Family Online Safety Guide

A practical guide to help you keep your family safe online

By Caroline Cockerill
Foreword by Kidscape

Norton™ from symantec

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 Internet 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

Foreword

'I heard my 12 year old daughter sobbing in her room and went in to find out what was the matter. She showed me the emails she had received from some girls in her class and then told me that they had also set up a hate website about her. I have to tell you that I was shocked. I had no idea that kids were using the internet to torment other kids.' This father rang our Kidscape helpline, himself in tears. He said he knew about the possibility of paedophiles grooming children online and had warned his children about that, but this aspect of the internet was new to him.

It would be to most parents. Our children and young people are expert at using the internet. While we use it for booking holidays and answering emails, they are setting up social networking pages, instant messaging with webcams, blogging, researching school projects, listening to music, playing online games, and emailing friends. Most use the internet safely and responsibly. Unfortunately, however, there is much about the internet that can facilitate dangerous behaviour by children, who have found it a powerful tool for bullying, and by adults, who make use of the anonymity and secrecy of the online world to approach young people.

The challenge for us, as parents, is to ensure that we see the positive aspects of the internet while thinking about:

- how to protect our children from predators online?
- what dangers lurk in social networking sites?
- how can we prevent cyberbullying?
- how can we talk to our children about these things when we don't understand them ourselves?

This booklet is a great way to find out what is going on – it certainly helped bring me right up-to-date. In clear, simple language it explains all those things our children already know or need to know and includes advice about how to protect your family while using the internet to the full.

Have a look at the range of products that Symantec provides for securing your computer and check out the Childnet website **www.childnet.com** , as well as our own Kidscape site **www.kidscape.org.uk** for more tips on keeping children and young people safe.

Michele Elliott
Chief Executive
www.kidscape.org.uk

Contents

Through the Ages

Early Primary School Children (ages 5-7)
This is the age when many children are introduced to the Internet. Now that more and more UK 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 Norton Online Living Report, research commissioned by Symantec and Harris Interactive in February 2008, UK children are becoming increasingly more confident online with 44 per cent constantly or frequently visiting social networking sites, 65 per cent at least sometimes downloading music and a massive 87 per cent at least sometimes sending emails. 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 and Club Penguin - can be entered at ages seven or eight and 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 favourite game or club site. Later you can introduce the concept of chatting with people they know, such as family and 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 and set up in a family room. It's a good idea to set the home page of your Internet browser to a child-friendly home page for younger children and consider bookmarking a range of sites which you are happy for them to review. Show them how to access these from a Favourites folder which you can set up with their name.[1] 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 okay 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, wherever possible
- 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 adventurous 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 (IM) 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, Piczo and Bebo 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.

[1] For both these services click on Tools button at the top of the Browser

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 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. Some 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. Let your child know that you are doing this to ensure that trust is not broken
- 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 behaviours (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. At this age teens have usually formed or joined online worlds such as MySpace, Facebook, Bebo 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. Web sites are also frequently used for the research and submission of home work for school. Digital

traces of their thoughts and activities 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 University or 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 behaviours (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
- Ask them not to download files (music, games, screensavers, 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 still need your support, involvement and care
- 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, 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 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 encrypt their wireless connection and 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
Remember these top tips for staying safe online from Childnet

- Take an active interest in what your children are doing online
- Remember children are accessing the Internet at school, friends' homes, libraries, Internet cafés, etc
- Encourage your children to speak to you if they see anything that upsets them online
- Remind your children never to give out personal information
- Children should never meet up with anyone they've met online without a trusted adult being present
- Encourage your children to be responsible Internet users
- Stick to the fun and positive sides of the Internet
- Don't think you have to deal with this all on your own, check out these sites:

www.childnet.com
www.symantec.co.uk
www.parentcentre.gov.uk
www.ceop.gov.uk
www.iwf.org.uk
www.kidscape.org.uk

Children and Young People
Follow Childnet's **SMART** Rules

Safe. Keep safe by being careful not to give out personal information - such as your name, email, phone number, home address, or school name - to people who you don't know or trust online.

Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents' or carers' permission and even then only when they can be present.

Accepting emails, IM messages, or opening files, pictures or texts from people you don't know or trust can lead to problems - they may contain viruses or nasty messages.

Reliable. Someone online may be lying about who they are, and information you find on the Internet may not be reliable.

Tell your parent, carer or a trusted adult if someone or something makes you feel uncomfortable or worried. You can report online abuse to the police at **www.thinkuknow.co.uk.**

Safe Browsing
Make sure your browser is set to offer you its 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 such as your birthday 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 customise 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. A note for parents - 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 are simple steps to follow 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 customise 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 that 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 potentially harmful materials.

Remember, though, that no software provides perfect protection. Parents need to use a combination of tools and rules to protect children, regardless of their age. The Internet 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, Facebook and Bebo 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 and Barbie. These sites provide games and activities including chat. They are in many ways like "social networking lite."

