



Internet Safety for Parents

With the exponential growth of the Internet and with more children going online at a younger age there is a need in Seneca County for parental awareness on the dangers associated with the Internet. Below are some tips, terms, and information to help you protect your children and yourself on the Internet.

Parenting Tips:

- Keep the computer in an open area – Adults should monitor what children are accessing with the computer.
- Beware of all requests for your personal identification online – Never give out personal information unless you initiate the correspondence.
- Respect your child's privacy – Respect your child's privacy, but make certain they know personally everyone on their e-mail "buddy" list. Work to generate parent and child trust that supports open and honest Internet use.
- Delete unsolicited attachments – Viruses and worms are activated by opening an infected e-mail attachment. Use updated anti-virus software, install a firewall, and regularly monitor your computer.
- Know intellectual property and copyright regulations – Using file-sharing programs for downloading music can open up your computer to identity thieves by giving access to your personal information. Downloading music and movies without paying for it is illegal.
- Be a part of your child's online experience – It can be a fun journey to explore the wonders of the Internet as a family.

Eluding Internet Predators:

- Keep usernames and profiles generic and anonymous – Discuss your child's online screen name(s), profile(s), and activities. Many provide too much information. Ensure all screen names and profiles are non-specific and purposely vague.
- Avoid posting personal photos – Pictures can be altered to embarrass or humiliate. They also provide personal information that can help an Internet predator to pretend to know you, your children, and/or their friends.

- Always keep private information private – With just three pieces of personal information, specialized Internet search engines can be used to locate someone anywhere. Internet conversations should never include any personal information.

Cyber Bullying Awareness Tips:

- Don't open/read messages from cyber bullies – Your child can't be intimidated by messages from cyber bullies they never open. Teach your child to curb his or her curiosity to read and respond to a message if they suspect or know a cyber bully has sent.
- Encourage your child to tell an adult – For some children, their reaction to being bullied is not only fright, but also confusion about how to react appropriately.
- Report cyber bullying – Internet Service Providers (ISPs) can often block a cyber bully, and schools have specific procedures and rules to handle bullying. Save the bully's message and screen name, then contact and report it.
- No chatting while angry – Sending angry, hostile or taunting messages attracts cyber bullies. Make certain your child is not using e-mail messages or chat rooms to vent their own anger in a way that hurts others.
- If you are threatened with harm, tell the police – Even if you don't know how to identify the individual who has made the threat, law enforcement often has access to the information and may be able to track down and arrest them before they do more harm.

Internet Terms:

Anti-virus	Software that protects a computer from malicious code.
Attachment	A data file sent from one computer to another along with an e-mail or an instant message.
Buddy List	Instant message addresses of favorite users.
Bulletin Boards	Message boards, public areas on the Internet where messages or comments can be posted for other board members to read and reply to.
Chat Room	A virtual room or gathering place, for Internet users with shared interests to congregate and converse.
Cyberspace	Virtual Internet community in which real people interact through electronic means.
Grooming	Process that online predators use to build false trust in order to meet them face to face.

Download	To copy information (data) from the Internet.
Flame	To send a mean or hurtful electronic message.
FW	Forward – informs the recipient a redirected message has been sent to them. The sender is not the author and, therefore, is suspicious.
Firewall	Set of related hardware and software programs designed specifically to protect a computer or computer network from unauthorized external use.
Hacker	A person who uses the Internet to break into a computer or computer network.
Identity Theft	When someone uses your personal information (e.g. Social Security #, credit card #) to steal your identity for illegal purposes.
IM	Instant messaging – real time Internet communication. A private “chat room.”
Looping	Website code that does not allow a visitor to exit. Feature of many adult Internet sites.
Malicious Code	Intentionally destructive computer program (e.g. viruses, worms, and Trojan horses)
Parental Controls	Special features or software packages that enable restrict access to Internet sites.
Phishing	Phishing attacks use “spoofed” e-mails and fraudulent websites designed to fool recipients into divulging personal financial data.
Piracy	Theft to produce counterfeit copyrighted software and other material.
Posting	Placing a message or photo to an online message board or website.
Screen Name	Online name or nickname. An alias used in Cyberspace.
SPAM	Mass mailing or posting of messages. Also known as Internet junk mail.
Spoofs/Spoofing	Fake e-mail messages or web pages mimicking those of legitimate businesses in order to trick you into providing personal information.
Trojan Horse	A malicious code that appears harmless yet launches a virus or worm.

