CONTACT:
Research Section
5000 NASA Blvd., Suite 2400
Fairmont, WV 26554
Ph: 877-628-7674
Fax: 304-368-2359
Web: www.nw3c.org

Cyberstalking (March 2015)

Cyberstalking is the online version of and is often an extension of offline stalking.[1] There is some debate about exactly what behaviors constitute as cyberstalking; however, a common definition is "an escalated form of online harassment directed at a specific person that causes substantial emotional distress and serves no legitimate purpose. The action is to annoy, alarm, and emotionally abuse another person."[2] Perpetrators utilize social media accounts, publicly accessible information and sometimes illegally accessed information to learn more about their targets. The perpetrators may also spread rumors and misinformation to discredit or intimidate them. Regardless of the methods used, cyberstalking is an online crime that disrupts lives, instills fear, and if taken offline may result in physical violence to the targeted victim.[3]

The growth of the Internet, a multitude of social media websites, and the proliferation of information available online creates new arenas that cyberstalkers use to hunt and terrorize their victims. Those new arenas combined with advancements in technology that allow individuals to access social media accounts and the Internet at large from any location, lead to a situation in which victims of cyberstalking may experience constant bullying and/or harassment.[4]

Cyberstalkers may obtain personal information about their victims (e.g., home address, phone number) from the Internet and utilize this information to meet their victims in person. They can use any of a number of methods available online to assist them in their endeavors, including downloading keystroke logger software to capture the information necessary to obtain private information from their intended victim and using social media to monitor and/or harass their victims. While their techniques are similar to those used for the identity theft the main goal of cyberstalking is not financial. The intent is to do damage, harass, intimidate, or otherwise harm the target of their actions, which may be accomplished via identity theft. The Center for Domestic Violence drives home the connection with and difference from identity theft by noting, "Cyberstalking is not identity theft. An identity thief, whether stealing from a stranger or a family member, has a very specific goal in mind — financial gain. Identity thieves are unconcerned by the consequences of their behavior on the victim's life, whereas the actions of a cyberstalker are deliberate and focused on the consequences to the victim".[5]

While instances of cyberstalking have increased over the years, it is still difficult for law enforcement to track and prosecute perpetrators. First, victims may not report their experiences to law enforcement or similar support agencies. Second, since the last recession, many law enforcement offices experienced plummeting budgets, loss of personnel, and a lack of training on how to investigate crimes that occur online. Third, the majority of anti-stalking laws stipulate that the alleged stalker must make a "credible threat(s) against the victim or the victim's immediate family" to be eligible for prosecution.[6] Finally, because this crime occurs online, often the perpetrator is not physically near their victim and is sometimes across the country or located in another country. Regardless of how disturbing or threatening their behavior is, it is difficult for law enforcement to prove the stalker is a "credible threat" if they are not in close

proximity to their victim. Investigating and prosecuting cyberstalking cases may also be difficult due to differing laws for handling alleged cyberstalkers in other countries.[7]

How It Happens

Put simply, Cyberstalking is a form of harassment that takes advantage of the anonymity and relative protection the Internet provides from law enforcement. Marian Merritt of Norton explains, "…harassment can take on many forms, but the common denominator is that it's unwanted, often obsessive, and usually illegal."[8] Online harassment ranges from annoying to deadly. The following is a list of actions that cyberstalkers use to abuse their victims. Keep in mind that these actions alone or in some combination do not necessarily constitute cyberstalking; rather cyberstalking is more often a combination of these actions in conjunction with repeated behaviors specifically intended to intimidate or harm a person.

- Leaving messages or comments on an individual's online post, publication, web blog, or website with the intent to threaten, harass, or cause emotional distress.
- Sending online correspondence that is inappropriate and unwanted.
- Posing as another person and posting material online using that person's name or likeness.
- Creating online material (including websites, blogs, and social media pages) with the name and/or likeness of another person in order to disseminate false and defamatory information or pictures.
- Purposefully sending malware or computer viruses to a specific person as a means to harass them or compromise their computer's security.
- Employing spyware on an individual's computer or other electronic devices in order to track their movements, the information they access, and who they interact with online.
- Hacking an individual's computer.
- Sending defamatory and/or harassing messages to an individual's friends, family, employer, coworkers, neighbors, students, teachers, or other community members either in their name or the victim's name.[9]

Victims have criminal and civil legal recourse with the enactment of anti-stalking legislation in all 50 states and U.S territories.[10] The National Conference of State Legislatures' website, www.ncsl.org, lists states cyberstalking and/or cyberharassment laws for all 50 states and Guam.[11] Also, victims can sue for injuries, including defamation, pain and suffering, and lost income. Perpetrators may be forced to pay civil penalties.

