THIRD UK EDITION

iParenting Media WINNER Award

Family Online Safety Guide

By **Marian Merritt**

Edited by **Caroline Cockerill**

STOP | THINK | CONNECT™

Norton™ by Symantec

Caroline Cockerill

Introduction

The Internet is a wonderful and diverse place, filled with an abundance of incredible information resources and a million opportunities to make new friends and build online communities. Yet for many parents and carers, who often have less knowledge and experience of the Net, it can be a place of trepidation. We worry about what or whom our children may encounter online, and how we can protect them with our own limited knowledge.

Our children have grown up with amazing technologies that we never could have dreamt of as youngsters. For them, the Internet is just another place to form and share opinions, to play and create things, or to 'hang out' with their friends. It's important that we balance our concerns about their safety online with empowering them to explore the Net in the knowledge that they can talk to us about anything they may run into.

My role as a Norton Online Safety Advocate is all about empowering people, parents and children alike, to make the most of the Internet, safely and securely, while having as much fun as possible. This booklet is a starting point on that exciting road, where you and your child can learn and grow together. I try to explain some of the latest popular online destinations and trends, whilst also highlighting potential areas for concern, and recommending steps to take to protect your children in these instances.

Whether your young child is just venturing online for the first time, or your teenager has developed a fascination with a social networking site, my best advice is not to be afraid and to learn with your child, using guides like this booklet to help you on the way.

Caroline Cockerill
Norton Online Safety Advocate
www.norton.com/uk/familyresource

Contents

Family Online Safety Guide

Third UK Edition

Through The Ages

The Basics

Risks

A Final Word

From the Makers of Norton Security Products

Through The Ages

Primary School Children (ages 5-7)

This is the age when some of today's children are introduced to the Internet. Parents share video chatting with relatives or show the child game sites and online videos. According to the EU Kids Online Survey[1], the average age for a UK child to first use the Internet is 8, younger than in other EU countries. More UK children go online at school as compared to the European average. So even if you're not online at home, your child may have computer labs, PCs or Mac®s in the classroom, and a full ICT curriculum. Others often get their first computer experience at home, learning from parents or older siblings.

Websites (often with online games)—such as CBeebies and Lego or Disney sites like Habbo Hotel—attract the youngest online children, aged as young as toddler years. Some sites are almost entry-level social networking sites because they may have chat and other communication features. Parents of young children should turn these features off initially. In the US, leading sites like Webkinz (a site built around the Webkinz cuddly toys) 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 the chat concept and start discussing online 'netiquette' and safety practises. Kinz Chat Plus is monitored chat and parents who feel their children 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 favourite 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 online.

[1] Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). Risks and safety on the Internet: the UK report. LSE, London: EU Kids 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 your child uses is within your view, in a public space like the kitchen, office space, or family room. Parental control software can help you by limiting the sites your child can access, even when you aren't around. The controls also limit any information you don't want your child sharing, whether it be their name, age, phone number, or any 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 children in primary schools.

KEY RECOMMENDATIONS:

- Use parental controls to limit approved websites and hours spent online.
- Set high security settings with browsers, membership, and social networking sites.
- Install and maintain Internet security software and parental controls.
- Monitor your child's computer use and sit with them when they're online.
- 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 14).

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. 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.

! **HOT TIP:** Use Norton™ Online Family to monitor the creation and use of social networking accounts. You can even see what age your child claimed 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 favourite 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 Online Family helps you monitor Web activity and prevents children from trying to delete visits from their history.

KEY RECOMMENDATIONS:

- 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 mobile phone or a social network, they may communicate with 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 behaviours (see Online Gaming and Signs of Addiction, see page 43).
- Keep computers and mobile phones visible in the home.
- Foster open communication and encourage your children to tell you if anything online makes them feel uncomfortable.
- Start having "The Talk" (see page 14).

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 children 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 Online 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 can be there for all to see, and it's probably there indefinitely. All it takes is a single Web search by a potential house mate, romantic interest, university admissions director or potential employer—five, ten, even twenty years from now— and all of the photos, opinions, and thoughts of your teen are there for all to see forever. Caution is so important!

We want to teach our children how to take risks without getting into trouble. It's for the very same reason, for example, that they take driving lessons 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 parent presentations using materials from your local police department, ChildNet or CEOP, as an example. Some of the best online safety education for teens can come from their peers, with proper training. Encourage your school to get the older children on board, coaching the younger students about managing their digital reputation, being kind online and other key lessons. You may find your children 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 children may have already "Googled" you!

