

Cyber Safety Guide

From Time Warner Cable
and CyberAngels



CyberAngels

A program of Guardian Angels
keeping it safe

A complimentary guide to
safe Internet use for parents

 **TIME WARNER**
CABLE

Table of Contents

A Note To Parents	3
Common Uses of the Internet	4–11
• Surfing	4
• Chat Rooms	4–5
• E-mail	6
• Instant Messaging	6–7
• Downloading/File Sharing	7
• Social Networking	8
• Gaming	9
• Online Child Solicitation	10
• Cyberbullying, Harassment and Stalking	10–11
When to Worry	12
Tips for Parents	13
Guardian Angels/CyberAngels	14
Time Warner Cable of NY & NJ	15
Additional Resources	Back Cover

A Spanish language version available online at timewarnercable.com/nynj



Time Warner Cable and CyberAngels: Your Partners in Internet Safety

Children today are communicating over the Internet through a multitude of ways—MySpace, Xanga and Facebook are just some of the more than 200 social networking websites. Add in instant messaging, chat rooms, blogging, and the challenge for parents to keep up is overwhelming. That's why Time Warner Cable, your Internet service provider, and CyberAngels, a program of the acclaimed Guardian Angels organization, have united to help you keep your child safe. The Internet is a powerful tool, but it's important to practice some safety measures and common sense. We are taking the initiative to provide a framework for you for teaching responsible Internet use to your children.

Understanding the responsibility that comes with technology is key to safety. It's unlikely that you would send your child out to cross the street without first giving a lesson in safe crossing. Nor would you hand over the keys to your car to your teen before learning how to drive and earning a driver's license. And the ramifications of an error in judgment online can be just as serious and long lasting. Through this guide, we want to empower both you and your family to use the Internet and enjoy all the positive benefits it offers.

This practical guide simplifies the complex lingo and activities that have become a phenomenon with young people. Here you can find everything from common acronyms to e-mail safety tips and security safeguards. Also included are suggested topics to discuss with your child and signs of potential problems, as well as a reference list of resources for further information and guidance. Get helpful hints on how to monitor your child's Internet behavior, establish boundaries and ensure that the experience is enjoyable, informative and all that it should be.

We encourage you to keep this guide within easy reach and refer to it often as you and your family continue to navigate this vast platform. After all, parenting your child is an ongoing effort.

Common Uses of the Internet

Surfing

Reading documents and visiting websites online is commonly referred to as “surfing” or “browsing”. Visiting virtual museums, accessing public government documents, reading complete books and viewing short films are just a few examples of the many ways in which you can use the Internet.

Be aware, however, that unmonitored computers can give your child access to material that is inappropriate.

WHAT PARENTS SHOULD KNOW:

Cookies

Each time you visit a website, a cookie is created. Cookies are simple text files that contain information about your travels on the web. Because the data contained in a cookie may reveal personal information about you, you should learn to set the proper security controls on your browser software.

Visit www.cyberangels.org for more information on managing and securing your browser.

Chat Rooms

“Chatting” online has become a favorite way for people to connect online in a group (a chat room) to share similar interests. Chatting is like talking, except that you type words rather than speak them. Typically, more than one “conversation” goes on simultaneously at a given time or chat room. There are two types of chat rooms—moderated and unmoderated. A chat room moderator enforces rules about what is acceptable to discuss in a given chat space. We recommend children be allowed to visit only moderated chat rooms that have been approved by you.

TALK TO YOUR CHILD ABOUT

Nicknames and Profiles

Avoid choosing provocative or identifiable nicknames. Keep personal information out of your online profile.

Receiving Files

If you are accepting files from someone you do not know, or even from a friend, be aware that files can carry a virus that may corrupt or delete data from your computer.

Strangers

Teach your child not to chat with online strangers.

Etiquette

Good etiquette should be used on the Internet as you would in person. While chatting, refrain from making comments that would be considered inappropriate or offensive in verbal conversation.

ACRONYMS PARENTS SHOULD KNOW:

AFK / BAK

Away from keyboard/
Back at keyboard

121

One-to-one

ASL?

Age, sex, location?

