ConnectSafely
Smart Socializing Starts Here™

Social Web Tips for Teens

Be your own person. Don't let friends or strangers pressure you to be someone you aren't. And know your limits. You may be Net-savvy, but people and relationships change, and unexpected stuff can happen on the Internet.

Be nice online. Or at least treat people the way you'd want to be treated. People who are nasty and aggressive online are at greater risk of being bullied or harassed themselves. If someone's mean to you, try to ignore them - often that makes them stop. Use privacy tools to block them from viewing your full profile and contacting you.

Think about what you post. Sharing provocative photos or intimate details online, even in private emails, can cause you problems later on. Even people you consider friends can use this info against you, especially if they become ex-friends.

Passwords are private. Don't share your password even with friends. It's hard to imagine, but friendships change and you don't want to be impersonated by anyone. Pick a password you can remember but no one else can guess. One trick: Create a sentence like "I graduated from King School in 05" for the password "IgfKSi05."

Read between the "lines." It may be fun to check out new people for friendship or romance, but be aware that, while some people are nice, others act nice because they're trying to get something. Flattering or supportive messages may be more about manipulation than friendship or romance.

Don't talk about sex with strangers. Be cautious when communicating with people you don't know in person, especially if the conversation starts to be about sex or physical details. Don't lead them on - you don't want to be the target of a predator's grooming. If they persist, call your local police or contact CyberTipline.com.

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 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.

[to be included with parent letter]

ConnectSafely
Smart Socializing Starts Here™

Social Web Tips for Parents

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 social-Web 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 because 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 - not in kids' rooms - to help you stay aware of their online time. 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.

Try to get your kids to share their profiles and blogs with you, but 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.

[to be included with parent letter]

How to use Facebook Privacy Settings

Some basic advice on how to configure Facebook's privacy settings.

By Larry Magid

Facebook's privacy settings, in most cases, don't permit you to expose your information to everyone on the Web. By default, the settings typically show your profile and other data only to "My Networks and Friends." While that might include a lot of people, it doesn't include the entire world.

These settings can be modified, but most of them can only be tightened. With a few exceptions, you don't even have the option to make a lot of your information available to the public at large. One exception is media files such as photos and videos, which, by default, can be viewed by "everyone." But you can use privacy settings to restrict who can see your photos all the way down to specific friends or even "only me."

Mouse over to privacy settings

Start by hovering your mouse over the "Settings" tab near the upper-right corner and select Privacy Settings. There you'll find options to control who can see your profile as well as other information about you, such as your "personal info," status updates, photos, videos tagged of you, and who your friends are. You can control who can see your profile within Facebook and you can turn off access to public search engines such as Google. There are plenty of other settings, including ones to control who can write on your wall and who can comment on notes, photos, or other elements of your site.

Settings vary according to what you're trying to control and, because of the confusing user interface, you might have to hunt around a bit. For example, to change the privacy settings on your own photo albums within the Privacy Settings area you would have to find the fine print under Photos Tagged of You that says "Edit Photo Albums Privacy Settings" or navigate from the Applications tray at the bottom left corner of your browser. That "privacy wizard" they're

working on can't come a moment too soon.

Another relatively unknown feature is the ability to create multiple friends lists and assign different privileges to people on different lists. For example, if you want only certain people to know your cell phone number you can create a list like "good friends" and another called "colleagues" to make that information available only to people on those lists. You can create lists by clicking on the Friends tab on the blue navigation bar and then clicking on "Make a New List" in the left column.

Third party applications

Be especially careful when it comes to third-party applications. For example, I use an application from Eye-Fi that automatically syncs my photos to Facebook and Flickr through my Wi-Fi network. When I review cameras, I often take ugly and stupid test pictures and, if I'm not careful, those pictures can be automatically loaded to my Facebook page for everyone to see. But my most embarrassing moment was about a year ago, when I tried out the New York Times Quiz on a day I hadn't read the paper, only to have my low score posted for all my Facebook friends to see, including my editor at The New York Times.

Regardless of how you configure your privacy settings, there is a reality of the social Web that can't be configured away. Any digital information that is posted can be copied, captured, cached, forwarded, and reposted by anyone who has access to it. Even if some embarrassing photo or information is up for only a few minutes, there is the possibility that someone might copy it and send it around. And--as many people are painfully aware--friends can become ex-friends. So even if you're reasonably careful about who you let on your page, you never know what they might do with the information you post.

