



Internet Safety and Security Tips for Parents

While their age helps youth easily adapt to new technologies, their immaturity also makes them more likely to unintentionally engage in risky behaviors or be targeted by other users, more often peers than strangers. For many young people, there is little divide between their “real world” and online selves. As a parent, consider doing the following:

- **Remain positively engaged.** Pay attention to and know the online environments your children use. Appreciate your children’s participation in their online communities and show interest in their friends. Try to react constructively when they encounter inappropriate material. Make it a teachable moment.
- **Support their good choices.** Expand your children’s online experience and their autonomy when developmentally appropriate, as they demonstrate competence in safe and secure online behavior and good decision making.
- **Protect your hardware.** Safety and security start with protecting all family computers. Install a security suite (antivirus, antispyware, and a firewall) that is set to update automatically. Keep your operating system, Web browser, and other software current as well, and back up computer files on a regular basis.
- **Know the protection features** of the Web sites and software your children use. Your Internet service provider (ISP) may have tools to help you manage young children’s online experience (e.g., selecting approved Web sites, monitoring the amount of time they spend online, or limiting the people who can contact them) and may have other security features, such as pop-up blockers. Third-party tools are also available. But remember that your home isn't the only place they can go online.
- **Review the privacy settings** of social networking sites, cell phones, and other social tools your children use. Decide together which settings provide the appropriate amount of protection for each child.
- **Teach critical thinking.** Help your children identify safe, credible Web sites and other digital content, and be cautious about clicking on, downloading, posting, and uploading content.
- **Explain the implications.** Help your children understand the public nature of the Internet and its risks as well as its benefits. Be sure they know that any digital info they share, such as emails, photos, or videos, can easily be copied and pasted elsewhere, and is almost impossible to take back. Things that could damage their reputation, friendships, or future prospects should not be shared electronically.



NATIONAL CYBERSECURITY AWARENESS MONTH

- **Help them be good digital citizens.** Remind your children to be good “digital friends” by respecting personal information of friends and family and not sharing anything about others that is potentially embarrassing or hurtful.
- **Just saying “no” rarely works.** Teach your children how to interact safely with people they “meet” online. Though it’s preferable they make no in-person contact with online-only acquaintances, young people may not always follow this rule. So talk about maximizing safe conditions: meeting only in well-lit public places, always taking at least one friend, and telling a trusted adult about any plans they make – including the time, place, and acquaintance’s contact information (at least a name and cell phone number). Remind them to limit sharing personal information with new friends.
- **Empower your children to handle problems,** such as bullying, unwanted contact, or hurtful comments. Work with them on strategies for when problems arise, such as talking to a trusted adult, not retaliating, calmly talking with the person, blocking the person, or filing a complaint. Agree on steps to take if the strategy fails.
- **Encourage your children to be “digital leaders.”** Help ensure they master the safety and security techniques of all technology they use. Support their positive and safe engagement in online communities. Encourage them to help others accomplish their goals. Urge them to help if friends are making poor choices or being harmed.
- **Learn more at www.staysafeonline.org.**

Content developed collaboratively by NCSA’s K-12 Working Group.