WHITE PAPER ON

Cyberstalking

Prepared by **Mohammed Samiuddin**

Contents

Introduction

Stalking is a criminal activity that has been reported since the 19th century. It involves the persistent and obsessive trailing and harassing of a person, group of persons or organisations to infuse threat, fear, injury, assault, bully, false accusations, false victimisation, slander, emotional distress, harass, embarrass, spam, disrupt life, etc.

Technology has opened up new vistas in the areas of mobile communication, GPS navigation, the Internet, etc. facilitating access to information and performing a host of online activities. The flip side to this is the misuse of technology to commit crimes using internet.

What is Cyberstalking?

Although the term cyberstalking lacks a generally accepted definition, it normally refers to stalking another person by using on-line environment. It involves the use of the internet or electronic means to stalk and is one of the numerous forms of misusing technology for committing crimes. The criminals misuse the anonymity feature offered by the internet to conceal their identity.

Corporate cyberstalking is the use of the Internet or other electronic means to harass an individual, a group, or an organisation. The motives for this can be ideological, desire for financial gain, or revenge.

A Global Issue

Cyberstalking is a criminal offense and comes under the purview of anti-stalking, slander, and harassment laws. A cyberstalking conviction can result in a restraining order, probation, or even criminal penalties against the assailant, including imprisonment.

The common characteristics of cyberstalking include false accusations, monitoring, threats, identity theft, and data destruction or manipulation. It also includes exploitation of minors and the harassment can take on numerous forms.

Some people believe that cyber-stalking is an intrusion but not a physical threat, which is not necessarily true. A potential stalker may not be comfortable in a face-to-face confrontation but will not hesitate to use electronic communications to harass the victim.

Cyberstalking is a global issue and a menacingly increasing social problem that creates new offenders and victims. The rapid increase in use of the internet provides criminals new opportunities to commit crimes and remain hidden, although, many users are unaware of the fact that the criminal opportunities available offline also exist online.
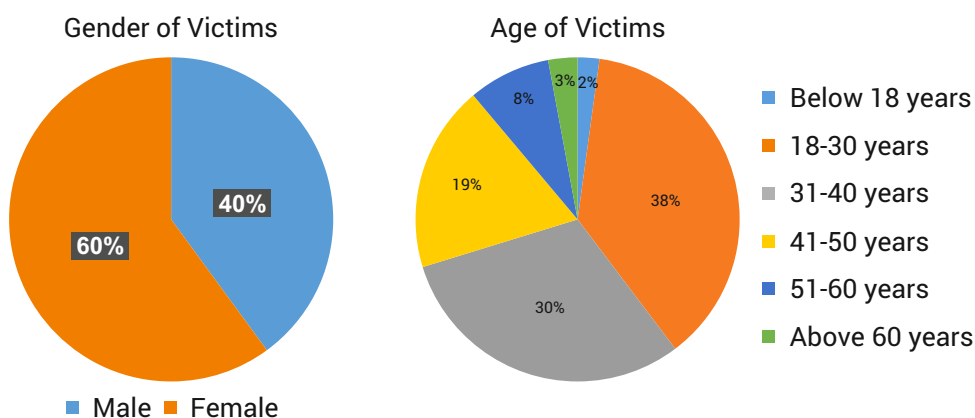
What is Cyberstalking?

Information Gathering to Cyberstalk

Although a great deal of personal information is available about most people on the internet, information gathering is generally a slow process. Most cyber criminals are highly enterprising in collecting the required information and also engage in social engineering (contacting the acquaintances of victims and soliciting the participation of the victims instead of hacking into their systems directly) to learn even more about the victims. In most cases, the targets are the victims that give the information without their knowledge as the attackers exploit human vulnerabilities to make this task easier.

Cyberstalking Targets / Victims

Cyberstalking statistics all over the world consistently show that majority of victims belong to the age group of 18-30 and most of them are females. Stalker from any side of the globe can access their victim's information to perform the criminal activities.

