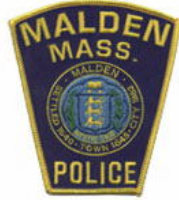


Internet Safety Tips for Parents and Kids



Malden Police Department

200 Pleasant Street
Malden, MA 02148
781-397-7171

Internet Guidelines for Children (10 years old and younger)

- Never give your name, address or phone number to anyone on the internet.
- Do not go into chat rooms without your parent's help.
- If you get a message that makes you feel uncomfortable, don't respond to it, and be sure to tell your parents.
- Don't join a mailing list without your parent's permission.
- Don't open e-mail from anyone you don't know. It might be a virus which could damage your computer.
- Don't believe everything people on the internet tell you. Since you can't see the other person, you don't know who they really are.
- Never agree to buy or trade anything on the internet without your parent's permission.
- Never agree to meet anyone you met on the internet, and never send pictures of yourself over the internet.

Internet Guidelines for Teenagers

- Never give out your personal information, your real name, address, or phone number, or any personal information about your family or friends without their permission.
- Be careful in chat rooms. Don't get involved in fights or use obscene language. You could be reported and have your internet service suspended or cancelled.
- If you are in a chat room and someone makes you feel uncomfortable, attempts to start a fight with you, or uses offensive language, leave the room.
- Ignore obscene or offensive messages. Replying may cause the sender to continue to send such messages.
- Be careful in joining mailing lists, some may make your personal information public. Don't provide an address or phone number. The information for which you are signing up is sent to the e-mail address you provide, so they don't need your address or phone number.
- Beware of offers for free items, get rich quick, or weight loss offers. They may be a scam.
- Beware of e-mail from people you don't know or e-mail you weren't expecting. It may contain a virus designed to damage your computer or send your account name and password back to the sender.
- Never send your picture to someone you don't know or trust. Remember, the internet allows people to become anyone they want to be, and they may be someone you don't really want to know.

Internet Guidelines for Parents and Guardians

- Place the computer in a common area of the residence rather than a bedroom. This will encourage online time to be a family oriented activity.
- Become familiar with the people and web sites your children are interacting with on the internet, just as you would get to know all of their other friends.
- Choose a family oriented Internet Service Provider or Online Service and use Parental Controls or software to regulate the type of information and material your children can access on the Internet. Most of the Parental Controls and software allow adults to restrict access to age appropriate levels. In the event the children do receive objectionable material, teach them to avoid responding to

messages that are suggestive, obscene, threatening or makes them feel uncomfortable. Make sure they are comfortable in making you aware of these types of messages. Immediately notify your Internet Service Provider of the receipt of such material.

- Try to select non-descriptive Account Names and Screen Names for your children. Their online names should not be too specific or identify or describe them in detail.
- Remind your children not to provide their real name, phone number, address, or other personal information to anyone to whom they meet online, and never to meet face to face with anyone they have met through the internet without your permission. If you do permit such a meeting, it should be in a public place and that you or another responsible adult should accompany your child.
- Set reasonable guidelines for your children's time online and remember that the computer should not be thought of as a "babysitter". The guidelines should be age appropriate. Remember, what is acceptable for a teenager may not be acceptable for a younger child.
- Remind your children that the rules are the same for any computer they use, whether at home, a friend's house, school, or the public library.
- Assure your children that they can talk with you about things that happen on the internet. If they fear that they will lose their internet access, they may be reluctant to talk about anything bad that happened on the internet.
- Utilize Parental Controls provided by your Internet Service Provider. Check with your provider directly to determine availability and usage.
- Educate yourself about Internet safety for both children and adults at any of the many online sites such as:
 - <http://www.staysafe.org/> Information for kids, teens, parents, 50+ and more.
 - <http://www.isafe.org/> i-SAFE is a non-profit foundation whose mission is to educate and empower youth to make their Internet experiences safe and responsible.
 - <http://www.safekids.com/>
 - <http://www.safeteens.com/>
 - <http://www.fbi.gov/publications/pguide/pguidee.htm> FBI's "A Parent's Guide to Internet Safety"
 - http://www.wiredkids.org/wiredkids_org.html Information for children of all ages, parents, educators, etc.
 - <http://www.missingkids.com/> Good resource for Internet safety as well as child molestation prevention, etc.
 - <http://www.netsmartz.org/> Provided by National Center for Missing & Exploited Children

