Teen Cybersafety Guide

I know. You're sick and tired of being lectured to. You know how to keep yourself safe online. You're not a baby! You use privacy settings on Facebook. You aren't meeting strangers offline. You are careful. You aren't sharing too much info and you think the media has blown the risks out of proportion. Great. You can stop reading now and go have fun doing something else.

For the rest of you, just in case there is something you hadn't thought about, or you have a friend who isn't as careful and smart as you are…

Don't Be Stupid!

Most teens understand enough about cybersafety to write a book. They don't want to be hurt or get into trouble. The problems that WiredSafety are seeing when teens are connected through cell phones, game devices or the Internet itself are either because the teen didn't know enough about the technology, or because they were just being stupid.

Stupid is when you decide to pose nude for a cell phone photo or webcam video for any reason. Stupid is when you believe your boyfriend when he tells you he would never share the photo with anyone and no one else will see it. (Even if he is trustworthy, he might have a little brother who isn't, or a parent who checks his cell phones once in awhile.) Stupid is when you think no one can figure out that the anonymous email, IM or MySpace post you made came from you. (They collect the electronic footprint when you interact online that can be traced back to your computer.) Stupid is when you do things online that you would never do offline just because you can. Stupid is when you think that cute sixteen year old boy or girl you met online is always a cute sixteen year old boy or girl. Stupid is when you think someone will send you an iPod just for playing a game and giving them some "harmless" personal information (like your dad's credit card number). Stupid is when you know better, but do it anyway.

There is something about the technology that makes you think that the people who are reading your posts or blogs are only the ones you want to read them. You talk to them. You post pics and videos for them. You are funny for them. But sometimes "they" include others who would love to harass you, get you back for something or are just plain old creeps.

And when you are typing as fast as you do, you leave out words or letters, think something is clear when it's not or even send it to the wrong person. When you make these mistakes, the person who receives it may not know that you weren't trying to freak them out. And they may react as though they were harassed or threatened. That's when you get reported to Facebook or the police, or the target of an "Oh, yeah? Well you started it," campaign.

Okay, Already. You Told Me What I Can't Do. What CAN I Do?

Teens tell Parry Aftab (a cyberlawyer who is also the founder of WiredSafety) and her Teenangels (Teenangels.org) that they know what *not to do* already. They want to know what they *can* do. So here goes.

Copyright © 2009 Parry Aftab, All Rights Reserved by WiredSafety.
May be duplicated by schools and community groups.

You can post a picture online. Just make sure it's one your parents, principal, a predator and the police can see without you getting hurt. And for good measure, add in prospective college recruiters and employers and the love of your life too. And the picture you post should be your own. If others are in it, ask first. It's common courtesy and hopefully will be reciprocated when they are thinking about posting that picture of the two of you in sixth grade that you thought (and desperately hoped) was deleted long ago!

And be careful what you tag. Every tag identifying you in a pic is a potential sharing of too much information. A picture can say a thousand words and in cases where the pics are tagged and circulated, can come back and haunt you. Tagging makes it easier for college recruiters to see what you really do, instead of what you said on your application you do. Your parents might see you drinking at a party. Or when you were somewhere you weren't supposed to be at that time, you are outed big time.

You can have a Facebook (or other social networking) profile and still be safe. It just requires that you are choosy. You have to be choosy about who can see it and what they can see. (Visit Facebook.com/privacy and understand your privacy choices.) You can decide that one friend can see everything, but another one can't see some pics. You have to be choosy about the site itself. Who else is on that site and what kind of an impression does the site make? Fun? Freaky? Wild? Slimey? Choosing your social networks is like choosing where you want to live. Remember who your neighbors will be.

You should also delete old profiles you are no longer using. It's pretty easy if you know your login and password. But if you forgot the login and password, or aren't using the same email address you had in sixth grade when you set it up, it can be harder. Ask the network for help if you need it. Most have a procedure to shut down old profiles and prove they are yours.

You can talk to online "strangers" safely too. We know that parents will freak if they read this one. They have warned you since you were three to avoid "strangers." Then "strangers" were creepy men in black raincoats who hadn't shaved in weeks. Now "strangers" are people you don't know in real life that you have met online.

Think of it this way. If you were on a bus with your mother when you were five and an old lady sitting across the aisle compliments you on your shoes, would you run screaming from the bus? She's a "stranger" right? But she wasn't threatening, creepy or inappropriate. At the same time, your mother would not have whipped out her wallet and told the old lady that she had bought the shoes at Walmart and paid for them with her VISA card and given the old lady the account info.

