6-1-2008

Wired Safety's International Stop Cyberbullying Conference

In Memory of Megan Meier

November 6, 1992 to October 17, 2006

THE MEGAN PLEDGE

@Cyberbullying.org

WiredSafety's International Stop Cyberbullying Conference

veri on

June 2nd - 3rd 2008

wired ET

Westchester gov.com

McAfee Proven Security

AOL

Microsoft

PACE UNIVERSITY

P&G

PRCAST

Welcome to WiredSafety's International Stop Cyberbullying Conference. Cyberbullying is a growing problem. It affects at least 85% of the 45,000 middle schoolers I polled in person last year, yet only 5% of them will tell their parents. In a smaller poll, 70% of students admitted to having cyberbullied others.

It has become a silent epidemic, stalking our children on social networks, instant messaging, interactive games and cell phones. While the more dramatic stories have made the headlines, from Megan Meier's suicide following harassment by a neighborhood mom posing as a cute sixteen year old on MySpace, to cheerleaders beating one of their own on video, most cases are less newsworthy, but no less painful .

Cyberbullying has many stakeholders, from families whose lives are shattered by the loss of teens who chose suicide rather than face repeated torment, to students who are afraid to check their e-mail, to teachers being attacked online by students, mental health professionals trying to stay ahead of their patients, to the media trying to grapple with covering a story without further exploiting the victims, to regulators who are seeking answers and the industry who is struggling in its effort to identify and manage risks while attempting to herd cats. More, perhaps, than any other single issue, cyberbullying takes a village to address. In this first ever international cyberbullying conference, every member of the village will have a voice. Together we can fashion solutions and encourage change. And by the end of the two days, all stakeholders will knowabout being part of the solution, instead of part of the problem.

What do we need to know to address the problem and help frame meaningful solutions? What is the role of the Internet industry, media, government, advocacy groups and schools? Over two concentrated days, WiredSafety will help all stakeholders understand the problem better and find manageable solutions and collaborations. It will give community participants a chance to be heard, and the industry, media, advocacy groups and regulators a chance to listen and share their own viewpoints.

At a large community "town meeting" hosted in White Plains, NY, hundreds of students, teachers, parents, law enforcement officers, mental health experts and community leaders will join forces to examine the problem from all perspectives and determine what they need from the important stakeholder leaders and influencers. On the second day, in Manhattan, the leaders of the industry, media, regulators, advocacy groups will join students, teachers, parents and other key stakeholders for the "industry day" portion of the conference to address the "wishlist" created during the first day, look for solutionsand identify industry best practices. The community will meet the leaders.

I would like to thank our partners, Pace University and Westchester County Executive's Office, and our generous sponsors, Verizon (whose Chairman and CEO, Ivan Seidenberg will speak at our VIP luncheon on June 3rd), Microsoft, AOL, McAfee, Disney, The Girl Scouts of the USA, Procter & Gamble, Child Safety Research & Innovation Center (Canada), WiredTrust, and iCast Media Productions. And, thanks to all our incredible volunteers at WiredSafety!

Cyberbullying Hurts! Take it seriously!

Parry

Dr. Parry Aftab
Executive Director and Founder
WiredSafety.org (home of StopCyberbullying.org)

STOP
CYBERBULLYING

Cyberbullying.org

Community, Policy and Industry: A Hands-On Community Approach to Combating Cyberbullying

Day One: *June 2, 2008 "Community Day" Westchester County Center, White Plains, New York*

Agenda

9:30am – 10:30am Registration and Pre-Conference Media

10:30am – 10:40am Welcome

10:40am – 11:00am Keynote by Tina Meier, introducing the Megan Pledge

11:00am – 11:30am Teenangels Presentations of Research on Cyberbullying

11:30am – 12:30pm Cyberbullying Hurts! Panel of Experts, Victims and Their Families

12:30pm – 1:15pm Lunch (Concessions are open) and Q&A

1:15pm – 2:15pm What Can We Do About It? Panel of Experts and People Behind the News

2:30pm – 3:45pm Breakout Sessions (By Demographic Group)

3:50pm – 4:00pm Awards Given

4:00pm – 4:15pm Workshop Conclusions Presented by Facilitator Team

4:15pm – 4:45pm Participant Interactive Discussions to Frame Final Issues for Industry, Media and Government Section of the Conference on 2nd Day from the Entire Conference

4:45pm – 5:00pm Conclusions Settled and Closing Ceremonies

5:00pm Conference Closes

Using the UN-Style for an Experts Conference, this Community Day Both Provides Information and Engages the Participants in Helping Frame the Issues for the Second Day of Industry, Government, Educators, Community and Advocacy Groups and Media Representatives. Aided by leading Experts in their Field - The Community Will Have Its Say!

