

STATE OF



**INTERNET
SECURITY**

Q207 Focus:

Protecting Children Online



TABLE OF CONTENTS

- Overview 01**
- Introduction 02**
- Children on the Internet 03**
 - Challenge 1: Keeping Children Safe Online 05
 - Predatory Behavior 05
 - Pornography 06
 - Bullying 06
 - Challenge 2: Keeping Computers Safe from Online Children 07
 - Downloading Harmful Files 07
 - Challenge 3: Keeping Online Children on the Right Side of the Law 07
 - Bullying 07
 - Downloading Illegal Files 07
 - Potential Parental Liability 07
- The Role of Parents 08**
- The Role of Government 10**
- The Role of Technology 12**
- Empowering Parents 13**
 - Setting and Enforcing the Rules 13
 - Rule 1: Time Online 13
 - Rule 2: Allowed Sites 14
 - Rule 3: Approved Contacts 14
 - Rule 4: Private Information 15
 - Rule 5: Computer Ownership 15
- Conclusion 16**
 - Online Kids Need Online Parents 16
 - About Webroot Software, Inc. 17
 - About the Research 17
- Appendix 18**
 - Resources for Parents 18
- Sources 19**

O V E R V I E W

Children are exposed to real risks when they go online. Parents' commitment to understanding their children's online activities and setting age-appropriate rules, along with the use of software to help monitor and enforce the rules, provide the best combination to protect kids online.

Report Highlights:

Kids Online

- Almost 60 percent of children three and older are using the Internet (page 3).
- Forty-three percent of teens who use social networking sites reported having been contacted online by complete strangers (page 5).
- Thirty-seven percent of children ages 11 to 17 reported they had received a sexually explicit email or pop-up advertisement within the past year (page 6).
- In homes where children under 18 used the Internet, there was a 28 percent greater incidence of spyware infections in the preceding 6 months (page 7).

Discrepancies Between Parents and Kids

Over 70 percent of U.S. 11 to 17 year-olds said that their parents ask them about their online activities. Yet, there are still discrepancies between children's responses and parents' responses about Internet use. For example:

- Approximately 45 percent of kids responded that they spend an average of three or *more* hours on the Internet daily, while approximately 76 percent of parents said their children spend an average of two hours or *less* per day on the Internet at home (page 8).
- Over half of the children said they buy things online at least sometimes while 71.2 percent of parents responded that their 11 to 17 year olds never buy over the Internet (page 9).

Government Support

- Attempts to enact online child protection laws have been fraught with difficulties (page 10).
- Several courts, including the U.S. Supreme Court, have concluded that technical solutions are the most effective means – more effective than laws – to protect children from harmful online content. Yet, only about half of parents use a parental control application (page 12).

“I received invitations from someone I don't know on MySpace.”
- Girl, 14, Illinois

I N T R O D U C T I O N

Classic children's stories like *Hansel and Gretel* and *Little Red Riding Hood* are cautionary tales about trusting strangers and traveling alone in unfamiliar surroundings. Today, there are many news stories and television programs delivering these same messages for the Internet age.

For the past four years, Chris Hansen of Dateline NBC has conducted a series of hidden camera investigations called "To Catch a Predator" devoted to the subject of identifying and detaining potential child sexual abusers who attempt to contact children over the Internet. In March 2007, Hansen released his book, *To Catch a Predator: Protecting Your Kids from Online Enemies Already in Your Home*, which details his experience meeting adults who pose as young teens, exchange emails with children and then show up in person to meet their would-be victims.

NBC isn't the only network addressing the topic of online predators targeting our children. U.S.-based cable network Nickelodeon, home of well-known kid cartoons, aired a feature in December 2006 called "Online and in Danger? How to Protect Yourself in the Virtual World."

While the threats are certainly real, simply disconnecting is not a practical solution. In the words of Nick News host Linda Ellerbee, "The goal of this show is not to scare kids offline or encourage parents to unplug computers, but to help kids better understand and use this evolving technology, and show them ways to protect themselves in the process."

It is in this same spirit that Webroot® Software's State of Internet Security report for the second quarter of 2007 focuses on *Protecting Children Online*. The State of Internet Security report provides an in-depth review and analysis of timely topics on a quarterly basis. These reports focus on specific aspects of Internet security.

Protecting Children Online provides a review and analysis of the online habits of children, the risks of Internet usage and how parents can protect their children online.

Future reports will concentrate on Internet security topics that impact Webroot's consumer and business customers around the globe.

"I had to take info to police because a 26 year old male was pursuing my 14 year old."
- Mother of 14 and 16 year-old children, Illinois

CHILDREN ON THE INTERNET

In September 2006, the U.S. National Center for Education Statistics issued a report about Computer and Internet Use by Students in 2003 (the most recent census relating to computer usage). According to the report, about 91 percent of children age three and over in nursery school through grade 12 were using computers, and about 59 percent were using the Internet. As broadband deployment in the U.S. has accelerated since 2003, it is safe to assume these numbers have only increased over the past several years.

