Reporting Terms of Service Violations

Often, the only recourse you have to stop an online bully is to report them to their e-mail service provider, social network, IM service, or ISP. (Cellphone providers are much easier to find and deal with.) If the actions violate the terms of service of that provider, they may lose their account or have it suspended temporarily. This is frequently enough to stop the bully in their virtual tracks. You start by visiting their ISP or e-mail service provider's terms of service or terms of use section. Read the policy carefully. Make notes about which sections you believe were violated and how.

In the majority of cases, there is also a link for abuse reports. Copy yourself on the communication so you have a record of what you sent, where you sent it, and when.

Don't expect too much, though. It has been our experience that most ISPs are reluctant to act on a first contact, if at all. They have good reasons for this: Sometimes the cyberbully poses as the victim in an attempt to get the ISP to unknowingly assist in the harassment. It is also typical that some of the "evidence" being provided has been fabricated or "enhanced" to be more serious than it actually is. There are also privacy and legal considerations that they must consider. Additionally, they receive hundreds of thousands of TOS reports and have to prioritize them.

The likelihood of getting a response and the provider taking any disciplinary action depends on how well you make your case. All reports should follow the rules the ISP or e-mail provider sets out in their report TOS information. Check and double check to make sure you have it all and have clearly identified whatever you have. Most ISPs require the following information:

- Date and time that the violations of their TOS took place (keep each violation separate in the report). Let them know your time zone.
- Copies of e-mails, complete with headers. (We teach you how to do that at WiredSafety.org if you don't know. Your e-mail application's "help" instructions may walk you through it also, step-by-step.). Alternately, the full and correct URLs of newsgroup or bulletin board postings (copy the exact address in your browser when you read it and paste it "as is" into the report).
- Screen shots of offending IMs (save these also to your computer, as the site may change and you will need proof of what used to be there).
- A timeline of how the situation developed, including copies of all communications. (Using a monitoring application like SpectorSoft Pro can be very helpful here. It can be found at SpectorSoft.com.)
- Any information you can provide as to what steps, if any, you have taken to try to alleviate the situation.

- Don’t tell them things about the harasser you know in real life or make unfounded accusations unrelated to the communications unless you know the harasser to be violent and dangerous (and then make sure you let them know who you are and how you know these things, as a school). Also, do not ask them for the identity of the harasser. They are not permitted to give out that information except through valid legal process.

You need to follow up in a few days if you have not received any response other than an "auto responder" and the situation is continuing. Be firm and consistent when you follow up. Remind them of the previous e-mail or resend it marked as “resent on [fill in the date].” Always copy yourself on these reports for your own records. Do not copy help groups and the FBI and others on the correspondence, unless these entities request it. We at WiredSafety.org typically disregard all reports we receive that copy other help groups, assuming that one of the other groups is dealing with it.

Be focused and clear and you will probably get the help you need. And keep copies of everything!

If they don’t respond, contact the PR contact for the site, your state Attorney General’s office, WiredSafety, or your local police to drive it up the priority line.