Cyberbullying 101

What is Cyberbullying?

"'Cyberbullying' is "any cyber-communication or publication posted or sent by a minor online, by instant message, e-mail, website, diary site, online profile, interactive game, handheld device, cell phone, game device, digital camera or video, webcam or use of any interactive device that is intended to frighten, embarrass, harass, hurt, set up, cause harm to, extort or otherwise target another minor."

Parry Aftab provides a shorter definition of cyberbullying: "'Cyberbullying' is when minors use technology as a weapon to intentionally target and hurt another minor." And the shorter definition works pretty well. With one exception, all cyberbullying must be intentional. It requires that the cyberbully intends to do harm to or annoy their target. (In the one exception to this rule, the student is careless and hurts another's feelings by accident. It's called "inadvertent cyberbullying," because the target feels victimized, even if it is not the other student's intention. Since it often leads to retaliation, traditional cyberbullying and cyber warfare, it is considered one of the four main types of cyberbullying.)

Cyberbullying needs to have minors on both sides, as target and as cyberbully. (If there aren't minors on both sides of the communication, it is considered "cyber - harassment," not "cyberbullying.") When a student harasses a teacher, it falls under cyberharassment, not cyberbullying. (Note that some new cyberbullying laws classify this as "cyberbullying" for those purposes, though.) Rather than getting caught up in semantics, Parry Aftab created a checklist for law enforcement first responders (those who take the call when it comes in initially or show up to interview the victims). It measures the nature of communications, frequency and identity or anonymity of the cyberbully for the risk assessment. She has also tailored it for parents in the Cyberbullying Checklist for Parents.

How Prevalent is Cyberbullying?

Cyberbullying is out of control and growing like crazy. Parry visited schools around North America (primarily in the US) and polled the students in each session. In total, in 2008 she polled approximately 45,000 students in middle school and early high school, as well as 6th graders in some grammar schools. She listed the kinds of things that typically constitute cyberbullying and asked the students to raise their hands if any of those things had happened to them in the last year. She then counted the hands raised and did the math on what percentage of the students in the group admitted to having been cyberbullied. (The only way to accurately research cyberbullying is to avoid using that term. "Cyberbullying" means different things to different students. So polls and surveys are often inaccurate if they ask whether someone "has been cyberbullied.")

She never had fewer than 85% of the students admit that they had been

targeted at least once in the last year. In 2006, in Westchester County, New York (an affluent county outside of New York City where most students have multiple devices with Internet connections), 97% of the middle-schoolers polled admitted to having been cyberbullied. And in one boarding and laptop school in Canada, 100% of the students responded that they had been cyberbullied. (For more information about the effect of laptop programs and boarding school Internet access on cyberbullying, read the "Laptop Programs Guide" for schools from aftab.com)

Yet only 5% of students would tell their parents if they are targeted by a cyberbully, the same students reported. There are 67 different reasons they have given Parry why they wouldn't trust their parents with their being targeted by a cyberbully. Most believe that their parents would blow things out of proportion, find out they were using a game, site or device they weren't supposed to be using or fear that they will turn off the technology. The rest span the typical spectrum – embarrassment, not wanting parents to know they are unpopular or fearing that their parents will believe the falsehoods and rumors.

In 2008, our polls disclosed that 50% of middle-schoolers had heard of or seen a website/profile/quiz bashing another student in their school, and 75% had visited one. 40% have either had their password stolen and changed by a cyberbully (locking them out of their own account) or had communications sent to others posing as them. Those percentages have increased steadily since then, with the latest polls showing that 100% of the students had heard of or seen a website/profile/quiz or tweets/texts or app posts bashing another student in their school, 85% of the students have visited or internationally viewed one of these and 55%have reported that their accounts had been "hacked" by a cyberbully, had their password stolen and abused or had communications sent to others by someone posing as them.

Cyberbullying begins as early as 1st and 2nd grade, depending on the age when cell phones, virtual worlds, apps and Internet use begin. Interestingly, it peaks in 4th grade and again in 7th and 8th grade.