This trend is higher or at least comparable in other parts of the world.

- The *Young Canadians in a Wired World* survey issued by the Media Awareness Network in 2005, found that 94 percent of young people in grades 4 to 11 go online from home, compared with 79 percent in 2001.
- According to a UK Office of Communications' Media Literacy Audit published in February 2006, 64 percent of UK children ages 8 to 15 have access to the Internet at home.
- In December 2005, Nielsen/NetRatings New Zealand issued its *eGeneration* report that found 80 percent of kids ages 6 to 17 use the Internet for homework, 70 percent use email, 69 percent play online games and 42 percent use instant messaging (IM).

In May 2007, Webroot Software conducted a survey to learn more about Internet usage among U.S. children ages 11 to 17. Based on the results, almost half responded that they average three hours or more per day using the Internet from home.



Almost 60 percent of children ages three and older are using the Internet.

Average Daily Internet Usage for U.S. 11-17 Year-Olds							
Location	Not online	> 1 Hr.	1-2 Hrs.	3-4 Hrs.	5-6 Hrs.	7+ Hrs.	Don't Know
Home	0.2%	11.3%	41.2%	23.7%	10.1%	11.6%	2.0%
School	18.9%	56.0%	19.9%	2.6%	0.7%	0.5%	1.5%

Webroot Youth Internet Usage Survey, May 2007 (N=603)

State of Internet Security: Protecting Children Online

Close to 100 percent of the 11 to 17 year-olds surveyed use the Internet for email at least some of the time. Three-fourths also reported using IM at least some of the time, and 73.6 percent use social networking sites such as MySpace® and Facebook®, at least some of the time.

Frequency of Internet Activities for U.S. 11-17 Year-Olds					
Type of Activity	Almost Every Day	Often	Some-times	Never	Don't Know
Social networking (e.g., MySpace, Facebook)	39.7%	16.5%	17.4%	25.6%	0.8%
Instant Messaging (IM)	39.7%	16.5%	19.8%	23.1%	0.8%
Emailing	34.7%	29.8%	33.1%	1.7%	0.8%
Playing online video games	27.3%	26.4%	30.6%	15.7%	0.0%
Homework	17.4%	47.9%	31.4%	2.5%	0.8%
Downloading music	16.5%	29.8%	33.9%	19.8%	0.0%
Blogging	9.9%	13.2%	22.3%	52.9%	1.7%
Visiting chat rooms	8.3%	10.7%	25.6%	55.4%	0.0%
Buying products or services	0.8%	10.7%	39.7%	48.8%	0.0%

Webroot Youth Internet Usage Survey, May 2007 (N=603)

“I just got my IM set up this week but will be on that every day. I play on-line games about 40 hours a week.”
- Boy, 13, Pennsylvania

Given the pervasive use of the Internet by school-age children, parents are faced with a number of challenges including:

- How to best keep children safe when they are online.
- How to make sure children's online activities don't harm the computer.
- How to make sure children do not do anything illegal while online.

Challenge 1: Keeping Children Safe Online

According to a recent Webroot survey, U.S. parents who have children ages 5 to 17, with home access to the Internet, are most concerned about predatory behavior by strangers and exposure to pornography. They are also concerned about their children giving out personal information or participating in inappropriate IM or chat room discussions.

Parents' Top Concerns About Children's Online Computer Use	
Rank	Concern
1	Predatory behavior by strangers
2	Exposure to pornography
3	Giving out personal information
4	Inappropriate chat room or IM discussions
5	Downloading harmful files
6	Access to violent sites
7	Downloading music or video files illegally
8	Online bullying
9	Making unauthorized purchases
10	Peer-to-peer gaming
11	Online gambling

Webroot Parental Controls Survey, May 2007 (N=609)

Forty-three percent of teens who use social networking sites reported being contacted online by complete strangers.

Exposure to Predatory Behavior

In spite of the increasing focus in the media via television programs and news stories about online child predators, the problem will not disappear.

In Webroot Software's May 2007 survey, 18.2 percent of 11 to 17 year-olds across the U.S. reported they received an invitation via the Internet within the past year to meet someone they do not know. This percentage is even higher with an older age group, and higher still among teens that use social networking sites. *Teens, Privacy & Online Social Networking*, issued by the Pew Internet and American Life Project in April 2007, found that a third of teenagers (ages 12-17) who use the Internet, and 43 percent of teens who use social networking sites, reported having been contacted online by complete strangers.



State of Internet Security: Protecting Children Online

Exposure to Pornography

In 2006, the U.S. Department of Justice commissioned Philip Stark, PhD, a professor at the University of California at Berkeley and nationally recognized statistician, to study the prevalence of sexually explicit web sites on the Internet and the frequency of searches that include sexually explicit sites in the results.

