

FOURTH  
EDITION



# Family Online Safety Guide

By Marian Merritt



STOP | THINK | CONNECT™



**Norton**  
by Symantec



*Marian Merritt*

# Introduction

---

My husband and I are parents to three wonderful children who are active users of our family's computers. My kids are constantly challenging my knowledge and beliefs about technology and how it fits into their lives. I understand the joys and dangers of the Internet. But as they navigate their way around the Web—finding new game sites, downloading music, and communicating with friends through their social network and texting—I realize that it's all about knowledge and staying in touch with what our children are doing.

We're all trying to manage our children's growing independence and doing our best to defend them and our computers from the many serious dangers on the Internet. In this short guide, we'll go through the top Internet concerns, but if you are interested to dive more deeply, I'll recommend websites and publications that can keep you informed as the conditions change each day. I congratulate you for your interest in the topic and willingness to learn more. Nothing frustrates me more than parents who throw their hands in the air and say, "My kids know more about this than I do!" You can learn enough to help and enough to know when you need the assistance of security professionals and software to get matters back under control.

So whether your concerns are about elementary school-aged children learning to use search engines or managing your high schooler's growing dependency on a social networking site, we'll explore these issues and give you easy-to-understand tips and guidelines for each topic. *Hang in there!*

**Marian Merritt**

*Author, Parent, and Norton Internet Safety Advocate*

# Contents

## Family Online Safety Guide

Fourth Edition

### Through The Ages

Pre-school Aged Children (ages 3-4) .....	6
Elementary School Children (ages 5-7) .....	6
Tween Children (ages 8-12) .....	8
Teens (ages 13-17) .....	11
Off to College and Beyond .....	14
Talking “The Talk” .....	15

### The Basics

Cybercrime is Real Crime .....	20
Viruses, Worms, and Spyware .....	20
Scamware .....	22
Click Jacking .....	22
Bot Seriously... ..	23
Private Information and Identity Theft .....	24
Inter-personal Problems .....	25
Cyberbullying and Cyberstalking .....	25
Protect Your Password .....	27
Internet Predators .....	29
Sexting .....	30
Safe Browsing .....	31
Secure Your Wireless Network .....	31
Parental Control Software .....	32

**Risks**

Plagiarism and Cheating . . . . . 34  
File Sharing, Music and Video Downloads . . . . . 34  
Social Networking Sites . . . . . 35  
Porn, Gambling, Racism, Anorexia, and Hate Sites. . . . . 37  
Digital Reputation. . . . . 38  
Teen Online Privacy. . . . . 38  
Email. . . . . 39  
Instant Messaging. . . . . 40  
Cell Phone Safety . . . . . 41  
Mobile Device Safety . . . . . 42  
Blogging . . . . . 43  
Digital Photos and Privacy . . . . . 44  
Online Shopping . . . . . 45  
Online and Mobile Banking and Bill Paying . . . . . 46  
Online Gaming and Signs of Addiction . . . . . 47  
Stop. Think. Connect. . . . . 47

**Top Tips**

Top Tips for Adults . . . . . 48  
Top Tips for Kids . . . . . 49

**A Final Word**

Resources. . . . . 50  
Other Important Internet Safety Resources to Know . . . . . 51

**From the Makers of Norton Security Products . . . . . 52**

**Marian Merritt . . . . . 54**

# Through The Ages



## **Pre-school Aged Children (ages 3-4)**

Ever since the arrival of touch-screen smartphones and tablets, children still in their baby chairs can access technology with ease. That doesn't mean the fun and educational apps come without risk. Pay attention to the programs your tot is using. Is there advertising? Can they click a button and purchase add-ons that cost real world money? If they push the wrong icon will they see inappropriate images or play music with profane lyrics? Use parental control settings and pay close attention to the devices you share with your youngest children. And protect the devices from sticky fingers and accidents with screen protectors and cushioned cases.

## **Elementary School Children (ages 5-7)**

This is the age when many of today's children are introduced to the Internet. Now that more and more U.S. schools have computer labs, PCs, Macs, or tablets in the classroom, a child's first use of a computer may be at school. Others will get their first computer experience at home, learning from parents or older siblings. Children aged 5-9 average 29 minutes spent online every day.<sup>1</sup>

Websites (often with online games)—such as NickJr and Webkinz— attract the youngest online children, aged as young as toddler years. Some sites are almost entry-level social networking sites because they have chat and other communication features. Parents of young children should turn these features off initially. It's helpful to note that leading sites like Webkinz have become popular because of their extra efforts to provide a safe environment. Within Webkinz World, parents don't have to 'turn off' chat for young children, because they offer a 2-pronged approach. Kinz Chat is completely pre-scripted so parents can allow children to send notes etc. and 'chat' with friends without worries. It's a great way to introduce

1. [http://joanganzcooneycenter.org/upload\\_kits/jgcc\\_alwaysconnected.pdf](http://joanganzcooneycenter.org/upload_kits/jgcc_alwaysconnected.pdf)

the chat concept and start discussing online ‘netiquette’ and safety practices. Kinz Chat Plus is monitored chat and parents who feel their kids are mature enough must still actively give permission, and can always revoke it.

Make sure your younger children understand you want to limit their online chatting even if it’s within the friendly interface of a favorite game or club site. Later, you can introduce the concept of chatting with people they know, such as aunts, uncles, or friends—being sure to reinforce that they should always ask you before talking to anyone new online.

Ideally, when your children are this age, you will be actively involved with their online activities the same way you are with their homework. For example, you should make sure the computer or device your child uses is within your view, in a public space like the kitchen, den, or family room. Remember, with our growing use of mobile devices to access the Internet, trying to monitor a stationary computer just isn’t going to be enough. Parental control software can help you by limiting the sites your child can access when you aren’t around, or on devices that disappear into backpacks and bedrooms. The controls also can limit any information you don’t want your child sharing, whether it be their name, age, phone number, or other private information. You should turn on all the filtering and security features in your computer’s search engine (such as the Google SafeSearch™ feature) to prevent your young child from inadvertently arriving at an adult or other inappropriate site as they do their homework. Be sure to show your child how to close a browser window and let them know it’s always OK to close a site if something surprising or disturbing occurs. Tell them never to chat, type messages, or share information with anyone on these sites unless you are with them.



**HOT TIP:** Teach the youngest children never to share passwords, even with their best friend! We’re seeing account theft (a junior version of identity theft) happen to kindergartners.

## KEY RECOMMENDATIONS:

- Use parental controls to limit websites and hours spent online.
- Set high security and privacy settings with browsers, membership, and social networking sites.
- Install and maintain Internet security software on all devices.
- Monitor your child’s screen use and sit with them when they’re online as much as possible.
- Talk about protecting private information (name, phone number, etc.) and never sharing passwords with friends.
- Start having “The Talk” as part of your regular “Back to School” preparations (see page 15).

## Tween Children (ages 8-12)

Tweens are far more social and adventuresome in their computer use. They talk to their peers at school and learn about the newest and “coolest” sites. They will sign-up for their first email and instant messaging accounts. Ask your child about those accounts and what the passwords are, so that you can monitor their activities, and know with whom they are communicating. Children at this age may also start to check out social networking sites that are popular with older teens and adults. A study from Consumer Reports estimates there are 5.6 million underage kids on Facebook.<sup>2</sup> Most won’t create an account until they are a little older (and the usual legal age to begin is 13 years), but they will visit the pages and posts of friends, older siblings, and other relatives who have their own pages and profiles. If your young child creates a social network before they are the approved age and it is discovered by the company, their account will be deleted.

Some tweens are using photo sharing and blogging sites as a junior version of social networking. You may not realize they can post messages, comment and share among a network of friends using these apps. Pay attention to ALL the sites your children visit, especially those that occupy most of their time. Don’t assume time spent on a photo sharing site is due to a new interest in digital photography alone!

2. [http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm#How\\_children\\_fare\\_on\\_Facebook](http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm#How_children_fare_on_Facebook)





**HOT TIP:** Use Norton™ Family to monitor the creation and use of social networking accounts. You can even see what age your child claims to be.

Tweens are also interested in music, and the Internet is an easy way to listen, discover and download new tunes, as well as meet others who share their musical interests. They might follow news about a favorite group or celebrity by visiting their blog or website; check out different sites to get the latest gossip along with downloadable photos; or join a Twitter feed.

Online video sites are enormously popular. Some of the videos contain strong language or violent material, so you need to monitor your tween's visits carefully. And remind your tween not to click links in video comments which may take them to dangerous or inappropriate sites. The more creative tweens are learning how to take their own digital photos, edit videos, and share their creations with friends and family. With your help or the help of a more experienced friend, they are starting to post their creations online as well.



