can “Unlike” if desired.

- Continue to edit each category (**Subscribe to, Your Subscribers, Events**) and any other category you may have
- Select who can view this information on your Facebook page.

Screen
shot #5



Select the  on the upper right corner and select **Privacy Settings**. Select **Custom** settings. Explore and edit each category carefully and determine who will have access to viewing your information. Remember less is more in cyberspace!

Choose Your Privacy Settings **Apps, Games and Websites**

[← Back to Privacy](#)

On Facebook, your name, profile picture, gender, networks, username and user id (account number) are always publicly available, including to apps ([Learn Why](#)). Also, by default, apps have access to your friends list and any information you choose to make public.

Edit your settings to control what's shared with apps, games, and websites by you and others you share with:

Apps you use

You're using 9 apps, games and websites, most recently:

[Edit Settings](#)

FoxNews

July 23

SoundCloud

July 9

Twitter

More than 6 months ago

Remove unwanted or spammy apps.

Turn off all apps.

How people bring your info to apps they use

People who can see your info can bring it with them when they use apps. Use this setting to control the categories of information people can bring with them.

[Edit Settings](#)

Instant personalization

Lets you see relevant information about your friends the moment you arrive on select partner websites.

[Edit Settings](#)

Public search

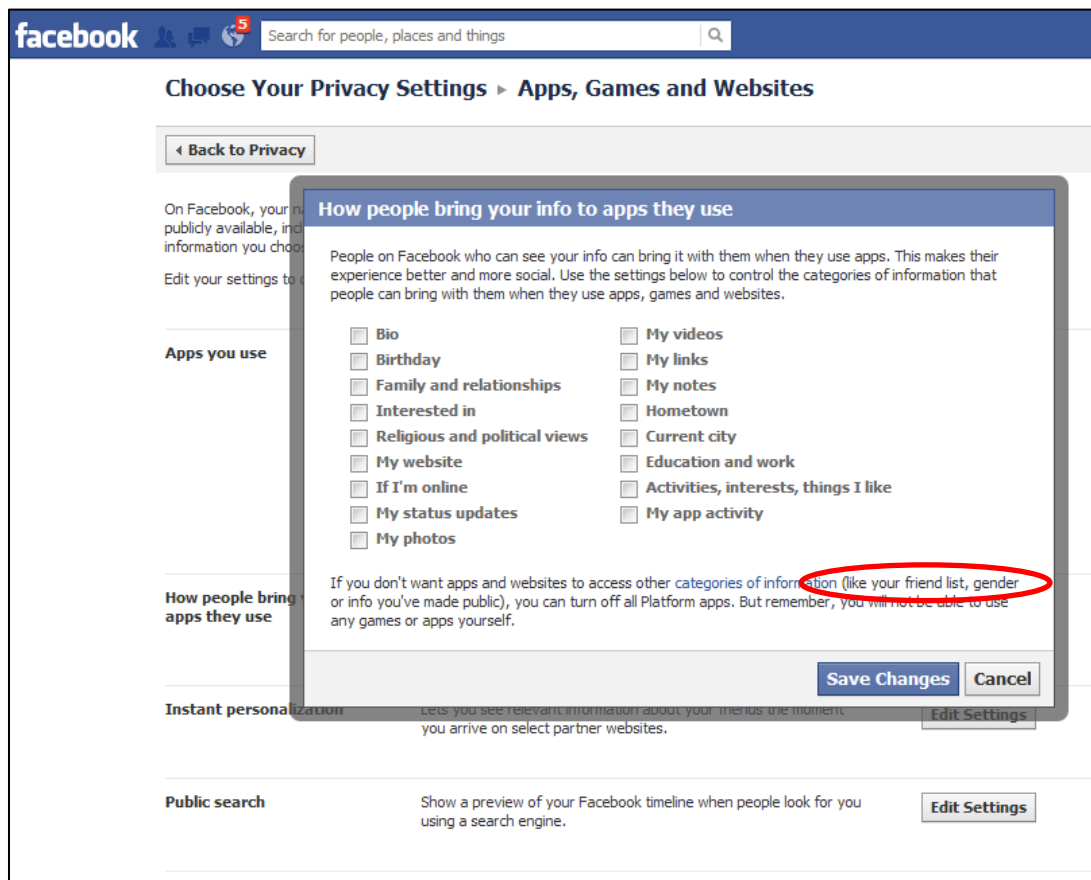
Show a preview of your Facebook timeline when people look for you using a search engine.

[Edit Settings](#)

Screen
shot #6

When you select the **Ads, Apps and Websites** category it is very important to go into each subcategory, read carefully, and choose the appropriate options for greatest security.

Screen
shot #7



Note specifically, **How people bring your info into apps they use**. When you authorize your apps you are giving them all access to your Facebook information, even those you have set to private, your posts, and the app has access to all of your Friends' info too.

