# Global Information Assurance Certification Paper

# Cyberstalking: A Modern Dilemma

Shelli Patrick
GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4c, Option 1
January 23, 2005

## Abstract

Stalking via the Internet, or cyberstalking, is a form of harassment that occurs every day. The rapid development of the Internet, and ultimately new tools of harassment, caused the U.S. government to redefine the legal definition of stalking to include telecommunication devices as a source of stalking. This paper describes the typical cyberstalker, including the tools and motives of stalking, and the preventative measures one can follow to prevent becoming a cyberstalking victim. This paper also discusses the legal ramifications of cyberstalking and the existing laws to protect a victim. However, determined stalkers find new and better Internet tools every day to aid them in their cyberstalking crimes, making it nearly impossible for the law to keep up with the cyberstalker.

## What is Cyberstalking?

According to the model antistalking code drawn up by the U.S. government in 1989, the stalker is defined as “any person who willfully, maliciously and repeatedly follows or harasses another person in a course of conduct that makes a credible threat with the intent to place that person in reasonable fear of death or great bodily harm." [1] The introduction of the Internet produced a new type of criminal, the cyberstalker, and ultimately changed the model antistalking code to account for this unexpected crime. The cyberstalker can harass another person without even coming into physical proximity of that person by utilizing tools that developed from the advent of the Internet. The introduction of the Internet, however, did not change the motives for harassing. Stalkers and cyberstalkers alike share similarities in their motives for stalking.

## Types of Stalkers

Different reasons drive different people into stalking their victims. Stalkers and victims alike range in gender, age, social status, notoriety and wealth. Sometimes the stalker has never met the victim before, such as in cases of celebrity stalking. Other times, the stalker turns out to be an acquaintance. But most often the stalker has had a close relationship with the victim in the past. There is no single profile under which every stalker falls, however, typical stalkers are male while typical victims are female.

Whether the stalker is male or female, one typical goal persists among stalkers: becoming the most important aspect in the victim's life. This ultimate goal is the reason a stalker repeatedly harasses the victim, so that the latter is thinking about the former at all times. Whether an ex-boyfriend is jealous of a new love or a lonely person is looking for an object with which to keep the mind occupied, the reasons for stalking vary greatly in number and are hard to predict in most cases.

Along with the types of stalkers and their reasons for stalking, the outcomes

also vary greatly. Some stalkers seek to inflict bodily harm or worse, death. Others seek just to annoy the victim. Stalking varies greatly in every degree, from the types of stalkers to the ultimate outcome. The tool that stalkers have begun to utilize more in recent years is the Internet because it allows them to remain anonymous.

## Free Cyberstalking Tools

In the previous definition of stalking, “course of conduct" can further be defined as “repeatedly maintaining a visual or physical proximity to a person or repeatedly conveying verbal or written threats." [1] The Internet provides the easiest means of repeatedly sending written threats through electronic communications. The use of services on the Internet, such as anonymous re-mailers, provides untraceable anonymity to anyone. No special computer skills are required to use these tools, a fact which allows novice cyberstalkers ease in carrying out their cyberstalking activities. The following is a list and description of six types of harassment tools that cyberstalkers often utilize for free via the Internet.

### 1. Free E-mail Providers

E-mail providers such as Yahoo! and MSN Hotmail offer e-mail privileges at no cost. A cyberstalker can create numerous e-mail addresses, complete with harassing names, and send vulgar, unwanted e-mails to the victim. In response, the victim can contact the e-mail administrators to report the abuse of the e-mail. The administrators may shut down the cyberstalker's account; but since the e-mail is free, the cyberstalker can just create a new account and continue to harass the victim. In this case, the victim should make arrangements for a new e-mail address and only release this new contact information to individuals he or she can trust. However, a determined cyberstalker can probably engage in a bit of social engineering to find out the new e-mail address and, thus, continue to harass the victim at the new e-mail address. This cycle can continue endlessly unless the cyberstalker is caught.

### 2. Anonymous Re-mailers

An anonymous re-mailer is a service that allows someone to send an e-mail message without the receiver knowing the sender's identity. A re-mailer strips off the headers of the original e-mail and forwards it to the recipient with new headers. Some re-mailers act as anonymous middle men. The re-mailer gives users pseudonyms so that recipients can reply to messages without knowing the source of the e-mail message. The re-mailer then forwards the reply back to the owner of the pseudonym. Other re-mailers offer full anonymity and therefore cannot support replies. Re-mailers are used legitimately to provide a privacy buffer between the owner of the message and the public. [2] Dating services, such as Match.com, use these “double blind e-mail communications” to protect the identities of its members. [3] However, anonymous re-mailers also allow anybody to participate in criminal activity while concealing his or her identity.

