Internet Safety for Kids & Families

Safety Tips for Social Networking

As a social medium, the Internet enables young people to stay in touch with friends when they are physically separated from them and sometimes to meet new people who share their interests. Social networking sites, chat rooms, message boards, and blogs are some of the many ways this is possible on the Internet.

Know the Risks

If a young person is socially active on the Internet,he or she is very likely managing at least one personal profile on one or more social-networking sites which require or allow them to publicly divulge something about themselves. While this ability is not inherently bad, there may be people familiar or unfamiliar to them who could take advantage of this.

Unwanted contact

Behaviors such as online grooming (technique used by a sexual predator to convince an underage person to have relations with them offline) and cyberbullying (online harassment of classmates or peers) are some examples of unwanted online contact that parents and care-givers should understand and help young people recognize and act on if they ever experience it. In both cases, the first and best response is to encourage kids not to respond to such messages and to alert their parents so they can figure out the next steps together. It's also a good idea not to delete the messages in case they later need to be used as evidence.

For more information, see our safety tips for Online Grooming and Cyberbulling at www.trendmicro.com/go/safety

Aggressive commercialism

In addition to unwanted contact, parents and caregivers should be mindful of online messages - sometimes legitimate, sometimes malicious - that entice young people to acquire products or services in exchange for information or money. It is important to be aware of how this type of commercialism is delivered, what is being offered, and what young people may do as a result of it. Vendors are using more creative ways to promote their goods and embed their marketing messages, which may make it difficult for a young person to differentiate between an advertisement and the content they are accessing or even interacting with (a technique called immersive advertising). Free offers and promotions for age-inappropriate products and services (dating services, gambling services, etc.) may also be compelling enough to a young person to enter personal information that could later be used by the advertiser to deliver continuous, intrusive advertising (as spam or pop-up advertising) or worse, perpetrate cybercrime (hack attacks, identity theft, etc.).

Covert web threats

Social networking sites are also an increasingly popular place for cybercriminals to trick people into divulging information or downloading software onto their computers for any number of uses. Their methods range from simple to elaborate.

Sometimes a young person will just see an advertisement or link to download seemingly harmless software that they can use on their own social networking profiles, such as a widget, but which in fact has been infected with malicious software that gets downloaded along with the legitimate software.   Some applications that run on social networking sites may encourage young people to complete a survey or provide information that might not be appropriate to share with others. Other times, a young person can be lured to see an "attractive" video   but is told it is necessary to download a viewer in order to see it. While downloading a viewer is a normal action necessary to see videos online the viewer could be infected with other software that, once installed, can be used by the cybercriminal to steal information from the computer, spy on the activities of its owner, or other uses depending on the type of malicious software installed.

For more information, see our demo "Web Threats and the Social Web" at www.trendmicro.com/go/safety.

Behaviors toward others

The anonymity of the Internet can unfortunately encourage offline bad behavior to continue and be exacerbated online. Young people can be victims as well as participants in behaviors such as cyberbullying and harassment. It is important for them to know that information they post can be accessed by anyone virtually forever and can potentially be traced back to them, so it is best to be respectful of others, online or off. More severe comments, particularly those involving physical threats, may also be considered a criminal offense.

Be Prepared

Parents, teachers, and others who care for young people who are socially active online should first set reasonable expectations. Forbidding young people to use social networking sites may force them to go “underground” and find other avenues (e.g. library computers, mobile phones, friends’ computers) to continue their social life online. A positive alternative is to teach them how to think critically about what they are seeing, reading, hearing and sharing online.

Below are some guidelines **for young people** to follow when they are using social networking sites, chat rooms, blogs, or message boards:

1. **Use a nick name or code name.**
   It is best not to use your real name or to use names that might be sexually suggestive or offensive to others in any way. This can help reduce the likelihood of your being harassed online.

2. **Set your profiles to private.**
   Social networking sites can be a great tool for connecting with others. A good way to stay safe using these services is to set your profile to private – this way only people you invite can see what you post.

3. **Keep personal information to yourself.**
   It is best not to share your address, phone number or other personal information online, with strangers. Don’t reveal your actual location or when and where you plan to be somewhere.

4. **Think about what you post.**
   Be cautious about sharing provocative photos or intimate details online, even with people you know or even in a private email or text conversation. The information or conversation could be copied and made public by anyone you share it with - and tough to get removed. Remember: what you say in a chat room or instant messaging session is live - you cannot take it back or delete it later.

5. **Keep your security software up-to-date.**
   Social networking sites are very popular. Because there are so many people using them, cybercriminals have been known to use stealthy tactics in order to infect the computers of people who use them.

6. **Read between the “lines.”**
   It may be fun to meet new people online for friendship or romance, but be aware that, while some people are nice, others act nice because they are trying to get something. Flattering or supportive messages may be more about manipulation than friendship or romance.

7. **Avoid in-person meetings.**
   The only way someone can physically harm you is if you’re both in the same location, so – to be 100% safe – don’t meet them in person. If you really have to get together with someone you “met” online, don’t go alone. Have the meeting in a public place, tell a parent or some other solid backup, and bring some friends along.

