Family Online Safety Guide

By Marian Merritt

Foreword by Lauren Nelson
Miss America 2007

Norton™
from symantec

Foreword from Lauren Nelson, Miss America 2007

One of my goals, as Miss America 2007, is to heighten awareness around protecting our children on the Internet. The topic of Internet safety became important to me at age 13 when some friends and I were approached in an online chat room by someone we later discovered was an online predator. We made the mistake of giving out our personal information, including names, our locations and ages. A week later, we received inappropriate photographs in the mail. We immediately told our parents and were lucky the situation was defused without incident. We learned a valuable lesson about how to protect ourselves online.

It is my hope that children will learn these lessons before they find themselves in a dangerous situation, like my friends and I did. The Internet is a great tool for getting news, conducting research and communicating with others,but it also has an unsavory side—spammers, scammers, and online predators. By teaching kids early and often about the dangers of the Internet and how to avoid them, we can help make the Internet a safer place for our children.

The Miss America Organization has partnered with Symantec for the purpose of raising awareness on the dangers of the Internet and educating parents on how to keep their children safe online. We wanted a partner that was the leader in security technology and had a large enough voice and the trust of millions of consumers to further promote my personal platform of keeping kids safe on the Internet.

Symantec shines as a company, and has shown its commitment to the youth of America through numerous "Digital Family" and child safety initiatives. As I travel the country this year, I have the opportunity to share my message along with their philosophy to educate and raise awareness about this serious subject.

My goal is to help parents provide guidance to their children who are using the Internet. We also want to make sure kids have a safe online environment where they can explore, have fun and grow up to be good "cybercitizens." By working with Symantec, we can help make the Internet a better place for children to communicate, socialize and connect.

Lauren Nelson

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 email and instant messaging—I realize 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. We'll go through the top Internet concerns in this guide but if you are interested to dive more deeply, I'll recommend Web sites 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

Contents

Contents *(continued)*

Through the Ages

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 or Macs in the classroom, a child's first use of a computer may be at school. Others often get their first computer experience at home, learning from parents or older siblings. According to the U.S. Senate resolution naming June as Internet Safety Month, 35 million U.S. children from kindergarten through grade 12 have Internet access, and 80 percent are online at least 1 hour per week.

Young children are often completely engaged by simple games and educational sites, but they will quickly learn about new sites from their peers. Web sites—such as Neopets, Webkinz, and Club Penguin—start by ages 7 or 8. We refer to these as entry-level social networking sites because many have chat and other communication features. Parents of young children should turn these features off initially. It's difficult for children of this age to understand the "stranger danger" associated with someone contacting them through 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 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. 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 Google's "SafeSearch" feature, found under "Preferences") 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.

Key recommendations:

- *Limit approved Web sites and hours spent online*
- *Set high security settings with browsers, membership, and social networking sites*
- *Install and maintain Internet security software and parental controls*
- *Use parental controls to limit the Web sites your child can visit*
- *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*

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 might 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, such as MySpace, Facebook, and Friendster that are popular with older teens and adults. Most won't create a page until they are a little older, but they will visit, join, and chat with friends, older siblings, and other relatives who have their own pages and profiles.

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 Web site and checking out different sites to get the latest gossip along with downloadable photos. Online video sites, such as YouTube! are enormously popular. Many of the videos contain strong language or violent material, so you need to monitor your tween's visits carefully. 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.

Key recommendations:

- *Frequently check your computer's Internet history to see the sites your children have visited, and monitor their email and instant messaging accounts to see who they communicate with*
- *Set rules about online communication, illegal downloading, and cyber bullying*
- *They should know to never 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.)*
- *Keep computers in a common area in the house*
- *Foster open communication and encourage your kids to tell you if anything online makes them feel uncomfortable*

Teens (ages 13-17)

Teens are developing ever greater independence and this is reflected in their online lives. With that independence comes responsibilities, including being careful in their online world. Yes, at these ages, teens have usually formed or joined online worlds such as MySpace, Friendster, Facebook and others. 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 Google™ search by a college 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!

Key recommendations:

- *Reinforce rules of appropriate online behaviors (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*
- *Ask them not to download files (music, games, screen-savers, ringtones) or make financial transactions without your permission*
- *Teach them to never share passwords and be wary about typing private information when on a shared or public computer, or one they think might not be secure*
- *Teach them to never click a link in an email or IM—this is a common way people get viruses or reveal private and valuable information to criminals*
- *Keep computers in a common area in the house 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 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.*

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 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 security.

Follow the Rules

Parents

- **Keep Current** with technology. You don't have to be an expert, but a little understanding goes a long way towards keeping your family safer online. Get basic technical training and learn about new products as they get released. Visit www.norton.com/familyresource to stay up-to-date.
- **Keep Communicating** with your children about everything they experience on the Internet. Learn their lingo, and ask them when you don't understand something. Work to keep your communication lines open.
- **Keep Checking** your children's Internet activity. Know where they go online. Let them know that you'll keep checking because you love them, and you want them to understand that the Internet is a public forum and never truly private.