PA/ PAL/ POS/ P911

Parent alert/Parents are
listening/ Parents over
shoulder/ Parent alert

NIFOC

Naked in front of computer

MorF

Male or female

SorG

Straight or gay

LMIRL

Let's meet in real life

TDTM

Talk dirty to me

ADR

Address

WYCM?

Will you call me?

F2F

Face to face

WRN?

What's your real name?

WUF?

Where are you from?

53x

Sex

Cyber

Cybersex, sex over the
computer

WTGP

Want to go private?

E-mail

E-mail is one of the most commonly used features of computers with Internet connections. E-mail can be used effectively in a variety of ways by children—to write to family members and friends, communicate with teachers, even contact famous people and experts in various fields.

E-MAIL SAFETY TIPS

Select “Smart” Passwords

Choose a password that is not easy for a hacker to guess, preferably one that includes upper AND lower case letters, as well as one or two numbers. Don't share the password with anyone.

Don't open suspicious attachments

Never download or open attachments from people you don't know. Be careful opening attachments from people you DO know—the message may be spoofed (the return address may be fake), or it may be that your friend's computer is infected with a virus.

Spam


Do not respond to spam (unwanted e-mails). Many e-mails include an "unsubscribe" link that will actually verify your address to spammers—resulting in even more spam.

Log Out

If you are using a public computer and a web-based mail system (such as Yahoo, AOL, or Hotmail), always be sure to log out of your account when you are finished. Just directing the browser to a new page doesn't log you out, and leaves your account accessible to anyone else who sits down at that terminal.

Instant Messaging

An instant message (“IM”) allows two or more people to talk by typing back and forth in real time. IM programs usually appear on screen as boxes of some kind, a split screen, or small screen where the typed messages are passed back and forth. Some of these programs allow you to see what the person is writing as they are writing it.



They are usually free, easy to download, and fairly simple to operate. Many IM programs also allow you to transfer files such as photos or music files (eg, mp3 files).

DID YOU KNOW?

Some parental control software programs can filter outgoing information, and actually prevent certain words or phrases from being typed. This type of blocking can keep your last name, your street, school or phone number from being sent out online. Road Runner and many other Internet service providers offer blocking and filtering tools. To find out more information about how to access these features, please visit roadrunner.com.

Downloading/File Sharing

File sharing is another activity for many teens. File sharing is accomplished through easily obtainable programs that allow users to connect directly to other computers and copy (share) music files, movies, and other programs or files. This use of the Internet is a security risk because the files can be infected, and also may violate copyright protections.

BE AWARE

Security Risks

There is a very real security risk to every user who chooses to use P2P (peer-to-peer) file-sharing software. P2P software leaves your computer open to other users, and the files you download could be infected with trojans, worms or viruses, potentially leaving your computer vulnerable to attack or misuse.

Legal Implications

Individuals who share personal copies of films, television or music files on the Internet are at risk for lawsuits.

Social Networking: Blogging and other online diaries

Children are no longer restricted to playgrounds, sports teams or malls to meet new people. The world around them has become digital and VERY accessible. Students can set up a free e-mail address, web pages and online photo albums within minutes. Blogs (short for web logs) are like online journals and allow people to share their most intimate thoughts with a worldwide audience.

Many children have discovered that MySpace, Facebook, LiveJournal, and many other social networking sites are a great way to communicate with friends all over the globe. They are able to post messages, photos, and list all their favorite things about themselves. What children don't always understand is how public this information really is.

As parents, the best way to keep your children safe is to remind them that having an online "personality" places them at potential risk. Information posted online means exposure to the entire world.

SOCIAL NETWORKING SAFETY TOPICS TO DISCUSS WITH YOUR CHILD:

- Assume everyone has access to your site, and always will.
- Think carefully before posting information or photos.
- Assume that predators are looking at everything you write and post.



Gaming

Gaming is another option for young people—and gaming online can be very exciting. The thrill of competition, the ease of access to new games and excellent graphic effects make this activity fun for kids. But because of the ability to also chat with other players, safety issues should be discussed in the same manner as chat and IM concerns.

