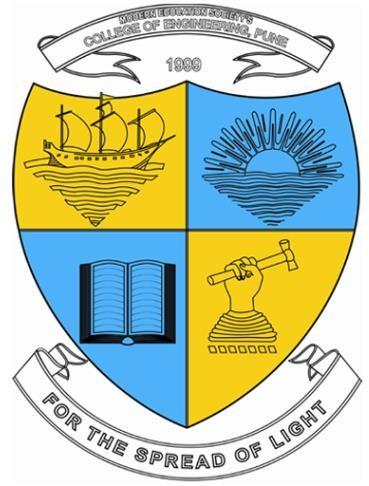
# Savitribai Phule Pune University

**Modern Education Society’s Wadia College of Engineering, Pune**

19, Bund Garden, V.K. Joag Path, Pune – 411001.

**ACCREDITED BY NAAC WITH “A++” GRADE**

**DEPARTMENT OF COMPUTER ENGINEERING**



A REPORT ON

## Case Study on Case Study of Cyberstalking and Related Cases

## B.E. (COMP III)

*SUBMITTED BY*

Ms. Megha

**DEFINITION:**

Cyberstalking is a form of harassment or stalking carried out over the internet. It involves repeated and deliberate use of the internet and other electronic communication methods to harass or threaten an individual, group, or organization. Cyberstalks may use various methods such as social media, email, and other online platforms to intimidate, control, or blackmail their targets.

### ISSUE:

The primary issue with cyberstalking is the psychological and emotional trauma it can inflict on victims. Unlike physical stalking, cyberstalking allows perpetrators to maintain anonymity, which can make it difficult for law enforcement to identify and apprehend them. Additionally, the pervasive nature of the internet means that victims can be targeted anytime and anywhere, often leading to a sense of helplessness and fear.

### LOSSES THAT CAN HAPPEN:

Cyberstalking can lead to various significant losses, including:

1. Emotional and Psychological Damage: Victims may experience anxiety, depression, and post-traumatic stress disorder (PTSD).
2. Reputational Damage: Public humiliation and false accusations can severely damage the victim's reputation.
3. Financial Losses: Some cases involve financial extortion or identity theft, leading to financial loss.
4. Loss of Privacy: Cyberstalkers often invade personal privacy by hacking into personal accounts or spreading private information.
5. Physical Danger: In severe cases, cyberstalking can escalate to physical stalking, putting the victim’s safety at risk.

### PREVENTING MEASURE:

1. Awareness and Education: Educating the public about the dangers of cyberstalking and how to protect themselves online.
2. Strengthening Legal Frameworks: Implementing and enforcing laws specifically targeting cyberstalking.
3. Use of Technology: Employing software and tools that enhance online privacy and security, such as VPNs and encrypted communication.
4. Reporting Mechanisms: Encouraging victims to report incidents of cyberstalking to authorities and providing clear channels for such reports.
5. Support Systems: Providing psychological support and counseling services for victims.

### CASE STUDY:

### Case: The Cyberstalking of Anita Sarkeesian

Year: 2012-2014

Origin: United States

### Overview:

Anita Sarkeesian, a well-known feminist media critic and the founder of the video series "Feminist Frequency," became the target of an extensive and highly coordinated cyberstalking campaign beginning in 2012. Sarkeesian launched a Kickstarter project to fund a web series titled "Tropes vs. Women in Video Games," which aimed to critically examine the portrayal of women in video games and challenge gender stereotypes within the gaming industry.

This project quickly attracted the ire of certain segments of the online gaming community, who perceived her work as an attack on gaming culture. What began as isolated negative comments soon escalated into a full-scale harassment campaign. Over the course of several years, Sarkeesian received an overwhelming number of threats, including death threats, rape threats, and graphic messages of violence directed at her across multiple platforms such as Twitter, YouTube, email, and even in comments sections on various websites.

The harassment was not limited to mere online insults; it included doxxing, where her personal information was leaked online, leading to fears for her physical safety. Sarkeesian was forced to cancel public speaking events due to credible threats, and the relentless nature of the harassment took a significant toll on her mental and emotional well-being. Despite this, Sarkeesian continued her work, speaking out about the abuse and advocating for greater awareness and action against cyberstalking and online harassment.

This case became a focal point in discussions about the toxicity within online communities, the challenges women face in male-dominated industries, and the need for stronger legal and societal responses to cyber harassment.

### Attack Vector:

* Social Media Harassment: Anonymous users and coordinated groups sent threats and harassing messages through social media platforms.
* Doxxing: Sarkeesian’s personal information, including her home address, was leaked online, leading to increased fear for her physical safety.
* Online Campaigns: Various forums and websites hosted discussions aimed at discrediting Sarkeesian’s work and encouraging harassment.

### Loss Happened:

* Emotional Trauma: The relentless nature of the harassment led to significant emotional and psychological distress for Sarkeesian.
* Public Image: Despite the harassment, Sarkeesian’s reputation was bolstered as she continued to speak out against the harassment and cyberstalking.
* Legal Action: Although some harassers were identified, the lack of clear legal recourse at the time made it difficult to take substantial legal action against the perpetrators.

### Prevention Measures Taken:

* Platform Policy Changes: Social media platforms like Twitter introduced stricter policies against harassment and more robust reporting tools.
* Public Awareness: Sarkeesian’s case brought widespread attention to the issue of cyberstalking, leading to increased public discourse on the topic.
* Legal Advocacy: Sarkeesian worked with legal experts to push for stronger legal protections against cyberstalking.