For more information on how this section works, select **categories of information**.

facebook

Search for people, places and things

Mark Seguin

Choose Your Privacy Settings ▶ Instant Personalization

◀ Back to Apps

Instant Personalization

We've partnered with a few websites to provide you with great, personalized experiences the moment you arrive, such as immediately playing the music you like or displaying friends' reviews. To tailor your experience, these partners only access public information (like your name and profile picture) and other information you've made public.

When you first arrive at the following sites, you'll see a notification message and an option to turn off the personalized experience:

- Bing - Social Search
- Pandora - Personalized Music
- TripAdvisor - Social Travel
- Yelp - Friends' Local Reviews
- Rotten Tomatoes - Friends' Movie Reviews
- Clicker - Personalized TV Recommendations
- Scribd - Social Reading
- Docs - Document Collaboration
- Zynga - Social Games (The Ville and Indiana Jones Adventure World)
- Kixeye - Social Games (War Commander and Battle Pirates)
- EA - Social Games (SimCity Social)

To turn off instant personalization on all partner sites, uncheck the box below.

☐ Enable instant personalization on partner websites.

In the **Instant Personalization** category, you can watch a video to learn how this option works. For the tightest security, disable personalization.



Bubba Cuz

Update Info

Activity Log

⚙



Screen
shot #9

Select **Activity Log** and choose **View as** to see how others see your timeline page. Go back to each category to make any changes as necessary.

Screen
shot
#10

Facebook Ads

Ads and friends

Everyone wants to know what their friends like. That's why we pair ads and friends—an easy way to find products and services you're interested in, based on what your friends share and like. Learn more about [social ads](#).

Here are the facts:

- Social ads show an advertiser's message alongside actions you have taken, such as liking a Page
- Your privacy settings apply to social ads
- We don't sell your information to advertisers
- Only confirmed friends can see your actions alongside an ad
- If a photo is used, it is your profile photo and not from your photo albums

Here's an example of a Facebook Ad:

Denver Sushi



The best sushi in Denver. Try our daily lunch specials for \$9.95. Fan our page for special offers.

Denver Sushi



The best sushi in Denver. Try our daily lunch specials for \$9.95. Fan our page for special offers.

Like · Bubba Cuz likes this.

This setting only applies to ads that we pair with news about social actions. So, independent of this setting, you may still see social actions in other contexts, like in Sponsored Stories or paired with messages from Facebook. You can learn more about how social ads, Sponsored Stories, and messages from Facebook work in the [Help Center](#).

Pair my social actions with ads for **No one**

[Save Changes](#)

[Cancel](#)

- Select the next option about Ads and Friends.
- Choose to show the information to No One.

BE ADVISED: Facebook's settings often change so explore your pages regularly to make sure you know what the new options are.

How to Deactivate or Delete your Facebook account (there IS a difference):

To **deactivate** your Facebook profile means your account is suspended but still retains all of the data in case you want to restore it at a later date. Your data can still be sold even if you are no longer active. People on Facebook will not be able to search for you or view any of your information.

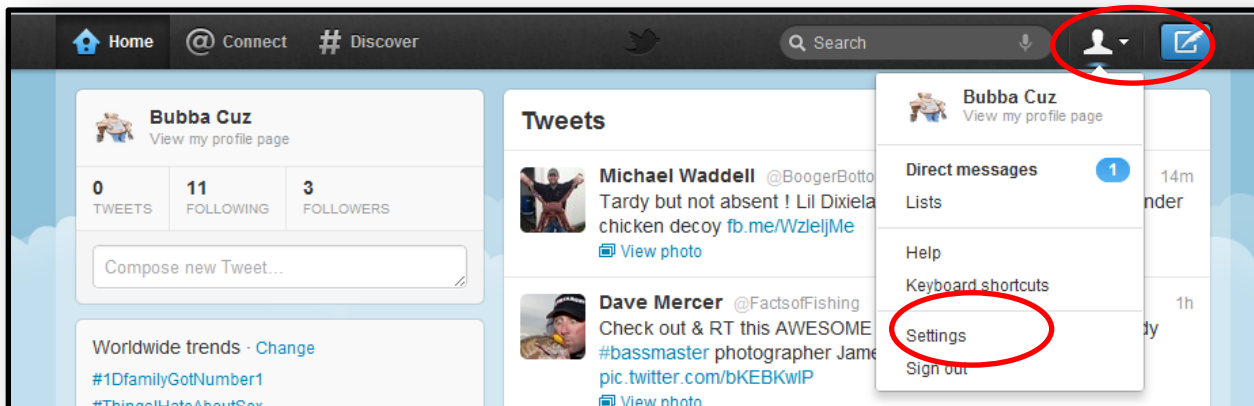
1. Click on the account menu  at the top right of any Facebook page.
2. Choose **Settings**.
3. Select **Security** from the left-hand menu.
4. Click on "Deactivate your account".

To **delete** your Facebook page, you can request to have your account permanently deleted. Keep in mind you will not be able to reactivate the account or retrieve any of the content or information that has been added.