TIPS FOR PARENTS OF GAMERS

Educate Yourself

- Carefully read the game ratings for age recommendations.
- Read the privacy policies of each site.
- Review the acceptable use terms with your child (this may also be referred to as the Code of Conduct).

Set Limits

Suggested rules include limiting play time and never chatting with strangers or giving out any personal information, including the child's real name or where he or she lives.

Monitor Your Child

Read his/her chat logs and discuss language and behavior that may be inappropriate. Point out examples within the logs and role-play ways to handle potentially unsafe situations.

Help Choose Safe Nicknames

Encourage your child to choose non-gender specific nicknames, and be sure that profiles do not include personally identifiable information.

Protect the Password

Tell your child to never share a password with a friend or allow someone else to access their account.

Join the Game

Ask your children to teach you how to play the game. This exercise encourages your child to be the teacher, and allows you to identify possible safety issues while playing with your child.

Online Child Solicitation

The most serious danger for children online is the risk of becoming a victim of a sexual predator. Unsupervised children may find their way into chat rooms or forums, which are proven venues that pedophiles use to lure victims.

If you suspect that your child has been approached online by a predator, save any and all computer and/or phone communications, and report it to the National Center for Missing & Exploited Children's CyberTipline at www.cybertipline.com. Contact your local police department if you suspect your child is in immediate danger.

Cyberbullying, Harassment and Stalking

The feeling of anonymity on the web makes it a perfect playground for students to engage in cruel behavior. A 2007 study from the National Crime Prevention Council (NCPC) indicates that 43 percent of teens reported being victims of cyberbullying. Cyberbullying can consist of spreading lies and rumors about a person, insulting and targeting a student's sexuality or physical appearance, deceiving students into revealing personal information and then publishing it, and posting personally identifiable information or photos without the victim's consent. Technology used may include cell phones, instant message programs, chat rooms, e-mail, websites, polls and blogs.



TIPS FOR DEALING WITH CYBERBULLYING

Tell the person harassing you in straightforward terms, "Leave me alone, stop harassing me. Do not contact me again."

Do not reply to anything else the harasser says. Don't reply to e-mails, taunts or lies.

Log all chats and IMs and print a copy as evidence. Save all e-mails and text messages as well as voice mails or voice messages. Take screen shots as well. Print all evidence, but keep the files on your hard drive.

In the case of e-mail harassment, you need to contact the harasser's ISP (Internet Service Provider) and register a complaint. If an offending website has been posted about you, contact the web hosting service. If there are posts on a forum or bulletin board, contact the moderators.

Keep in mind that some types of bullying (threats to your child, or exposing them to danger) may be illegal. Report such actions to local law enforcement along with copies of the materials that you have collected.



When to Worry

There are a number of signs that may signal trouble. You know your child better than anyone else, so follow your instincts.

Screen Switching

If your child quickly changes screens or turns off the monitor when you come into the room, it is likely he/she is viewing something they don't want you to see. Be calm and ask them to move so that you can view the screen.

Odd Phone Calls

If your child suddenly begins receiving phone calls from strange adults (or even other children) you may have a problem. Install a caller ID program to determine where the calls are coming from and ask your child to explain them.

Odd Hours of the Night

If your child is up typing away in the wee hours of the night, he/she may be chatting online. This activity should be reserved for times and places that are supervised.

Sudden Influx of Cash

If your child suddenly has more cash than can be accounted for, or shows up in unfamiliar clothing or with gifts that you can't explain, this may be a sign of questionable activity. A pedophile often spends a great deal of money cultivating a relationship with a child.

Unusually Upset at an Internet Interruption

It is not normal to cry or to become overly upset when the Internet goes down for an hour or two. This type of behavior should raise a red flag and prompt frank discussions with your child.

Withdrawal from Family or Friends

Pedophiles work very hard to drive a wedge between children and the people who support and care for them. The larger the gap between the child and his /her family, the easier it is for a predator to create a relationship.



Tips for Parents—Talk to Your Child

Don't rely on software to do your job

Filtering and blocking programs can be a part of your Internet safety plan at home, but they don't take the place of an informed and involved parent.

