STOP cyberbullying

www.stopcyberbullying.org

Telling the difference between flaming, cyber-bullying and harassment and cyberstalking (A guide for law enforcement)

It's not always easy to tell these apart, except for serious cases of cyberstalking, when you "know it when you see it." And the only difference between "cyberbullying" and cyber-harassment is the age of both the victim and the perpetrator. They both have to be under-age.

When you get a call, your first response people need to be able to tell when you need to get involved, and quickly, and when it may not be a matter for law enforcement. It might help to start by running through this checklist. If the communication is only a flame, you may not be able to do much about it. (Sometimes ISPs will consider this a terms of service violation.) But the closer it comes to real life threats the more likely you have to get involved as law enforcement. We recommend that law enforcement agents ask parents the following questions. Their answers will help guide you when to get involved and when to recommend another course of action.

The kind of threat:

- The communication uses lewd language
- The communication insults your child directly ("You are stupid!")
- The communication threatens your child vaguely ("I'm going to get you!")
- The communication threatens your child with bodily harm. ("I'm going to beat you up!")
- There is a general serious threat. ("There is a bomb in the school!" or "Don't take the school bus today!")
- The communication threatens your child with serious bodily harm or death ("I am going to break your legs!" or "I am going to kill you!")

The frequency of the threats:

- It is a one-time communication
- The communication is repeated in the same or different ways
- The communications are increasing
- Third-parties are joining in and communications are now being received from (what appears to be) additional people

The source of the threats:

- Your child knows who is doing this
- Your child thinks they know who is doing this
- Your child has no idea who is doing this
- The messages appear to be from several different people

The nature of the threats:

- Repeated e-mails or IMs
- Following the child around online, into chat rooms, favorite Web sites, etc.
- Building fake profiles, Web sites or posing as your child's e-mail or IM
- Planting statements to provoke third-party stalking and harassment
- Signing your child up for porn sites and e-mailing lists and junk e-mail and IM.
- Breaking in to their accounts online
- Stealing or otherwise accessing their passwords
- Posting images of the child online (taken from any source, including video and photo phones)
- Posting real or doctored sexual images of the child online
- Sharing personal information about the child
- Sharing intimate information about the child (sexual, special problems, etc.)
- Sharing contact information about the child coupled with a sexual solicitation ("for a good time call …" or "I am interested in [fill in the blank] sex…")
- Reporting the child for real or provoked terms of service violations ("notify wars" or "warning wars")
- Encouraging that others share their top ten "hit lists," or ugly lists, or slut lists online and including your child on that list.
- Posting and encouraging others to post nasty comments on your child's blog.
- Hacking your child's computer and sending your child malicious codes.
- Sending threats to others (like the president of the United States) or attacking others while posing as your child.
- Copying others on your child's private e-mail and IM communications.
- Posting bad reviews or feedback on your child without cause.
- Registering your child's name and setting up a bash Web site or profile.
- Posting rude or provocative comments while posing as your child (such as insulting racial minorities at a Web site devoted to that racial minority).
- Sending spam or malware to others while posing as your child.
- Breaking the rules of a Web site or service while posing as your child.
- Setting up a vote for site (like "hot or not?") designed to embarrass or humiliate your child.
- Masquerading as your child for any purpose.
- Posting your child's text-messaging address or cell phone number online to encourage abuse and increase your child's text-messaging or cell phone charges.
- Launching a denial of service attack on your child's Web site
- Sending "jokes" about your child to others or mailing lists.

The more repeated the communications are, the greater the threats (or enlarging this to include third-parties) and the more dangerous the methods, the more likely law enforcement or legal process needs to be used. If personal contact information is being shared online, this must be treated very seriously.

If the child thinks they know who is doing this, that may either make this more serious, or less. But once third-parties are involved (hate groups, sexually-deviant groups, etc.) it makes no difference if the person who started this is a young seven year old doing it for a laugh. It escalates quickly and can be dangerous.

It's best to work out relationships with the big ISPs in your area well before you need them. Find their offline contact information, including off hours. Learn how to track an IP address and preserve evidence. And make sure that you issue your subpoenas in the form they need, using your time zone for tracking the dynamic IP addresses of record. Many ISPs discard the subscriber/IP data after a week to thirty day period. So time is crucial. If you need to get your paperwork together, send them a quick note asking them to preserve the records pending your formal subpoena. They will usually do this on a less formal request on law enforcement letterhead.