**HOT TIP:** Check your browser's history to see where your children are visiting and how often they go to those sites. Norton Family helps you monitor Web activity and prevents kids from trying to delete visits from their history.



## KEY RECOMMENDATIONS:

- Set a password on all computers and mobile devices, especially cell phones.
- Frequently check your computer's Internet history (or your parental control history) to see the sites your children have visited, and monitor their email and instant messaging (IM) accounts to see who they communicate with. Note: if your child is using a cell phone, social network, photo sharing, or blogging service they may communicate through those media rather than in traditional email.
- Set rules about online communication, illegal downloading, and cyberbullying.
- They should know never to click a link in an email or IM—this is a common way people get viruses or reveal private and valuable information to criminals.
- Discuss risks and concerns about posting and sharing private information, videos, and photographs.
- Watch for signs of obsessive or addictive online behaviors (see Online Gaming and Signs of Addiction, see page 47).
- Keep computers and cell phones visible in the house.
- Foster open communication and encourage your kids to tell you if anything online makes them feel uncomfortable.
- Start having “The Talk” (see page 15).

## Teens (ages 13-17)

Teens are developing even greater independence and this is reflected in their online lives. With that independence comes responsibilities, including being careful in their online world. By now most teens have created at least one if not several accounts on social networks. Some kids friend their parents without difficulty while others resist the online connection strenuously. Still other teens create a “fake” profile that they use to friend and connect with parents and family while the real and more questionable action is happening on another account. Using a program like Norton Family allows a parent to spot that sort of subterfuge.

So what’s the big appeal of social networking and other teen online interests? With screen names, memberships, blogs, profiles, and other Internet elements that they visit daily, teens communicate the details of their lives with each other. Digital traces of their thoughts can be left all over the Web. Often they don’t know—or they forget—that everything posted on the Web is there for all to see, and it’s probably there indefinitely. All it takes is a single Web search by a potential roommate, romantic interest, college admissions director or potential employer—five, ten, even twenty years from now—and all of the photos, opinions, and thoughts of your teen could be there for all to see forever. It’s never too early to start managing your digital reputation (see page 38).



We want to teach our children how to take risks without getting into trouble. It's for the very same reason, that they take driver's education classes before they actually drive a car. Or why you sat patiently poolside during all those swimming lessons. The same type of caution needs to be used regarding the Internet. Yes, your teens might roll their eyes when you try to explain the "rules of the road" when going online. Instead, you might try to arrange with your school to have Internet Safety presentations brought in through the numerous organizations that will do this. Examples include your local D.A.R.E. officer, district attorney's office, iKeepSafe, i-SAFE and others. Some of the best online safety education for teens can come from their peers, with proper training. Encourage your school to get the upper classmen on board, coaching the younger students about managing their digital reputation, being kind online and other key lessons. You may find your kids actually pay more attention to the same information when it comes from outside the family. And don't forget to set up a similar presentation for the parents and teachers. We all have so much to learn!



**HOT TIP:** Perform a Web search on your children and show them what you find. Or do a search on yourself as a teachable moment and be honest about anything you find that is objectionable. After all, your kids may have already "Googled" you! You can also set up a Google or Yahoo alert.



**HOT TIP:** Parents who are friends with their children on social networks should NOT comment on their child's posts or news feed. Keep communications private.

## KEY RECOMMENDATIONS:

- Reinforce rules of appropriate online behavior (language, private information and imagery, cyber ethics, illegal downloading, limiting hours of usage, and avoiding inappropriate adult sites).
- Be aware of your teen’s online life (social networking sites, photographs, private information, club and sports activities) whether on their site, a friend’s site, or their school’s Web pages.
- Review the sites your teen visits; don’t be afraid to discuss and possibly restrict sites that offend or concern you.
- Remember your teen is accessing the Internet at home, school, a friend’s house, the library, via cell phone, or even a gaming system—so talk to your teen about their activities in all those scenarios.
- Talk to your teen about the privacy issues regarding sexting (see page 30). Sexting is most common for older teens in a romantic relationship and is perceived by many young people as a normal activity.
- Ask them not to download files (music, games, screensavers, ring tones) or make financial transactions without your permission.
- Teach them never to share passwords and be wary about typing private information when on a shared or public computer, or one they think might not be secure. They should always log off of accounts, even when at home.
- Teach them never to click a link in an email or IM—this is a common way people get viruses or reveal private and valuable information to criminals.
- Whenever possible, keep computers and cell phones in a common area in the house and not in your teen’s bedroom. At least, make your teen charge their phone outside the bedroom at night, to avoid late night temptations and disruptions to their sleep.
- Foster open communication and encourage your teen to tell you when something online makes them feel uncomfortable. Remember, they are teens but they are still kids.
- Remind your teen to take responsibility for keeping Internet security software maintained and up-to-date, as much as for their protection as yours.
- Have “The Talk” and be sure to ask your teen to teach you something new about the Internet (see page 15).

## Off to College and Beyond

As your teen grows up and leaves home, whether for school or work, they will need to understand the additional adult responsibilities to be found in the online world. That includes protecting their privacy, especially their Social Security Number (SSN) and financial information; preventing identity theft; and related risks to their credit history, which is particularly important for a young adult. If your teen is using a laptop at college or in their new job, make sure they understand the added risks of using wireless connections and that they purchase the necessary security software including a reliable backup solution. They might be tempted to skip these optional items, so it's good to insist on vigilance when it comes to their laptop's security.



**HOT TIP:** Check your Norton account ([www.mynortonaccount.com](http://www.mynortonaccount.com)) to see if your family's security software can be installed on another computer. Some of the Norton security suites include multiple installations on computers and other devices in the same home.

If your teen is going to a college away from home, find out what the computer policies are. Some schools dictate particular operating systems or software configurations for incoming freshmen so it's best to have that information before you head off to the computer store. Some classrooms and dormitories are configured with wireless technology (commonly called WiFi), so you'll want to be sure you get an appropriate WiFi card so your college-bound offspring will be able to enjoy those services.



**HOT TIP:** Keep in touch with your grown kids with Voice Over Internet Protocol calls (VOIP). Look for free services for voice and video chats from Skype or within your favorite social network.

## Talking “The Talk”

“What you don’t know won’t hurt you.” You don’t actually believe that when it comes to your kids and what they’re doing online. Yet so many of us act as if we are in denial about the varied menu of dangers available on the Internet. If you are like most parents, you aren’t an Internet expert or even as skilled as your children might be online. That’s OK. In fact, it’s not necessary to be an expert in order for you to help your children enjoy the Internet safely. What you need to do is TALK to your kids about what they are doing on the Internet, and explain your family rules. And then repeat the talk as frequently as you deem necessary to get them to understand the importance of what you are sharing with them.

I’m going to give it to you straight: getting your children to tell you, with honesty, about their Internet experiences is difficult. One in five children worldwide admits that they are doing things on the Internet of which their parents wouldn’t approve. Still, 62% of kids worldwide have already had a negative online experience.<sup>3</sup> Your child may not be telling you without you asking—so it’s time to ask!



3. According to the Norton Family Report: <http://us.norton.com/norton-online-family-report/promo>

While half of all parents say they are talking to their kids about Internet safety, it's usually a onetime effort that includes two pieces of advice: "People online aren't always who they say they are" and "Stay away from online strangers." Kids fear if they tell you about their online mistakes, parents will react by taking away their computer, their Internet connection, their access to their friends, and the rest of the world. They figure Mom and Dad just don't "get it" when it comes to the online world.

Nevertheless, at Norton, we've learned through our global research with parents and kids that kids want their parents to know more about the Internet. They are also overwhelmingly willing to talk to their parents about the Web. That's good news.

So now that you know that your kids are willing to talk to you, and you realize you want to learn more about what they are doing, how do you begin? How do you connect with your kids in a way that allows them to be honest with you? How do you avoid judging, overreacting, or panicking about what you might hear? How do you create a conversational, non-confrontational discussion that is productive enough so that you can repeat the activity without your kids putting their hands over their ears and chanting "LALALA!"

I'd like to introduce a new twist on an old concept called, "The Talk." I recommend talking with your children about their online activities right away and then do it again, regularly. Your children's online activities keep changing. As they get older, they visit different websites, try new activities, and create new social networking accounts. Yesterday, for example, everyone was talking on email. And today, they use the built-in messaging in their social network or text on their cell phone to communicate. As your children get older, their need for privacy will increase at the same time the online risks they take may also increase. Taking risks is part of the normal adolescent maturation process. But as the parent, it's your job to set boundaries so those risks don't destroy your child's reputation or their future. Just know that those boundaries are likely to get stepped on or over from time to time.



