

Internet Safety

While children need a certain amount of privacy, they also need parental involvement and supervision in their daily lives. The same general parenting skills that apply to the “real world” also apply while online. If you have cause for concern about your children’s online activities, talk to them. Also seek out the advice and counsel of teachers, librarians, and other Internet and online service users in your area. Having open communication with your children, using computer resources, and getting online yourself will help you obtain the full benefits of these systems and alert you to any potential problem that may occur with their use. If your child tells you about an upsetting message, person, or web site encountered while online, don’t blame your child but help him or her avoid problems in the future. Remember — how you respond will determine whether they confide in you the next time they encounter a problem and how they learn to deal with problems on their own.

Beyond these basics, there are some specific things that you should know about the Internet. For instance did you know that there are chat areas, newsgroups, and web sites that have material that is hateful, is violent, or contains other types of material that parents might consider to be inappropriate for their children? It’s possible for children to stumble across this type of material when doing a search using one of the web sites that is specifically designed to help people find information on the Internet. Most of these sites, called “search engines,” do not, by default, filter out material that might be inappropriate for children, but some offer a childsafe option and some are designed specifically for use by children.

Also the Internet contains newsgroups, web sites, and other areas designed specifically for adults who wish to post, read, or view sexually explicit material including pictures, stories, and videos. Some of this material is posted on web sites where there is an attempt to verify the user’s age and/or a requirement for users to enter a credit-card number on the presumption that children do not have access to credit-card numbers. Other areas on the Internet make no such effort to control access. Nevertheless, consider monitoring your credit-card bills for such charges. In addition to “adult” pornography, there are also areas on the Internet that contain illegal child pornography. If you or your children come across this type of material, immediately report it to the National Center for Missing & Exploited Children’s (NCMEC) CyberTipline® at www.cybertipline.com.

Some online services and ISPs allow parents to limit their children’s access to certain services and features such as adult-oriented “chatrooms,” bulletin boards, and web sites. There may be an area just for children where it is less likely for them to stumble onto inappropriate material or get into an unsupervised “chatroom.” At the very least, keep track of any files your children download to the computer, consider sharing an E-mail account with your children to oversee their mail, and consider joining them when they are in private chat areas.

In addition there are ways to filter or control what your children can see and do online. One type of filter, called a “spam” filter limits unsolicited E-mail including mail promoting sexually explicit material. Some ISPs and E-mail services include filters as part of their service but, if not, there is software you can purchase that will attempt to limit the type of mail that gets through.

There are also ways to filter what a child can see on the world wide web. Check with your service provider to see if they offer age-appropriate parental controls. If not consider using a software program that blocks chat areas, newsgroups, and web sites that are known to be inappropriate for children. Most of these programs can be configured by the parent to filter out

sites that contain nudity, sexual content, hateful or violent material or that advocate the use of alcohol, drugs, or tobacco. Some can also be configured to prevent children from revealing information about themselves such as their name, address, or telephone number. You can find a directory of these filtering programs at www.getnetwise.org/ tools.

Another option is to use a rating system that relies on web-site operators to indicate the nature of their material. Internet browsers can be configured to only allow children to visit sites that are rated at the level that the parents specify. The advantage to this method is that only appropriately rated sites can be viewed. The disadvantage is that many appropriate web sites have not submitted themselves for a rating and will therefore be blocked.

While technological-child-protection tools are worth exploring, they're not a panacea. To begin with, no program is perfect. There is always the possibility that something inappropriate could "slip through" or something that is appropriate will be blocked. Finally, filtering programs do not necessarily protect children from all dangerous activities. For example some do not control instant messaging or chat services which are particularly dangerous because they put a child in instant communications with other people. Also some filters do not work with peer-to-peer networks that allow people to exchange files such as music, pictures, text, and videos. These peer-to-peer networks are sometimes used to distribute pornography, including child pornography. Filters are not a substitute for parental involvement. Regardless of whether you choose to use a filtering program or an Internet rating system, the best way to assure that your children are having positive online experiences is to stay in touch with what they are doing. One way to do this is to spend time with your children while they're online. Have them show you what they do, and ask them to teach you how to use the Internet or online service. You might be surprised by how much you can learn from your children.