1. From the  at the top right of any Facebook page select "Help"
2. Type in "delete account"
3. Click on "How do I permanently delete my account?"
4. Click on "fill out this form"
5. Select Delete My Account

How to Register and Use Twitter

Twitter is an online social networking service that enables its users to send and read text-based posts of up to 140 characters, known as "tweets". Tweets can also be sent to mobile phone numbers as text messages.



- Go to www.twitter.com to set up a twitter account
- Log in
- Click on the down arrow in the top right hand corner
- Click "settings". As you go through all settings, use the same choice as you did on Facebook as a guide for do's and don'ts.

Your email:

NO

We will not store your password or email anyone without your permission.

☒ Automatically find new email contacts ?

Most social networking platforms will automatically send you an email requesting to send all your contacts an invite to connect with you. Refrain from doing this; choose one contact at a time.

How to Use Instagram Safely

Instagram has become one of the coolest new apps on the market these days. It allows you to make your photos look amazing, by applying one of their present filters. It is very simple to share photos and follow friends' feeds by just scrolling down the homepage.

However, there are also many privacy risks that Instagram may open. From making your photos available to the world wide web, to giving away your location every time you take a photo, take these steps to stay safe while using Instagram.

Make your photos private so that you have to approve “follow” requests.



Step 1: Go to your profile page and click on the gear in the top right corner:



Step 2: Tap on the “Photos Are Private” to switch it “On”



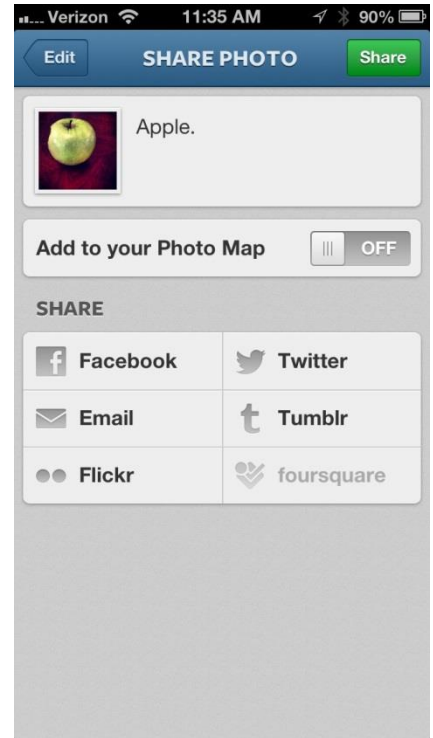
Step 3: Tap “Yes, I’m sure.”



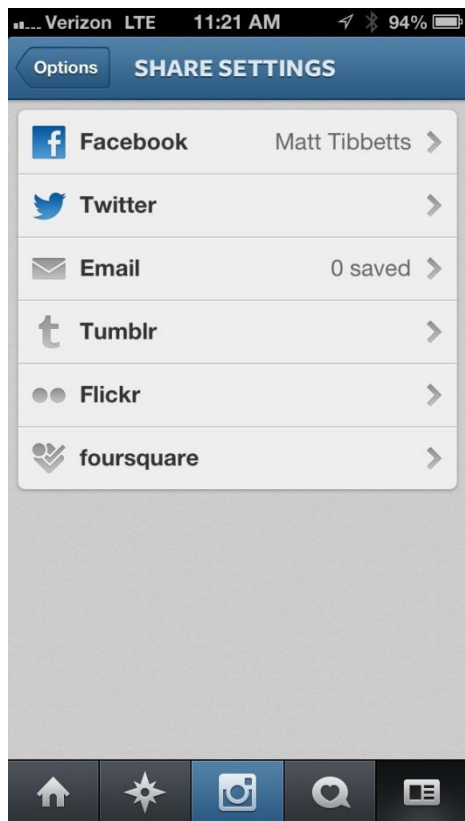
Step 4: Now your photos should be private.

Locking down your sharing settings.

Step 1: Whenever you share a photo, you have the option of sharing it to Facebook and Twitter. You can choose to check those choices on a per photo basis.