There are five questions to focus on for “The Talk.” These questions should work with kids of all ages, though you’ll need to adjust the content to be age appropriate. Make sure to give your child space (both physical and time-wise) to provide you the answers to these questions. Personally, I love having these conversations with my kids in the car (for some reason, when everyone is looking at the road ahead, it seems easier for kids to be more open with their parents).

- 1. What are your friends doing online?** This question directs the attention away from your child and towards the general online activities in his/her crowd. It is a good way to start and keep things neutral and generic. You want your son or daughter to give you honest feedback and you must reassure them that you won’t punish them for their answers. You will start to hear about such activities as gaming, chatting, building social networks, even homework and research activities.
- 2. What are the coolest or newest websites and apps?** Ask your child to tell you why these sites and programs are cool. You can also ask about the ones that aren’t popular anymore and why.
- 3. Can you show me your favorites?** Yes, I want you to take 20 minutes out of your incredibly busy life to look at penguins sliding down a snowy hill or your child’s dreadlocked warrior avatar swinging a sword around. Ask how you set security or privacy settings (look at the top and bottom of the screen for those areas of the site). Maybe you’ll be tempted to play along and set up your own account. (If you do, be sure to let your child know). Ask your child how they use the site and why these sites are favored over other sites.

**4. Have you heard of ‘cyberbullying’ and have you ever experienced it in anyway online?** Your child may not know “cyberbullying” by name but he or she knows what it looks and feels like. Some kids call cyberbullying “drama” or “just joking around.” Talk about stories you’ve read or seen in the news about nasty emails, embarrassing photos, or personal information that was shared or sent around to other kids. Ask about fake social networking profiles. Find out if your child has ever heard of this kind of behavior going on. Make sure your child knows cyberbullying is common and if they haven’t seen any yet, that’s good. Make sure they know how to react if it does occur (they should not respond to any email or IM that contains the cyberbullying; they should try to save or print it so they can show someone; they should block it if they know how; and most important, they should ALWAYS report it to Mom/Dad or another trusted adult.)

**5. Has anything online ever made you feel weird, sad, scared, or uncomfortable?** This is an opportunity to discuss cyberbullying, accidental browsing discoveries (such as porn or racist sites) or even something strange involving a friend or peer in the neighborhood. The idea is to make sure your child knows they can come to you and they won’t be punished when something unusual or bad happens online. Experiencing something bad is almost inevitable when your child is active on the Internet. Make sure your child knows they can come to you for help and you won’t overreact.

**Extra credit or questions for families with older kids:**

- Do you really know everybody on your ‘friends’ list?
- Do you know how to use and set privacy and security settings? Can you show me how?
- Do you ever get messages from strangers? If so, how do you handle them?
- Do you know anyone who’s made plans to meet someone offline that they’d been talking to online?
- Are people in your group of friends ever mean to each other online or on phones? If so, what do they say? Has anyone ever been mean to you? Would you tell me about it if they were?
- Sometimes kids take nude or sexy photos and send them to others. Has that ever happened at your school or with anyone you know?

That’s it. That’s The Talk. It’s not hard, it’s not technical, it’s totally doable and I hope you’ll give it a try. If you are a teacher, you can try it in a discussion with your class.



# The Basics



You will find as we discuss Internet risk that it really falls into three types: Cybercrime, inter-personal problems and reputation/privacy issues. Throughout the remainder of this guide, we'll discuss the contributing issues within each area but you may find it helpful to think of online problems as being caused by “unknown bad guys”, “people I know”, and “my own mistakes”.

## **Cybercrime is Real Crime**

Cybercrime is a real, global and growing phenomenon. Norton has conducted several global studies and interviewed thousands of adults and kids around the world. In the 2012 Norton Cybercrime Report, we found that 2/3 of adults globally have already been a victim of some form of cybercrime.<sup>4</sup> That might be a virus, worm, Trojan Horse or other malware but it can also include online scams, hijacked social networks, and email accounts and online predators. While Norton has many tools to help you combat cybercrime, the most important step you can take is to install good Internet security software on all your computers and mobile devices before you go online.

## **Viruses, Worms, and Spyware**

Computer viruses have been around for more than 25 years in various forms. But with the popularity of email and file exchange on the Internet, the distribution of these threats really took off! Those who create viruses and other forms of malicious code or “malware” used to wreak their havoc to prove their software skills or show off to each other. I call those early days the time of virus writing for “Fame.” But today, the stakes are much higher and many of the bad guys are international cybercriminals, motivated by financial gain through their illegal activities. So now we are in the time of virus writing for “Fortune.” Some security analysts estimate that a cybercriminal can make several hundred thousand dollars per year through cybercriminal activities. At Norton, we're seeing over a million new types of malware a DAY!<sup>5</sup>

4. Source: Norton Cybercrime Report, [www.norton.com/2012cybercrimereport](http://www.norton.com/2012cybercrimereport)

5. Source: Symantec's Internet Security Threat Report 2011

In 2010, we saw a new form of malware emerge that could cause trouble by harming our physical infrastructure. That means, when the Stuxnet malware took down an Iranian nuclear facility, we have evidence of the first organized and structured cyber attack that was designed to harm manufacturing and industrial systems. It made a lot of people in the internet security space sit up and pay notice!

In terms of what you have to worry about now, malware such as spyware, keystroke loggers, and bots can cause you enormous trouble. Spyware and keystroke loggers monitor your normal computer activity and then report your private data out via the Internet to the criminals. Dangerous links in email, instant messages, or social networks can silently install malware on your computer or get you to visit malware hosting websites. Help keep your children and your computers safe by installing Internet security software on your family's computers and making sure it's updated with the latest protection files. Tell your children not to turn off the virus scanner or firewall, even if they think it might speed up a game. It's just not a safe risk to take!



## **Scamware**

Scamware, rogue antivirus, or fake antivirus is a malware threat that can jeopardize your computer as well as your wallet. Typically, the problem begins when the innocent Web surfer encounters a strange pop-up advertisement. The ad mimics an operating system message or a virus alert from your computer. The message tells you your computer “has detected a virus” and you are instructed to run the scanner to find it. Many people follow the instructions, believing the alert is genuine. Children, especially, are vulnerable to this threat because they often believe they can help their parents by “cleaning up the virus.”

What happens then is pure cybercriminal evil genius. The “scan” shows you your computer is infected with many problems and you’re told to purchase the cleanup tools. Many fall for this and both download a dangerous file containing more malware and share their credit card information with the crooks. The scamware or rogue antivirus then hijacks your computer, preventing your security software from working and you from seeking help via the Internet. And it’s likely your credit card is now being traded on the international black market.

Make sure you and your children know not to fall for these dangerous scams. If you have an infected computer, there’s help available from Norton. We have a free tool called Norton Power Eraser, designed to eradicate these malicious pieces of code. If your computer is so compromised you can’t access the Internet, you’ll have to download it from a second computer (ask a friend) to put the program onto a disk or thumbdrive. Our technicians at NortonLive ([www.norton.com/nortonlive](http://www.norton.com/nortonlive)) are also available (for a fee) to do the work for you and remove the virus.

## **Click Jacking**

In social networks, scammers try different tricks to get you to click and download their malware or share your private information. A funny video with a clever caption, (“OMG! You won’t believe what this girl did!”) or a fake app that can show you who was reviewing your profile can be very tempting.

## **Bot Seriously...**

Have you heard the one about the robots taking over the world's computers? It's no laughing matter. "Bots" and "botnets" are now a major threat impacting our online security. Bots (short for robots) are forms of stealth software that can sneak into your computer and cause it to send out spam and phishing emails to others.

Many illegal businesses now thrive on these bots that can spread like wildfire, leveraging the computing power of hundreds of thousands of unsuspecting personal computers for the sole purpose of stealing your personal information and cheating you out of your hard earned money.

How do they do it? A bot is a type of malicious software, snuck onto your machine by cybercriminals, allowing the attackers to take control over your affected computer. These "Web robots" are usually part of a network of infected machines that are used to carry out a variety of automated tasks, including the spreading of viruses, spyware, spam, and other malicious code. Worse, the bots are used to steal your personal information and can wreak havoc on your credit through the unauthorized use of your credit cards and bank accounts. The bots can also display phony websites, pretending to be legitimate, and fooling you into transferring funds and providing your user names and passwords to be used for more illegal activity.