Exploring the Issues, the Solutions and Industry Best Practices

Day Two: *June 3, 2008 "Industry Day" – Pace University, Downtown, Manhattan*

Agenda

8:00am registration opens

8:45am – 9am Introductions and Welcome

9:00am – 9:30am Keynote: Connecticut Attorney General Richard Blumenthal

9:30am – 10:00am Introduction to Cyberbullying and Key Findings from the Community (Preteen and Teen Panelists discuss cyberbullying and Community Day Facilitators report on the Community Day)

10:05am – 10:45 Shattered Lives (families affected by cyberbullying and the people behind the stories)

10:45am – 12:00pm Industry Leadership Panel (CEOs, Founders, Compliance Officers, Corporate Policymakers and Chief Safety Officers)

12:00pm – 12:50pm Lunch (on your own)

For special invited guests only:
Private VIP lunch, Ivan Seidenberg, Chairman and CEO, Verizon - Luncheon Speaker
Award Ceremony

1:00pm – 2:10pm Governmental Leadership Panel (Leaders from the AGs, FTC, Canadian Data Protection, Law Enforcement and Local Governmental Leaders)

2:15pm – 3:30pm Break-Out Workshops – Choice of Three Break-Out Sessions: Cyberbullying and the Law, Teaching Kindness and Herding Cats. (More information on the Break-Out sessions on following page.)

3:35pm – 3:45pm Awards

3:45pm – 4:55pm Cyberbullying, the Media and Thought Leaders (Members of the Media, NGOs and Public Policy Leaders)

4:45pm – 5:00pm Conference Closing

Day One Break-Out Sessions: Day one participants are put to work to help frame the issues from their stakeholder group's perspective. Working with facilitators and a team of experts matched to the needs of that group, the participants will be guided to decide what they expect from the five key sectors in connection with cyberbullying – the Internet and interactive industry; education; the media; governmental and law enforcement leaders; and community and advocacy groups.

1. **Students** – Kids, tweens and teens will work together in this break-out session to frame the issues. As the largest day one demographic (with more than 180 students signed up already), this group will remain in the plenary location while the others move to adjoining rooms. Parry Aftab will facilitate this group, joined by Teenangels, Tina Meier, Mary Lou Handy, Sheriff Judd, Girl Scouts of the USA, Jacqueline Beauchere (Microsoft), and Westchester Safety Commissioner Tom Belfiore.

2. **Educators** – Teachers, school administrators, guidance counselors and educational policymakers will join forces in helping frame their issues. This group will meet in Room "Educators" (signs will be located outside of the Little Theatre). Margaret Sullivan, Art Wolinsky, Aaron Byran, Edwinna Lucyk, Sheriff Maurer and Tim McShane will facilitate this group.

3. **General Audience** – Everyone who isn't in education or is over the age of 18 ☺ will make up this third group. They will meet in Room "General Audience" (signs will be located outside of the Little Theatre). Robin Raskin ("Internet Mom"), Al Kush (Deputy Executive Director, WiredSafety) and Valerie Schmitz will facilitate this group, joined by Holly Hawkins (AOL), Girl Scouts of the USA, and Lisa Hicks-Thomas (DAG, VA).

Day Two Break-Out Sessions:

1. **Cyberbullying and the Law** – Free speech versus regulation, when do mean words cross the line? What's the limit of a school's authority for off-premises speech and actions? Current laws and what's coming? Lawyers, regulators, school administrators and civil rights advocates explore the current state of the law and its limits. John Morris, Chief Counsel, CDT moderating with Brittany Bacon, law student and Teenangel Director, Emeritus.