8. **Be nice online.**
   Treat people the way you’d want to be treated. Harassing or bullying anyone online, if considered threatening, can also be considered a criminal offense.

9. **Think about how you respond.**
   If someone says or does something that makes you uncomfortable, block them and don’t respond. If they continue, let your parents or another adult know. If the messages are threatening in any way, save the messages and tell your parents as this may be considered a criminal offense.

10. **Be smart when using a cell phone.**
    All the same tips apply with phones as with computers. Except phones are with you wherever you are, often away from home and your usual support systems. Be careful who you give your number to and how you use GPS and other technologies that can pinpoint your physical location.

Be Prepared

Below are some guidelines **for parents** to consider when it comes to letting kids use social networking sites, chat rooms, blogs, or message boards:

1. **Be reasonable and try to set reasonable expectations.**
   Pulling the plug on your child's favorite social site is like pulling the plug on his or her social life. Instead of being protective, it can shut down communication and send kids "underground" where they're more at risk. It's too easy for them to set up free blogs and profiles from anywhere, including friends' houses or even a cell phone.

2. **Talk with your kids about how they use the services.**
   They, not news reports or even experts, are the ones to consult about their online social experience. Help them understand basic safety guidelines, such as protecting their privacy (including passwords), not harassing peers, never talking about sex with people they don't know, avoiding in-person meetings with people they "meet" online, and taking care in what they post - because anything people put online can be grabbed, reworked, and used against them.

3. **Support critical thinking and civil behavior.**
   No laws or parental-control software can protect better than a child's developing good sense about safety and relationships. Research shows that kids who are aggressive and mean online toward peers or strangers are at greater risk of becoming victims themselves. So teach them to be good citizens and friends online as much as offline.

4. **Consider requiring Internet use in a high-traffic place in your home.**
   Try to stay aware of your kids' time online by keeping the computer in a shared area of the house. This way, you can encourage a balance between online time and their offline academic, sports, and social times. Know that there are also many ways kids can access the Internet away from home, including on many mobile phones and game players.

5. **Try to get your kids to share their profiles and blogs with you.**
   Be aware that they can have multiple accounts on multiple services. Use search engines and the search tools on social-networking sites to search for your kids' full names, phone numbers and other identifying information. You're not invading their privacy if they're putting personal info in public "places" online. If their pages are private, that's a good thing, but it's even better if they share it with you.

Childnet International   common sense media   ConnectSafely Smart Socializing Starts Here™   TREND MICRO™

Be Prepared

Safety tips for sharing videos online

Below are some guidelines for young people to follow when posting and sharing videos online.

1. **Tough to take back.**
   Whatever you post is basically permanent. Even if you later delete it, there is a chance that it has been copied, forwarded or reposted. And there are Web archives that hang on to content even after it has been taken down.

2. **What the background reveals.**
   Think about what's in the scene you're recording: posters on your wall, photos on a shelf, school or team t-shirts people are wearing, address signs in front of a house or car license-plate numbers all can reveal your identity or location. What you say during recording can, too.

3. **'You are what you wear.'**
   It's an old maxim with new meaning in online video. Think about what your appearance "says" about you. Would you feel comfortable showing this video to your boss or potential employer, a relative or your future mother- or father-in-law?

4. **Respecting others' privacy.**
   Be respectful of the privacy rights of people in your video. If taping in a public place, be sure to ask permission before including bystanders, and never take video of children without their parents' permission..

5. **Everybody's a videographer.**
   Don't think someone needs a videocamera to record video. Most cell phones and still cameras are also now video recorders. Be aware that when people take out a cell phone, they could be using it as a camera or camcorder.

6. **Be a good citizen.**
   It's your right to express your point of view and even make fun of public officials or policies, but don't be mean or nasty, especially when it comes to people who aren't in the public eye. You can be held legally responsible if you slander, libel or defame someone.

7. **Respect terms of use.**
   Most video sites have terms of service that you must adhere to. Most of them prohibit sexually explicit content, gratuitous violence, and videos that are harassing, defamatory, obscene, libelous, hateful, or violating other people's privacy. Most responsible sites report videos depicting child exploitation and threatening or illegal acts.

8. **Respect copyrights.**
   All reputable video-sharing sites prohibit the unauthorized use of copyrighted material. Of course that means that you can't rip-off segments from TV shows or movies. But it also means: Think about the music tracks you use in videos.

9. **Talk with kids about video bullying.**
   Creating a video that makes fun of or ridicules another person can be extremely hurtful. This and other forms of cyberbullying are a growing problem on the Internet which affects many children and teens.

10. **Kids' Web video viewing.**
    As with all media, parental discretion is not only advised - it's a necessary part of parenting. Even though most of the major sites prohibit pornography and gratuitous violence, there are videos that are not suitable for younger children and there are some sites that do permit video that may be inappropriate for children or teens.

Childnet International

commonsense media

ConnectSafely Smart Socializing Starts Here™

TREND MICRO™