Little can be done to protect oneself against the anonymous re-mailer. As with regular e-mail addresses, the best way to prevent re-mailer harassment from a cyberstalker is for the victim to change his or her e-mail address.

### 3. E-mail Bombs

An e-mail bomb is an “attempt to overwhelm an e-mail server or, more specifically, a single inbox, with so many messages that it becomes unusable.” [4] The e-mail bomb is basically a software program designed to send random text messages to a specified recipient. The cyberstalker uses the e-mail bomb to annoy the victim and potentially flood the victim's e-mail account to shut it down. Some e-mail bombs are capable of sending harassing e-mails at a rate of about 10 messages per second. The bomb usually uses anonymous servers so that the messages are difficult to trace. Some e-mail bombs even use multiple anonymous re-mailers in succession before the victim receives the e-mail to provide even more protection against the original source of the e-mail bomb.

One can do little to protect against the e-mail bomb. Again, victims can get a new e-mail address, but then will have to notify all of their contacts about the new e-mail address so they can continue their correspondence. Victims also can contact the technical support at their Internet Service Provider (ISP) to try to get some help. More often than not, the ISP will just assign a new e-mail address after minimal investigation.

### 4. Internet Chat

Many avenues of Internet chat exist today. Two of the more widely used chat services are AOL Instant Messenger and MSN Messenger Service, and they provide little security to protect against an unwanted chat session. A cyberstalker can send a message to the victim if the cyberstalker knows the victim's chat name. If the victim receives an unwanted message, he or she can block that person from sending any future messages. However, the cyberstalker can create a new chat name and continue to send unwanted messages to the victim. The victim has several options to stop the cyberstalker from future chat sessions, such as: changing his or her chat name so that the cyberstalker does not know the new name, blocking all incoming messages from any unknown chat names, or discontinuing the use of chat services. However, the option of no longer using chat services gives the cyberstalker a sense of accomplishment since the victim cannot continue with life in the way that he or she wants.

Another way in which the cyberstalker can abuse the use of chat services is by pretending to be the victim when chatting with another person. The cyberstalker can start a conversation with a random person and continue the conversation until it gets deep and personal. The cyberstalker may then give that person the victim's phone number and prompt that person to call so they can continue the conversation in a more personal manner. In this case, the cyberstalker does not directly contact the victim, but prompts another person to do so. This outsider will unwittingly call the victim thinking that he is calling the person with whom he

has been chatting. One way the victim can stop the cyberstalker in this case is by changing telephone numbers and then giving the new contact information to individuals the victim trusts.

### 5. Message Boards

A message board allows an Internet user to post a message on a Web site for other Internet users to read and to reply with another message. Message boards exist all over the Internet and are used for a variety of reasons. Some are classified ads looking to sell or buy items; others are simple messages as a way to keep in touch with people. A cyberstalker can indirectly harass a victim by posting contact information and vulgar, false messages about the victim on message boards throughout the Internet. The message can prompt other readers to contact the unknowing victim, who can do little about the posting of false messages. The victim can contact the owner of the message board and request that the false message be removed from the Web site. But if users of the message board already have the victim's contact information, then the victim will need to change e-mail addresses or telephone numbers, or both, to prevent any future unwanted communication.

### 6. Phishing

A cyberstalker also seeks to harass the victim by gaining access to personal account information including credit card numbers and passwords. One method of gaining this type of information is through phishing. According to the Anti-Phishing Working Group Web site, “phishing attacks use 'spoofed' e-mails and fraudulent Web sites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc.” [5] The first phishing incident was recorded in September of 2003 by an individual trying to obtain illegal access to a bank account. A cyberstalker can use these same phishing techniques to gain access to a victim’s e-mail account and ultimately, contact information of friends and family members to broaden the circle of harassment. All Internet users, not just victims of cyberstalking, can only prevent this phishing attack by being aware of its existence. Users should not respond directly to e-mails from their bank or credit card companies, but should type the Web address directly into the browser to access those Web sites.

