**Internet Security for Children**

The Internet offers many positive educational and social benefits to young people, but unfortunately there are risks, too. As in any other area of life, children and young people are vulnerable and may expose themselves to danger, knowingly or unknowingly, when using the internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal.

#### Talking To Your Children

The first thing to do is talk to your children about the [Dangers They Can Face Online](http://www.safekids.co.uk/childreninternetrisks.html). Tell them not to talk to strangers, and certainly never reveal details about themselves. Help them choose a screen name that's neutral and anonymous. Encourage them to talk to you about their times online, especially about any problems.

#### Inappropriate Material

One of the key risks of using the internet, email or chatrooms is that young people may be exposed to inappropriate material. This may be material that is pornographic, hateful or violent in nature; that encourages activities that are dangerous or illegal; or that is just age-inappropriate or biased. One of the key benefits of the web is that it is open to all, but unfortunately this also means that those with extreme political, racist or sexual views, for example, are able to spread their distorted version of the world.

In the case of pornography and child abuse images, there is no doubt that the internet plays host to a large amount of legal and illegal material.

#### Physical Danger

The threat of physical danger is perhaps the most worrying and extreme risk associated with the use of the internet and other technologies, and is probably the risk most reported by the media.

A criminal minority make use of the internet and chatrooms to make contact with young people with the intention of developing relationships which they can progress to sexual activity. Paedophiles will often target a child, posing as a young person with similar interests and hobbies in order to establish an online 'friendship'. These relationships may develop to a point where the paedophile has gained the trust in order to meet in person. These techniques are often known as 'online enticement', 'grooming' or 'child procurement'.

#### Bullying

[Cyber Bullying](http://www.safekids.co.uk/cyber-bullying-facts-how-prevent-it.html) – whether by internet, mobile phone or any other method – is another aspect of the use of new technologies that provide an anonymous method by which bullies can torment their victims. While a young person may or may not be in physical danger, they may receive email, chat or text messages that make them feel embarrassed, upset, depressed or afraid. This can damage their self-esteem and pose a threat to their psychological wellbeing.

#### Illegal Behaviour

Some young people may get involved in inappropriate, antisocial or illegal behaviour while using digital technologies. Just as in the real world, groups or cliques can form online, and activities that start out as harmless fun, such as voicing an opposing opinion to another member of a chatroom, can quickly escalate to something much more serious.

#### Illegal Activity

Some children and young people may become involved in other equally serious activities. Possible risks include involvement in identity theft or participation in hate or cult websites, or in the buying and selling of stolen goods. The ease of access to online gambling, suicide sites, sites selling weapons, hacking sites, and sites providing recipes for making drugs or bombs are also of great concern. There is some evidence to suggest that young people have become involved in the viewing, possession, making and distribution of indecent and/or child abuse/pornographic images.

#### Divulging Personal Information

Most parents do not allow their children to give out personal information online and around 50% of children acknowledge this. Just under half of 9-19 year old children who go online once a week say that they have given out personal information, such as their full name, age, address, email address, phone number, hobbies, name of their school etc., to someone they met on the internet.

#### Popular Search Engines for Children

A variety of children’s search engines exist on the Web today, each with its own unique way of filtering out questionable content. Ask Kids (www.askkids.com) is a sister site of the adult search engine Ask Jeeves and allows children to ask fully phrased questions such as “How high is the Empire State Building?” just as they would when asking a teacher or tutor.

Yahooligans (www.yahooligans.com) is a sister site to Yahoo and is the web’s oldest directory for children, having gone live back in 1996. This search engine specifies that its target audience is children aged between 7 and 12 years and will only display results hand picked from its own fully vetted listings. KidsClick! (www.kidsclick.org) was designed as a mega-directory of about 5,000 sites selected by librarians as useful to and appropriate for a younger audience.

Other search engines that cater to a child audience include Cybersleuth Kids (www.cybersleuth-kids.com) and FactMonster (www.factmonster.com).

**Windows:**

• Windows Vista: [Any version](http://www.cnet.com/windows-vista.html)
• Internet connection

**Step 1: Create a user account for your child**
Parental controls are computer settings that are applied to a user account. As such, you should have a password-protected user account on your Vista computer, but your child should have his or her own account. This way, you can apply the controls to his or her account without placing restrictions on your account. The good news is you can create a user account for your child quickly and easily.

**Open User Accounts**
Click Start | Control Panel. In Control Panel, click the Add or Remove User Accounts link under the User Accounts and Family Safety section.