2. **Teaching Kindness and Respect** – What programs work and don't? How can schools address cyberbullying through education and through peer-counseling programs? How young do we have to start? Educators and non-profits in the field explore efficacy and trends, failures and successes. Art Wolinsky, Technology Education Director, WiredSafety.org moderating with Valerie Schmitz, Ph.D, Director of Technology, Hortonville Schools, Wisconsin.

3. **Herding Cats!** – What's involved in managing cyberbullying risks in a social network or Web 2.0 provider? Who's doing it right and who isn't? Learning from those in the trenches and better ways of managing risks. Moderators, safety officers and customer service managers from the leading networks discuss the trials and tribulation, along with experts in risk management and safety advocates. Parry Aftab, Executive Director, WiredSafety, moderating with Tim McShane, Risk Manager Support Advisor, WiredTrust.

The International StopCyberbullying Conference is an experts' conference. Used by the UN in running conferences when the audience contains as many experts as on the stage, the strategy is to tap into that expertise and creativity and build from the participants, not just from formal speakers. So be involved, be outspoken, be part of the event. Share what you know! Ask the hard questions and help frame the issues. Be an active part of the event!

Video Cyberbullying Confessionals – Throughout both days, participants will have an opportunity to share their experiences, comments and questions "MTV-style." They can do it during the conference itself, or they can do it on video at our Video Cyberbullying Confessionals Booth. Videos will be recorded and used in creation of documentaries, educational programs and in creating solutions to cyberbullying.

The Megan Pledge – The Megan Pledge was created by a group of Teenangels, from New Rochelle, NY. Trained in all aspects of cybersafety and responsible use, this Teenangels Chapter decided to do something to get other teens involved in the fight against cyberbullying. They created the Megan Pledge, named for Megan Meier, the young teen who took her own life rather than face the continued harassment at the hands of a local mom posing as a cute 16-year-old boy on MySpace. (A copy of the Megan Pledge is the handouts.) They hoped for 1 million takers this year.

...and myYearbook.com Through the generosity of myYearbook.com, conference participants can take the Megan Pledge online, as well as by signing the pledge manually. In the first 24 hours since myYearbook.com/MeganPledge launched, more than 100,000 people took it online. Within 48 hours, 200,000 had taken it. And many shared their own stories, comments and sent their prayers and thoughts to Tina Meier (Megan's mom). With myYearbook's help, the Teenangels hope to get their 1 million by the end of the summer. To take the Pledge online, visit myYearbook.com/MeganPledge.

McAfee's Live Blog – McAfee, a trusted partner of WiredSafety and one of the sponsors of this conference, will be blogging during both days of the conference live from the conference venue. Got something to share with the world? Share it with the McAfee blogger during the conference.

Webcasting – iCast Media Productions is generously donating the two day webcast for the StopCyberbullying Conference. With live webcasting of the key speakers and panels and on demand webcasting of the break-out sessions and workshops, people from home and their work can participate and revisit the conference.

Teenangels Mentoring – With experts and experts' experts abound, this conference is a great way to mentor younger people in cybersafety, industry best practices and how to get others involved in a cause. Mentors such as Catherine Bolton (former Exec Director of the PSRA), Joe Alhadeff (CPO and Chief Compliance Officer, Oracle), Geoff Cook (CEO, myYearbook.com), Chris Kelly (CPO, Facebook.com), Lisa Hicks-Thomas (DAG, Virginia), Tina Meier (Megan's mom and honorary chair, Megan Pledge), Stephanie Stahl (CMP), Kathleen Zanowic (CPO, Verizon) and others are already mentoring teens and tweens in WiredSafety's Teenangels and Tweenangels programs. Offer to help, and even star in a short video teaching them something you can share. You'll find Teenangels and Tweenangels armed with video cameras throughout both days. Flag one down and spread the wealth of what you know!

