Cyberstalking: Dangers on the Information Superhighway

By: Trudy M. Gregorie, Director of Training
National Center for Victims of Crime, 2001

Although there is no universally accepted definition of cyberstalking, the term is generally used to refer to the use of the Internet, e-mail, or other telecommunication technologies to harass or stalk another person. It is not the mere annoyance of unsolicited e-mail. It is methodical, deliberate, and persistent. The communications, whether from someone known or unknown, do not stop even after the recipient has asked the sender to cease all contacts, and are often filled with inappropriate, and sometimes disturbing, content. Essentially, cyberstalking is an extension of the physical form of stalking.

Most state and federal stalking laws require that the stalker make a direct threat of violence against the victim, while some require only that the alleged stalker's course of conduct constitute an implied threat. Although some cyberstalking conduct involving annoying or menacing behavior might fall short of illegal stalking under current laws, such behavior may be a prelude to real-life stalking and violence and should be treated seriously. Cyberstalking has the potential to move from a URL address to a real address—from virtual to actual.

In a 1999 U.S. Department of Justice report, *Cyberstalking: A New Challenge for Law Enforcement and Industry*, cyberstalking is identified as a growing problem.[1] According to the report, there are currently more than 80 million adults and 10 million children with access to the Internet in the United States. Assuming the proportion of cyberstalking victims is even a fraction of the proportion of persons who have been the victims of off-line stalking within the preceding 12 months, the report estimates there may potentially be tens or even hundreds of thousands of cyberstalking victims in the United States.

Criminal Conduct

Experienced prosecutors are also beginning to recognize the dangers on the information superhighway. Linda Fairstein, Chief of the Sex Crimes Unit in the Manhattan District Attorney's Office and a Board member of the National Center for Victims of Crime, has said, "By the use of new technology and equipment which cannot be policed by traditional methods, cyberstalking has replaced traditional methods of stalking and harassment. In addition, cyberstalking has led to off-line incidents of violent crime. Police and prosecutors need to be aware of the escalating numbers of these events and devise strategies to resolve these problems through the criminal justice system."[2]

Cyberstalking victims who call the National Center for Victims of Crime often complain of not being taken seriously or of not even being recognized as victims by law enforcement agencies they have contacted. Responding to a victim's complaint by saying "you can't be hurt on the Internet—it's just words" or "just turn off your computer" is not acceptable or responsible. It's unreasonable to expect cyberstalking victims to walk away from their on-line activities, which may comprise their professional career, in order to avoid this kind of problem. On-line harassment and threats are just as frightening and distressing as off-line harassment and threats.

A recent incident described in the *Cyberstalking Report* from the U.S. Attorney General is typical of the lack of law enforcement training and expertise that can be so frustrating for victims.[3] A woman complained to a local police agency that a man had been posting information on the Internet claiming that her nine-year-old daughter was available for sex, and including their home phone number with instructions to call 24 hours a day. Numerous calls were received. Although every call was reported to local police by the family, the police officer simply advised them to change their phone number. Subsequently, the Federal Bureau of Investigation was contacted and they opened an investigation. The FBI discovered that the local police agency did not have a computer expert, and the responding police officer had never been on the Internet. The local agency's lack of familiarity and resources may have resulted in a failure to understand the seriousness of the problem and the options available to law enforcement to respond.

The lack of state-of-the-art technology and an adequately trained, experienced workforce are two of the greatest challenges for law enforcement and prosecutors faced with investigating and trying cybercrime cases. The criminal justice system must become more sensitive to cyberstalking complaints, and the genuine threat that such stalking poses, and must devote the necessary training and resources to allow proper investigation and prosecution.

Ready Access

The only thing a cyberstalker needs is access to a computer and a modem. Due to the enormous amount of personal information available through the Internet, a cyberstalker can easily locate private information about a potential victim with a few mouse clicks or key strokes. Information is power, and stalking of any kind is all about power and control. There is little security on-line. Turning on a computer can expose anyone to harassment. Everyone who receives e-mail or uses the Internet is susceptible to cyberstalking.

Internet users are most vulnerable in cyberspace areas in which they interact with others. These include chat or Internet relay chat lines, message boards or newsgroups, where Internet users post messages back and forth, and users' e-mail boxes. E-mail harassment usually begins with initial contact in live chat or newsgroup situations.