The User Accounts interface opens. You'll see the account you created when you installed Windows and a Guest account, which is probably turned off. Notice the Create a New Account link. Click this link to create the new account for your child.

**Create the new user account**
In the window that appears, you can create the new user account for your child. First, give the account a name. Since your child will be logging onto the computer using this account, just name the account your child's name (or a nickname, if you prefer). By default, the Standard user button is selected. This setting is a restricted setting that allows the user to access software and even change system settings that do not affect the security of the computer. On the other hand, you have an Administrator option which essentially gives the user the ability to change settings that affect every user and the computer's security. You should never give your child Administrator privileges, so keep the Standard user button selected. Click the Create Account button.

You now see the new account appear in the User Accounts window. Click your child's new account. You now see the option to make changes to the user account, such as creating a password, changing the picture, and such. For younger children, you may wish to skip creating a password; that way, they can simply click their user names when they start Windows. Older children may want passwords to ensure some sense of privacy.

When you have your child's user account created, you can set up parental controls for that child. Click Start | Control Panel. Under the User Accounts and Family Safety option, click Set Up Parental Controls for any user. In the window that appears, click your child's user account to set up the controls. This opens the parental controls window for that user.

To begin the process, first turn on parental controls by clicking the On radio button. You can now configure some different Windows settings that will control what your child can and can't do, as you can see in the Windows Settings area of the screen.

**Configure the Windows Web filter**
The first control area you can configure is the Windows Vista Web filter. This control enables you to place restrictions on Internet usage. Click the Windows Vista Web Filter option to open the Web filter window.

Here's how you configure the Web filter:

• The first two buttons allow you to block some Web content or not. If you choose the "allow" option, the Internet is an open book for your child. So, keep the default setting to block some Web sites or content selected.

• In the next section, you can choose to allow or block specific Web sites or allow only the Web sites that are on the allow list. Edit the Allow or block list, enter the sites, and then click the "Only allow Web sites which are on the allow list" check box. Now, the Internet is completely locked down to only these sites, preventing your child from stumbling onto another Web page. Depending on your child's age, you may want to take this highly controlled approach.

• In the Block Web Content Automatically section, you can choose a restriction level for your child. The High or Medium setting is typically best, depending on your child's age. You can click each radio button here and read a summary of what is blocked. You might also want to click the "How does the Web filter work" link to read a summary. Note that if you choose to allow only Web sites that are on the Allow list, this entire section is unavailable to you because site access is completely controlled by the Allow list.

• The last setting you can enable is the Block File Downloads option. This feature stops the ability to download any files from the Internet. For younger children, this is a good setting to enable because it prevents the possible download of information you may not want to them to have.

**Control time limits**
The next setting you can configure in the parental controls window is time limits. If you click the option, you see a calendar where you can control when your child is allowed to use the computer. You can use this feature to restrict your child from using the Internet during times when you are not home to supervise, or in the middle of the night for an older child or teen. Simply click and drag to turn the desired hours and days blue in order to block these times. White areas mean the time and day is available, while blue areas are blocked. If you make a mistake or decide to change the time limits later, just click the blue areas to turn them white again.

**Allow or block specific programs**
The final setting you can enable in parental controls is to allow or block specific programs installed on your computer. Maybe you have programs installed that you do not want your children to use for various reasons. Click the option in parental controls, and then choose the radio button that appears allows your child to only access the programs you have selected. Click OK.

You'll then see a listing of all programs installed on your computer. You need to click the check boxes of the programs that you want your child to be able to use. All programs not checked are automatically blocked, as you can see in the following illustration. Make your selections, then click OK.

**Step 3: View your child's activity report**
If you open parental controls for your child's user account, you'll see an option to view your child's activity report. This feature is very helpful because you can simply review on a periodic basis what your child is doing on the computer, rather than having to constantly look over your child's shoulder. This report feature enables you to see what your child has done on the Internet, what system changes have been made; applications that have been used; games they've played; e-mail that has been received and sent, as well as contacts changes; instant messaging activities; media viewed; and even general system changes. Simply click the report option, then use the categories on the left side of the window to see your child's activity.

