

Educate yourself and your kids about the risks

Revealing more information than is safe

Many kids share their passwords, or volunteer information that identifies them or makes them easy to find. This may leave them vulnerable to hate attacks, identity theft, fraud, and other criminal abuse.

Acting carelessly online without realizing the consequences

Sharing files with strangers or carelessly downloading ringtones, music, or games can lead to trouble. Some share files that look like music or videos, but are actually pornography or contain viruses or software that can leave a computer open to attack. Web cams and phone cameras can also encourage risky behavior.

Unintentional or deliberate exposure of information by others

School or club Web sites often reveal too much student or member information. Teens may expose friends through comments left on friends' blogs or by broadcasting compromising photos. Online businesses may sell personal information they collect.

Flaws or gaps in technologies and services

Web businesses may put teens at risk by failing to implement effective filtering and safety technologies, neglecting to effectively monitor their services, and by encouraging teens to disclose more information than is necessary.

More Helpful Info

- For further practical online safety advice, visit microsoft.com/protect/parents/childsafety/internet.aspx.
- For age-based guidance, visit microsoft.com/protect/parents/childsafety/age.aspx.
- For information written especially for teens, visit iLOOKBOTHWAYS.com/docs/DOC-1129.



Get to Know the Internet Risks for Tweens and Teens

Smarter Online = Safer Online

Protecting "Tweens" and Teens on the Internet

For most tweens and teens, being online is as natural and easy as breathing—whether they are sending instant messages (IM) or creating Web pages on a computer, gaming on a console, or texting on a cell phone. And while the Internet is mostly a positive place for them, it also opens up areas and activities that may not be appropriate.

You may not feel that you have the same technical savvy as kids do, but you have been teaching them about safety ever since they were old enough to crawl. You simply need to learn how to apply what you already know about safety and privacy to their digital world.

- Get to know the Internet risks for tweens and teens
- Practical advice to keep young people safer on the Internet
 - What to do if there are problems



© 2009 Microsoft Corporation. All rights reserved. The information contained in this brochure is provided for educational and informational purposes only. Microsoft and the other sponsors of this resource make no representations that the suggestions and recommendations provided will prevent any harmful conduct to children, teens, or others. Microsoft, Windows, Windows 7, Windows Vista, Xbox LIVE, and Zune are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names and logos of actual companies and products mentioned herein may be trademarks of their respective owners.



Practical Advice to Keep Young People Safer on the Internet

For parents: guidance not control

Online safety is a family effort, not a power struggle. Teens and tweens don't want to be cheated or manipulated, or put family or friends at risk any more than you do. As they become increasingly independent, you can help them develop a smart sense of how to deal with situations, information, and people on the Web—skills they need now and when they leave home.

- > Periodically ask your kids to show you what they're doing and who they're meeting and talking to on the Web—what sites they visit or create, what games they play, what they talk about, and so on.
- > Negotiate clear guidelines for Internet use that fit your kid's and family's values. Discuss the kinds of sites that are off limits, what information should not be shared, and boundaries for communicating with others.
- > Watch for signs of online bullying (being upset when online or reluctance to go to school) and talk with kids about how to deal with it. Discuss how cyberbullying is never acceptable, and make the consequences clear.
- > Be the administrator of your home computer. Find out how to create different user accounts in Windows® 7, Windows Vista®, or Windows® XP at microsoft.com/protect/parents/childsafety/steps.aspx#acct.
- > Defend your computer against Internet threats. Use firewall, antivirus, and antispyware software. Password-protect your wireless router. Keep security software current with automatic updates. See how Microsoft can help at microsoft.com/security/pypc.aspx.



For tweens and teens: protect your information, respect others, act responsibly

Use the points below to jumpstart a conversation with your kids.

Keep your personal information to yourself

Your personal information has a lot of value to those who want to misuse it, so guard it carefully. This means your first and last name, phone number, address, age, school, passwords, photos of yourself, even feelings (especially those of loneliness or sadness).

Sharing personal info online with anyone but close friends invites problems—it can become public and even permanent. Friends may not be friends forever—think about how others might misuse information you've shared.

- > Make your blogs and social network pages private to limit those who can see personal details.
- > Make up strong passwords, and DON'T SHARE THEM with anyone—not even your best friend. Learn how at microsoft.com/protect/fraud/passwords/create.aspx.
- > Create screen names, e-mail addresses, and profile pages that reveal nothing personal and aren't suggestive.
- > Be choosy when you add new friends on cell phones, IM contact lists, social Web sites, or in games.

Treat others as you would like to be treated

- > Never say something online that you wouldn't say face-to-face.
- > Don't log on to a friend's computer or online accounts to do harm.
- > Don't hack a friend's blog or steal access to their cell phone and pretend to be them.
- > Don't share personal details of friends and family members online without permission.

Act responsibly

- > Don't make illegal copies of music, video games, and so on; it's just like stealing from a store. Plagiarism is also stealing.
- > Meeting an online "friend" in person is very risky. Plan your safeguards in advance—for example, bring a parent or friend with you and meet in a busy public place. Make sure a trusted adult always knows where you are.
- > Think twice (even if you know the sender) before you open attachments or click links in e-mail. They might open an upsetting image or release a virus or other malicious software. For the same reasons, don't download or share music, games, or ringtones with someone you don't know personally.

Get help from technology

Put a password on your cell phone to keep anyone who steals it from making calls or getting your personal info.



What to Do If There Are Problems

Teach tweens and teens to trust their instincts

If something feels uncomfortable or alarming, it almost always is. Let them know they can come to you and that you will help solve the problem. Make it clear that you won't punish them or take away computer, game, phone, or other privileges.

Immediately report:

- > Physical threats, ongoing cyberbullying, financial fraud, or any form of exploitation to the appropriate authority.
- > Inappropriate content or behavior to the school (if it involves another student) and to the Internet service provider, cell phone company, or Web service. For example, in Microsoft® services and software, look for a **Report Abuse** link, or contact us at go.microsoft.com/?linkid=9669236.
- > Content that exploits minors or threatens to harm them to the National Center for Missing and Exploited Children at **800.843.5678** or online at cybertipline.com.