Kids and Tweens Cybersafety Guide

Kids and tweens want to stay safe. They want to be able to play games online without getting cyberbullied. They want to know how dangerous things really are and what they can do about it. They want to know when and how to ask for help. They want to know how to find good sites and avoid bad ones and how to tell the difference. We'll share what you want to know and how you can be safer and help keep your friends safer online too.

Talking to Your Parents

Even though kids may know more about technology, parents know more about life. That's why we need to trust them when we need help online. Maybe they won't know how Club Penguin works, or the best way to earn points on Webkinz or BuildaBearville, but they can help when things go wrong. It's their job to protect you. But if you don't ask for their protection, they won't know that you need their help.

The best time to talk with your parents about staying safe online is now, before something goes wrong. Some parents know lots about the Internet and cell phones, but some don't. If your parents already use the Internet, you should show them your favorite sites and talk to them about why you like them. Let them know who your online friends are and how you are already working on keeping yourself safer online. If your parents don't use the Internet, or only use it a little, you might have to take it slowly and show them how Google works and help them understand about online games and virtual worlds where you can play online with lots of other kids and tweens.

Show them how instant messaging works, and let them see who is on your "buddy list." Most parents are surprised about how careful kids and tweens are. Let them know your own safety rules and how you and your friends find ways to stay safer online.

If you are lucky enough to have a cell phone, show your parents how it works. Parents usually use cell phones just for making calls, or sometimes use it for email or texting. But they don't know all the cool things their cell phone or yours can do. Show them how to download and play music. Help them send a photo message or play a game. Download some fun ringtones with them. If you know, show them how to set passwords or security on the cell phone and if you don't know, find out how. Set a screen saver of you and your parents for their cell phone. (That way you can choose the pic you like instead of a boring one. ☺)

Get them to promise not to overreact if anything goes wrong. Also remind them that you are trustworthy and careful. You may want them to sign a safe surfing contract with you. (WiredSafety has one you can download and print out.) In the contract, you promise to follow some rules and they promise not to overreact.

Promise that you will come to them when things go wrong online. But to do that you'll need to how and when to get help.

When and How to Get Help When Things Go Wrong Online

If someone is being mean to you or has threatened you or someone you care about, you have to tell right away. Even if you aren't sure if they are serious. The thing to think about is whether or not they scared you or made you worried. If so, you should get help from your parents. Print out the messages to show them, and save a copy if you can. Then log off. Do something else until you can talk with them.

If you end up at a bad site by mistake, don't worry that your parents will blame you for going there. You already got them to promise not to. Let them know right away. They can help you feel better.

If someone is threatening to hack you, has stolen your passwords (we'll teach you how to make that harder for them next) or accessed your accounts without your permission, let your parents know as soon as you can. They may need to install or update your antivirus software and firewalls, help you get your account back or notify the site that your account has been compromised. (That means someone used it without your permission.)

WiredKids.org and StopCyberbullying.org say to "stop, block and tell!" if anything hurts your feelings or upsets you online. Stop – don't answer back, Block the person or message and Tell! a trusted adult (like your parents).

Strangers Online

A great thing about the Internet is being able to connect with kids and tweens from all over the world. They are "strangers," but not the way we mean when we say "don't talk to strangers." Those strangers are creepy old people. But you can't always tell if it's a ten year old from Australia or a creepy 50 year old trying to trick you.

Some kids and tweens worry a lot about this. You shouldn't. You can avoid them and stay safe. So, how do you avoid creepy people online? It's easy if you follow some simple rules.

1. Don't talk to people you don't know in real life when you are online, without your parent's permission. Not everyone is creepy, but it's better to be extra careful since they can be tricky.
2. Don't open IMs, emails or webcam chat requests from anyone you don't know in real life. Restrict the people who can message you to those on your buddy list. It's safer that way.
3. Don't share personal information online, even with people you know. Tweenangels (Tweenangels.org) say not to post anything online that you wouldn't put on a billboard on a superhighway for everyone to see.
4. Only use sites that are safe for kids and tweens. That means don't lie about your age to use Facebook or YouTube. You're safer with kids and tweens your own age than you are at a site with lots of grownups and older teens. Kids and tweens are more fun anyway! ☺
5. If anyone asks you questions, shows you pictures or otherwise makes you feel uncomfortable or acts creepy in anyway, tell your parents. By reporting them, you might be saving another kid or tween who isn't as careful as you are.