The best defense against these horrible little bots is to install top-rated security software and be sure to set your software's settings to update automatically so you know you're getting the latest protection. The experts also advise that you never click on attachments or links inside of emails unless you can verify the source, which is something you need to teach your kids. Once infected with a bot, these devious programs try to hide from your security software, so you may need to visit the Norton website to download special free tools to remove them.

## Private Information and Identity Theft

Your children don't automatically know what "private" information is, so you need to explain the concept that it's any information that allows a stranger access to personal or financial information. Private information includes real world data like your name, telephone numbers, address, mother's maiden name, sports club, school, even the name of a doctor. Bad guys can turn even a small clue into a full record on a child and parent, and they can trade and sell that private data to make money. It's easy for bad guys to apply for credit in your child's name and get real world merchandise and money, while ruining the child's (or your) credit rating and good name.

If you do suspect you or your child have been a victim of identity theft, you'll want to monitor your credit report to look for evidence of new accounts or loans. You are entitled to receive one free annual report from each of the three credit reporting services: Equifax®, Experian®, and TransUnion®. It is good to rotate your request from the three firms, every four months, just to make sure your identity and credit are safe. Once you find evidence of identity theft, you will need to report it to law enforcement, beginning with your local police station. That police report will strengthen your case when you work with the other sites and companies involved. You may also be able to put a "freeze" on your credit report. Visit [www.ftc.gov](http://www.ftc.gov) for more information. Another helpful resource is the Identity Theft Resource Center at [www.idtheftcenter.org](http://www.idtheftcenter.org).





## Inter-personal Problems

The Internet connects people to each other in ways we could hardly have imagined a few years ago. And with all those connections and forms of communication, a few bad players can make it entirely uncomfortable or painful for the rest of us. The very anonymity of the Internet enables a freedom of expression that often crosses the line, causing pain and suffering to others. Fortunately most young people want to behave appropriately online and off. With some Internet safety education we can help our children learn the correct and kind ways to navigate the Internet and how to manage when others are unkind. What are “Inter-personal” problems on the Internet? They include issues like cyberbullying, password theft, and sexting.

## Cyberbullying and Cyberstalking

Technology gives our children more ways to connect, socialize, and create than ever before. Unfortunately, some kids use email, instant messaging, cell phone photos, social networks, and text messages to embarrass or bully other children. Also, kids’ digital messages can be edited to change the meaning, then forwarded to other kids to embarrass, intimidate, or insult. Children don’t report their cyberbullying experiences enough so it’s hard to get good statistics on the problem. Most studies put the problem at about 1 in 5 kids have been cyberbullied, but research from the National Crime Prevention Center put it as high as 43%.<sup>6</sup>

Make sure your children know they must guard even the most casual text message and watch their own written words. They should never be cyberbullies, and they should always tell you if and when they are being cyberbullied. A password on a cell phone can stop unwanted peeks at private emails, photos and messages.



**HOT TIP:** If you or your child are being cyberbullied: don’t respond. A response gives the bully or bullies the reaction they seek. Silence will confuse them. If your child gets asked “did you see that post or message?” teach them to say they didn’t, or even say, “My mom was working on my computer last night. Maybe she saw it.”

6. <http://www.ncpc.org/resources/files/pdf/bullying/Teens%20and%20Cyberbullying%20Research%20Study.pdf>

Keep a copy of any bullying message by using the “Print Screen” key on your keyboard or the camera feature on your smartphone. You never know when a full record of events will be needed by a school official or law enforcement.

If appropriate, report the cyberbullying to the website or provider, to the school, etc. If the cyberbullying involves kids at school (and most targets know who is involved or have strong suspicions), you can report it to the principal, a teacher, the counselor, or the school resource officer. Almost all schools now have a cyberbullying policy that spells out exactly what will happen. Make sure you keep good written records and ask the school to give you their action plan in writing. If any of the bullying involves threats of further action or violence, you may need to involve the police. Often the police can assist you in contacting website owners to get offensive material taken down but you will have to manage the ongoing efforts aggressively.

Schools are responding to the growing awareness of cyberbullying by creating policies and pledges to address the issue. Often they are required to provide policies and school-wide training by state law. The tragic suicide of U.S. teen Megan Meier in part due to (among other factors) cyberbullying has become a rallying cry. More recent stories linking cyberbullying and teen suicide include Phoebe Prince and Tyler Clementi. What is important to remember is that no matter how serious the cyberbullying situation, suicide is rarely due to a single cause or a single event. If you ever see an online comment indicating the poster is considering suicide, treat it as a serious statement and report it to law enforcement, the host of the website or service, or the National Suicide Prevention Lifeline at 1-800-273-8255.

Wherever we have an online bully and a target, we have silent observers who witness the harassment and give it more power by providing an audience. Make sure your children know they must never engage in cyberbullying even if all they are asked to do is visit a site, open an email, pass along a cruel message, or add their comments to a mean social networking page. Give your child the training to respond to a target/victim with kindness, support, and friendship. How powerful it can be to call someone going through cyberbullying merely to say, “I saw what they did. It was unkind and I’m sorry.”

Cyberstalking is a dangerous extension of cyberbullying and can be used by those who engage in stalking in the real or “offline” world. According to the U.S. Department of Justice, 1 in 12 U.S. women will be a victim of stalking in their lifetime.<sup>7</sup> Women between ages 18 and 24 are at the highest risk of being stalked both offline and online. With awareness of the issue, our older teens can learn to defend themselves and parents should know how to help. The stalker may hijack an email account and pose as the person whose email they’ve hijacked. The attacker might deface a social networking page or send hateful messages to the victim’s friends, engage in outright identity theft, or try to destroy somebody’s credit and reputation.

Cyberstalking can be dangerous and should be reported to law enforcement, Internet service providers, and website hosts. Keep all evidence of both cyberstalking and cyberbullying.

### **Protect Your Password**

When I talk to kids at schools, I’ll often ask if anyone has ever had someone else use their password or change it without their permission. Even with children as young as five years old (kindergarten), about ¼ will raise their hands. It’s a common way for kids to abuse trust even with good friends or siblings. Although it may be meant as a joke, it sets up a child to have their accounts mismanaged, their private information shared and their social networks used to cause trouble. Logging out is another great technique to ensure no one has access to your accounts. My son found this out the hard way when he forgot to logout of his social network while at a friend’s home and the boy posted some rude comments on his page!

Guide your children to use passwords that they share only with you. Make sure that you prioritize passwords for email and social networks as the most important to make complex and unique. Avoid using easy-to-guess passwords such as dictionary words, names, or dates that your child or an Internet hacker might break.

Here’s a good way to manage passwords. Pick a single master password that you’ll be able to remember, and then customize that password for different websites. The first step is to choose a good master password

7. <http://www.ncvc.org/src/AGP.Net/Components/DocumentViewer/Download.aspxnz?DocumentID=40616>

that uses more than six characters and some combination of letters and numbers (rather than real words).

In this case, let's use the phrase "I want to go to Paris." Reduce that phrase to each of the first letters, use the number "2" for the word "to" and you'll end up with "lw2g2P". Then add the first and last letter of the website to it (Symantec.com's website would be: "Slw2g2Pc"). This little trick helps me remember all those various passwords and yet keep things complex enough that it's hard for a computer hacker to crack. This sequence makes sense to me but not to anyone else. It also helps that I get different passwords for different accounts. If one password to one account is compromised, the rest are still secure.

Even with complex and unique passwords it's easy to get overwhelmed by how many you need to enter in a day. There are some computer applications that manage passwords, and some browsers now feature the ability to store multiple passwords. It's very insecure to keep track of passwords in a list stored on a computer, on paper notes next to the computer, and so forth. I use Norton Identity Safe, a password management feature built-in to Norton 360 and Norton Internet Security software programs.

I mentioned earlier that your priority for unique and complex passwords should be for email and social networks but did you wonder why? If a hacker gains control of your email, they can change all your other passwords by clicking on the "forgot my password" link on the other websites. And if they gain control of your social network, they can scam or send dangerous links to all of your contacts.

**Parent note:** Make sure you have your child's passwords for email, IM, social networking sites, and their devices. It's a good idea, so you can review who is communicating with your child, and in the event of trouble, you'll have important access. If your child forgets their password on a mobile device like a music player or phone, it might be impossible to recover it. Work together on your family's password strategy.