Cyberbullying in a Nutshell

[excerpted from upcoming The STOPcyberbullying Toolkit Guide for Parents, copyright 2008 Parry Aftab]

Sometimes, largely because they feel that they are anonymous people do things online they would never dream of doing in real life. These range from rude conduct and lewd language ("flaming"), to insults, defamation and bullying ("cyberbullying"), to creating fear ("harassment"), to credible threats of actual harm offline ("cyberstalking"). Typically we define "cyberbullying" as "a communication or posting by one or more minors using cyber-technology or digital media designed to hurt, threaten embarrass, annoy, blackmail or otherwise target another minor." It can involve txt, gaming devices, Internet, IM or images.

Unfortunately, in a majority of the cases, the only way to tell the victim and cyberbully apart is by which one clicked the mouse last. Depending on what they are doing and how they are doing it, their actions may just be annoying, may violate their ISP's terms of service or school disciplinary code or may even be criminal.

The ways cyberbullies harass their victims expand every day as new technologies are released and the cyberbullies find ways to abuse them. They use profiles, e-mail, instant messaging, blogs, bulletin boards, chatrooms, photo and videophones, digital images posted online, text messaging and cell phones, handheld communication and gaming devices and Web sites. They often pose as their victim, doing things or saying things to get the target into trouble online. They may even break-into their victim's accounts by either misusing or guessing their passwords, and once there either spam their victim's friends and sometimes even change the password locking the victim out of their own account, so they can't fix it.

They may use intimate details about the other's sexual activities or preferences or relationships or post real or manipulated images at porn sites, on other Web sites and in blogs. They may place sexually-explicit advertisements posing at the victim, or make public very private information and images of the victim. They may post real or fake secrets about their victims. They may also sign them up for pornography Web sites, lots of e-mailing lists and disgusting content. They may put their head on someone else's naked body.

They sometimes use the terms of service rules against the victims, by provoking an angry response and then reporting the victim's angry response as a terms of service violation. These are called "notify" or "warning" wars. Often bullies will also hack their victim's computers or send them viruses or other malicious codes.

The most dangerous kind of cyberbullying is cyberbullying by proxy. That means the cyberbully uses others to do their dirty work. Notify or warning wars are less harmful examples of this kind of attack, where AOL, Facebook or MySpace terminate the victim's account because of the reports or defacing of their profile by someone posing as them.

The dangerous proxy attacks get hate or sexual predator deviant groups involved. They may pose as (or report) a minority teen on a white supremacy group site, hate site or a neo-Nazi site, posting things to get an angry reaction against the victim with their contact information posted. They may post an advertisement posing as the victim, looking for sex with adults. The hate group or deviant group members then attack, solicit or approach the victim online or in real life and never know they are being manipulated by a teen or preteen. When adults get involved, minors are at serious risk for bodily harm.

Several young teens have taken their own lives rather than face continued cyberbullying. Several physical assaults have been linked to cyberbullying, as has one murder (in Japan).

environment, smaller kids or the local resident geeks. They do it for the same reason the other PH CBs do, but have to be anonymous when they do it to avoid a f2f confrontation they can't win. They are called "Revenge of the Nerds." They 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. It's also ego-driven, but for other reasons. Here the main motive is to impress others with their status. The more people who witness it and let them get away with it the better. Sadly, because they are often the most popular kids in school, the other students often do whatever the MG CB wants them to do, including joining-in to CB the victim.

MG CB aren't always girls, but they are always mean. They do it in groups, often as a social event. Instead of threats, MG CB use rumors, insults, and innuendo. Their weapons are words and attack reputations. Sometimes their tactics are the most hurtful. In all cases Parry knows of, the cyberbullying-driven suicides resulted from MG attacks. Words can kill.

Vengeful Angels see themselves as the "Robin Hoods" of cyberspace. They do it to defend others they consider weaker and incapable of defending themselves. They think they are righting wrongs and standing up for others. They aren't defending themselves, though.

VA CB are surprised that anyone might consider them a cyberbully. They see themselves as the "good guys." They are often more prevalent when a school is not handling bullying very well. They feel that taking matters into their own hands is their only option. They cannot conceive that any attacks against others, even if you think they deserve it or started it, is wrong. Since they are not typically the thuggish type and may want to avoid physical confrontations, they have to avoid anyone figuring out who they are. They do their cyberbullying anonymously or posing as the bully they are targeting. They often use cyberbullying-by-proxy methods, to get the ISP, parents or the school to do the dirty work for them.