Guidelines for Parents

Set reasonable rules and guidelines for computer use by your children

By taking responsibility for your children's online computer use, parents can greatly minimize any potential risks of being online. Make it a family rule to:

- Never give out identifying information — home address, school name, or telephone number — in a public message such as chat or newsgroups, and be sure you're dealing with someone both you and your children know and trust before giving out this information via E-mail. Think carefully before revealing any personal information such as age, financial information, or marital status. Do not post photographs of your children in newsgroups or on web sites that are available to the public. Consider using a pseudonym, avoid listing your child's name and E-mail address in any public directories and profiles, and find out about your ISP's privacy policies and exercise your options for how your personal information may be used.
- Get to know the Internet and any services your child uses. If you don't know how to log on, get your child to show you. Have your child show you what he or she does online, and become familiar with all the activities that are available online. Find out if your child has a free web-based E-mail account, such as those offered by Hotmail and Yahoo!®, and learn their user names and passwords.
- Never allow a child to arrange a face-to-face meeting with someone they "meet" on the

Internet without parental permission. If a meeting is arranged, make the first one in a public place, and be sure to accompany your child.

- Never respond to messages that are suggestive, obscene, belligerent, threatening, or make you feel uncomfortable. Encourage your children to tell you if they encounter such messages. If you or your child receives a message that is harassing, of a sexual nature, or threatening, forward a copy of the message to your ISP, and ask for their assistance. Instruct your child not to click on any links that are contained in E-mail from persons they don't know. Such links could lead to sexually explicit or otherwise inappropriate web sites or could be a computer virus. If someone sends you or your children messages or images that are filthy, indecent, lewd, or obscene with the intent to abuse, annoy, harass, or threaten you, or if you become aware of the transmission, use, or viewing of child pornography while online immediately report this to the NCMEC's CyberTipline at 1-800-843-5678 or www.cybertipline.com. Set reasonable rules and guidelines for computer use by your children.
- Remember that people online may not be who they seem. Because you can't see or even hear the person it would be easy for someone to misrepresent him- or herself. Thus someone indicating that "she" is a "12-year-old girl" could in reality be a 40-year-old man.
- Remember that everything you read online may not be true. Any offer that's "too good to be true" probably is. Be careful about any offers that involve you going to a meeting, having someone visit your house, or sending money or credit-card information.
- Set reasonable rules and guidelines for computer use by your children. (See "My Rules for Online Safety" on the back cover.) Discuss these rules and post them near the computer as a reminder. Remember to monitor your children's compliance with these rules, especially when it comes to the amount of time your children spend on the computer. A child's excessive use of online services or the Internet, especially late at night, may be a clue that there is a potential problem. Remember that personal computers and online services should not be used as electronic babysitters.
- Check out blocking, filtering, and ratings applications. Be sure to make this a family activity. Consider keeping the computer in a family room rather than the child's bedroom. Get to know their "online friends" just as you get to know all of their other friends. If your child has a cellular telephone, talk with him or her about using it safely. The same rules that apply to computer use, also apply to cellular telephones.
- Be sure to make this a family activity. Consider keeping the computer in a family room rather than the child's bedroom. Get to know their "online friends" just as you get to know all of their other friends.
- Children should also be cautioned to never give out their Internet or AOL password to anyone even if the person claims to work for AOL or an Internet service provider. When in doubt, children should ask their parents and parents should know their provider's policy regarding passwords (AOL staff, for example, will **never** ask a member for their password).

