



Safety Tips

- Look into safeguarding programs or options your online service provider might offer. These may include monitoring or filtering capabilities.
- Always read a website's privacy policy before giving any personal information. Also make sure that a website offers a secure connection before giving credit card information.
- Websites for children are not permitted to request personal information without a parent's permission. Talk to children about what personal information is and why you should never give it to people online.
- If children use chat or e-mail, talk to them about never meeting in person with anyone they first "met" online.
- Talk to children about not responding to offensive or dangerous e-mail, chat, or other communications. Report any such communication to local law enforcement. Do not delete the offensive or dangerous e-mail; turn off the monitor, and contact local law enforcement.
- Keep the computer in the family room or another open area of your home.
- Get informed about computers and the Internet.
- Let children show you what they can do online, and visit their favorite sites.
- Have children use child-friendly search engines when completing homework.
- Know who children are exchanging e-mail with, and only let them use chat areas when you can supervise. NetSmartz recommends limiting chatroom access to child-friendly chat sites.
- Be aware of any other computers your child may be using.
- Internet accounts should be in the parent's name with parents having the primary screenname, controlling passwords, and using blocking and/or filtering devices.
- Children should not complete a profile for a service provider and children's screennames should be nondescript so as not to identify that the user is a child.
- Talk to children about what to do if they see something that makes them feel scared, uncomfortable, or confused. Show them how to turn off the monitor and emphasize that it's not their fault if they see something upsetting. Remind children to tell a trusted adult if they see something that bothers them online.
- Consider using filtering or monitoring software for your computer. Filtering products that use whitelisting, which only allows a child access to a preapproved

list of sites, are recommended for children in this age group. NetSmartz does not advocate using filters only; education is a key part of prevention.

- If you suspect online "stalking" or sexual exploitation of a child, report it to your local law-enforcement agency. The National Center for Missing & Exploited Children (NCMEC) has a system for identifying online predators and child pornographers and contributing to law-enforcement investigations. It's called the CyberTipline. Leads forwarded to the site will be acknowledged and shared with the appropriate law-enforcement agency for investigation.