Kids *(courtesy of iKeepSafe.org)*

- **Keep Safe:** Keep your personal information safe—all of it! Never give your real name, address, phone number, the name of your school, or a picture of yourself to anyone online.

- **Keep Away:** Internet strangers are dangerous—STAY AWAY. No matter what anyone tells you, NEVER meet anyone in person. You have no way of knowing who they really are. Don't talk with them online, and never tell them where you live.
- **Keep Telling:** Tell your parents or a trusted adult about everything you see on the Internet. Always tell them when something makes you feel uncomfortable. Remember, not everything you see and hear on the Internet is "true" or even "normal."

The Basics

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 some safety features. For example, Google's SafeSearch, found in "Preferences" on the main Google landing page, allows you to restrict explicit (sexual) sites and content from appearing in your family's search results. Of course, any knowledgeable user can easily remove the setting, but it's helpful with younger Web surfers.

Protect Your Password

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, then customize that password for different Web

sites. 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 "mifflin8". Then add the first and last letter of the Web site to it (Amazon.com example: "Amifflin8n"). It 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.

Passwords are multiplying like rabbits! Each one is more complicated than the next. It's hard for anyone to stay on top of them and retrieve them when needed. So how do you manage them? 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 on a computer, on paper notes next to the computer, and so forth. 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.

Secure Your Wireless Network

Home wireless networks 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 defeats your efforts to monitor their activities.

If you have wireless (or "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. 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 your child is able to go 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 provide a "white list" of pre-selected and parent-approved Web sites 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 time limits so your children don't spend hours on the Web instead of doing homework or chores.

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.

Remember, though, that no software provides perfect protection. 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.

Online Faves

Social networking sites like MySpace, Friendster, Facebook, and Xanga are extremely popular with teens. YouTube is popular but a parental concern because there isn't any filtering for language or adult content. Check with the computer lab administrator at your child's school to see which ones are used most. Ask your teens if they have accounts (but always try to check for yourself too).

Younger children visit and join hobby sites such as Stardoll, Webkinz, and Club Penguin. These sites provide games and activities including chat. They are in many ways like "social networking lite." Educational sites such as Starfall.com and funbrain.com help teach reading and math skills. Whether your kids are teens, tweens, or younger, ask them about which sites are popular with them and their friends. Ask them which ones they've joined and have them show you around. You'll quickly know whether you approve or not. Keep the conversation "impersonal" so they don't feel they are being interrogated.

Risks

Internet Predators

While statistically, your child is unlikely to be approached online by a sexual predator, there are enough high-profile cases with tragic outcomes that any parent worries about this. The National Center for Missing and Exploited Children

has conducted studies showing that 1 in 7 children will be solicited sexually online, but some of those contacts are from peers, rather than strangers. 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 and report it to their Cybertipline. It's not acceptable to talk about sex with a stranger and any child who has a stranger ask about sexual matters should notify a parent or trusted adult immediately.

Plagiarism and Cheating

It's very easy to find homework guides to all the popular school textbooks online and many Web sites 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. Also, explain to your child why user-generated content such as that found at Wikipedia isn't always as reliable as more traditional sources of information such as encyclopedias but can serve as a great starting place for new research.

Cyber Bullying and Cyber Stalking

Technology gives our children more ways to connect, socialize, and communicate than ever before. Unfortunately, some kids use email, instant messaging, and cell phone photos 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. According to the National Crime Prevention Center (February 2007), 43 percent of children have been a victim of cyber bullying! Make sure your children know they must guard even the most casual text message and watch their own written words. They should never be cyber bullies, and they should always tell you if and when they are being cyber bullied. 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.

Cyber stalking is a dangerous extension of cyber bullying 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. 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. Cyber stalking is dangerous and should be reported to law enforcement, Internet service providers, and Web site hosts. Keep all evidence of both cyber stalking and cyber bullying.

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 let strangers have access to your computer. Using file-sharing sites may

expose your computer and information to "bot" software, spyware, keystroke loggers, viruses, and other dangerous malicious code. 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.

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, name, telephone numbers, address, 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. They, in turn, 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. 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 can also put a "freeze" on your credit report and for your children. Visit ftc.gov for more information.

Social Networking Sites

Social networking Web sites are among the fastest growing phenomena on the Internet for both kids and adults, but it is tweens and teens who are driving that growth. Among the most popular social networking sites are MySpace, Friendster, Xanga, and Facebook. All of them provide a place for kids to get together online with new and existing friends. When used cautiously, these sites offer great ways for kids to communicate and share their experiences. When used carelessly, however, they can expose your children to identity theft and predators.

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.

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. Once strangers are in the network, others in the network will assume a level of trust with them, based upon their relationship with your child. If the stranger is a predator, they may try to take advantage of your child or the friends within the network.