It's not talking to strangers that is the problem. It's what you talk about. This works online and offline. If you meet someone online from Australia, it would be interesting to find out what an Australian teen does for fun. Do they all have pet kangaroos? And they would have similar questions about teens from Texas. Do they all ride horses to school? And maybe they will have less boring things to share too. ☺

When communicating with new people online that you don't know in real life, remember the bus story. No credit card information ☺ and nothing you wouldn't tell a stranger on a long bus ride. And remember:

- They are not your "friends" just people you met online.

Copyright © 2009 Parry Aftab, All Rights Reserved by WiredSafety.
May be duplicated by schools and community groups.

- They shouldn't get information you wouldn't give to an offline stranger.
- And that cute sixteen year old boy (or girl) you met online may not be cute, may not be sixteen and may not be a boy (or girl).

How can you be safer when meeting online friends offline?

There's no way to be entirely safe when you meet people in real life, period! And while we will tell you never to meet them in real life, some of you will ignore us and meet them anyway. The idea is to get you back safely, if you do. So, if you are going to ignore our advice about meeting people offline, you can stay safer as long as you remember:

- Go as a group. (Parry suggests bringing some sumo-wrestlers with you too. ☺) They can always give you some privacy later once the person is who they said they were. Even consider bringing a parent (if they are cool parents ☺).
- Meet in a very public place, but not a noisy one like an amusement park.
- Have an exit strategy. If you decide this was a bad idea, have a plan for leaving safely and quickly.
- Start out by telling them before you meet that your parents are waiting for you in the Mall (or wherever you are meeting) and you won't have much time. You can change that if you feel comfortable.
- Have realistic expectations. Remember that everyone lies a little, so be prepared and make sure *you* only lied a *little*.
- Take things very slowly. You may think you know and can trust them, but you only know what they said, not necessarily who they are inside. Give yourself time to get to know them in real life before taking it any further.
- Trust your gut. If things feel wrong – get out of there right away. Don't worry about hurting their feelings.
- And if it's a creep, not the person you thought you were meeting, report them. Even though your parents might find out and be very unhappy, you might be helping protect the next potential victim.

Now, for what you *should* do

ThinkB4uClick! Suggesting that a teen slow down and proofread their texts or IMs is probably a waste of time. But taking a second to decide if you really want to send that or whether you will regret posting something is a good idea. They only time you can protect yourself from the consequences of things going wrong is BEFORE you click the "send" button. What you post online stays online – forever! (One of Parry's favorite lines, but true.) Deleting it afterwards may not delete it from everyone else's copies, Google or what was already printed out or forwarded.

Copyright © 2009 Parry Aftab, All Rights Reserved by WiredSafety.
May be duplicated by schools and community groups.

Use privacy settings on all your profiles and photo and videosharing pages. You want to decide who can see what. But always remember, while you may restrict your Facebook to the group for teens in your high school, most groups have people in them who don't belong there, starting with teachers and school administrators and coaches. Assume they are reading your stuff too when you post to a group.

Respect yourself and others. It's a boring message, but probably the most important one we can share. Put yourself in a mental time machine and fast forward to when you are 30 years old. What will you be doing with your life? Who will be important people in your life then? Now look at your profiles and online posts, pics and videos. Is there anything there that you wish (as a 30 year old) you could erase? The time to do it is now, before it affects your future. What seemed like a good idea at the time, especially if you had a beer or two at a party, may not be when you wake up in the morning. And don't do anything online that you wouldn't do offline – that's the Internet Golden Rule.

Choose a password that is easy to remember but hard to guess. Most teens (and adults) choose passwords based on "20 Questions." They use the same 20 questions to come up with their passwords, like their middle name, their pet's name, their birth date, the town they live in, their favorite movie, their best friend's name, the car they want to drive, the year they graduate, the college they want to attend, etc. The problem is that these are pretty easy to guess when you know someone pretty well. Just think about how many of these you could answer about your friends and others in your class. And if you can guess theirs, they can probably guess yours too, unless you are careful.

Lots of security experts tell you to use a password with upper and lower case letters, numbers and symbols. That might be good for security experts, but it's really hard to remember. So, you have to write it down and stick it on a post-it sheet on your monitor to remember. How secure is that? Not very!

