The Review of Contemporary Scientific and Academic Studies
An International Multidisciplinary Online Journal
www.thercsas.com
ISSN: 2583-1380 Vol. 3 | Issue No. 5 | May 2023 Impact Factor: 4.736 (SJIF)

Women and Cyberspace: The Challenges and Security in Cyberspace

Swapna Siddamsetti (swapnangit2021@gmail.com), Corresponding Author
Research scholar, Department of Computer Science, GITAM Institute of Sciences, GITAM University, Visakhapatnam; & Assistant Professor, Neil Gogte Institute of Technology, Hyderabad, India
Chirandas Tejaswi (chirandastejaswi22@gmail.com)
Student, Neil Gogte Institute of Technology, Hyderabad, India

Abstract: *Information and communication technologies (ICTs) are making everyone's lives easier and more convenient. They are unprecedentedly transforming our lives, especially those of women, by providing a different range of opportunities to people, businesses, and social relations. With the exponential growth of the "social internet", privacy is becoming a blurred concept as women are more eager to share information about their daily experiences, professional gains, and social relations. All these led people and organizations to enjoy parallel virtual lives in cyberspace. Cyberspace means the virtual and dynamic space created by machine clones. It can be compared to a human brain, where the network of computers represents the innumerable neurons and the connections between them. Therefore, it can be considered a link between the physical and the infinite worlds. The main victims of cyberspace are women, who get harassed over social media, and due to a lack of knowledge or sometimes due to fear of defamation, the culprits are not made accountable for their misdeeds, and justice is denied to these victims. Cyberbully is defined as making use of computer networks to impose or threaten violence on another person, which leads to sexual, psychological, or economic harm, and can include the exploitation of situations, qualities, and so on. Additionally, the world witnesses a digital gender divide (i.e., more men than women have smartphones, and men dominate the ICT jobs); as a result, women and girls are more vulnerable to cyber assault. This paper aims to understand the scenario of cyber-crimes and cyber security and analyze the perception of women towards awareness of cyber security. In this paper, we plan to suggest several preventive measures to counter the ever-increasing cyber-crimes against women in India. Unless women are being cautious and responsible, choices made in cyberspace can be costly and dangerous, due to the distinct characteristics that render cyber violence's gendered impact. In this paper, we will also examine the various laws that exist to protect women in such cases. We will include various case studies on cyber-crimes.*

Keywords: Cyberbully, Cyberspace, Cybercrimes, Cyber Security, Gender

Introduction

In the 21st century, the internet has grown into an indispensable element of our everyday lives. Technology has transformed the way we interact, study, work, and do business. Although the internet has also brought new challenges, particularly in the area of women's safety and security, Women face numerous online threats, including cyberstalking, cyberbullying, and online harassment. These forms of cybercrime have far-reaching implications for women's safety and security, as they can cause emotional, psychological, and even physical harm. Therefore, it is critical to comprehend the magnitude and nature of cyber-attacks against women and to investigate potential remedies. In social, economic, and political revolutions, technology for communication and information (ICT) is a developing weapon of globalization. Business Process Outsourcing and Knowledge Process Outsourcing are two examples of ICT technologies for management, education, financial marketing and development, having an impact on female empowerment in India. [1] Hence, cybercrime is a combination of technology and criminality. Simply described, "any act or criminal offence using an electronic computer" is cybercrime. The total number of cybercrime occurrences climbed by 18.4% in 2019, reported the National Bureau of Criminal Records, but the number of cybercrime charges against women increased by 28%. According to the statistics, 10,730 (or 20.2%) of the 52,974 events documented in 2021 were identified as crimes against women. Karnataka will have the greatest proportion of instances (2,243) in 2021, followed by Maharashtra (1,697) and Uttar Pradesh (958). [2]Every year on March 8, we mark International Women's Day to demonstrate our respect, love, admiration, and gratitude for the accomplishments of women in all realms of the economy, politics, and society. Women are respected exclusively at places of worship, religious activities, and festivals; but, in everyday life, they are exposed to many sorts of abuse and are constantly victims of physical, psychological, and sexual exploitation. Also, India is the world's most exploited country for women. According to estimates, 75% of victims were women,