[to be included with parent letter]

ConnectSafely
Smart Socializing Starts Here™

How social influencing works

One of the best protections for online youth is awareness of how other people try to influence them - here are some of the ways....

by Anne Collier

Now that our kids' entire circles of friends, in their school and beyond, are in public spaces on the Web, blending the details of their personal and social lives with messages and images from people with all sorts of interests and intentions - from finding friends to promoting a band to sexual exploitation - it's a good idea for them to get a handle on how people influence each other.

"One important foundation for making safe and responsible choices online is ensuring that you are, indeed, the one who is making the choice," writes Nancy Willard, director of the Center for Safe and Responsible Internet Use, who has researched this in the context of teen social-networking for a book she's working on.

Of course, sometimes the results of social influence are good: for example, in encouraging, for example, tolerance or conservation, Nancy explains. Other times, a result can be destructive. "Grooming," the term used by law enforcement people to describe how a sexual predator influences a child toward an in-person meeting, is one stark example. "Virtually all of the Internet's risks ... are grounded in the negative impact of social influence," she writes. It's always empowering to understand how social influencing works - kids can see influencers' techniques for what they are and socialize more safely and confidently, online or offline.

Here are six basic influencing techniques, described in much more detail in a chapter in Nancy's forthcoming book, reprinted with permission here:

1. **Rule of reciprocity**. An "extremely strong basic norm," it goes: If someone gives you something, you're obligated to give him something back. Something in return for gifts given (a sexual predator's tactic), but also the reason why charities put address stickers in

their solicitations for support. Sub-tactic: "rejection-then-retreat." The manipulator makes an extreme request; it's rejected; she then responds with a smaller request, increasing the rejecter's sense of obligation. Solution to consider: "This person's attempt to manipulate you cancels any obligation or indebtedness you might feel."

2. **Commitment & consistency**. "But you *told* me you'd do it, right?" The influencer's basically saying, "You made a commitment to this, so be consistent, or you're not trustworthy." Consistency is valued [in society] because ... a person who is consistent can be trusted to act in certain ways under certain conditions," Nancy writes. Sexual predators use this one a lot, she adds. The question often asked is, "You trust me, don't you?" "It is a rare child who will respond with a 'no'." There's also the effect of group commitment (the obvious downside being groups promoting hate, violence, suicide, eating disorders, etc.) Toward avoiding manipulation: "The way you can tell if you have made a commitment that is now wrong is to pay close attention to how you feel inside. If you have a gut reaction that something g is wrong, be sure to pay attention to this."
3. **Social proof**. Another form of group think: Even if the evidence contrary to a group's philosophy or decision is plain, an individual will in many cases go along with the group's position, a study found. It works best, Nancy writes, "when there is some level of uncertainty or ambiguity in the situation." For example, viral (word-of-mouth) marketing, collaboration in or condoning of bullying, promotional seminars for a business model. Again: "Listen to your 'gut' and take a close look at the situation. You might need to get away from others to think about on your own... Make your own choices."
4. **Liking**. If we like someone, we're "far more likely to comply" with what they want. We're usually more influenced by people we like because of a number of possible factors: they're attractive, they're "like us," they praise us, they convey a sense of familiarity, or they're associated in our minds with positive things. "The Internet provides [influencers] the ability to 'image manage' - to create an online 'persona' that makes them more likable. Solution: Critical thinking - asking ourselves how much we *really* know about the persona or image being presented (and knowing that the Net's anonymity can make person and persona seem like the same thing).
5. **Authority**. "There is strong pressure in our society to comply with requests or demands from a person in a position of authority," though Nancy later adds that there's evidence the Internet is eroding this tendency. "Young people who are growing up with this technology appear to be far less sensitive to ... authority." Answer: two key questions, actually. Ask yourself: "Is this authority truly an expert - is there independent evidence of

his/her person's expertise and credibility?" and "How truthful can we expect this expert to be" - does he/she have something to gain from my acceptance or compliance?

6. **Scarcity**. An influencer may present something (product, behavior, opportunity) as scarce, unusual, or having restrictions attached to it, which tend to make it more valuable or appealing in people's minds. Nancy looks at the impact of this principle on, for example, "Managing youth access to pornography through the use of filtering software, [which] would backfire by creating an increased level of 'value' for the restricted 'thing'.... Parents should remain mindful of the scarcity principle in seeking to guide their child's Internet use... 'Just say no' is likely to be significantly less effective than 'Just say know'."