Chat Abbreviations:

AFAIK = As far as I know
AFK = Away from keyboard
ASAP = As soon as possible
BBL = Be back later
BBS = Be back soon
BF = Boyfriend
BRB = Be right back
BTW = By the way
CYA = See you
CYAL8R = See you later
EMSG = E-mail message
FYI = For your information
GF = Girlfriend
GFN = Gone for now
H&K = Hug and kiss
IC = I see
IMO = In my opinion
JMO = Just my opinion
KIT = Keep in touch
L8R = Later
LOL = Laughing out loud
LTNS = Long time no see
LTS = Laughing to self
LY = Love ya
MTF = More to follow
NRN = No reply necessary
OL = Old lady (significant other)
OM = Old man (significant other)
PM = Private Message
QSL = Reply
QSO = Conversation
QT = Cutie
SO = Significant other
SOT = Short of time
SWL = Screaming with laughter
SYS = See you soon
TA = Thanks again
TNT = Till next time
TOY = Thinking of you
TTFN = Ta ta for now
TTYL = Talk to you later
WB = Welcome Back

Emoticons:

Hugs and Kisses:

:* kisses
:-X a big wet kiss!
:-x kiss kiss
:--{ } blowing a kiss

Happy, Smiling, Laughing:

:-) smiling; agreeing
:-D laughing
l-) hee hee
;-) so happy, I'm crying

Teasing, Mischievous:

;-) winking; just kidding
;-> devilish wink
:*) clowning
:-T keeping a straight face

Affirming, Supporting:

:^D Great! I like it!
;-o Wow!
^5 High five

Unhappy, Sad:

:-(Frowning; boo hoo
:-C Really bummed
&-l Tearful
:'-(- Crying and really sad

Angry, Sarcastic:

>:-< Angry
:-ll Angry
:-V Shouting
:-r Sticking tongue out
:-l indifferent
\-o bored

The Dangers

Predators

The biggest danger by-far is the possibility of predators targeting your children while they are online. Predators sometimes pose as children and will be-friend your child. They attempt to gain your child's confidence and will instruct them to be secretive about the relationship. A young impressionable child is almost no match against these devious people.

Pornography

Another danger is that your child may accidentally run into pornography. There are many very graphic images on the Internet that are readily available and easily found. Also there are messages of hate that are readily available.

Financial Theft

Passwords to your Internet service provider and passwords to user accounts on Websites are like keys to your house and blank checks.

Information About You

Did you know that with just a couple of bits of information someone can search and obtain your full name, address, telephone number and directions to your house?

Now that we have reviewed what the dangers are, let's dig into learning about how to protect yourself.

Although there is no substitute for you being right there while your child is online, filtering software can help.

Filtering Software

Selecting filtering software can be confusing. There are many programs and they have many different features. The features that you need will depend on what you are trying to do with the program.

Are you trying to catch someone in a lie? Do you want to stop pornography from being displayed? Do you want to limit the time your kids can be online? The answers to these questions will help you decide what type of program to select.

Programs operate in different ways. Some require you to download a list of sites that are not acceptable while some scan the page for unacceptable words before it is downloaded. Here are categories of how they work:

Acceptable Sites - You enter a list of acceptable sites and only those sites can be visited.

Activity Logs - Creates a list of activities that were done on the computer.

Monitoring - Creates pictures of the activity on your computer that you can look at.

Server-based List - Logs onto their server to check to see if a site is excluded.

Downloaded List - You download updates and the software checks to see if a site is excluded.

Internet Service Provider - You dial into the Internet Service Provider instead of using the one you currently use.

