Strategies for Internet Safety

1. Establish a parent-child internet use contract.
2. Explain to older children and adolescents the potential hazards of online sexual solicitation and the risks associated with internet communication with strangers. Younger children may not need as detailed a discussion, but should be cautioned about the dangers of talking to people they do not know.
3. Discuss the dangers of face-to-face contact with someone met online.
4. Teach your child to avoid sending personally identifying information (e.g., real name, address, school, telephone number, photos, family member names) via the internet.
5. Install a firewall, privacy filtration software, anti-adware, and an antivirus program.
6. Encrypt your wireless home network.
7. Discourage your child from downloading games and other media which could contain Trojan and worm programs that enable remote access to computers by unauthorized users.
8. Supervise/monitor internet friends in a fashion similar to how neighborhood and school friends are monitored.
9. Monitor the amount of time your child spends online and frequently check the computer’s web browsers, which provide information on the websites that have been accessed.
10. Set the internet browser (e.g., Internet Explorer, Google Chrome, Firefox) security features to “high.”
11. Understand and approve children’s screen names.
12. Know your children’s screen names and passwords.
13. Place computer in a public location such as a den or living room as opposed to a child’s bedroom.
14. Contact the Cyber Tip Line at (800) 843-5678 or [www.cybertipline.com](http://www.cybertipline.com) if you suspect an online predator has contacted your child.