Instead, use a sentence with a number in it. You start it with a capital letter and end it with punctuation (a symbol!). Upper case, lower case, numbers and a symbol. Easy to remember and hard to guess. Just make sure you aren't using your favorite quote or something you have posted on your Facebook page. Teenangels (teen Internet safety experts at teenangels.org) tell other teens to use a different password for each site. You can use the site name in the sentence and it's different for each site and secure, as well as easy to remember. "Facebook has more than 225 million users!" Wow! (And it's a pretty good password once you leave out the spaces.)

Or choose something only you would know, that is easy for you to remember and no one else can guess (even and **especially** your "BFF"). Choose your favorite character in a book and how old you were when you first read that book, or the best birthday present you ever got and how old you were when you got it. That gives you numbers and letters and is easy for you to remember, but hard for others to guess. Get it?

More than 70% of teens polled said that they had shared their passwords with at least one friend (often their boyfriend or girlfriend). That's one friend too many, especially when friends get into fights or couples breakup. It's not smart since, when armed with your secrets and your passwords, friends can do some serious damage.

It's also not a good idea to click "save my login and password" when using a computer that anyone else can access, like your little brother or sister, your friend's computer or one at school. Let your friends

Copyright © 2009 Parry Aftab, All Rights Reserved by WiredSafety.
May be duplicated by schools and community groups.

know that friends don't ask for their friend's passwords. Find another way to show them how much you trust them.

Cyberharassment, Stalking and Cyberbullying

Teens say that "cyberbullying" is sooo "middle school." They are too mature to do those kinds of things in high school. Think again! While it might be called cyberharassment instead, or might not even have a name in high school, when people take over your accounts, pass nasty rumors, have a quiz on how ugly, fat or stupid you are…they are cyberbullying you. Cyberbullying is when one minor uses technology as a weapon to hurt another minor. Whether they are passing around a nude pic of their victim to embarrass her, or sending around IMs lying about what she said or did, or reprogramming his cell phone, it's cyberbullying. When they steal or misuse your password and pretend to be you online, it's cyberbullying. So, call it what you want, teens use technology to hurt each other all the time.

All fifty states have cyberharassment laws and if you send a message online designed to harass or annoy someone anonymously, you can go to jail for up to two years under federal law too.

Often offline bullies start this stuff. But sometimes you start it when you overreact to something someone else did or said. "They started it" doesn't matter. The best way to handle any harassing message you may receive is to "stop, block and tell!" You should stop and not answer back. It only feeds the harassment campaign. You should block the person or message. Why torment yourself further or give them access to you? And you should tell someone you trust, preferably an adult. Teens have committed suicide when cyberbullying gets out of control. Talking to someone can help you keep things in perspective. Using an adult to confide in means you are never confiding (without knowing it) in the cyberbully. (Seventy percent of cyberbullying occurs anonymously, so you never know if it's your best friend or worst enemy. But you know for sure it's not your teacher, guidance counselor or your parents.)

And if you are tempted to answer back…do something else. Parry Aftab and Teenangels call this "Take 5!" Do something you love to do for five minutes to help you calm down. Just make sure it doesn't involve a cell phone, computer game device or computer, so you won't do something you will regret later.

Cyber-Romance

You're bored, it's Saturday night and he has a great pic on his Facebook. You are finding love in all the cyberplaces. But how safe is it to flirt online, or meet someone in real life that you only know online?

Before we begin, remember that "flirting" doesn't mean taking off your clothes for the camera. You should already know that's just plain stupid. (If not reread "Don't Be Stupid" above. ☺) Flirting should also not involve "cybering," since that can come back and haunt you. Be funny. Be interesting. Be gorgeous or an athlete. Be smart. Talk about things that you won't regret later on. Don't share secrets.

Then if you want to take it further, move to a webcam or the phone. (Block caller ID though and remember that they could be recording the cam chat.) Take it slow. And check them out. Visit their school website or Facebook group and see if you can find them there. Check any other personal details they have provided too. If enough time has gone by and s/he is consistent, hasn't been lying (to your knowledge) and checks out, you can consider meeting them F2F. But you'll need to follow the safer

Copyright © 2009 Parry Aftab, All Rights Reserved by WiredSafety.
May be duplicated by schools and community groups.

meeting rules above. And remember, the only thing hurt is your reputation if something goes wrong online. But teens have really been killed by someone they agreed to meet in real life, after only knowing them online. So, think twice, three times…be careful.

