A Qualitative Research on the Impact and Challenges of Cybercrimes

V Krishna Viraja and Pradnya Purandare*
Symbiosis Centre for Information and Technology,
Symbiosis International (Deemed University), Pune, Maharashtra, India
Email: pradnya@scit.edu*

Abstract. We are in the digital era where we cannot imagine our lives without the Internet. Technology has become an integral part of our daily routine, and with the significant rise in technology, we see huge growth in cybercrimes. The use of information is increasing every day with the advent of more social media platforms that utilize millions of data per second globally. These data include sensitive information such as trade secrets, privacy, and security issues. The number of crimes is increasing day by day, and these cyber crimes can impact an individual, an organization, or even a whole nation. The research study aims to spread awareness about cybercrimes by offering a detailed analysis of the awareness, impact, and challenges to anyone vulnerable to cybercrime. The methodology adopted to study and analyze the impact and challenges caused due to cybercrimes is qualitative research. On a concluding note, the study will present suggestions to overcome the challenges and talk about the research's future scope.

Keywords: Cybercrime; Internet; Challenges; Technology; Impact; Awareness

1. Introduction
Cybercrime is the world’s biggest industry when it comes to criminal growth [1]. Any criminal activity that involves a computer, networked device, or a network is termed a cybercrime. Some cybercrimes are performed to create profit for cybercriminals; some cybercrimes are perpetrated directly against computers to harm or disable them, whereas others are using computers or networks to spread malware, illicit information, photos, or other content [2]. The world is seeing an escalation in cybercrimes year by year, both in size and sophistication as the technology is advancing rapidly, and there is a huge need to surmount the challenges that are imposed because of these crimes [3]. The paper presents the details of these crimes’ impact and challenges and discusses suggestions to the challenges.

2. Literature Review
The paper proposed presents the results of the use of Information Technology by organized crime groups. The paper discussed low-tech and high-tech cybercrimes using IT. As further research, the impact that these crimes cause can be studied. The method gave a detailed study of the youth perception on cybercrime in South Asia. The authors developed a close-ended and open-ended questionnaire for the research purpose. The paper is limited to youth and not any other age groups. Further research can be studied among different age groups belonging to different professions.
The authors have given a brief study on five top cyber frauds and cybercrime categories. However, as further research, the impact and challenges these crimes cause can be studied. The author presents a narrow sphere of types of cybercrimes and threats that it brings to small businesses. Further study can be done on the impact that these threats will bring. The author reviewed the threats of emerging cybercrimes and suggested measures to minimize cyber fraud. These studies can be further extended to analyzing the impacts that develop due to cybercrimes. The research paper conducted an analysis of cyber-attacks and determining patterns and trends in cybercrime. A gist of the impact that cybercrimes cause has been studied. However, a detailed study is not done. The countermeasures that IT organizations can take have been mentioned. A study of the reasons why cybercrimes are increasing in India has been studied in their research paper. The challenges have not been clearly defined. Their research focused on Social Engineering, one of the types of cybercrimes. The challenges to organizations because of cybercrimes are limited to psychological variables.

In the paper the author has given a very detailed introduction of cybercrimes' evolution and stated a few difficulties or challenges in general. Along with that, the types of cyber jurisdiction are also explained. The research paper showed a survey of cybersecurity in the context of Confidentiality, Integrity, and Availability and proposed a new taxonomy of various cybercrimes. They have done a detailed classification of cybercrimes, although the challenges proposed are limited. The authors in their paper mentioned the issues of cybercrimes and the possible ways to reduce them, however, the challenges have not been mentioned.

In his research studied in detail the various types of cybercrimes. The author cites a few challenges that organizations face because of cybercrimes. It explained Personally Identifiable Information (PII) and how it exposed to different cyber threats. The study can be further extended to studying the challenges of disclosing PII. In the paper the author tells in detail what Phishing is and how Phishing attack affects an organization. Here they have taken PayPal as an example. The paper also explained the impact Phishing causes on an organization. The research paper proposed a model and suggested a hypothesis on employee's fear of cybercrimes and their compliance with the organization's Information Security policies. This could be considered as an impact that cybercrimes cause on the organization. It gave the details of spamming, its formats, discussed the details of why it is prominent and its challenges. It discussed cyber harassment among women who use social media. The author examined the extent of harassment experienced by women and presented the various behaviours that put a woman at risk. It examined the costs of cyber-attacks along with their causes and performed a descriptive analysis of cyber events.