KEY RECOMMENDATIONS:

- Reinforce rules of appropriate online behaviour (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 mobile phone, or even a gaming system—so talk to your teen about their activities in all those scenarios.
- 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 mobile phones in a common area in the home and not in your teen's bedroom.
- 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 children.
- 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 14).

Off to University 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 passport, personal 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 university 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**) 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 in the same household.

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

Talking "The Talk"

"What you don't know won't hurt you." You don't actually believe that when it comes to your children 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 children about what they are doing on the Internet, and explain your family rules. And then repeat the talk every year, or 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 children worldwide have already had a negative online experience (according to the Norton Online Family Report: **www.norton.com/nofreport**.) Your child may not be telling you without you asking—so it's time to ask!

While half of all parents say they are talking to their children 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." Children 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 Mum 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 children that children 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 children 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 children 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 each year?

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, year after year. 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 mobile 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 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 children 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 children in the car (for some reason, when everyone is looking at the road ahead, it seems easier for children 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 circle of friends or peer group. 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? Ask your child to tell you why these sites are cool. You can also ask about the sites that aren’t popular anymore and why.

3. Can you show me your favourite sites? 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 favoured over other sites.

4. Have you heard of ‘cyberbullying’ and have you ever experienced it in any way online? Your child may not know “cyberbullying” by name but he or she knows what it looks and feels like. 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 children. Ask about fake social networking profiles. Find out if your child has ever heard of this kind of behaviour going on. Make sure your child knows cyberbullying is incredibly common and if they haven’t seen any yet, it’s just a matter of time until they do. Make sure they know how to react when 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 ALWAYS report it to Mum/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 neighbourhood. 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 children:

- 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 children 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 children around the world. We've found that 2/3 of adults globally have already been a victim of some form of cybercrime[2]. That might be a virus, worm, Trojan Horse or other malware but it can also include online scams, hijacked social network, 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 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.

The most recent type of malware to emerge in 2010 demonstrates the possibility to cause trouble in the real world attacks on physical infrastructure. This potential is demonstrated by the "Stuxnet" worm. While details of the attack are still unfolding, it is estimated that vulnerabilities allowed attackers to steal confidential design and usage documents for industrial systems such as those used by the energy sector. The Stuxnet incident provides a real life case study of how such an organised and structured cyber attack on critical infrastructure systems can succeed and how they could be used in the future.

[2] Source: Norton Cybercrime Report, www.norton.com/cybercrimereport

These type of targeted attacks are not aimed at the everyday consumer however. 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 jeopardise your computer as well as your wallet. Typically, the problem begins when the innocent Web surfer encounters a strange pop-up advertisement. The advert 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 (**http://security.symantec.com/nbrt/npe.aspx?lcid=1033**), 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 programme onto a disk or thumbdrive. Our technicians at NortonLive are also available (for a fee) to do the work for you and remove the virus.

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. Bots have become so common, it's estimated by Symantec's Security Response Center that 11% of U.S. computers are already infected!

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 defence 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 children. 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. In turn, 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've been a victim of identity theft, you'll want to monitor your credit report to look for evidence of new accounts or loans. Contact any of the three credit reporting services: Equifax™, Experian®, and CallCredit™. If you find evidence of identity theft, you will need to report it to Action Fraud, part of the Home Office. Details are available here:, **http://www.identitytheft.org.uk/what-if.asp**. That official report will strengthen your case when you work with the other sites and companies involved. In the case of Identity Theft, you do need to take responsibility yourself for rectifying the situation, which can take a long time, so it's best to take steps to protect yourself before it happens. You may also be able to put an "alert" on your credit report. For more information on identity theft and your consumer rights, visit **www.identitytheft.org.uk**.

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, socialise, and create than ever before. Unfortunately, some children use email, instant messaging, mobile phone photos, and text messages to embarrass or bully other children. Also, children' digital messages can be edited to change the meaning, then forwarded to other children to embarrass, intimidate, or insult. Children don't report their cyberbullying experiences enough so it's hard to get good statistics on the problem. According to Beatbullying (a UK organization dedicated to fighting both online and offline bullying), 50% of children have been bullied online[3]. Most U.S. studies put the problem at about 1 in 5 children being regularly cyberbullied.

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.

! **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 mum was working on my computer last night. Maybe she saw it."

[3] 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 and copying the message into your word processing program. 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 children at school (and most targets know who is involved or have strong suspicions), you can report it to the head teacher, a teacher, a school counsellor if the school has one, or the school office staff. BeatBullying's CyberMentors.org website offers trained volunteers and a chat environment for children experiencing bullying.

Many 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.

