Tips For Safe Surfing

The Internet has some pretty dark and scary back corners, and sometimes malicious software can pop up where you least expect it. No one can guarantee that you'll be 100% safe, but if you follow these tips and suggestions, you will definitely be safer, and able to browse with a bit more peace of mind.

- Create simple, easy-to-read house rules about using the Internet and post them on or near the monitor. You and your kids can establish a family contract outlining your family's rules of acceptable Internet usage. And don't be afraid to enforce it!
- Use an outbound traffic analyzer to be notified when an application begins emitting new or unexpected traffic.
- Manually control web cookies while web browsing. The procedure for enabling this setting is different for each World Wide Web browser (Internet Explorer, Safari, Firefox, Opera, Chrome, etc.). In order to enable this setting in Firefox click on "Tools", then "Options", choose the "Privacy" tab at the top then check the boxes "Accept cookies from sites" and "Accept third-party cookies". In the drop down menu below those boxes select "Keep Until: Ask me every time". After setting this option you will be presented with a choice whether to accept or deny cookies for most of the websites you visit. If you deny cookies related to the website you are attempting to visit then the website may not function as intended. Generally, most third party cookies are safe to "deny," but not always.
- Always keep anti-virus software definitions up to date. Upon installation, most antivirus software will ask you if you want definitions updated automatically. It will also be presented as an option within the software itself. Often your ISP (Internet Service Provider) will provide anti-virus software to you at no cost, so check their documentation for more information.
- Practice "defense-in-depth" by installing more than one anti-virus and/or anti-spyware/malware application. Contrary to popular belief, anti-virus vendors often have widely variable delays before a particular signature gets into their database. While they may be effectively the same 30 days after a piece of malware is released, you are most vulnerable in the hours immediately after release, a time at which having multiple anti-virus applications may save you from infection.
- Use a firewall. Firewalls come in many shapes and sizes with varying degrees of functionality and protection. Firewalls can be hardware or software based.
- Remember that *everyone* on the Internet is exposed to online criminals. Sources of both commercial and free software are targets for hacking, and care should be exercised when downloading and installing Internet-based software.
- Follow Microsoft's best practices for updating various Windows operating systems.
- Never blindly accept a security dialog or execute an unexpected file, even if it comes from a web site that you visit often. Even the largest web sites can be compromised to include malware downloads and other security risks. Always carefully read and evaluate the provided text before making a decision. When in doubt - deny or cancel.
- Use filtering software. This is your first line of defense. We suggest http://www.browsesafe.com as well as some others on the Filters Handout.
- Limit the number of hours each day that you are on-line. Remember the Internet can be addictive. Even innocent surfing can become time-consuming and a big time-waster.
- Keep your computer centrally located in a well-trafficked room in your house. Isolated or secluded locations lead to temptation and are not easy for a parent to monitor.
- Keep your last name private. Never give out your full name, address, phone number or other personal information. While you can confidently give it to secure online stores, resist the temptation to post it on a message board or reveal it in chat rooms. Be sure to spell out the specifics of allowed chat room behavior in your family contract!
- Have at least two email accounts. Keep one private and only share the address with family and friends. Use the other account when you subscribe to Internet mailing lists, or register as a user at a web page. This will help you limit your junk mail to one inbox. (Much junk mail is inappropriate for children.) When signing up for anything online, even free software where your personal information may be requested before you can download, always think carefully about the kind of information you are being asked to supply. For instance, if something is free you should not have to give credit cards details. Consider registering a free email address at gmail, hotmail, yahoo, or opera and using that when asked to enter an email before a download. This will keep your main email address safe from abuse.
- Remember that you are not *completely* anonymous. Your computer lists the websites visited, and your Internet Service Provider (ISP) can watch you surf and create a profile about you; however, you can surf through www.anonymous.com to get more of an anonymous filter for free.
- Watch Out For Dangerous E-mails. Talk to your children about not responding to offensive or dangerous e-mails, chat, or other communications. Report any such communication to your local law enforcement agency or to the National Center for Missing & Exploited Children's website at www.cybertipline.com.Never download programs or email from the Internet without a good anti-virus program system installed.
- Never arrange a meeting with someone you have met online.
- Have the children tell the parents if they come across something that makes them feel uncomfortable.
- Never give out your passwords to anyone.