**Kid-friendly security software**

Before you get started with this project, we recommend that you have the following:

* An Outlook Express spam filter such as [OnlyMyEmail](http://dw.com.com/redir?oid=4520-11344_7-6424378-2&ontid=11344&siteid=7&edid=3&lop=txt&destcat=ex&destUrl=http://www.onlymyemail.com), a Web client with spam protection such as [Thunderbird](http://download.cnet.com/Mozilla-Thunderbird/3000-2367_4-10418663.html), or a Web e-mail client with spam blocking, such as Hotmail or Yahoo Mail.
* A child-friendly Web browser, such as [Crayon Crawler](http://dw.com.com/redir?oid=4520-11344_7-6424378-2&ontid=11344&siteid=7&edid=3&lop=txt&destcat=ex&destUrl=http://www.crayoncrawler.com), [KidRocket KidSafe](http://dw.com.com/redir?oid=4520-11344_7-6424378-2&ontid=11344&siteid=7&edid=3&lop=txt&destcat=ex&destUrl=http://www.kidrocket.org), or [Noah's Web](http://dw.com.com/redir?oid=4520-11344_7-6424378-2&ontid=11344&siteid=7&edid=3&lop=txt&destcat=ex&destUrl=http://www.noahsweb.com).
* A child-protection Net package such as [CyberPatrol](http://download.cnet.com/3000-2162_4-10439639.html) or [Net Nanny](http://dw.com.com/redir?oid=4520-11344_7-6424378-2&ontid=11344&siteid=7&edid=3&lop=txt&destcat=ex&destUrl=http://www.netnanny.com).

## Block explicit sites in your browser



### Internet Explorer's filtering utility is dependent on sites rating themselves.



### Crayon Crawler is a kid-friendly browser that automatically blocks objectionable sites.

Children can easily find explicit material on the Web--and if they don't, it often finds them. If your daughter happens to type "www.girl.com" instead of "www.gURL.com," the popular site for teenage girls, she'll end up at a porn site. And until it was shut down recently, the porn site www.whitehouse.com displayed inappropriate images to young students who probably meant to type "www.whitehouse.gov."

Sites like these, which count on erroneously entered URLs, are shut down quickly, but as soon as they are, more crop up to replace them. And the most popular Web browsers offer little in the way of blocking tools.

Mozilla Firefox offers no content filtering. Microsoft Internet Explorer 6 has some tools, but they're weak. Blocking in IE is based on a self-rating system devised by the Recreational Software Advisory Council (now the Internet Content Rating Association). The downside: Most Internet sites haven't rated themselves, and if you set Internet Explorer to block all unrated sites, you'll lose access to some useful sites, including Amazon.com, Google, and even Computer Shopper.

To turn on the basic content-filtering utility in IE, follow these steps.

1. Go to Tools > Internet Options > Content, and in the Content Advisor box, select Enable.
2. In the new window, you'll see four categories: Language, Nudity, Sex, and Violence.
3. To enable blocking, move the slider directly below the categories to the lowest level, then click Apply.

A better alternative is to download a child-friendly content-filtering Web browser, such as [Crayon Crawler](http://dw.com.com/redir?oid=4520-11344_7-6424378-3&ontid=11344&siteid=7&edid=3&lop=txt&destcat=ex&destUrl=http://www.crayoncrawler.com), [KidRocket KidSafe](http://dw.com.com/redir?oid=4520-11344_7-6424378-3&ontid=11344&siteid=7&edid=3&lop=txt&destcat=ex&destUrl=http://www.kidrocket.org), or [Noah's Web](http://dw.com.com/redir?oid=4520-11344_7-6424378-3&ontid=11344&siteid=7&edid=3&lop=txt&destcat=ex&destUrl=http://www.noahsweb.com). Noah's Web comes with three browsers: one for children ages 4 to 12, one for teens, and one for parents.

To ensure that your child can use only the child-friendly browser you install for Net surfing, create a user account in Windows that prevents installation of new apps.

1. Go to Control Panel > User Accounts and select "Create a new account."
2. In the wizard, enter a name for the new account and select Limited.
3. Next, password-protect any other accounts that aren't Limited.

This still leaves Internet Explorer, however, because it comes with Windows and can't be uninstalled. To prevent your child from using Internet Explorer, password-protect it. Go to Tools > Internet Options, and select the Content tab. Under Content Advisor, click Enable. On the General tab, locate the Supervisor Password area. Type in a password, then hit Apply.

Tip

Mac users seeking robust content controls should check out [BumperCar 2](http://download.cnet.com/BumperCar/3000-2143_4-10383871.html) for Mac OS X systems.