Sexting and Sexing

Sexting uses cell phones to take nude or sexual images and share them with one or more people through text messages. Sexing uses any technology to take, share or store sexual or nude images. While sexting is relatively new, sexing has been going on for years. The first case Parry encountered was in 1998, where a teen girl took videos of herself to give to a boy she liked. He shared that video with everyone on Limewire! (And didn't ask her out either.)

All teens know it's not smart to do this. But many do it anyway. They do it because they are in love. They do it because their boyfriend begs them to do it. They do it when they are bored, desperate, drunk, high or just plain stupid. They do it when they like someone and want to get their attention fast. They do it to impress others with how sexy or well-endowed they are. Younger teens and preteens do it to attract older boys or because they think it makes them more "mature." The point is not why they do it. The point is what happens afterwards.

Jessie Logan, an eighteen year old high school senior from Ohio, took a nude picture and shared it with her boyfriend. They broke up. You know the drill. Everyone in her town saw the picture. They called her names and were horrible to her. When no one tried to help her, she ended up taking her own life. While this is an extreme case, the humiliation can be more than some teens can handle. And the pics often end up in the hands of creeps who post and share them with other creeps. Some teens have even been blackmailed into doing things they didn't want to do, because the blackmailer knew about or had a copy of one of those pics or videos.

And police and prosecutors are now treating this as a serious sex crime. Teens who have taken a nude picture of themselves are being charged across the US as child pornographers and are becoming registered sex offenders. Those who forward the pics are being charged with distribution of child pornography. And those who keep a copy are being charged with possession of child pornography. If you become a registered sex offender you can't live near a school or public park. Your college must be informed and so will your employers. You will be forever grouped with those creeps we try to avoid. And try and explain that the reason you are a registered sex offender is because you took a nude pic of yourself and posted it on MySpace. Who will believe you? Everyone will think you molested a child.

These are real risks and happening to teens across the US right now. So if he tells you that you can prove you love him by taking a nude pic and sending it to him, tell him if he loved you, he wouldn't ask.

Confiding in Strangers Online to Provide You with Important Advice

It's tempting to share secrets or search for places online where you can get advice on things you may not want to discuss with friends or even your parents. But what makes you think that a stranger in an online forum is smart enough to give good advice? And why would you post information in public that you wouldn't share with family or friends in private?

Copyright © 2009 Parry Aftab, All Rights Reserved by WiredSafety.
May be duplicated by schools and community groups.

There are some very good places to visit online where experts can advise you on health, safety and personal matters. But you can't always tell which ones are trustworthy or which ones are crackpots posing as experts. Ask around. Ask your guidance counselor at school, or use a trustworthy resource to help you find one. You can start by looking for a .gov site (they are all run by governmental agencies). Or find a charity you know offline or have heard about in a magazine or on a TV show you trust. Then use privacy settings, a special email address you create just for this and think carefully before you share. The best advice may come from people you trust who know you in real life. But online help can be there when you need it 24/7.

Who Knows More – Teens or Parents?

If we are talking about the Internet, the answer is obvious (even if your dad is Bill Gates). Teens know more about the Internet, at least the way they use it. They know more about cell phones and gaming devices too. But, like it or not, parents know more about life. The good thing is that you can both share what you know with each other pretty easily.

You should "have the talk" with them and let them know you won't do anything stupid, you care about staying safe and know what you need to know to do that. Show them your Facebook profile. (Whether you "friend" them or not is up to you.) Show them where you spend most of your time online. Teach them how you search for things. Help them install and use security software.

And offer to help keep your siblings, nieces, nephews or cousins safer online. Help your parents set up their own Facebook or Flickr account. Show them how YouTube works. (But be careful which videos you show them. ☺) Teach them about privacy settings and remind them to check with you before posting any pics of you online. Talk with them about what you want them to do to help you.

Parry Aftab said "the best filter is the one between your ears." Let your parents know you have a pretty powerful filter that's called good judgment and strong values. Remind them that they can trust you and promise to come to them if anything goes wrong. They can't help you if they don't know you need help. You should never face things alone. That's what families are for.

Now, have fun and be safe! And if you want to learn more and help others stay safe online, join Teenangels. (Drop by Teenangels.org and get an application.)

Copyright © 2009 Parry Aftab, All Rights Reserved by WiredSafety.
May be duplicated by schools and community groups.