Remember…it's your parent's job to help keep you safe and protect you online and offline. Trust them and let them know when you need their help.

Passwords – Easy to Remember, Hard to Guess

Most kids and tweens (and even adults) choose passwords based on "20 Questions." That means that they use the same kinds of questions to come up with their passwords, like their middle name, their pet's name, their birthdate, the town they live in, their favorite movie, their best friend's name, the car they want when they grow up, etc. Just think about how many of these you know about your friends or how easy it is to guess those things about your friends and others in your class. They can guess your answers to these questions too. Why make it easy for them to guess your password?

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 try a trick that the Girl Scouts created, called "Designer Passwords." (They have a great site on cybersafety at lmk.girlscouts.org.) Choose two words that you can connect in a special personal way, like your favorite movie and your favorite candy to eat in the movies. (Don't use that one, though, in case your friends read this too!) Is your favorite movie Star Trek? Okay. Is your favorite movie candy Twizzlers? Great. Your "designer password" is "startrektwizzlers." But you're not done yet.

Tweenangels.org tells you to use a different password for each site. That way if someone guesses your password for one site, they can't get access to them all. So, we take your designer password and add something that stands for the site where you are using it. For example, your Webkinz password can be "startrek<u>wknz</u>twizzlers" with the" wknz" part standing for WebKinz. Or if your Webkinz name is "Starangel" you can shorten it to "SA" and add that to your password for Webkinz. (You can do the same thing for each site, to help you remember your password and still have a different one for each site.)

Or choose something only you would know, that is easy for you to remember and no one else can guess. Like your favorite character in a book, or the best birthday present you ever got and how old you were when you got it, like the DSi you got for your 12th birthday = "DSi12". Easy to remember and hard to guess! You can create a special version for each site, just like the designer password versions for each site.

Just two more things. More than 85% of elementary school students have shared their passwords with at least one friend. That's one friend too many, especially when friends get into fights. If your friends have your passwords and your secrets, they can do lots to hurt you online.

And make sure you don't click "save my login and password" when using a computer that anyone else can access, like your brother or sister, or your friend's computer or one at school. The only ones to have your password should be your parents. You can trust them not to use it to hurt you, steal your points or

send mean messages while pretending to be you. Let your friends know that friends don't ask for friend's passwords if they care about you.

Now that you are a password expert, teach your parents how to choose their own passwords that are easy to remember but hard to guess. They will be surprised at how smart you are!

Finding "Good" Sites and Avoiding "Bad" Sites and Safe Searching

There are some sites we know are fun and safe. Disney.com, PBSkids.org, Nick.com, Webkinz.com, ClubPenguin.com, BuildaBearville.com, KidZui.com, SesameWorkshop.com, Nickjr.com, CartoonNetwork.com, Lego.com, Candystand.com and Yahooligans.com. We know that because our teachers, school librarians and friends tell us about them. We may read about them in Weekly Reader or Scholastic Magazine. Sometimes we find them on the packages of our favorite toys.

But what about finding new sites? How can we find the good ones and avoid the bad ones? If you type something into Google, the sites that come up might not all be good sites that are appropriate for kids and tweens. If you are looking for funny videos and search YouTube, not all of them will be right for kids and tweens. So, what can you do to find more good and fun sites? Here are a few tips:

1. Ask for suggestions. Ask your teachers and your school librarian. If you have a library media specialist in your school, ask them too. Visit sites like Tweenangels.org for recommendations from other kids and tweens. Ask your friends and family (but make sure you only ask the trustworthy friends and family members).
2. Trust the companies you trust offline. Most of the sites we mentioned are built by companies we trust offline too. Build-a-Bear Workshop is a fun place to visit in the malls, just as it is fun to visit online. Everyone loves Disney and Nickelodeon, almost as much as they love Disney.com and Nick.com. NationalGeographic.com, Scholastic.com and Discovery.com have great videos online too. You love your WebKinz and Webkinz.com. See, it's easy!
3. Use Kid and Tween-Sized Search Engines. Yahooligans was the first kid and tween-sized search engine in the world. It was designed to find all the fun sites for kids and tweens out there. The experts at Yahoo review every single site to make sure it's safe and appropriate.
   Other search engines have filters to try and block out the bad sites, but they don't always block every bad site. KidZui.com, the "Internet for kids," has parents and teachers review all their sites and YouTube videos to make sure they are right for kids and tweens. You can search your favorite kids and tween sites for additional sites they host too, like searching Disney.com for information about bears, or NationalGeographic.com or Discovery.com for penguins or magic. If you are looking for pics for a school report, make sure you only use a safe search engine, like Yahooligans or KidZui. Gross pics can come up on lots of innocent searches, otherwise.
4. Have your parents or older brother or sister check the new sites out first. If you have heard about a site from someone or can't find one on your own, get your parents or siblings to help. Have them search for some sites that are just right for kids and tweens.

5. Make sure your parents use filtering or parental controls. Sometimes kids and tweens type so fast that they misspell the website address. Or, they guess at the right spelling or enter in a name they think will give them the website of a toy, place or game they like offline. Sometimes the sites that come up are pretty creepy. If your parents use the right filters or parental controls, it will block the bad sites when that happens before you have to see them.

Cyberbullying

Cyberbullying is bullying someone online and with cell phones, game devices and on game sites. It's when one kids or tween uses technology as a weapon to hurt another kids or tweens.

Sometimes, when kids and tweens aren't careful or don't know enough about using a certain technology safely, they hurt others by accident. They might have been kidding around or they might have forgotten to include a ☺ or "jk" (for just kidding) and the other person took it seriously Maybe they sent it to the wrong person and instead of their friend who would understand it was just a joke, it went to someone else on your buddy list or a stranger. They might not know it was only a joke and get scared or angry.

But most of the time it's on purpose. When kids and tweens are angry or hurt, they often send mean messages or do mean things to hurt others. They might think that it's okay because they didn't start it. But it's never okay to be mean online. Many times kids and tweens will pretend to be someone else when they are doing mean things online. They make hack into someone's account or use their password without permission and say mean things to your friends pretending to be you. Or they may disguise their identity and not let you know who they are. You never know if they are your best friend or worst enemy.

One of WiredSafety's Tweenangels said that "cyberbullying hurts your heart." Her best friend got into a fight with her and was very hurtful to her online. Words can hurt a lot. And if the cyberbully tries and make it look like you did something mean to your friends, it can cost you all your friends.

The best way to avoid being a cyberbully is to proofread your IMs, text messages and emails before sending them. Did you address it to the right person? Did you leave out a word that changes the meaning of the message? Is it possible that they will think you were mean, even if you weren't trying to be mean? Treat each other with respect. Follow the WiredSafety " Internet Golden Rule" and never do anything online that you wouldn't do offline.

The best way to avoid being the target of a cyberbully is to protect your password, not share personal information that they could use to hurt you and to follow WiredSafety's Internet Golden Rule. By treating people the way you want to be treated, it is less likely that they will try and hurt you.

If you do everything you are supposed to do, but are being cyberbullied anyway, remember to Stop, Block and Tell! WiredKids.org and StopCyberbullying.org say to "stop, block and tell!" if anything hurts your feelings or upsets you online. Stop – don't answer back, Block the person or message and Tell! a trusted adult (like your parents). Otherwise, you are feeding the bully!

Games and Virtual Worlds

All kids and tweens love games. It's your favorite online activity. Most kids and tweens visit WebKinz, Club Penguin, Neopets, BuildaBearville and other virtual worlds. Some sites, like Disney.com and CandyStand.com have free and fun simple games. You can play them online, offline and on your cell phones, handheld gaming devices, like DS, DSi and PSP, or on game consoles, like Xbox, PlayStation or Wii.

