



Staying Safe Online

<http://www.netsmartz.org/InternetSafety>

<http://www.nationalcac.org/prevention/internet-safety-kids.html>

Internet Safety Tips for Kids and Teens

1. Spend time having fun with your parents online and helping them understand technology!
2. Never post your personal information, such as a cell phone number, home number, home address, or your location on any social networking site or through mobile apps like Snapchat or Instagram.
3. Never meet in person with anyone you first “met” on the internet. If someone asks to meet you, tell your parents or guardian right away. Some people may not be who they say they are.
4. Check with your parents before you post pictures of yourself or others online. Do not post inappropriate pictures of anyone.
5. Never respond to mean or rude texts, messages, and e-mails. Delete any unwanted messages. You may need to delete friends who continuously bother you or post things that are not appropriate.
6. NEVER share your password with anyone, including your best friend. The only people who should know your password are your parents or guardian.
7. If you wouldn't say something to another person's face, don't text it or post it online.
8. Do not download or install software or anything on your computer or cell phone before checking with your parents or guardian.
9. Use the privacy settings of social networking sites.
10. If anything makes you feel uncomfortable online, while gaming or when using your cell phone, talk with your parents or guardian right away.

Source: Netsmartz.org and safekids.com.

<https://staysafeonline.org/stop-think-connect/tips-and-advice>

Practice good online safety habits with these tips and advice:

Keep A Clean Machine.

- **Keep security software current:** Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.
- **Automate software updates:** Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option.
- **Protect all devices that connect to the Internet:** Along with computers, smart phones, gaming systems, and other web-enabled devices also need protection from viruses and malware.
- **Plug & scan:** "USBs" and other external devices can be infected by viruses and malware. Use your security software to scan them.

Protect Your Personal Information.

- **Secure your accounts:** Ask for protection beyond passwords. Many account providers now offer additional ways for you verify who you are before you conduct business on that site.
- **Make passwords long and strong:** Combine capital and lowercase letters with numbers and symbols to create a more secure password.
- **Unique account, unique password:** Separate passwords for every account helps to thwart cybercriminals.
- **Write it down and keep it safe:** Everyone can forget a password. Keep a list that's stored in a safe, secure place away from your computer.
- **Own your online presence:** When available, set the privacy and security settings on websites to your comfort level for information sharing. It's ok to limit who you share information with.

Connect With Care.

- **When in doubt, throw it out:** Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.
- **Get savvy about Wi-Fi hotspots:** Limit the type of business you conduct and adjust the security settings on your device to limit who can access your machine.

- **Protect your \$\$:** When banking and shopping, check to be sure the site's security is enabled. Look for web addresses with "https://" or "shttp://", which means the site takes extra measures to help secure your information. "Http://" is not secure.

Be Web Wise.

- **Stay current. Keep pace with new ways to stay safe online:** Check trusted websites for the latest information, and share with friends, family, and colleagues and encourage them to be web wise.
- **Think before you act:** Be wary of communications that implore you to act immediately, offers something that sounds too good to be true, or asks for personal information.
- **Back it up:** Protect your valuable work, music, photos, and other digital information by making an electronic copy and storing it safely.

Be a Good Online Citizen.

- **Safer for me more secure for all:** What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.
- **Post only about others as you have them post about you.**
- **Help the authorities fight cybercrime:** Report stolen finances or identities and other cybercrime to the Internet Crime Complaint Center (www.ic3.gov) and to your local law enforcement or state attorney general as appropriate.

Practice **STOP. THINK. CONNECT.** and encourage others to do it as well. - See more at: <https://staysafeonline.org/stop-think-connect/tips-and-advice#sthash.Zm1feat8.dpuf>