2.1 Literature Review Summary

Table 1 consists of the author's name, the title of the paper, its source, and gaps found or future scope. The search criteria are as follows: (i) Period: 2015 – 2020; (ii) Search terms for the data sources [4] - IEEE, CORE, ACM, Google Scholar are the following: Cybercrimes, Cybercrime challenges, Cybercrime challenges to Organizations, Cyber frauds, Cybercrimes in businesses, Cybercrimes impact, Impact of Cybercrime, Types of Cybercrimes, Impact and Challenges of cybercrimes, Challenges of cybercrimes. Table 1 shows the Literature Review details.

The below papers are selected out of the 550 overall hits as these papers are more related to the current topic chosen for the study.

| Author | Title of the paper | Source | Gaps found/Future scope |
|--------|--------------------|--------|-------------------------|
| E. Rutger Leukfeldt, Edward R Kleemans, Edwin W. Kruijsbergen and Robert A. Roks | Criminal Networks in a digested word: on the nexus of borderless opportunities and local embeddedness | CORE | Impact and Challenges can be studied |
| Authors | Title | Conference | Keywords |
|---------|-------|------------|----------|
| Kamruzzaman, Md Ashraful Islam, Md Shahidul Islam, Md Shakhawat Hossain, Md Abdul Hakim, Md | The plight of Youth Perception on Cybercrime in South Asia | Google Scholar | The perception of different age groups can be further studied. |
| Rajesh Kumar Goutam Deepak Kumar Verma | TOP 5 Cyber frauds | Google Scholar | Impact and Challenges can be studied |
| Brenda Van Rensburg Tim Kennedy | Online vulnerabilities facing small business today | Google Scholar | Various types of cybercrimes and the impact of the threats mentioned can be studied. |
| Kumar Harsh, Tanya Singh, Pramod Kumar Singh | Emerging threats of cybercrimes | Google Scholar | Impacts of the threats can be studied |
| Andreea Bendovschi | Cyber-Attacks – Trends, Patterns, and Security Countermeasures | Google Scholar | A detailed study of the impact of the attacks can be studied |
| June Iqbal Bilal Maqbool Beigh | Cybercrimes in India: Trends and Challenges | Google Scholar | Challenges are not clearly defined |
| Nabil Y Conteh and Paul J. Schmick | Cybersecurity: risks, vulnerabilities, and countermeasures to prevent social engineering attacks | Google Scholar | Challenges were limited to psychological variables only. |
| Mr. Kush Kalra | The emergence of Cybercrimes: A challenge for the new millennium | IEEE | Impacts can be researched. |
| Harmandeep Singh Brar and Gulshan Kumar | Cybercrimes: A Proposed Taxonomy and Challenges | Google Scholar | Limited challenges have been proposed. |
| P. K. Paul & P. S. Aithal | Cybercrime: Challenges, Issues, Recommendation, and suggestion in the Indian context | Google Scholar | Challenges are not clearly defined |
| Dr.P.B.Pathal | Cybercrime: A Global Threat to Cyber community | Google Scholar | Impacts can be studied further. |
| A.J. Burns Eric Johnson | The Evolving Cyberthreat to Privacy | IEEE | Challenges of disclosing PII can be studied |
| Brad Wardman | Assessing the Gap: Measure the Impact of Phishing on an Organization | Google Scholar | The threats and risks caused can be studied further research. |
| Jaffar Ahmad Alalwan | Fear of Cybercrime and the Compliance with Information Security Policies: A Theoretical Study | ACM | Challenges can be studied further. |
| Mamoun Alazab | Spam and criminal activity | Google Scholar | Impacts can be researched. |
| Sloane Burke Winkelman Jody Oomen-Early Ashley D. Walker Lawrence Chu Alice Yick-Flanagan | Exploring cyber harassment among women who use social media | Google Scholar | The various impacts caused can be studied. |
| Sasha Romanosky | Examining the costs and causes of cyber incidents | Google Scholar | The effects of these incidents can be further researched. |

### 3. Research Methodology

The study adopts a systematic questionnaire of the qualitative type that is developed containing questions targeting different age groups that belong to different professions to understand the awareness, impact, and challenges of cybercrimes [5]. The questionnaire is designed to collect qualitative data, and the respondents answered most of the questions in the form of a Likert scale. The research methodology applied is qualitative data analysis of grounded theory.

A google form had been created consisting of questions, and data were collected from 110 respondents of different age groups to analyze the impact and challenges of cybercrimes [6]. The purpose of conducting this survey is to collect information that will bring the expected outcome and give a deep understanding of the current situation. The questions in the survey included personal details of the respondent like Age, Gender, Profession, Organization they worked or working in, Designation, and Place of stay. To maintain the respondent’s privacy [7], their profession, organization, and designation were not mandatory to answer, and they were also given prefer not to say option while choosing their gender.