**Stop objectionable spam**

Spam isn't good for anyone, but for children, it can be particularly harmful. Links in e-mail can lead to pornographic Web sites.

The solution: Install a spam filter. For e-mail clients such as Outlook or Outlook Express, [OnlyMyEmail](http://dw.com.com/redir?oid=4520-11344_7-6424378-6&ontid=11344&siteid=7&edid=3&lop=txt&destcat=ex&destUrl=http://www.onlymyemail.com) is a good add-on for blocking spam before it reaches your PC. But it's more likely your kids are using free Web-based mail systems such as Hotmail or Yahoo Mail. If the service has a built-in spam filter, set it to the highest level of protection. Just keep in mind nothing can stop your child from perusing the Junk E-mail folder in search of legitimate mail caught by the filter.

Tip

If your teenager uses Outlook Express, consider switching to Mozilla's free [Thunderbird](http://download.cnet.com/Mozilla-Thunderbird/3000-2367_4-10418663.html). It's similar to Outlook Express in appearance and function, but it includes a built-in spam filter.

**Web resources for safe surfing**

Staying aware of online threats goes a long way toward keeping your kids safe online. [GetNetWise](http://dw.com.com/redir?oid=4520-11344_7-6424378-8&ontid=11344&siteid=7&edid=3&lop=txt&destcat=ex&destUrl=http://kids.getnetwise.org), [ProtectKids.com](http://dw.com.com/redir?oid=4520-11344_7-6424378-8&ontid=11344&siteid=7&edid=3&lop=txt&destcat=ex&destUrl=http://www.protectkids.com), and [SafeKids.com](http://dw.com.com/redir?oid=4520-11344_7-6424378-8&ontid=11344&siteid=7&edid=3&lop=txt&destcat=ex&destUrl=http://www.safekids.com) offer plenty of articles, information, and resources, including links for reporting suspected cybercrimes. You'll also find information on software and Web tools designed specifically for children. Perverted-Justice, mentioned earlier, has a section for parents on how to curb their children's time online and how to spot if their kids are in danger.

Also, try bookmarking a selection of kid-friendly sites so that your children are less tempted to wander the Web aimlessly. [KidGrid](http://dw.com.com/redir?oid=4520-11344_7-6424378-8&ontid=11344&siteid=7&edid=3&lop=txt&destcat=ex&destUrl=http://www.kidgrid.com) is a Yahoo-like search engine with categorized links, all of which have been designated safe. [Kaboose](http://dw.com.com/redir?oid=4520-11344_7-6424378-8&ontid=11344&siteid=7&edid=3&lop=txt&destcat=ex&destUrl=http://www.kaboose.com) provides fun stuff for kids and parents alike, from online games to party planning.

Tip

It's one thing to safeguard your own PCs, but that doesn't help when your kids are online at their friends' houses. Communicate with other parents. Relay your concerns and share tips with them to make sure your child surfs safely, no matter whose computer he or she uses.

The ***EU Kids Online*** survey

This report presents the full findings from a new and unique survey designed and conducted according to rigorous standards by the EU Kids Online network. It was funded by the European Commissions’ Safer Internet Programme in order to strengthen the evidence base for policies regarding online safety.

A random stratified sample of 25,142 children aged 9-16 who use the internet, plus one of their parents, was interviewed during Spring/Summer 2010 in 25 European countries.

The survey investigated key online risks: pornography, bullying, receiving sexual messages, contact with people not known face- to-face, offline meetings with online contacts, potentially harmful user-generated content and personal data misuse.

In this report, ‘children’ refers to internet- using children aged 9-16 across Europe. ‘Using the internet’ includes any devices by which children go online and any places in which they go online.

Uses and activities online

Use is now thoroughly embedded in children’s daily lives: 93% of 9-16 year old users go online at least weekly (60% go online every day or almost every day).

Children are going online at ever younger ages - the average age of first internet use is seven in Denmark and Sweden and eight in several Northern European countries. Across all countries, one third of 9-10 year olds who use the internet go online daily, this rising to 80% of 15-16 year olds.

The most common location of internet use is at home (87%), followed by school (63%). But internet access is diversifying – 49% use it in their bedroom and 33% via a mobile phone or handheld device. Access via a handheld device exceeds one in five in Norway, the UK, Ireland and Sweden.

Children do a range of diverse and potentially beneficial things online: 9-16 year olds use the internet for school work (85%), playing games (83%), watching video clips (76%) and instant messaging (62%). Fewer post images (39%) or messages for others to share (31%), use a webcam (31%), file-sharing sites (16%) or blog (11%).