Many schools are responding to the growing awareness of cyberbullying by creating policies and pledges to address the issue. The tragic suicide of U.S. teen Megan Meier as a result of (among other factors) cyberbullying has become a rallying cry. More recent stories linking cyberbullying and teen suicide include UK teen Tom Mullaney and US teens 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 someone you know is possibly suicidal, contact Samaritans.org for advice. 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. If a child is looking for assistance, they can contact Childline at 0800 1111. Childline also now has a safe online chat room, 'Your Locker', through which you can confidentially talk to a counceller. If you are an adult worried about a child, contact the NSPCC at 0808 800 5000.

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 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. The British Crime Survey finds a shocking 23% of women report having experienced stalking since the age of 16. 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 children 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 (reception classes in primary schools), about a quarter will raise their hands. It's a common way for children 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 prioritise 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 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 America". Reduce that phrase to each of the first letters, use the number "2" for the word "to" and you'll end up with "Iw2g2A". Then add the first and last letter of the website to it (Symantec.com's website would be: "SIw2g2Ac"). 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's 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, even social networking sites. 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.

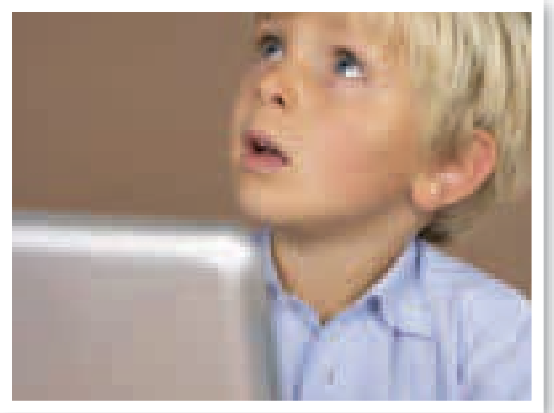
Internet Predators

Statistically, your child is unlikely to be approached online by a sexual predator, yet it remains a top parental concern. Whenever I speak to parent groups, parents want to hear my advice for keeping children away from online strangers. The U.S. National Centre 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.[4] Norton's own research from June 2010 showed that while online, one in ten UK children will experience someone they don't know asking them to meet offline.

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.

[4] http://www.ncvc.org/src/AGP.Net/Components/DocumentViewer/Download.aspxnz?DocumentID=40616

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 **http://www.ceop.police.uk/Ceop-Report/ to report it**. The site is provided by the Child Exploitation and Online Protection Centre (CEOP). Facebook has a special reporting button on each UK member's home page that also goes through to the CEOP reporting system. 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

A relatively new phenomenon, "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 mobile phone, then sent to others as a multimedia messaging service (MMS) message. Pew Research in the US reports that 4% of mobile-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.

UK research from Ofcom (April 2011) cites that 29% of children aged between 12 and 15 have heard of someone having embarrasing pictures being posted or sent to other people against their wishes.

You can imagine the powerful forces at play when a group of popular children 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 mobile phone, it cannot be pulled back. Often, young girls are being 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 counselling 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 their built-in security and safety features. For example, Microsoft Internet Explorer (the most popular browser) 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 Online 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 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 children' laptops, gaming devices and web-enabled music players at bedtime. It's helped our children 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—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 customise 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 Online Family.

Norton Online Family is an award-winning family safety service that works on both PC and Mac. 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 ”the man on the street” 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, customise 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 Online 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 Online Family is free, why not give it a try? To create an account, just go to **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 children 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 programmes, 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 children and adults, but it is tweens and teens that are driving that growth. The most popular site, Facebook, now boasts an incredible 800 million members on its site. All social networks provide a place for children 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.

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.

Social networking sites enable children to form networks of friends who can communicate freely with one another. Make sure your children 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. 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. This limits even a good friend's opportunity to post an embarrassing but funny photo, or make a remark you'd prefer Grandma not see! For great tips on using privacy settings effectively on social networking sites, visit

ConnectSafely.org's website. 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**.

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 links you suspect are spam in your news 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 most children have seen online pornography by the age of 11.[5] 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 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 behaviours such as anorexia and cutting. You may only discover this by regularly talking about their motivation for visiting these sites. 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.

[5] 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 children putting things online that later caused them scholastic, financial, or romantic harm. An American secondary 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? Well done 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.

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 child'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 new Norton Cybercrime Index, a free tool to evaluate the current risk of being a cybercrime victim, 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 "screenscrapers" 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. You may not be able to track it as easily but you should explore services, like Norton Online Family or those available from your mobile 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

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.
- Children 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.