Dr. Stark's study estimated that 1.1 percent of all sites catalogued by the Google™ and MSN® search engines are sexually explicit. Yet, the study also found that sexually explicit web sites seem to be disproportionately popular. Dr. Stark estimates that of all search queries conducted via AOL®, Google, MSN and Yahoo!®, six percent retrieve at least one sexually explicit web site in the first page of results displayed, and 40 percent of the most popular search queries produce at least one sexually explicit web site.

The sheer volume of sexually explicit content makes it concerning for parents whose children are online. Compounding this concern are spam emails that deliver explicit content to children's addresses and pop-up advertisements that can begin showing up on computers infected with spyware.

In Webroot's May 2007 survey, 37.2 percent of children ages 11 to 17 reported they had received a sexually explicit email or pop-up advertisement within the past year.

Exposure to Bullying

In addition to exposure to pornography and predators, children may also be the victims of online bullying, or cyberbullying, which is when kids send or post text or images intended to hurt or embarrass another person. According to the National Crime Prevention Council, cyberbullying affects almost half of all American teens.

Cyberbullying can take many forms. In some cases, it involves mean, vulgar or harassing messages. It can also include "outing" - when secret or private information is shared to embarrass a target, or "trickery" - when someone is led to share information under false pretenses. Cyberbullying can also involve more serious situations such as stalking and threats of physical harm.

In cases of off-line bullying, home is usually the child's safe, "bully-free" zone. When the bullying is done online, however, it invades the child's home and can be even more harmful as the victim may feel there is no escape. Victims of harsh and continuous cyberbullying can struggle with depression and other psychological impacts including suicidal feelings.

Cyberbullying can also escalate to assaults and vandalism in the real world. It is important that children, parents and educators see online bullying as a serious situation and intervene early.

"My child has not specifically herself received a bullying message; however she sees them frequently when she goes to others she associates with on MySpace."

- Mother of 9 and 12 year-old children, Washington

Challenge 2: Keeping Computers Safe from Online Children

Beyond the concerns that parents have about keeping their children safe, there are also ways that children can, usually unknowingly, cause harm to the computer while they are online.

Downloading Harmful Files

Parents need to be very concerned about cyber crooks interested in stealing passwords, credit card numbers, social security numbers and other financial information. These bad guys often include spyware programs in emails or web postings that will load onto the computer when the child unwittingly opens an attachment, navigates to a link or downloads a game or a cute smiley face.

Just as social networking sites and chat rooms pose the greatest potential exposure to online predators, they are also a leading source for spyware and schemes that can lead to data theft. Consumer Report's *State of the Net* survey issued in September 2006, found that in homes where children under 18 used the Internet, there was a 28 percent greater incidence of spyware infections in the preceding six months.

This is particularly alarming if a child is using the same computer a parent uses for Internet banking or storing other personal and sensitive information. Even if a child has a separate computer that does not store any sensitive information, spyware can significantly impede the computer's performance, and serious spyware infections can render a machine inoperable.

Challenge 3: Keeping Online Children on the Right Side of the Law

While parents are seriously concerned about their children's exposure to online solicitations and harmful content, there are also times when children are the ones breaking the law or victimizing others.

Bullying

For kids who are victims of online bullying, the bullies are usually other kids. These cyber-bullies use IM, email, social networking sites and online group games to alienate their victims, start or perpetuate lies or damage their victim's reputation. In the teen years, cyberbullying can also cross over into sexually harassing behavior. While most online bullying behavior is cruel and unkind but not illegal, cyberbullying can sometimes escalate into real world physical assaults and vandalism.

Downloading Illegal Files

Another way in which children must learn to respect others rights while online relates to copyrights. Children may be illegally downloading copyright protected content, such as music or videos that could bring potential liability for copyright infringement. There are also times when children and teens, out of curiosity, experimentation, peer pressure or malicious intent, engage in hacking or other potentially damaging behaviors.

Potential Parental Liability

In some U.S. states, such as California, New York and Texas, parents can be held legally liable for any "property damage" caused by their children. That means if a child intentionally sends spyware, misappropriates intellectual property or engages in other potentially illegal actions, parents may find themselves in court.

In homes where children under 18 used the Internet, there was a 28 percent greater incidence of spyware infections.

THE ROLE OF PARENTS

Parents play a central role in setting guidelines and talking to children about safe and appropriate online behaviors. Some parents may feel their children are more knowledgeable than they are about computers and the Internet, and thus may not feel comfortable having these conversations. Fortunately, this is not the case for most parents. In Webroot's May 2007 survey, 71.3 percent of U.S. 11 to 17 year-olds said that their parents ask them about their online activities. Only 11 percent responded that their parents do not monitor their online activities.