There are four things kids and tweens need to think about when playing computer and video games:

1. Think before your register. While some sites are trustworthy, others aren't. Before you give away your email address, name or other personal information, ask your parents. Don't use a site that asks for too much personal information and think about using a special email address just for signing up at sites, so you aren't giving your official email address away.
2. Make sure the gaming site or game is appropriate for kids and tweens your age. Offline games are rated by the ESRB for different ages. It's good to stick with games rated for your age, unless your parents agree that a different rating is okay for you. You may be a very good gamer, but the others on a game site are all 25 year olds and aren't very nice to kids or tweens playing the game. If the game site is limited to teens and older, don't lie about your age to pretend you are older. You can get the site into trouble and can get into trouble yourself if they find out.
3. Find out how much it costs first. Some game sites and virtual worlds are free, or are free for kids or tweens who buy their toys or offline products. Others either cost money to join or have a section or features you can use only if you pay for them. Check with your parents before joining anything that costs money. Even if you have their credit card or PayPal information, or access to your own payment account, check first. And look for hidden fees or sites that try and get you to buy things every day to dress your avatars or decorate your rooms. These fees can add up fast!
4. Practice password safety. Choose your password carefully. Remember – easy to remember, hard to guess! Don't share it with anyone even your best friend. And if you are going away and can't feed or care for your avatar or online pet, don't give it to someone so they can care for your pet in your absence.
   All top virtual worlds have a way to keep your pet or avatar well while you are offline. (You might have to ask them in advance how to do that, though.) If you want a friend who is a really good gamer to help you earn more points in a game or virtual world, you should log on privately before you let them use your account. If they are a good friend, they won't mind. And if you think someone is using your account without your permission, let your parents and the game company know so they can help you.

Cell phones

If you're lucky, you have a cell phone. Or maybe you'll get one in a few years. All cell phones come with a certain cell phone plan that gives you a certain number of text messages or call minutes a month. Find out what your plan is and make sure you don't send more text messages or make more calls than you are allowed. They can be very expensive. Some plans let you make all the calls you want after a certain time of night. One company or plan may set 6pm as the time, others may set 9pm. Find out what time

applies to your plan, and if you change cell phone providers or plans check again. Many kids and tweens have ended up getting into trouble because they thought their free calling time started earlier than it really did.

Most cell phones don't have a way to limit calls or text messaging to just your friends. So it's up to you to avoid strangers and creeps who call or message you. A good rule is to ignore any text message or call from "no caller id", "private callers," "restricted number" or numbers you don't recognize. If it's a friend, they can always reach you another way.

Keep an eye on your cell phone. While someone may try and steal it, more often others in your school will try and use it to get you into trouble. They may use it when you aren't looking and send a mean text message to your friends while pretending to be you or reprogram your address book.

Ringtones, games, music, videos and special features can cost money, too. They may end up being charged to your cell phone account and your parents will be surprised with a huge bill at the end of the month. So ask first before downloading anything on your phone or saying "yes" to any text message ads you may receive.

If you lose it or it is stolen, make sure you tell your parents right away so they can shut it off and warn others if personal information or pics are stored on the lost phone. See if you can set password protection to keep others from programming your phone or using it without your permission.

And be careful with it. It might be fun to shoot pics of your friends when at the beach, but sand and water can damage it easily. Some cell phone suppliers offer insurance, which can be a big help when you lose your cell phone or your mom forgot to check your pants pocket before dropping them into the washing machine.

Facebook, MySpace and myYearbook, YouTube and Video-sharing Sites

Facebook is one of the most popular websites in the world. It's a "social network." MySpace and myYearbook are social networks too. But if you read their rules, you'll see that users have to be at least 13 and over and in high school to join. A law in the US requires that social networks and other sites where you can communicate with others must either get your parent's permission or limit the users to teens and up. Congress did this to keep kids and preteens safer online. While it might be easy to lie about your age to set up an account pretending to be 14 and in high school in your town, they will shut down your account if they find out. How would you feel if you were really talking to an 8 year old when you thought he was 15? And lying isn't right either.

YouTube and the other video-sharing sites don't permit kids or preteens either. But they are a bit different. It is more about viewing videos (where you don't have to create an account) or posting your own (where you do need an account). Instead of lying about your age and setting up your own account, why not ask your parents to create a family account that you can use and review your videos before you post them? Just make sure that you are careful when you search for videos to view. Some are pretty

gross! KidZui has YouTube videos that are funny and appropriate for kids and tweens. They have parents and teachers who search YouTube to find the best ones to use in KidZui. Start there.

Instead of lying to Facebook and the others, find one just for kids or tweens. Every week new tween communities open up. It's much more fun to hang out with others your age, instead of having to lie to hang out with grownups. What do you think?

