Social Networking Safety

Tips for Parents

They love it! And oftentimes it seems that they can't live without it. The rise of social networking sites has teens throughout the United States fanatical about these addictive websites. Social networking is a platform of online sites that focus on building relationships among people who may share the same interest or activities. It provides a way for users to interact over the Internet.

Users are often identified by their profiles, which can consist of photos and basic information, such as location, likes and dislikes, as well as friends and family. Well-known sites such as Facebook, MySpace, and SnapChat, have taken social networking to a new level. In addition to the convenience of being able to access these websites from a computer, there are also applications on mobile devices that make it easy to access social applications anywhere and anytime.

As a parent, you want to make sure your child is safe when he or she is engaged in social networking. You may find it challenging to keep up with the ever-changing technology. You may also feel like your child is much more Internet savvy than you are, and in fact, that may be true. But as savvy as your teen may be, he or she may not be aware of the dangers of online networking and what precautions he or she should take to stay safe. It is time to talk to your teen about social networking safety.

Familiarizing yourself with the basic terminology that is used on most social networking sites will help you communicate effectively with your teen about the topic.

- Post -A message that can be updated to notify your selected followers of what you are doing or thinking.
- Tagging-To label friends in a photo and link to their profile pages. If tagged, you're notified so that you can de-tag or stay linked to the comment, video, or photo.
- Wall-Area on your profile where friends can post their current locations, comments, pictures, or links.
- Places- This feature allows a user to post his or her current location. This information is then shared with all of the user's followers.
- Friend Request-A person interested in being a friend will send a request, which can either be accepted or denied.
- Blocking- Prevents another user from searching and viewing your profile; you can ban access temporarily or permanently.
- Hacker- Someone who breaks into computers or computer networks and accesses a profile user's information to get money or to break into other personal accounts. Some may also create false profiles or pose as another user.

The four major dangers of using social networking websites are

- Over sharing information. When creating a profile page, most websites will ask for personal information such as home addresses, birthdays, and phone numbers. Giving this information can be very dangerous and will be made public to anyone who visits a user's profile page, especially if privacy settings are not set correctly. Even if account settings are set to private, users are still at risk of their accounts being hacked. If someone hacks into an account he or she will be able to view and use the information. Sharing simple things like your favorite color can tip off a hacker to try to see if you used that as a password on your account. The biggest threat of over sharing information is identity theft. Identity theft is not uncommon in the world of online social networking. Online computer criminals look to steal identities in obvious and not so obvious ways. An obvious way would be someone asking for your social security number. A not so obvious way is luring a user to click on a link that will allow the criminal to download all of the user's personal information. The anonymity provided online makes it easier for computer criminals to go undetected.

- He's not who you think he is. Social networking sites make it very easy to pretend to be someone else. Even if an individual may be friends with someone on the site, anyone can take control of a user's account if he or she can obtain the user's password. As a result, someone who is a "Friend" can ask for money or gain personal information that

can be used to hack into other accounts. For example, you may get a message from a relative asking you for your banking information because he or she would like to wire you some money for your birthday. You may think you're talking to your relative, but in fact the information is being requested by someone who has hacked into your relative's account.

- Location-based services. Location-based services can be one of the most dangerous features provided by social networking sites. It exposes the profile user's location and whereabouts. The service also has a feature that allows users to tag who they are with at any given time. While it can be fun to share your location with friends and family, it can also increase your vulnerability, potentially opening you up to being robbed, sexually assaulted, or worse. Predators can use this tool to track your movements and determine when you are alone or when you are not at home.

- Posting photos. One of the features of online social networking that many teens enjoy is the photo-sharing feature. This feature allows you to post photos 24 hours a day. Whether it is from your computer or mobile device, posting photos can be done in seconds. The Internet makes it easy to obtain photos and use the images in any way a person may choose. Posting inappropriate photos that may be deemed as fun, cute, or sexy, can end up where one least expects it. Photo tampering is a big threat when it comes to posting photos online. The use of photo editing tools allows people to manipulate online images in any way they choose, whether it's used for good or bad purposes. While posting pictures and sharing them with friends can be fun, it can also be risky.

Teaching Your Teen Three Simple Steps To Increase Safety

1. Don't give optional information-When creating a profile, you do not need to enter all of the information that is requested. The set-up page usually requires you to fill out basic information, such as your name and email. Everything else is optional. Do not feel obligated to put your address and telephone number.
2. Third level of privacy- There are three levels of privacy settings to choose from for your profile. There is "open to everyone," "open to friends of friends" and "friends only." The best setting to use is the "friends only" setting on all of your privacy choices. "Friends only" is the strictest level of security; it only allows people that you have accepted as a friend to view information about you.
3. Accept only people you know- Accepting only people you know and trust is a great way to ensure safety when using social networking sites. Doing this can protect you from spammers, pedophiles, and other people who use social networking sites to commit crimes.

When discussing social networking safety with your child, encourage him or her to always use discretion when posting any type of photo, location status, and message. Tell your teen to ask him or herself these four questions before posting to the world:
"Think Before They Post"

1. Should I share this? Will the information you share put yourself or someone else in danger?
2. Do people really need to know where I am and who I am with? - Is it a good idea to let everyone know my exact location?
3. Am I selecting friends online that I can trust? –Always keep in mind that it's not just about what you post, but how others may use that content.
4. Is the information I am sharing transparent? - Before sharing information to the public, does your post give out too much personal information?

Having a discussion with your teen about social networking sites can ease some anxiety about your child's safety. Social networking sites help us stay connected to family and friends. However, it's important to make sure your child knows how to be safe while online. Encourage them to enjoy the sites but to be safe at all times.

For more information on social networking safety visit www.ncpc.org