Setting Up The Victim to Take the Fall! (*Cyberbullying by Proxy*):

Often people who misuse the Internet to target others do it using accomplices. These accomplices, unfortunately, are often unsuspecting. They know they are communicating provocative messages, but don't realize that they are being manipulated by the real cyberharasser or cyberbully – often a 12 year old. That's the beauty of this type of scheme. The attacker merely prods the issue by instigating a reaction and then sits back and lets others do their dirty work.

It's very powerful. It is also one of the most dangerous kinds of cyberharassment or cyberbullying. Teens do this often using AOL, MSN, Facebook or another ISP as their "proxy" or accomplice. When they engage in a "notify" or "warning" war, they are using this method to get the ISP to see the victim as the "bad guy." A notify or warning war is when someone provokes another, until the victim lashes back. When they do, the real attacker clicks the warning or notify button on the text screen. This captures the communication and flags it for the ISP's review. If the ISP finds that the communication violated their terms of service agreement (which most do) they may take action. The ISP does the attacker's dirty work when they close or suspend the real victim's account for a "terms of service" violation. Most knowledgeable ISPs know this and are careful to see if the person being warned is really being set-up.

Sometimes kids use the victim's own parents as unwitting accomplices. They provoke the victim and when the victim lashes back, they save the communication and forward it to the parents of the victim. The parents often believe what they read, and without having evidence of the prior provocations, think that their own child "started it." (This works just as well when the cyberbully launches a txt-bomb attack sending thousands of TM to the victim, anonymously from the Internet, and the victim's TM bill goes through the roof. The parents do the cyberbully's dirty work when they take away the cell phone or otherwise discipline the victim.)

This is very effective in a school disciplinary environment, where the cyberbully hopes to have the school blame the victim. They may make it look like the student/victim posted something nasty about the principal or a teacher. That's why those in authority should never take any cyberbullying at face value before doing further investigation.

Just because a message looks like it was sent from someone, doesn't mean it was sent by that person. The only way to be sure is to track electronic data. A print-out won't help find the culprit. You need to save the electronic communication on your device, to be able to gather the necessary info, electronically.

Many teens have no idea that MySpace, Facebook and YouTube collect this digital data and will turn it over to the police under legal process. It will lead them right to your computer or other device. You're never anonymous online.

The Cyberbullying Risk Checklist

It's not always easy to tell flaming and cyberbullying apart, except for serious cases of cyberstalking, when you "know it when you see it." But you can 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 can get help from the authorities.

The kind of threat:

- The communication uses lewd language
- The communication insults you directly ("You are stupid!")
- The communication threatens you vaguely ("I'm going to get you!")
- The communication threatens you 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 you or someone you care about with serious bodily harm or death ("I am going to break your legs!" "Say goodbye to your dog!" 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:

- You know who is doing this
- You think you know who is doing this
- You have 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 without a threat
- Following the victim around online, into chat rooms, favorite Web sites, etc. and letting them know they are there
- Building fake profiles, Web sites or posing as the victim
- Planting statements to provoke third-party stalking and harassment
- Signing the victim 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 victim online (taken from any source, including video and photo phones) without their permission
- Posting real or doctored sexual images of the victim
- Sharing personal or intimate information about the victim
- Targeting the victim for a third party sexual solicitation ("for a good time call ..." or "I am interested in [fill in the blank] sex...")
- Reporting the victim 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 the victim on that list or encouraging others to post nasty things about them.
- Hacking the victim's computer and sending them malicious codes
- Sending threats to others (like the president of the United States), sending malicious code or attacking others while posing as the victim
- Copying others on the victim's private e-mails and IM communications or faking them
- Registering the victim's name and setting up a bash Web site or profile
- Posting rude or provocative comments while posing as the victim (such as insulting racial minorities at a Web site devoted to that racial minority)
- Masquerading as the victim for any purpose
- Posting the victim's text-messaging address or cell phone number online to encourage abuse and increase their child's text-messaging or cell phone charges.

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 should be used. If personal contact information is being shared online, this must be treated very seriously.

If the victim 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 12-year old doing it for a laugh. It escalates quickly and can be dangerous. You have to report it to the police!