How Does Cyberbullying Work?
Cyberbullying can be conducted using most digital and interactive technologies. When a new technology is released, students find ways to use them as weapons within days. They misuse cell phones, handheld gaming devices and text devices, digital still and video cameras, online game sites, social networks, webcams, virtual worlds, passwords, instant messaging, e-mails, blogs, photos, iPods and voice over IP devices.

There are five different cyberbullying methods:
1. Direct attacks (messages sent to the target directly);
2. Posted and public attacks designed to humiliate the target;
3. Cyberbullying-by-proxy (using others to help cyberbully the victim, either with or without the accomplice's knowledge);

4. Inadvertent cyberbullying (or accidental cyberbullying) when communications are not intended to hurt anyone, but result in hurt feelings; and
5. Privacy intrusions and exposure of private facts.

Because cyberbullying by proxy often gets adults involved in the harassment (without their knowing they are being manipulated by kids), and since it often involves both online and offline actions, it is much more dangerous than any other type of attack.

What Are the Different Kinds of Cyberbullies?

There are four different profiles of cyberbullies (and one sub-type). They are categorized based on their motivations for the cyberbullying. They may use the same methods as the other kinds of cyberbullies, but the reasons for their actions are very different. Parry has designed an interactive that lays out the different types of cyberbullies, their motives, methods and solutions to each. It's called "Cyberbully Descriptions" and can be found on WiredSafety.org under "Resources/Interactives."

The four types of cyberbullies include:
- The "Vengeful Angel"
- The "Power-Hungry" (or "Revenge of the Nerds" sub-type of Power-Hungry)
- The "Mean Girls"
- The "Inadvertent Cyberbully" (sometimes called the "Accidental Cyberbully")

Some methods of cyberbullying are unique to a certain kind of cyberbully and so are the ways the cyberbullies maintain their anonymity or broadcast their actions to others. Some are secretive; some require an audience and some are entirely inadvertent.

"The Vengeful Angel":
In this type of cyberbullying, the cyberbully doesn't see themselves as a bully at all. They see themselves as righting wrongs, or protecting themselves or others from the "bad guy" they are now victimizing. They believe they are the Rob in Hoods of cyberspace. Vengeful Angels may be angry at something the cyberbully (or offline bully) did and feel they are taking warranted revenge or teaching the other a lesson. The Vengeful Angel cyberbully often gets involved trying to protect a friend or another student whom is being bullied or cyberbullied. When Vengeful Angels arise in a school, it is usually a sign that something in the system isn't working. They step in because no one else does.

The "Power-Hungry" and "Revenge of the Nerds" (a sub-type of Power Hungry cyberbullies):
Just as their schoolyard counterparts, some cyberbullies want to exert their authority, show that they are powerful enough to make others do what they want and some want to control others with fear. Sometimes the student wants to hurt another student. Sometimes they just don't like the other student, are just seeking

a reaction or are just targeting the next person to log on (the classic wrong place at the wrong time motive). They are looking for attention and want to see their target(s) sweat. These are no different than the offline tough schoolyard bullies, except for their use of technology. And in most cases, they are the schoolyard thugs that use offline intimidation and their fists to hurt and control others and this is just another method of attack.

A sub-type profile of the "Power-Hungry" is called "Revenge of the Nerds." This type of cyberbully is often the victim of typical offline bullying. They may be female, or physically smaller, the ones picked on for not being popular enough, or cool enough (the "girls and the geeks"). They may have greater technical skills, as well.

They use technology to level the playing field between the strong and the weaker but tech-skilled. It is their intention to frighten or embarrass their victims in the same way as their beefier Power-Hungry cyberbully counterparts. And they are empowered by the anonymity of the Internet and digital communications and the fact that they never have to confront their victim in real life and risk being physically hurt. They may act tough online, but are not tough in real life. They are often not a bully but "just playing one on TV."

"Mean Girls":
This type of cyberbullying is always mean, but not always committed by girls. It occurs when the cyberbully is bored or looking for entertainment. It is a social - exclusion method, where the cyberbully or teams of cyberbullie s are showing their social clout. It is largely ego-based and they are the most immature of all cyberbullying types.