Educational sites such as Topmarks.co.uk and the BBC's www.bbc.co.uk/onionstreet help teach reading and maths 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, it is rare that your child would be approached by a sexual predator online, there are enough high-profile cases with tragic outcomes that would make any parent worry about this. Make sure your children know they must never email, chat, or text message with strangers. It's never okay to meet a stranger offline or online. Make sure they understand that someone they see or meet online is still a STRANGER, no matter how often they see them online. Children who discuss sex with strangers online have been shown to be more likely to arrange offline meetings. It's very important that you tell your children that it is never acceptable to talk about sex with a stranger online and that they should notify you or a trusted adult immediately or report this if it happens. You can report suspicious activity towards your children on the Internet to the Child Exploitation and Online Protection Centre (CEOP) **www.ceop.gov.uk** which has a special young person's reporting service called 'Think you Know' - see **www.thinkuknow.co.uk.**

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 but not for copying. Encourage your children to always check the source of information they read on the Internet and explain why user-generated content, such as that found at Wikipedia, can serve as a great starting place for new research but isn't

always reliable. It's good to check information found online against more traditional sources of information such as encyclopaedias.

Cyber Bullying and Cyber Stalking
Technology gives our children more ways to connect, socialise, and communicate than ever before. Unfortunately, some kids use email, IM, and mobile 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 research carried out for the Anti-Bullying Alliance in the UK 22 per cent of young people reported being the target 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 retaliate back to the bully, 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 computer keyboard and copying the message into your word processing program. It's important to help your child know where and how to report if they are the victim of cyber bullying and there is specific advice for schools which Childnet has produced and is available at **www.childnet.com/digizen.**

Cyber stalking is a dangerous extension of cyber bullying and used by those who engage in stalking in the real or "offline" world. 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 the police, Internet service providers, and Web site hosts. Keep all evidence of both cyber stalking and cyber bullying.

File Sharing, Music and Video Download
Children quickly learn about the joys of sharing music with each other. And it's often at the tween stage that they discover file-sharing sites, which enable them to swap music or videos online. Explain to your children 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.

Private Information and Identity Theft

Many children will not automatically know what "private" information is and the importance of keeping this private both online and offline so you need to explain the concept that it's any data that individually identifies them and may allow 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. Fraudsters 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 surprisingly easy for people with such intentions 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 request a report from any of the credit reporting services for a small administrative fee (the UK Data Protection Act credit reporting services are allowed to charge £2 for each request an individual makes for his or her statutory credit report): Equifax, Experian, and Callcredit all follow this. 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 **http://www.ico.gov.uk** for more information.

Social Networking Sites

Social Networking Sites are among the fastest growing phenomena on the Internet for children, young people and adults, but it is tweens and teens who are driving that growth. Among the most popular social networking sites are MySpace, Facebook and Bebo. All of them

provide a place for kids to get together online with new and existing friends. When used sensibly, 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 to set their profiles to private so that only invited friends can view their information. They should not post private information or inappropriate or misleading photographs. This information, once posted, can become public and can be stored on the computers 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 other people.

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. 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 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 and they would prefer not to be seen.

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 behaviours such as anorexia and self harm. 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 child's school's Web site is password protected or requires a login for more than superficial, public information. For example, schools nowadays might use a Web site to communicate itineraries and lists of names to sports teams or other travelling groups. It is obviously imperative that this information is not in the public domain.

Email and Instant Messaging

Make sure your children's email accounts have the highest level of spam filtering turned on. According to a Symantec research study, 80 per cent 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 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 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 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 software that can sneak into your computer and cause your PC to send out spam and phishing emails to others, without you even knowing.

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
A "bot" is a type of malicious software, put 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 unauthorised 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 defence against these bots is to install top-rated security software and be sure to set-up your software's settings to update automatically so you know

you're getting the latest protection.

Digital Photos
Many kids 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, 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 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 padlock 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 favourite shop or sale. You

should type the shop's 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. Credit card companies offer consumer protection and will work with you to manage any disputed or unauthorised charges.

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 addiction. 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 or within the game) and any other concerns you might have. Signs of addiction to online gaming can be the same as with real-world gamblers, such as craving, withdrawal symptoms, loss of control and neglect of other activities.

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 cyber world 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 practices yourself.

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 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/uk/familyresource
www.symantec.com/uk
www.childnet.com/kia
www.childnet.com/digizen
www.ico.gov.uk/
www.parentcentre.gov.uk
www.ceop.gov.uk
www.iwf.org.uk
www.kidscape.org.uk

Go to **www.childnet.com**
If you want to get the latest information on evolving Internet threats
If you want to subscribe to our Family Online Safety Newsletter
Go to **www.symantec.co.uk**