

Be Safe in CyberSpace

A Family Guide to CyberSafety



Mark Seguin

(903) 533-9123

mark@BeSafeinCyberSpace.com

Website: BeSafeinCyberSpace.com

Table of Contents

Introduction.....	3
Safer Social Networking	4
Tips for Parents.....	4
Tips for Your Kids & Teens.....	5
Cyberbullying.....	7
Tips for Parents.....	7
Tips for Your Kids & Teens.....	8
Sexting/Texting	9
Tips for Parents.....	10
Tips for Your Kids & Teens.....	10
Smartphone Safety	11
Tips for Parents.....	11
Tips for Your Kids & Teens.....	12
Identity Theft	13
Learn the Lingo	13
Helpful “How To’s”	14
Review Browsing History.....	14
How to Turn off Geo-Tagging	14
Resources.....	15
Internet Filtering Software.....	16
Family Internet Contract.....	16

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, without the written permission from the publisher.

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.

The internet can be used by children in many ways:

- find assistance with school assignments
- increase knowledge base
- keep in touch with family and friends
- learn new skills or further develop abilities
- meet new people and share comparable interests

However, there are risks in participating in internet activity. 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 some restaurants.

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.

The area of internet safety and security is very, very broad and encompasses many aspects. Therefore, only key issues are covered in this guide. User 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.



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 can be a great way to keep in touch with friends and family and basically just hang out and visit. Currently, Facebook alone has more than 800 million active users; social networking sites now reach 82 percent of the world's online population representing 1.2 billion users around the world.

Different social networking sites have different purposes, including:

- **Facebook** and **MySpace** – create communities of friends
- **YouTube** and **Google Video** – create, download and upload video content
- **Facebook**, **Photobucket** and **Flickr** – share still photos

Often kids can forget who they are communicating with and who might see the information they post. It's often easier to say and do things online that they might not do in "real life". Consequently, it is important for kids to stop and think about how their behavior will affect others as well as themselves.



Tips for Parents

- **Keep** your computer in a public or common area of your home. Set up an internet content filter (like *Safe Eyes* or *Net Nanny*) or other security software and update it often.
- **Talk to your child** about unsuitable websites, pornography and digital disrespect. This way, they can be prepared and aware so if they are exposed they will know what to do.
- **Stay educated** in 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 and see for yourself what they're doing. **By being involved, you also keep them safe.**
- **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?
- **Learn how** to turn off geo-tagging (see page 14 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 hate and harassment when it occurs.
- **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.

- **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.
- **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.
- **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.** Content posted online can be there forever. You can put it up, but can't automatically take it down.
- **Make sure** you don't put any key personal information on your profile. 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. (See "How to" on page 14.)
- **Keep in mind** you are not a "member" of Facebook or any other social networking sites. The price is privacy: your data is gathered and then they sell your info such as likes and activities.
- **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 private so only people you accept as friends can see what you're posting. Privacy settings change from time to time 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's great to have online friends, including them on your



“friends” list allows people who don’t 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’ve 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.
- **Don’t respond** if someone sends you unkind or inappropriate messages or asks you to do something that makes you feel uncomfortable or scared. Instead, tell your parents or another adult you can trust.
- **Don’t share** passwords with friends – no matter how close you are with them. Passwords are private.
- **Stop and think** before you “check in” somewhere. Geolocators 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. Don’t 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 geolocators which can expose you or your friends’ location.



Cyberbullying

Cyberbullying occurs when the internet, email or smartphones are used to deliberately and repeatedly engage in hostile behavior to harm someone. 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) can include 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 (day and night) this harassment is amplified. Harassment by excessive texting and inquiries (“where are you,” “what are you doing,” “who are you with”) is digital disrespect as well.

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.

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:

- **Don't 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 them. 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 repond or retaliate to the sender** of these messages and block the person who is behaving badly. Report them to your Internet Service Provider.

- **Stand up and speak up** if you see or know about cyberbullying happening to a friend; it is important to support them and report the bullying.
- **Guard** your privacy – don't post information or photos that you wouldn't want everyone to see.
- **Only share** your login and password details with your parents or another trusted adult.
- **Use** a screen name different than your email address and do not give ANY private information such as full names, addresses, phone numbers, personal identification numbers, passwords, school names or names of family members or friends. Don't post anything that you would not want to be made public.
- **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. Remember the police can recover messages – 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 canceled. If you break the law, you may also be reported to the police.

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, 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 young person'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.

Tips for Parents

- **Remind** them 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.
- **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 can be there forever. You can put it up, but you can't necessarily 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.
- **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.

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 can't always be there to supervise, means there are potential risks. These include:

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

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.)
- **Find out** how to access the internet and manage other services. This information is usually available on the smartphone carrier's website.
- **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 setup to gather their usage and other data.
- **Remind your child** that they shouldn't 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.
- **Teach 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.

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.
- **Just say no!** 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. Geolocators can tell strangers where you are.
- **Tell your parents** or another trusted adult if someone sends you mean or bullying messages or asks you to do something that makes you feel uncomfortable. Make a note of the number it came from, the date and time of the call, or save the message. It may need to be followed up by your school, Internet Service Provider (ISP), smartphone carrier or the police.



