Musik in bayern

ISSN: 0937-583x Volume 88, Issue 10 (Nov -2023)

https://musikinbayern.com

DOI https://doi.org/10.15463/gfbm-mib-2023-*256*

Digital Solution for Cyber Crime against Feminine Victim

[1]Gomathy M
Research Scholar,
School of Computing Sciences,
Vels Institute of Science, Technology and Advanced Studies (VISTAS),
Chennai, India
marimuthu.gomathy@gmail.com

[2]Dr. K. Kalaiselvi,
Professor,
School of Computing Sciences,
Vels Institute of Science, Technology and Advanced Studies (VISTAS),
Chennai, India
kalairaghu.scs@velsuniv.ac.in

To Cite this Article

Gomathy M , Dr. K. Kalaiselvi ,” Digital Solution for Cyber Crime against Feminine Victim”

Musik In Bayern, Vol. 88, Issue 10, Nov 2023, pp225-256

Article Info

Received: 24-10-2023   *Revised: 04-11-2023*   *Accepted: 14 -11-2023*   *Published: 24-11-2023*

***Abstract*- In this contemporary era, internet has become the mode of communication and has changed the life style of individuals with advancement in technology. Modern electronic gadgets made us more dependent on it directly or indirectly for most of the people regardless their age [1]. The tremendous attain of the internet, the speedy unfold of mobile data, and consequently the extensive use of online forum has paved the way for online Crime. Cybercrime and victimization on female gender are excessive and it poses as a serious threat to the safety of an individual as an entire. Smart devices with web connections and social media platforms supports to explore huge information including objectionable materials. These offensive contents include pornography, cyberbullying, sexual abuse and threats, ferocity, gambling endanger more among ladies and youngsters on the net [2]. These unsolicited information’s has an impact to increases the vulnerability of crime against women and among younger age group children including adolescents. Cyber parental control is a method that afford a safe environment in the internet world for individual in particular women and youngsters to work in a controlled atmosphere for accessing internet with a healthy soul and mind. Considering the above context, the objective of this systematic review is two-fold, (1) To explore and understand various women related issues due to use of virtual platform, and (2) To analyse and propose an effective system for cyber parental control, the probable digital solution to reduce the vulnerability against cybercrime in specific among the feminine victim.**

Keywords: Adolescents, cybercrime, parental control, systematic review, victimization, women.

I.INTRODUCTION

Cybercrime is described as any unlawful act committed through computers or other digital devices to commit or facilitate the commission of crime that causes detrimental effect on individual or organization or to the society. Typically, cybercrimes can be divided as Crimes that focus on pc networks or devices without delay or Crimes facilitated through virtual networks or gadgets. Commonplace styles of atrocities in cyber world are cyber pornography, identification theft, cyber defamation, credit score card theft, cyber blackmailing on sexually specific content, facts leakage, cyber phishing, cyberstalking.

A. Cyber Crimes against Women

The cyberworld has provided a furnished space wherein ladies and children can savor their freedom of expression, sharing of personal information and privacy of communication. However, cybercriminal might also make use of those treasured records to impose violence against them. Furthermore, various types of electronic gadgets connected with internet are utilized for implementing illegal activities that includes executing several cybercrimes like stalk, abuse, traffic, intimidate and humiliate women and young girls is palpable not only in underdeveloped countries but also in developing and developed countries [3]. Additionally, in a latest document, submitted by National Crime Records Bureau (NCRB) in India, it highlights that cyber-crime cases have escalated by means of 11.8% in 2020 as compared to preceding year. Specifically, Cyber-Crime instances towards women have elevated by 24%and occurrences against children have increased by 26.1% in step with Crime in India – Statistics Volume II by NCRB [4]. The privacy and personal protection of the women and growing young adults are under risk with these mounting issues of cybercrime in the online world. The most common and often reported assortments of cyber-crimes against ladies encompasses