The FTC makes the following recommendations:

- Don't give out your account password to anyone, even someone claiming to be from your online service. Your account can be hijacked, and you can find unexpected charges on your bill.
- People aren't always who they seem to be in Cyberspace. Be careful about giving out your credit card number. The same applies to your Social Security number, phone number and home address.
- Be aware that when you enter a chat room, others can know you are there and can even e-mail you once you start chatting. To remain anonymous, you may want to use a nickname for your screen name.
- E-mail is relatively private — but not completely. Don't put anything into an electronic message that you wouldn't want to see posted on a neighborhood bulletin board.
- Check your online service for ways to reduce unsolicited commercial e-mail. Learn to recognize junk e-mail, and delete it. Don't even read it first. Never download an e-mail attachment from an unknown source. Opening a file could expose your system to a virus.
- You can be defrauded online. If an offer is too hard to believe, don't believe it.
- Credit rights and other consumer protection laws apply to Internet transactions. If you have a problem, tell a law enforcement agency.
- Teach your children to check with you before giving out personal — or family — information and to look for privacy policies when they enter a web site that asks for information about them. Many kids' sites now insist on a parent's approval before they gather information from a child. Still, some openly admit they will use the information any way they please.

<http://www.safekids.com/>

What Parents Need to Know About Blogging

by Anne Collier

Editor, NetFamilyNews.org

Blogs are new to a lot of parents, but they're nothing new to kids. Fifty-two percent of all blogs belong to 13-to-19-year-olds, according to a recent study at Georgetown University, the number of blogs has been put at anywhere between 10 million and 32 million, and a new blog is created about every 5.8 seconds. That's why we'll keep coming back to this moving target of a subject, and we recommend that you check the News often, because we report on teen blogs a lot. But here are some basics for parents:

What's a Blog?

"Blog" is short for "Web log," an online journal or diary with - depending on the blogging service - varying degrees of privacy. Having one is a lot like having your own web site, only much easier to create and maintain (no techie know-how required), and in most cases it's free. If you can do word-processing or email, you can have a blog. Anyone, regardless of age, can start one just about anywhere there's a computer and an Internet connection (e.g., at home, a friend's house, cybercafes, libraries, etc.).

Blogging's pretty new, but so far there are basically three kinds of blogs: professionals' blogs (where journalists, techies, researchers, etc. talk about what they're working on), amateur blogs about interests and hobbies (film, music, parenting, sports, pets, etc.), and social blogs. Kids' blogs certainly involve their interests too, but usually in the context of their social scene - a lot like instant messaging. A blog is just another "place" for kids to hang out with their friends.

Sometimes the better part of a high school will be blogging on one of the services popular among teens like MySpace.com and Xanga.com, so - as with instant messaging - teenagers tend to use the service their friends use. Which one they use is not really negotiable (if your friends aren't there, there's no point in being there, the thought goes).

Because it's so social, blogging usually isn't meant to be private like a diary, even though many teens publish very personal information in their blogs. They post (or type into the blog) their thoughts and feelings - about themselves, friends, music, parties, what's going on at school, etc. - and friends post their replies. Like instant-messaging, blogs also include a personal profile - a place where friends and strangers can click to find out the blogger's description of herself, her favorite tunes, celebrities, Web sites, etc. Many blogs expect you to post a picture of yourself to go with the profile. Some allow you to post other pictures and audio clips and links to music playlists. Some people just use blogs to share photos. The pictures part has been a shock to some parents who've read teen blogs, but we'll come back to that.

Young bloggers' privacy

So far, privacy clearly has not been an issue for teen bloggers themselves - except, of course, when their parents read their blogs. A young blogger could be posting the most intimate details of his life for anyone in the world to find in a search engine, but when a parent sees the post, very often a teen's privacy-invasion flag goes up. Complete strangers are less of an issue. This will probably change, as public (and parent) awareness grows and adults get more engaged in kids' blogging experiences.