Snooping On Your Kids

If your child has been spending a lot of time on the Internet lately, you may want to check up on their activity. You may feel as though it is spying, but checking what they have been viewing may avoid further problems, by talking to them about what they have seen. Or, perhaps they ran across something that made them feel uncomfortable and they feel uncomfortable telling you about it. A couple of minutes spent viewing the history of your browser will tell you what kind of sites your child has been viewing. Please be aware though, that a child can clear the history of sites visited.

If you use Internet Explorer or Netscape you can view your browser's history and adjust how many days are kept in the history. Another nice feature is that you can clear your browser's history, which will sometimes speed up how fast your browser loads new pages.

Here are instructions to view the history, adjust the number of days kept in history, and clear the history.

For Internet Explorer

- **To view the history:**
There is a history button on the top, or you can click on "View" then "Explorer Bar" then "History"
- **To adjust the number of days kept in the history:**
Click on "View" then "Internet Options" then use the up or down arrow in the history section to adjust the number of days.
- **To clear history:**
Click on "View" then "Internet Options" then click on "Clear History" button in the history section.

If you use a different version browser or a different browser altogether, use the help option to find out if history is available and how to access it.

If your child has started clearing the history file, this should send a signal to start monitoring more closely. There are monitoring programs available that you can install.

Now that you know all about filtering software, let's learn about the dangers of email and how to keep safe while using it.

Email Safety

Email is a fun, cost efficient way to communicate with family and friends. One of the biggest misunderstandings about email is that email is like sending a postcard through the mail. Anyone can read it along the way. Your message is not secure.

Important information, such as your full name, address, phone number and passwords should not be shared through email. It is unlikely that your email would be high-jacked and used for malicious purposes, but it never hurts to play it on the safe side. Also, it sets a good example for the children.

Did you know that when you sign up with an Internet service provider, they may instruct you to have your first and last name substituted for your email address? Most people don't even realize that their full name is being sent out with every email.

This may be fine for businesses but it may present a security risk for your family. Find out if you are giving out your name and how to change it.

Email Settings

Do you give out your entire first and last name every time you send an email? Check what name that appears in the "from box" when you send an email. Do you really want a stranger that you don't know having that much information about you? If someone knows your first and last name and the state that you live in, chances are they could come knocking on your door. To avoid this problem, don't give out your last name. Here are the instructions to change the name your email client automatically provides when you send an email.

If you use a different email program, than these below, to get your email, call your Internet Service Provider. They should be happy to help you with this.

Outlook Express Users

- Open Outlook Express
- On the menu across the top, click on "Tools"
- Then click on "Accounts"
- Select "Mail Tab"
- Click on the email account you would like change
- Then "Properties"
- Under the General tab, User Information, you can Change the User Name
- If you are using an older version of this email client, you can search the help option for "Accounts, change settings for" or call your Internet Service Provider.

Netscape Mail Users

- Open the Netscape Message Center
- On the menu across the top, click on "Edit"
- Then on "Preferences"
- If necessary, click on the + sign next to "mail & groups" on the left hand side
- Click on "identity" under the "mail & groups"
- Change "your name" on the right hand side
- If you are using a different version, search help for the word "identity" or call your Internet Service Provider.

Eudora Light Users

- Open Eudora Light
- Select "Tool" on the menu at the top
- Then "Options"
- On the left hand side, select "Personal Info"
- Change the information in the "Real Name" field

- For different versions of this program search the help option for "real name" or contact your Internet Service Provider.

Now that you are not giving out your name with every email, let's concentrate on the kids! Most kids want their own email address! There is a safe email address and program that you can give them!

Safe Email for Kids

There really isn't a way to make sure email is safe for kids. They can communicate with any one online if they have an email address.

One suggestion to make it safer is to filters in your email program to filter there messages directly to a folder and instruct the child only to view messages in that folder. You will need to create message rules that take a message from a certain person and send it to their folder.