Typically, in the "Mean Girls" bullying situations, the cyberbullies are female. But Parry is seeing more males joining in existing Mean Girls groups or creating their own social groups of males who are in the "in crowd." This style of cyberbullying is used more often by girls to harass others girls than any other type of cyberbullying. (Boys most often use a Power-Hungry or hacking attacks tactic.) It is used more often for cross-gender cyberbullying as well and spreads very quickly. Mean Girls cyberbullying is often a campaign, rather than a one -off incident.

Mean Girl cyberbullies can do serious damage, especially to young teens and older preteens. In each case (to Parry's knowledge) of teen cyberbullying-related suicide, the cyberbullies used "Mean Girl" tactics to harass their victims.

Bystanders are crucial in a Mean Girls campaign, they are expected to be active and forward along mean messages and vote in bashing sites and quizzes. And because they fear that they will be the next victim if they don't join in, they tend to be very involved in helping perpetuate the cyberbullying.

"The Inadvertent Cyberbully":
Inadvertent cyberbullies usually don't think they are cyberbullies at all. They didn't mean to hurt anyone but were just careless. Parry terms this group "careless and clueless." She sometimes calls them the "accidental cyberbully" too, since students have problems spelling "inadvertent." They are also the one exception to the "cyberbullying requires intent" rule.

Often they leave out crucial words like "not," when typing, or type faster than they can think and are not careful about what and how they say things. The recipient doesn't understand that the hurt was unintentional. And that's why it is still cyberbullying. Inadvertent cyberbullies may also be pretending to be tough online, or role playing, or they may be reacting to hateful or provocative messages they have received. Unlike the "Revenge of the Nerds" cyberbullies, they don't lash out intentionally. They just respond without thinking about the consequences of their actions. They may feel hurt, or angry because of a communication sent to them, or something they have seen online. And they tend to respond in anger or frustration. They don't think before clicking "send."

Sometimes, while experimenting in role-playing online, they may send cyberbullying communications or target someone without understanding how serious this could be. They do it for the heck of it. They might have been kidding around and their joking not appreciated, or may have used a new screen name that the "target" doesn't recognize. And maybe they just sent a message to the wrong person and that person takes offense.

Why Do Students Cyberbully Each Other?
Who knows why students do anything? When it comes to cyberbullying, they are often motivated by anger, revenge or frustration. Sometimes they do it for entertainment or because they are bored and have too much time on their hands and too many tech toys available to them. Many do it for laughs or to get a reaction. They may do it because they think it's fun. And a growing number do it to make a point to others, to improve their profile's popularity or video's page views, get attention or their "15 megabytes of fame."

Each of the four types of cyberbullies (and the one sub-type) does it for their own particular motive:

1. The Power-Hungry cyberbullies do it to torment others and to enhance their view of themselves as being in charge.

    a. Revenge of the Nerd cyberbullies (a sub-type of Power-Hungry cyberbullies) may start out defending themselves from traditional bullying only to find that they enjoy being the tough guy or gal.

2. Mean Girl cyberbullies do it to help bolster or remind people of their own social standing.

3. Vengeful Angel cyberbullies think they are righting wrongs and standing up for others.

4. Inadvertent cyberbullies never meant to hurt anyone, but because they were careless hurt them by accident.

While the tactics may differ, most are motivated by anger, lack of impulse control, frustration, ego-boosting, revenge, jealousy, the need to teach someone a lesson, the desire to impress others, to make a point, to be funny or become more popular, to

draw attention to their online posts and presence, by boredom or by being careless, thoughtless and typing without thinking.

Because their motives differ, the solutions and responses to each type of cyberbullying incident have to differ too. Unfortunately, there is no "one size fits all" when cyberbullying is concerned. You have to target each cyberbully profilethe response that counters their motives.

What Ages are Impacted by Cyberbullying?

Cyberbullying typically starts at about 7 years of age (younger in very connected communities) and usually ends (as "cyberbullying") around 15. After then the cyber harassment continues but it changes. It usually becomes sexual harassment or is done for revenge against a former boyfriend or girlfriend or former friend. It often involves threats to share sexts or other types of sextortion.

