



## A Parent's Guide to Cyberbullying and How to Handle It

**What is it?:** Cyberbullying is any cyber-communication or publication posted or sent by a minor online, by instant messenger, e-mail, website, diary site, online profile, interactive game, handheld device, cell phone or other interactive device that is intended to frighten, embarrass, harass or otherwise target another minor. If there aren't minors on both sides of the communication, it is considered cyberharassment, not cyberbullying. Most kids don't consider a one-time rude or insulting communication to be cyberbullying. They think it needs to be repeated, or a threat of bodily harm, or a public posting designed to hurt, embarrass or otherwise target a child.

**What ages does it usually affect?:** Cyberbullying typically starts at about nine years of age and usually ends around fourteen. After fourteen it usually becomes sexual harassment. Many cases of cyberbullying occur right after a child receives their first IM account when they often try to see what they can get away with. (These kids usually stop when they understand the consequences of their actions.)

**How prevalent is it?:** Very. Ninety percent of the middle school students we polled admitted to having had their feelings hurt online. Sixty-five percent of the students we polled between eight and fourteen have been involved directly or indirectly in a cyberbullying incident as either the cyberbully, the victim or a close friend of one or the other. Fifty percent have heard of or seen a website bashing another student in their school, and seventy-five percent have visited a bashing website. Forty percent have either had their password stolen and changed by a bully (locking them out of their own account) or had communications sent to others posing as them. Many studies that ask kids if they have been "cyberbullied" fall short of measuring the real problem, because the kids often do not consider many of these actions to be "cyberbullying." Only fifteen percent of parents polled even knew what cyberbullying was.

**How does it work?:** There are two kinds of cyberbullying, direct attacks (messages sent to your kids directly) and cyberbullying by proxy (using others to help cyberbully the victim, either with or without the accomplice's knowledge). These include bashing websites, where kids are encouraged to vote for the ugliest, fattest, etc. victim. Because cyberbullying by proxy often gets adults involved in the harassment, it is much more dangerous.

**What's the profile of a typical cyberbully?:** There are four different kinds of cyberbullying. They are motive-driven, based on the motives for the cyberbullying. They may use the same methods as the other kinds of cyberbullies, but the reasons for their actions are very different. Solutions require that we understand the motives involved to address them effectively.

The four types of cyberbullies include:

- The Vengeful Angel
- The Power-Hungry or Revenge of the Nerds
- The "Mean Girls"
- The Inadvertent Cyberbully or "Because I Can"

“The Vengeful Angel”: In this type of cyberbullying, the cyberbully doesn’t see themselves as a bully at all. They see themselves as righting wrongs, or protecting themselves or others from the “bad guy” they are now victimizing. The Vengeful Angel cyberbully often gets involved trying to protect a friend who is being bullied or cyberbullied. They generally work alone, but may share their activities and motives with their close friends and others they perceive as being victimized by the person they are cyberbullying.

Vengeful Angels need to know that no one should try and take justice into their own hands. They need to understand that few things are clear enough to understand, and that fighting bullying with more bullying only makes things worse. They need to see themselves as bullies, not the do-gooder they think they are. It also helps to address the reasons they lashed out in the first place. If they sense injustices, maybe there really are injustices. Instead of just blaming the Vengeful Angel, solutions here also require that the situation be reviewed to see what can be done to address the underlying problem. Is there a place to report bullying or cyberbullying? Can that be done anonymously? Is there a peer counseling group that handles these matters? What about parents and school administrators. Do they ignore bullying when it occurs, or do they take it seriously? The more methods we can give these kinds of cyberbullies to use official channels to right wrongs, the less often they will try to take justice into their own hands.

The “Power-Hungry” and “Revenge of the Nerds”: Just as their schoolyard counterparts, some cyberbullies want to exert their authority, show that they are powerful enough to make others do what they want and some want to control others with fear. Sometimes the kids want to hurt another kid. Sometimes they just don’t like the other kid. These are no different than the offline tough schoolyard bullies, except for their method. Power-Hungry cyberbullies usually need an audience. It may be a small audience of their friends or those within their circle at school. Often the power they feel when only cyberbullying someone is not enough to feed their need to be seen as powerful and intimidating. They often brag about their actions. They want a reaction, and without one may escalate their activities to get one.