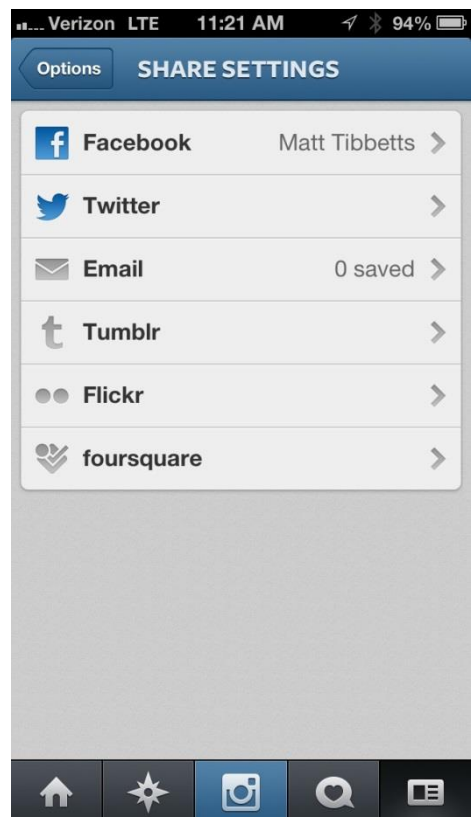


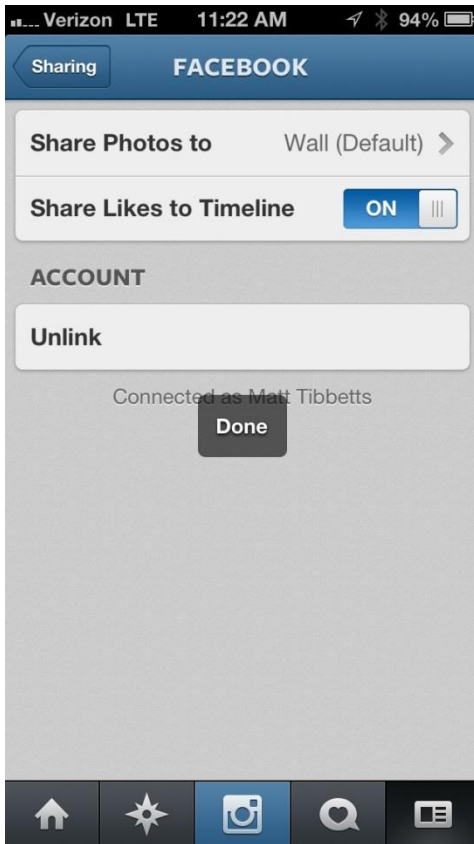
Step 2: Go back to your settings.



Step 3: Tap “Share Settings.”

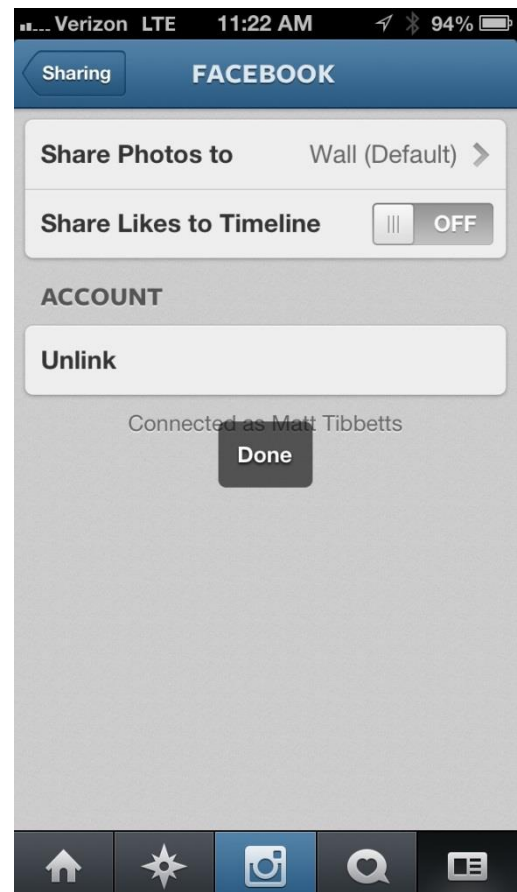
Step 4: Decided whether or not you want to have your Facebook and Twitter linked to your Instagram (matter of personal preference).





Step 5: Tap on Facebook and check the settings in there. You may want to turn off the “Share Likes to Timeline” function so that your Facebook friends don’t see every photo that you like.

Tap the on/off switch on “Share Likes to Timeline.”

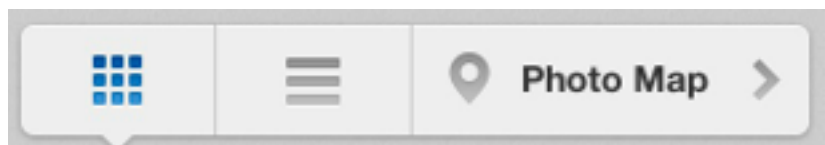


Step 6: Likes will no longer be shared to Facebook.



Hashtags

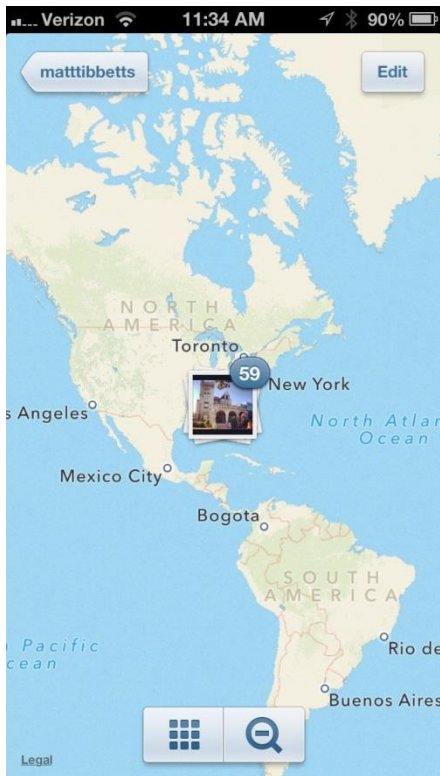
One of the ways to get your photos into a public realm is to add hashtags (#). Those hashtags create a public search of all photos that have the same hashtag on it. When you hashtag your photo, know that it is going to show up in a feed of other hashtags. Think before you hashtag.