Instant Messaging, Email, iChat and Chat Lingo

When parents let their kids have email for the first time, it's a big deal. But most kids don't use email to communicate with their friends once they learn how to use the Internet. They want IM! Email takes too long. IM is like talking to someone in person, but better, since you can talk to lots of different people at the same time in different windows. AIM (AOL's instant messaging tool) is the most popular one in the US.

When you use IM, though, you don't type out the whole message or word formally like a school report. You often don't use punctuation, capital letters or even whole words. Spelling rarely counts (except when the person who receives it doesn't know what you were trying to say). LOL (laughing out loud), BRB (be right back), ROFLOL (rolling on the floor and laughing out loud) are examples of "chat lingo." Chat lingo was created to allow you to type faster, using fewer letters and characters. But since sometimes things can be confusing for people receiving chat lingo if they don't understand the term, they also invented "emoticons." Emoticons are smileys or frownies. They help the recipient understand whether you are just kidding around, if you are upset or if you are just being funny. When they can't see your face to know what you really mean, the emoticon has to do that for them instead.

Because you type so fast and rarely proofread your IMs, other kids and tweens who get them might have their feelings hurt by accident. They may feel cyberbullied, even if you didn't mean to hurt their feelings. That's why it is important to take an extra second or two and check what you wrote, making sure that it's clear and being sent to the write person.

Webcams, like iChat, can be lots of fun to use. So are Xbox and other game devices that have built-in webcams. But many kids and tweens get into trouble for how they use them. They may say and do things they shouldn't, and now there is video proof of what they did or said. These videos can be captured and shared with others to hurt your feelings, or hurt the feelings of others. You should think about what you are going to webcam before you do it. Afterwards, it's too late.

Sometimes when you have friends over, they may try and do something using the webcams or the computer that will get you into trouble. You should talk about this with your parents ahead of time. They may come up with ideas that make it easier to say "no" when friends want to do something they shouldn't do online at your house.

Be extra careful about posting pics online too. Get your friends' permission before posting any pic of them online and ask them to get your permission before posting pics of you too. Be careful of "tagging"

where you can be identified online in a pic. Lots of personal information can be shared through a pic. Does it show you in your Girl Scout or Boy Scout uniform? Is your house in the background? Are you doing something in the pic your parents wouldn't like? Are others? They say "a pic is worth a thousand words" and online, they are right.

WiredSafety says never to post anything or do anything online that you wouldn't want your parents, your principal, the police or a predator to see. That's good advice.

Netiquette

"Please, thank you, you're welcome"…we all know how to be polite offline (even if we don't always do it ☺). But how can you use good manners online? Offline good manners are called "etiquette" and online good manners are called "netiquette" WiredSafety's founder, Parry Aftab, wrote a netiquette guide she calls "Ms. Parry's Guide to Netiquette." Here are some things from that guide.

- Use the Internet Golden Rule – Don't do anything online you wouldn't do offline and offline follow the real Golden Rule.
- Treat others with respect online – don't make fun of them, be rude to them or hurt them intentionally.
- Don't use someone's password or account without their permission. And make sure that if they give their password to you for one reason, you don't use it for any other reason.
- If others are being mean to someone, don't join in. Either get offline and do something else, or ignore them. You don't have to lecture them, but you don't have to help them either.
- Let an adult know if someone is being cyberbullied. It's not tattling – it's helping others!
- ThinkB4uClick! Before you send or post something, take a second to read it over. Is it what you wanted to say? Is it clear? Is it being sent to the right person? Are you sure? Will you regret sending it later? If so, don't send it now.
- Don't steal. And that includes downloading music, movies, software and games illegally. If you are not sure if it's legal or not, find out before you download. Ask your parents.

In addition to being nicer, netiquette can keep you out of trouble. When you hurt the feelings of others, they are more likely to hurt you back. Lots of cyberbullying campaigns start by accident or when someone was thoughtless. So protecting the feelings of others helps protect you online.

Viruses, Pop-Ups and Hacking

Kids and tweens worry more about viruses than even adults do. That means that they have to be the family "chief security officer." The good thing is that viruses are easy to avoid if you practice "safe computing." That means you need to use a good anti-virus security software, a firewall and be careful about what your download or the files you accept from others.