## Internet Predators

Statistically, the chances of your child being approached online by a sexual predator is low, yet it remains a top parental concern. Whenever I speak to parent groups, parents want to hear my advice for keeping kids away from online strangers. The National Center for Missing and Exploited Children conducted a study in 2006 showing that 1 in 7 children will be solicited sexually online, but most of those contacts are from peers, rather than strangers and the contacts were not worrisome to the child.

Make sure your children know they must never email, chat, or text message with strangers and it's never OK to meet a stranger in the real world. Make sure they understand that someone they see or meet online is still a STRANGER, no matter how often they see them online.

A particular worry is for any child that discusses sex with strangers online—this has been shown to lead to even more offline meetings. Should a stranger approach your child online to talk about sex, please visit [www.missingkids.com](http://www.missingkids.com) (a site from the National Center for Missing and Exploited Children) and report it to their CyberTipline. Teach your children to report any request for “A/S/L” – which stands for “age, sex and location” or anything like that to you or to another trusted adult.



## **Sexting**

“Sexting” is when a sexual image or video is sent electronically. Commonly an image is created using the built-in camera or video camera on the cell phone, then sent to others as a multimedia messaging service (MMS) message. Pew Research reports that 4% of cell-phone-owning teens have sent sexts and 15% have received them. Amanda Lenhart of Pew describes the purpose of such sexual imagery as a kind of “relationship currency” used to build intimacy, signal availability, or romantic interest. Pew’s study breaks down sexting scenarios to three types:

1. Exchanges of images solely between two romantic partners;
2. Exchanges between partners that are then shared outside the relationship;
3. Exchanges between people who are not yet in a relationship, but where often one person hopes to be.

You can imagine the powerful forces at play when a group of popular kids target another, less powerful teen to solicit a sexual image. The less powerful teen may give in as a ploy to gain access to a boy, a group, or social status.

Where it gets particularly scary is that the image might be considered a form of child pornography, putting both the creator and the recipient in legal hot water. Once that photo leaves the computer or cell phone, it cannot be pulled back. It has been the case that young girls have been pressured by older boys at their school to create these photos in a sort of hazing episode. In New Zealand, a 12-year-old girl was being blackmailed to produce these images by someone who had erased her account in an online gaming world. Law enforcement is highly aware of this trend but somewhat conflicted in how to proceed. Their job is to stop the creation of child pornography, but when the creator is a child and also a possible victim, the next step can be difficult to discern. We’re starting to see the legal system take a more balanced approach to dealing with these situations, offering counseling and community service where, even a few months ago, there might have been jail time or being placed on the sex offender registry.

## **Safe Browsing**

Make sure your browser is set to offer you its built-in security and safety features. For example, Microsoft® Internet Explorer offers security and privacy settings. These are found under “Tools,” then “Internet Options.” Popular search engines such as Google also offer safety features. For example, Google’s SafeSearch is designed to screen sites that contain sexually explicit content and remove them from your search results. While no filter is 100% accurate, SafeSearch helps you avoid content you may prefer not to see or would rather your children did not stumble across.

By default, Moderate SafeSearch is turned on, which helps keep explicit images out of your search results. If you prefer you can change your setting to Strict filtering to help filter out explicit text as well as images. You can modify your computer’s SafeSearch settings by clicking on Search settings at the top right of the Google homepage. Norton Family can help you set and lock those safe search settings.

## **Secure Your Wireless Network**

Home wireless networks can present other security problems, and there’s a lot you need to do to ensure that they are secured from unknown intruders who might use your bandwidth, or worse, host their spam and other attacks from your system. Also, a laptop, smartphone or tablet and a wireless network allow your children to access the Internet from all over your house, which makes your efforts to monitor their activities that much harder.

If you have wireless (“WiFi”) at home, make sure you do everything possible to make it secure: reset the router password so it follows good password rules and isn’t easy to guess; enable wireless encryption to prevent a stranger from spotting your network from the Internet; restrict the access your system shares on the network and make sure your Internet security software is kept up-to-date. In my home, we have occasionally used the router’s controls to turn off access to our kids’ laptops, gaming devices and web-enabled music players at bedtime. It’s helped our kids to deal with temptations to chat and post late at night. Some parents go so

far as to disconnect their router and take it into their bedroom at night and other parents change the WiFi password daily—whatever works for you is fine.

### **Parental Control Software**

Parental control software enables you to choose where and when your child goes online, and to ensure that they don't view inappropriate subject matter. Parental controls differ depending on the application offering the feature. Usually there are varying levels so you can customize the program according to the child being protected. For example, for a five-year-old, you would create a "white list" of pre-selected and parent approved websites where you would allow the child to visit.

Or you might set up accounts requiring a parent's login to enable the child to surf the Web, or to set up time limits. You can allow older children or teens more access and flexibility. You might restrict Web access by categories of sites in the program's library to prevent them from being exposed to racist, pornographic, or other objectionable materials. One to try is our FREE program, **Norton™ Family** (also available in Premier Version for a fee.)

**Norton Family** is an award-winning family safety service that works on PC, Mac® and Android™ devices. You can use it in any of the 25 languages it's available in. What I love about it is how easy to use it is. It really was designed with regular folks in mind. You can install it on all the computers in your home, then login from anywhere, even from your web-enabled smartphone. You can put limits on the types of sites each child can access, customize with time limits, monitor social networking and searches and view their Web history. Since the information is stored "in the cloud," your child can't fudge what they're doing by deleting their history.



Our Advisory Council of experts includes child development, law enforcement, and online safety experts, even a “youthologist.” They worked with our **Norton Family** team to design a flexible yet powerful program. The team was guided by a principle of encouraging parent/child communication. You can’t use the program to spy on your child since it is always visible to the child, appearing with each start of the computer and as an icon in the tool tray. We hope parents will work with their children to explain how it works, what they can see, and agree together on the House Rules. Since Norton Family is free, why not give it a try? To create an account, just go to [www.onlinefamily.norton.com](http://www.onlinefamily.norton.com) and get started. Remember, though, that no software provides perfect protection from every possible Internet risk. Parents need to use a combination of software, education, oversight, and communication to protect children, regardless of their age. The Web is a rich resource, and it defeats the purpose to lock it down entirely. Parents need to talk with their children to ensure that their beliefs, morals, and values are upheld when their children go online.



# Risks



## **Plagiarism and Cheating**

It's very easy to find online homework guides to all the popular school textbooks and many websites offer essays and thesis papers for sale!

Cheating has never been easier, more available and more tempting to our children. Remind your kids that it's very important to use the Internet for research only. Explain to your child why user-generated content such as that found at Wikipedia may not be entirely reliable. Teach your child to use such online resources as a starting place and show them how to find the most credible and trustworthy online research sites.

## **File Sharing, Music and Video Downloads**

Children quickly learn about the joys of sharing music with each other. And it's often at the tween stage when someone tells them about file-sharing sites, especially the free ones. Let your children know the dangers of file-sharing sites and programs, which, by definition, let strangers have access to some portion of your computer. Using file-sharing sites may expose your computer and information to "bot" software, spyware, keystroke loggers, viruses, and other dangerous malicious code.

I once attended a law enforcement seminar where they demonstrated how quickly you can find sensitive financial documents from popular file sharing sites, simply by running a search. The officer opened up one of these programs, typed in the phrase "tax return" and within seconds, hundreds of actual tax returns were available. He double-clicked on one and we could see the poor person's unwitting sharing of his private and valuable financial information. Additionally, downloading music or videos for free is often illegal. Show your children where they can legally download music and video from sites such as iTunes® and Amazon.

## **Social Networking Sites**

Social networking websites are among the fastest growing phenomena on the Internet for both kids and adults, but it is tweens and teens that are driving that growth (remember, users are legally required to be 13 years and older to use social networks). The most popular site, Facebook, now boasts an incredible 1 billion members on its site. All social networks provide a place for kids to get together online with new and existing friends. When used cautiously, these sites offer great ways for all of us to communicate and share experiences. When used carelessly, however, social networking sites, like all sites, can expose your friends, family, and network to malware, cybercriminals, even identity theft.

Cybercriminals can spread malware within our favorite social networks by fooling us into clicking a video link, downloading a program or re-logging in on a spoof page that mimics the social network. The idea is to steal your account login, spread the malware to your network of friends, infect your computer with malware or get you to visit an infected site where a drive-by download awaits. Teach your kids to avoid these clever tricks and if they fall for it, delete any dodgy posts in your account, change your password and report it to the social network security team.