- **Cyber Stalking** It's the utilization of the online platform to stalk or harass a person , group, or enterprise to threaten or annoy them in virtual way inclusive of email, mobile messaging ,messages posted to a discussion group or in an online forum. Cyber stalkers utilize the obscurity afforded with the aid of the internet to stalk or annoy their victims, from time to time without being stuck, punished or maybe detected. The harasser primary purpose may be to monitor the victim's online activities, track the victim's locations, intimidate, frighten, control or blackmail the victim.
- **Cyber Phishing** It's miles an attempt in social engineering platforms that are used to steal consumer facts, like login credentials, credit score card range, bank records. In this form of cybercrime, the victims are communicated with the aid of electronic mail, telephone or message via someone posing as a relied entity to dupe the victim to activate the records. After that, the recipient is deceived towards activating a malicious hyperlink, which could lead to the malware being activated, the freezing of the gadget owing to a ransomware assault or the unveiling of confidential facts [5].
- **Cyber pornography** It is the dissemination of pornographic information's with Internet as medium. Information's can be in the form of pictures, textual content, audio digital pictures.
- **Harassment through electronic mail** It consist of extorting, threatening and consistent transmitting of abusive letters or embarrassing mails in anonymous names. On-line harassment is a canopy to describe how internet is used to annoy, threaten or maliciously embarrass another party via e-mail aimed at a person, a set of humans, or even a corporation. E-harassment is similar to the letter harassment by posting the information from fake ids or cloned profiles in order to harass, humiliate, or denigrate female netizens.
- **Morphing-** In this type of cyber-crime, the authentic photo is morphed with the help virtual tools into unsolicited photographs. Typically, women are affected due to this kind of techniques. The cyber criminals down load images from numerous social web sites through faux or actual profiles and then morph them with the intension to blackmail them or their family with the aid of threatening to put up the morphed snap shots in targeted structures like Facebook and pornographic web sites.
- **Defamation-** Cyber defamation approach is publishing of fake declaration about a person in cyberspace which could injure or demean the recognition of that individual. The reason of making defamatory assertion is to bring down the reputation of the person. Normally it happens, when a person posts defamatory information about an individual on internet site or sends emails containing offensive facts to all that of individual's pals.
- **Email spoofing** - This approach is a forgery of an electronic mail header. The message seems to have obtained from reputed source These usually used with the intension to make the victim to open an email with the trust that email has been sent by a legitimate source. By altering aspects of the e-mail, such as the header, senders address, return-route, and reply-To fields, adverse users could make the e-mail seem as that it's from the real sender.

- **Cyber Impersonation:** It is an act of pretending to be another person online for the purpose of entertainment or fraud. Pretending to be a person else and sending or posting material to get the victim in hassle or harm their recognition. Furthermore, the criminals create a fake profile in victim's identification in order to annoy, threaten or defraud them. In addition to it, the offenders additionally make use of the victim's identification to collect all of the confidential records about them from the virtual contacts.

II. REVIEW OF RELATED RESEARCH

- Farzana Quayyum et.al. summarized the contemporary studies, analysis and practises on the state of cybersecurity awareness, with a focus on children. The author identifies that the game-based learning helps to create cyber security awareness among children. Warning and nudging mechanism also has significant effect in creating alertness among youngsters [6].
- Saurabh Dubey discussed upon the various types of cybercrimes that are inflicted upon women in India. The author has also briefly analysed of the legal rights of women to protect against cybercrime. Various challenges that are experienced by women in receiving the legal rights were also discussed. The paper gives clear idea on Cyber Crime Prevention Against Women and Children (CCPWC) scheme inducted by means of the Government of India for an online cybercrime reporting platform. The articles also discuss about method of tracing the cyber stalkers by locating their IP address [7].
- Rahman N. A. A et.al. explored the importance to versed about the hazards associated with online activity and the strategies that stakeholders may use to increase cyber security education in academic institutions. The article also highlights the crucial role for schools to educate and gain knowledge on issues related cybersecurity as well as methods to organize cybersecurity education and awareness programs (GENCYBER). The author could able to identify that most significant risk like cybersex is not given importance by school teacher, parents, Government in cybersecurity education [8].
- Dr. Jobi Babu et.al. shows the mind-set and women's knowledge of cyber sexual offences underneath the frame of IT Act 2000.The author also explains that the level of awareness can be increased by experts assist in providing assertive therapy, legal awareness to the women in cyber space. The author specifies that Women were not aware about the laws made for preventing these problems and most of them ignore the issue or divert the problem differently. The Article also highlights that exposure to new gadgets also increase in the number of crime rate among women [9].
- Mohammed Daffalla Elradi et.al. analysed the level of cyber security awareness among professors and students in Sudanese college. The author explains in the paper different types of cyber security awareness methods. From the data collected the author identified that maximum of the members has been aware about the importance of preserving themselves and being comfortable in on-line world. However, the realistic implementation in the mechanism of protecting mindset maintained through students and staff members is substantially unsecure and exposes them to cyber dangers easily [10].
- Mansi et.al. explains some of the remedial measures to protect cybercrime against women were suggested. The author also specifies the use of ISP and SMTP to trace and detect the cyber stalking and cyber email spoofing. The paper also insists to regulate the legislation in cybercafes more tightly for the safety women and girls in cyber space. In this article the author could find that most of the Cybercrimes against women remain a lightweight problem and there is no support to curb morphing, email spoofing [1].
- S.Poulpunitha et.al. investigates the concerns and problems of cybercrime against women and girls in order to demonstrate preventive approaches and tactics to tackle the problem with the support of a unified force. From the data collected, the author highlights the various factors that have major impact on cybercrime among women and younger generations. The paper also specifies that IT Act 2000 in India has not included the exploitation and threat to the safety of women [11].
- Shakila Akhter, has inspected the prevalence of exploitation among grownup ladies in cyberspace and from the collected investigation reports, the article has exposed that greater number of ladies are cyber sexually abused compared to men. The important risk factors identified were age, uncontrol balance using and exposing details in social media sites. due to cyber victimization emotional misery, pathological ruminations and despair are pronounced as outcome that has to be addressed to safe guard women victimization in cyber world [12].