Until then, it would be good for parents and kids to have a conversation about basic privacy protection while blogging (click here to read how one father and 12-year-old blogger worked through the issues). All the basic online-safety rules should apply in the blogging space as much as with any other online activity (see the rules at SafeTeens.com and SafeKids.com).

Basic blogging smarts

It's always a good idea to ask your child if s/he has a blog. If the answer is no, search for his or her full name in a Web search engine just to be sure (parents should have no

qualms about ensuring that a child isn't putting any information online that identifies him or her personally - this is basic child protection). If the answer is yes, good for your child for being up front about it! Only two basic questions need to follow:

You're not publishing any personally identifiable information in your blog, right? (Examples: full name, school name, street address, phone no., etc.) The most important policy by far is never to use your full name online.

Are there privacy protections at your blogging service, and do you use them? The safest policy is: Keep it among friends - don't let strangers read your posts, comment/reply to them, or add themselves to your group or Friends list. Also, don't make your email address or IM screenname public unless it's a "throw-away" account you can delete if someone starts harassing you.

That second question is really the start of a discussion, since teenagers and parents usually have different definitions of privacy and its importance. Also, different blogging services have different levels and types of privacy protection - keep reading.

Beware the three "P's"

That would be **Posts** (blog entries), **Profiles** (bloggers' and instant messengers' descriptions of themselves), and **Pictures**. These are all wonderful means of self-expression and getting to know people, but they're also the areas where young bloggers' privacy, and possibly safety, is most vulnerable. We all know kids are risk-takers and often use the anonymous online environment to experiment with identity. So most online kids know that what you see isn't always what you get online (people fudge their ages and sometimes post pictures of "themselves" that aren't recent or even real), but kids don't always think about what other people can do with the information they post in blogs, whether friends, former friends, or strangers. If a friend somehow switches loyalties or gets mean, someone posting very personal information or pictures can really get hurt. Help your kids think about the implications of forgoing privacy and revealing their innermost thoughts.

Blogging sites' privacy options (the 4th "P")

Though your child may not be using one of the more protective services (and, to her, switching may be "social death"), most do have some pretty good privacy features. In most cases, the protections are obvious right when you sign up (you might start a test blog to see what it's all about). Your child can also show you how s/he configured them, which might be a good thing to run through together. Here are some examples of privacy options in most blogging services:

- At sign up (or reconfiguring account set-up), opting for friends-only or me-only (like a diary) instead of public blogging
- When posting, making each entry private or friends-only
- Not allowing her blog to be in the service's searchable directory
- Allowing only friends to post replies in his blog
- Not allowing people they don't know to add them to their Friends or Buddy list.

Depending on maturity level, if your child is a tween or young teen, it might be a

good idea to go through the blogging service's privacy options right alongside him or her. Then go to the blog together and click around. Make sure the profile doesn't reveal anything someone with bad intentions could use to contact him or her; check out his or her photos (or have her sub in a favorite pop artist, pet, flower, or animation); click to friends' blogs; and talk, as you go, about how much your child really feels comfortable about revealing to friends who can be fickle. Again depending on trust and maturity levels, it's also a good idea for parents to know their child's username and password. Kids won't like it, but they need to know that it's not to embarrass but to protect them.

A few specifics on the services

This is by no means a comprehensive list, but the blogging services teens tend to prefer are sites like MySpace.com, Xanga.com, LiveJournal.com, and Blurty.com. All provide a measure of privacy, but seldom seem to act upon abuse reports - users are pretty on their own. Then there are the big-company services like MSN Spaces, Yahoo 360, Google's Blogger.com, and AOL's RED Blogs for teens (the most protective, but only for AOL members). MSN Spaces and Yahoo 360 both provide at least two levels of privacy, Blogger is all-public-all-the-time (except you can choose not to have your blog listed on its home page or available to search engines). MySpace, which says it's only for bloggers 14+ (and says it'll delete profiles of under-14s if it finds out) makes its privacy options a little harder to find (go to "Account Settings," then "Privacy Settings"), and there are no privacy settings for individual entries (that can be clicked on before posting). For example, some services allow the blogger to make sure only friends read a particular post, or to go back later and change its privacy level. MySpace may eventually become more overt about user privacy, because its parent company, InterMix, has been acquired by large media company News Corp., which makes it about as "mainstream" as Microsoft, Google, and Yahoo.