Chatting

Chatting can be a lot of fun and educational also. You can meet and talk to people from all over the world. Often you can learn about different cultures. I have been fortunate to chat with people from China, Australia, England, Pakistan, Paraguay, Jamaica and other far away lands. From these conversations, I have been able to gain a different perspective of other points of view.

Chatting can have a down-side though. People aren't always truthful in chat. You must take everything you read with a grain of salt. Also, chat rooms are one of the favorite hang-outs of predators. You have to be on your toes.

Before you jump into chatting, you should learn what chatting is all about!

First Time Chatting

Chatting can be a lot of fun and it is easy. It is especially entertaining after you have spent a long day with the kids, just to have some grown up conversation. You get to meet interesting people from all over the world. For most people, their first time chatting is an almost scary experience. You hear about obnoxious users so you might be afraid to try it. After all, no one wants to go somewhere for fun and get verbally abused. Then, when you try it, you just do not know what to say and everyone is writing in shorthand with abbreviations, so you don't even understand half of what is being said. Just remember, everyone in that room had a first time experience and almost everyone will help guide you. Here are some suggestions to make your first time chatting experience fun and easy! For you old pros, you can brush up your chatting skills!

There really are not that many obnoxious people in chat rooms.

At About.com chat rooms, you can ignore them, simply by clicking on the obnoxious user's name, the click on the ignore user box. Also, if the ADM is in the room, he or she has the power to expel the obnoxious user out of the room. So do

not let the fear of obnoxious users stop you. Almost everyone voluntarily follows chatting etiquette. Follow the rules of common courtesy just like you would in real life.

Sometimes, knowing what to say when you enter a chat room is hard! After the initial hello is over and where everyone is from has been discussed, silence may follow. When this happens, ask a question or you can share a funny story that happened to you. For instance a good question to ask is, "does anyone have any kids?" or "what hobbies is everyone interested in?" More good advice is available about striking up the right conversation. Before you know it, the conversation will start to flow.

To be chat savvy, there is just a few abbreviations you will need to know. For instance, a very common abbreviation is "LOL" that stands for Laughing Out Loud. You type this in when you find something funny or you are writing something that is meant to be funny. This helps a lot because when you type something, rather than then say it, someone else can't see your face or hear the tone of your voice, so they don't realize you are kidding around. If you have to leave to go get a drink or answer the phone, type in "brb" (be right back). That way, someone that has a question for you will wait, until you let them know that you are back. Another source of abbreviations used in chat is express yourself in your email and chat. If you see an abbreviation you don't understand, just ask! I am sure the person that wrote it will be glad to explain it.

Chatting is very entertaining. There are usually many laughs and I am sure you have heard the saying; laughter is the medicine for anything that may ail you. Don't be shy come join us! Before you know it, you will be an old pro at chatting and a part of the global community, with friends all over the world! Relax and enjoy!

The kids will want to have fun too! Should you let them chat?

Chatting Safety

Kid's love to chat! Chatting can be dangerous. However, the kids can have a lot of fun if they are aware of the dangers and know how to protect themselves.

Safety must be discussed before allowing your kids to go to a chat room! If they are already chatting, daily safety reminders are in order. Here are a few points to consider.

- **They must not give their real name and location, under any circumstances!** Instruct them to use a nickname. Other chatters will ask where they are located. Tell them to say the state name. Often, someone else will be from that state and they will ask them what city. Talk about this ahead of time. They could say, "I am from the northeast part of the state." If someone persists with asking the exact location, tell them it is all right to say, "My mom does not want to me to tell."
- **Make it clear they are not to meet anyone they talk to online.** For safety sake, they should not meet anyone they talk to in chat unless you arrange it and you are there. Often predators will try to meet the child.