The Review of Contemporary Scientific and Academic Studies
An International Multidisciplinary Online Journal
www.thercsas.com
ISSN: 2583-1380 Vol. 3 | Issue No. 5 | May 2023 Impact Factor: 4.736 (SJIF)

albeit these percentages are more hypothetical. The real numbers are unlikely to be known because the vast majority of these crimes are undetected, do not entail direct threats of physical violence, and are poorly understood or practised (Jaishankar and Sankary). Because of this, cybercrime targeting women continues to rise. This piece provides a summary of the position of women inside cyberspace and highlights the variables that contribute to women's online victimization. While it is impossible to eradicate all forms of cybercrime, this article provides several suggestions that can aid in the battle against cybercrime targeting women.

Literature Review and Methods

Women's safety and security in cyberspace is a growing concern globally. With the increasing use of the internet and social media platforms, women are subjected to numerous types of internet abuse, abuse and violence. This literature review examines research on women's safety and security in cyberspace, including the types of online harassment and violence women experience, the impact on their mental health, and the measures being taken to solve the situation.

The following are examples of internet harassment, including violence against women:

Research shows that women experience various forms of online harassment and violence, including cyberstalking, revenge porn, doxing, online trolling, and hate speech. Cyberstalking involves persistent and unwanted communication and contact online, which can escalate to physical violence. Revenge porn is the non-consensual sharing of intimate images online, often by a former partner. Doxxing is the publishing of personal and private information online, which can result in harassment and threats. Online trolling is the use of abusive language to harass and intimidate women online, and hate speech is the use of derogatory and abusive language to discriminate against women based on their gender, race, or religion.

Cyber Harassment: This is a type of harassment that involves blackmail, threats, and sending love letters or humiliating emails to those other users' mailboxes regularly. This conduct is meant to irritate Internet users. Sexual abuse is a specific sort of sexual harassment that includes, among other things, persistent and unwelcome sexual behavior.

Cyber Stalking: Cyberbullying is a common and often discussed cybercrime nowadays. It may follow a person's Internet travels by posting threatening comments on message boards, visiting chat rooms preferred by the victim, persistently flooding the victim's inbox, and so on. Men stalking women, or adults stalking children, are the most common perpetrators.

Cyber Pornography: It is described as the dissemination of pornographic content over the Internet. Another risk for female Internet users is that they have no idea which of their activities are being recorded and potentially published on the web. It is an uninvited action in which videos and pictures of the victim are collected in various ways, like hacking the victim's phone or computer, social media accounts, and so on. This has an adverse effect on the lives of victims in the real world. This violation is partially covered under Section 67 of the IT Act of 2000.

Cyber Defamation: Defamation is a crime, whereas online defamation is defamation done using computers and the World Wide Web. It occurs when people begin publishing libellous remarks or obscene content on numerous online social networking platforms. Because a user's comment board is available to all of the other users, anybody can put a defamatory comment on it, and it becomes visible to all. Online libel is another term for defamation on the internet.

Morphing: It is about creating a picture that is completely or just slightly distinct from its source by using a false identity. The assailants took images of the ladies from their accounts on social media, modified them (changed them), and posted fresh photos under bogus accounts. The alteration is frequently done using two photographs, one of which is merged into the other and displayed in a compromising circumstance or pose that appears to make the lady acquiesce to the conduct portrayed in the image. Then there's extortion, where the lady is threatened to do something, and if she doesn't, the images are broadcast over the internet, embarrassing the woman in the community and lowering her position. Infringers are prosecuted under articles 43 and 66 of the IT Act of 2000

Email Spoofing: Email spoofing is the fraudulent and unlawful alteration of an email's genuine source. The address headers and sender address are altered in such a manner that it's impossible to tell that the email has

The Review of Contemporary Scientific and Academic Studies
An International Multidisciplinary Online Journal
www.thercsas.com
ISSN: 2583-1380 Vol. 3 | Issue No. 5 | May 2023 Impact Factor: 4.736 (SJIF)

been faked and appears to come from a different source. Men frequently use these emails to send women filthy and disgusting images, brag about their attractiveness, request favors, and ask for just a date or the cost of an evening with them.