Interestingly enough, a sub type of the Power-Hungry cyberbully is often the victim of typical offline bullying. They may be female, or physically smaller, the ones picked on for not being popular enough, or cool enough. They may have greater technical skills. Some people call this type the “Revenge of the Nerds” cyberbully. It is their intention to frighten or embarrass their victims. And they are empowered by the anonymity of the Internet and digital communications and the fact that they never have to confront their victim. They may act tough online, but are not tough in real life. They are often not a bully but “just playing one on TV.”

This kind of cyberbullying usually takes place one-on-one and the cyberbully often keeps their activities secret from their friends. If they share their actions, they are doing it only with others they feel would be sympathetic. They rarely appreciate the seriousness of their actions, and often resort to cyberbullying-by-proxy. Because of this and their tech skills, it can be the most dangerous of all cyberbullying.

Power-Hungry cyberbullies often react best when they know that few things are ever anonymous online. We leave a trail of cyber-breadcrumbs behind us wherever we go in cyberspace. And, with the assistance of a law enforcement or legal subpoena, we can almost always find the cyber-abusers and cybercriminals in real life. Shining a bright light on their activities helps too. When they are exposed, letting the school community know about their exposure helps prevent copycat cyberbullying.

Helping them to realize the magnitude of their activities is also helpful. Often their activities rise to the criminal level. The more this type of cyberbully understands the legal consequences of their actions, the more they think about their actions.

Ignoring them can also be very effective. But sometimes, instead of going away when ignored, they escalate their actions to get others involved, through a cyberbullying-by-proxy situation. Whenever a Power-Hungry cyberbully is suspected, it is crucial that law enforcement is notified and that the victim keeps a careful watch on themselves online, through “googling themselves.” They can even set a Google Alert to notify them by e-mail if anything new is posted online with their personal contact information.

“Mean Girls”: The type of cyberbullying occurs when the cyberbully is bored or looking for entertainment. It is largely ego-based and the most immature of all cyberbullying types. Typically, in Mean Girls bullying situations, the cyberbullies are female. They may be bullying other girls (most frequently) or boys (less frequently).

Mean Girls cyberbullying is usually done, or at least planned, in a group, either virtually or together in one room. It may occur from a school library or a slumber party, or from the familyroom of someone after school. This kind of cyberbullying requires an audience. The cyberbullies in a Mean Girls situation want others to know who they are and that they have the power to cyberbully others. This kind of cyberbullying grows when fed by group admiration, cliques or by the silence of others who stand by and let it happen. It quickly dies if they don't get the entertainment value they are seeking.

The most effective tool in handling a Mean Girls cyberbullying case is blocking controls. Block them, block all alternate screen names and force them to go elsewhere for their sick entertainment. In addition, if threatened with loss of their AIM accounts, they wise up fast!

The “Inadvertent Cyberbully”: Inadvertent cyberbullies usually don't think they are cyberbullies at all. They may be pretending to be tough online, or role playing, or they may be reacting to hateful or provocative messages they have received. Unlike the Revenge of the Nerds cyberbullies, they don't lash out intentionally. They just respond without thinking about the consequences of their actions.

They may feel hurt, or angry because of a communication sent to them, or something they have seen online. And they tend to respond in anger or frustration. They don't think before clicking “send.”

Sometimes, while experimenting in role-playing online, they may send cyberbullying communications or target someone without understanding how serious this could be. They do it for the heck of it “Because I Can.” They do it for the fun of it. They may also do it to one of their friends, joking around. But their friend may not recognize that it is another friend or may take it seriously. They tend to do this when alone, and are mostly surprised when someone accuses them of cyberabuse.

Education plays an important role in preventing Inadvertent Cyberbullying. Teaching them to respect others and to be sensitive to their needs is the most effective way of dealing with this kind of cyberbully. Teaching them to Take5! is an easy way to help them spot potentially bullying behavior before it's too late.