Less encouraging were the results of a study issued in July 2006 by the leading children's charity in the United Kingdom, NCH (formerly called the National Children's House) in which nearly 60 percent of UK children aged 11 to 16 said their parents have not talked to them about what types of web sites they are allowed to visit. In addition, 53 percent of the children in the study said they are never or hardly ever supervised while online, yet 81 percent of the parents said they know what their children are doing online all or most of the time.

The Webroot study also found divergences when children's responses are compared to a similar survey of parents of 11 to 17 year-olds. For example, 45.7 percent of kids responded that they spend an average of three or more hours on the Internet daily, while 75 percent of parents said their children spend an average of two hours or less per day on the Internet at home. This may indicate a lack of knowledge on the part of parents, but it may also reflect wishful thinking of parents who answered with what they felt was most appropriate, knowing that their child is spending more time on the Internet than would be deemed "best." Even when parents do take the time to discuss Internet use, the survey found that what matters most is the content of those conversations.

Almost forty-six percent of kids spend an average of three or more hours on the Internet.

Average Daily Home Internet Usage U.S. 11-17 Year-Olds						
Response	> 1 Hr.	1-2 Hrs.	3-4 Hrs.	5-6 Hrs.	7+ Hrs.	Other Response
Kids' Response	11.3%	41.2%	23.7%	10.1%	11.6%	2.2%
Parents' Response	28.2%	47.5%	19.0%	2.8%	0.0%	2.5%

*Webroot Youth Internet Usage Survey, May 2007 (N=603)
Webroot Parental Controls Survey, May 2007 (N=358)*

There are also differences between how often children say they engage in certain Internet activities compared to parents' point of view. For example, 14.2 percent of the parents surveyed said their children never use email, yet only 1.7 percent of children agreed.

State of Internet Security: Protecting Children Online

There was an even larger gap in responses about buying products and services online. Over half of the children said they buy things online at least sometimes, while 71.2 percent of parents responded that their kids never buy over the Internet.

Frequency of Internet Activities for U.S. 11-17 Year-Olds										
Activity	Almost Every Day		Often		Sometimes		Never		Don't Know	
	Kids View	Parents View	Kids View	Parents View	Kids View	Parents View	Kids View	Parents View	Kids View	Parents View
Social networking	39.7%	29.6%	16.5%	16.5%	17.4%	20.7%	25.6%	29.7%	0.8%	3.6%
Instant Messaging (IM)	39.7%	26.3%	16.5%	16.5%	19.8%	26.8%	23.1%	27.1%	0.8%	3.4%
Emailing	34.7%	26.0%	29.8%	28.8%	33.1%	29.9%	1.7%	14.2%	0.8%	1.1%
Playing online games	27.3%	18.4%	26.4%	21.2%	30.6%	37.7%	15.7%	20.9%	0.0%	1.7%
Homework	17.4%	20.4%	47.9%	39.4%	31.4%	34.4%	2.5%	5.3%	0.8%	0.6%
Downloading music	16.5%	8.9%	29.8%	22.9%	33.9%	34.1%	19.8%	30.7%	0.0%	3.4%
Blogging	9.9%	2.5%	13.2%	9.8%	22.3%	20.4%	52.9%	57.8%	1.7%	9.5%
Visiting chat rooms	8.3%	3.6%	10.7%	8.7%	25.6%	24.3%	55.4%	56.7%	0.0%	6.7%
Buying products or services	0.8%	0.0%	10.7%	2.5%	39.7%	25.1%	48.8%	71.2%	0.0%	1.1%

*Webroot Youth Internet Usage Survey, May 2007 (N=603)
Webroot Parental Controls Survey, May 2007 (N=358)*

Whether parents are not talking to their children as much as they think they are or whether kids are not listening as parents hope they are, there is a clear opportunity for ongoing and more detailed conversations to be taking place. Resources to empower parents to take a leadership role in education and guidance are included in the Appendix.

There is a clear opportunity for ongoing and more detailed conversations to be taking place.

THE ROLE OF GOVERNMENT

In addition to their efforts to discuss online safety with their children, many parents have expressed their concerns to their elected officials. As a result, parents' concerns about online safety have generated a proliferation of government and non-profit led efforts over the past decade to improve Internet safety for children around the world. Some of the most prominent of these are included in the Appendix.

In addition to supporting educational efforts, governments also assist in the pursuit of increasing online safety by increasing inter-governmental coordination. For example, the FBI leads the Innocent Images International Task Force (IIITF), formed in 2004, to foster international cooperation between law enforcement officers from the United Kingdom, Norway, Finland, Ukraine, Belarus, Australia, Thailand, the Philippines, Croatia, Latvia, Germany, the Netherlands, New Zealand, Canada, Sweden, Fiji, Cyprus, and Europol (European Law Enforcement Organization).