Geo-Tags (Photo Map)

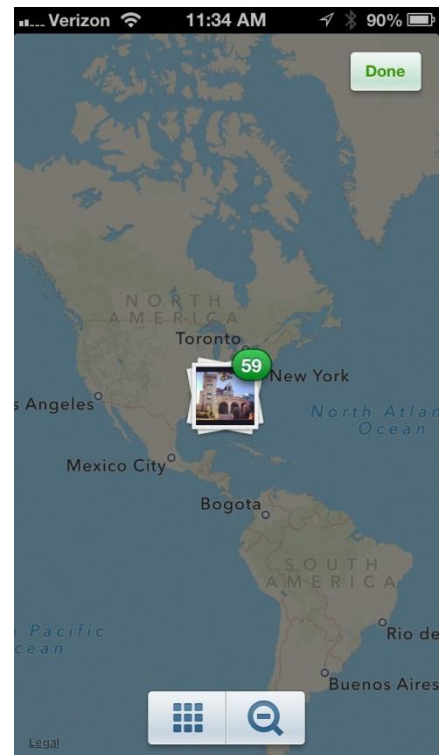
When you post photos to your photo map, it will show all of your followers where you took the photo to within 3 feet of the location. This opens up many privacy concerns, since people can then find out where you live, where you work, etc. Here's how to turn this off.

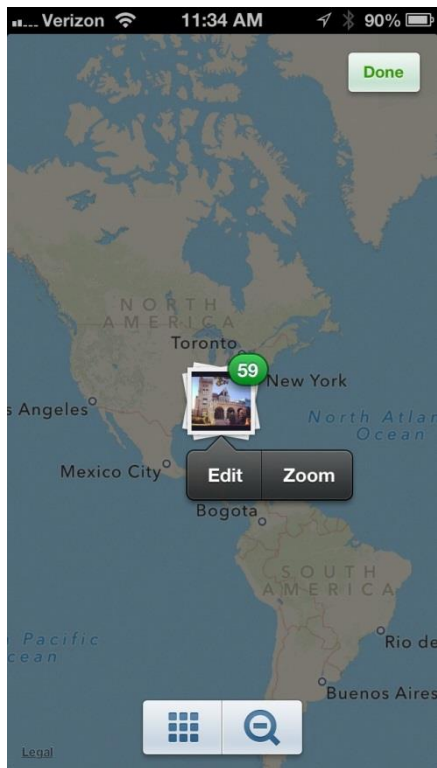
Step 1: Go to your profile page and tap on "Photo Map."



Step 2: Tap “Edit” in the top right corner.

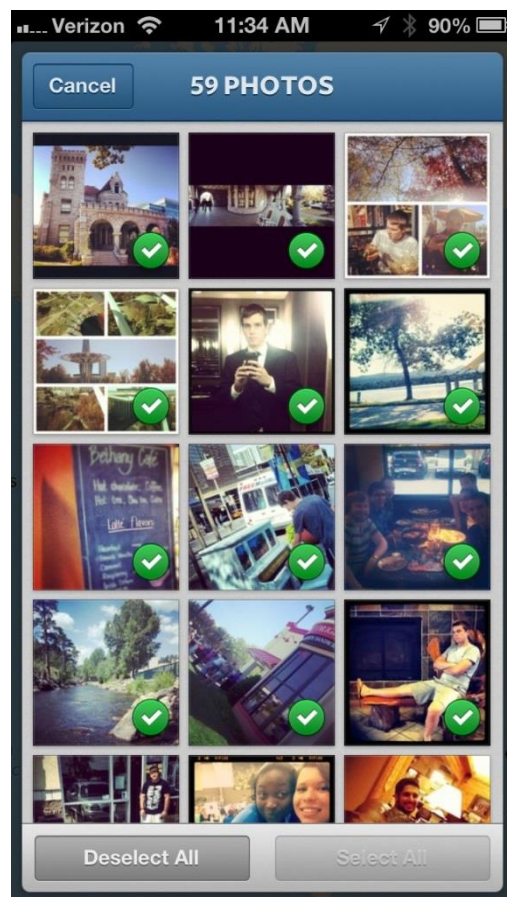
Step 3: Tap on the stack of photos in the middle of the screen.