Reporting terms of service violations

Often, the only recourse you have to stop a bully online is to report them to their e-mail service provider, social network or ISP. If the actions violate the terms of service (TOS) 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. There, read the policy carefully. Make notes about which sections you believe were violated and how.

In the majority of cases, they also have 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. And 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 has been 'enhanced' to be more serious than it actually is. There are also privacy and legal considerations that they must consider. And they receive hundreds of thousands of TOS reports and have to prioritize them.

The likelihood of getting a response and their 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:

1. Date and time that the violations of their TOS took place (keep each violation separate in the report). Let them know your time zone too.
2. Copies of emails (complete with headers (we teach you how to do that at WiredSafety.org if you don't know). Your "help" instructions with your e-mail application may walk you through it also, step-by-step.), or 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).
3. 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).
4. A time-line of how the situation developed, including copies of all communications. (Using a monitoring application, like SpectorSoft Pro can be very helpful here).
5. 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. 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 may 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. 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.

ThinkB4uClick

One of the biggest problems we have online is that no one thinks between their brain dump typing and clicking "send." There is a filter between what we think and our mouths called "being polite." Generally this filter kicks in when we are looking someone in the eye and think about how they would respond and how others around you would respond if you say what you really wish you could say. But when we sit in front of the computer, there are no eyes to look into. Just us and the computer monitor. And just as we can say outrageous things in our diaries, typing them online seems private.

It is also fun to say things that you know you shouldn't say. Wouldn't it be really kewl to tell that bully off? Or tell your best friend how mean they were...or that snotty girl in class that she really isn't as gorgeous as she thinks she is...or that "popular" guy how he is just

- Repeated e-mails or IMs without a threat
- Following the victim around online, into chat rooms, favorite Web sites, etc. and letting them know they are there
- Building fake profiles, Web sites or posing as the victim
- Planting statements to provoke third-party stalking and harassment
- Signing the victim 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 victim online (taken from any source, including video and photo phones) without their permission
- Posting real or doctored sexual images of the victim
- Sharing personal or intimate information about the victim
- Targeting the victim for a third party sexual solicitation ("for a good time call ..." or "I am interested in [fill in the blank] sex...")
- Reporting the victim 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 the victim on that list or encouraging others to post nasty things about them.
- Hacking the victim's computer and sending them malicious codes
- Sending threats to others (like the president of the United States), sending malicious code or attacking others while posing as the victim
- Copying others on the victim's private e-mails and IM communications or faking them
- Registering the victim's name and setting up a bash Web site or profile
- Posting rude or provocative comments while posing as the victim (such as insulting racial minorities at a Web site devoted to that racial minority)
- Masquerading as the victim for any purpose
- Posting the victim's text-messaging address or cell phone number online to encourage abuse and increase their child's text-messaging or cell phone charges.

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 should be used. If personal contact information is being shared online, this must be treated very seriously.

If the victim 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 12-year old doing it for a laugh. It escalates quickly and can be dangerous. You have to report it to the police!

Reporting terms of service violations

Often, the only recourse you have to stop a bully online is to report them to their e-mail service provider, social network or ISP. If the actions violate the terms of service (TOS) 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. There, read the policy carefully. Make notes about which sections you believe were violated and how.

In the majority of cases, they also have 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. And 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 has been 'enhanced' to be more serious than it actually is. There are also privacy and legal considerations that they must consider. And they receive hundreds of thousands of TOS reports and have to prioritize them.

The likelihood of getting a response and their 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:

1. Date and time that the violations of their TOS took place (keep each violation separate in the report). Let them know your time zone too.
2. Copies of emails (complete with headers (we teach you how to do that at WiredSafety.org if you don't know). Your "help" instructions with your e-mail application may walk you through it also, step-by-step.), or 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).
3. 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).
4. A time-line of how the situation developed, including copies of all communications. (Using a monitoring application, like SpectorSoft Pro can be very helpful here).
5. 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. 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 may 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. 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.