As another example, Viviane Reding, the European Commissioner for Information Society and Media, met with Yoshihide Suga, the Japanese Internal Affairs and Communications Minister, during her trip to Tokyo in April 2007. The two believe that the number of illicit and inappropriate websites has become a major social issue in both Japan and Europe and they agreed to increase their cooperation to enhance Internet safety.

Beyond education and cooperation, there have been some attempts to enact laws to protect children online. These efforts, however, have generally been fraught with difficulties because of the fine line between freedom of speech and censorship, and because one parent's views about what is objectionable will vary from those of another.

In the U.S., the Communications Decency Act of 1996 was Congress's first attempt to make the Internet safer for minors by criminalizing certain types of Internet speech. The law was found to be unconstitutional by the Supreme Court. Congress then passed the Child Online Protection Act (COPA) of 1998. COPA required all commercial distributors of "material harmful to minors" to restrict their sites from access by minors. The Act was quickly challenged in the courts.

COPA also mandated a congressionally appointed commission to "...identify technological or other methods that will help reduce access by minors to material that is harmful to minors on the Internet."

The COPA Commission report, delivered to Congress on October 20, 2000, concluded that the most effective means of protecting children from harmful content on the Internet are: aggressive efforts for public education, consumer empowerment, increased resources for enforcement of existing laws, and greater use of technology.

Attempts to enact online child protection laws have been fraught with difficulties.



State of Internet Security: Protecting Children Online

The Supreme Court agreed with the Commission. In June 2004, the Supreme Court upheld an injunction on enforcement of COPA, concluding that the law was likely to be unconstitutional and remanded the case to the District Court. In doing so, the Supreme Court noted that, “filtering’s superiority to COPA is confirmed by the explicit findings of the Commission on Child Online Protection, which Congress created to evaluate the relative merits of different means of restricting minors’ ability to gain access to harmful materials on the Internet.”

On March 22, 2007, the District Court issued an order permanently preventing the enforcement of COPA, finding that the law violates the First and Fifth Amendments. The court also concluded that technical solutions such as content filters are a more effective means of restricting children’s access to materials harmful to them than COPA could be.

There were two other U.S. laws enacted around the same time as COPA that were more narrowly crafted to withstand legal challenges and have since remained in effect. The Children’s Online Privacy Protection Act of 1998 (COPPA) restricts online marketing to children under 13 and details the requirements web site operators must fulfill to protect children’s privacy and safety online. The Children’s Internet Protection Act of 2000 (CIPA) requires schools and libraries to use filtering software if they receive government funding.

Several courts have ruled that technical solutions are the most effective means to protect children online.

THE ROLE OF TECHNOLOGY

Technology problems are best matched with technology solutions. Leading child advocacy groups such as Childnet and the National Center for Missing and Exploited Children (NCMEC), policy makers and the courts agree that software programs, along with education and conversation, are parents' best tools to protect their children online.

In spite of the emphasis on software filters and similar programs as an effective means to control children's exposure to harmful content, only about half of parents have chosen to use such applications.

A March 2005 study by the Pew Internet & American Life Project found that 54 percent of families with teens who go online said they used a content filter. This percentage is lower when families with younger children are included. While the court decisions repeatedly refer to "filters," today's parental control programs offer considerably more functionality while content filters have become increasingly sophisticated to minimize the amount of legitimate and educational content that may be blocked inadvertently.

Parents should evaluate programs for their filtering effectiveness as well as their ability to manage computer time, online chat and online game-playing. Programs also need to prevent children's attempts to bypass or override the monitoring features, or change any of the computer's administrative settings. Easy-to-read usage reports that can be viewed online or emailed are an important feature to evaluate, too.

In addition to parental control programs, there are also ongoing efforts to set guidelines and standards that will help parents screen web sites. The Family Online Safety Institute (FOSI) started a project in February 2007 scheduled to run through March 2008 to develop a protocol for Web description resources (also referred to as content labels).

Policy makers and the courts agree that software programs, along with education and conversation, are parents' best tools to protect their children online.

EMPOWERING PARENTS

Ultimately, parents must serve as their children's primary mentor when it comes to establishing guidelines and a dialogue about safe Internet usage. Software programs aimed at helping parents keep their children safe online need to offer a range of functionality to adapt over time as the child's exposure and use of the Internet develops and evolves.

Setting and Enforcing the Rules

Part two of the Canadian Media Awareness Network's study, *Young Canadians in a Wired World*, 2005, found a strong correlation between the rules parents set and the behavior reported by children. For example, when parents have set and communicated a clear rule about what sites the child is not supposed to visit, that child reports lower exposure to inappropriate (porn, hate, gambling) sites.