Make sure that your child sets the communication features properly so they can approve any postings 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!

Porn, Gambling, Racism, Anorexia, and Hate sites

The darkest corners of the Internet world include some dangerous and illegal elements. 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.

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. 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.

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.

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

Email and Instant Messaging

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. The same is true for instant messaging. If a child messages or chats with more than one group, they should maintain different screen names, because predators often follow children from one chat room to another.

Make sure your children's email accounts have the highest level of spam filtering turned on. According to a Symantec research study, 80 percent of children report receiving inappropriate spam on a daily basis. They should use email account names that can't lead strangers to them.

For example, 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, even with friends. 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.

Key Recommendations:

- *Teach children not to click on links within emails that they receive, since links can lead to fake Web sites.*
- *Disable the preview function in email. This prevents potential malicious code in the message area from executing.*
- *Kids should not respond to emails or instant messages from anyone they don't know or didn't expect to receive*
- *Never accept a link or download a file through IM.*
- *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 like Yahoo!® (and others) 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.*

Blogging

A blog is an online journal or diary. Some 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 Web site 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 Web sites 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. Don't let your teen become a blog victim.

Viruses, Worms, and Spyware

Computer viruses have been around for more than nearly 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. But today, the stakes are much higher and many of the bad guys are international cybercriminals, motivated by financial gain through their illegal activities.

Spreading via email, instant messaging, infected social networking pages, and file-sharing sites, 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. Bots (short for robots) are forms of stealth software that can sneak into your computer and cause your PC 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 percent of U.S. computers are already infected!

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!

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 becoming some of the latest threats to emerge from the dark side of technology. 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 percent of U.S. computers are already infected!

Many illegal businesses now thrive on these 'bots' that can spread like wildfire among 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 cyber-criminals, 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 wreak havoc on your credit including the unauthorized use of your credit cards and bank accounts. The bots can also display phony Web sites, 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 (Norton™ AntiBot is a good choice) and be sure to set-up 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 emails unless you can verify the source, which is something you need to teach your kids.

Digital Photos

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, such as Flickr, make sure you don't allow others to use your photos, especially photos of people.

Key Recommendations:

- *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 Web site 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 web site 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 Bill Paying

Stay on top of all banking activity as you do with credit cards. Regularly access your teen's 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.

Online Banking

If you or your child engage in online banking, never do so on a public or shared computer or on a wireless network lacking security features such as a firewall. You might risk a hacker capturing your account and login information and stealing your money. Always type the Web address of your bank into the Web browser, never click a link from an email.

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." Titles such as World of Warcraft, Lord of the Rings, and Everquest are currently popular. 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 on eBay 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 behavior online serves as a role model for your children by engaging in safe Internet practices yourself. Thank you!

Top Tips for Protecting Your Family Online

- Keep the computer in a common room
- Establish rules for using the Internet
- Understand social networking
- Help your children keep their personal information protected
- Protect your children's passwords
- Frequently check your online computer's Internet history
- Spend time with your children online
- Teach your children cyber ethics
- Be computer savvy
- Teach your children to tell a parent, teacher, or trusted adult if they feel uncomfortable about anything they've seen on a computer

Important Resource Sites

www.norton.com/familyresource
www.ftc.gov
www.annualcreditreport.com
www.staysafeonline.org
www.ikeepsafe.org
www.webwisekids.org

Marian Merritt

Marian is the Internet Safety Advocate for Symantec Corporation, makers of Norton Software. 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.

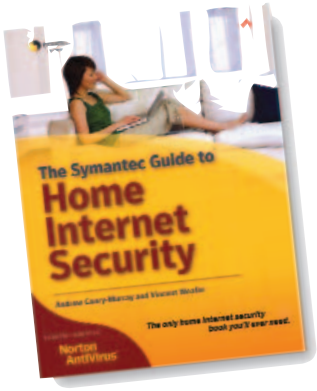
Go to www.norton.com/familyresoure:

- 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
- If you want to subscribe to our family online safety newsletter
- If you want to read Marian's blog

Or you can ask Marian a question by writing to her: marian@norton.com

From the makers of Norton™ security products.

"Own Your Space" BY LINDA MCCARTHY, is the first serious security book to address Internet security from a teenager's point of view. This book covers online threats, MySpace security issues, identity theft, and more, focusing on how these issues impact teens and how you can stay safe online.



"The Symantec Guide to Home Internet Security" BY ANDREW CONRY-MURRAY AND VINCENT WEAFER. The Internet is crawling with risks; if you bank or shop online, or even just surf the Web and send e-mail, you are exposed to hackers, thieves, and con artists. Today's bad guys don't need to pick your locks or break your windows: they can attack you and your family over the Internet. Are you prepared? Enjoy a safer online experience with easy, step-by-step help from Symantec, the world's most trusted security provider.

Norton™
from symantec

13522845