59% of 9-16 year olds have a social networking profile – including 26% aged 9-10, 49% aged 11-12, 73% aged 13-14 and 82% aged 15-16. Social networking is most popular in the Netherlands (80%), Lithuania (76%) and Denmark (75%), and least in Romania (46%), Turkey (49%) and Germany (51%).

Among social network users, 26% have public profiles – more in Hungary (55%), Turkey (46%), and Romania (44%); 29% have more than 100 contacts, although many have fewer.

Among social network users, 43% keep their profile private so that only their friends can see it. A further 28% report that their profile is partially private so that friends of friends and networks can see it. Notably, 26% report that their profile is public so that anyone can see it.

Digital skills

It is likely that more use facilitates digital literacy and safety skills. Only a third of 9-16 year olds (36%) say that the statement, “I know more about the internet than my parents,” is ‘very true’ of them, one third (31%) say it is ‘a bit true’ and one third (33%) say it is ‘not true’ of them.

Younger children tend to lack skills and confidence. However, most 11-16 year olds can block messages from those they do not wish to contact (64%) or find safety advice online (64%). Around half can change privacy settings on a social networking profile (56%) compare websites to judge their quality (56%) or block spam (51%).

Risk and harm Pornography

Risk does not necessarily result in harm, as reported by children. Children who use the internet were asked if they had encountered a range of online risks and, then, if they had been bothered by this, where ‘bothered’ was defined as something that “made you feel uncomfortable, upset, or feel that you shouldn’t have seen it.” Findings vary by child (e.g. age, gender), country and risk type, so generalisations should be treated with caution.

12% of European 9-16 year olds say that they have been bothered or upset by something on the internet. This includes 9% of 9-10 year olds. However, most children do not report being bothered or upset by going online.

Risks are not necessarily experienced by children as upsetting or harmful. For example, seeing sexual images and receiving sexual messages online are encountered by one in eight children but they are generally not experienced as harmful except by a few of the children who are exposed to them.

By contrast, being bullied online by receiving nasty or hurtful messages is relatively uncommon, experienced by one in twenty children, but it is the risk most likely to upset children.

Further, only 1 in 12 children have met an online contact offline, and also this risk

rarely has a harmful consequence, according to children.

Boys, especially teenagers, are more exposed to sexual images online, while teenage girls are slightly more likely to receive nasty or hurtful messages online. However, girls are generally more likely to be upset by the risks they experience.

The survey asked about a range of risks, as detailed in what follows. Looking across all these risks, 41% of European 9-16 year olds have encountered one or more of these risks.

Risks increase with age: 14% of 9-10 year olds have encountered one or more of the risks asked about, rising to 33% of 11-12 year olds, 49% of 13-14 year olds and 63% of 15-16 year olds.

14% of 9-16 year olds have in the past 12 months seen images online that are ***“obviously sexual – for example, showing people naked or people having sex.”***

Of those who have seen sexual or pornographic images online, one in three were bothered by the experience and, of those, half (i.e. one sixth of those exposed to sexual images or around 2% of all children) were either fairly or very upset by what they saw.

Looking across all media, 23% of children have seen sexual or pornographic content in the past 12 months – with the internet now as common a source of pornography as television, film and video.

Older teenagers are four times more likely than the youngest children to have seen pornography online or offline and the sexual images they have seen online are more explicit. But, younger children are more bothered or upset by sexual images online than teenagers.

53% of those who had been bothered by seeing sexual images online told someone about this the last time it happened – 33% told a friend, 25% told a parent. However, 25% simply stopped using the internet for a while and a few changed their filter or contact settings.

Bullying

In relation to online bullying, 6% of 9-16 year olds have been sent nasty or hurtful messages online, and 3% have sent such messages to others. Over half of those who received bullying messages were fairly or very upset.

Since 19% have been bullied either online or offline (compared with 6% online), and 12% have bullied someone else either online or offline (compared with 3% online), it seems more bullying occurs offline than online.

Most children who had received nasty or hurtful messages online called on social support: a quarter had not told anyone. Six in ten also used online strategies – deleting hurtful messages or blocking the bully; this last strategy was seen by children as effective.