Step 4: Tap “Edit”

Step 5: Tap “Deselect All”



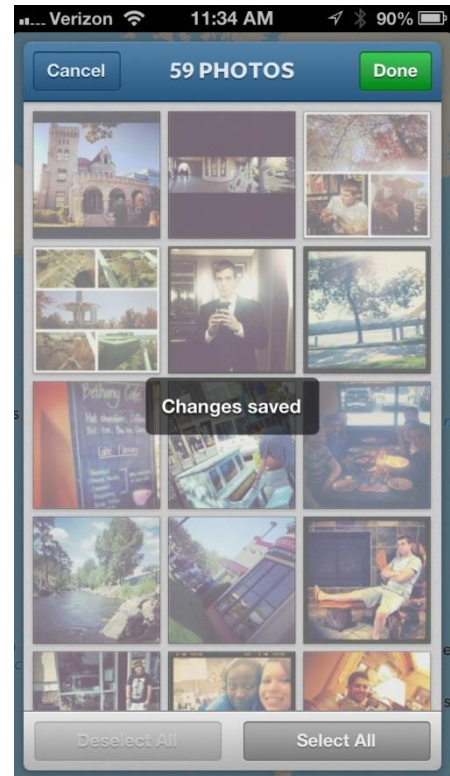


Step 6: Tap “Done.”

Step 7: Tap “Confirm”



Step 8: Now you are all set!



How to Safely Use Google+

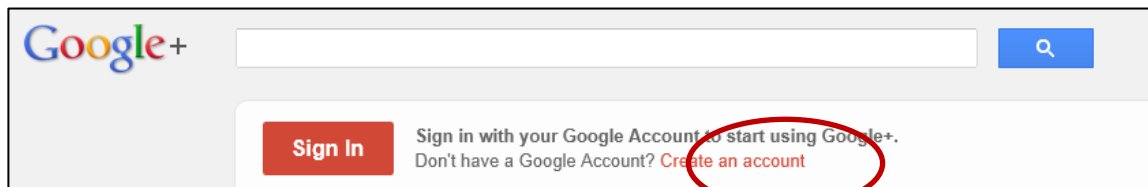
Google+ is similar to Facebook in that you can connect with others by creating “circles” of friends, business associates, etc., and communicate with them via post. You can also add video links, photos and just “hang out” with others. Just as with Facebook, Google+ requires that users are at least 13 years of age, so when creating an account it is best to be truthful about a teen’s birth year because Google+ has special default settings for teens. The defaults can be over-ridden, but discuss the safeguards with your teen.

The special safety and privacy settings for teens include:

- If teens post something to extended circles or the public, they will get a warning message reminding them that “when you share to your extended circles, people you haven’t added to your circles will be able to view your posts and may be able to comment.”
- All Google+ users can control “who can notify me.” For teens the default is people in their circles, for adults, the default is “anyone.”
- By default only people that are in your teen’s circle can comment.
- In an adult’s profile, Employment and Education can be seen by anyone, but for teens, the default is “just your circles”.
- The profile information for teens such as home address, phone number and birth date are set to “Only you”.
- By default, a teen’s physical location is never attached to their posts.
- For teens, Relationship Status can only be seen in “Your circles”. For adults “Relationship Status” can be seen by people in their extended circles.
- Google+ does not display the name of people under 18 alongside ads.
- People under 18 are not allowed to co-watch age-restricted videos in hangouts.
- Teens are not allowed to click directly to pages that are designated for 18 and older.

Signing up: Go to plus.google.com

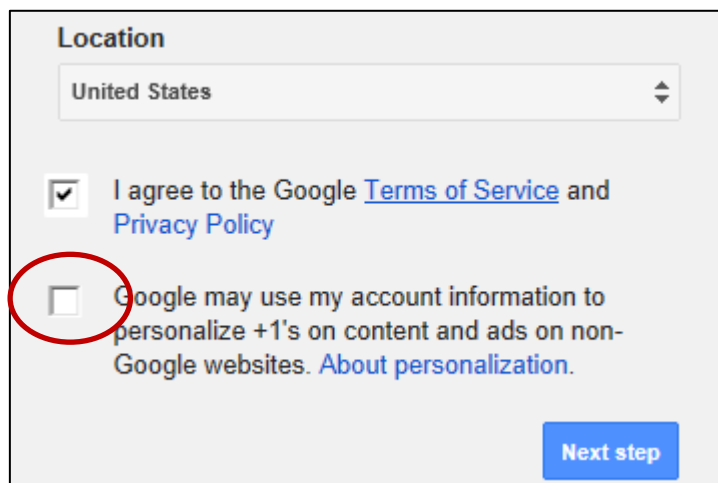
SCREEN
SHOT #1:



If you already have a Gmail account you can use it to sign into Google+. If not, from Google.com/+, choose to Create an Account with a Gmail address. Do not use your work email address. You will be given an opportunity to add a profile picture and then you'll be whisked directly into Google+.

On the bottom portion of the Create an Account section you will be asked:

SCREEN
SHOT #2:



Location

United States

☒ I agree to the Google [Terms of Service](#) and [Privacy Policy](#)

☐ Google may use my account information to personalize +1's on content and ads on non-Google websites. [About personalization.](#)

Next step

Do not select this option; leave it blank.