Techniques

Cyberstalkers use a variety of techniques. They may initially use the Internet to identify and track their victims. They may then send unsolicited e-mail, including hate, obscene, or threatening mail. Live chat harassment abuses the victim directly or through electronic sabotage (for example, flooding the Internet chat channel to disrupt the victim's conversation). With newsgroups, the cyberstalker can create postings about the victim or start rumors that spread through the bulletin board system. Cyberstalkers may also set up a web page on the victim with personal or fictitious information or solicitations to readers. Another technique is to assume the victim's persona on-line, such as in chat rooms, for the purpose of sullying the victim's reputation, posting details about the victim, or soliciting unwanted contacts from others. More complex forms of harassment include mailbombs (mass messages that virtually shutdown the victim's e-mail system by clogging it), sending the victim computer virii, or sending electronic

junk mail (spamming). There is a clear difference between the annoyance of unsolicited e-mail and on-line harassment. Unsolicited e-mail is to be expected from time to time. However, cyberstalking is a course of conduct that takes place over a period of time and involves repeated, deliberate attempts to cause distress to the victim.

People who do not have access to the Internet, or who choose not to go on-line, are not immune from cyberbased crime. Databases of personal information available on the Internet can enable a stalker to trace a victim's user name to their real name, address, telephone number, and other personal information, or can enable a stalker to impersonate the victim on-line. The offender can then harass the victim on the computer via e-mail or at home through mail, telephone calls, or even by appearing at the victim's home or workplace. Telecommunication technologies also make it much easier for a cyberstalker to encourage third parties to harass and/or threaten a victim.

For example, in the first successful prosecution under California's new cyberstalking law, prosecutors in the Los Angeles District Attorney's Office obtained a guilty plea from a 50-year old former security guard who used the Internet to solicit the rape of a woman who rejected his romantic advances. The defendant terrorized his 28-year old victim, who had never been on-line and did not even own a computer, by impersonating her in various Internet chat rooms and on-line bulletin boards, where he posted, along with her phone number and address, messages that she fantasized about being raped. On at least six occasions, sometimes in the middle of the night, men knocked on the victim's door offering to rape her in response to the Internet "personal ad." The defendant pleaded guilty in April 1999 to one count of stalking and three counts of solicitation of sexual assault. As a result of the stalker's actions, the victim was eventually forced from her apartment, lost her job, suffered significant weight loss, and developed a fear of going outside of her residence.[4]

Most of the cyberstalking cases that have been prosecuted did not involve technically complex forms of stalking, and e-mail was simply being used as an alternative form of communication. However, this is not always the case. The availability of anonymizing software provides a high degree of protection for stalkers seeking to cover their tracks more effectively. Examples of these types of technologies are "anonymous re-mailers," which automatically shield the sender's identity with pseudonyms and send the e-mail through servers that instantly erase digital tracks to prevent later access by anyone, even law enforcement. Another example is *Stratfor's Shredder*, a software program for Windows 95 that acts like an electronic paper shredder that automatically overwrites deleted files, including all the routine computer backups.[5] The more complex software and computer technologies become, the easier it is for cyberstalkers to operate anonymously, and the more difficult it is for law enforcement to investigate and collect enough evidence to support prosecutions.

In order to address cyberstalking, it is critical to understand stalking in general. In many cases, cyberstalking is simply another phase in an overall stalking pattern, or it is regular stalking behavior using new technological tools. Therefore, strategies and interventions that have been developed to respond to off-line stalking can often be adapted to on-line stalking situations. There are federal, state, and local criminal justice agencies which have begun to focus on stalking, and some have recently developed special task forces to deal with cyberstalking.

Effects

As with all stalking, the greatest trauma is the faceless terror that it brings into a victim's life—24 hours a day, seven days a week. The Internet becomes an electronic curtain behind which the stalker hides while terrorizing the victim at home and work, with friends and neighbors, and with countless people that the victim does not even know. Cyberstalkers may be located on the other side of the world, across the country, across the street, or in the next cubicle at work. They could be a former friend or lover, a total stranger met in a chat room, or simply a teenager playing a practical joke. The inability to identify the source of the harassment or threats is one of the most ominous aspects of this crime for a cyberstalking victim.

The fact that cyberstalking does not involve physical contact may create the misperception that it is less threatening or dangerous than physical stalking. Cyberstalking is just as frightening and potentially dangerous as a stalker at the victim's front door. The psychological torment is very real, even in the absence of a distinct physical threat. It totally disrupts a victim's life and peace of mind. Cyberstalking presents a range of physical, emotional, and psychological trauma for the victim, who may begin to develop or experience:

- ❑ Sleep disturbances;
- ❑ Recurring nightmares;
- ❑ Eating pattern disturbances;
- ❑ Hypervigilance;
- ❑ High levels of stress;
- ❑ A feeling of being out of control; and/or
- ❑ A pervasive sense of the loss of personal safety.