6

￼￼‘Sextin’

 15% of 11-16 year olds have received peer to pe***er “sexual messages or images ...[meaning] talk about having sex or images of people naked or having sex***,” and 3% say they have sent or posted such message

 Of those who have received such messages, nearly one quarter have been bothered by this. Further, of those who have been bothered, nearly half were fairly or very upset. So, overall, one eighth of those who received such messages, or nearly 2% of all children, have been fairly or very upset by sexual messagin

 Among those who had been bothered by ‘sexting’, about four in ten blocked the person who sent the messages (40%) and/or deleted the unwanted sexual messages (38%). In most cases, the child said that this action helped the situation. Such constructive coping responses could be encouraged among more children.

Meeting online contacts offli

 The most common risky activity reported by children online is communicating with new people not met face-to-face. 30% of European children aged 9-16 who use the internet have communicated in the past with someone they have not met face-to-face before, an activity that may be risky but may also be fu

 It is more rare for children to meet a new online contact offline. 9% of children have met an online contact offline in the past year. 1% of all children (or one in nine of those who went to a meeting) have been bothered by such a meetin

 Although 9-10 year olds are the least likely to have met an online contact offline, they are most likely to have been bothered by what happened (31% of those who had been to such a meeting).

Other ris

 The second most common risk is exposure to potentially harmful user-generated content. 21% of 11-16 year olds have been exposed to one or more types of potentially harmful user- generated content: hate (12%), pro-anorexia

(10%), self-harm (7%), drug-taking (7%) or suicide (5%

 9% of 11-16 year olds have had their personal data misused – abuse of the child’s password (7%) or their personal information (4%), or they have been cheated of their money online (1%

 30% of 11-16 year olds report one or more experiences linked to excessive internet use ‘fairly’ or ‘very often’ (e.g. neglecting friends, schoolwork or sleep).

Comparing across countries, encounters with one or more online risks include around six in ten children in Estonia, Lithuania, Norway, the Czech Republic and Sweden. Lower incidence of risk is found in Portugal, Italy and Turkey.

Children are more likely to say they have been bothered or upset by something on the internet in Denmark (28%), Estonia (25%), Norway and Sweden (23%) and Romania (21%); they are less likely to say this in Italy (6%), Portugal (7%) and Germany (8%).

The more children in a country use the internet daily, the more those children have encountered one or more risks. However, more use also brings more opportunities and, no doubt, more benefits.

The greatest range of activities online is also claimed by children in Lithuania, the Czech Republic Estonia, France and Sweden, while the least are undertaken in Ireland and then Turkey. In other words, internet use brings both risks and opportunities, and the line between them is not easy to draw.

Parental awareness:

 Among those children who have experienced one of these risks, parents often don’t realise thi

 40% of parents whose child has seen sexual images online say that their child has not seen them; 56% of parents whose child has received nasty or hurtful messages online say that their child has no

 52% of parents whose child has received sexual messages say that their child has not;

**A Parent's Guide to Internet Safety**



*Dear Parent:*

*Our children are our nation's most valuable asset. They represent the bright future of our country and hold our hopes for a better nation. Our children are also the most vulnerable members of society. Protecting our children against the fear of crime and from becoming victims of crime must be a national priority.*

*Unfortunately the same advances in computer and telecommunication technology that allow our children to reach out to new sources of knowledge and cultural experiences are also leaving them vulnerable to exploitation and harm by computer-sex offenders.*

*I hope that this pamphlet helps you to begin to understand the complexities of online child exploitation. For further information, please contact your local* [*FBI office*](http://www2.fbi.gov/contact/fo/fo.htm) *or the* [*National Center for Missing and Exploited Children*](http://www2.fbi.gov/cgi-bin/outside.cgi?http://www.missingkids.com/) *at 1-800-843-5678.*

*Louis J. Freeh, Former Director
Federal Bureau of Investigation*

**Introduction**

While on-line computer exploration opens a world of possibilities for children, expanding their horizons and exposing them to different cultures and ways of life, they can be exposed to dangers as they hit the road exploring the information highway. There are individuals who attempt to sexually exploit children through the use of on-line services and the Internet. Some of these individuals gradually seduce their targets through the use of attention, affection, kindness, and even gifts. These individuals are often willing to devote considerable amounts of time, money, and energy in this process. They listen to and empathize with the problems of children. They will be aware of the latest music, hobbies, and interests of children. These individuals attempt to gradually lower children's inhibitions by slowly introducing sexual context and content into their conversations.