**Why do kids cyberbully each other?:** Who knows why kids do anything? When it comes to cyberbullying, they are often motivated by anger, revenge or frustration. Sometimes they do it for entertainment or because they are bored and have too much time on their hands and too many tech toys available to them.

Many do it for laughs or to get a reaction. Some do it by accident, and either send a message to the wrong recipient or didn't think before they did something. The Power-Hungry do it to torment others and for their ego. Revenge of the Nerd may start out defending themselves from traditional bullying only to find that they enjoy being the tough guy or gal. Mean Girls do it to help bolster or remind people of their own social standing. And some think they are righting wrongs and standing up for others.

**What's the profile of a typical cyberbullying victim?:** Anyone age nine to fourteen. After that, the bullying becomes more dangerous and usually involves sexual harassment. We consider this cyberharassment, not cyberbullying, because of the nature of the attacks and the age of the actors.

**What can you do to prevent it?** Educating the kids about the consequences (losing their ISP or IM accounts) helps. Teaching them to respect others and to take a stand against bullying of all kinds helps too. (Read more about this in "what role can education play in this" below.)

**How can you stop it once it starts?:** Because their motives differ, the solutions and responses to each type of cyberbullying incident has to differ too. Unfortunately, there is no "one size fits all" when cyberbullying is concerned. Only two of the types of cyberbullies have something in common with the traditional schoolyard bully. Experts who understand schoolyard bullying often misunderstand cyberbullying, thinking it is just another method of bullying. But the motives and the nature of cybercommunications, as well as the demographic and profile of a cyberbully differ from their offline counterpart. (To learn more about the methods that work best with the four different kinds of cyberbullies, read about "the profile of a typical cyberbully," above.)

**What is the school's role in this?:** When schools try and get involved by disciplining the student for cyberbullying actions that took place off-campus and outside of school hours, they are often sued for exceeding their authority and violating the student's free speech right. They also, often lose. Schools can be very effective brokers in working with the parents to stop and remedy cyberbullying situations. They can also educate the students on cyberethics and the law. If schools are creative, they can sometimes avoid the claim that their actions exceeded their legal authority for off-campus cyberbullying actions. We recommend that a provision is added to the school's acceptable use policy reserving the right to discipline the student for actions taken off-campus if they are intended to have an effect on a student or they adversely affect the safety and well-being of student while in school. This makes it a contractual, not a constitutional, issue.

**What's the parents' role in this?:** Parents need to be the one trusted place kids can go when things go wrong online and offline. Yet they often are the one place kids avoid when things go wrong online. Why? Parents tend to overreact. Most children will avoid telling their parents about a cyberbullying incident fearing they will only make things worse. (Calling the other parents, the school, blaming the victim or taking away Internet privileges.) Unfortunately, they also sometimes under react, and rarely get it "just right." (You can read more about this in "Not Too Hot, Not Too Cold! Goldilocks and the CyberParents" at [wiredkids.org](http://wiredkids.org).)

Parents need to be supportive of their child during this time. They may be tempted to give the "stick and stones may break your bones, but words will never hurt you" lecture, but words and cyberattacks can wound a child easily and have a lasting effect. These attacks follow them into your otherwise safe home and wherever they go online. And when up to 700 million accomplices can be recruited to help target or humiliate your child, the risk of emotional pain is very real, and very serious. Don't brush it off.

Parents should also let the school know so the guidance counselor can keep an eye out for in-school bullying and for how your child is handling things. You may want to notify your pediatrician, family counselor or clergy for support if things progress. It is crucial that you are there to provide the necessary support and love. Make them feel secure. Children have committed suicide after having been cyberbullied, and in Japan one young girl killed another after a cyberbullying incident. Take it seriously.

Parents also need to understand that a child is just as likely to be a cyberbully as a victim of cyberbullying and often go back and forth between the two roles during one incident. They may not even realize that they are seen as a cyberbully. (You can learn more about this under the “Inadvertent Cyberbully” profile of a cyberbully.)

Your actions have to escalate as the threat and hurt to your child does. But there are two things you must consider before anything else. Is your child at risk of physical harm or assault? And how are they handling the attacks emotionally?