ThinkB4uClick

One of the biggest problems we have online is that no one thinks between their brain dump typing and clicking "send." There is a filter between what we think and our mouths called "being polite." Generally this filter kicks in when we are looking someone in the eye and think about how they would respond and how others around you would respond if you say what you really wish you could say. But when we sit in front of the computer, there are no eyes to look into. Just us and the computer monitor. And just as we can say outrageous things in our diaries, typing them online seems private.

It is also fun to say things that you know you shouldn't say. Wouldn't it be really kewl to tell that bully off? Or tell your best friend how mean they were...or that snotty girl in class that she really isn't as gorgeous as she thinks she is...or that "popular" guy how he is just

stupid? Or tell your teacher that she isn't as smart as she thinks, or [fill in the blank]? Everyone has things they wish they could say. But usually when we break the rules and say them, we wish we could take it back.

That's the problem. You can never really take it back. When you send or post something online, it lives on forever in archives, caching and other places...like the energizer bunny, it keeps on going and going and going. So, what can you do? The more you plan in advance how you will deal with hurtful things online, the easier it will be when they happen.

Be your own filter. Use the one between your ears. You can think before you type. And think again before you click "send." Read what you wrote. Does it really say what you wanted it to say? Can it be misunderstood? Are you sending it to the right address? Are you sure? Will you regret sending it? If there is any question, don't send it. And give yourself as much time as you can. Walk away from the computer. Listen to some music. Take 5!

Write it but don't send it. Set up a file on your computer. A kinda "brain dump" journal, where you can save things you wish you could say, but know you shouldn't. Sometimes just writing them down is enough to make you feel better. You can always go back and read what you wrote later and see how you feel about it. Most of the time you will probably be happy you never sent it. Sometimes you may forget what made you angry to begin with.

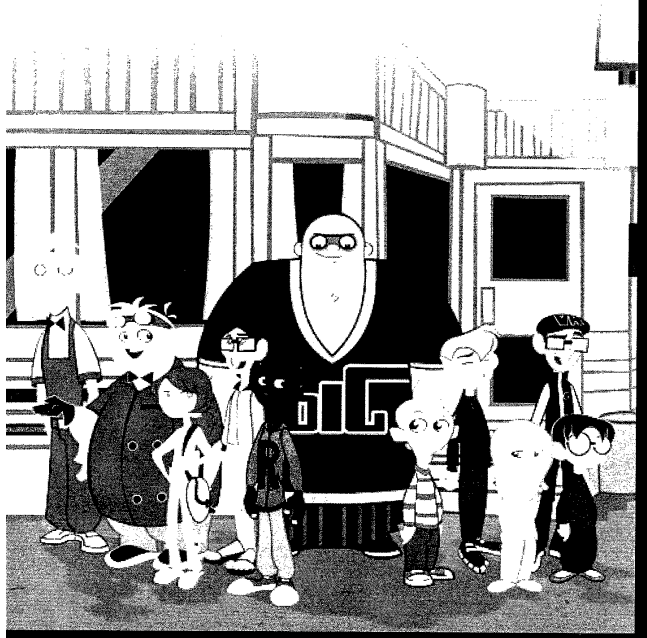
Just make sure that if you are going to keep these mean things on your computer, you keep them private. Use a password to protect them, or encrypt them. And if you are saying mean things about people in your family you may not want to keep them on your computer at all. And when you don't need something in this journal anymore, delete it. And learn from what you delete. Are you relieved that you never sent it? Did writing it make you feel better?

Write it but only send it to your cyber-buddy. Sometimes just writing and saving it isn't enough. You are angry and want to share that with someone. Instead of sharing it with the person you really want to attack, find a trustworthy friend or family-member you can send it to. Choose someone who is understanding and a good listener. Choose someone who keeps secrets. Choose someone who really cares about you. If you have a good relationship with your parents, you may want to choose one of them.

Write it, but wa it 24 hours before sending it. Sometimes just writing it or sending it to your cyber-buddy isn't enough. Sometimes you really think you should send it. Okay. Maybe you should. But before you do, write it and save it in your 24 hour file first. That may give you enough time to calm down. It usually works.

The Case of the Bully in the Machine

Coming Soon to a Computer Near You



ALEX WONDER

KID CYBERDETECTIVE

SNAP Cyberbullying.org