IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cyber Stalking: An Open Source Intelligence

***Rajratna Jadhav **Prof. R. N. Mangoli**

***Research Scholar, Dept. of Criminology and Criminal Justice, Rani Channamma University, Belgavi-591156**

****Research Guide, Dept. of Criminology and Criminal Justice, Rani Channamma University, Belgavi-591156**

Abstract

The world of internet is immense. With day to day development in the field it's becoming far more multi-dimensional. But ultimately it's a technology and like every technology internet also has its drawbacks. This regularly developing world of internet has provided a wide area for the perpetrators of crime. The information available on internet is at risk if not taken proper care and protection. In recent years the cyber crime rate is increasing rapidly and it won't be understatement to say that in coming time these crimes will overpass traditional crime rate. The following paper discusses about one of such crime i.e. cyber stalking and types of stalkers online and also about precautionary measures to be taken.

Key Words:- Multi-dimensional, Cyber crime, Cyber Stalking.

Introduction

Cyber stalking is the use of the internet or other electronic means to stalk or harass an individual, group or organization. When carried out sensibly and securely, communication through social networks and other online public forums can be beneficial, both socially and professionally.

However, if you're not careful, it can lead to numerous undesirable consequences, one of which is cyber stalking. Cyber stalking can take many different forms, but in the broadest sense, it is stalking or harassment that takes place via online channels such as social media, forums or email. While blame shouldn't be placed on cyber stalking victims, the current online scenario is such that it creates easy targets. Cyber stalking doesn't have to involve direct communication, and some victims may not even realize they are being stalked online. Perpetrators can monitor victims through various methods and use the information gathered for crimes like identity theft. Attackers can collect your personal data, contact your friends and attempt to harass you offline. Most cyber stalkers are familiar with their victims. Being monitored by or receiving intrusive messages from an unfamiliar person or a casual acquaintance can be considered cyber stalking. It can have many motives including revenge, anger, control or even lust. The internet grants cyber stalkers access to a vast amount of personal information with relative ease. Information that was once considered private and confidential a few decades ago can easily be accessed

through a variety of brokerage websites that cater specifically to individuals innocently searching for friends or loved ones. Some of these websites are free, but the large majority will charge a small service fee in exchange for a person's name, phone number, address, social security number, date of birth and other confidential identifying information. One of the many advantages that cyber stalkers have over the traditional stalker is that these offenders typically have a high level of computer proficiency and aptitude, essential skills that allow the stalker to take crucial steps toward avoiding detection. The anonymity of the internet allows the cyber stalker to easily conceal one's identity through a variety of inexpensive and simple tactics. For instance, cyber stalkers can connect to several different internet service providers, thereby creating a number of screen names, which will make it nearly impossible to track the origin of the emails.

Types of Stalkers

The Intimate Stalker – The intimate stalker cannot accept that his/her relationship has ended and begin to stalk the partner through the Internet. The victim usually has no knowledge they are being stalked, and when they do, the stalking has intensified. The intimate stalker believes that the stalking attempts, professed love, bullying, threats, or public shame will harm the partner or win back the affection of that partner.

The Vengeful Stalker – The most dangerous and destructive types of internet stalker are known, as the vengeful stalker. These internet stalkers should be considered dangerous as they are more likely to take their online obsessions to real world form. The vengeful stalker are not limited to obsessive stalking techniques, profane bullying, or sexually explicit harassment. Operating with the motive to cause misery to the victim, this type of stalker may act to publicly shame or create falsifications to assassinate the character of the victim.

The Erotomanic Stalker – These internet stalkers form non-existent relationships with their victim. These stalkers believe their actions, of abuse, will lead to the victim falling into love with them; and that any attention from the victim is a display of that love interest. The Erotomanic stalkers goal is to be loved, sexually fulfilled, or given attention; they may resort to violence to get their wants, desires, and needs met.

The Trolling Stalker – These internet stalkers often post obsessively violent statements to their victims; these comments may also be controversial, irrelevant, inflammatory and off-topic. These stalkers derive their self-pleasures by causing harm, electronically, to their victims and usually act without the victim's knowledge.

The Predatory Stalker – These stalkers are classic sexual predators. The predatory stalkers are motivated by the desire for sexual gratification and power over the victim. Usually sexually deviant, this type of stalker may also have poor social skills and lowered intelligence, they most commonly keep to themselves as sociopathic individuals and come from a troubled existence with past hardships. Sexual predators pray on those who appear to be weaker usually females and children and may engage in behaviors such as surveillance, monitoring internet activities, obscene phone calls, fetishism, voyeurism, sexual masochism, sexual sadism and/or exhibitionism. Victims to this type of stalker can be a known individual or complete stranger.

