

How to Stop or Remove CyberInfo

**Submitted by Ms. Phyl Burger – Educational Consultant
Bully Police Minnesota, Co-Director**

Stop or remove the material

Most e-mail can be traced back to the sender's address. An excellent resource site is: <http://www.internetsuperheroes.org/cyberbullying/>
Click on 'How to copy the e-mail headers for reporting an abusive e-mail' for a user-friendly guide to assist you.

It is important to know that sending or posting inappropriate language is generally a violation of the "Terms and Conditions" of most web sites, Internet service providers, email services, and mobile phone providers. Here are steps to help the student and parents:

1. Send *one* message to the cyber bully stating clearly: "Do not communicate with me again or I will contact the appropriate authorities." Save the message you have sent.
2. Contact the Internet service provider of the cyber bully (you can determine the ISP from the email address), forward the messages that have been received, and request that the account be terminated. You can send the message to abuse@<domain name of provider> or visit the web site of the service provider and look for a page on complaint procedures.
3. If the cyber bully's comments appear on a third-party Web site, such as a teen community or web host (e.g. <<http://www.webhostname.com/~kid'sname.html>>) go to site's home page (e.g. <<http://www.webhostname.com>>) and look for words like "Terms and Conditions" to find out the complaint procedure. Provide the troubling material; indicate how it violates the site's Terms and Conditions, and request prompt removal.
4. If the offending comments are on a web site with its own domain name (e.g. <http://www.xyzkid.com>), you can usually find the owner of the site and the company that hosts the site by going to Whois (<http://www.whois.net>) and typing in the domain name. This will usually tell you the hosting company's web site. Then go to the hosting company's site, find the Terms and Conditions and complaint procedure, and file a complaint.
5. If the cyber bully's comments are coming through text on a mobile phone, trace the number and contact the phone company.
6. Change your child's email address and/or screen name, and possibly email provider.
7. Change the phone number the cyber bully has been using.

Ignore the Cyberbullying

In some cases, ignoring the cyber bully is the best option. There are two ways to ignore a cyber bully:

1. Simply leave the communications environment (chat, IM, email, etc.).
2. Block all further communications. Use the block function for instant messaging and mobile phones (go to "Options" or "Preferences" and block the cyber bully's screen name). With email, set the email filter to direct all mail from the cyber bully into a specific folder. This way, it is saved, as evidence if needed in the future, however, is not in your child's regular in-box.

When to contact Law Enforcement: Resource: Cyberlawyer Parry Aftab

If there is a threat or personal contact information about a child posted online, we must take action and report it to the authorities.

The kind of threat:

- The communication uses lewd language
- The communication insults the child or youth directly ("You are stupid!")
- The communication threatens vaguely ("I'm going to get you!")
- The communication threatens the child or 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 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:

- The student knows who is doing this
- The student thinks they know who is doing this
- The student 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 student around online, into chatrooms, favorite websites, etc.
- Building fake profiles, websites or posing as another students e-mail or IM
- Planting statements to provoke third-party stalking and harassment

- Signing a student 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 someone's blog or guestbook.
- Hacking a computer and sending a student malicious codes.
- Sending threats to others (like the president of the United States) or attacking others while posing as another student
- Copying others on private e-mail and IM communications.
- Posting bad reviews or feedback about a child without cause.
- Registering a students name without their knowledge and setting up a bash website or profile.
- Posting rude or provocative comments while posing as someone else (such as insulting racial minorities at a website devoted to that racial minority).
- Sending SPAM or malware to others while posing another student.
- Breaking the rules of a website or service while posing another.
- Masquerading as someone else for any purpose.
- Posting a students' text-messaging address or cell phone number online to encourage abuse and increase student text-messaging or cell phone charges.
- Launching a denial of service attack on a students' website.
- Sending "jokes" about a student to others or mailing lists.