It is interesting to note that high school students deny that cyberbullying exists in high school. High school students insist that "cyberbullying" is for middle-schoolers and something that happens before they mature into high-schoolers, Parry doesn't call it "cyberbullying" in high school. She calls it "cyber-harassment" or "digital drama" instead. These terms resonate with high-schoolers far better than the term "cyberbullying."

Many cases of cyberbullying also occur right after a child receives their first IM or cell phone accounts when they often try to see what they can get away with. Some don't appreciate the consequences of their actions. (Many stop when they understand the consequences or how much their actions are hurting others, which points to the need for early education.)

Password theft and misuse and the theft of points or game "gold" from their friend's game account are often the earliest forms of cyberbullying among 6 -7 year olds. Interestingly, the younger kids use extortion as their preferred method of traditional cyberbullying. Cyberbullying has been trending younger and younger as the kids are using these technologies at earlier ages than ever before. Virtual worlds like Disney's become popular with kids as young as 3 or 4.

At the same time we are seeing cyberbullying trend downward in age, it is also trending upwards as a result of the growth of social networking sites and communities. Cyberbullying activities extend into universities, medical and law schools. (As defined, cyberbullying is only between or among minors, and technically this would fall into the "cyber harassment" category. Cyber-harassment of adults by adults began before children had access to the Internet, and continues to grow.)

Who is a Typical Target?

Any child, preteen or teen is a potential cyberbullying target. They don't need to have home Internet access, a cell phone or any cyber -connection. The cyberbullies are perfectly happy to have the technology do their dirty work in destroying reputations or creating offline responses to online provocation.

Obviously, when friends have a falling out or romance takes a bad turn, cyberbullying is a viable option to settle scores and share hurt feelings. According to Teenangels' research and surveys, 70% of cyberbullying comes from friends or acquaintances.

Bigotry, hate and intolerance are big motivators, as well. Anyone who has been the target of offline bullying or is more vulnerable to it is a likely target too. Jealousy plays a powerful role in motivating cyberattacks by those involved or formerly involved in relationships, or those rebuffed by the ones they like. Friends pile on fast to "defend" their friends' honor, and lines are drawn in cyberspace.

The more a student shares personal and private information, gets involved in heated online debates or has an offline problem, the more likely they are to be targeted.

The less careful they are the fewer security settings and tools they use and the less care they take in their communications, the more likely they will be targeted. And, if their password is vulnerable, so are they. And 85% of grammar school students and 70% of middle and high school students have shared their passwords with at least one other person.

The more digitally-literate the students are, the less vulnerable they will be. Many leave themselves open to attack, hacking and having their personal information misused by cyberbullies. And an easy mark is far more obvious online than offline. Parry sees adoption of "digital hygiene" practices as an important step in preventing cyberbullying.

Cyberbullying starts early and continues to adulthood if things don't play themselves out or if they don't learn how to protect themselves.

The Risks by Technology

The kinds of technologies used to cyberbully someone fall into three types – those that allow communication, those that share content and those that cost money or put technology at risk. Parry calls these "the 3Cs – contact, content and cost" and they include services, features and technologies.

While the students are very creative and can find new ways to misuse more services, features and technologies, there are favored types of technologies for each of the three methods of cyberbullying:

- Communication tools and features are used for direct attacks and to help spread rumors.

- Content tools and features share embarrassing and harassing images, information and comments; and

- Cost tools and features end up with text-bombs and high cell phone bills,

hacking attacks and ID theft.

While the technology being used changes with the trends and times, we can be sure of one constant – if it can be used as a weapon to hurt someone, it will be.

Although cyberbullying can be conducted using most technologies, cell phones and social networks lead the pack. They have several things in common – they are fast and easy to use, the communications can spread quickly and they are impulsive in nature. Cell phones are used more in direct attacks and social networking for social and public attacks. Sadly, with the new applications and Internet-connected cell phones, social networking attack campaigns can be launched quickly from a cell phone, videos and all!