The following charts indicate the cyberstalking statistics related to the gender and age of victims.

Gender of Victims

Male: 40%
Female: 60%

Age of Victims

- Below 18 years: 2%
- 18-30 years: 38%
- 31-40 years: 30%
- 41-50 years: 19%
- 51-60 years: 8%
- Above 60 years: 3%

Source: *Statista*
1). Gender of Victims: Cyber stalking: share of victims 2013, by gender
2). Age of Victims: Cyber stalking: share of victims 2013, by age group

Motive

Various factors induce the stalkers and the most prominent among them are: pathological obsession (professional or sexual); unemployment or failure in their job or life; intention to intimidate and cause others to feel inferior. The stalker is delusional and believes he/she knows the target and wants to instil fear in a person to justify his/her status; a belief they can get away with it (anonymity); intimidation for financial advantage or business competition; revenge over perceived or imagined rejection.

Types of Cyberstalkers

Rejected Stalker

The rejected stalker is the most common, persistent, and intrusive of all the other types. A rejected stalker is the one who is obsessed with someone who might be a former romantic partner or a friend, and who has ended their relationship, or indicates that he / she intends to end the relationship.

Resentful Stalker

A resentful stalker is the one who is probably looking for revenge against someone who has upset them. The victim could be someone known to the stalker or a complete stranger. The stalkers intent is to frighten and distress the victim.

Predatory Stalker

A predatory stalker is the least common type, whose plan will be to physically or sexually attack the victim.

Intimacy Stalker

An intimacy stalker seeks to establish an intimate and loving relationship with the victim. These type of people think that the victim owes them love and affection because of all the time and effort it took for them to stalk the victim.

Incompetent Suitor

The incompetent stalker looks for a short-term sexual relationship. These type of stalkers can be easily discouraged by confronting them.
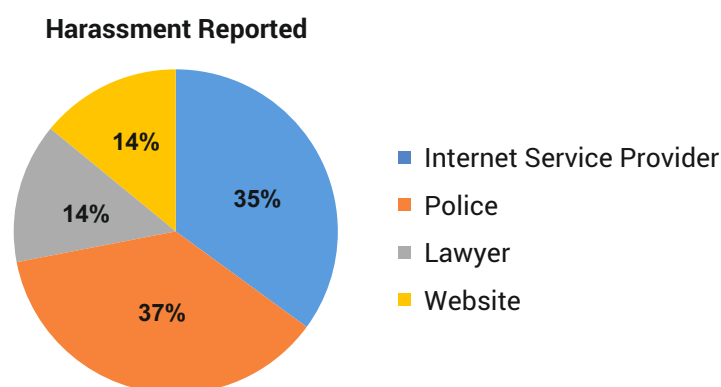
Erotomania and Morbidly Infatuated

The stalker of this type is generally affected by delusional illness. They imagine that the victim is in love with them and live in fantasies. The stalker must be psychologically treated or arrested to keep away from the victim.
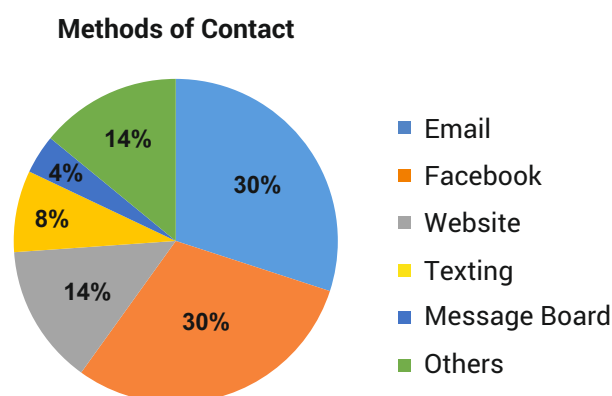
Cyberstalking Statistics

The following chart indicates the cyberstalking harassment reported to authorities by the cyberstalking targets / victims.