Statistics

While not exclusively about cyberstalking, a 2009 stalking victimization study by the Bureau of Justice Statistics and the National Institute of Justice did measure some aspects of cyberstalking. Namely, it measured how many victims receive "unsolicited or unwanted letters or e-mails", and how often a stalkers actions include "posting information or spreading rumors about the victim on the Internet, in a public place, or by word of mouth.[12] This study employed data from the

National Crime Victimization Survey, specifically its Supplemental Victimization Survey (SVS). Based on this data researchers estimate that 5.3 million U.S. residents 18 years of age or older were stalked or harassed in the year prior to the SVS interview process. Of that number, 1.5 percent of those people were victims of stalking which was defined in this study as "repetitive behaviors associated with stalking in addition to feeling fear or experiencing behaviors that would cause a reasonable person to feel fear."[13] Individuals in online environments also experience harassment, typically seen as separate from stalking, from both known persons and strangers. For the purposes of this study, victims of harassment were signified as experiencing "behaviors associated with stalking but neither reported feeling fear as a result of such conduct nor experienced actions that would cause a reasonable person to feel fear."[14]

The SVS data also showed:

- Almost 1/3 of stalking victims are divorced or separated, a higher percentage than those who are married, never married, or widowed.
- 70% of stalking victims knew the person stalking them.
- Females are more likely to be victims of stalking than males.
- Males and females experience harassment at the same rate.
- Of those individuals who reported being stalked, almost 40% said it lasted for six months or less.[15]

There is little recent research that specifically discusses victims of cyberstalking detached from instances of traditional stalking. One academic attempt comes from the University of Bedfordshire's National Centre for Cyberstalking Research (NCCR). The Centre's first major research project culminated in the Electronic Communications Harassment Observation (ECHO) 2011 report.[16] For this study, the NCCR defines cyberstalking as "a course of action that involves more than one incident perpetrated through or utilising electronic means, that causes distress, fear or alarm." Because there is not a common definition of cyberstalking in the United Kingdom (or anywhere else), the researchers chose to ask the respondents about exposure to harassment, how that harassment occurred, and what feelings the victims experienced. The researches then used the above definition of cyberstalking to identify data by those individuals who reported experiencing specific kinds of harassment and feelings; specifically fear.[17]

The NCCR data showed:

- 92% of respondents reported experiencing cyberharassment.
- 94% of the respondents were female and 87% were male.
- 81% of respondents were between 20 – 49 years of age.
- The largest age group, 30 – 39 years of age, represented 1/3 of respondents.
- 94% of those who reported an experience of cyberharassment also reported feeling distress in relation to that harassment. 81% reported they experienced fear.
- Females were more likely to experience both distress and fear than males.

- 24% reported feeling "primarily afraid of personal physical injury," and almost twice the number of females than males reported being afraid of personal physical injury.
- Females were more concerned than males that their harasser would harm their family, colleagues, or pets.
- About 1/3 of respondents noted they were afraid of "damage to their reputation," with almost 50% of male respondents indicating they feared "damage to their reputation." About 25% of females indicated the same fear.
- Males were about twice as likely as females to fear a financial loss.[18]

The Pew Research Center's Internet Project researchers also conducted a survey on cyberharassment. Like other similar surveys, few questions distinctly refer cyberstalking, but some aspects of their questions may also represent instances of cyberstalking. Harassment is typically defined as behaviors directed at an individual with the intent to consistently bother them and create a hostile and/or uncomfortable environment. For this study the researchers qualify the following common behaviors as harassment in an online environment: embarrassing someone, physically threatening someone, sexually harassing someone, stalking someone, harassing someone over a long period of time.[19]