There are other individuals, however, who immediately engage in sexually explicit conversation with children. Some offenders primarily collect and trade child-pornographic images, while others seek face-to-face meetings with children via on-line contacts. It is important for parents to understand that children can be indirectly victimized through conversation, i.e. "chat," as well as the transfer of sexually explicit information and material. Computer-sex offenders may also be evaluating children they come in contact with on-line for future face-to-face contact and direct victimization. Parents and children should remember that a computer-sex offender can be any age or sex the person does not have to fit the caricature of a dirty, unkempt, older man wearing a raincoat to be someone who could harm a child.

Children, especially adolescents, are sometimes interested in and curious about sexuality and sexually explicit material. They may be moving away from the total control of parents and seeking to establish new relationships outside their family. Because they may be curious, children/adolescents sometimes use their on-line access to actively seek out such materials and individuals. Sex offenders targeting children will use and exploit these characteristics and needs. Some adolescent children may also be attracted to and lured by on-line offenders closer to their age who, although not technically child molesters, may be dangerous. Nevertheless, they have been seduced and manipulated by a clever offender and do not fully understand or recognize the potential danger of these contacts.

This guide was prepared from actual investigations involving child victims, as well as investigations where law enforcement officers posed as children. Further information on protecting your child on-line may be found in the National Center for Missing and Exploited Children's Child Safety on the Information Highway and Teen Safety on the Information Highway pamphlets.

**What Are Signs That Your Child Might Be At Risk On-line?**

**Your child spends large amounts of time on-line, especially at night.**

Most children that fall victim to computer-sex offenders spend large amounts of time on-line, particularly in chat rooms. They may go on-line after dinner and on the weekends. They may be latchkey kids whose parents have told them to stay at home after school. They go on-line to chat with friends, make new friends, pass time, and sometimes look for sexually explicit information. While much of the knowledge and experience gained may be valuable, parents should consider monitoring the amount of time spent on-line.

Children on-line are at the greatest risk during the evening hours. While offenders are on-line around the clock, most work during the day and spend their evenings on-line trying to locate and lure children or seeking pornography.

**You find pornography on your child's computer.**

Pornography is often used in the sexual victimization of children. Sex offenders often supply their potential victims with pornography as a means of opening sexual discussions and for seduction. Child pornography may be used to show the child victim that sex between children and adults is "normal." Parents should be conscious of the fact that a child may hide the pornographic files on diskettes from them. This may be especially true if the computer is used by other family members.

**Your child receives phone calls from men you don't know or is making calls, sometimes long distance, to numbers you don't recognize.**

While talking to a child victim on-line is a thrill for a computer-sex offender, it can be very cumbersome. Most want to talk to the children on the telephone. They often engage in "phone sex" with the children and often seek to set up an actual meeting for real sex.

While a child may be hesitant to give out his/her home phone number, the computer-sex offenders will give out theirs. With Caller ID, they can readily find out the child's phone number. Some computer-sex offenders have even obtained toll-free 800 numbers, so that their potential victims can call them without their parents finding out. Others will tell the child to call collect. Both of these methods result in the computer-sex offender being able to find out the child's phone number.

**Your child receives mail, gifts, or packages from someone you don't know.**

As part of the seduction process, it is common for offenders to send letters, photographs, and all manner of gifts to their potential victims. Computer-sex offenders have even sent plane tickets in order for the child to travel across the country to meet them.

**Your child turns the computer monitor off or quickly changes the screen on the monitor when you come into the room.**

A child looking at pornographic images or having sexually explicit conversations does not want you to see it on the screen.

**Your child becomes withdrawn from the family.**

Computer-sex offenders will work very hard at driving a wedge between a child and their family or at exploiting their relationship. They will accentuate any minor problems at home that the child might have. Children may also become withdrawn after sexual victimization.

**Your child is using an on-line account belonging to someone else.**

Even if you don't subscribe to an on-line service or Internet service, your child may meet an offender while on-line at a friend's house or the library. Most computers come preloaded with on-line and/or Internet software. Computer-sex offenders will sometimes provide potential victims with a computer account for communications with them.