- Dr. P. Sritharan, explains about the nature and the extent of cybercrime victimization of women, reporting behavior of the victims and the victim 's attitude towards the police. From the data collected the author raised awareness measures on using the major social media platform and also showcased various methods how women are easily victimized in social media platforms. The results also highlight the negative impact on cops in some cases, towards the women cyber victims [13].
- Ritu Dubey Tiwari, has given a clear idea on cybercrimes, the classification and different types of cybercrimes, which will affect the children. Author has also presented various theories like gratifications theory, protection motivation theory, social learning theory and rational choice theories which will make the framework for protection of children against cybercrime. The study reveals that the parents are not having much knowledge about the different types of Cybercrimes and not giving importance to its consequences [14]
- Sreehari A et.al. highlights the consciousness level of e-crime amongst college students in Kochi and also analyzed the knowledge about various authorities' intrigue and programs obtainable to fight against online crimes amongst college students. The paper discussed about numerous cybercrimes and cybers legal guidelines in India to be applied to cut down and fight against the crime. The authors have also suggested various security measures to avoid digital crime. From the data analyzed, the author revealed that most of the students are aware only on hacking in cybercrime compared to other types and form of cyber-attack [15].
- Ahmed E. Arafa et.al. identified the level of vulnerability to cyber sexual harassment amongst the students of female gender in Beni-Suef college and explore the associating elements. The article revealed that age and every day hours of internet use have been capability hazard elements. Moreover, anger was expressed as the main psychological key risk among the female victims [16].
- Dr. Monika Jain, conducted a predictive evaluation of cyber-crimes towards women in India and legal guidelines that prohibit one from cyber victimization in trendy and in particular amongst girls. The paper explains the IT Act2000, various sections used to curb cybercrime against women. The author additionally explains the online protection vulnerabilities in opposition to women [17].
- Shefali Singh explained regarding online crimes and numerous sorts of e-crime in opposition to women with examples in and round India. Various IPC sections regarding cybercrime were also discussed in this paper. The author could identify that the younger generations were unaware concerning the terrible facet of the on-line world which is the foundation reason of most of the cybercrimes [18].
- Senthilkumar et al. conducted a web - based questionnaire of 500 Tamil Nadu university graduates on various cyber security threats. The findings revealed that 70% of the people were completely aware of protection methods to obstruct from virus assaults and participant has the practice of utilizing updated antivirus software program. On the other hand, the final 30% of participants had been reported the use of outdated antivirus software program and One-fifth of them had never used antivirus software before [19].
- Sarmistha Neog, has made an attempt to have a look at the diverse issues associated with victimization of girls in on-line world and tried to map out the impact of this digital Crime in their physical life give rise to trauma, fright, melancholy, molestation, denigration and so forth. The writer has analyzed and evaluated numerous cyber associated laws in worldwide as well as countrywide discussion board and highlighted how it can be utilized to shield women in our on-line world [20].

