



## Virus Protection

**Virus, worms, Trojans, spyware, and adware** are malicious code that could invade your computer, especially if you have an “always on” broadband connection. Malicious code can spread through all different types of computer medium: e-mail, floppy disks, instant messages, file-sharing services, pop-ups, etc.

### What You Need to Know

Keeping your computer software up-to-date is the best defense. Verify that Windows Update is running automatically and regularly. Install virus and spyware protection and keep them current. Fairfax County Public Schools provides antivirus software for home use by current faculty, staff, and students. The software may be checked out from each school’s library.

Be careful with e-mail attachments. Check with the sender and scan it before opening.

Use a firewall at home to protect your computer from possible intrusions.

## Afterthought

A little common sense goes a long way in minimizing the risks online. Keep in mind that no amount of tips can replace good parenting. A trusting relationship, open communication, shared family time—just “old fashioned” family bonding will help you guide your child through a trouble-free youth, on or off-line.

[www.isafe.org/fcps](http://www.isafe.org/fcps)



## Online Safety: Social Networking, Chat, IM, and Others

### According to an i-SAFE survey:

- One in five children has been solicited by a pedophile in a chat room
- 20% of students in grades 5-12 have met in person with someone they originally met online, but only 3% of parents believe their children have done so.

Many children are unaware of these dangers and act recklessly online: making their profile public, sharing details of their lives, posting provocative language and images...

### What You Need to Know

Talk to your child about the potential dangers on the Internet. Help your child to develop a proper screen name and online profile. Insist that your child share this information with you. Screen names and profiles are public information and should be kept generic and anonymous. Personal information is often revealed unintentionally, in one’s screen name and profile, which can attract online predators. For example, “depressed16” would be a bad screen name because it gives out your age and publishes your vulnerability.

Teach your child how to respond to specific questions. If you talk in general terms, your child may not get your message. Instead, set up guidelines on what specific information should or should not be given. For example, if asked about their location, the child can say “near DC” since DC is a large city. But they should not mention the name of their town, school, or neighborhood. Instruct your

child not to give out a particular time or location of their activities.

Put your child’s computer in an open area where you can monitor their online activities. Set up guidelines for computer usage.

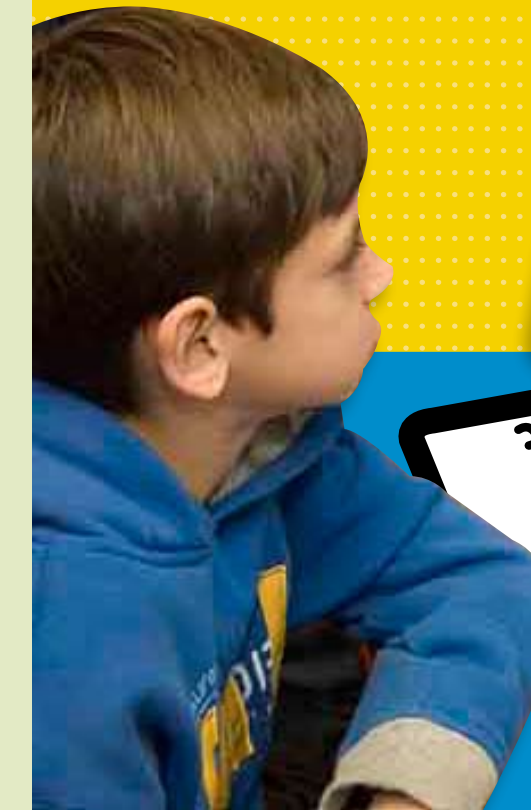
How to respond if there is a problem:

- First, make sure your child knows to come to you with anything they find uncomfortable on the Internet, whether it is the language used in the conversation, a request for personal contact information (i.e. e-mail address, phone number), or anything else that does not feel quite right.
- Collect as much evidence as possible—save the e-mail, log the content of the conversation, record the “friend’s” profile and contact information. If anything makes you uncomfortable on the Internet, call the police.