**What Should You Do If You Suspect Your Child Is Communicating With A Sexual Predator Online?**

* Consider talking openly with your child about your suspicions. Tell them about the dangers of computer-sex offenders.
* Review what is on your child's computer. If you don't know how, ask a friend, coworker, relative, or other knowledgeable person. Pornography or any kind of sexual communication can be a warning sign.
* Use the Caller ID service to determine who is calling your child. Most telephone companies that offer Caller ID also offer a service that allows you to block your number from appearing on someone else's Caller ID. Telephone companies also offer an additional service feature that rejects incoming calls that you block. This rejection feature prevents computer-sex offenders or anyone else from calling your home anonymously.
* Devices can be purchased that show telephone numbers that have been dialed from your home phone. Additionally, the last number called from your home phone can be retrieved provided that the telephone is equipped with a redial feature. You will also need a telephone pager to complete this retrieval.
* This is done using a numeric-display pager and another phone that is on the same line as the first phone with the redial feature. Using the two phones and the pager, a call is placed from the second phone to the pager. When the paging terminal beeps for you to enter a telephone number, you press the redial button on the first (or suspect) phone. The last number called from that phone will then be displayed on the pager.
* Monitor your child's access to all types of live electronic communications (i.e., chat rooms, instant messages, Internet Relay Chat, etc.), and monitor your child's e-mail. Computer-sex offenders almost always meet potential victims via chat rooms. After meeting a child on-line, they will continue to communicate electronically often via e-mail.

Should any of the following situations arise in your household, via the Internet or on-line service, you should immediately contact your local or state law enforcement agency, the [FBI](http://www2.fbi.gov/contact/fo/fo.htm), and the [National Center for Missing and Exploited Children](http://www2.fbi.gov/cgi-bin/outside.cgi?http://www.missingkids.com/):

1. Your child or anyone in the household has received child pornography;
2. Your child has been sexually solicited by someone who knows that your child is under 18 years of age;
3. Your child has received sexually explicit images from someone that knows your child is under the age of 18.

If one of these scenarios occurs, keep the computer turned off in order to preserve any evidence for future law enforcement use. Unless directed to do so by the law enforcement agency, you should not attempt to copy any of the images and/or text found on the computer.

**What Can You Do To Minimize The Chances Of An On-line Exploiter Victimizing Your Child?**

* Communicate, and talk to your child about sexual victimization and potential on-line danger.
* Spend time with your children on-line. Have them teach you about their favorite on-line destinations.
* Keep the computer in a common room in the house, not in your child's bedroom. It is much more difficult for a computer-sex offender to communicate with a child when the computer screen is visible to a parent or another member of the household.
* Utilize parental controls provided by your service provider and/or blocking software. While electronic chat can be a great place for children to make new friends and discuss various topics of interest, it is also prowled by computer-sex offenders. Use of chat rooms, in particular, should be heavily monitored. While parents should utilize these mechanisms, they should not totally rely on them.
* Always maintain access to your child's on-line account and randomly check his/her e-mail. Be aware that your child could be contacted through the U.S. Mail. Be up front with your child about your access and reasons why.
* Teach your child the responsible use of the resources on-line. There is much more to the on-line experience than chat rooms.
* Find out what computer safeguards are utilized by your child's school, the public library, and at the homes of your child's friends. These are all places, outside your normal supervision, where your child could encounter an on-line predator.
* Understand, even if your child was a willing participant in any form of sexual exploitation, that he/she is not at fault and is the victim. The offender always bears the complete responsibility for his or her actions.
* Instruct your children:
	+ - to never arrange a face-to-face meeting with someone they met on- line;
		- to never upload (post) pictures of themselves onto the Internet or on-line service to people they do not personally know;
		- to never give out identifying information such as their name, home address, school name, or telephone number;
		- to never download pictures from an unknown source, as there is a good chance there could be sexually explicit images;
		- to never respond to messages or bulletin board postings that are suggestive, obscene, belligerent, or harassing;
		- that whatever they are told on-line may or may not be true.

**Frequently Asked Questions:**

**My child has received an e-mail advertising for a pornographic website, what should I do?**

Generally, advertising for an adult, pornographic website that is sent to an e-mail address does not violate federal law or the current laws of most states. In some states it may be a violation of law if the sender knows the recipient is under the age of 18. Such advertising can be reported to your service provider and, if known, the service provider of the originator. It can also be reported to your state and federal legislators, so they can be made aware of the extent of the problem.

**Is any service safer than the others?**

Sex offenders have contacted children via most of the major on-line services and the Internet. The most important factors in keeping your child safe on-line are the utilization of appropriate blocking software and/or parental controls, along with open, honest discussions with your child, monitoring his/her on-line activity, and following the tips in this pamphlet.

**Should I just forbid my child from going on-line?**

There are dangers in every part of our society. By educating your children to these dangers and taking appropriate steps to protect them, they can benefit from the wealth of information now available on-line.