If there is any indication that personal contact information has been posted online, or any threats are made to your child, you must run...do not walk, to your local law enforcement agency (not the FBI). Take a print-out of all instances of cyberbullying to show them, but note that a print-out is not sufficient to prove a case of cyber-harassment or cyberbullying. You'll need electronic evidence and live data for that.

Using a monitoring product, like Spectorsoft, collect all electronic data necessary to report, investigate and prosecute your case (if necessary). While hopefully you will never need it, the evidence is automatically saved by the software in a form useable by law enforcement when you need it without you having to learn to log or copy header and IP information.

### **A quick guide on the escalating levels of response to a cyberbullying incident:**

**Talk to your child:** Caution them about responding “in kind.” This is not a time for them to lash out or start a cyberwar themselves. See if they think they know the identity of the cyberbully or cyberbullies. See if this is related to an offline bullying situation, and deal with that quickly. And don't confuse the language most kids use online with cyberbullying. It may be shocking to us, but unless it is shocking to your child, it's not cyberbullying.

**Ignore it:** A one time, seemingly unthreatening act, like a prank or mild teasing should probably be ignored. (If it's a threat, you must report it.) At the same time, you may want to consider using some preventive measures:

**Restrict the people who can send you communications:** Consider restricting all incoming communications to pre-approved senders, such as those on your child's buddy list. (If the cyberbully is someone on their buddy list, though, this method won't help. In that case the cyberbully will have to be removed from the buddy list and/or blocked.)

**Restrict others from being able to add your child to their buddy list:** Cyberbullies track when your child is online by using buddy lists, and similar tracking programs. It will let them know when one of their “buddies” is online, when they are inactive and, in some cases, where they are. This is like adding a tracking device to your child's online ankle, allowing their cyberbullies to find them more easily and target

them more effectively. This feature is usually found in the privacy settings or parental controls of a communications program.

**Google Your Child:** Make sure that the cyberbully isn't posting attacks online. When you get an early warning of a cyberbullying campaign, it is essential that you keep an eye on your child's screen name, nick names, full name, address, telephone and cell numbers and websites. You can also set up an "alert" on Google to notify you whenever anything about your child is posted online. To learn more about "Googling" yourself or your child, read "Google Yourself!"

**Block the sender:** Someone who seems aggressive, or makes you uncomfortable and does not respond to verbal pleas or formal warnings should be blocked. This way, they will not be able to know when you are online or be able to contact you through instant messaging.

Even if the communicates are not particularly aggressive or threatening, if they are annoying, block the sender. (Most ISPs and instant messaging programs have a blocking feature to allow you to prevent the sender from getting through.)

**"Warn" the sender:** If the cyberbully uses another screen name to avoid the block, otherwise manages to get through or around the block or communicates through others, "warn" them, or "notify" the ISP. (This is usually a button on the IM application.) This creates a record of the incident for later review, and if the person is warned enough, they can lose their ISP or instant messenger account. (Unfortunately, many cyberbullies use "warning wars" or "notify wars" to harass their victims, by making it appear the victim is really the cyberbully. This is a method of cyberbullying by proxy, getting the ISP to be an unwitting accomplice of the cyberbullying.)

**Report to ISP:** Most cyberbullying and harassment incidents violate the ISP's terms of service. These are typically called a "TOS violation" (for a "terms of service" violation), and can have serious consequences for the account holder. Many ISPs will close a cyberbully's account (which will also close their parents' household account in most cases.) You should report this to the sender's ISP, not yours. If you use a monitoring software, like Spectorsoft, this is much easier.

If your child's account has been hacked or their password compromised, or if someone is posing as your child, you should make a formal report to *your* ISP as well. You can call them or send an e-mail to their security department (NOT their terms of service reportline). But before changing your password, you should scan your computer for any hacking programs or spyware, such as a Trojan horse. If one is on your computer, the cyberbully may be able to access the new password. Most good anti-virus programs can find and remove a hacking program. All spyware applications can. We recommend SpyBot Search and Destroy (a freeware) or Ad-Aware (by Lavasoft, they have a free "lite" program).