Select "Next Step". The service may ask you to "find people you know on Google+ by entering an email address from Yahoo or Hotmail. This is optional. Google+ will not contact the people in your contact list but will import contacts from those services and give you the option of adding your contacts from those services to your Circles. Refrain from adding your whole contact list, add one contact at a time. Choose "Continue" until you reach the profile page:

**SCREEN
SHOT #3:**

Keep your image fresh
Share a few details on your profile. You can always change the visibility later



Bubba Cuz

 **SNAP A PHOTO**

Or [upload an image](#)

Where do you work? 

Where have you gone to school? 

Your profile page is a reflection of you on the web. Remind your teen to present themselves in a positive light online. Choose a picture that you wouldn't mind everyone seeing.

You can edit your profile by clicking on your picture (or the default icon if you haven't posted a picture). To add or change your profile, click on the section you wish to edit. Be as generic as possible or leave fields blank for the greatest security. You get to decide who gets to see your information. It can be only you, your circles, your extended circles or anyone on the web.

The default setting for adults is that people who look at your profile can see the people in your circle (not which circle), as well as who has you in their circles, but you have the option to hide both the list of people in your circles and the people who have added you to a circle. For teens, the default setting is that people in their circles and people who have added them do not show up.

SCREEN
SHOT #4:

What happens when you add someone to a circle?

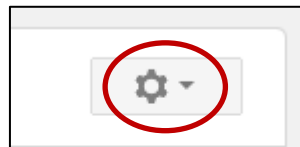
- You can share with them and see what they're sharing with you.
- You can chat with anyone in your circles who also has you in their circles.
- They'll be notified and can add you to their own circles, but they'll never see the names of the circles you've added them to.
- They'll appear on your public profile. [Change](#)

Okay, got it!



When you search for friends to add to your circles, notice your options (including changing how they will appear on your public profile).

SCREEN
SHOT #5:



Change your settings by selecting the gear symbol on the upper right-hand side of your screen.

SCREEN
SHOT #6:

Who can interact with you and your posts

Who can send you notifications? [Learn more](#)

Who can comment on your public posts? [Learn more](#)

Extended circles ▾

Anyone ▾

Notification delivery

Email:  bubbacuz80@gmail.com

[Add email address](#)

Phone: ☒ [Add phone number](#)

Not recommended, but optional

Manage email subscriptions

Weekly updates about top content from my circles

Occasional updates about Google+ activity and friend suggestions

Optional

Select who can send you notifications and who can comment on your public posts. You may even choose to be notified of new messages or posts via cell phone (SMS). This is not recommended.

**SCREEN
SHOT #7:**

Receive notifications

Notify me by email or SMS when someone...

Posts	Email
Mentions me in a post	☒
Shares a post with me directly	☒
Comments on a post I created	☒
Comments on a post after I comment on it	☒
Circles	Email
Adds me to a circle	☒
Photos	Email
Tags me in a photo	☒
Tags one of my photos	☒
Comments on a photo after I comment on it	☒
Comments on a photo I am tagged in	☒
Comments on a photo I tagged	☒
Messenger	Email
Starts a conversation with me	☒
Communications about Pages	Email
Receive invitations to manage Pages	☒

Customize choices for notification, keeping in mind that you want to know as much as possible about what is being posted about you.

**SCREEN
SHOT #8:**

Your circles

When you share posts, photos, profile data, and other things with "Your circles," you're sharing with all of your circles, except the ones you're just following.

Customize

Customize your settings for sharing posts, photos, data, etc.

**SCREEN
SHOT #9:**

Photos

☐ Show photo geo location information in newly uploaded albums and photos.

☐ Allow viewers to download my photos

☐ Find my face in photos and prompt people I know to tag me. [Learn more](#)

People whose tags of you are automatically approved to link to your Profile:

 Your circles ×

 + Add more people

When a tag is approved, it is linked to your profile, and the photo is added to the "Photos of you" section.

You can change the visibility of your [photos](#) and [videos](#) tabs on your profile.

For the greatest security, customize your choices to reflect these choices.

Understand that a Google+ “Hangout” is basically a video chat room with other people on Google+ where you can see and hear everyone in the room. Anyone on Google+ can create a hangout and anyone with a link to that hangout can join. Also, anyone who joins a hangout can invite others to join, though for teens only, Google+ will temporarily pull them out of a hangout if someone outside any of their circles joins in to make sure it is ok.

Because hangouts allow teens to use their webcams, anyone in the hangout can see and hear everything within range. So make sure your teen knows to dress appropriately and think about people, things or conversations in the background that they (or you) don’t want shared with people outside your home.

How to Safely Use Other Social Media Platforms

There are a growing number of social medial tools available, with many more being introduced almost daily for online use as well as smartphone apps. Becoming a user or to register is relatively the same with each tool, however, the key is to lock down your privacy settings as much as possible. Selecting options to over-share, “approve all” or add too much personal identifier information can leave the user much more vulnerable to privacy infringement, stalking, identity theft or worse.