Challenges Faced By Women in Cyberspace

The challenges faced by women in cyberspace are complex and multifaceted. Some of the challenges faced by women in cyberspace:

1. Online harassment: Women face a high level of online harassment, including cyberstalking, cyberbullying, and revenge porn. According to a 2019 Pew Research Center study, 41% of women and 26% of men had been sexually harassed online. [3]
2. Cyber violence: Women are also subjected to internet violence in the form of threats, hate speech, and violent incitement. This can lead to psychological harm and even physical harm in some cases. [4]
3. Gender-based discrimination: Women also face discrimination in cyberspace, including discrimination in employment and pay as well as exclusion from online spaces and communities. [5]
4. Lack of representation: Women are also underrepresented in technology and related industries, including cyber security, which can limit their career opportunities. [6]
5. Online privacy: Women's online privacy is also at risk, as their personal data can be stolen, leaked, or used without their consent. This can lead to identity theft and other forms of cybercrime. [7][13][14]

Laws and Policies Made to Protect Women in Cyberspace

Some laws and policies have been made to protect women in cyberspace. Here are some examples:

1. The United Nations General Assembly passed the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) in 1979. CEDAW is a comprehensive framework for eliminating gender discrimination in all aspects of life, including online. It compels agencies to take steps to eliminate all types of discrimination against women, including cyberbullying and internet harassment. [8]
2. The Istanbul Convention, also known as the European Council Convention on Preventing and Combating Violence Against Women and Domestic Abuse, was approved in 2011. It acknowledges that violence against women and girls may occur both physically and digitally. States parties are required under the Convention to adopt steps to prevent and eliminate violence against women, especially online abuse. [9]
3. The European Union's General Data Protection Regulation (GDPR) came into effect in 2018. The GDPR regulates the processing of personal data and applies to all companies that process the personal data of EU citizens, regardless of the company's location. It includes provisions to protect individuals' privacy rights, including the right to be forgotten, which allows individuals to request that their personal data be deleted. [10]
4. The Cybercrime Prevention Act of 2012 in the Philippines criminalizes various forms of online abuse, including cyberstalking and online harassment. The law imposes penalties on perpetrators of such acts, including imprisonment and fines. [11]
5. The Online Harms White Paper, released by the UK government in 2019, proposes a regulatory framework for online platforms to address harmful content online. The proposed framework would require companies to take steps to protect users from harmful content, including cyberbullying and online harassment. [12]

The Effect on Women's Psychological Health: Internet harassment and abuse may have serious consequences for women's mental health, including anxiety, sadness, and trauma. Women who have experienced online harassment and abuse are more likely to have anxiety and depression symptoms, to feel alone and uncomfortable, and to have low self-esteem. The fear of harassment and violence can also lead

The Review of Contemporary Scientific and Academic Studies
An International Multidisciplinary Online Journal
www.thercsas.com
ISSN: 2583-1380 Vol. 3 | Issue No. 5 | May 2023 Impact Factor: 4.736 (SJIF)

women to self-censor their online activities, limit their online presence, and avoid certain topics or discussions.

Measures to Address the Issue: Various measures are being taken to address women's safety and security in cyberspace. These include legal measures, such as criminalizing online harassment and violence, and creating safe spaces and reporting mechanisms for victims of online harassment and violence. Other measures include educational campaigns and training for internet users on safe online behaviour and responsible use of social media platforms. Many tech companies are also taking steps to address online harassment and violence, including implementing stricter community guidelines, using AI algorithms to detect and remove abusive content, and providing reporting mechanisms for users to report online harassment and violence.

