Get to know the Internet risks

You have taught your kids about safety since they were toddlers. To teach online safety, start by educating yourself about Internet risks.

Revealing more information than needed. Many kids give out information that can mar their reputation with potential long-term consequences. They may also share their passwords or volunteer information on social networks or in text messages that identifies them or their location. This may leave them vulnerable to cyberbullying, identity theft, scams, and other abuse.

Acting carelessly online without realizing the consequences. Downloading applications, music, games, or video from suspect websites or freely sharing these files from strangers can lead to trouble. It can open a computer to attack, or expose kids to inappropriate content. Webcams and phone cameras can also encourage risky behavior.

Exposure of information by others. School or club sites often reveal too much student or member information. Friends and family may expose teens through comments and photos. Some sites share or sell—even own—the personal data they collect.

Web services may put tweens and teens at risk by encouraging them to disclose more information than is prudent, failing to put effective safety technologies in place, and neglecting to monitor their services well.

What to do if there are problems

Teach tweens and teens to trust their instincts.

Let them know they can come to you for help in solving the problem. Be clear that you won't punish them or curtail computer, game, or phone privileges because of someone else's actions.

Immediately report

> Physical threats, cyberbullying, or any exploitation to the police.

> Inappropriate behavior, like cyberbullying, to the school (if it involves another student), and to the phone carrier or web service. For example, in Microsoft services or software, look for the **Report Abuse** link, or contact us at **microsoft.com/reportabuse**.

More helpful info

> You can use family safety settings to help monitor kids' online activity. Compare these from Microsoft: **aka.ms/compare-tools**.

> Cybersafety talk directed right to teens: **tinyurl.com/iLBW-Teen-safety**.

> Top tips for online safety written just for tweens and teens: **aka.ms/student-tips**.

> An online forum where teens can chat with other teens (or become a cyber mentor themselves): **cybermentors.org.uk**.

Content contributor LOOKBOTHWAYS ilookbothways.com

1011 PN 098-110820

Microsoft

Protecting "Tweens" and Teens Online

> Get to know the Internet risks for tweens and teens

> Practical advice to help keep young people safer online

> What to do if there are problems

Microsoft

Practical advice to help keep young people safe online

For parents: Guidance, not control

Tweens and teens don't want to be cheated or put family or friends at risk any more than you do. You can help them develop the skills and ethics they need to deal with situations, information, and people on the web.

- Periodically ask kids to show you—the sites they visit, pages they create, games they play, what they talk about and with whom. If you plan to use family safety software for monitoring, let them know.
- Negotiate clear guidelines for Internet use that fit your kid's maturity and family's values. Discuss the kinds of sites that are off limits, such as social sites not meant for those under age 13. Talk about what information should not be shared and boundaries for respectful communication with others.
- Watch for signs of online bullying like being upset when online or a reluctance to go to school. Talk with kids about how to deal with it and how you can help. Also discuss how cyberbullying is never acceptable, and make the consequences clear.
- Be the administrator of your home computer. Find out how: **aka.ms/user-accounts**.
- Defend your computer against Internet threats. Keep all software (including your web browser) current with automatic updating. Install legitimate antivirus and antispyware software. Never turn off your firewall. Microsoft can help with the details: **microsoft.com/security/pypc.aspx**.

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

Use the points below to jump-start a conversation with your kids.

Keep personal information to yourself

Your personal information is valuable to those who want to exploit it, so guard it carefully. This includes your full name, phone number, home address, age, school, passwords, photos, even feelings like those of loneliness or sadness.

Sharing personal info online with anyone but close friends can invite problems. Information you have shared about yourself or comments you have made can become public and be used to embarrass you, damage your reputation, or steal your identity. And they can be permanent—for example, a future employer might see them.

- Use strong passwords, and DO NOT SHARE THEM—not even with your best friend. Learn how: **aka.ms/passwords-create**.
- Lock your phone with a PIN.
- Create email addresses and profile pages that reveal nothing personal and aren't suggestive.
- Make your social network pages private. Look for **Settings** or **Options** to set privacy controls.
- Don't share suggestive photos or videos. You lose all control of where they go.
- Be choosy about adding friends on phones or social sites, or in games.

Be a real friend

- If you wouldn't wear it (on a T-shirt, say), don't share it online.
- Stand up for your friends. Cyberbullies are less likely to target someone who has a strong group of friends, and usually stop when a victim's friends rally around him or her.
- Don't share personal details of friends and family online without their permission.

Connect honestly and carefully

- Don't download illegal copies of copyrighted music, video games, and so on. Plus, pirated files are often used to distribute viruses and spyware without the user's knowledge.
- Use only social networks that are right for your age.
- Think twice (even if you know the sender) before you open attachments, or click links in email or on a social site. You might release malicious software.
- Meeting an online "friend" in person can be risky. Protect yourself: always bring a trusted adult or friend and meet in a busy public place.