# Online Safety

for You and Your Children





## Internet Safety Basics for Parents

**There is no doubt that the Internet** has become an important part of our lives, and an even bigger part of our children's lives. While we enjoy the expanded horizon this wonderful new technology has created, we need to educate ourselves regarding safe online behaviors and practices. This brochure provides information on the five most common Internet safety issues: identity theft, spam and phishing e-mail, computer viruses, online safety, and cyber bullying.



## Identity Theft

**Identity theft occurs when** someone uses your personal information (i.e. name, Social Security Number, credit card number) to commit fraud or crime. Identity theft is the fastest growing crime in the United States.

### What You Need to Know

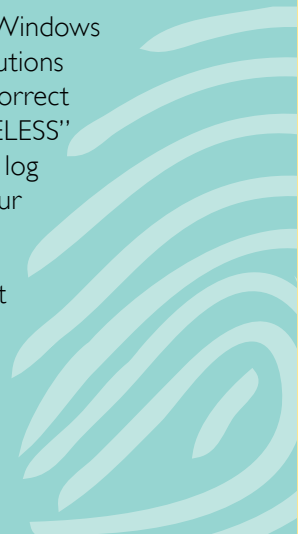
Never reveal your personal information in public forums such as in a chat room, bulletin board, or in your online profile.

Do not respond to unsolicited e-mails, pop-up ads, or any other request for your personal information that you do not anticipate and can not positively verify.

Protect your password. Avoid the obvious. Use a combination of characters, letters, special characters, or a password phrase which is hard to crack and easy to remember, for example, "Blast Off!!!" or "U Not Listening."

If you have to work in a public area, turn on the Windows firewall to fend off possible intruders. Take precautions to verify that you are actually connecting to the correct access point. Do you know "wireless" and "WIRELESS" represent two different wireless networks? If you log on to the wrong one, you could be sending all your information to hackers.

Monitor your credit situation. Obtain a free credit report from [annualcreditreport.com](http://annualcreditreport.com). You are entitled to a free credit report once every 12 months from each of the nationwide consumer credit reporting companies: Equifax, Experian, and TransUnion.



## E-mail Threat: Phishing, Spam, and Others

**Phishing e-mail is e-mail that solicits** personal information by using the name of reputable institutions. You probably receive tons of spam e-mail messages everyday. More than a few will likely be phishing e-mail. Phishing e-mail takes on a look and feel so real that even experienced users can be fooled. How do you navigate the sea of deception when handling e-mail?

### What You Need to Know

Activate spam-blocking utilities offered by your Internet Service Provider (ISP).

You can be assured that plenty of spam will still slip through the spam blocker and end up in your mail box. Delete without opening or previewing them. NEVER respond to spam or click on any part of a spam message.

A legitimate company will never ask for personal information in an e-mail or pop-up message. Do NOT respond to any e-mail or pop-up that asks for personal information.

Spam is frequently used as a delivery mechanism for malicious software. Do not open any attachments or click on any URL or image even if it looks like it is coming from a friend or colleague. Check with the sender first.



## Cyber Bullying

**Online bullying** comes in many different shapes and forms: mean words, distorted images, mocking and embarrassing postings, threatening messages, etc. Bullying causes emotional turmoil and trauma. Every child should be protected from being bullied and taught that bullying behavior is unacceptable.

### What You Need to Know

Children are often frightened and confused about how to react when they are bullied. Encourage your children to talk to you or a trusted adult. Make sure that your children know that you will listen and protect them.

Talk to your children about how to handle their emotions when they are online. Teach your children to avoid chatting, texting, or e-mailing when they are angry.

Tell your children that they don't have to read every message they receive. They can ignore and block the ones they know or suspect are coming from a bully. Sometimes this is the best strategy in fending off unwelcome bullying.

Many Internet Service Providers (ISPs) have a mechanism to block content from a bully. Report the cyber bullying to your ISP when necessary.

Save the evidence and report the bullying to local law enforcement if your children are threatened or harassed.

Teach empathy and compassion to your children so they do not become cyber bullies.

