WHITE PAPER ON

Cyberbullying

Prepared by **Mohammed Samiuddin**

Contents

Introduction

The term Cyberbullying is a technology aided 21st century variant of bullying. Cyberbullying has emerged from the term "bullying". Bullying means a deliberate and persistent act of aggressive or overbearing behaviour by using force, threat, coercion, abuse, cruelty, or any other form of hostility to physically, mentally or emotionally hurt, harass or dominate smaller or weaker persons. Bullying can manifest itself in various forms. It can be: verbal, social or physical abuse, and ranges from one-to-one bullying to more complex forms where a primary bully is assisted by one or more accomplices or secondary bullies.

Rapid technological advancements in communication, the Internet, etc., has provoked the misuse of technology with criminal intent. Physical world crime has emerged as an avatar of Cyber World with innovations and ingenuity. Criminals ingeniously adapt new technologies to commit regular, newer forms, and variants of old crimes. Cyber World technologies serve as new outlets for criminals to commit crimes. It simplifies and eases the process of committing crimes, changes the face of the crime drastically, and helps criminals hide anonymously. One such avatar is cyberbullying, an extension of physical world bullying, in which computers, cell phones, and other electronic devices are used as aids to harass or mistreat a victim.

Bullying is a world-wide problem that needs to be taken seriously and dealt with firmly. It triggers anxiety, depression, low self-esteem, and in some extreme cases even incites suicidal tendencies among its victims.

Cyberbullying

Difference between Conventional Bullying and Cyberbullying

Though it is profusely debated throughout the virtual world, cyberbullying is just as real as conventional bullying and has extreme repercussions when compared to conventional bullying. The National and International laws therefore treat both forms of bullying in the same way. Despite this, conventional bullying and cyberbullying has several major differences. The following exhibit 1 differentiates the two forms of bullying.

Exhibit 1: Bullying ~ Cyberbullying	
Bullying	**Cyberbullying**
Face-to-face / direct bullying	Online bullying
Bully easily identified	Bully remains anonymous by hiding behind the anonymity feature offered by the Internet
Generally one-to-one	Can be one-to-one or highly complex where a primary bully is assisted by several accomplices / secondary bullies
Bullying occurs at specific times and at specific locations / localised	Occurs 24x7x365 nonstop, and not restricted to locations
Bullying durations are generally short to medium	Lasts for longer periods
Limited onlookers / localised audience	• Beyond geographical boundaries and therefore has vast / global audience • Enormous speed and reach - attacking materials can be accessed by millions all over the world within seconds
Bullying methods: verbal, nonverbal, through gestures, and physical	Bullying methods: posting text, pictures, audio and video recordings, etc.
Onlookers can see the emotional reactions of victims and can empathise with the victims	Reactions of the victims not seen, hard to empathise with the victims
Victims can escape physically by going away from the bullying location	No safe escape in the virtual world
Repercussions are generally localised and limited	Repercussions are beyond geographical boundaries and extreme

BULLYING

Cyberbullying and its Types

The menace of cyberbullying is rapidly increasing all over the world. The general argument about bullying and cyberbullying is that it affects only children, preteens or teens and the offenders and victims generally belong to the same age group. If adults become involved, it becomes a case of cyber harassment or cyberstalking. Adult cyber harassment or cyberstalking is not considered as cyberbullying, and these crimes are no different from conventional bullying in the eyes of the law. Therefore, based on the extent and reach of the crime, cyberbullying can be classified as follows:

Cyber Lynching

Cyber Lynching is group bullying or bullying by mob and is also referred as group bullying or cyber mob.

Masquerading

Masquerading involves the creation of false account to harass the victim anonymously. The bully can also impersonate someone and send messages to the victim to humiliate and attack.

Flaming

Flaming is harassment through online via emails, messaging, or chats. The bully uses angry, vulgar, and violent words against the victim to provoke them.

Text Bullying

Text bullying is an old school method of cyberbullying, which is generally a result of relation break up. It uses the basic cell phone messaging functions such as SMS or MMS to harass the victim.

Outing (Social Engineering)

Outing (Social Engineering) aims at manipulating the victim to willingly divulge embarrassing information or do something embarrassing. This information will be used to harass and embarrass the victim.

