



Social Networking

Social networking websites are a place for internet users to come together. For example, Facebook, Twitter and Instagram are services people can use to connect with others to share information like photos, videos and personal messages.

Do not trust that a message is really from who it says it is from.

As the popularity of these social sites grows, so do the risks of using them. These sites encourage and enable people to exchange information about themselves, share pictures and videos, and use blogs and private messaging to communicate with friends, others who share interests, and sometimes even the world-at-large. Hackers, spammers, virus writers, identity thieves and other criminals follow the traffic. Because you must divulge some level of personal information in order to use and fully benefit from social networking sites, the risk of identity theft exists.

Tips to protect yourself

- **Choose your social network carefully.** Evaluate the site you plan to use and make sure you understand the privacy policy. Find out if the site monitors the content people post. You will be providing personal information to this website, so use the same criteria you would to select a site where you enter your credit card.
- **Know what you have posted about yourself.** Be wise and mindful of what you post. Do not announce when you will be leaving town. Protect your reputation. Assume everything you put on a social networking site is permanent. Think twice before posting pictures you would not want your parents or future employers to see. Recent research found that 70% of job recruiters rejected candidates based on information they found online. Be cautious about how much personal information you provide on social networking sites. The more information you post, the easier it may
- **Know and manage your friends.** Social networks can be used for a variety of purposes. Some of the fun is creating a large pool of friends from many aspects of your life. That does not mean all friends are created equal. Use tools to manage the information you share with friends in different groups. If you are trying to create a public persona as a blogger or expert, create an open profile or a “fan” page that encourages broad participation and limits personal information. Use your personal profile to keep your real friends (the ones you know and trust) more synched up with your daily life.
- **Be honest if you are uncomfortable.** If a friend posts something about you that makes you uncomfortable or you think is inappropriate, let them know. Likewise, stay open-minded if a friend approaches you because something you have posted makes him or her uncomfortable. People



have different tolerances for how much the world knows about them. Respect those differences.

- **Keep a clean machine.** Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.
- **Make passwords long and strong.** Combine capital and lowercase letters with numbers and symbols to create a more secure password. Remember to use separate passwords for online banking and social networking sites to thwart cybercriminals.
- **Use caution when you click links you receive in messages from friends on your social website.** Treat links in messages on these sites as you would links in email messages. If it looks suspicious, even if you know the source, it is best to delete or, if appropriate, mark as junk email.
- **Do not trust that a message is really from who it says it is from.** Hackers can break into accounts and send messages that look like they are from your friends, but are not. If you suspect a message is fraudulent, use an alternate method to contact your friend to find out. This includes invitations to join new social networks.
- **Do not allow social networking services to scan your email address book.** When you join a new social network, you might receive an offer to enter your email address and password to find out if your contacts are on the network. The site might use this information to send email messages to everyone in your contact list or even everyone you have ever sent an email message to from your email address. Social networking sites should explain they are going to do this, but some do not.
- **Type the address of your social networking site directly into your browser or use your personal bookmarks.** If you click a link to your site through email or another website, you might be entering your account name and password into a fake site where your personal information could be stolen.
- **Be careful about installing extras on your site.** Many social networking sites allow you to download third-party applications that let you do more with your personal page. Criminals sometimes use these applications to steal your

personal information. To download and use third-party applications safely, take the same precautions you take with any other program or file you download from the internet.

- **Online bullying.** Online bullying can take many forms. From spreading rumors online and posting personal information, forwarding private messages without the sender's OK, to sending threatening messages. The words you type and the images you post can have real-world consequences. They can make the target of the bullying feel bad, make the sender look bad, and, sometimes, can bring on punishment from the authorities. Encourage your kids to talk to you, if they feel targeted by a bully.
- **Know what action to take.** If someone is harassing or threatening you, remove them from your friends list, block them, and report them to the site administrator. If you feel you could be in danger, report it to the police.
- **Google yourself regularly.** Know what information about you is out there. You can contact each website operator directly to find out how you can request your information be removed.