Pew's data showed:

- Of respondents who indicated they witnessed another person experiencing harassment online, 24% reported seeing "someone being harassed for a sustained period of time and 18% reported seeing someone being stalked.
- Of those who reported experiencing online harassment, 8% reported being stalked and 7% reported being "harassed for a sustained period."
- More men than women reported experiencing sustained periods of harassment, and more women than men reported being stalked.
- 27% of respondents described the harassment experience as either very or extremely upsetting.
- 38% of women and 17% of men reported feeling very or extremely upset by an online harassment experience.[20]

For Victims

It is important to note that those experiencing cyberharassment or cyberstalking are victims of a crime and it is not the result of their actions, beliefs, or physicality. Victims do not cause cyberharassment or cyberstalking rather; a perpetrator commits cyberharassment and cyberstalking. Victims and their families have options for legal recourse.

- **Learn about and use privacy settings**. Each social media platform has unique privacy setting. For example, some platforms allow users to tailor who may see their profiles and the extent to which another person can see their information. Become familiar with the privacy policy for each of the platforms used.
- **If available, use a two-factor or double authentication security option.** Two-factor authentication options ask the user to supply a second form of authentication when

accessing a social media or other online account. This requires a user to enter a username and password, then supply another piece of predetermined information to access the account. The second authentication options may require the user to answer a question about the user or the account or provide a special code sent to a device (phone) or email associated with the account.

- **Carefully consider the personal information supplied on public accounts**. Hometown, current city, birth date, email address, phone number, names of family members, schools attended, places of employment, and personal pictures are bits of information someone can use to obtain other publically available information about a person. That information can include the existence of arrest or prison records, businesses owned, residences, vehicles owned, past employers, current salary, and places frequently visited. Sharing hobbies or interests such as movies, television shows, music, places, etc. can provide cyberstalkers with information they can use to obtain more information that is personal.
- **Do not be "friends" with or accept "follower requests" from people not personally known**. The user should note on the publically viewable profile that the user does not accept association requests from people he or she does not personally know. Also, note that requestors should include a message outlining who they are and how they know the user with the request. Do not reply to requests from individuals not personally known, especially via personal email or phone. If an association request is received from someone unknown to the user, they may contact them using the platform's messaging application and ask the requestor to verify a personal connection.
- **Tell friends not to post your personal information (even pictures) without your permission**. Many people do not grasp the amount of personally identifiable information given out when they share about another's life online. Tell friends, both online and offline, not to share personal information about another's life, and then remind them occasionally.
- **DO NOT publically share pictures or other identifying information about your children or other close family members.** The saying a picture is worth a thousand words is true. A cute picture of a child's first day at school or a spouse's running meet is full of information about the places an individual's family members frequent. This includes where the child goes to school, the parks and movie theaters visited, and locations where family members work and play. In addition, one can unwittingly share information about another person's child when sharing one's own pictures. Before posting any personal images, make certain that those in the picture give permission to post their image online.
- **Leave all those online quizzes and polls alone.** Yes, those "what kind of _____ am I?" quizzes are fun, but many of them are a means for companies or individuals to collect personal information.
- **Do not publically RSVP to events.** On some social media platforms events are sometimes public and others can see when someone accepts an invitation. Even the semi-public event pages allow the "friends" of those invited to view the list of those attending.
- **Pay attention to the information disseminated by electronic devices.** On some social media platforms if the privacy settings are not set correctly, the public can see any updates posted from electronic devices (phone, tablet, etc).

- **Use strong and different passwords for each online account.** It is difficult to remember many passwords, but it is important for general security online security, and especially for victims of a cyberstalker. Make passwords strong, unique. Be sure change them every few months.[21]

Failure to follow these suggested actions do not cause cyberstalking; people who stalk others cause cyberstalking. These tips are not the sole remedy to any incident of stalking; if you think or know someone is stalking you or if a person online has threatened you or given you cause for fear of harm, then contact your local authorities and file a report. Make it known what is happening to you and seek out support from law enforcement, friends, and family. You are not alone and there law enforcement personnel, counselors, and organizations who will help victims of cyberstalking.