Motive

Every crime has a motive and the motive of cyberbullying is the same as conventional bullying; centred on distorted perceptions of human relationships, power, and control. The bullies try to establish power and control over others they perceive to be weak or small. Bullies are basically cowards in reality; they bully to conceal their numerous psychological weaknesses while cyberbullies find a safe haven in the cyberspace due to the anonymity provided by the Internet.

Cyberbullying Statistics

24% of students' aged between 12 to 18 years are being reported to be cyberbullied online:
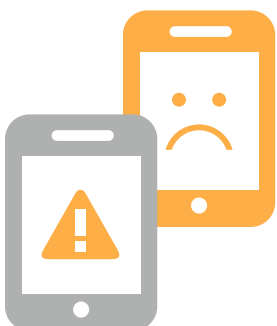
- 4.4% bullied through text messages
- 3.6% were bullied in Internet
- 2.7% bullied through Instant Messages
- 1.9% bullied using emails
- 1.5% bullied while gaming

When cyberbullied:

- 47% of high school students have not revealed it
- 40% of bullied students notified an adult after a school incident
- 26% of cyberbullied students notified an adult after an online incident

Statistics source:

http://www.adl.org/assets/pdf/education-outreach/Bullying-Cyberbullying-Statistics-Overview-One-Sheet.pdf

Effects of Cyberbullying

The victims of Cyberbullying are affected for the rest of their lives. When cyberbullied, the victim:

- Feels sad, stressed, depressed, worried, nervous, anger, hatred, scared, hurt, hopeless, frustrated, embarrassed, vulnerable, powerless, helpless, humiliated, falsely exposed, indicted, insecure, etc.
- Is triggered to react in ways such as: disinterest in almost all areas of life
- Loses their self-esteem, self-confidence, and sense of security
- Feels a high sense of insecurity and self-pity
- Seeks loneliness, avoids others, and stops socialisation
- Falls into stress induced illness (headaches, stomach ulcers, skin conditions)
- Changes the sleep patterns (insomnia, excessive sleep, and experience nightmares) and eating patterns (sulking, gluttonous)
- Gets numerous physical and psychological health complaints
- Lacks concentration, shows disinterest in academics and attending school, and develops tendency to skip school / absenteeism and drop out from school
- Develops violent behaviour or tendency to retaliate with violence
- Becomes alcoholic or drug abuser
- Develops vengeful feelings, seeks revenge, and vents anger by cyberbullying others (related / unrelated persons)
- Provokes suicidal tendency

Prevention / Impact Reduction

A few recommendations that can help prevent or reduce the impact of cyberbullying:

- Report bullying incidents to a trusted adult
- Do not open or read messages sent by cyberbullies
- Report bullying incidents to your school if it is school related
- Do not delete the messages as they are needed to take action
- Protect yourself: never agree to meet the cyberbully or any other person
- If you received the bullying messages through chat or instant messaging, the 'bully' can often be blocked
- If you are threatened of being harmed, inform the local police

Conclusion

The menace of cyberbullying cannot be eradicated completely but can be transformed from a fatal version to a less threatening version with all persons establishing adequate control and preventive mechanisms. To prevent cyberbullying, parents must watch the sites their children visit frequently, install monitoring programs, and encourage the children to inform them when cyberbullied. The young ones must understand that they will not be secluded when they inform the parents or teachers of being bullied.

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

http://cyberbullying.ph/2013/01/22/different-forms-of-cyberbullying/

http://www.cyberbullying.info/whatis/book.php?shelf=types&pg=Masquerading

http://www.isafe.org/outreach/media/media_cyber_bullying

http:www.stopcyberbullying.org

http://www.stopbullying.gov/cyberbullying/prevention/

https://sites.google.com/site/jointheupstanders/the-8-types-of-cyberbullying

http://andreaurbanfox.wordpress.com/2013/03/22/internetabuse/

http://www.stopbullying.gov/

Statistics: http://www.adl.org/assets/pdf/education-outreach/Bullying-Cyberbullying-Statistics-Overview-One-Sheet.pdf

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.

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