STOP cyberbullying

www.stopcyberbullying.org

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 Web sites. 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 please 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 or, block the sender. (Most ISPs and instant messaging programs have a blocking feature to allow you to prevent the sender from getting through.)

Copyright © WiredKids, Inc. All rights reserved.
Executive Director: Parry Aftab, Esq.

"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. (For more information about how to make a report, read "Making a Report to Their ISP." 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 report line). 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. In the United States , 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 any 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 your 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.

Copyright © WiredKids, Inc. All rights reserved.
Executive Director: Parry Aftab, Esq.

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.

Copyright © WiredKids, Inc. All rights reserved.
Executive Director: Parry Aftab, Esq.