**Report to School:** Most cases of cyberbullying occur off school grounds and outside of school hours. Often the school has no legal authority to take action relating to an off-premises and off-hours activity, even if it has an impact on the welfare of their students. The laws are tricky, and vary jurisdiction by jurisdiction. So while you should notify the school (especially if your child suspects whom is behind the attacks), they may not be able to take disciplinary action. They can keep an eye on the situation in school, however. And since many cyberbullying incidents are combined with offline bullying incidents, your child may be safer because of the report.

Also, while the school may have limited authority over disciplining the cyberbully, they can call the parents in and try and mediate the situation. They can also institute an educational and awareness program to help stop further cyberbullying by students, and to help educate parents about the problem.

**Report to Police:** Someone who threatens you physically, who is posting details about you or your child's offline contact information or instigating a cyberbullying by proxy campaign should be reported to the police. (Although you should err on the side of caution and report anything that worries you.) Using a monitoring program, such as Spectorsoft, can facilitate the investigation and any eventual prosecution by collecting and preserving electronic evidence. Print-outs, while helpful in explaining the situation, are generally not admissible evidence. If you feel like your child, you or someone you know is in danger, contact the police immediately and cut off contact with this person or user, staying offline if need be until you are otherwise instructed. Do not install any programs, or remove any programs or take other remedial action on your computer or communication device during this process. It may adversely affect the investigation and any eventual prosecution.

**Take Legal Action:** Many cases of cyberbullying (like their adult cyber-harassment equivalent) are not criminal. They may come close to violating the law, but may not cross the line. Most of the time, the threat of closing their ISP or instant messaging account is enough to make things stop. But sometimes, either because the parents want to make an example of the cyberbully or because it isn't stopping, lawyers need to be brought in. It may also be the only way you can find out whom is behind the attacks.

Think carefully before you decide to take this kind of action. Even if you win in the end, it may take you two or three years to get there and cost you tens of thousands of dollars. You may be angry enough to start it, but make sure that you have something more than anger to sustain the long months and years of litigation.

**What's law enforcement supposed to do?:** First, they need to be trained to tell the difference between annoying communications and dangerous ones. They also need to understand how to investigate a cybercrime and how to obtain information from an ISP.

Law enforcement can assist parents by steering them to their cyberbully's ISP. Most ISPs prohibit cyberbullying and harassment using their services and will terminate the cyberbully's Internet account. Sometimes this can be more effective than threatening the cyberbully with jail.

**What role does awareness and education play in this?:** Education can help considerably in preventing and dealing with the consequences of cyberbullying. The first place to begin an education campaign is with the kids and teens themselves. We need to address ways they can become inadvertent cyberbullies, how to be accountable for their actions and not to stand by and allow bullying (in any form) to be acceptable. We need to teach them not to ignore the pain of others.

Teaching kids to "Take 5!" before responding to something they encounter online is a good place to start. Jokingly, we tell them to "Drop the Mouse! And step away from the computer! That way nobody will get hurt!!" We then encourage them to find ways to help them calm down. This may include doing yoga, or deep-breathing. It may include running, playing catch or shooting hoops. It may involve taking a bath, hugging a stuffed animal or talking on the phone with friends. Each child can find their own way of finding their center again. And if they do, they will often not become a cyberbully, even an inadvertent cyberbully.

There are several ways we can educate kids not to support cyberbullying:

- Teaching them that all actions have consequences;
- Teaching them that cyberbullying hurts;
- Teaching them that they are just being used and manipulated by the cyberbully;
- Teaching them that the cyberbully and their accomplices often become the target of cyberbullying themselves; and
- Teaching them to care about others and stand up for what's right.

And, in addition to not lending their efforts to continue the cyberbullying, if given an anonymous method of reporting cyberbullying websites, profiles and campaigns, kids can help put an end to cyberbullying entirely. School administration, community groups and even school policing staff can receive these anonymous tips and take action quickly when necessary to shut down the site, profile or stop the cyberbullying itself.

We need to teach our children that silence, when others are being hurt, is not acceptable. If they don't allow the cyberbullies to use them to embarrass or torment others, cyberbullying will quickly stop. It's a tall task, but a noble goal. And in the end, our children will be safer online and offline. We will have helped create a generation of good cybercitizens, controlling the technology instead of being controlled by it.