III PROPOSED METHODOLOGY

A. Parental Control

The majority of today's youth are heavily reliant on the internet in their daily lives. As a result, it is critical to take necessary steps to ensure that the digital public sphere is a safe environment for all individuals, particularly women and young girls [21] as well as to overcome cognitive disorders [22]. Therefore, it is crucial to take security precautions to overcome it. To prevent cybercrime and abuses against women numerous software applications, help lines, antivirus software, and fire walls can be employed in the system. One leading solution is to block these sites /videos/images to avoid popping of unsolicited information. To handle such issues and provide a secure, controlled internet environment, feasible key is to depend on parental control. Parental Control in the electronic devices not only helps to monitor remote device but also restricts one in visiting inappropriate sites or stumble upon unsolicited information's in the form of messages, videos or images.

B. Method

In this section a methodology is proposed to enhance the parental control to protect individual from visiting inappropriate information's in digital world. For text classification and image recognition, a hybrid model NBLR model using both Naive Bayes (NB) and Logistic Regression (LR) models are utilized. The performance based on the variants features are mentioned here.

a) Naïve Bayes (NB) Model

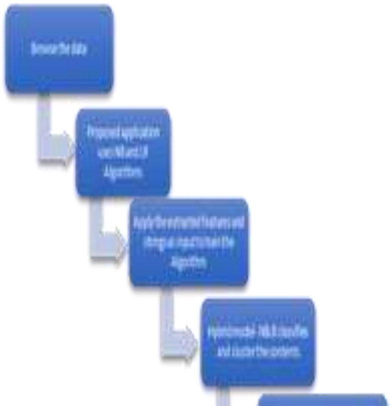
Naive Bayes works best with categorical response variable rather than data series. It outperforms with even fewer independent data sets. It is more effective for snippet data than lengthy records. The classifier assigns the same degree of significance towards each feature throughout classification. The parental control application created with Naïve Bayes classifier algorithm can easily filter the documents containing abusive text based on their age criteria. Moreover, Naive bayes performance on snipped text is more accurate. Using TDM (Term Document Matrix), it is possible to conceal the vulgar context while exploring online. As a result, it is feasible to restrict certain media files by setting an age requirement and avoid displaying or popping malicious content while browsing. This model's performance level indicates 91 percent accuracy.

b) Logistic Regression (LR)Model

Logistic regression is a classification algorithm that uses supervised learning to predict the likelihood of a response variable. It is convenient to identify the optimal variables for text classification. Moreover, this algorithm much more efficacious for longer text than short phrases or documents for classification. It employs a word2vec model to convert documents into feature vector, with each term in the document designated a scoring rate. As a result, this parental control, which employs logistic regression, is capable of blocking controversial content, pornography sites, and photographs evoked by error. The overall performance of this model using LR is evaluated to be 85 percent accurate.

c) Proposed Hybrid Model-NBLR Model

In this proposed methodology, we combined and discriminative and generative classifiers and presented a model with a modified version in which a Logistic regression is built over Naives Bayes. The proposed Hybrid -NBLR model employs log-count ratios as wavelet coefficients and demonstrates that it is an excellent performer throughout all types of tasks. The NBLR model employs TDM and word2vec the features of the Logistic regression classification model and the Naives Bayes classifier, resulting in a hybrid model with high predictive power. The developed hybrid model-NBLR employs the Bidirectional Encoder Representations from Transformers (BERT) feature, which aids the design deal with vague terms in the message and predicts phrases even in a blank document. With these features, the proposed NBLR model aims to reinforce parental control by restricting not only offensive, adultery-related websites, but also by camouflaging derogatory language showcased inside any documents while being in virtual worlds. The accuracy of this hybrid model-NBLR, is 93 percent, which is higher than the accuracy of NB model and LR model. The following figure gives a clear idea on working of the proposed model.