A school cell phone policy will do more than keep the students focused on schoolwork. It can help prevent cyberbullying during the school day and from school premises. In addition, when sextbullying is involved (forwarding sexually provocative or nude images taken and shared through text messages), cell phones are used as weapons. In cases where the images are of someone under the age of 18, under US federal law, those images constitute child pornography and the taking, sending or possession of them can result in serious criminal consequences. (To learn more about the items a cell phone policy should address, visit the School Policies section under WiredSafety.org/resources.)

What Can You Do To Address Cyberbullying?

Creating a school cyberbullying policy and established set of procedures and communicating them to all stakeholders is crucial. To do that and address the need for getting students, parents, network and school administrators and community safety experts working together, every school should start with the creation of a WiredSafety School team. By bringing all stakeholders to the table (especially the students), the right tone to address cyberbullying on a school by school basis can be identified and the policies determined, written, communicated and enforced more easily.

In the early days of schools online we had a favorite motto: "Educate, don't legislate!" While we still believe that education is the first and last place to turn, we need some help here in legislation too. Laws that permit schools to get involved in off-premises cyberbullying can be very helpful, but need to be narrowly drawn to avoid First Amendment challenges. Having a criminal law in place to allow law enforcement to investigate who is behind the messages is crucial. How can we teach accountability if we don't know whom to hold accountable?

But, as we said, it all starts with you – the educators! Educating the kids about the consequences of cyberbullying (losing their YouTube or Instagram accounts or having the police show up at their door) helps. Teaching them to respect others and to take a stand against bullying of all kinds helps too.

Teaching them Internet and information literacy skills have to be our primary mission. Password abuse is one of the keys to all cyberbullying evil. They use

each other's passwords without permission or hack into their account s to set them up, steal their points or items from game sites or change their passwords without letting their target know. Guiding them to use privacy settings when they use social networks, authenticating their devices (when available as a social media security option) and not share anything online that they wouldn't want their parent s, principal, predators, potential employers and high education institutions or the police to see is important too. The less personal information their potential cyberbullies have about them, the less ammunition they have to use against them.

Awareness of how much cyberbullying hurts can make all the difference in the world. Amanda Todd's tragic story has hit home with the students. Teens designed a program called "The Amanda Todd Pledge." It gets students to step up and take a pledge in Amanda's name not to cyberbully or see suicide as an option. To date more than 500,000 people have taken one of our StopCyberbullying Pledges. To take the pledge, print it out and have your students sign it and either return them to us at the address in the pledge instructions or e-mail us with the name of the school and how many took the pledge. We have a digital version at StopCyberbullying.org as well.

For those who want a more generic form of pledge, the StopCyberbullying Pledge covers all the cyberbullying issues, but leaves out the suicide references. It can be customized for each school and works very well with younger students who might be too young for the anti-suicide message in the Amanda Todd Pledge.

It's More Than Just Another Medium for Bullying

Experts who understand schoolyard bullying often misunderstand cyberbullying, thinking it is just another method of bullying. But the motives and the nature of cyber communications, as well as the demographic and profile of a cyberbully differ half the time from their offline counterparts.

One of the biggest problems Parry encounters is with traditional bullying experts who don't truly understand cyberbullying but provide advice anyway (which is often very wrong). They tell victims and their parents to use print -outs to help prove the cyberbullying (which is utterly worthless given the ease in which typed communications can be altered). And they often tell young victims to stand up for themselves when dealing with a cyberbully (which works offline, but only provokes more cyberbullying online).

While cyberbullying is a tactic used by some traditional bullies, most cyberbullying is very different. Only two of the types of cyberbullies have something in common with the traditional schoolyard bully and may slip from offline to online and vice versa. These are Mean Girls (always mean, but not always girls) and Power -Hungry (the ones who are the thugs of the schoolyard).

Cyberbullying is more about impulse control, technology tricks and entertainment than about interpersonal behavior. It's often less about conflict resolution than about getting their 15 megabytes of fame. And unless we recognize and accept this, we will not be able to effectively address the problem.