Statistics

Eight out of 10 people in India have experienced some form of online harassment, with 41% of women having faced sexual harassment on the web, according to a new survey commissioned by cyber security solutions firm, Norton by Symantec. The study also found that of the four countries from the Asia-Pacific region which were surveyed India, Australia, New Zealand and Japan, India recorded the highest level of online harassment, with 45% of the respondents having experienced cyber stalking. According to NCRB report 2019 cyber crime registered cases raised to 63.5% over 2018. Out of total 44,546 cases 60.4% cases

registered were with motive of fraud (26,891) followed by sexual exploitation with 5.1% (2,266 cases) and causing disrepute with 4.2% (1,874 cases). These cases are registered under different sections of the Indian Penal Codeand are read with the IT Act.

Legislations

Cyber laws in India or cybercrime law in India are important because of the prime reason that cybercrime act in India covers all the aspects which occur on or with the internet transactions and activities which concern the internet and cyberspace. The rise of the 21st century marked the evolution of cyber law in India with the Information Technology Act, 2000. The objective of the Information Technology Act in India is as follows:

- To provide legal recognition for all e-transactions.
- To give legal recognition to digital signatures as a valid signature to accept agreementsonline.
- To give legal recognition to keeping accounting books in electronic form by bankers aswell as other organizations.
- Protection of online privacy and stopping cyber crimes.

IT Act, 2000 went through amendments in the year 2008. These were made in light of the laws on cybercrime. They were enforced at the beginning of 2009 to strengthen the cyber security laws. Modifications in the Information Technology Act, 2008 included the change in the definition of some terms such as communication devices. The amendment for the definition ofcommunication device was to include:

1. The current use.
2. To validate the digital signature.
3. To make the IP address owner accountable.
4. Impose liability for data breaches.

Women who are being stalked can complain to the National Commission for Women (NCW)and the Commission will take the matter up with the police. Any woman, in any part of India, can file this complaint. The Commission asks the police to then expedite the investigation. In serious cases, the commission forms an inquiry committee, which makes a spot inquiry, examines witnesses, collects evidence, etc. The Commission also has powers to summon the accused, the witnesses and police records, to facilitate the inquiry.

Protect yourself against Cyber stalking

- Review what online information exists about you and keep it to a minimum.
- Regularly change your e-mail and passwords for key online accounts and keep them safe.
- Review all your privacy and security settings.
- Avoid public forums.
- Ensure that your computer and mobile devices have updated antispywaresoftware installed and turned on.
- Ensure your wireless hub/router has security turned on.
- Unless you are using a secure web page, do not send or receive private information whenusing public WiFi.
- Limit the personal and financial information you share on or offline.
- Educate friends, family and work colleagues into the risks.

Conclusion

To sum up, though a crime free society is perfect and exists only in illusion, it should be constantattempt of rules to keep the criminalities lowest. Especially in a society that is dependent more and more on technology, crime based on electronic law-breaking are bound to increase and the law makers have to go the extra mile compared to the impostors, to keep them at bay. Raising awareness and implementing the strategies suggested above can go a long way in protecting oneself and his/her loved ones from threats of cyber stalking.

References

1. Michael L. Pittaro 2007, Cyber stalking: An Analysis of Online Harassment and Intimidation, International Journal of Cyber Criminology https://www.cybercrimejournal.com/pittaroijccvol1is2.htm

2. https://www.tripwire.com/state-of-security/security-awareness/what-cyberstalking- prevent/

3. https://www.thebetterindia.com/45671/stalking-india-women-complaint-online/

4. https://en.wikipedia.org/wiki/Cyberstalking

5. https://www.getsafeonline.org/protecting-yourself/cyberstalking/

6. https://socialmediacast.wordpress.com/tag/six-types-of-cyber-stalkers/

7. https://www.thehindu.com/news/national/8-out-of-10-indians-have-faced-online-harassment/article19798215.ece

8. https://www.thenewsminute.com/article/first-time-india-has-data-cyber-stalking-and- cyber-bullying-women-111064

9. https://www.myadvo.in/blog/what-is-the-cyber-law-in-india/

10. https://timesofindia.indiatimes.com/india/ncrb-crime-data-2019-cases-registered-up-1-6-crimes-against-women-rise-7-3-cyber-crimes-jump-63-5/articleshow/78394087.cms