Browse the data
Proposed application uses NB and LR Algorithms
Apply the extracted features and strings as input to train the Algorithm
Hybrid model- NBLR classifies and cluster the contents.

d) Design and Implementation

The esoteric design of the proposed system is presented and discussed in this section. The internet as a source that has been used to transmit data as well as services demands from a device to a domain controller and to revert back information to the user. The following picture shows the block diagram of developed hybrid model -NBLR Parental Control Application

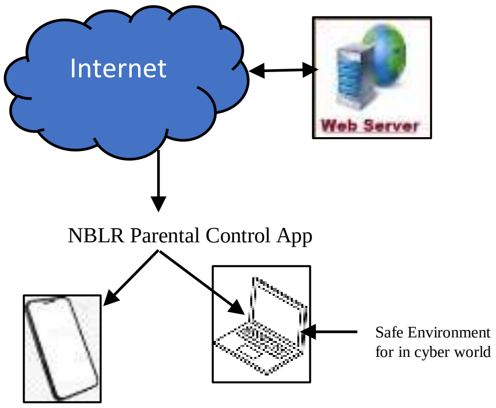


Fig.2. Block Diagram of NBLR Model

AND DISCUSSION

The proposed hybrid model -NBLR - to improve parental control is created by combining Logistic Regression and Naive Bayes, two machine learning classification algorithms. The NBLR model is used in the analysis and filtering of obnoxious contents. The model contributes to the mechanism for governing and analysing women's and adolescent online usage which is a critical tool in the prevention of cybercrime. We analysed and compared the performance of the classifier machine learning algorithms Logistic Regression (LR), Naives Bayes (NB) and the proposed hybrid algorithm (LRNB) to showcase their performance in predicting offensive contents using classification accuracy in Fig.3. When the machine learning algorithms are evaluated, Logistic Regression has an accuracy of 85 percent, Naive Bayes has an accuracy of 91 percent, and the proposed LRNB algorithm has an accuracy of 93 percent.LR and NB classifiers have been consistently demonstrated to be a reliable mechanism for Text classification and interpretation The hybrid algorithm (LRNB) is used in the development of parental control to enhance its features has shown greater accuracy compared to the other machine learning algorithms. The proposed application functions as a digital solution for combating cybercrime, particularly among female victims, because it can easily predict unsolicited contents and images and block them before they can be viewed by the person.

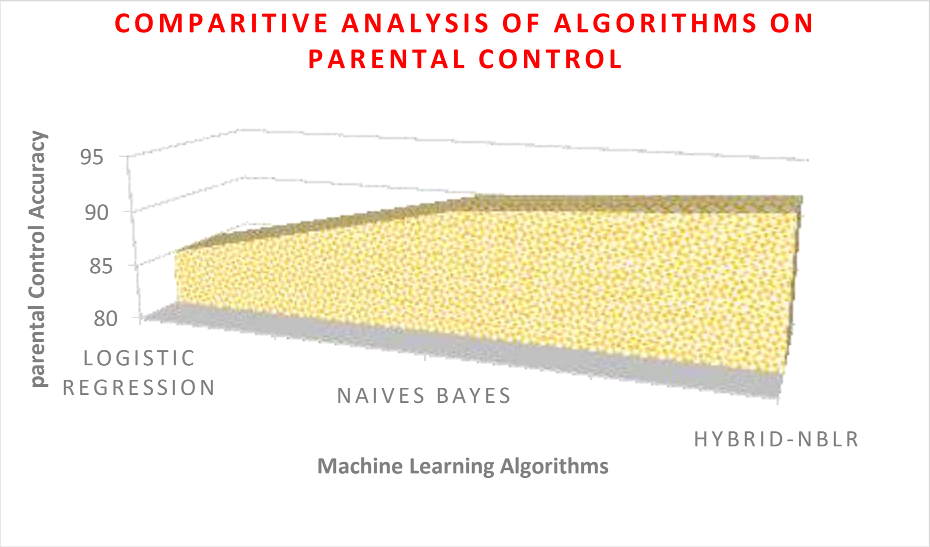


Fig.3. Comparative Analysis of Algorithms on Parental Control

V.CONCLUSION

The rapid rise of digital communication has changed the way people interact with social media platforms, academic procedures, and their desire for recreation. Despite the fact that the online technology has plethora of benefits, the cyberspace is likewise a vicinity for exploitation and victimization of women and female adolescents. This paper gives a clear idea about various cybercrime against feminine victim and also provides the prevention strategies to be followed. Among the protection and prevention strategies suggested, parental control is one technique to overcome cybercrime which work through monitoring and restricting their online behaviours either through self-regulation or restricting inappropriate information's. The paper proposes a hybrid model that improves parental control applications which can provide individuals with a safer cyber space environment. The developed application through machine learning algorithm is helps to reduce risk through filtering and blocking offensive programs in cyber space in an efficient manner.