As the U.S. Supreme Court observed, it is difficult to set a "one size fits all" rule for what is appropriate. Rather than a single universal set of rules, parents should customize a specific set of rules for each child. Once created, the rules can be printed and signed by parents and children and kept next to the computer as a reminder. It is also very important for parents to be clear that the rules apply all the time, not only on the home computer since children can also access the Internet at school, a friend's house or, as they get older, at Internet cafes.

Parents' commitment to understanding their children's online activities and setting age-appropriate rules, along with the use of software to help monitor and enforce the rules, provide the best combination to protect kids online. Suggested topics for rules include:

- Time Online
- Allowed Sites
- Approved Contacts
- Private Information
- Computer Ownership

Rule 1: Time Online

Children as young as one year-old may spend some time looking at web sites for young children or viewing family photos or videos. As soon as a child is online it is appropriate to begin communicating when computer time is done.

Parents need to determine the appropriate amount of online time for each child. This may mean only certain days of the week, some extra time on the weekends or enforcing a set time at night by which the computer must go off.

As children get older, the time allowed will likely increase, but the importance of managing and limiting time can be even more necessary. As children begin to use email, instant messaging and social networking sites to interact with their friends online, these activities can be habit-forming.



"I love using my PC and if I tried and messed with the program, I would be banned for a month!!"

- Girl, 13, Kentucky

State of Internet Security: Protecting Children Online

Parental control software that includes time control functions empowers parents to set and manage schedules that allocate the amount of time that each child may spend accessing the Internet or playing games or other computer activities.

Rule 2: Allowed Sites

Once they enter school, almost all children will be exposed to computers and the Internet. It's important for parents to begin discussing "good sites" and steering their children to sites that are designed specifically for their age group.

Initially, parental control programs can be used to limit access to only select sites that are most appropriate for the child. Many children-oriented sites include numerous advertisements that can lead kids away from children-safe sites into other areas of the Internet. Parental control programs prevent children from navigating to any of these advertising sites that are not on the approved site list.

Parents should consider limiting children under 12 to using search engines that are specifically geared to kids, such as Ask for Kids™, Yahoo! Kids and the Google kids and teens directory.

As children get older and seek to access additional information via the Internet for school projects, or to play more sophisticated games or chat with friends, parents will need to carefully adjust filtering to provide strong protection while still enabling access to school-recommended sites and homework resources. An important feature for a parental control program is a temporary, one-time use password to bypass the filter if a legitimate site is inadvertently blocked.

As older children are given access to regular search engines and a greater number of sites, online activity reports can be especially helpful to provide parents a view of the sites children are visiting without the child feeling that their parents are looking over their shoulder.

Parents may consider blocking peer-to-peer sites to help prevent their children from downloading pirated software, movies, or music. Parents can sign up their child for iTunes or another legal music service and then fund their download account as part of an allowance or reward system.

Rule 3: Approved Contacts

The people children can contact online should be screened and pre-approved by parents. Particularly for younger children, additions to the email address book and the IM buddy list should only be made by a parent. Parental controls software can be used to block contacts from anyone not in the address book or on the buddy list.

The need for parents to be involved in approving online contacts does not go away as children get older. By the time kids are 11, their online focus shifts significantly to using the Internet to communicate with friends. Email and instant messaging become more primary activities over visiting web sites and playing games. This greatly increases the risk of exposure to: cyberbullying, inappropriate content in spam and other emails, contact from strangers and spyware programs.

Many children-oriented sites include numerous advertisements that can lead kids away from children-safe sites into other areas of the Internet.

State of Internet Security: Protecting Children Online

In addition to email and instant messaging, there are many other online ways for kids to connect, including social networking sites, chat rooms and blogs. Parents should carefully review any web sites, profiles and screen names kids post online.

Parents should be particularly concerned about children sharing pictures online or using a webcam. Parental control programs should have the ability to block certain programs that can include webcam driver software. Ensure that children have a clear rule about not meeting anyone in person that they have only met online without being accompanied by a parent or guardian.

Rule 4: Private Information

In all cases – web sites, email, IM, chat rooms – children need to know not to give out any personal information online. There are many kid-oriented sites that will ask kids for information and use it for marketing purposes. These forms can come up on game sites that offer “bonus points” for filling out the form, and as submissions to win prizes like a PlayStation® or Xbox®. Children need to know that they should not fill out any online forms without parental approval and involvement.

In addition to being educated about not sharing personal information online, children also need to be educated about keeping their passwords private and not sharing them with their friends. The unfortunate reality for children and adolescents is that someone who is their “best friend” today may not be their friend any longer in a couple months. It is important that they know certain information cannot be shared with anyone, not even their close friends. In addition, creating an effective password that does not use obvious personal information such as the family pet’s name and one that is made up of numerals, special characters and upper-case letters, should be part of the discussion.

Rule 5: Computer Ownership

Most of the rules can remain the same with some minor updating as children age. The most significant change is likely to be the amount of resistance parents receive as their children get older.