Teach your children not to post private information or inappropriate or misleading photographs. This information, once posted, becomes public and can be stored on the PCs' and Internet history files of others. Even if you remove such information or photos, they may still be out there on the Internet and in the hands of people who can use and abuse them. If you or your child are asked to "untag" someone or to remove a comment or other posting, be sure you both demonstrate good online etiquette and comply immediately.

Even how we define social networks needs updating. Some under-age tweens have started using photo sharing sites and blogging services as social networks. Post a photo of a piece of paper with information about where everyone is meeting and all your "followers" can comment and update the plan. And it all is happening away from parent view because the photo sharing site isn't a social network "by definition." Pay attention to all the sites your children use.

Social networking sites enable kids to form networks of friends who can communicate freely with one another. Make sure your kids don't allow people they don't know to join their networks. They should keep the pages private, so only invited friends can find them on the site. Review the account privacy and security settings together.

You and your family should always be mindful when accepting friend requests, and never accept a request from someone you don't know. According to the 2012 Norton Cybercrime Report, 35% of online adults have friended someone they didn't know in their social network. These strangers, once part of your network, can expose both you and your friends to both malware and cybercrime. Make sure that your child sets the privacy settings features properly so they limit who can see photos or videos to their page. For help with that, I recommend ConnectSafely's "A Parents' Guide to Facebook" ([www.fbparents.org](http://www.fbparents.org)), and for great tips on all aspects of social Web safety (on any device) click to ConnectSafely.org's Tips & Advice page ([www.connectsafely.org/tips](http://www.connectsafely.org/tips)). Facebook has many valuable security tips like registering multiple email addresses to the account, or enabling alerts for new logins. For more information on the latest methods for keeping your account safe, visit [www.facebook.com/security](http://www.facebook.com/security).

A major concern within the world of social networks is spam and phishing attacks. We need to stay as alert and cautious about responding to strange messages or clicking links within social networking sites. In most cases your security software can block the majority of harmful sites you might link to, or prevent spyware, keystroke loggers, or other malicious code from being downloaded. But if a hacker gains control of your social network, they can trick less protected friends into clicking dangerous links or visiting dangerous sites. Common online scams, where the crook pretends to be you to scam your network for money, are growing due to their effectiveness. If you ever see spammy links in your Feed, be sure to remove them quickly and to mark as Spam, so you can help protect

others online. Norton Safe Web is a free tool available for anyone on Facebook. It can scan all the links found on your Facebook page to check for any that might be dangerous.

### **Porn, Gambling, Racism, Anorexia, and Hate Sites**

The darkest corners of the Internet world include some dangerous and illegal elements. Research has shown that many children have seen online pornography by the age of 11.<sup>8</sup> Without parental controls or browser filters, it's almost inevitable your child will run into something you and he/she will find upsetting. Make sure your child knows to tell you when and if that should happen and reassure them you won't be angry if it does. The most important thing is to address it and prevent it from happening again.

Some children and teens may become curious about sites featuring racist or hate messages, or promoting risky or damaging behaviors such as anorexia and cutting. You may only discover this by regularly checking your computer's browser history or reviewing your Norton Family data. Even a single visit should prompt you to talk to your child about it. Don't assume it was idle curiosity. Explain your house rules about such sites and ask your child about their motivation for visiting. As you talk, if your child reveals issues, such as depression or self-loathing, don't delay in getting your child professional help from a therapist or other trained specialist to deal with such matters.

8. [http://news.cnet.com/8301-17852\\_3-20006703-71.html](http://news.cnet.com/8301-17852_3-20006703-71.html)

## Digital Reputation

Your digital reputation is the impression created when your life is viewed through a search engine result. There have been numerous stories in the news about kids putting things online that later caused them scholastic, financial, or romantic harm. A high school student posted photos of themselves holding a bottle of beer, resulting in a lost scholarship. An employee posted comments about their boss on a social network and was later fired. Even if your child is cautious about what they post, it's important to review their online activities to see if anything they've said, uploaded, or commented on might serve to harm their future. It's never too late to adjust your social network privacy settings or to delete comments, photos, videos, and posts that are offensive, juvenile, or simply foolish when viewed by a stranger.

It can be tough to get things taken down from other sites or prevent them from showing up on search engine results. Still, it's worth examining what your digital reputation is and taking steps to ensure it's accurate. If you excel at sports, make sure your accomplishments can be viewed online. Won a debate competition? Post a video on a video sharing site and tag it with your name. Raised money for a charity by joining a walk-a-thon? Kudos and be sure the charity website spells your name correctly. In this way, you can make sure the first results found on you are positive and push any negative items farther down in the results.



**HOT TIP:** Set up a web alert in your name and your child's name and discuss what shows up.

## Teen Online Privacy

Educate your teens about the Internet. By now, they are savvy enough (or should be) to know that people online aren't always who they say they are. It's easy to lie about your age, sex, and location online; so many people do it for innocent and not-so-innocent reasons. Continually remind your teens that they can't trust strangers online any more than they can in face-to-face contacts. They should never allow a stranger to join a buddy list or a

chat or IM conversation. And they should never accept free software, ring tones, or screen savers from strangers.

Remind your teen that email addresses, user account names, and IM handles should not be their real name, the name of their school, or some combination of the two; they shouldn't be provocative or otherwise inviting to a predator. They should be as anonymous as possible. Also, they should never share a password, even with a friend. That may sound obvious but there are trends among older teens to share passwords as a "friendship" test. Not a good idea!

Make sure your kid's school's website is password protected or requires a login for more than superficial, public information. For example, a school in my home town posted a travel schedule that included flight information and the names of students traveling for a sports team trip on its website. Other possible problems include lists of class names and student addresses and home telephone numbers published on the website.

## **Email**

Both children and adults should have different email addresses for different purposes. For instance, it's a good idea to have one address for online shopping, another for online banking, and another for corresponding with friends and family. That way, for example, if you receive a notice from your bank on your family email, you'll know that it's malicious spam that you should delete.

Make sure your children's email accounts have the highest level of spam filtering turned on. According to a Norton research study, 80% of children report receiving inappropriate spam on a daily basis. The Norton Cybercrime Index, a free tool that tracks and warns computer users about daily cybercrime risks around the world, reports spam regularly makes up about 80% of the world's emails. If your children aren't old enough to ignore or delete spam (some of which can contain highly offensive images and content), don't allow them to manage their own account. Avoid posting your email address online to prevent "scrapers" from adding you to their spam target list. Type your address online as "name at isp dot com". As an example, my email would be "marian at Norton dot com".

A child's email account should be created with care. Select a name that won't allow a stranger to find them. They shouldn't use first and last name combinations. They also shouldn't use suggestive screen names or addresses, such as "sexylexy" or "wildthing," even if it seems "cool" to do so. Make sure they use strong passwords that are never shared with anyone other than their parents. You should know your children's email account passwords so you can monitor their activity, frequently. Look at who they send email to and receive email from. Do you know everyone? And let your child know you will be doing this to help keep them safe and not because you don't trust them.

### **Instant Messaging**

Instant messaging (IM) isn't a new function but it has become more challenging for parents simply because it's included in social networks and less visible to monitoring. It's also a popular service available on mobile devices. You may not be able to track it as easily but you should explore services, like Norton Family or those available from your cell phone provider.

Here are some common messaging abbreviations and their meanings.

- POS/P911/PAW/PAL - Parent alerts
- BFF - Best friends forever
- BRB - Be right back
- G2G, GTG - Got to go
- L8R - Later
- LOL - Laugh out loud
- NM JC - Nothing much, just chilling
- TTYL - Talk to you later
- TY/TX - Thanks
- YW - You're welcome
- For a more complete list go to:

[http://en.wiktionary.org/wiki/Appendix:Internet\\_slang](http://en.wiktionary.org/wiki/Appendix:Internet_slang)



## KEY RECOMMENDATIONS:

- Teach children not to click on links within emails that they receive, since links can lead to fake websites. Never accept a link or download a file through IM.
- Disable the preview function in email. This prevents potential malicious code in the message area from executing.
- Kids should not respond to emails or unexpected instant messages from anyone they don't know.
- They shouldn't make their instant messaging profile or social networking page public.
- Set instant messaging preferences to keep strangers at bay.
- They shouldn't allow sites to show when they are online or to display their ID or private information on pages they visit.
- They should always log out when not using IM or when editing their social networking page to make sure their privacy is protected.

## Cell Phone Safety

As your children graduate into middle school and high school, they will ask (demand?) for a cell phone. A recent Pew study found that 75% of kids ages 12-17 years have cell phones. It's not at all uncommon for kids 6-9 years old to have them as well, often receiving the hand-me-down phone of a sibling or parent. There is such a range of phone types and service plans—it pays to do your homework before choosing. Just because your 12 year old wants a phone doesn't mean they need unlimited texting or Web access.