For Law Enforcement

Knowing that it may be difficult to track and prosecute alleged cyberstalker, there are a few suggestions to help aid those investigations.

The following tips are points of consideration in deciding how or if to proceed.

- Identify the type of message received and if it is an actual threat from a known individual. There are types of SPAM[1] emails sent out en masse with insincere threats of exposing the recipient of the email as an inadvertent or purposeful perpetrator of a crime. These threats typically accuse the recipient and demand payment for the sender's continued silence. Another version of this type of SPAM threat is when a perpetrator portrays themselves as a hit man that a third party hired to kill the recipient. The sender "offers" the recipient the opportunity to pay the hit man directly and avoid any action taken on their life or the lives of their immediate family members. For more information visit: http://www.fbi.gov/news/stories/2007/january/threatscam_111507. [22] If the message is SPAM, then the recipient may send a complaint to the spammer's Internet Service Provider or ISP, and the Internet Crime Complaint Center (IC3) at http://www.ic3.gov.
- Encourage the recipient of a threat to reply once to say that the sender's correspondence is not wanted and that they want the messages to stop. After that initial response, regardless of what the reply from the original sender, do not engage them further. [23]

The following steps are a guide for law enforcement officials when first tasked with investigating an incident of cyberstalking.

[1] Defined by the Internet Crime Complaint Center (IC3) as "unsolicited bulk email" that is most often "multiple identical messages sent simultaneously" to a great number of email addresses. IC3 warns that SPAM may also be a "vehicle for accessing computers and servers without authorization and transmitting viruses and botnets. The subjects masterminding this Spam often provide hosting services and sell open proxy information, credit card information, and email lists illegally." "Internet Crime Schemes." *Internet Crime Complaint Center (IC3)*. Web. 25 Feb. 2015. http://www.ic3.gov/crimeschemes.aspx#item-17.

- As with any other investigation, one should collect all information associated with the incident(s) including but not limited to a description of what occurred, contact information of all those involved, a list of all the arenas (social media websites, blogs, etc.) the cyberstalking took or continues to take place.
- Do not make assumptions about a relationship between the alleged perpetrator and the victims. Victims often know their stalkers (either online or offline), but sometimes they do not know who is stalking them or why. Make a special effort to ensure the victim (and others involved) hears you say that what is occurring is not their fault. This is occurring because someone decided to commit a crime against them and not because of their behavior.
- When victims are interviewed, make sure to confirm that a crime was committed against them or one of their family members. Interview any potential witnesses including individuals that know the victims or perpetrators in both online and offline arenas.
- If the stalking is ongoing, direct the victims to document any and all attempts the perpetrators makes to contact them, their family members, or other individuals associated with the victims. Sometimes cyberstalkers will impersonate their victims or send defamatory information to family members, coworkers, church leaders, and anyone else who know the victims personally.
- Assess why the perpetrators chose to cyberstalk the victims and determine the risk level to the victims and their family members. What is the motivation of the cyberstalker?
- Determine and assess where incidents of stalking take place online. Which online spaces do the perpetrators inhabit? In what online spaces do the crimes take place?[24]

Real Life Cyberstalking Stories

- *Busting a Cyberstalker: How Carla Franklin Fought Back – and Triumphed* - http://www.thedailybeast.com/articles/2012/10/12/busting-a-cyberstalker-how-carla-franklin-fought-back.html.
- *How the Law is Standing Up to Cyberstalking* - http://www.newsweek.com/2014/08/22/how-law-standing-cyberstalking-264251.html.
- *"I Was a Victim of Cyberstalking" – One Woman's Story* - http://womensissues.about.com/od/violenceagainstwomen/a/CyberstalkStory.htm.

