

GENDER-BASED CYBER THREATS AND HARASSMENT

Mate Gumberidze, Giorgi Mikeladze

Revised by: Elena Tsatsua

Abstract

The presentation delves into the realm of gender-based cyber threats and harassment, focusing on specific types of cyber threats, online harassment, and cybercrimes, including cyberbullying, blackmail, and stalking, from a gender perspective. Through an exploration of the existing situation, the presentation sheds light on the prevalent forms of gender-based cyber threats and harassment. With the increasing integration of technology into everyday life, the internet has become a common platform for perpetrating various forms of gender-based violence. This research aims to analyze the specific types of cyber threats and online harassment targeting individuals based on gender, providing insights into the nature, prevalence, and impact of these actions. By understanding the current landscape, we can develop more effective strategies and interventions to combat gender-based cyber threats and harassment.

Introduction

Cyber bullying refers to the use of digital technologies, such as the internet, social media, and mobile phones, to harass, threaten, or humiliate individuals. Unlike traditional bullying, cyber bullying can occur 24/7 and reach a victim even when they are alone.

Cyber-bullying and harassment include, but is not limited to, sending threatening messages, spreading rumors online, sharing private or embarrassing information without consent, impersonation, and exclusion from online groups or activities.

With the rise of Cyber-bullying, it became more and more apparent that women are more likely to be targeted by a harasser, according to Cybersmile.org (2017) their research resulted that women were more than twice likely to be targeted on a base of Gender than men.

Researches and Data

A European Union study reveals that 73% of women have experienced online abuse (EU Agency for Fundamental Rights 2014). In Germany, a survey indicated that women are more likely to face cyber harassment and stalking than men. Heartbreaking cases like that of 26-year-old Athira from Kerala, who took her own life following persistent cyber-violence, underscore the gravity of this issue. Girls as young as 12 in Spain, women in Pakistan, and female users of Facebook and WhatsApp in Peru are facing similar forms of cyber-harassment. The United Nations estimates that 95% of online aggression, harassment, abusive language, and denigrating content are directed at women.

According to the official website of United Nations: Over a four-year period, from the analysis of 19 million tweets, a Ditch the Label and Brandwatch report found that there were almost 5 million cases of misogyny on Twitter alone. Fifty-two per cent of the misogynistic insults recorded were authored by women and typically targeted the appearance, intelligence and sexual preferences of other women. The report found 7.7 million cases of racism, 390,296 instances of homophobia and 19,348 transphobic messages sent on Twitter. Only public data

First Student Conference: “Gender Dimension of CyberSecurity”

was examined, so when the figures are extrapolated from the entire Internet to include both public and private communication channels, the level of online hate speech is overwhelming.

According to the eSafety Commissioner, online abuse significantly affects women's mental health (41%) and self-esteem (35%), often causing them to withdraw from professional and public activities. Many women temporarily (22%) or permanently (5%) stop work-related online activities, 8% give up leadership roles, 5% leave their jobs, 9% avoid public discussions, and 5% delete social media accounts. When confronted with abuse, women most commonly do not respond (56%), block the perpetrator (54%), or delete posts/comments (37%) to avoid escalation (44%) and minimize stress (24%). Thirty percent believe acting wouldn't help. Over a third (38%) report abuse, mainly to social media platforms, with only 8% reporting to authorities. Sixteen percent take an activist stance by calling out abuse online or raising it in the media.

According to Pen America: After multiple instances of physical abuse over several years, a woman was granted a protective order (aka, a restraining order) against her abuser, Parris Deshaunte Evitt, in 2017. Evitt then turned his harassment and threats to the virtual realm, using texts, phone calls, emails, and Facebook messages to contact the victim over the course of two years. In 2020, Evitt was found guilty of violating the protective order and sentenced to nearly four years in prison. He was also ordered to pay compensation for the victim's hotel costs after she fled her home in the face of his threats.

An article made by Erika Yeung describes her life in the world of video games as a woman, sharing her enthusiasm of virtual world and struggles she had to endure while being a part of opposite gender from her then teammates. One of the stories goes as follow:

"I started playing Valorant as soon as it came out in 2020, another first-person shooter game. Two teams of five are put against each other, attackers and defenders, with the objective of planting or defusing a bomb. It quickly became my new favorite game.

I also discovered voice chat technology while playing Valorant, a system that allows players from all over the world to talk to each other without having to show their faces. But as soon as I spoke, my teammates heard my feminine voice and started making comments like “Oh we're gonna lose, we have a girl on our team.” Some even left the game." - Erika Yeung

In Georgia 18-year-old Mariam Grigalashvili is being distributed defamatory videos on "TikTok" with sexually explicit texts and disclosure of personal data. Before the girl began to speak publicly about cyberbullying, she turned to the police (right after the videos were released), where they told her that there was no point in writing a statement, citing the difficulty of investigating similar cases as the reason.

"My first video was posted on "TikTok" in the month of February, which included text with such terrible and sexual content, I can't repeat it. The content was an ordinary video, taken from the "Facebook" of my friends and parents. Under the video, such comments gradually appeared, I turned away, immediately went to the police in the department." - Mariam Grigalashvili

Solutions and conclusions

Gender-based cyber harassment is rising due to the pervasive nature of technology, exposing more people to online abuse and threats. The discussed statistics and stories highlight the severity and widespread nature of this issue, particularly affecting women. The mental health impacts, professional withdrawal, and reduced public engagement underscore the need for solutions. The University of Chicago suggests temporarily disabling or privatizing social media

First Student Conference: “Gender Dimension of CyberSecurity”

profiles to limit unwanted interactions. Responding to harassment can prolong incidents, so it's often best to avoid engaging. Other protective steps can be taken to mitigate these issues.

Ignore: The goal of social media agitators (commonly referred to as trolls) is to elicit a response. In many cases, trolls move on if you ignore them long enough.

Mute: If what someone is saying about you online is causing you distress, you can change your settings to mute them and never hear from them again, and since the typical troll doesn't go further than snide remarks or derogatory comments this tends to be the most effective way.

Block: Several social media platforms allow you to selectively prevent others from following you, seeing your posts, or commenting on your content, Along with muting this also is considered the best way to handle the online harassers, the only disadvantages however could be that, this notifies them of being blocked so if they want to, they could make a different account which you will have to block again.

Report: Reporting a user's behavior to social media platforms could result in their account being suspended if they violated the platform's guidelines. This strategy has limitations, as harassing messages might come from multiple accounts, making it difficult to pinpoint a culprit. Additionally, some posts might be harassing in nature but do not violate specific platform guidelines.

But there are, as we discussed, times when trolls cross the line and become actual criminals with malicious intent. Doxxing you and leaking your personal, sensitive information over the internet. This requires much more than previous ways to combat these types of criminals. It is very important to report these accounts, whether they are "fake" and report the incident to your local authorities as soon as possible. In certain situations, it is possible to track someone through the "fake" accounts, especially if it is involved in illegal activity, bringing them to justice.

References

1. <https://www.infrastructure.gov.au/media-technology-communications/internet/online-safety/esafety-commissioner>
2. <https://www.dexerto.com/>
3. <https://www.researchgate.net/>
4. <https://youthcomm.org/>
5. <https://www.cybersmile.org/>
6. <https://www.statista.com/>
7. <https://www.zonamovilidad.es/>
8. <https://www.britannica.com/>
9. <https://www.coe.int/en/web/portal>
10. https://www.ohchr.org/en/ohchr_homepage
11. <https://www.annapolis.gov/>
12. <https://eige.europa.eu/>