Be proactive

Attend cyber safety classes and spend some time listening to and speaking with other concerned parents.

Participate with your child online

Familiarize yourself with the services and programs your child uses.

Plan ahead

Talk to your child about the things that could be encountered online, and what he/she can do.

Encourage their other interests

Children shouldn't spend an excessive amount of time online. Encourage them to participate in other types of activities, too.

Think "mall"

You wouldn't drop your young child off alone in a mall, so don't "drop them off" online either. Remember to keep an eye on them.

A time and place for everything

Keep your computer in a "common" room— where you can keep an eye on it. Grant your child Internet access only when you are at home and awake.

Explore the Internet

Take the time to explore the use of your computer and the Internet. They are valuable tools that can enrich the lives of every member of your family. The more you know, the better you can protect your family.

Guardian Angels—Beyond the Streets

The red beret of The Guardian Angels has become an icon for safety around the world. Founded in 1979 by Curtis Sliwa, The Guardian Angels began as a group of 13 dedicated volunteers who patrolled the subways, streets and neighborhoods of New York City to combat and deter crime. The organization has evolved into today's global network of Angels—volunteers from all walks of life, respected by law enforcement, welcomed by citizens and applauded by governments.

As part of its move “beyond the streets,” The Guardian Angels responded to citizens’ calls for protection from online threats with the launch of CyberAngels in 1995. The volunteer-based CyberAngels is one of the oldest and most respected online safety education programs in the world. This non-profit organization offers information, workshops, seminars, lesson plans and a website to promote safeguards for children’s online activities.

With selfless dedication and passionate community service spanning nearly three decades, The Guardian Angels stands today as a leading violence prevention and safety education organization.

Whether you are a parent, educator, or even a victim, CyberAngels makes many resource tools, free tutorials and more in-depth information or assistance available at their website, cyberangels.org, including:

- **Software for securing your computer**
- **Tips on how and where to report online crime**
- **Ways to encourage the best use of the Internet**
- **Internet 101-learn the basics of using your home computer**
- **Online seminars for parents**
- **Specialized sections for victims, educators, and families**
- **Educational video segments**
- **Examples of cyber crime, signs of cyber crime and what to do**
- **Information about Phishing**

Time Warner Cable—Beyond Television

Time Warner Cable understands the responsibility it has to its customers. Beyond offering the latest in technological equipment and service, the company provides resources and tools that allow you and your family to use and enjoy its services with all intended positive benefits.

The complexities of the world we live in today prompted us to create this Cyber Safety Guide for you. The Internet is a powerful tool that carries the potential to go beyond its practical uses for research, entertainment and communication. In addition to security filters and firewalls, parental monitoring and an awareness of the risks associated with the World Wide Web, we want to help you recognize and respond to the signs of possible Internet misuse.

Time Warner Cable also offers two free On Demand channels that feature brief lessons on cyber safety, cyberbullying, safe social networking, surfing the Internet, gaming and downloading. Tune to Channel 100 for Answers On Demand and Channel 1111 for Local On Demand to view these programs.

This guide is one example of Time Warner Cable's commitment to education, which includes scholarships and grants, free high-speed Internet access and video service to public schools, internship and trainee programs, complimentary teacher resource guides and workshops for educators. For more information about our educational initiatives, please visit timewarnercable.com/nynj.

Additional Resources

For further information, we recommend the following resources:

AOL Security Central

safety.aol.com

Cable in the Classroom

Media Smart

ciconline.org/media-smart

Common Sense Media

commonsensemedia.org

CyberAngels

cyberangels.org

Internet Safety Coalition

ikeepSAFE.org

i-Safe

isafe.org

National Cable Television Assn.

pointsmartclickSAFE.org

National Cyber Security Alliance

staysafeonline.org

Net Smartz Workshop

netsmartz.org

Road Runner Security Tips

roadrunner.com

Time Warner Cable

timewarnercable.com/nynj



Public Affairs Department
120 East 23rd Street
New York, NY 10010
timewarnercable.com/nynj



CyberAngels

A program of Guardian Angels
keeping it safe

717 Fifth Ave.
Suite 401
New York, NY 10022
cyberangels.org