Mobile Phone Safety

As your children graduate into juniors or secondary schools, they will ask (demand?) for a mobile or smart phone. Recent Ofcom Digital Literacy research (April 2011) found that 65% of children have their own mobile by aged 10, and over 90% of 12-15 year olds have a mobile phone. It's not at all uncommon for children 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 mobile phone, you will have to learn how to send a text message. The US 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! Ofcom research in the UK shows a slightly different picture, with teen girls (12-15) sending on average 140 texts a week. Tweens and teens have pretty much moved off of email to communicate and favour both texting and the built-in messaging of their favoured social network. The only time a child 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 favourite 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. Norton offers security products for smart phones, Norton Mobile Security, and you can find them on our **www.norton.com** website.

KEY RECOMMENDATIONS:

- Set a password on the phone/device to prevent unwanted access.
- Install security software to protect phone and data if it's lost or stolen.
- Charge the device overnight in your kitchen to minimise 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

Beyond the mobile phone, our children carry powerful computers in their pockets at all times. Consider 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 unauthorised 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 unauthorised 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 mobile phones and mobile devices to make purchases by sending authorisation 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 payment and monitor your accounts with care. Also, do be aware that if you are handing down your mobile device with this type of functionality to your child, they may end up using your account without your authorisation.

Blogging

A blog is an online journal or diary. You can read mine at **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 children 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 children have mobile 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 mobile 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 mobile 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 favourite 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 favourite 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 unauthorised 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 realising 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 paycheques to your bank is a great security measure, preventing someone from stealing your cheque from your postbox, and it speeds up your access to the funds. It's also a cost saver for your employer. Online tax filing is available from the HM Revenue & Customs website.

The latest trend from banks is mobile banking. There are numerous apps for Apple and Android devices from the major financial institutions, making depositing a cheque as easy as taking and sending a mobile phone photo. Naturally, the early adopters of such technology are the younger members of the population but with practise, 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 Many banks now offer card readers for use when transacting online. To stay safe online when carrying out internet banking it is best practice to use the card reader, and if you haven't received one already you should contact your bank.

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, 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.

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 behaviour online serves as a role model for your children by engaging in safe Internet practises yourself. Thank you!

Top Tips for Protecting Your Family Online

- Use Internet security software on all computers
- Don't open suspicious emails or click unknown links
- Keep the computer and mobile phones visible whenever possible
- 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 rules for using the Internet
- Understand social networking—join and use privacy and security settings
- Help your children keep their personal information protected
- Create complex and unique passwords and keep them private
- Use parental control software and frequently check your online 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

Resources

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

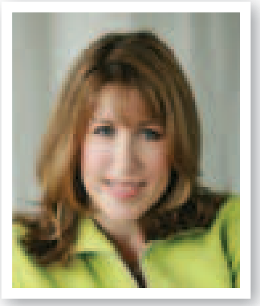
Here are some suggestions of groups to contact. It's also good to ask around among your friends and neighbours to see what your local community may have to offer.

- Local police station's e-crime officer – if they don't have an officer locally, they should have one regionally.
- CEOP – The Child Exploitation and Online Protection Centre **http://www.ceop.police.uk/**
- ChildNet **http://www.childnet-int.org/**
- BeatBullying **http://www.beatbullying.org/** This organisation also runs Cybermentors, where children help children online with all sorts of issues
- Children's Charities Coalition on Internet Safety (CHIS) **http://www.chis.org.uk/**
- Childline - **http://www.childline.org.uk/pages/home.aspx**
- NSPCC - **http://www.nspcc.org.uk/**

Other Important Internet Safety Resources to Know

- **www.norton.com/familyresource**
  (articles, newsletters, blogs, videos)

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**:
- 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**. And you can ask Marian your questions by writing to her at **marian@norton.com**.

From the Makers of

Norton Security Products

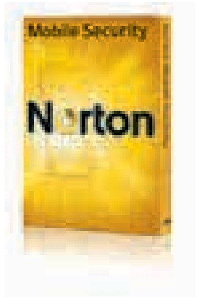
Norton 360™

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, socialise, 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



Your life is stored on your phone. Keep both safe with Norton Mobile Security. Its triple theft protection lets you remotely disable your phone, erase your personal information, and even get GPS coordinates of your phone if its lost or stolen. Downloads and installs on your phone with just a few clicks.

Norton™ Online Family

A smarter way to keep your children safe online. Norton Online 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.

Family Online Safety Guide

By **Marian Merritt**

Edited by **Caroline Cockerill**

Norton
by Symantec

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.