- **Not everyone your child will be meeting is actually who they say they are.** Remind your child that anyone can say they are 12 and from Hawaii! Unfortunately, children are gullible and will believe just about anything. Remind them constantly that their 12-year-old friend may actually be a 40-year-old person with very bad intentions.
- **Will private chat will be allowed?** Often in a busy room, other chatters will ask your child if they want to private chat. This can be dangerous, but mainly it is innocent. The dangers are if the person is a predator, they can gain your child's confidence in private chat.
- **Should you allow your child to give out their email address to their chat buddies?** If you do allow this consider getting them their own free email address. Only allow them to give out their email address in private chat. Do not allow them to post it publicly. Monitor their mail! It is for their own protection. If you start to become suspicious of someone, change the child's email address to another.
- **Will you only allow them to enter monitored chat rooms?** This will not assure their safety, but it does afford some protection. A monitor has no way of knowing if the person that says he is 12, actually is. In some monitored chat rooms, the monitor cannot monitor private chat. The best monitor is you, sitting with your child at the computer and watching everything that they are saying! At the minimum, it is a good idea to check on the conversation often.
- **Remind them to use their manners!** Just as they would use manners in a classroom, they should use their manners in a chat room. Offenders can lose their ISP privileges if a major offense occurs.

Be sure to learn about chatting before you try it! Good resources are available that will fill you in on the lingo of chat.

Family Friendly Searching

One of the worst places to send a kid on the Web is a search engine. They search for something innocent, like "girl sites" and the results can be quite shocking. Search engines have realized that families need options to get results without unwanted, offensive material.

A couple of the major search engines have added an optional family filter. You have to make sure it is turned on before starting your search, by setting the options. When you do this, each time you go back the filter will be active. Altavista has a family filter option that is a little confusing to operate. Initially I thought I had the family filter on, and I didn't. When you open Altavista it does not show if you have the family filter on until you actually do a search, but once you initiate the filter it will be on every time you go there.

Go Network clearly shows that you have the Go Guardian feature on, when you go back to the site after leaving.

To alleviate looking whether or not you have the filter on, going directly to a search engine that is only family friendly is easier, especially for children. Ask Jeeves for

Kids is a good option and it is simple for any child to use. Instead of searching for terms, all they have to do is enter a question. It also has a spell check option for their question. Another place to search is KidsClick. You can search through sites that have been hand picked by librarians.

Another option is to use directories, such as About.com. Instead of searching, you go to the category you want information about. For instance, if you want information about Barbie dolls, you would go to the main page, select "hobbies", then click on "collecting", and then choose "Doll Collecting". By using directories, you control what comes on your screen. Several search engines also offer directory options to locate what you are looking for.

With so many sites available, it can be a very difficult task to find the information you are looking for, quickly and easily. One of the biggest problems with search engines is that they return irrelevant results. Search engines are trying to remedy this problem, but in the meantime, at least you can filter out the offensive material.

Often children see Website addresses on television and want to visit. Great! The Internet is a great interactive compliment to television. There is a problem with this though. Many cyber-squatters have registered address that are close to popular sites. The worst part of the cyber-squatter problem, is that they have pornography on their sites. The purpose is to hold up the company for money. Here is how to protect yourself from this practice.

Typing URLs

Typing in a URL can lead to an unwanted surprise. URL stands for Uniform Resource Locator or Webpage address. Several pornographic sites prey on typing errors, and not knowing what the actually domain extension is. They may do this because they get more money from advertising, they just like to shock you, or perhaps it is just coincidence. Whatever the reason is that this happens, it does. Learn how to protect yourself from these unwanted surprises.

A popular site among teenage girls is <http://www.gurl.com>. They offer free email, advice columns and is really a great site. If someone verbally told a young lady about this site, they may type in <http://www.girl.com> and they would reach a pornographic site. There are many more of these pornographic sites that have close spellings to children's sites.

This is in no way the company's fault. Whoever buys a domain name owns exclusive rights to it.

A common way for a site to obtain traffic is to use a popular name and then use .net, .org, or .com equivalent. For instance, <http://www.whitehouse.gov> will bring you to the United State's White House where you can learn more about President Clinton and other Presidents. Make the error of typing in <http://www.whitehouse.com> and you will be brought to a pornographic site with no warning page. Whitehouse.com even brags that it has been mentioned on many networks news broadcasts. Whitehouse.org is also a pornographic site, but at least they have a warning page that you must be over the age of 18 to enter. Whitehouse.net is a parody site of the whitehouse.gov site. This site does not have any advertising on it, but is very

misleading because the page looks very similar to the real White House. This happened because the United States government did not have the fore-thought to buy those domain names, before someone else did. Once someone buys a domain name, they may sell it, but they name the price.