<http://www.blogsafety.com/>

Safe Blogging Advice for Parents

by Larry Magid

Kids will express themselves online. Help them to it safely

Most adults define their community in geographical terms - the people who live nearby. But thanks to the Internet, many teens and some preteens also live in virtual communities that have no geographical boundaries. For better or worse, the Internet has opened them up to the world.

Nowhere is this more profound than the recent trend of "blogging." Short for "web log," a "blog" is a web page maintained by an individual, organization or business for the purpose of communicating with others. There are millions of blogs out there and, according to researchers at Georgetown University more than half of them are run by people between 13 and 19.

Kids are using these blogs for all sorts of things, ranging from describing their homework assignments to exploring their hobbies to exposing their innermost thoughts. Some kids post photos on their blogs or put up links to their favorite music or movies.

There are a lot of positive aspects to blogging. For one thing, it helps teens develop language and communications skills -- and becoming an Internet publisher can greatly enhance a teenager's sense of self-esteem. Blogs offer young people not only a sounding board for what's on their mind, but also feedback and validation from others, who can comment on what they write using a feedback mechanism on the blog itself.

Blogs can also be used as learning tools. There are some teachers and schools, for example, that encourage students to use blogging tools to discuss their assignments.

Although there are some commercial blogging services that charge money, most kids take advantage of the free services like MySpace, LiveJournal, Xanga, or MSN Spaces. In compliance with the Children's Online Privacy Protection Act, most of these sites are open only to children 13 or older (although check the Terms of Use for any particular site to be sure), but younger children to lie about their age if they're determined to create a blog.

Like so many other positive things on the Net, there is also a dark side to blogs spaces and other online social networking tools. Because they are generally open forums where people can post just about anything, they are also subject to misuse. Some children and teens, for example, have put personal information on blogs that make it too easy for a stranger to locate them, call them on the phone or send them e-mail. Others have posted photos, which can make it easier for a stranger to identify them. There are cases where students have also posted photos with inappropriate poses and clothing, or lack thereof. Some reference or even celebrate the use of drugs, alcohol or harmful diets. Tragically, there have even been blogs that encourage suicide.

If your child or teen has a blog, ideally it would be good if he or she told you the blog's web address so you could monitor what was being posted and be sure your child isn't posting any personal information or anything else that could be harmful. But the truth is that many kids who have blogs are reluctant to tell their parents because they use the blogs to express themselves in ways that they may not want to share with their parents. This is a tough issue. On one hand, parents have a right (some would say obligation) to stay on top of what their kids are doing, especially when it comes to a publicly accessible Internet site. On the other hand - right or wrong -- it's hardly unusual for kids to want to keep some secrets from their parents, especially when it comes to emotional issues which are so often explored in teen blogs. Though this doesn't always work, parents can attempt to find if their child has a blog by using the blogging service's search feature to search for the child's email address, first and last name, nicknames, school name, or any other word that you think your child may have used in a profile.

At the very least, you should have a discussion with your child. Ask if they have a blog, and ask how they are using it and if you can get them to share the web address. But, regardless of what they say, it's still a good idea to talk with them about the safe and unsafe use of blogs. Some blogging services offer safety and privacy tips for their members as well as tools to limit who can visit member blogs. Ask your kids they've read the service's tips and policies and whether they're using any available privacy features. If not, ask them why.