Therefore, women's safety and security in cyberspace is a growing concern, with various forms of online harassment and violence impacting their mental health and well-being. It is essential to continue researching this issue and implementing measures to address it, including legal measures, education campaigns, and technological solutions. We can make the internet a safer and much more inclusive place for everyone if we all work together.

Methodology

Ensuring women's safety and security in cyberspace involves adopting a comprehensive methodology that takes into account various aspects of online safety. Here are some key steps that can be followed:

1. Understand the risks: The first step in ensuring women's safety and security in cyberspace is to understand the risks they face. This includes online harassment, cyberbullying, cyberstalking, revenge porn, and other forms of online violence.
2. Educate women: Women need to be educated about the risks they face online and how to protect themselves. This includes teaching them about privacy settings, password management, and safe online behavior.
3. Provide safe online spaces: It is important to provide women with safe online spaces where they can express themselves without fear of harassment or violence. This includes creating moderated online forums and social media groups that are free from hate speech and other forms of online abuse.
4. Develop policies and guidelines: Organizations and institutions should develop policies and guidelines that promote women's safety and security in cyberspace. This includes policies on online harassment, cyberstalking, and revenge porn, as well as guidelines for reporting and responding to these incidents.
5. Encourage reporting: Women need to feel comfortable reporting incidents of online harassment and violence. Organizations and institutions should provide clear and confidential reporting mechanisms and ensure that those who report incidents are supported and protected.
6. Hold perpetrators accountable: Perpetrators of online harassment and violence should be held accountable for their actions. This includes legal action where necessary as well as social and cultural sanctions against such behavior.
7. Collaborate and coordinate: To guarantee the security and safety of women in cyberspace, many players, including the government, civil society groups, and the corporate sector, must collaborate and coordinate. This involves exchanging knowledge, tools, and best practices to make cyberspace a safer place for women.
8. Conduct a needs assessment: It is essential to assess the specific needs and concerns of women in cyberspace. This can be done through surveys, focus groups, and interviews. The information gathered can help in identifying the areas that require improvement and the measures needed to address the issue.
9. Raising awareness through campaigns and outreach programs can help educate women on online safety and security. It can also promote a culture of respect and accountability among users.

The Review of Contemporary Scientific and Academic Studies
An International Multidisciplinary Online Journal
www.thercsas.com
ISSN: 2583-1380 Vol. 3 | Issue No. 5 | May 2023 Impact Factor: 4.736 (SJIF)

10. Provide Training and Support: Training programs can be developed to equip women with the necessary skills to navigate cyberspace safely. Support services can also be established to provide emotional and legal assistance to victims of cybercrime.
11. Collaborate with Law Enforcement Agencies: Collaboration with law enforcement may aid in the identification and prosecution of cybercriminals. It can also convey a strong message to cybercriminals that they will not be allowed.
12. Encourage technological innovation: technological innovation can help in developing tools and systems that promote women's safety and security in cyberspace. For instance, the development of AI-powered chatbots can provide emotional support to victims of cybercrime.
13. Evaluate and Monitor Progress: It is essential to evaluate and monitor progress regularly to determine the effectiveness of the measures taken. This can be done through surveys, feedback forms, and the analysis of data on cybercrime incidents.

Overall, ensuring women's safety and security in cyberspace requires a sustained effort from all stakeholders. By adopting a multi-faceted approach, we can make significant progress in creating a safer and more secure cyberspace for women.

Results

Women's safety and security in cyberspace is a critical subject that has garnered more attention in recent years. Following are some major discoveries and figures related to the topic:

1. Cyber harassment and online abuse: A survey conducted by the Pew Research Center found that 41% of women in the United States have experienced online harassment, with 27% reporting that they have been stalked or sexually harassed online.
2. Online bullying: Girls and women are disproportionately affected by online bullying, with a study by Plan International finding that 58% of girls aged 15–24 have experienced online abuse, compared to 48% of boys.
3. Cyberstalking, which involves repeated and unwanted online contact or harassment, is a serious concern for women. A survey by the National Cyber Security Alliance found that 19% of women have experienced cyberstalking, compared to 9% of men.
4. Privacy and data security: Women may be more vulnerable to privacy violations and data breaches due to the amount of personal information they share online. A study by the Pew Research Center found that women are more likely than men to say they have experienced hacking attempts or unauthorized access to their online accounts.
5. Lack of representation: Women are underrepresented in the technology industry, which can contribute to a lack of consideration for women's safety and security in cyberspace. According to a report by the National Center for Women & Information Technology, women make up just 25% of the computing workforce.
6. Online dating safety: Women are particularly vulnerable to online dating scams and other forms of fraud. According to a report by the Federal Trade Commission, women are more likely than men to be the victims of a romance scam, with a median loss of $2,600.
7. Intersectional factors: Women who belong to marginalized groups, such as women of color, LGBTQ+ women, and women with disabilities, maybe at even greater risk of online harassment and cyber-attacks.

Overall, these results demonstrate that women's safety and security in cyberspace is a complex issue that requires attention from policymakers, tech companies, and society as a whole.

Discussion

As more individuals utilize the web and technological advances in their everyday lives, the problem regarding women's safety online becomes more pressing. With the growing number of cyber threats and the

The Review of Contemporary Scientific and Academic Studies
An International Multidisciplinary Online Journal
www.thercsas.com
ISSN: 2583-1380 Vol. 3 | Issue No. 5 | May 2023 Impact Factor: 4.736 (SJIF)

increasing sophistication of these threats, it is essential to focus on developing effective strategies to safeguard women's safety and security in cyberspace. Here are some possible future directions for addressing this issue:

1. Increasing Awareness: One of the most significant steps in ensuring women's safety and security in cyberspace is to increase awareness of the potential risks and threats. There is a need to educate women about safe internet practices, cyber-security measures, and the importance of protecting their personal information online.
2. Strengthening Legal Framework: Governments need to develop legal frameworks to protect women from cyberbullying, cyberstalking, and other forms of online harassment. The laws must be enforced to ensure that women are protected against online threats.
3. Developing Technology: Technology has the potential to play a crucial role in ensuring women's safety and security in cyberspace. There is a need to develop user-friendly and secure technologies that are accessible to women, particularly those who are vulnerable and marginalized.
4. Collaboration: Collaboration is essential to address the issue of women's safety and security in cyberspace. Governments, civil society organizations, the private sector, and other stakeholders need to work together to develop comprehensive and effective strategies to tackle cyber threats and promote women's safety.
5. Capacity Building: Capacity building is essential to enhance women's resilience to cyber threats. There is a need to provide training, education, and support to women to help them develop the skills and knowledge they need to protect themselves online.

In conclusion, the issue of women's safety and security in cyberspace is complex and multifaceted, and it requires a coordinated and collaborative effort from all stakeholders. By developing effective strategies, increasing awareness, and leveraging technology, it is feasible to make the internet a more secure and safer place for women.

Conclusion

The safety and security of women in cyberspace is an issue of paramount importance in today's digital age. While the internet has brought unprecedented access to information and opportunities for women, it has also created new avenues for harassment, abuse, and exploitation. Women face various forms of online violence, including cyberbullying, online stalking, revenge porn, and doxing.

To address this issue, it is essential to create awareness about the risks and challenges that women face in cyberspace. Education and training can help women protect themselves online and ensure that they are aware of the tools and resources available to them. This includes knowledge about privacy settings, secure browsing, and digital literacy.

In addition, it is crucial to hold perpetrators accountable for their actions. This requires robust legal frameworks that criminalize online violence against women and provide swift and effective remedies. Law enforcement agencies must be trained to handle cases of online harassment and abuse and work with digital platforms to take down offensive content.

Finally, it is vital to foster an inclusive and supportive online community that respects the rights and dignity of all individuals, regardless of gender. This may be accomplished by encouraging healthy social standards and developing secure online forums for women to tell their stories and seek help.