## Purchased Cyberstalking Tools

The tools listed above are widely available on the Internet and can be found easily with a quick search. The Internet provides an ever-increasing number of tools to help the cyberstalker carry out his or her cyberstalking activities. For more serious harassers willing to invest their money, cyberstalkers can terrorize their victims in even different ways:

- Hackers on the Internet have learned how to obtain passwords for e-mail providers such as Yahoo! and MSN Hotmail that provide e-mail to their customers for free. One such service, known as E-mail Surveillance

Services (ESS), does not charge a flat rate for services provided and will "attempt to gain access to an e-mail account for valid reasons." [6] The disclaimer on the Web site also indicates that "any illegal use of this service will be reported to the proper authorities." [6] A cyberstalker who is determined enough to obtain the password of the victim can probably be smart enough to submit a reason that looks valid in the eyes of a service like ESS. After the cyberstalker receives and changes the password to the victim's e-mail account, victims can find themselves locked out of their own e-mail accounts.

- Twenty dollars is not a steep price for a determined cyberstalker to pay to find out the physical address or phone number of his or her victim. By purchasing a background check on the victim, the cyberstalker can obtain this information by posing as an employer inquiring information about a possible new hire. Knowing that kind of personal information about the victim will make the cyberstalker feel like he or she has even more power over the victim.
- Cyberstalkers also can seek to terrorize the victim by purchasing a domain name in the victim's name and creating a mock, personal Web site about the victim. Many domain name hosts have restrictions on their naming conventions, but there are limitations to those restrictions. For instance, a naming program might have the rule that a domain name cannot contain a vulgar word. However, by separating a single word with underscores or dashes – for example, w_o_r_d – the domain name can contain a vulgar word spelled out and thus, the naming convention has been violated. The domain name dispute law, known as Anticybersquatting Consumer Protection Act enacted in November of 1999, is "intended to give trademark and service mark owners legal remedies against defendants who obtain domain names "in bad faith" that are identical or confusingly similar to a trademark or service mark." [7] This essentially makes it illegal for a person to obtain a domain name of a well-known product, e.g. McDonalds or Coca-Cola, and attempt to profit from it either by selling the domain name back to the owners of the product or by some other means. This law does not address the issue of domain names in "bad faith" that include a person's name in the domain name. When this law was enacted, a study was requested by Congress for research and recommendations regarding legislation for disputes using domain names involving personal names. In a report dated January of 2001, The Department of Commerce stated "there is insufficient evidence as of this date to suggest that personal name holders lack redress when their names are abusively registered as Internet domain names." [8] Thus, no laws regulate the use of abusive domain names involving personal names.

The tools listed above, both those that are free and those that are available for purchase, offer the cyberstalker many choices in carrying out his or her cyberstalking activities. These lists are by no means comprehensive, as new

tools are being developed every day, and even existing tools are being used in new, abusive ways. The Internet makes these tools widely available at a minimal cost.

## Preventative Measures

Once the victim knows the techniques that a cyberstalker uses, he or she can prevent cyberstalking from occurring, or at least lessen the effects once the cyberstalking starts. The potential victim should use a search engine on the Internet to determine all the various Web sites that may contain personal information about the victim.

The victim should also research any organization or company to which the victim belongs to find out if any member lists are posted on the Internet. These lists often contain contact information of all members of the organization. For instance, universities must comply with the U.S. Department of Education's Family Educational Rights and Privacy Act of 1974, which allows personal information about students to be viewed publicly unless the student desires to withhold any information:

> Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. [9]

The student must fill out and submit a form requesting the information be withheld from the directory. Even if the potential victim is not a student, he or she should contact all organizations that post personal contact information on the Internet and ask them to remove the listing from the public view. If a cyberstalker has access to this public information, he or she can use it to his or her advantage unless the victim takes the appropriate measures to be removed from personal listings.

Organization or company lists are not the only places that a person's name can appear on the Internet. Friends and family members also may have posted information about the victim on their personal Web sites. This type of information gives the cyberstalker even more personal information than a background check would. To help prevent any potential cyberstalkers from gaining this personal information, the potential victim should ask the owners of the Web sites to remove all mention of the potential victim.

## Antistalking Laws

Until 1989, no laws were in place to protect victims of stalking. Even then, a large gap in the laws prevented any legal action against a potential stalker until the stalker physically took action against the victim. After much pressure from

the public, the federal government developed an antistalking code which the states were to use to model their state antistalking laws. At that time, stalking was usually a local problem and therefore did not fall under the scope of the federal government. Within five years of developing the code, all 50 states had antistalking laws in place, each of varying degrees. Therefore, “no single legal definition of stalking exists and there is considerable variation in the application and sanctions of laws in each U.S. state." [10] Some of the states require proof of “credible threat," as mentioned previously in the definition of stalking. Some states even require proof of emotional distress to the victim before any action can take place against the stalker. Therefore, if the stalker's goal is to simply annoy the victim, no legal action can be used against the stalker unless the stalker takes physical action against the victim.

