



Online Safety Tips for Parents

1. Be sure to fill your Internet Security shopping list: antivirus software, spyware protection, firewall, and patches.
2. Realize that MySpace isn't going away. If you're concerned, sit down together and review your teen's MySpace page. Drill your teen and friends about not giving out full names, addresses, school names, or other personally identifiable information.
3. Keep your teen's PC in an open space where you can see what's going on – not behind a closed bedroom door.
4. Avoid webcams. (Teens are too often drawn to use webcams to post photos they may deeply regret in later life. Remove that temptation!)
5. Don't be afraid to be the grownup. If you're concerned about your teen visiting inappropriate sites, install software with parental controls to block those sites. (Remember when you child-proofed your kitchen with safety latches and electronic plug guards? Especially if your child is a young teen, it's OK to "teenproof" the Internet a bit as well.)
6. Don't be afraid to play the cop either if you need to. If you suspect your teen is doing something wrong online, strongly consider purchasing monitoring software. If your teen is doing something inappropriate, it's much better to be caught by a concerned parent than a real law enforcement officer.
7. Don't forget to protect your own data as well. (Think of this as protecting your teen's allowance or college fund!) Particularly if your teen downloads software, music, or other items, you should keep your financial details and banking information on your own computer – not the one your teen uses.
8. If your family shares a single computer, look into software designed to protect your financial transactions and personal information. Make sure you install that software if you're banking online or using your PC for other financial transactions such as online bill paying or shopping. I do not recommend you use the same computer to do banking as your kids use to play games and download software from the Internet.
9. Remind your teen to think about the future. What teens post today will still be hanging around the Net years from now when they're working on developing real careers. Stupid comments and photos today can translate into unemployment in years to come.
10. Watch out for social engineering. Just because someone calls you on the phone and tells you he is from the FBI, it doesn't mean he really is! Verify it. Teach your teens not to give out any personal information over the phone, email, IM, and so on, that could identify their location or provide key personal information.