Even if a child is the primary or sole user of a particular computer in the home, it’s important to set expectations early that the computer is owned by the adults in the family. Parents should be very cautious about thinking of the computer as the child’s private space like a diary might be. Online access for non-school related activities should be given as a privilege by parents and respected as a responsibility by kids.

Parents should retain password control. In addition, parents should educate themselves about how to reset passwords. Parents should also remember to keep their own passwords secure, so that children cannot sign in as parents. Parental control software should include robust features that prevent children from making any configuration changes to the computer.

Parents must ensure that effective antispyware, antivirus and pop-up blocker programs are running, and are regularly updated to prevent unwanted and malicious programs from getting on the computer. Parents should also consider keeping the computer in a central location rather than allowing kids to be online in their bedroom or behind a closed door.

“The computer is in the kitchen and they watch what I do!”

- Girl, 17, Wisconsin

C O N C L U S I O N

Few parents would consider handing their son or daughter the car keys without having spent time with him or her behind the wheel to see if their skills warrant the privilege of taking the car out on their own. Yet some parents give their kids a computer with Internet access and set them free, claiming their kids know more than they do.

Online Kids Need Online Parents

Children need support and guidance from their earliest computer experiences through the teen years. Eventually they will be online adults and the Internet skills they gain as kids will help them throughout their lives to make good choices, protect their personal information and avoid sites and emails that could be scams or spyware facades. In addition to monitoring and actively discussing children's online activities, parents can and should participate with them whenever possible.



- Parents can ask their children to teach them how to use programs they use and show them their favorite sites.
- Emailing and instant messaging are two increasingly common ways for parents to ask their children about their day at school, their homework assignments, weekend plans and friends.
- Parents can sign up through various online services, such as Google Alerts, to receive news stories about children's online safety issues, and email relevant articles to their children to read for themselves the things they need to be aware of and cautious about.
- Parents should continue to encourage their teens to come to them with any concerns.
- Parents can ask a responsible teen to serve as a role model for a younger brother or sister learning about how to navigate the Internet safely.
- Parents need to be diligent about educating themselves and keeping pace with their children's computer knowledge via books, web sites, parent groups, school programs and computer education classes.

While it might take some effort, there are numerous resources and some very effective, user-friendly products to provide parents with the knowledge and skills they need to be actively involved in their children's online activities.

“When all is said and done, the most important thing you can do is educate your child about the dangers of the Internet. If they do not follow specific rules, then you need to be consistent and enforce these rules.”

- Mother of 5 and 13 year-old children, California

State of Internet Security: Protecting Children Online

About Webroot Software

Webroot Software, Inc. provides industry leading security software for consumers, enterprises and small and medium-sized businesses worldwide. Globally recognized for its award-winning Spy Sweeper® line of anti-spyware products, Webroot recently incorporated anti-virus protection into two new products for consumers and SMBs: Spy Sweeper with AntiVirus and Webroot SME Security. The company has also expanded into the parental controls software market with the introduction of Webroot Child Safe®. The Boulder, Colorado-based company is privately held and backed by some of the industry's leading venture capital firms, including Technology Crossover Ventures, Accel Partners and Mayfield.

Webroot's software consistently receives top review ratings by respected third-party media and has been adopted by millions globally. Available as either branded solutions or on an OEM basis, Webroot products can be found at www.webroot.com and on the shelves of leading retailers worldwide.

To find out more about Webroot, visit www.webroot.com or call 1-800-772-9383.

About the Research

Webroot sponsored an online survey in May, 2007, of 603 11 to 17 year-olds with access to the Internet at home and 609 parents of 5 to 17 year-olds with access to the Internet at home, of which 358 were parents of 11 to 17 year-olds. The margin of error for each study is ± 4.0 percentage points. For the subset of parents of 11-17 year-olds (N=358), the margin of error is ± 5 percentage points. Survey Sampling International provided the sample for the study.

© 2007 All rights reserved. Webroot Software, Inc. Webroot, the Webroot icon, Spy Sweeper and Child Safe are registered trademarks of Webroot Software, Inc. in the United States and other countries. All other trademarks are properties of their respective owners.

NO WARRANTY. Analysis based on research conducted by Webroot Software, Inc. The information is provided AS-IS and Webroot makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained herein is at your own risk. Documentation may include technical or other inaccuracies or typographical errors. Webroot reserves the right to make changes without prior notice.

Certain data is available upon request.

A P P E N D I X

Resources for Parents

Canada

In Canada, the Canada Safety Council (www.safety-council.org/info/child/webrules.html) and the Media Awareness Network (www.media-awareness.ca/english/parents/Internet/index.cfm) are two leading sources for information and tools to assist parents in better understanding and discussing their children's online activities.

