Cyberstalking

Nathan Burns
Cybersecurity Department
Western Washington University
Bellingham, WA, USA
Email Redacted

ABSTRACT

Cyberstalking is an invention of the internet age that has widespread impact on the current ecosystem of the internet. It's pervasive in every service, platform, and communication avenue. The impact it has on its victims can range from a minor annoyance to leading to depression and thoughts of suicide and has a profound impact on our nation's youth. Throughout this paper I'll detail legislation that helps prevent cyberstalking, discuss different methods cyberstalkers employ, and present worrying statistics on how widespread of an issue it is. Towards the end I'll give possible solutions and ways communities can prevent cyberstalking.

1 INTRODUCTION

To put it simply, cyberstalking is the act of using electronic or digital means to harass or stalk someone. The impact on someone being cyber stalked can be a simple annoyance or inappropriate nuisance or in more serious cases it can involve threats of physical violence and sexual harassment. Some victims report physical ailments like headaches, stomach ulcers, or mental issues such as PTSD or depression as a result of cyberstalking, and in extreme cases, they may become suicidal.

In 1990, California became the first state to enact a law against stalking and since then all 50 states have enacted anti-stalking laws [1]. Cyberstalking is illegal at the federal level by U.S.C 47 223(c), although it only applies to interstate or foreign communications [2]. To be found guilty of Cyberstalking in Washington State one must make an electronic communication with the intent to harass, intimidate, torment, or embarrass any other person or a third party:

a. Using any lewd, lascivious, indecent, or obscene words, images, or language, or suggesting the commission of any lewd or lascivious act.
b. Anonymously or repeatedly whether or not conversation occurs; or
c. Threatening to inflict injury on the person or property of the person called or any member of his or her family or household.

Cyberstalking is a felony if the perpetrator has previously been convicted of harassment with the same victim or threatens to kill a person, otherwise, it is a misdemeanor [3].

2 METHODS

The most defining characteristic of cyberstalking as opposed to physical stalking is that it's easier. Before the invention and widespread use of the internet, if I wanted to stalk my ex, I'd have to physically take substantial time out of my day to follow them *physically*, build up a schedule, take physical photos, and the like. This is a high-energy task, both physically and psychologically. The psychological "barrier" to cyberstalking is also lower the aforementioned physical method of stalking takes time, allowing someone to "cool down" or give them time to reconsider. It also makes it easier for law enforcement to take action against my physical stalking and increases the likelihood of being detected. Nowadays if I wanted to stalk my ex, I can do it all from the comfort of my home at any time.

Akin to how many organizations and law-enforcement departments consider marijuana a "gateway drug" into more hardcore substances, cyberstalking is a gateway "drug" into physical stalking. Cyberstalkers prime their behavior and build a connection with their victims online which later allows them to rationalize physical stalking easier.

Email is the most common form of cyberstalking [4]. This is due to the fact that first, everyone has one, and second, it's easy to imitate someone else. There are no checks in place to ensure that when I make nathanburns@gmail.com that my name is Nathan Burns if I know a stalker has a relationship with someone else I can easily create fake email addresses and try and pretend I'm them and intimidate or harass them to greater effect. This happened to Roni Jacobson and her stalker "Danny." Her stalker started harassing her friend due to her having the "Best Friend" status on social media (more on this later) and used that to send spoofed emails to Roni's friend calling her "ugly" and "slut" while pretending to be her or a mutual friend [5]. This has a huge impact on the victim because of the strain it puts on genuine relationships. While some friends might stick with her, some might

give in to the stalker and break off the friendship. This tactic is also used in business relationships where a stalker will harass potential business partners or customers, leaving many to cut ties with the victim.

Email might be the most common form of cyberstalking, but Facebook is where the most cyberstalking incidents are escalated. 22% of victims who reported an escalation had this happen on the platform [5]. This is due to a multitude of reasons:

1. Facebook is a more intimate social media platform. It's where people connect with family members and make relationships in public. This makes it a prime target for cyberstalkers to gather information and engage with their victim. Status's like "Best Friend" and "In a relationship with X" make it easier to get additional targets to stalk and/or harass.
2. A majority of people have one. Facebook has almost 3 billion active users, 2 billion of those using the platform every day [6].
3. Facebook's algorithm prioritizes inflammatory posts such as a cyberstalker spreading false information about a victim.
4. 63% of Facebook profiles are visible to the public with less restrictive privacy settings being the default [5].

Social media in general is an enticing platform of choice for the would-be cyberstalker. 55% of teens will share personal information with the general public without any privacy settings in place [5]. Social media companies need to do more to help limit this, making default privacy protections stricter will go a long way in this regard.

In recent years we've seen malicious actors use the same tactics that some cyberstalkers also use in an attempt to extort victims to send money. Cyberstalkers or scammers will send emails to victims saying they have compromising videos of them performing sexual acts and claim they will send these videos to their friends, co-workers, or colleagues unless they send them money. The FBI labels this as "sextortion" and has seen the behavior in malware variants like "MyloBot" that send threatening emails demanding payment in cryptocurrency [7, 8]. A cyberstalker uses this tactic to scare and threaten their target whereas a threat actor or malware operator uses it for financial means.