Once your child has a cell phone, you will have to learn how to send a text message. The Pew study also found that 54% of teens send text messages every day. Half of teens send 50 or more text messages per day and for teen girls, the average is over 100 texts per day! Tweens and teens have pretty much moved off of email to communicate and favor both texting and the built-in messaging of their favored social network. The only time a kid uses their cell phone to make a voice call, it's to call their parents. Some also still use instant messaging and video chats on their computers. But increasingly even those services are simply part of their favorite social network and not as visible as a separate activity.

If your child's phone has Web access, consider adding security to it. You can block anyone from adding spy software to the phone, or tapping the global positioning system (GPS) feature to track their physical location. You can also set up remote lock and wipe features in the event of loss or theft. Norton offers security products for smartphones, and you can find them on our [www.norton.com](http://www.norton.com) website.

### **KEY RECOMMENDATIONS:**

- Set a password on the phone/device to prevent unwanted access.
- Tape a contact phone number to the back of the phone, in case it's lost.
- Install security software to protect the phone and data if it's lost or stolen.
- Charge the device overnight in your kitchen to minimize late night texts or inappropriate photos using the cell phone camera.
- Research provider services like Web filters, time limits, number blocking and other parental controls.

### **Mobile Device Safety**

From the most recent Norton Cybercrime Report, 35% of online adults have had their mobile device lost or stolen. We know from Symantec's 2012 "Honey Stick" project that when a smartphone is lost, only half of those who find the device will try to return it. And almost all the finders will first access the phone's data. Prevent someone from reviewing your private messages, contacts and images by setting a password on the device. Then put a piece of tape (yes, a low tech solution!) on the phone with a contact number, such as your home or office number, to help a Good Samaritan who wishes to return the device to you.

Beyond the cell phone, our children carry powerful computers in their pockets at all times. Consider the many popular gaming devices that offer Web browsers or tablets like the Apple® iPad™. The capabilities offered by these devices are impressive but we do need to consider security threats and online safety risks, even with devices we primarily use for e-reading and games.

Set a password for all mobile devices. This can prevent someone from installing spyware or purchasing an app without permission. Set up filters

and parental controls, either on the device or use your home's WiFi network. Install security software to detect spyware or block unauthorized access. Routers offer a wide variety of ways to control how your home's network is used by these devices. Set time limits, filter websites by category, even deny access to unauthorized users by adjusting router settings.

One trend to watch is the ability to make purchases with our mobile devices. New technology called "near field communications" enables cell phones and mobile devices to make purchases by sending authorization signals. Applications are already available for a wide variety of providers to help people purchase coffee, make person to person payments, conduct online banking—all with a wave of a mobile device. We can be sure that cybercriminals are going to figure out an exploit so be cautious about the use of mobile payments and monitor your accounts with care.

## **Blogging**

A blog is an online journal or diary. You can read mine at [www.norton.com/askmarian](http://www.norton.com/askmarian). Some blogs are topical, dedicated to a particular subject matter. Often teens have blogs that are more like traditional private diaries—except they are open to everyone on the Internet via the teen's own website or on a social networking site—which is like placing their diary online for the world to see. Your kids should be sure of their objective in blogging before doing so. Search engines can usually pick up the information that is posted, so your best efforts to protect your privacy are defeated. If you publish photos or links to private websites on your blog, you also reduce your privacy.

In addition, people such as potential employers or school admissions officers may read your blog, and this exposure may affect other areas of your life as well. For example, people interviewing for jobs have been declined because of items in their personal blogs or in the blogs of friends and family that mention them. Make sure you run online searches for yourself and family members. If you object to something another person posted, you can and should request they remove it. If they refuse, you can report them to the website host. If it's slanderous or illegal, you can also involve law enforcement.

## **Digital Photos and Privacy**

Many kids have cell phones that include a camera and many also have their own digital cameras. Talk to your children about the need to protect photographs online from strangers or even from peers who might use them inappropriately. You can track the sending of digital photos from the phone (just check your online or paper statement). Make sure your child shows you the photos on their phone so you can advise them about anything you deem risqué or not appropriate for sharing. If you are using photo sharing sites, make sure you don't allow others to use your photos, especially photos of people. There have been cases where photos on photo sharing sites were used in advertising without the subject's permission.

Many cell phone and digital cameras tag photos with geo-location information. This allows you to figure out the location you were in when the photo was taken and might be handy to create a photo map of a drive across the country, or a hike to a remote waterfall. But as a default setting, it's not a great idea to advertise your location with every image. Check the camera or phone settings to turn geo-location tagging off in your images. And if your child is using a social media driven geo-location service or checking into locations with their social network, talk about any privacy concerns this might raise.

### **KEY RECOMMENDATIONS:**

- Turn off geo-location tags on your camera or cell phone photos.
- Don't make private photo albums public.
- Require visitors to a photo-sharing site to use a password.
- Back up photos with backup software because computer crashes, power failures, building fires, or natural disasters can easily wipe out your photos and other computer files.
- Use only online photo services that provide security protection.
- When an online photo service provides you with the option to send email through their service, protect your friends' privacy by sending them a link to the site instead.

## **Online Shopping**

The Internet is a shopper's paradise, especially for teens with a credit or pre-paid gift card (or access to yours). There are, however, rules they should follow to shop safely. Begin any online shopping session by making sure your security software is turned on, and is updated. Shop with only known and reputable sites, as using an unknown website can be risky. One way to increase safety is to make sure any page where you enter personal data such as your address or credit card number uses encryption. You can tell if it uses encryption by the Web address, which will start with: https. Another thing to look for is the lock icon at the bottom of the browser frame, which is intended to indicate that the website you are visiting uses encryption to protect your communications.

Shopping on reputable sites is just the first step in being a safe online shopper. Don't click links in email to get to a favorite store or sale. You should type the store address in the browser window. This will help prevent you from becoming a victim of a phishing attack, in which you are transferred to a fake version of your favorite store's site. Phishers can steal your passwords, logins, stored credit card information, and worse.

Check credit card statements as often as possible—monthly at minimum. This is the best way to know who is using the card and to spot problems before they are difficult to resolve. The credit card company offers consumer protection and will work with you to manage any disputed or unauthorized charges. Don't use debit cards online. Credit cards provide additional layers of protection, including the ability to question unusual charges. With a debit card, money may be removed from a bank account without anyone realizing it until the monthly statement appears. And it may take a while to get it back.

## **Online and Mobile Banking and Bill Paying**

More and more people are thoroughly comfortable with online banking. Direct deposit of paychecks to your bank is a great security measure, preventing someone from stealing your check from your mailbox, and it speeds up your access to the funds. It's also a cost saver for your employer. Online tax filing will soon be the standard method in the U.S.

The latest trend from U.S. banks is mobile banking. There are numerous apps for Apple and Android devices from the major financial institutions, making depositing a check as easy as taking and sending a cell phone photo. Naturally, the early adopters of such technology are the younger members of the population but with practice, I'm sure more of us will give it a try.

Cybercriminals are ready to take advantage of these tools. We've already had a spate of malware like the ZeusTrojan that looked for online banking credentials and stole millions of dollars from victims. Some malware targets those who manage small business and charity accounts, taking information off of websites to send targeted "spearphishing" messages.

Stay on top of all electronic banking activity as you do with credit cards. Regularly access your account to check transactions. Make sure bills are paid on time and in the correct amount. Keep your computer protected in the same way you do for general Internet security to prevent people from stealing passwords or banking information. And don't access your accounts from public computers, kiosks, or insecure wireless connections. Always type the Web address of your bank into the Web browser, never click a link from an email. When finished, be sure to logout of your account. Don't store account login information in the browser.

## **Online Gaming and Signs of Addiction**

MMORPG—what is that? It stands for the increasingly popular and potentially addictive “massive multiplayer online role-playing games.” These can be highly immersive and for some teens, especially boys, a real distraction from their real lives. Set rules with your children about the amount of time that can be spent on these sites, whether or not they get money to spend for membership or to purchase gaming accessories (in the real world, such as online auction sites or within the game) and any other concerns you might have.

According to the Computer Addiction Services at Harvard University-affiliated McLean Hospital ([www.computeraddiction.com](http://www.computeraddiction.com)), these are some of the psychological and physical symptoms of addiction:

- Inability to stop the activity.
- Neglect of family and friends.
- Lying to employers and family about activities.
- Problems with school or job.
- Carpal tunnel syndrome.
- Dry eyes.
- Failure to attend to personal hygiene.
- Sleep disturbances or changes in sleep patterns.