One federal law protects victims of stalking by making it illegal to convey threatening comments across state boundaries: Title 18, Part 1, Chapter 41, Section 875 of the U.S. Code makes it a federal crime to “transmit in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another.” [11] This law was passed in 1934. The first person charged under this law in relation to cyberstalking was Jake Baker, a student at the University of Michigan, in January of 1995. Baker posted a story on an online message board that described in detail the rape, torture and murder of a woman with the same name as one of his fellow classmates. He also communicated this story via e-mail to a man in Ontario, Canada, by the name of Arthur Gonda. Because Baker’s story described a threatening act against another person, he was arrested and charged with violation of Section 875. Baker’s attorneys argued that the private e-mail correspondence between Baker and Gonda was protected under the First Amendment, which allows free speech. However, the First Amendment does not protect the right of free speech when true threats are communicated. Charges were ultimately dropped against Baker because prosecutors could not prove that Baker communicated a “true threat” with the intent of carrying out the crime detailed in the story. Even the 6th Circuit Court of Appeals upheld the dismissal of the charges against Baker, ruling that the e-mail messages did not constitute a credible threat. [12]

The United States v. Baker case in 1995 proved that the law had limitations in its anti-cyberstalking legislation, especially if the intent of the cyberstalker is simply to annoy the victim rather than physically threaten the victim.

In 1996, the U.S. government passed the Interstate Stalking Punishment and Prevention Act. This law indicates the following:

> Whoever travels in interstate or foreign commerce … with the intent to kill, injure, harass, or intimidate another person, and in the course of, or as a result of, such travel places that person in reasonable fear of the death of, or serious bodily injury to, that person, a member of the immediate family of that person, or the spouse or intimate partner of that person … shall be punished. [13]

This law essentially makes it illegal for stalkers to cross state lines to carry out their stalking activities. However, this still does not address the issue of the cyberstalker who can carry out cyberstalking activities against a victim regardless of the states in which they both reside.

The Telecommunications Act of 1996 did address the issue of the cyberstalker when it proposed a change in the Communications Act of 1934 from the words "interstate or foreign communications by means of a telephone" to the words "by means of a telecommunications device". This Act makes it illegal for anyone to use a telecommunications device to initiate the transmission of "any comment, request, suggestion, proposal, image, or other communication which is obscene, lewd, lascivious, filthy, or indecent, with intent to annoy, abuse, threaten, or harass another person," [13] regardless of state boundaries.

Though the Telecommunications Act was signed into law in February of 1996, more than eight years passed before the first person was charged with this federal crime when in April of 2004 cyberstalker Robert James Murphy was charged with "26 accounts of using his computer to 'annoy, abuse, threaten and harass'" Seattle resident Joelle Ligon. [14] The two had not seen each other in 13 years after their seven year relationship had ended. Murphy began harassing Ligon in 1998 when he sent harassing e-mail messages and faxes to Ligon and her coworkers. He continued to do so as she moved to different jobs and even as she moved to different states. In 2002 Ligon began saving the harassing messages for evidence and eventually went to the police. In October of 2004, South Carolina resident Robert James Murphy, pleaded guilty to two accounts of cyberstalking and received five years of probation, 500 hours of community service and more than $12,000 in restitution to the City of Seattle "to compensate for work time lost by employees dealing with the harassment." [15, 16]

Ligon had to endure almost six years as a victim of cyberstalking before the law enforcement caught up with technology. Ligon had no legal right to prosecute Murphy under the Interstate Stalking Punishment and Prevention Act of 1996 since he did not physically cross state borders to carry out his cyberstalking activities. The Telecommunications Act of 1996 at that time was not well known and there was no precedent in a case like this. Also, the Sate of Washington did not include cyberstalking in its state anti-stalking legislation. Ligon's lobbying efforts paid off in March of 2004 when Washington's state anti-stalking laws were amended to include cyberstalking. Ultimately, Murphy was arrested for violation of the Telecommunications Act after the FBI took a role in the investigation that proved Murphy was the actual cyberstalker. [17] This case is indicative of the typical qualities of stalking: the victim is female and knows her male harasser from a prior relationship.