Reference

[1] Mansi, Pukhraj Agarwal, Cyber Crime: Women Combating with the Negative Effect of Technology in the Era of Globalisation,2020, International Journal of Management and Humanities (IJMH) ISSN: 2394-0913 (Online), Volume-4 Issue-7, March 2020

[2] A preliminary study of cyber parental control and its methods ,HHM Altarturi, NB Anuar - 2020 IEEE Conference on Application, Information and Network Security (AINS)

[3] A Munyua, M Mureithi, G Githaiga, Women and cybercrime in Kenya: the dark side of ICTS,2010,Available at kictanet.or.ke

[4] Aishwarya Acharya,2017, Available at https:// www.femina.in/ relationships/parenting/ impact-of-cybercrimes-how-women-can-stay-safe-from-cyber-threats-212417.html

[5] Saurabh Dubey, Cyber Crimes and Cyber Laws: A Perspective Women Victimization, 2021, IJARSCT

[6] Farzana Quayyum , Daniela S. Cruzes, Letizia Jaccheri , "Cybersecurity awareness for children: A systematic literature review ",2021, International Journal of Child-Computer Interaction

[7] Saurabh Dubey," Cyber Crimes and Cyber Laws: A Perspective of Women Victimization",2021, International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

[8] Rahman N. A. A, Sairi I. H., Zizi N. A. M., and Khalid F.," The Importance of Cybersecurity Education in School ",2020, International Journal of Information and Education Technology

[9] Dr. Jobi Babu & Dr. P Jayakumar," Attitude and Awareness of Women About Cyber Sexual Offences: An Area of Social Work Intervention ",2020, Studies in Indian Place Name, ISSN: 2394-3114

[10] Mohammed Daffalla Elradi Altigani Abd Alraheem Altigani Osman Idriss Abaker, Cyber Security Awareness among Students and Faculty Members in a Sudanese College,2020, Electrical Science & Engineering | Volume 02

[11] S. Poulpunitha, K. Manimekalai, P. Veeramani," Strategies to Prevent and Control of Cybercrime against Women and Girls ",2020, International Journal of Innovative Technology and Exploring Engineering (IJITEE)

[12] Shakila Akhter," Cyber Victimization of Adult Women", 2020, www.diva-portal.org/smash/get/diva2:1486357/FULLTEXT01.pdf

[13] Dr. P. Sritharan," Cybercrime Victimization - A Study Among Working Women in Chennai City",2019, SOCIAL MEDIA ADDICTION Disconnect to Connect, ISBN: 978-81-934473-8-3

[14] Ritu Dubey Tiwari," An Analytical Study on The Awareness of Parents About Cybercrimes Against Children ", 2019, International Journal on Transformations of Media, Journalism & Mass Communication

[15] Sreehari A, K. J Abinanth, Sujith B, Unnikuttan P. S, Mrs.Jayashree," A Study of Awareness of Cyber Crime Among College Students with Special Reference to Kochi ", 2018, International Journal of Pure and Applied Mathematics

[16] Ahmed E. Arafa, Rasha S. Elbahrawe, Nahed M. Saber, Safaa S. Ahmed, Ahmed M. Abbas," Cyber sexual harassment: a cross-sectional survey over female university students in Upper Egypt ", 2018, International Journal of Community Medicine and Public Health

[17] Dr. Monika Jain," Victimization of Women Beneath Cyberspace in Indian Upbringing ", 2017, Bharati Law Review, April – June, 2017

[18] Shefali Singh," Cybercrimes Against Women in India ", 2017, Journal of Legal Studies and Research

[19] Senthilkumar K., Easwaramoorthy S. A survey on cyber security awareness among college students in Tamil Nadu. IOP Conference Series: Materials Science and Engineering, Volume 263, Computation and Information Technology, Tamil Nadu, 2017: 1-10

[20] Sarmistha Neog," Legal Treatment of Cyber Crime against Women- Global and National Perspective ",2015, The Legal Frontier.' Research Journal of USLR, USTM

[21] European Institute for Gender Equality (2017), "Cyber Violence Against Women", Available at https://eige.europa.eu/publications/cyber-violence-against-women-and-girls.pdf

[22] Stanley Clark," The Psychological Impact on the Lives of Cyber-Attack Victims",2017, Available at https://paintedbrain.org/blog/the-psychological-impact-on-the-lives-of-cyber-attack-victims