"For More Information" Links

CyberAngels.org - http://www.cyberangels.org

WiredSafety.org - https://www.wiredsafety.org

National Center for Victims of Crime - http://www.victimsofcrime.org/our-programs/

Privacy Rights Clearinghouse - http://www.privacyrights.org/

U.S. Department of Justice - http://www.justice.gov/

Working to Halt Online Abuse - http://www.haltabuse.org/index.shtml

Cyberstalking Investigation and Prevention - http://www.crime-research.org/library/Cyberstalking.htm

National Network To End Domestic Violence – Safety Net Project - http://nnedv.org/projects/safetynet.html

Maintenance and Revisions maintained by the NW3C Research Section

This project was supported by Grant No. 2012-MU-BX-4004 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Endnotes

[1] Parsons-Pollard, Nicolle, and Laura J. Moriarty. "Cyberstalking: Utilizing What We Do Know." *Victims & Offenders: An International Journal of Evidence-based Research, Policy, and Practice* 4.4 (2009): 435-41. Print.
[2] J. A. Hitchcock, "Cyberstalking and Law Enforcement," *The Police Chief* 70 (December 2003): 16–27.
[3] Sheridan, L. P., and T. Grant. "Is Cyberstalking Different?" *Psychology, Crime & Law* 13.6 (2007): 627-40. Print.
[4] Pittaro, Michael L. "Cyber Stalking: An Analysis of Online Harassment and Intimidation." *International Journal of Cyber Criminology* 1.2 (2007): 180-97. *International Journal of Cyber Criminology*. Web. <http://www.cybercrimejournal.com/pittaroijccvol1is2.htm>.
[5] What is Cyberstalking?; Retrieved from http://womensissues.about.com/od/violenceagainstwomen/f/Cyberstalking.htm. July 1, 2013
[6] J. A. Hitchcock, "Cyberstalking and Law Enforcement," *The Police Chief* 70 (December 2003): 16–27.
[7] Quarmby, Katharine. "How the Law Is Standing Up to Cyberstalking." *Newsweek* 13 Aug. 2014. Print.
[8] Straight Talk About cyberstalking. Retrieved from http://us.norton.com/cyberstalking/article July 1, 2013
[9] J. A. Hitchcock, "Cyberstalking and Law Enforcement," *The Police Chief* 70 (December 2003): 16–27.
[10] Privacyrights.org. (2013). Fact Sheet 14: Are You Being Stalked? Retrieved February 12, 2013, from https://www.privacyrights.org/fs/fs14-stk.htm#3.
[11] "State Cyberstalking And Cyberharassment Laws." *Cyberstalking and Cyberharassment Laws*. 5 Dec. 2013. Web. 21 Nov. 2014. <http://www.ncsl.org/research/telecommunications-and-information-technology/cyberstalking-and-cyberharassment-laws.aspx>.
[12] Catalano, Shannan. "Stalking Victims in the United - Revised." *U.S. Department of Justice*. 1 Sept. 2012. Web. 8 Dec. 2014. http://www.bjs.gov/content/pub/pdf/svus_rev.pdf.
[13] Ibid
[14] Ibid
[15] Ibid
[16] "The National Centre for Cyberstalking Research." *University of Bedfordshire*. Web. 8 Dec. 2014. http://www.beds.ac.uk/research-ref/irac/nccr/echo.
[17] "Cyberstalking in the United Kingdom An Analysis of the ECHO Pilot Survey." National Centre for Cyberstalking Research. Web. 8 Dec. 2014. <http://www.beds.ac.uk/__data/assets/pdf_file/0003/83109/ECHO_Pilot_Final.pdf>.
[18] Ibid
[19] Ibid
[20] Duggan, Maeve. "Online Harassment." *Pew Research Centers Internet American Life Project RSS*. Pew Research Center, 22 Oct. 2014. Web. 8 Dec. 2014. http://www.pewinternet.org/2014/10/22/online-harassment/.
[21] "Fact Sheet 14: Are You Being Stalked?" *Are You Being Stalked?* Privacy Rights Clearinghouse, 1 July 2014. Web. 9 Dec. 2014. https://www.privacyrights.org/are-you-being-stalked#7.
[22] "E-Mail Scam Includes Hit-Man Threat." *FBI*. FBI, 15 Jan. 2007. Web. 21 Nov. 2014. http://www.fbi.gov/news/stories/2007/january/threatscam_111507.
[23] J. A. Hitchcock, "Cyberstalking and Law Enforcement," *The Police Chief* 70 (December 2003): 16–27.
[24] Casey, Eoghan. "Investigating Cyberstalking." *Digital Evidence and Computer Crime*. 2e Éd. ed. Amsterdam: Elsevier/Academic, 2004. Print.