## Conclusion

Although the motives are often similar, stalkers are discovering new ways to pester their victims. Cyberstalking is a new phenomenon of harassment that only recently has begun to be regulated by the U.S. government. The emergence of the Internet into mainstream society during the last decade has caused the federal system to step up its intervention into the cyberspace realm. Court cases, such as United States v. Baker, and the charges brought up against Robert James Murphy have shown that steps are slowly being taken to alter laws with the goal of preventing cyberstalking, but determined stalkers continue to find new Internet tools every day to hassle their victims.

## References

[1] Domestic Violence, Stalking, and Antistalking Legislation. 1996. U.S. Department of Justice. 3 January 2005. <http://www.ojp.usdoj.gov/ocpa/94Guides/DomViol/appendb.htm>.

[2] Bacard, Andre`. "Anonymous Re-mailer FAQ" November 2003. Jan. 2005. <http://www.andrebacard.com/re-mail.html>.

[3] "Privacy Statement". 2003. Match.com, L.P. 31 December 2004. <http://www.match.com/registration/privacystatement.aspx>.

[4] "E-mail Bombs". 2002. Moon & Back Graphics. 8 January 2005. <http://www.leave-me-alone.com/hackers_e-mailbombs.htm>.

[5] Anti-Phishing Working Group Home Page. 2005. Anti-Phishing Working Group. 2 January 2005 <http://www.antiphishing.org>.

[6] E-mail Surveillance Services Home Page. 2004. E-mail Surveillance Services. 7 January 2005. <http://www.esurveillance.info>.

[7] "Domain Name Disputes: FAQ: The Anticybersquatting Consumer Protection Act ." 20 April 2001. Keyt Law. 13 January 2005. <http://www.keytlaw.com/urls/acpa.htm>.

[8] Report to Congress: The Anticybersquatting Consumer Protection Act of 1999, section 3006 concerning the abusive registration of domain names. 21 January 2001. United States Patent and Trademark Office. 13 January 2005. <http://www.uspto.gov/web/offices/dcom/olia/tmcybpiracy/repcongress.pdf>.

[9] Family Educational Rights and Privacy Act (FERPA). 1974. U.S. Department of Education. 4 January 2005 <http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>.

[10] Mullen, P., M. Pathe and R. Purcell. Stalkers and their Victims, Cambridge: University Press, 2000.

[11] "875. Interstate communications." 6 August 2004. Legal Information Institute. 14 January 2005. <http://assembler.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00000875----000-.html>.

[12] Swanson, Peter. "Timeline of Events in Baker Case". 29 January 1996. 15 January 2005. <http://www.mit.edu:8001/activities/safe/safe/cases/umich-baker-story/Baker/timeline.html>.

[13] Title 18. Crimes and Criminal Procedure: Part I – Crimes: Chapter 110A – Domestic Violence and Stalking. January 2003. U.S. Department of Justice. 7 January 2005. <http://www.usdoj.gov/criminal/cybercrime/2261ANEW.htm>.

[14] Associated Press. "Man pleads innocent to Internet stalking." USA Today. 23 April 2004. 10 January 2005. <http://www.usatoday.com/tech/news/techpolicy/2004-04-23-cyberstalking-inocent-plea_x.htm>.

[15] Associated Press. "Man gets probation after admitting to Net stalking." USA Today. 29 October 2004. 10 January 2005. <http://www.usatoday.com/tech/news/internetprivacy/2004-10-29-net-stalker-chided_x.htm>.

[16] “South Caroline Man Sentenced in First Federal Prosecution of Internet Harassment”. 29 October 2004. United States Attorney’s Office: Press Room. 12 January 2005. <http://www.usdoj.gov/usao/waw/press_room/2004/oct/murphy.htm>.

[17] Shukovsky, Paul. “FBI arrests suspect in cyberstalking”. 10 April 2004. Seattle Post-Intelligencer. 11 January 2005. <http://seattlepi.nwsource.com/local/168567_cyberstalker10.html>.

Additional Reading Material:

Davis, Joseph A., ed. Stalking Crimes and Victim Protection. Boca Raton: CRC Press, 2001.

Thomas, D. and B. D. Loader, eds. Cybercrime. London: Routledge, 2000.

Mackaay, E., D. Poulin, and P. Trudel, eds. The Electronic Superhighway. The Hauge: Kluwer Law International, 1995.

Stephenson, Peter. Investigating Computer-Related Crime. Boca Raton: CRC Press, 2000.