Many parents think that if their children are home using a computer, they are safe and not getting into trouble. Nothing could be further from the truth. Your child could be the target of cyberbullying, or they could be causing harm to others from your own family room.

Some parents think they have protected their children because they have installed filtering software. Filtering software provides a false sense of security. Not only can children still access material parents don’t want them to access, filtering cannot prevent cyberbullying or address other concerns.

Make it your business to know what your child is doing online. Teenagers are likely to take the position that their online activities are their business. But parents have a moral, as well as legal, obligation to ensure that their children are engaged in safe and responsible behavior—including online behavior. Here are some ways to stay involved:

- Keep the computer in a public place in the house. Periodically check on what your child is doing. Discuss the kinds of Internet activities your child enjoys. Find out who your child’s online friends are.

- Help your child distinguish between three kinds of personal information:
  
  - **Personal contact information**: Name, address, phone number, and any other information that could allow someone to make contact in the real world. This information should be shared only in secure environments, when absolutely necessary, and with your permission.

  - **Intimate personal information**: Private and personal information that should only be discussed with a relative, close friend, or professional. This information should never be shared in public online communities or through public communications such as chat or discussion groups. Disclosures in private communications with trustworthy friends or in professional online support environments may be appropriate.

  - **Personal interest information**: Non-intimate information about interests and activities. This kind of information can generally be safely shared on
public community sites or communication environments, including blogs, personal Web pages, chat, and discussion groups.

- Increase your child’s online “stranger danger” awareness. Anyone your child meets online should be considered potentially dangerous until it is possible to determine from independent real-world sources who this person is and that this person has a background that provides assurances of safety.

- Be sure you know the online communities your child participates in and your child’s usernames in these communities. Review your child’s public postings, including your child’s profiles, Web pages, and blogs.

- Discourage active involvement in the kinds of environments that promote excessive self-disclosure of intimate information and rude behavior. Your child may object and claim that these postings should be considered private. A child who makes this argument simply does not understand. The material posted on these sites is not private—anyone can read it. If your child is uncomfortable about your review of the material, then this is a good clue that the material should not be posted.

- Be up front with your child that you will periodically investigate the files on the computer, the browser history files and buddy lists, and your child’s public online activities. Tell your child that you may review his or her private communication activities if you have reason to believe that you will find evidence of unsafe or irresponsible behavior.

- Watch out for secretive behavior. It’s a danger sign if your child rapidly switches screens as you approach the computer or attempts to hide online behavior by emptying the history file.

- You can install keystroke monitoring software that will record all of your child’s online activities. The use of such software raises trust concerns. The best way to use such software is as deterrence. Tell your child monitoring software has been installed, but not yet activated and explain what actions on his or her part could lead to your investigation. These actions could include: not being willing to talk about online activities, late night use, extensive use, decline in grades, evidence your child is seeking to cover his or her online tracks, report of inappropriate activity, appearing really upset after Internet use, and the like. If your child has engaged in unsafe or inappropriate behavior, the most appropriate consequence is the use of monitoring software and consistent review of all public and private online activity.

**Important Note**
If you ever find any evidence that your child is interacting with a sexual predator, do not confront your child. Your child could warn or run off with the predator. Call your local police and ask for a youth or computer crimes expert. If you suspect this kind of activity, consider installing or activating monitoring software, but not telling your child.