Internet Safety Tips

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
Inappropriate content • Pornographic • Violent, Self-destructive (eating disorders, substance abuse, etc.) • Inaccurate or Extreme	Personal/private information • 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
Unwanted contact • Grooming (sexual predator behavior) • Cyberbullying (peer harassment)	Disparaging comments and inappropriate content • Libelous, lewd, racist comments • Bullying peers, classmates, relatives • Sexting (explicit images taken and sent via cell phones)

Aggressive or undesired commercialism • Blur between content and advertising • Sweepstakes & requests for personal information (leading to spam, or annoying/malicious pop-up ads)	Unintended and/or illegal file-sharing • 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 or hacked by outsiders
Computer Security Threats • Spyware, spam, viruses, identity theft	

What may Reach Them

✓ *Inappropriate Content*

A lot of discussion and concern has centered on 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.

Safety Tip

- Keep the computer in a common area where you can supervise as needed.
- Use parental control features in most security software to block categories of sites, set time limits, and prevent personal information from being posted online.

✓ *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.

Safety Tip

- Ignore contact from strangers or from people that are attempting to bully.
- Report repeated, hurtful, or troubling contact to the website and to a responsible adult who can help track the communications for remedial action.

✓ *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.).

Safety Tip

• Think critically about offers that are too good to be true. Turn on pop-up blockers in your web browser.
• Use up-to-date security software and if available, the ad-blocking feature which can prevent ads being displayed.

✓ *Computer Security 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. 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.

Safety Tip

• Always use up-to-date security software.
• Stick to reputable sites and read the user license agreements carefully for anything you are downloading.

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 see it. It could also be used by hackers for the purposes of identity theft. 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.

Safety Tip

• Understand anything posted online could be made public and is permanent. Avoid sharing too much information–in words, pictures or videos–that could hurt you in the end.
• Use privacy settings and never share your username or password with anyone.

✓ *Disparaging Comments and Inappropriate Content*

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.

A new trend is the use of cell phones by kids for "sexting", the act of sending sexually explicit messages or photos electronically, primarily between cell phones. The photos are often of themselves or kids they know. This may seem funny to them, but they don't realize they could be charged with the distribution of child pornography, a very serious criminal offense.

Safety Tip

• Do not post or forward anything online that could hurt another person. Some types of harassment or content can be considered a criminal offense, and can be traced back to you.
• Report any bullying or inappropriate content that can be hurtful to another.

✓ *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.

Safety Tip

• Determine if your kids need to use these services at all. They can open up your system to security risks and may be encouraging them to share illegally copied material.
• Always use up-to-date security software to help prevent hackers from installing malicious software on your computer and stealing your personal information.

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:

✓ 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.

✓ Agree to Time Limits for Using the Internet and all Social Devices.

Per day, per week, etc. Some security software will allow you to set specific times when your kids can access the Internet.

✓ Keep Security Software Up-to-Date. (Provided by NPS with Issued Equipment)

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

✓ 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.

✓ Use Web Filtering. (Provided by NPS to Filter the same at Home as in School)

Use the URL filtering capability, a parental control feature in most computer security software, to ensure your kids access only the kinds of sites you feel are most appropriate for them.

- ✓ **Review Content and 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.

- ✓ **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.

- ✓ **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 feels he/she's in danger in any way.

- ✓ **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 visited.

Be Prepared for What They Might Share

In general, common sense and critical thinking are the foundation for young people to become safe, responsible users of the Internet. Any interactions they have online should be done with the same approach as they would offline, so talk to your kids about using the guidelines below:

- ✓ **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.

- ✓ **Use the Privacy Tools Available in Social Networking Sites.**
  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.

- ✓ **Where Possible, Use Nicknames, Not Your Real Name, to Identify Yourself.**
  On social-networking sites, in chat rooms, on blogs.

- ✓ **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 in trouble.

- ✓ **Use Legal File-Sharing Services Only and Ensure They are Set Up 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.

Social Networking Tips

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.

✓ ***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.).

✓ ***Cybercrime***

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.

✓ ***Behaviors Toward Others***

Kids and adults believe everything we do online is anonymous and cannot be tracked back to us. Unfortunately, this believe can encourage bad behavior done offline 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 students** to follow when they are using social networking sites, chat rooms, blogs, or message boards:

✓ **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.

✓ **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 use the highest level of privacy settings possible, that still allows flexibility to use the site in a way that is useful.

✓ **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.

✓ **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.

✓ **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.

✓ 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.

✓ 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.

✓ 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.

✓ 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.