Europe

Insafe (www.saferInternet.org), Europe's Internet safety portal, provides detailed information about agencies and non-profits across 25 countries, all dedicated to protecting children on the Internet across. Countries included in the Insafe site are: Austria, Belgium, Cyprus, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovenia, Spain, Sweden and the United Kingdom.

There are many UK based resources, including Think U Know (www.thinkuknow.co.uk) that provides resources for children, parents and educators and NCH (www.nch.org.uk) the UK's leading children's charity.

Global

Childnet International (www.childnet-int.org), based in London, was established in 1995 and has provided programs in countries around the world. In recent years, Childnet staff have spoken at conferences in Armenia, Ireland, Jamaica, Japan, Korea, Thailand and the U.S.

United States

In the U.S., the Federal Trade Commission in coordination with other government agencies runs the site OnGuard Online (www.onguardonline.gov). Numerous non-profit groups also exist that have focused on increasing Internet safety and providing education for parents and children, including:

- Cyber Angels – www.cyberangels.org
- Enough is Enough – www.enough.org
- GetNetWise – www.getnetwise.org
- iKeepSafe – www.ikeepsafe.org
- iSAFE – www.isafe.org
- National Center for Missing and Exploited Children – www.ncmec.org
- NetSmartz – www.netsmartz.org

In addition to a wealth of resources, NetSmartz has an online response team to answer parents' questions. NetSmartz411 (www.netsmartz411.org) is a web site where parents can review questions asked by others, as well as submit questions.

S O U R C E S

Court Related Documents

ACLU v. Gonzales

U.S. District Court for the Eastern District of Pennsylvania
Final Adjudication by Judge Lowell A. Reed, Jr.
Issued March 22, 2007

Ashcroft v. ACLU

U.S. Supreme Court Decision
Issued June 29, 2004

Expert Report of Philip Stark, PhD
Commissioned by the U.S. Department of Justice
In the proceedings of *ACLU v. Gonzales*
Submitted to the court May 8, 2006

Studies and Surveys

Computer and Internet Use by Students in 2003

National Center for Education Statistics
U.S. Department of Education
Issued September 2006
<http://nces.ed.gov/pubs2006/2006065.pdf>

Get I.T. Safe: Children, Parents and Technology Survey 2006

NCH – the children's charity
London, United Kingdom

Internet Usage – U.S. children ages 11-17

Webroot Software Research
Survey conducted May 2007

Japan, EU to Boost Cooperation on Internet Safety

Japan Today
April 2007

Media Literacy Audit

UK Office of Communications
Issued in February 2006
http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/children/

Online and in Danger? How to Protect Yourself in the Virtual World

A program produced by Nick News
Aired December 2006 on Nickelodeon Network

Online Controls – U.S. parents of children ages 5-17

Webroot Software Research
Survey conducted May 2007

Parental Liability for Copyright Infringement by Minor Children

Electronic Frontier Foundation
November 1, 2005; Revised May 1, 2007
http://www.eff.org/IP/P2P/Parent_Liability_Nov_2005.pdf

State of the Net Survey 2006

Consumer Reports
Published September 2006

Teens, Privacy & Online Social Networking

Pew Internet & American Life Project
Issued April 2007

Teens and Technology

Pew Internet & American Life Project
July 2005

Young Canadians in a Wired World

Media Awareness Network
Phase One conducted in 2001
Phase Two conducted in 2005
<http://www.media-awareness.ca/english/research/YCWW/>

Young New Zealanders are Avid Internet Users

Nielson/NetRatings New Zealand
December 2005
http://www.netratings.com/pr/pr_051219_newzealand.pdf

Web Sites

Canada Safety Council

<http://www.safety-council.org/info/child/webrules.html>

Childnet International

<http://www.childnet-int.org>

Enough is Enough

<http://www.enough.org>

Family Online Safety Institute

<http://www.fosi.org>

Federal Bureau of Investigation Cyber Division

<http://www.fbi.gov/cyberinvest/cyberhome.htm>

Federal Trade Commission

<http://www.ftc.org>

GetNetWise

<http://www.getnetwise.org>

iKeepSafe

<http://www.ikeepsafe.org>

Innocent Images National Initiative

<http://www.fbi.gov/publications/innocent.htm>

Insafe

<http://www.saferinternet.org>

iSAFE

<http://www.isafe.org>

Media Awareness Network

<http://www.mediaawareness.ca/english/parents/internet/index.cfm>

National Center for Missing and Exploited Children

<http://www.ncmec.org>

National Crime Prevention Council

<http://www.npc.org/media/cyberbullying.php>

NetSmartz

<http://www.netsmartz.org>



Webroot Software, Inc.
P.O. Box 19816
Boulder, CO 80308-2816
USA
www.webroot.com
Phone: 303.442.3813
Fax: 303.442.3846
Consumer Sales & Support: 866.612.4227
Consumer Sales & Support: www.webroot.com/support