So what do you do to protect yourself? First of all, consider a filtered Internet Service Provider or filtering software. If this does not appeal to you, instruct your children not to type URLs. Have them use a portal site, like an About.com kid's site to surf from. Consider using a kid safe search engine like Ask Jeeves for Kids. Finally if someone sends a non-clickable link by email, learn how to copy and paste it, without retyping the entire URL without the chances of a typo.

I have been told that school children have had their Internet privileges revoked because they have reached pornographic sites accidentally by typing wrong URLs. Arming yourself with knowledge that these exist and how to protect yourself is more than half the battle. Make your Internet experience much richer without embarrassing yourself or your children, and do not make these pornographic sites more popular.

Now you know how to find what you need safely! Fantastic! Next, let's talk about protecting your identity.

Protecting Your Identity

How easily can you be found? Do you realize that if you have a listed telephone number, chances are, anyone can get directions to your home, with just a few keystrokes? Try using an Internet telephone and address finder, like InfoSpace or Switchboard to see if you are listed. If you are concerned with identity theft, your personal safety, and not getting junk mail, you will want to take action. Most likely you will not be able to completely unlist yourself in the information age, but you can remove yourself from address finders and make sure that your name will not find it's way back to these directories. [HR] Let's get unlisted!

Family Use Agreement

Internet safety is important for your family's security. Many schools, libraries, and other places have established user agreements, so that the rules are not misunderstood. Why not establish a set of rules in your house? (And it isn't just for the kids, mom and dad!) Setting an example for your children to follow is very important.

Setting rules, clearly listing them, then following the rules, will make an impression with your children that safety is important. Let them know that you care and you want them to be safe. Make a big deal about it! The computer is a powerful tool in your home, but used unwisely, it can be very dangerous. You are given a driver's license as an agreement that you would operate a car safely, because a car can be just as dangerous as it can be helpful. Make a family rule that you will use the computer wisely so no one gets hurt.

What Can You Do To Help?

There are many evils around the world and online too. If you witnessed a bank robbery, you probably would report it. The same should hold true when you are online.

First you need to be able to identify what is legal and what is illegal. Clearly child pornography is illegal and absolutely should be reported. If you ran across child pornography, would you know where to report it?

Another way that you can help is to turn in spammers. You probably have gotten those annoying unsolicited emails and just clicked on the delete key. But, what about the thousand's of these messages that are being sent, that are clogging up the Internet?

First we will concentrate on reporting child pornography because there is a proper way to report it.

Reporting Child Pornography

What if you found child pornography by accident? What would you do? For the sake of all children you should turn it in! It is confusing though were to actually report it. You may feel as though you do not want to get involved.

There may be a fear that since you technically downloaded it to your computer you could get into trouble. Do not worry about accidentally running into child pornography. You would get into trouble if you download it and then send it to someone else. When you report it, just transmit the address where you found it to the appropriate agencies.

- **Cyber Angels**
Cyber Angels is a division of the well known, Guardian Angels. They have a program where you can report cyber-crime to their Cyber911 email address.
- **National Center For Missing and Exploited Children**
You can contact them either through their website, or by calling their 24-hour hotline. (1-800-843-5678)
- **Your Local Police Department**
Do not hesitate to call your police department. Most police departments are trained to handle online investigations and they take them seriously.
- **Your Internet Service Provider**
Your ISP will know what to do if you are in doubt. Do not hesitate to contact them also.

If you have been threatened online or if you think a predator may be trying to gain your child's confidence, you should report this too to the above agencies.

Another thing that may or may not be illegal is spam email. Spam clogs up the Internet for all of us, so instead of just deleting it, let's stop it.