This paper provides a summary of the studies and literature on women's security and safety in cyberspace, with a particular emphasis on the many kinds of cyber-violence involving women and its consequences. Further study is required to understand the scope of the problem and create effective treatments to avoid and react to cyber-violence against women. It is also important to educate young people about the risks of online interactions and promote a culture of respect and safety online.

In conclusion, ensuring women's safety and security in cyberspace is an ongoing challenge that requires a comprehensive and multi-pronged approach. By raising awareness, strengthening legal frameworks, and promoting positive social norms, we can create a digital world that is safe and empowering for all women.

ISSN: 2583-1380 Vol. 3 | Issue No. 5 | May 2023 Impact Factor: 4.736 (SJIF)

References

1. Choudhary, Rajat. (2022). Cyberspace and Women- Dimensions of Cybercrime against Women in India. Design Engineering. 73-80. 10.17762/de.vol2022iss1.8685.

2. Saha, T. & Srivastava, Akancha. (2014). Indian women at risk in the cyberspace: A conceptual model of reasons of victimization. International Journal of Cyber Criminology. 8. 57-67.

3. Bagchi-Sen, Sharmistha & Rao, Raghav & Upadhyaya, Shambhu & Chai, Sangmi. (2010). Women in Cybersecurity: A Study of Career Advancement. IT Professional. 12. 24 - 31. 10.1109/MITP.2010.39.

4. Oyebisi, David & Njenga, Kennedy. (2019). ON WOMEN, CYBER-FEMINISM AND INFORMATION SECURITY: ASSESSING SECURITY THREATS BY GENDER.

5. Pradeep, S & Kanikannan, M & Meedunganesh, A & Leema, Anny. (2020). Implementation of Women's Safety System using Internet of Things. 258-261.

6. Mundhe, Dr. (2021). THE STUDY ON ISSUES AND CHALLENGES OF WOMEN EMPOWERMENT IN INDIA. 36. 41-46.

7. T, Srinivasa. (2017). Women Empowerment: Issues and Challenges. International Journal of Indian Psychology. 4. 10.25215/0402.092.

8. Poulpunitha, Dr & Kalidasan, Manimekalai & P., Veeramani. (2020). Strategies for Prevention and Control of Cybercrime against Women and Girls. International Journal of Innovative Technology and Exploring Engineering. 9. 2278-3075. 10.35940/ijitee.K2408.019320.

9. Kumar, Sanjeev & Priyanka. (2019). CYBER CRIME AGAINST WOMEN: RIGHT TO PRIVACY AND OTHER ISSUES.

10. Mokha, Anupreet. (2017). A Study on Awareness of Cyber Crime and Security. Research Journal of Humanities and Social Sciences. 8. 459. 10.5958/2321-5828.2017.00067.5.

11. Gupta, Shalini & Jaggarwal, Shiv. (2023). A DESCRIPTIVE STUDY ON CYBER CRIMES AGAINST WOMEN WITH REFERENCE TO CYBER SECURITY LAW. 9. 31-42.

12. Verma, Deepak & Verma, Vinodini & Pal, Anamika & Verma, Drishti. (2022). Identification and Mitigation of Cyber Crimes against Women in India. IJARCCE. 11. 220-227. 10.17148/IJARCCE.2022.11440.

13.F. Begum and S. Siddamsetti, "Blockchain-Based Smart Home Gateway using Secure Chaotic Hash Function," 2022 Second International Conference on Interdisciplinary Cyber-Physical Systems (ICPS), Chennai, India, 2022, pp. 5-10, doi 10.1109/ICPS55917.2022.00009.

14.Siddamsetti, S., Srivenkatesh, M. (2022). Implementation of blockchain with machine learning intrusion detection system for defending IoT botnet and cloud networks. Ingénierie des Systèmes d'Information, Vol. 27, No. 6, pp. 1029-1038. https://doi.org/10.18280/isi.270620

Acknowledgements: Prof. Neil Gogte, Director, Neil Gogte Institute of Technology, Stephen Lobo, Co-founder, CyberGuard360, NC, USA for their support.

Conflicts of Interest: "The authors declare no conflict of interest."