## **Stop. Think. Connect.**

The National Cyber Security Alliance ([www.staysafeonline.org](http://www.staysafeonline.org)) offers guidance to consumers on how to protect yourself and keep the web a safer place for everyone. Their campaign, Stop.Think.Connect., is designed to get us to become more aware of online risks before we take action such as clicking an unknown link, opening an email attachment or visiting a new website.

# Top Tips



## **Top Tips for Adults**

- Use Internet security software on all computers and mobile devices.
- Set a password on all computers and mobile devices.
- Don't open suspicious emails or click unknown links. Remember to Stop. Think. Connect.
- Avoid using file sharing software programs.
- Be vigilant on public computers or WiFi networks.
- Back up your computer—go online with Norton™ Online Backup
- Establish House Rules for your family about how you'll use technology and set limits.
- Understand social networking—join and use privacy and security settings
- Help your children manage their digital reputation. Set search alerts for each family member.
- Post for permanency. Never “friend” a stranger and limit who can see your posts.
- Use parental control software and frequently check your computer's Internet history.
- Spend time with your children online and have “The Talk” regularly.
- Teach your children to tell a parent, teacher, or trusted adult if they feel uncomfortable about anything they've seen on a computer.
- Use complex and unique passwords for all your accounts. A password manager makes this easy.
- Regularly review online statements and accounts for banking, credit cards, cell phones and other services for suspicious activity.
- Install only well-known and well-reviewed software and mobile apps.
- Be kind online. Let your online activities be an example to others.



## **Top Tips for Kids**

- Be careful about clicking links in email, instant messaging and social networks.
- Use complex and unique passwords for all your accounts. A password manager makes this easy. Remember, don't share passwords with others.
- Secure your smartphone with a password to stop unauthorized users from viewing your information.
- Log out of accounts when you are done to prevent others from having access.
- Don't download, make online purchases or install software or apps without checking with your parents.
- Observe rules of all the online services you use. Don't join social networks until you are 13 years old and have your parents' permission. "Friend" your parents.
- Limit what you share online and use privacy and security settings wisely. Don't list private information in public online locations and only post photos and videos your parents would approve.
- Be kind online. Let your online activities be an example to others. Take things down if others ask. Report cyber bullying.
- If anything you see online or on your mobile device upsets you, tell your parent or another trusted adult.
- Make sure you use security software on all your computers and mobile devices.

# A Final Word



The Internet is a wonderful resource, with elements that often make it feel like an actual city. The Internet offers us education, entertainment, news from around the world, and improves our lives with access to tremendous services such as chat, email, online shopping, and more. By becoming educated and aware of the online risks and dangers, and using up-to-date Internet security software, you can help your growing child navigate this amazing cybercity with increasing levels of independence. Continue educating yourself by learning about new technology and online issues. Make sure your behavior online serves as a role model for your children by engaging in safe Internet practices yourself. Thank you!

## Resources

Want to have a parent or student Internet safety presentation in your school, church, or other local organization? There are numerous individuals and organizations that will provide free or low cost Internet safety presentations, but sometimes it's hard to know how to start.

Here are some suggestions of groups to contact. It's also good to ask around among your friends and neighbors to see what your local community may have to offer.

- D.A.R.E. or local police department's cybercrime officer
- District Attorney's office
- PTO or PTA organization in your school
- AntiDefamation League (ADL)
- iKeepSafe
- i-SAFE
- National Cyber Security Alliance

## Great Resource Sites for Parents

- Ask The Mediatrician: <http://cmch.typepad.com/mediatrician>
- Lady Gaga’s “Born This Way” Foundation: [www.bornthiswayfoundation.org](http://www.bornthiswayfoundation.org)
- Connect Safely: [www.connectsafely.org](http://www.connectsafely.org)
- Stop Bullying: [www.stopbullying.gov](http://www.stopbullying.gov)

## Other Important Internet Safety Resources to Know

- Norton’s Family Resource website: [www.norton.com/familyresource](http://www.norton.com/familyresource)  
(articles, newsletters, blogs, videos)
- Norton Family safety service: [www.onlinefamily.norton.com](http://www.onlinefamily.norton.com)
- Norton Cybercrime Index, a free resource to keep you informed as to the latest cybercrime threats around the world: [www.nortoncybercrimeindex.com](http://www.nortoncybercrimeindex.com)
- Federal Trade Commission offers numerous consumer friendly resources: [www.ftc.gov](http://www.ftc.gov)
- [www.annualcreditreport.com](http://www.annualcreditreport.com)  
(Order your authentic and free credit report at least once per year)
- [www.staysafeonline.org](http://www.staysafeonline.org)



From the makers of

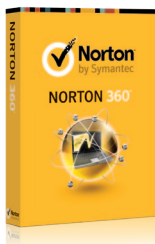
# Norton Security Products

.....



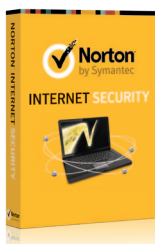
## Norton One™

Membership that makes protecting multiple computers and devices easier than ever. Secure any combination of Macs, PCs, iPhones, iPads, and Android devices with your favorite Norton security software. And add an extra layer of protection with anti-theft capabilities. If you need help, dedicated experts are available 24x7x365 with an average wait time of 2 minutes or less.



## Norton 360™

Norton 360 delivers comprehensive, easy-to-use protection that defends you, your computer, and your files from just about any threat. PC Tuneup fine-tunes your computer and automatic backup keeps your digital photos and other important files safe from loss.



## Norton™ Internet Security

Surf, shop, socialize, and bank online without worrying about viruses and cybercrime. Norton Internet Security delivers fast, light protection that stops threats and protects your identity without slowing down your PC.



## Norton™ Mobile Security

Norton Mobile Security—the simple, yet powerful, Web-based service that lets you protect your smartphones and tablets from online threats and mobile spam. It also helps you recover your lost or stolen devices and prevent strangers from accessing the private Stuff on them.

## Norton™ Family

A smarter way to keep your kids safe online. Norton Family gives you the tools to manage where they go, how long they are online, who they talk to, and what information they're sharing with others. Best of all, it helps you open up a positive dialogue with your children about good online habits.



## Norton™ SafeWeb for Facebook®

Norton SafeWeb for Facebook safeguards you against malicious URLs by scanning your Facebook feeds. It also helps protect your friends by advising them of malicious URLs you might have in your feed.



## Norton™ Hotspot Privacy

Norton Hotspot Privacy creates a private, secure connection when you use public WiFi hotspots. You can confidently connect on the go, knowing your user names, passwords, and online activities are protected from hackers and eavesdroppers.



## Norton™ Identity Safe

Norton Identity Safe is a free app that stores and synchronizes your user names and passwords across PCs, mobile devices, and browsers, so you can easily and securely access them anywhere you go.



# Marian Merritt

---



## **Marian Merritt**

Marian is the Norton Internet Safety Advocate for Symantec Corporation. She provides insights into technology issues impacting families. Marian translates technical issues into language that is readily understood by the public. She meets regularly with teachers, parents, and children to ensure the company “gets” what is happening in

today’s Internet world, and families and schools get the information they need to help create smart and safe technology users.

Previously, Marian held a number of consumer product management positions at Symantec. She, her husband, and their three children reside in Los Angeles, California.

Go to [www.norton.com/familyresource](http://www.norton.com/familyresource) and [us.norton.com/security-center](http://us.norton.com/security-center)

- If you want to get more training and educational materials
- If you’re a victim of an Internet crime
- If you want to get the latest information on evolving Internet threats

You can read Marian’s blog at [www.norton.com/askmarian](http://www.norton.com/askmarian). And you can ask Marian your questions by writing to her at [marian@norton.com](mailto:marian@norton.com).



# Family Online Safety Guide

By **Marian Merritt**



NO WARRANTY. This information is being delivered to you AS IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the documentation or the information contained herein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

Copyright © 2012 Symantec Corporation. All rights reserved. Symantec, the Checkmark Logo, Norton, Norton By Symantec, Norton 360, and NortonLive are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Apple, Mac, iMac, iPhone, and iPad are registered trademarks or trademarks of Apple Inc. in the United States and/or other countries. Microsoft Internet Explorer is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. The Stop. Think. Connect. logo is a trademark of The National Cyber Security Alliance. All rights reserved. Other names may be trademarks of their respective owners. Printed in the U.S.A. 12/12