### 4. Conceptual Model

To understand the impact and challenges of cybercrimes, it is equally important to know their causes and effects [8]. No crime occurs without a cause, and it leaves an effect once the attack is done. The causes and effects are depicted in Figure 1.

#### 4.1 Causes of Cybercrimes

Economically motivated – Most of the cybercriminals are motivated because of money. As these criminals hide behind the network, there is less threat of getting exposed, hence they demand huge financial rewards from the targets by engaging in malware, Phishing, identity theft, or other fraudulent activities [9].

Personal factors – Sometimes, cybercrimes occur because of the personal emotions of cybercriminals. For example, a disgruntled employee can commit a crime by injecting a virus into a system, or a person can create a fake account and send their friend threatening messages on email or social media and demand money due to a fight that happened in the past, and he seeks revenge [10].

Ideological Motivators – Cybercriminals have moral, ideological, or some other ethical reasons to perform cyber crimes by damaging networks or disrupting the computer equipment. By performing these activities [11], the attacker expresses grievances against individuals, organizations, or even governments.
4.2 Effects of Cybercrimes

Financial losses – Individuals, organizations incur financial losses because of cybercrimes. When a cybercriminal has access to sensitive company information, he uses this information to gain money [12]. The cybercriminals demand money by threatening the company that the information will be misused or leaked online. Individuals incur losses when they become victims of fraudulent activities like job fraud, charity fraud, get-rich-quick schemes, or other frauds.

Reputation loss – The Company’s reputation will be at stake when its clients' sensitive information is compromised because of a security breach, and the customers will lose confidence in the company [13].

5. Results

The questionnaire was filled by 110 respondents, out of which 42 are females, which constitutes to 38%, and 67 are males, which constitutes to 61%. Only one respondent did not reveal their gender, constituting to 1%. It is depicted in Figure 2, and the percentage of the respondents belonging to various professions is depicted in Figure 3.

The respondents gave their answers on a five-pointer Likert scale (1 = Least aware to 5 = Highly aware). From the responses, 23 of 110 respondents marked 5, 37 out of 110 marked 4, 17 out of 110 marked 2, and 7 respondents marked 1. This shows that the majority of the respondents belonging to different groups have awareness about cybercrimes.

It is found that 40 out of 110 marked 5, 33 respondents marked 4, 3 gave a 1, and 10 out of 110 respondents belonging to different age groups marked 2 when asked about their likeliness to read an article on cybercrimes [14]. The answer was given on the Likert scale (1 = Least likely to 5 = Highly likely). It shows that majority of the respondents have an interest in reading about cybercrimes.

For the statement that says the individual gives their personal information or One Time Password to a stranger over a call or a person who claims to be a bank employee, it is observed that 95 out of 110 respondents of different age groups gave their answer as 1 [15]. The answers were given on Likert scale (1 = Strongly disagree to 5 = Strongly agree) and 86 out of 110 respondents of different age groups marked 1 when asked if they click on an unknown source and give personal details if it claims to help someone in need/give reward/provide a job offer.
Individuals were asked a question on how private they would like to keep their information [16]. The answers were taken on the Likert scale (1 = Least private to 5 = Highly private). A total of 49 out of 110 respondents marked 5 and 13 marked 1.

A total of 40 respondents marked 5, and 15 individuals gave their answer as 4, and 32 respondents marked 2 for a statement that says the individual would log out of social media or any other sites every time they log in [17]. The answers were given on a Likert scale (1 = Strongly disagree to 5 = Strongly agree).

It is observed that 70 out of 110 individuals marked 1 to the statement that it is safe to share email account passwords with a close friend over the phone. The answer was recorded on the Likert scale (1 = Strongly disagree to 5 = Strongly agree).

5.1 Impact
A total of 81 respondents have been a victim of cybercrime once. Out of these, 31 (38%) are females (age group 18-24) and 49(61%) are males (age group 55-64). It is found that four females and 11 males have been a victim of cybercrime for 2-5 times, while seven females and seven males out of 110 have 'never been a victim of cybercrime. This shows that a large portion of the population has suffered the crime in this growing technology. The females that encountered a cybercrime once are homemakers in the majority, and when it comes to males, government employees stand the highest [18]. Private employees stand first in facing cybercrimes 2-5 times in the case of both males and females.