Harassment Reported

- Internet Service Provider
- Police
- Lawyer
- Website

35% 37% 14% 14%

Source: *Statista - Cyber stalking: authorities to whom harassment was reported 2013*

The following chart indicates the most frequently used cyberstalking contact methods.

Methods of Contact

- Email
- Facebook
- Website
- Texting
- Message Board
- Others

30% 30% 14% 8% 4% 14%

Source: *Statista - Cyber stalking: share of victims 2013, by how harassment began*

Note: *The "Others" included in the chart are methods of contact such as: Dating site, Twitter, My Space, Instant Messaging, Blogs, Impersonation, and You Tube.*

HELP

What if you are a victim?

- Report incidences of cyberstalking to the appropriate law enforcement agency
- Save all communications you had with the stalker for evidence
- Block the email address or chat room
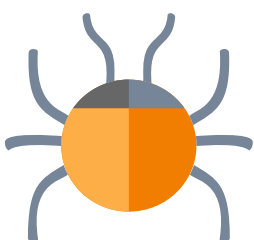- Capture and contact the stalkers ISP and file a complaint

Prevention

- Never give any personal information across the internet
- Do not share your password with anyone; also, change them frequently
- Do not share personal information online
- Do not use gender specific or provocative screen name or email address
- Use authentic and efficient firewall, antivirus applications, and update them regularly

About the Author

Mohammed Samiuddin spearheads the branding aspects & managing client relationships of ITMR. His passion includes speaking on cyber security threats, data security practices and new technological areas.

Reference

Cyber-Stalking: http://www.ccmostwanted.com/cyberstalking/

Types of Stalkers: http://melissanoon.hubpages.com/hub/The-Six-Types-of-Stalkers

Cyber-Stalking: http://www.teenchatdecoder.com/176/what-is-cyber-stalking/

Straight Talk About Cyber-Stalking: http://us.norton.com/cyberstalking/article/

Cyber-stalking:http://www.sans.org/reading_room/whitepapers/threats/cyber-stalking-privacy-intrusion-its-scariest_457

NW3C- Cyber-Stalking__(10-09)DEA10B7727C80144B56E5500

Statistics: http://www.statista.com/statistics/291217/cyber-stalking-victims-gender/

http://www.statista.com/statistics/291241/cyber-stalking-victims-how-harassment-began/

http://www.statista.com/statistics/291209/cyber-stalking-victims-age-group/

http://www.statista.com/statistics/291265/cyber-stalking-authorities-to-whom-harassment-was-reported/

http://en.wikipedia.org/wiki/Cyberstalking#Motives

About ITMR

Institute of Technology, Management and Research (ITMR), a division of Mamta Trust, is a premier institute that provides world class professional training programs for the corporates and academic sector. ITMR's motto 'yogah karmasu kausalam' means 'Yoga is excellence in action' and is the foundation of its vision to evolve into a "CENTRE OF EMINENCE" to offer cutting edge vocational skills and mold professionals to become business and technical domain experts. ITMR's professional and corporate training programs include several cutting edge to help working professionals acquire domain expertise and meet the current and emerging challenges in the IT world.

Our flagship training program on Cyber security has (PDCIL) Professional Diploma in Cyber Investigations and Laws is a top of the class cyber security program in the country that trains top officials in the Police departments, Indian and International Banks, Military, Legal fraternity, Fortune 100 Global companies and Blue Chip India IT companies.

ITMR also offers research programs on Cyber Security (network security monitoring and access products), in association with Secure IQ, a leading provider of network security software products with headquarters in Fairfax, Virginia, USA and operations and development in Chennai, India.

ITMR
योगः कर्मसु कौशलम्

Institute of Technology Management & Research
(Division of Mamta Trust)

2/850, Mugaliwakkam Road, Mugaliwakkam, Chennai - 600 125, Tamil Nadu, INDIA.
Admin Office: HTC Towers, No.41, GST Road, Guindy, Chennai – 600 032,
Tamil Nadu, INDIA. Phone: +91 44 4345 3500 / +91 44 4345 3349
Contact for More Information: training@htcitmr.ac.in