3 PUBLIC HEALTH ISSUE

The Center for Disease Control (CDC) labels stalking, both physical and digital a public health problem that affects millions of people in the United States [9]. According to the CDC, roughly 24% of female victims and 19% of male victims reported being stalked as minors, while 1 in 3 women and 1 in 6 men have been stalked at some point in their lives [9]. The impact of cyberstalking isn't limited to the digital world either, with 69% of female victims and 80% of male victims reporting threats of physical harm during their lifetimes. According to a US government survey, 1.5% of the entire population will be a victim at least once of cyberstalking within the next 12 months and 4% of all women will suffer from at least one incident[4]. Research has also shown there is a strong correlation between stalking and chronic disease and psychological distress such as depression and Post-Traumatic Stress Disorder (PTSD).

4 NOTABLE CASES

It's important to talk about specific cases relating to cyberstalking instead of just listing statistics. I'll be discussing the case of "Megan Meier", a young woman from Missouri whose death sparked nationwide outcry and resulted in anti-cyberbullying legislation with her name being passed in her home state.

Megan Meier was a teenager who suffered from bullying at her school, one day she created a myspace account and shortly received a friend request from a 16-year-old boy named "Josh Evans". The two exchanged messages for a time and Meier's parents said it had a positive impact on their daughter, but on October 16th, 2006, the tone of the messages changed. "Josh Evans" started sending troubling messages to Megan saying things like "I don't want to be friends with you anymore. You're not a nice person." The final message "Josh Evans" sent to Megan was "Everybody in O'Fallon knows who you are. You are a bad person and everybody hates you. Have a shitty rest of your life. The world would be a better place without you." Megan responded saying "You're the kind of boy a girl would kill herself over." Megan Meier would end up taking her own life the same day. The "Josh Evans" account was later found out to have been created by a neighbor of Megan who wanted to "mess with Megan". The case drew national attention after news broke of the "hoax" and the FBI investigated the case, Lori Drew, the adult who created the "Josh Evans" account was later indicted and convicted of violations of the Computer Fraud and Abuse Act (CFAA), but her conviction was later on vacated on the ground that the CFAA did no criminalize the conduct she was accused of [10]. This resulted in national backlash and the creation of numerous local, state, and federal legislation to cover loopholes in current laws. The most notable being HR 6123 or "Megan Meier Cyberbullying Prevention Act" which intended to close those loopholes nationwide.

This is just one of many *public* cases, most likely millions more go unreported or ignored by law enforcement every year. It is a national epidemic that requires the full attention of everyone, from lawmakers to teachers to law enforcement and classmates.

4 CONCLUSION

Cyberstalking is a widespread issue with no "one size fits all" solution. Everyone must work together to end cyberstalking and the most effective tool is communities creating a safe and supportive environment that shows the impacts of cyberstalking and promoting healthy relationships. We must start young and help to empower everyone to understand and address cyberstalking.

We've seen a growing change recently in the willingness of local law enforcement to pursue action against cyberstalkers, but we must do more.

Social Media companies have the greatest ability to help victims and prevent abuse. They need to provide easy-to-use reporting tools for victims and enhance privacy protections to make it harder for stalkers to thrive on their platforms. They can also provide educational materials for users engaging in cyberstalking activities to help prevent it from escalating.

REFERENCES

1. The Berkman Center for Internet & Society at Harvard Law School. 1999. State and Federal Stalking Laws. https://cyber.harvard.edu/vaw00/cyberstalking_laws.html
2. Cornell Law School Legal Information Institute. 2013. Obscene or harassing telephone calls in the District of Columbia or in interstate or foreign communications. https://www.law.cornell.edu/uscode/text/47/223
3. Washington State Legislature. 2004. Cyberstalking. https://app.leg.wa.gov/rcw/default.aspx?cite=9.61.260
4. Brandon Gaille. 2017. 21 Provocative Cyberstalking Statistics. https://brandongaille.com/20-provocative-cyberstalking-statistics
5. Roni Jacobson. 2016. I've Had a Cyberstalker Since I Was 12. https://www.wired.com/2016/02/ive-had-a-cyberstalker-since-i-was-12/
6. Data Reportal. 2022. Facebook Stats and Trends. https://datareportal.com/essential-facebook-stats.
7. Federal Bureau of Investigation. 2015. What is Sextortion? https://www.fbi.gov/video-repository/newss-what-is-sextortion
8. Ravie Lakshmanan. 2022. New MyloBot Malware Variant Sends Sextortion Emails Demanding $2,732 in Bitcoin. https://thehackernews.com/2022/02/new-mylobot-malware-variant-sends.html
9. Center for Disease Control. 2022. Preventing Stalking. https://www.cdc.gov/violenceprevention/intimatepartnerviolence/stalking/fastfact.html
10. Wikipedia. Suicide of Megan Meier. https://en.wikipedia.org/wiki/Suicide_of_Megan_Meier