Choose cautiously for yourself and help your kids choose carefully which social networking sites they join – encouraging them to constantly be aware of over exposing themselves to strangers or scams. When joining a new social media site, plan to spend about 30 to 45 minutes familiarizing yourself with the privacy settings and other available options.

Additional Resources & Websites

Resource Websites for the Family

Visit IDShepherd.com for a myriad of links and other free resources as well as updated news and tips to help keep your family guarded and protected.

www.IDShepherd.com (Great resources and information)

www.BeSafeinCyberSpace.com (More resources and information)

www.OnGuardOnline.gov (Practical tips)

www.FTC.gov/idtheft (The Federal Trade Commission)

www.cyberbully411.org (This is a good resource for kids)

www.fbi.gov/stats-services/publications/parent-guide/parent-guide (FBI Parent Guide to internet)

Internet filtering software:

- Safe Eyes (safeeyes.com)
- Net Nanny (netnanny.com)

Family Alternative to Facebook/Google+:

Fanlala.com Provides 24/7 monitoring for safe content. Kids can connect with friends, follow pop-culture news, play games, listen to family-friendly music and other safe-for-the-family activities.

Family Internet Contract

Use the following sample **Family Internet Contract** for your kids and teens. Share or print additional copies at MarkSeguin.com/Family-Contract.

Family Internet Contract

I understand that it is a privilege to have and use digital devices, including a cell phone and computer. Therefore, I agree to the following:

1. I will give my parents my user names and passwords for all sites I use and I will not share these with anyone else.
2. I will talk to my parents before setting up social network sites and we will set my privacy settings together.
3. I will not "friend" anyone that I do not know personally without my parent's permission.
4. I will talk to my parents about rules for going online. We will agree on how long and what sites I will visit. I will not access other sites or break these rules without their permission.
5. I understand my parents are concerned about my safety and my online reputation. I understand that my safety is very important and that I may disagree with my parents, but I will obey their rules.
6. If I "friend" my parents on social network sites so they can monitor me, they agree not to post anything unless we agree.
7. I will not meet anybody in person that I only know through the internet.
8. I will not give out personal information including my full name, age, address, birthday, city, phone numbers, email, school, etc., without my parent's permission.
9. I will tell my parents if I receive any messages that make me uncomfortable or are upsetting. We will discuss and agree on appropriate actions that may include blocking.
10. I will not do anything that hurts other people or is against the law on line. I will not bully anyone online, send or post pictures without permission. I will not setup fake profiles or create pages or websites that are mean or intended to hurt someone. I will remove any picture or video that has been requested to be removed.
11. If I post anything inappropriate, I will take responsibility, rectify the situation if I can and accept the consequences.
12. I will not use any technology to cheat on school work, games, etc.
13. I understand that not everything on the internet is correct. I will verify and use reputable sites for research.
14. I will not download anything or install software or apps, fill out surveys, enter contests or give out my email address without my parent's permission.
15. I understand that everything I put online (such as comments, posts, pictures & videos) including anonymous comments, has the ability to become public and remain online forever. I will not post, comment or send anything that I wouldn't want my family, teachers, college admissions or future bosses to see.
16. If my online reputation has been compromised in any way, I will discuss this with my parents immediately and take appropriate action.
17. I have discussed this contract with my parents and I understand the consequences for breaking any part of this contract.
18. My parents have the right to make exceptions, modify, update or add to this contract.

Child's signature

Date

Parent's signature

Date

About the Author

Mark's identity was stolen as a child, requiring a great deal of time and energy for full restoration. From this experience, Mark recognized the rising rate of identity theft and the devastating consequences in our society. These factors influenced Mark to build what is now a cutting-edge, social networking, identity theft awareness and data breach prevention solution company. Mark has specialized in educating and training in social networking safety and awareness, customer service, management, supervisory, management team building and employee development for over ten years.



Mark is a leader in the industry. He helps schools and business organizations reduce risk and liability from data loss by training about social networking safety and smart cell phone use resulting in identity theft by recognizing critical high-risk activities of students and employees and by implementing training that will "*Change Thinking, Change Behavior, Reduce Risk*". Mark is a certified ID theft risk management specialist certified by the Institute of Fraud & Risk Management.

Mark works with a variety of businesses including insurance, K-12, higher education, medical, oil and gas and non-profit industries. He has trained tens of thousands of employees and students.

As a father of five, Mark has first-hand knowledge of social media. He has seen the benefits of this high-tech communication as well as the risks involved. He uses his personal and real life business experiences in an engaging format to share critical information.

Mark also conducts staff development training at local junior colleges in the East Texas area. on safe social networking and identity theft prevention. Mark is a member of the MGMA, TMGMA, PCOT, TAC and Tyler Chamber of Commerce. He is also a board member of TACHE.

Mark is married to his wonderful wife Elizabeth of 19 years and they have five children ranging from 15 to 24 years of age. Mark and his family reside in east Texas and in his free time likes to play games, camp and cycle. He is a sixth generation Texan. If you would like Mark speak to your school, business or group, he can be reached at 903-533-9123 or Mark@MarkSeguin.com.