About Internet Scams and Identity Theft and Other Scams

- Be constantly wary of online scams, identity theft, personal information scams known as "phishing," spyware, and hoaxes*. Trustworthy sites such as those below provide a wealth of information:
 - <http://onguardonline.gov/index.html> Provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information. Especially relevant are their [Stop-Think-Click](#) tips.
 - <http://www.scambusters.org/index.html> Scams, phishing, identity theft, and much more.
 - <http://hoaxbusters.ciac.org/> U.S. Dept. of Energy's Computer Incident Advisory Capability (CIAC) provides hoax information.
 - www.symantec.com/avcenter/hoax.html Hoax information.
 - <http://www.consumer.gov/idtheft/> Federal Trade Commission Identity Theft information.
- Nine Tips To Protect Internet Shoppers From Fraud

1. Make sure the company name, physical address, and telephone number is posted on the web site. If not, do not purchase from that web site. The company could be located in Cuba for all you know. Adopt this rule: "If you can't find them, then don't do business with them."

2. Never give your social security number or date of birth over the Internet. If your date of birth is required to purchase or participate like in the case of a dating service, lie about it or don't buy. For the dating service provide a false month and day you were born, but use the correct year so that your prospects will not feel deceived about your age. Never lie to a law enforcement official even on the Internet. Police have a right to ask you to identify yourself. But don't give out your personal information to anyone that you don't know, other than a law enforcement official. Always make certain that you are talking to a real law enforcement official before you give out your DOB. Ask him to identify himself.

Check on him by calling the number he or she provides.

3. Sign up for one of the credit notification and protection services offered by the three largest credit reporting agencies.

4. Contact any ONE of the three major credit reporting agencies and have a security watch placed on your account. Make things difficult for anyone attempting to obtain your identity (social security number or date of birth) through a credit report without your knowledge or consent. People are getting private information on you right now through credit reports without you even knowing about it. The faster you stop them the safer you will be.

5. Be careful of all e-mail offers. If you "Click Here" make certain that doing so has directed you to the real web site of the company. For example, you may receive an e-mail requesting that you update your account information at E-Bay. Hackers use this trick to steal your user names and passwords. They direct you to a site that looks just like E-Bay. But that is not the real URL for the real E-Bay. The real address for E-Bay is [HTTP://www.ebay.com](http://www.ebay.com). Notice the thieves add extra letters to the web address.

6. Remember that people who do NOT use the Internet are victims of identity theft too. For example, recently a computer was stolen with all the private information of American veterans. Most of the veterans never made an Internet purchase. Their private information was stored on a computer so it is vulnerable to theft from the Internet or from within the an office like Veterans Affairs. Because people who do not use the Internet much so not know the tricks that thieves employ, they are more likely to become victims of identity theft.

7. Keep in mind that your credit card is not all that the Internet thief wants today. He knows that if he uses your credit card he most likely will get caught because you will know about it soon. Today it's your identity (social security number and date of birth) that the contemporary thief really wants. He wants to use your identify to apply for credit in your name, without your knowledge or consent. You need technology to catch him.

8. Look for the Better Business Bureau seal. The seal must be a hot link direct to the BBB. If there is no hot link to the BBB, or you are directed to another web site other than the official BBB site, there is a good chance the seal has been stolen and the merchant is not a member of the BBB.

9. Do not store your identity on your home computer if it is connected to the Internet. Store private information on a flash drive and remove the drive when not in use. Use a personal firewall at all times.

*Hoaxes may appear relatively harmless but the cost and risk associated is multiplied by millions of individuals propagating hoax e-mail. Costs involve wasted time and e-mail server processing resources, which may slow down to a crawl or crash under the heavy load. Spammers (bulk mailers of unsolicited mail) harvest e-mail addresses from hoaxes and chain letters.