

Direct Attacks

1. Instant Messaging/Text Messaging Harassment
2. Stealing Passwords
3. Blogs
4. Web Sites
5. Sending Pictures through E-mail and Cell Phones
6. Internet Polling
7. Interactive Gaming
8. Sending Malicious Code
9. Sending Porn and Other Junk E-Mail and IMs
10. Impersonation

1. Instant Messaging/Text Messaging Harassment

- a) Kids may send hateful or threatening messages to other kids, without realizing that while not said in real life, unkind or threatening messages are hurtful and very serious.
- b) Warning wars - Many Internet Service Providers offer a way of "telling on" a user who is saying inappropriate things. Kids often engage in "warning wars" which can lead to kicking someone offline for a period of time. While this should be a security tool, kids sometimes use the Warn button as a game or prank.
- c) A kid/teen may create a screenname that is very similar to another kid's name. The name may have an additional "i" or one less "e". They may use this name to say inappropriate things to other users while posing as the other person.
- d) Text wars or text attacks are when kids gang up on the victim, sending thousands of text-messages to the victim's cell phone or other mobile device. The victim is then faced with a huge cell phone bill and angry parents.
- e) Kids send death threats using IM and text-messaging as well as photos/videos (see below)

2. Stealing passwords

- a) A kid may steal another child's password and begin to chat with other people, pretending to be the other kid. He/she may say mean things that offend and anger this person's friends or even strangers. Meanwhile, they won't know it is not really that person they are talking to.
- b) A kid may also use another kid's password to change his/her profile to include sexual, racist, and inappropriate things that may attract unwanted attention or offend people.
- c) A kid often steals the password and locks the victim out of their own account.
- d) Once the password is stolen, hackers may use it to hack into the victim's computer.

3. Blogs

Blogs are online journals. They are a fun way for kids and teens to message for all of their friends to see. However, kids sometimes use these blogs to damage other kids' reputations or invade their privacy. For example, in one case, a boy posted a bunch of blogs about his breakup with his ex-girlfriend, explaining how she destroyed his life, calling her degrading names. Their mutual friends read about this and criticized her. She was embarrassed and hurt all because another kid posted mean, private, and false information about her. Sometimes kids set up a blog or profile page pretending to be their victim and saying things designed to humiliate them.

4. Web sites

a) Children used to tease each other in the playground; now they do it on Web sites. Kids sometimes create Web sites that may insult or endanger another child. They create pages specifically designed to insult another kid or group of people.

b) Kids also post other kids' personal information and pictures, which put those people at a greater risk of being contacted or found.

5. Sending Pictures through E-mail and Cell Phones

a) There have been cases of teens sending mass e-mails to other users, that include nude or degrading pictures of other teens. Once an e-mail like this is sent, it is passed around to hundreds of other people within hours; there is no way of controlling where it goes.

b) Many of the newer cell phones allow kids to send pictures to each other. The kids receive the pictures directly on their phones, and may send it to everyone in their address books. After viewing the picture at a Web site, some kids have actually posted these often pornographic pictures on Kazaa and other programs for anyone to download.

c) Kids often take a picture of someone in a locker room, bathroom or dressing room and post it online or send it to others on cell phones.

6. Internet Polling

Who's Hot? Who's Not? Who is the biggest slut in the sixth grade? These types of questions run rampant on the Internet polls, all created by yours truly - kids and teens. Such questions are often very offensive to others and are yet another way that kids can "bully" other kids online.

7. Interactive Gaming

Many kids today are playing interactive games on gaming devices such as X-Box Live and Sony Play Station 2 Network. These gaming devices allow your child to communicate by chat and live Internet phone with anyone they find themselves matched with in a game online. Sometimes the kids verbally abuse the other kids, using threats and lewd language. Sometimes they take it further, by locking them out of games, passing false rumors about them or hacking into their accounts.

8. Sending Malicious Code

Many kids will send viruses, spyware and hacking programs to their victims. They do this to either destroy their computers or spy on their victim. Trojan Horse programs allow the cyberbully to control their victim's computer remote control, and can be used to erase the hard drive of the victim.

9. Sending Porn and Other Junk E-Mail and IMs

Often cyberbullies will sign their victims up for e-mailing and IM marketing lists, lots of them, especially to porn sites. When the victim receives thousands of e-mails from pornographers their parents usually get involved, either blaming them (assuming they have been visiting porn sites) or making them change their e-mail or IM address.

10. Impersonation

Posing as the victim, the cyberbully can do considerable damage . They may post a provocative message in a hate group's chatroom posing as the victim, inviting an attack against the victim, often giving the name, address and telephone number of the victim to make the hate group's job easier. They often also send a message to someone posing as the victim, saying hateful or threatening things while masquerading as the victim. They may also alter a message really from the victim, making it appear that they have said nasty things or shared secrets with others.