

General Internet Safety Tips for Families



The Internet is now an integral part of everyday life for most people. And within a short period of time, it has evolved from simply being a tool for accessing information and conducting communication and commerce to becoming a significant venue for social activity and interaction. For many young people who have never known a world without the Internet, it is also a vehicle for self-expression, a source of entertainment, and a creativity and distribution tool unimaginable by previous generations.

Know the Risks

The Internet should be a place where kids have fun communicating with friends and learning about the world around them. While using the Internet is an integral part of a young person's life and a necessary life skill, there are risks

associated with it. Young people and parents should be aware of them to avoid or minimize their impact and help keep children's online time constructive.

In general, the positive impact and benefits of the Internet outweigh its risks. However, it is still essential to be aware of the risks and practice critical thinking and common sense to avoid them altogether. In considering the risks, it is important to take into account what may reach young people through the Internet as well as what they may share over the Internet with the outside world. Not all young people will encounter all of the potential hazards listed below, but by being aware of them, families can consider how to respond to them before ever going online.



What may reach them		What they share with the world	
<i>Inappropriate content</i>	<ul style="list-style-type: none"> • Pornographic • Violent, Self-destructive (eating disorders, substance abuse, etc.) • Inaccurate or Extreme 	<i>Personal/private information</i>	<ul style="list-style-type: none"> • That could be used by persons with bad intentions • That may damage a young person's (or a parent's or peer's) reputation, candidacy for school or job, etc
<i>Unwanted contact</i>	<ul style="list-style-type: none"> • Grooming (sexual predator behavior) • Cyberbullying (peer harassment) 	<i>Disparaging comments about others</i>	<ul style="list-style-type: none"> • Libelous, lewd, racist comments. Bullying peers, classmates, relatives
<i>Aggressive or undesired commercialism</i>	<ul style="list-style-type: none"> • Blur between content and advertising • Sweepstakes & requests for personal information (leading to spam, or annoying/malicious pop-up ads) 	<i>Unintended and/or illegal file-sharing</i>	<ul style="list-style-type: none"> • Music, videos, games, other files using a peer to peer service that is not legal or is not set correctly so that the computer can be accessed/hacked by outsiders
<i>Covert web threats</i>	<ul style="list-style-type: none"> • Spyware, hack attacks, viruses, other malicious software 		

What may reach them

Inappropriate content

A lot of discussion and concern has centered around young people's access to websites that promote pornography, violence or self-destructive behaviors. While parents and caregivers should be concerned about the content they see on the web, they also need to consider sites that are or look legitimate, but are fake, have been infected by malicious software, or are used by malicious hackers to steal passwords and other information. It is important to be aware of a website's security and privacy practices, especially if it requires a young person to provide personal information in order to use the site or features and software on it (such as widgets or 3rd-party code for use on social networking sites). Digital security and appropriateness of content are both important factors to think about when considering which sites are appropriate for young people.

Unwanted contact

As a social medium, the Internet enables young people to stay in touch with friends when they are separated from them or to meet new people who share their interests. If a young person is socially active on the Internet, they are very likely managing at least one personal profile on a social-networking site which requires or allows them to publicly share 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. 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 peers) are some examples of unwanted online contact that parents and caregivers should understand and help young people recognize and act on if they ever experience it. In both cases, the first and best response to encourage is to alert their parents so they can figure out next steps together.

For more information, see our Safety Tips on Grooming and Cyberbullying at trendmicro.com/go/safety.

Aggressive or undesired commercialism

The Internet is a powerful marketing tool, and advertising messages targeting young people are plentiful. Parents and caregivers should be mindful of messages that entice them 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 (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, may end up in the wrong hands (to perpetrate hack attacks, identity theft, etc.).



Covert web threats

The massive adoption of the Internet as a social medium has not made it immune to the risks of information security threats. Risks of spyware, spam, viruses, or hack attacks still exist as they always have. But in the case of the social web, attackers mask their attempts by preying on behavior that is normal or intuitive to a young person using the Internet. This is called "social engineering" and attacks can be cloaked with as simple a message as, "Hey, check out this video" in a video-sharing site. The attackers' motive is simple: to make money. And the Internet is an attractive place to make it, since it offers anonymity and a large user base comprised of many unsuspecting users who are more susceptible of falling for the techniques they use.

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

What they share with the world

Personal/private information

A young person who is socially active online – creating personal profiles, communicating with friends, and sharing things about themselves with others – is simply extending what they do offline onto the Internet. But in order to take advantage of online social venues they have to provide self-identifying information from user names to photos to personal opinions, likes and dislikes. In this vein of self-expression, they may also provide too much information, which could be used by people with bad intentions or that may damage their own reputations among people they never intended to have see it. Information posted online could be accessible at any point in the future, so young people should think before publicly sharing anything personal, through any online medium.