Recent Responses

On January 10, 2000, in a keynote speech, U.S. Attorney General Janet Reno described the Internet and other information technologies as bringing enormous benefits to society, yet also providing new opportunities for criminal behavior. She proposed a round-the-clock cybercrime network of crime enforcement personnel, regional computer forensic laboratories to analyze seized computers for evidence of unlawful activity, and a secure on-line clearinghouse that would allow federal, state, and local law enforcement to share information about cybercases.[6]

As part of the 2000 *Violence Against Women Act*, Congress extended the federal interstate stalking statute to include cyberstalking, 18 U.S.C. §2261 A. In 2000, Congress also passed the *Amy Boyer's Law*, 42 U.S.C. Section 1320 B – 23 (P.L. 106 – 553), which prohibits the sale or display of an individual's social security number to the public, including sales over the Internet, without the person's expressed consent, submitted either electronically or in writing. The law allows a person harmed by wrongful release of a social security number to sue the seller or displayer for equitable relief and monetary damages in U.S. district court. In addition, the Social Security Commissioner can impose on any such violator a civil penalty of $5,000 for each violation, with increased penalties (maximum of $50,000) if the violations constitute a general

business practice. This new law applies to violations effective on December 21, 2002, two years after its enactment.

Amy Boyer's Law is named after a young woman who was murdered after her stalker purchased her social security number over the Internet. With that information, he was able to locate her license plate number and place of employment. He detailed his plans to kill her on a web site posted under her name. Within minutes of his last web site entry, he drove to her workplace and executed her as she got into her car.

States have also begun to respond to cyberstalking by adding provisions to their current stalking and harassment laws that criminalize "stalking by electronic means" or "the use of computer equipment for the purposes of stalking."[7] About half of the states currently have language in their laws that specifically address harassing electronic, computer, or e-mail communications. Other states' laws contain broad language that can be interpreted to encompass cyberstalking behavior. Some have statutes prohibiting harassment via computer contact, while others have stalking statutes that include electronic communications. A few have both stalking and harassment statutes that encompass electronic communications. Other states have laws, outside of stalking or harassment, that criminalize computer communications or e-mail misuse. Some have statutes that prohibit making threats through e-mail or "electronically submitted communications."

Resources

Victims of on-line harassment and threats, often in collaboration with victim service providers, have had to fill the void of available resources and assistance by developing their own informal support networks and informational web sites to share strategies about how to respond to these crimes. One such program is **Women Halting Online Abuse (WHOA)**, which was founded by women to educate the Internet community about on-line harassment. WHOA also educates the on-line community to develop web site resources, including the creation of a safe-site and unsafe-site list to enable Internet users to make informed decisions, and providing information about how users can protect themselves against on-line harassment.
You can contact WHOA at:

www.haltabuse.org
E-mail address: *whoa@femail.com; whoa@haltabuse.org*

Other on-line resources include:

CyberAngels: A nonprofit group devoted to assisting victims of on-line harassment and stalking.
www.cyberangels.org

Safety Ed International: A nonprofit organization assisting the Internet community and providing specific advice, resources, and information to victims being harassed or stalked on-line.

www.safetyed.org

Privacy Rights Clearinghouse: A nonprofit consumer and advocacy program that offers consumers a unique opportunity to learn how to protect their personal privacy. PRC's services include a hotline for consumers to report privacy abuses and to request information on ways to protect their privacy. They have also produced fact sheets on privacy issues including Factsheet # 14, entitled "Are You Being Stalked? Tips for Your Protection" and Factsheet # 18, entitled, "Privacy in Cyberspace."

www.privacyrights.org

Online Privacy Alliance: A coalition of more than 80 global companies and associations committed to promoting the privacy of individuals on-line. Its purpose is to define privacy policy for the new electronic medium and foster an on-line environment that respects consumer privacy. Available on this web site are resources for consumers, model Internet privacy policies, and news stories about recent on-line privacy violations and issues.

www.privacyalliance.com

Network Solutions' WHOIS: An Internet company which provides searches in its registrar database to assist persons in determining the contents of a domain name registration record found in the header of a received e-mail. The result will provide the contact information for sender's Internet service provider.

www.networksolutions.com/cgi-bin/whois/whois

Federal Trade Commission, Consumer Affairs Department: A resource site for consumer information from the federal government, including contact information if you have been the victim of identity theft or misuse of a social security number and fraudulent credit card accounts.

www.consumer.gov/idtheft
FTC hotline: 877-IDTHEFT
Social Security Number Fraud Line: 800-269-0271

Recommendations for Victims of On-line Stalking

If you are being harassed on-line, there are several things you should do:

1. If you are under 18, tell your parents or an adult you trust that you are being harassed or threatened. Do not keep this to yourself. Parents must know what is going on to be able to help and support you.