Viruses can destroy your computer, erase all your games and songs and then move to your friends and do the same to them. All these kinds of software are called "malware" which means "badware." They

include spyware, where someone can track everything you say and do on your computer or just certain things. Hackers and advertisers use spyware. They include pop-ups too. These may pretend to be games and promise you that if you catch the jumping frog you can win an iPod or a DSi. Sometimes they have some disgusting pictures too.

They will ask you for your name, address and telephone number, and may also ask for lots of other information and even a credit card or PayPal account. They only thing you'll get, though, is in trouble for giving that information out. Their promises are fraud and designed to trick you into giving away your personal information.

Kids and tweens can get into lots of trouble with viruses and malware. If you download cheats and codes for your games, lots of them have malware hidden in them. And slimey people hide malware in other things kids and tweens download, pretending to be songs, or games or screen savers or videos. Once you download them, they can begin destroying your computer and files. They think you are easier to trick. But if you are careful and use the right software tools, you'll trick them instead! Wouldn't it be great if you were the smartest ones on protecting your computer from hackers, and viruses, pop-ups and spyware?

There are many software tools that block pop-ups. Some are built into your browser toolbar, and some are included in your anti-virus security software. Some are built into your operating system, like Windows Vista or the Mac operating system. They are free and work well with their own software. Others you can buy in stores and online, or they may come for a free trial period with new computers you buy. It's very important to use one of them and update them automatically.

But what about hackers? How can you lock the door on your computer the same way you can lock your front door in your house? You use a "firewall." Firewalls can be software or hardware. If you have a wireless network, your router (the device that shares the wireless signal with computers in the network) has a built-in firewall to keep others out. You need to set it up using a special password first. But a wireless router firewall can protect you when you didn't even know you had one. Firewall settings can be included in your anti-virus software too. And there are hardware devices that do the same thing. They all keep others out of your computer and your network.

But even the best software and hardware won't work if you don't use them. It's like having seatbelts in your car, but not buckling up. You have to do the same for anti-virus and firewall security products. You have to turn them on and make sure they know what to protect and you need to keep them updated with all the new protection every minute of every day. Luckily for you, the software updates itself, so you have time to play games and chat with your friends while it protects you.

Make sure you let your parents know how important security software is to protecting your computer and all the valuable files on it. And remind them to set it up and use it. After all – you're the best "chief security officer" in the house!

How to Report Things Online

You already know when and how to talk to your parents when things go wrong online. But there are others who need to know when things go wrong too. These include the website where someone is breaking the rules and sometimes the police. You can make a report to the site yourself. But only your parents should report things to the police when they think a crime has been committed or something serious has happened.

Every website, game or communication tool has a "terms of service." Those are the rules about using the site, game or tool. You have to follow those rules if you want to use them. If you break those rules, they can terminate your account, suspend you or even report you to the police. If you use AIM, you know about the "notify AOL" button to report someone who sent you a mean or disgusting message or who won't leave you alone. When you click that button, AOL captures the message and your report and will check it out. If the person broke the rules, they may get into trouble. If you sent a false report on purpose, you may get into trouble, just as you would if you pulled the fire alarm at school when there wasn't a fire. (If you thought they had broken the rules, and honestly reported them it's not a "false report" and you won't get into trouble anymore than if you thought there was a fire.)

Virtual worlds and games have report abuse buttons too. Some are more clear and ask you what kind of report you are making. Others just have one button for everything. If the site has the "Socially Safe" seal for kids and tween sites, they have to make it easy for you to report problems and promise to fix them.

It's really important to report it when things go wrong or you find something creepy or disgusting online. It's the only way a site or game can find them most of the time. You are helping keep your own cyber-neighborhood safe. Some sites and games, like Club Penguin, have kids who help keep the site safer. Club Penguin's "secret agents" can make a big difference if they do their job right. But even if they don't have a special group of kids and tween volunteers dedicated to protecting others on their site, you can make a big difference by reporting what you find. Who knows, maybe the report you make will protect lots of other kids and tweens from the creeps of the world or stop a cyberbullying attack against someone else. You can make a difference. And you can protect others and yourself at the same time!

Now…go have some fun out there – safely!