Think carefully about whether or not you should try to prohibit them from

having a blog at all. Some teens might go ahead and maintain a blog even if their parents object. But, whatever you do, be sure to talk with them about how they can protect their safety and privacy. Remind your kids that giving out personal information can be dangerous and that whatever they post on their blog can follow them for the rest of their lives. A photo or a piece of writing that may seem funny or cool or just a wee bit edgy to a 16-year-old could be very embarrassing a few years later when that same young person is trying to get a job or establish a relationship.
<http://www.blogsafety.com/>

Other Tips:

Credit card fraud - be very careful with your credit card number on the web. DO NOT EVER send it in email or post it in a newsgroup. And DO NOT USE YOUR DEBIT CARD FOR ANYTHING ON THE WEB. That comes directly out of your checking account - you may get it back from the bank if you can prove fraud, but at least with a normal credit card you are risking the banks money and not your own.

Identify Theft - Perhaps the most significant threat on the internet is identify theft. This is simply the stealing of your social security number (and other identifying information) with the intention of using it to obtain credit. Give out your information to the wrong person and you could find your credit rating is destroyed.

Chain Letters

If you've been on the internet for any length of time then you know exactly what I'm talking about when I mention chain letters. If you read newsgroups you will run into them every once in a while. You'll probably get some spam and you may find it posted in message boards. It's all the same junk. Just delete it and continue on with your life. Under no conditions should you respond to these offers or to the email or newsgroup post.

One good rule of thumb to spot a scam artist is "easy money." Most truly legal enterprises don't spend much time trying to convince you they that are legal. As a rule it's a great idea to just ignore anything that is "too good to be true". Some key phrases to look for include:

"You don't think it's possible?"

"Wealth and freedom can, and should, be yours"

"I want to give back."

"These are proven principles that have long been the secret of the rich"

"You have to be serious about..."

"You have to be willing to pay a price."

"Imagine The Possibilities"

Or anything along similar lines. One question I always ask myself is that if this money making scheme was so good why is this person selling it for only \$99 or \$39 or whatever? Wouldn't he be better off doing what he says and make a lot more money?

Before spending a dime always check your local better business bureau.

<http://www.makemoneynow.us/scams-and-cons.htm>

What is Spam?

- Unsolicited emails to a mass audience.
- Cross posting commercial email to multiple newsgroups or email lists
- Internet based telemarketing
- Sending unsolicited messages to chat and instant messaging services
- Attempting to fool search engines through massive or fraudulent submissions.

Two basic rules to follow regarding spam:

1. Everything stated by a spammer is a lie.
2. When in doubt, see rule #1.

You have to understand that you do not know who sent you the message. You have no easy way of checking the validity of the company, it's credentials, or anything else. It's just a way to get you to buy something or send money somewhere, or, occasionally, it's about something worse. Like pyramid schemes (illegal), religious rants, hate missives, or hardcore pornography.

Stopping Spam

What don't you do?

NEVER, EVER respond to the spam (this only confirms to the spammer that your email address is real and someone is looking at the messages). Do not buy anything advertised in a spam message. DO NOT give your credit card data or any other data to a spammer, and do NOT ever ask to be removed from the spammers mailing list (it just confirms to the spammer that you are a valid email address).

Do not directly post your email address in your web site (or any other web site). The reason for this is that many spammers use robots to scan web sites for email addresses.

What can you do?

Purchase a product such as Spamkiller. This product an excellent tool which effectively filters out most spam messages. Write to your legislators to get better laws passed. Complain to the ISP of the spammer.

Filters

Using the filters supplied with virtually all modern email and newsgroup clients, you can seriously cut down on spam and other unwanted messages. However, to be effective, you have to maintain your filters on a regular basis. Here's what I do: whenever I receive an email which is undesirable, I scan it quickly to identify something which would identify it. This might be the FROM address, the SUBJECT (some or all of it) or various phrases within the message body. If the FROM address is strange (which it often is in spam messages), then it's better to key off the subject or text body. These identifiers are then added to my filters. In other words, I tell the email client "if you see this phrase in the message body, then please automatically delete the message.

