Online Safety Tips for Tweens and Teens from the Federal Trade Commission

- Think about how different sites work before deciding to join a site. Some sites will allow only
 a defined community of users to access posted content; others allow anyone and everyone
 to view postings.
- Think about keeping some control over the information you post. Consider restricting access
 to your page to a select group of people, for example, your friends from school, your club,
 your team, your community groups, or your family.
- Keep your information to yourself. Don't post your full name, Social Security number, address, phone number, or bank and credit card account numbers — and don't post other people's information, either. Be cautious about posting information that could be used to identify you or locate you offline. This could include the name of your school, sports team, clubs, and where you work or hang out.
- Make sure your screen name doesn't say too much about you. Don't use your name, your age, or your hometown. Even if you think your screen name makes you anonymous, it doesn't take a genius to combine clues to figure out who you are and where you can be found.
- Post only information that you are comfortable with others seeing and knowing about you. Many people can see your page, including your parents, your teachers, the police, the college you might want to apply to next year, or the job you might want to apply for in five years.
- Remember that once you post information online, you can't take it back. Even if you delete the information from a site, older versions exist on other people's computers.
- Consider not posting your photo. It can be altered and broadcast in ways you may not be happy about. If you do post one, ask yourself whether it's one your mom would display in the living room.
- Flirting with strangers online could have serious consequences. Because some people lie about who they really are, you never really know who you're dealing with.
- Be wary if a new online friend wants to meet you in person. Before you decide to meet someone, do your research: Ask whether any of your friends know the person, and see what background you can dig up through online search engines. If you decide to meet them, be smart about it: Meet in a public place, during the day, with friends you trust. Tell an adult or a responsible sibling where you're going, and when you expect to be back.
- Trust your gut if you have suspicions. If you feel threatened by someone or uncomfortable
 because of something online, tell an adult you trust and report it to the police and the social
 networking site. You could end up preventing someone else from becoming a victim.

Tips for "friending" on Facebook

- Start with your kids' age. If they're in middle school, it may be a sound policy to know what they're posting, since kids that age don't necessarily understand that they're creating a digital footprint that will long outlast the passions of the moment.
- Talk to your high school-aged teens about whether or not they're comfortable letting you friend them. Many will be. This is a case of "know your kid," and it comes down to trust. But establish rules: No drug talk, no nudity, no pictures of drinking, no hate speech, no bullying, and no posting party locations all of these lead to ruin. Most of all, remind your teens that whatever they post will be in the cyberworld forever. (Keep watching Facebook's Terms of Service, by the way, since a recent and almost as recently recanted update said that the company owned everything anyone posted forever.)
- Don't fill your kids' pages with your comments. As it is, simply having parents is mortifying enough at this age. Their friends don't need evidence of your existence (and you can always send them private messages).
- Don't friend your kids' friends. See reasons above.
- Remember: They can see what you post. If you're a friend, also be a role model. Keep your nose clean.
- Choose your battles. You will see the good, the bad, and the truly unfathomable. If you don't want your kids to unfriend you, don't comment on every transgression. Keep it general.
- Remember, you're the parent. Even if you aren't your kids' Facebook "friend," your job is still to pass your values along to them and to help them learn how to be safe and responsible on or offline.

http://www.commonsensemedia.org/facebook-parents