2. If you are getting harassing e-mail, get a new account or request a new log-on name and password from your Internet service provider. Close your old account. Learn how to use the filtering capabilities of your e-mail program to block e-mail from certain addresses.

3. Save every piece of communication you get from the cyberstalker. Save all of the header information you can if it's an e-mail or newsgroup posting. Print a hard copy, and copy the communication to a disk for documentation.

4. Start a log of each communication explaining the situation in more detail. Document how the harassment is affecting your life and what steps you're taking to stop it.

5. Once and only once, contact your harasser directly and state in simple, strong, and formal terms to stop contacting you and/or posting anything about you. State that the communications are unwanted and inappropriate, and that you will take further action if it does not stop. E-mail a copy to the system administrator of your Internet service provider. Save copies of these communications, and note that you sent them in your log.

6. If you receive harassing on-line messages and it is possible to trace the origin of the unwanted message and you have informed the sender that you do not want to be contacted, you may want to consider reporting the on-line stalker to the Internet service provider (ISP) because many ISPs have policies that prohibit the use of their services to harass or abuse another person. Some ISPs may be willing to cancel the stalker's account. If you receive abusive e-mail, identify the domain (letters after the @ sign) and contact the ISP. Most ISPs have an e-mail address such as *abuse@*[*domain name*] or *postmaster@*[*domain name*] that can be used for complaints. If that does not work, you can usually find contact addresses by going to *www.networksolutions.com/cgi-bin/whois/whois* (do a "who is" search on whatever ISP you need). If e-mail complaints don't work, make a phone call. Save copies of these communications, and note all contacts in your log.

   Keep in mind, however, that this may be just a short-term fix or may even exacerbate the situation if the stalker discovers that you notified the ISP. [Under those circumstances, he/she may attempt to retaliate against you or begin/continue to stalk you off-line. Regardless of whether the on-line stalking ceases, you need to be aware that the stalker may have obtained personal information on you via the Internet or through other sources, and, consequently, you may be still at risk for off-line stalking, in which case you need to do appropriate safety planning.]

7. Contact your local police. Report every incident of on-line abuse and provide the police with copies of evidence you have collected. Save copies of any police incident reports, and note each contact to law enforcement in your log. If the stalker is out of state, you should also contact your local office of the Federal Bureau of Investigation.

1. Call the FBI Computer Crimes Unit in your local area. [*The Federal Interstate Stalking and Prevention Act*, 18 U.S.C. Section 2261A, was amended in 2000 to cover on-line stalking as well as stalking by phone and mail. Also, some on-line stalking cases may fall under 18 U.S.C. Section 875, Interstate Communications (to make threats to physically harm or kidnap another person in interstate communications is a felony) or 47 U.S.C. Section 223, Obscene or Harassing Telephone Calls in Interstate Communications.]

In order to better protect yourself on-line:

1. Use a gender-neutral screen name.

2. Never give your password to anyone, especially if someone sends you an instant message (IM).

3. Don't provide your credit card number or other identifying information as proof of age to access or subscribe to a web site run by a company with which you are unfamiliar.

4. Tell children not give out their real name, address, or phone number over the Internet without permission.

5. Use a free e-mail account such as Hotmail (*www.hotmail.com*) or YAHOO! (*www.yahoo.com*) to pass messages in newsgroups, mailing listings, enter chat rooms, fill out forms, or correspond with someone you don't know well.

6. Don't give your primary e-mail address out to anyone you don't know.

7. Spend time on newsgroups, mailing lists, and chat rooms as a "silent" observer before "speaking" or posting messages.

8. When you do participate on-line, only type what you would say to someone in person.

9. Don't respond to e-mail from a stranger; when you reply, you are verifying your e-mail address to the sender.

10. On a regular basis (at least once a month), type your name into Internet search engines to see what information, if any, pops up. To have your name removed from any directories, contact each search engine on which you are listed and request to be removed.

(Tips #1 – 8 were developed by the George Mason University Sexual Assault Services, 1999.)

ENDNOTES

---

1. U.S. Department of Justice. (August 1999). *Cyberstalking: A New Challenge for Law Enforcement and Industry — A Report from the Attorney General to the Vice President*. Washington, D.C.: U.S. Department of Justice, pp. 2, 6.

2. Ibid., p. 8.

3. Ibid., p. 8.

4. *The Los Angeles Times*, 1/23/99.

5. Riveira, Diane. (September/October 2000). "Internet Crimes Against Women," *Sexual Assault Report*, 4(1), p. 14.

6. U.S. Department of Justice Press Release. (Released January 10, 2000). "Attorney General Reno Proposes New Steps to Fight Cybercrime." Washington, D.C.: U.S. Department of Justice.

7. Riveira, pp. 1 - 2.