Tips to protect kids and teens

- **Take extra steps to protect younger kids.** Keep the computer in an open area like the kitchen or family room, so you can keep an eye on what your kids are doing online. Use the Internet with them to help develop safe surfing habits. Consider taking advantage of parental control features on some operating systems that let you manage your kids' computer use, including what sites they can visit, whether they can download items, or what time of day they can be online.
- **Talk, and talk often.** Make sure your kids know what information should be private, and what information might be appropriate for sharing. When they give out their personal information, they give up control of who can reach them, whether it is with a marketing message or something more personal. On the other hand, sharing some personal information may allow them to participate in certain activities or to get emails about promotions and events they are interested in.

- **Learn how your computer works.** Ask a computer-savvy adult friend to show you how to check your computer to see where your children have been online. Check your browser history and temporary files. Keep in mind that older kids may know how to delete these files or keep them from getting recorded. If you would like more controls, check to see what privacy settings your browser offers or consider monitoring software that offers a range of controls.
- **Know how your kids get online.** Kids may get online using your family computer or someone else's, as well as through cell phones and game consoles. Know what limits you can place on your child's cell phone. Some companies have plans to limit downloads, Internet access, and texting on cell phones; other plans allow kids to use those features at certain times of day. Check out what parental controls are available on the gaming consoles your kids use, as well.
- **Go where your kids go online.** Sign up for and use the social networking sites your kids visit. Let them know you are there, and help teach them how to act as they socialize online. Go to common online networking sites, sign up and create a profile for yourself. Provide only the information necessary to create a profile, nothing more. Then, you can search for your kids' page.

Remember, your kid may have given a false or code name, so this search might not find his or her page. You can also search using other information, such as the name of your kid's school. All kids who have listed this school in their profiles will be identified using this search. If your kid is not identified in this list, you can select friends of your kid to see if your kid is listed on their pages as a friend. You may also be able to perform searches using keyword and email addresses. In most social networking services, both users must confirm that they are friends before they are linked. Some sites have a "favorites" feature that does not need approval from the other user.

- **Create a safe screen name.** Encourage your kids to think about the impression that screen names can make. A good screen name will not reveal too much about how old they are, where they live, or their gender. For privacy purposes, your kids'

screen names should not be the same as their email addresses.

- **Make agreements.** Be sure your kids know what your family has decided is okay and not okay to divulge online. Consider writing down a list of rules your family has agreed on, and posting them where everyone can see them.
- **Review your child's friends list.** You may want to limit your child's online "friends" to people your child actually knows and is friendly with in real life. Social networks usually have privacy controls that allow the user to choose who can view their profile or contact them, etc.
- **Set rules about meeting online "friends" in public.** Establish clearly that if a child is going to meet a person he or she has only met on the Internet, it must be with your permission, in a very public place, and that you or another trusted adult must be present.
- **Understand sites' privacy policies.** Sites should spell out your rights as a parent to review and delete your child's profile, if your child is younger than 13. Sites may also provide software that allows parents to block access to their site. The Children's Online Privacy Protection Act (COPPA) requires websites to obtain parental consent before collecting, using, or disclosing personal information from children under age 13.

To learn more about staying safe online, visit the websites of the following organizations:

- Staysafeonline.org is an educational site intended to help consumers understand both the positive aspects of the Internet as well as how to manage a variety of safety and security issues that exist online.

staysafeonline.org

- WiredSafety.com is an Internet safety and help group. WiredSafety.com provides education, assistance, and awareness on cybercrime and abuse, privacy, security, and responsible technology use. It is also the parent group of Teenangels.org, FBI-trained teens and preteens who promote Internet safety.

wiredsafety.com

- ConnectSafely.org is a forum for parents, teens, educators, and advocates; designed to give teens and parents a voice in the public discussion about youth online safety, and has tips, as well as other resources, for safe blogging and social networking.

connectsafely.org

- OnGuardOnline.gov, managed by the Federal Trade Commission, provides practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information.

onguardonline.gov

*For more information or to file a complaint,
visit our website or contact:*

Wisconsin Department of Agriculture,
Trade and Consumer Protection
Bureau of Consumer Protection
2811 Agriculture Drive, PO Box 8911
Madison, WI 53708-8911

Email: DATCPHotline@wi.gov

Website: datcp.wi.gov

(800) 422-7128 TTY: (608) 224-5058