Note that you must be careful that the phrases are specific to the type of message you want to delete. Otherwise, you will wind up deleting messages which you actually want to receive. For example, let's say a common phrase is "sex movies for sale". You should add the whole phrase to your filter, not a short word like "sale" which could unintentionally delete messages about other things.

Note that your filter should move the messages to the trash, and you should always take a quick scan of the messages in your email trash can before deleting. This will help prevent you from accidentally deleting a valid message. Filters are not perfect.

Some good phrases to add to your filters are: *(Make sure that phrases are allowed, otherwise it will block every email with ANY word filtered.)*

- Click here to be removed.
- bulk e-mail
- bulk e mail
- MLM
- multilevel
- I just found your address by searching through
- adult
- adults only
- If you are under 21
- This is a one-time mailing
- This is not a spam
- million dollars
- senate.gov
- Section 301, Paragraph (a)(2)(C) of S. 1618
- Bill 1618 Title III
- Since your email address was listed on a related Web site...
- Claim your prize

Once you've spent some time creating a few filters, you will begin to realize the power at your fingertips. Using the filtering components of products such as Outlook and Outlook express, you can automatically file emails in specific folders, forward them without your intervention and of course delete spam. Have fun and use these to help improve your productivity.

To prevent spam, it's wise to simply not include your email address anywhere on any web site. If you must post an email address, be sure it's not your primary address (in fact, a throw-away free email address is perfect for this purpose). If you must post your real address, you can hide it by using forms or by placing the email address in a graphic image).

You can spell out parts of the email address if you like. This is a common practice in messages posted to newsgroups and such, but it is not so well known on the web. For example, you could say "my email address is 'tom at anyolddomain dot com'".

Likewise, if you've signed guestbooks, then the same email spiders can get your address from them. Many spammers specifically program their harvesters to look for email address-rich guestbooks.

Perhaps you like to sign up for free stuff or newsletters? If so, it's likely that at least one of them either was a spammer, or sold your email address to one. Again, it's a great idea to use one of those free email accounts to sign up for newsletters and free stuff.

A friend of yours may have sent an email to a list using "cc:" instead of "bcc:". This basically hands all of the email addresses in the "cc:" to everyone on the list. To prevent this, you need to educate your friends on the use of "Bcc:".

Internet listings - You may be listed in one or more of the various internet white or yellow pages. It's a good idea to check these once in a while and delete your email address when you find it.

Newsgroups - If you've posted to newsgroups with your real email address, then you've simply given it away. This is one of the spammers favorite places to get new email addresses. What they do is harvest email addresses by the thousands using automated software especially designed for this purpose. To make it even worse, newsgroup postings are available forever (especially now that they are supported by Google), which means even one posting leaves your address exposed to the world._

AOL Profiles - A rich source of email addresses is from AOL (and other) profiles. These are very easy to access and it's extremely common for spammers to attempt to do so.

Message Board Profiles - Be careful when entering your email address on message boards, especially in the profile. These can be retrieved by email harvesting programs. If you must include a publicly available email address, then either use a filtered account (such as spamcop.net) or a throw-away free email account._

IRC and chat rooms - It's pretty straightforward for spammers to harvest email addresses from IRC (a form of chat room) and AOL chat rooms. Use throw-away email addresses for use only when chatting - never use your primary email address.
<http://www.mailmsg.com/SPAM.htm>

What Should I Do To Secure My Home Computer?

Task 1 - Install and Use Anti-Virus Programs

Task 2 - Keep Your System Patched

Task 3 - Use Care When Reading Email with Attachments

Task 4 - Install and Use a Firewall Program

Task 5 - Make Backups of Important Files and Folders

Task 6 - Use Strong Passwords

Task 7 - Use Care When Downloading and Installing Programs

Task 8 - Install and Use a Hardware Firewall

Task 9 - Install and Use a File Encryption Program and Access Controls

<http://www.cert.org/homeusers/HomeComputerSecurity/>