✓ 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. And if your phone has a camera, be sure that the photos you take or share won't get you into trouble. Sending or sharing inappropriate photos of yourself or others to friends on social networks (or text) can end up getting you and others into serious trouble.

Be Prepared

It's important to note that most major social networking sites require all users to be age 13 or older, as noted in their Terms of Use. Assuming they are old enough, below are some guidelines for parents and tecahers to consider when it comes to letting kids use social networking sites, chat rooms, blogs, or message boards.

✓ Ease Into the Process Together.

If you're going to help your kids use social networks safely and responsibly, it's a good idea to use them yourself. There's no need to be a power-user or a technology expert. Just spend a few minutes setting up a profile, using the privacy settings, and connecting with a few close friends or family. It is the best way to help your own kids use it safely.

✓ Consider Keeping an Eye on their Social Network use From Time to Time.

One way is to connect with your kids is to connect with them on the social network. But if that feels like encroaching too much on their space or if you want your own privacy online, there are social network monitoring services that let you do this. You can also use search engines and the search tools on social-networking sites to search for your kids' full names, phone numbers and other identifying information. If you do it 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. You might also consider having them do this themselves so they can see and learn if they are putting too much out in the public domain that they never meant to.

✓ 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.

✓ 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.

✓ 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.

✓ 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.

Safety Tips for Sharing Videos and Photos Online

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

✓ 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.

✓ 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.

✓ '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 relatives, boss, potential employer, or college recruiter?

✓ 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.

- ✓ **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.

- ✓ **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.

- ✓ **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.

- ✓ **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.

- ✓ **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.

- ✓ **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. Depending on the age of your kids and their maturity, consider using the filtering features of sites like YouTube or be nearby whenever they are using video sites.

Glossary Of Terms

Acceptable Use Policy (AUP): A set of guidelines and expectations about how staff/students should conduct themselves online.

Blog: An online diary or chronological log of comments published on a web page.

Bandwidth: A measure of capacity for communication channels. It is usually expressed in thousands of bits per second (kbps).

Broadband: Communications or web access which includes cable and digital subscriber lines (DSL).

Browser History: The web browser maintains a list of websites accessed which allows users to review and quickly access again.

Cache: A place to store files which can be temporary or permanent and is used to speed up data transfer.

Chat: Real-time Internet conference between two or more users usually by typing on a keyboard.

Chat Room: A virtual room where the chat session is held.

Cookie(s): Visited web sites often use these to track users and their preferences so that the next time the user visits that site, it recognizes the user. The websites stores these files within the user's web browser.

Cyberspace: A reference made to the Internet or the online, digital world.

Database: A collection of information organized in a way in which certain pieces of the data stored can be accessed and selected**.**

Download: The process of copying a file(s) from an online source to your computer.

Encryption: A way to convert plain text into secret code (cipher text) to prevent anyone but the intended people to read it.

File attachment: A method used in email to attach files to the email message. A paperclip icon often represents the process of attaching a file to the email.

File Name Extensions: Usually three to four letters that appear after a file name and a period which are used to identify an application program that the file was created with.**(.doc, .exe, .TIFF, .JPG)**

Filter: A type of technology which blocks Internet material or activities which are considered not appropriate.

Firewall: Hardware and software that secures computer files by blocking unauthorized access.

Freeware: Software that is available for anyone to use without charge and cannot be sold or distributed without permission.

Graphics File: A file which holds an image. Popular formats are JPG, GIF, TIFF, PNG and BMP.

HTTP: An acronym for (Hypertext Transfer Protocol) which is the standard communication of the World Wide Web.

Hyperlink: A word, image or phrase that when clicked on will go to another location within the document or another website. It usually appears in a different font color.

Internet Service Provider (ISP): A company that provides access to the Internet.

Internet Surfing: A metaphor for browsing the World Wide Web (www).

IP Address: A numeric Internet address separated by periods that is assigned to each computer connected to the Internet.

Phishing: A form of identity theft scamming where email messages link to fake sites that look so similar to the real ones and personal information is requested to be submitted to the fake but very real looking sites.

Podcasts: A web based audio broadcast converted to an audio format for playback such as MP3.

Portal: Websites such as Yahoo and Google who offer services such as email, search engines and other resources as well.

RSS: An acronym (Really Simple Syndication) which will automatically update the subscribed user with updated news, blogs, audio and video.

Spam: Unwanted, junk email.

Upload: The transfer of a file from a computer to a remote site.

URL: An acronym (Uniform Resource Locator) which provides the specific location of accessing a specific item or source on the Internet.

Web Browser: A program used to access the Internet such as Firefox, Internet Explorer, and Safari.

Wiki: A website that allows visitors to add, edit and change contents posted to the site.