Identity Theft

There is a direct correlation between your CyberSpace identity and identity theft.

- About 1/3 of social networkers has information posted on their pages that could lead to identity theft. Source: PCWorld.com
- Every 14 seconds, someone becomes a victim of a cybercrime. Source: DarkReading.com



The Federal Trade Commission states that 26% of Consumer Complaints come from ID Theft. How is a victim's information misused?

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

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
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





Helpful “How To’s”

Review Browsing History

Find out where your kids have gone online:

If you need to, you can check your child’s or teen’s browser histories but don’t know exactly what that means; it’s simple, really. So simple your kids know how to do it - but you may not.

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, 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 think you don’t want them to 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

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

There are myriad 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 or follow the instructions from www.icanstalku.com for most iPhones, Androids and Blackberrys:

iPhone (iOS 4.x) Apple greatly simplified the way to turn off location services on a per-application basis. To see your settings, go to Settings, General, then Location Services. From there you can set which applications can access your GPS coordinates or disable it entirely.

iPhone (iOS 3.x) With the iOS 3.x there are two ways to disable Geotagging of photos. The first involves disabling of all location based services. To disable this feature, Go to Settings, General then set Location Services to off.

Be warned: This will turn off *ALL* location based services for *ALL* applications. Of course you may actually have need to use location based services for other applications (such as maps and driving directions, etc), but just not for your pictures.

There is no easy way to disable location based services for just one application. However, you can make the iPhone prompt us at first use for each application. Once reset, the first time you enter the application you can enable or disable location based services for the application. To do so you need to go to Settings, General, Reset.

Be careful here! Select Reset Location Warnings, and then Reset Warnings. This restores all of your Location based warnings for each application to the default, which in most cases is "Ask on first use".

From here, you enter into the default Camera app on the iPhone, you select Don't Allow. This will prevent the Camera app from geotagging your photos.

Google Android (Verizon Droid Phones)

Like the iPhone, there are two ways to turn off geotagging. To completely disable GPS location finding for all applications, do the following:

Press the Menu Key and then Settings; Then press Location and security. By default, GPS is on. Uncheck it to turn it off. Like disabling the GPS in the iPhone, this will break location based information for all applications, including legitimate uses.

In order to disable for just the camera application, start the Camera app to make sure that you are not saving your location. This is the menu on the left side of the camera application; it slides out from left to right.

Select "Store Location" and make sure it is set to off. Once this is disabled, the camera app will no longer add geotags to your images.

BlackBerry Devices

There are multiple ways to disable the geo-tags on Blackberry. Detailed are three ways:

Select Options, Advanced Options, GPS, press Menu key, Select Disable GPS and select Yes to confirm. This will disable all GPS capabilities on the phone.

Select Options, Security, Applications Permissions, menu select Edit on the application (default is Prompt for BB Core), Expand Connections, Change Location (GPS) to "Deny", or you can disable within the application. Most apps i.e. Google Maps, etc... will just default everything to "allow" for app permissions regardless of app settings chosen during setup.

Go into picture-taking mode (via HomeScreen, click icon "Camera"), press the Menu button and choose "Options". Set the "Geotagging" setting to be "Disabled". Finally, save the updated settings.

The exact directions on how to disable may vary by phone but we suggest checking under the Options menu of the Camera application and also any kind of "Location" or "GPS" menu under your phone's control panel.

Resources

Internet Filtering Software

After extensive research of internet filtering software, we recommend:



Net Nanny
POWERED BY **content watch.** **ID Shepherd.com**

PRODUCTS LEARNING CENTER BLOG SUPPORT

Net Nanny Internet Filter

86,520,618 Adult Sites Blocked Last Month

With the parental control tools provided by this powerful internet filter, parents can feel comfortable knowing that what their children do on the internet is in their hands.

Family Internet Contract

To access and download a free **Family Internet Contract** for your kids and teens, go to IDShepherd.com.

IDShepherd.com also provides myriad links and other free resources as well as updated news and tips to keep your family guarded and protected.

Materials Presented by:

Mark Seguin

*Husband / Father of Five / 6th Generation Texan
Certified Identity Theft Risk Management Specialist
Educator / Keynote Speaker / Trainer*

*Mark is available to speak at your club, school, church or organization on
Social Media and Identity Theft issues*

Rules for Safe and Fun Internet Use

Think before you post information online – once posted it stays posted.

Ask your parents/adult before you give anyone on the internet your name, address or any personal details

Be careful who you trust online. Making new friends can be fun, but there's a chance that they may not be who they say they are.

Always keep your password a secret

Set your profile to "private" so your personal information is kept secret.

If someone is nasty, offensive or makes you uncomfortable online, don't respond and leave right away

Don't open messages from people that you don't know. These could be nasty, contain viruses or be trying to sell you something.

Don't accept offers that seem too good to be true – they probably are.

Tell your parents if you are upset by language, pictures or anything scary on the internet.

Be Safe in CyberSpace!