Disparaging comments or harassment of others

The anonymity of the Internet can unfortunately encourage offline bad behavior to continue and be exacerbated online. As noted earlier, young people can become targets of cyberbullying, but they can also be as much a participant as a victim in this behavior. Because the information they post can be accessed by anyone virtually forever and can potentially be traced back to them, it is best always to be respectful of others, online or off. More severe comments, particularly those involving physical threats, may be considered a criminal offense.

Peer-to-Peer (P2P) File-sharing services

File-sharing services are a popular tool that enables young people to share media files such as music, movies, or video games. The public discussion and concerns surrounding these types of services have focused a lot on the legal issues (copyright infringements) as well as the age appropriateness of the media being shared (such as pornography or violent games). But in addition to these risks, file-sharing services have increasingly become a destination for cybercriminals to fool people into downloading fake or malicious software. As noted before, their primary motivation is money. A combination of awareness of what is legal and what isn't, proper use of the file-sharing service, and security technology can help young people safely and securely enjoy sharing their favorite forms of media with their friends.

For more information, see our safety tips on P2P File-sharing services at www.trendmicro.com/go/safety



Be Prepared

For what may reach them

Below are some additional basic safety measures you and your child can do together today particularly if your children are just beginning to explore the Internet:

1. Keep computer in a common area.

Where you can be present while your child is using the computer or spot-check its use, as appropriate to the child's age.

2. Agree to time limits for using the Internet and all social devices.

Per day, per week, etc.

3. Keep software security up-to-date.

Make sure you have purchased and installed up-to-date security software to protect your computer from things such as viruses, spyware, spam.

4. Agree on websites your kids can visit (for younger children).

Create a list of websites they would like to visit. Make sure they only use sites that are age-appropriate – for example, many social networking sites have minimum age requirements.

5. Use URL filtering.

Set the URL filtering capability, a parental control feature in most computer security software, to ensure your kids do not see/access sites you do not wish them to see (pornographic, violent, etc.)

6. Download a website reputation service and visit the websites.

Download a free website reputation service and visit each of the websites on your list to see if they are safe from digital security threats (like TrendProtect). This type of service will also continuously provide you with information indicating if a site visited is free from any malicious software that may get installed on your computer without your knowledge.

7. Review the content and the privacy and security policies of the sites your child frequents.

Ensure the content of the site is age appropriate; make sure you understand how and what type of personal information might be collected by the site and how it may be used.

8. Talk with your kids about entering personal information online.

Advise kids to stay on the agreed upon websites only and not give out personal information such as name, address, phone number, age. If they are tempted to do this because of a contest, poll, or membership form, ask them to discuss with you first and only proceed with your permission and involvement; it could be opening the door to spam or something more harmful such as spyware.

9. Ignore unwanted contact from people they have never met.

Unwanted online contact will usually stop if they do not respond or react to it. If it persists, advise them to let you or any adult know about it. You should also report this to the site or service being used to contact your child, and the authorities if you or your child feel he or she is in danger in any way.

10. Run a manual scan with your software security and check browser history.

After they are finished using the computer, do a manual scan to ensure no infections have occurred; you can teach them how to do this and let them to do it themselves if they are old enough. If you wish to, you can also let your kids know that you will check the browser history when they are finished using the computer to ensure they did not wander off onto websites they shouldn't have gone to.

Be Prepared

For what they might share

In general, using common sense and critical thinking are a strong foundation for a young person to stay safe online. Any interactions they have on the Internet should be done with the same approach as they would offline, so talk to your kids about using the guidelines below whenever they are online.

1. Be cautious and wise about what you post.

Think before sharing thoughts, photos, videos that are very personal or less than positive about you, knowing they could also be used against you.

2. Set profiles on social-networking sites to private.

Only those you invite to join your network should be able to see details about you and the people in your network. Even so, it is still wise to think twice before posting anything that is not intended for others to see or know because it can be passed along by friends.

3. Use nicknames, not your real name, to identify yourself

On social-networking sites, in chat rooms, on blogs.

4. Be respectful of others.

Avoid posting anything about another person that is libelous, lewd, racist or in violation of a site's or service's terms of service. Not only will it be taken down, but it could be traced back to you and - if it is considered illegal - may land you or your parent into trouble.

5. Use legal file-sharing services only and ensure they are set properly.

If files are being shared illegally, whether it was intentional or not, you could be held legally responsible for copyright infringement. Also, having the proper settings for the service will ensure that your computer and its contents aren't vulnerable to hackers, viruses, spam, spyware, etc.

For more detailed information and safety tips on the topics discussed in this document, go to:

www.childnet.com

www.connectsafely.org

www.trendmicro.com/go/safety