A total of 54 out of 110 respondents of different age groups marked 1, and 27 respondents belonging to different age groups marked 4 when asked how likely they get afraid that their information will be misused when their accounts get hacked [19]. The answers were given on the Likert scale (1 = Extremely likely to 5 = Least likely). This shows most of the respondents belonging to different age groups have an emotional impact because of cybercrimes. It is depicted in Figure 4.
It is observed that 4 out of 110 respondents encountered hacking the most, and 15 out of 110 encountered Internet harassment. A total of 6 individuals faced online frauds the most, and five individuals faced Spamming the most, and nine individuals faced virus attacks the most. It is analyzed that individuals of the age group 25-64 faced hacking, and the age group of 18-24 faced harassment the most. Online frauds were majorly faced by the age group 55-64. Phishing was majorly faced by the age group 25-34. Spamming was faced by the age group 45-54 the most. Virus attacks are faced by the age groups 55-64 the most.

A total of 52 out of 110 respondents (67% male and 33% female) fear being a fraud victim. 22 individuals (77% male and 23% female) fear hacking, 12 fear internet harassment (83% female, 9% male 8% 'prefer not to say') 12 fear Phishing (58% male and 42% female) 12 fear virus attacks (58% male and 42% female). It can be said that people belonging to different age groups do face cybercrimes, and being a victim of fraud is the most feared cybercrime compared to the other crimes taken for analysis.

5.2 Challenges
It is found that 56 out of 110 respondents belonging to different professions marked their response ‘No’ when asked if they were told or trained about cybercrimes in their organizations that they have worked in or working in. It is shown in Figure 5.
A total of 51 out of 110 respondents belonging to different professions marked 1, and 22 respondents marked 2 to the statement that organizations/educational institutions/media are taking enough efforts to spread awareness about cybercrimes. The answer was recorded on the Likert scale (1 = Strongly disagree to 5 = Strongly agree). This shows that the majority of the respondents do not agree with the statement. It is shown in Figure 6.

Figure 6: Count and Percentage of Different Professions Who Strongly Disagree that Organizations and Educational Institutions are Taking Enough Efforts to Spread Awareness About Cybercrimes

A total of 78 out of 110 respondents marked 1 to the statement that they feel safe giving their personal information online. The answer was recorded on the Likert scale (1 = Strongly disagree to 5 = Strongly agree).

It is observed that 38 of the total 110 respondents think 'Knowing about cybercrimes but being negligent about them' is the reason why cybercrimes are increasing, 35 respondents think that 'Not being aware of cybercrimes', 25 individuals think 'Security policies and features are not tight' and 12 respondents think 'Advanced technology' is the reason why cybercrimes are increasing. It becomes a big challenge since being negligent is human behavior, and every individual should know the consequences of being a victim of cybercrime. It is shown in Figure 7.

Figure 7: Count and Percentage of Individual’s Response to the Reason for Increase in Cybercrimes

Individuals were asked to rate themselves on a Likert scale (1 = Poor to 5 = Excellent) in using any IT product or tool, or device. 18% of the age group 18-24 rated themselves 5, and 59% of the same age group rated themselves '4'. 58% of the age group 25-34 rated themselves 4 and 21% of the same age group rated themselves 3. 50% of the age group 35-44 rated themselves four and 30% of the same age group rated themselves 3. 45% of the age group 45-54 rated themselves 2 and 32% of the same age
group rated themselves 3. 60% of the age group 55-64 rated themselves 2, 86% of the age group 65 plus rated themselves 1. This shows that individuals belonging to the age 55-64 and 65 plus do not find it easy to handle an IT Product/tool/device compared to the other age groups. This is a serious concern since, in this era of smartphones and computers, anyone can become a cybercrime victim, especially when they do not know the basics of operating an IT tool or device.

A total of 36 individuals marked 1, and 22 individuals marked 2 to the statement that they are aware of laws that protect them against cybercrimes. The answers were recorded on the Likert scale (1 = Strongly disagree and 5 = Strongly agree). Not being aware of the laws/Acts that protect individuals against cybercrimes also becomes a challenge which is the same as not being aware of crimes.

6. Inference and Suggestions

6.1 Inferences

It is found that Spamming is the most encountered cybercrime compared to the others that are taken for analysis. Individuals can protect themselves from spam emails by downloading anti-spam software. It is suggested to turn the spam filter On and look out for the sender's email addresses when the email or message seems suspicious and not reply or click on links from such email or messages. By not providing email addresses and phone numbers to unknown sites, one can prevent spam. Countries like the USA, Canada, Australia having anti-spam laws like the CAN-SPAM Act 2003, CASL, Spam Act of 2003, respectively, and breach of the laws will result in huge penalty and sometimes even imprisonment.

From the analysis, it is found that Internet frauds are the most feared cybercrime. Internet frauds result in huge monetary losses, reputation losses and put the individual in emotional trauma. These frauds will also indirectly impact companies when their customers become a victim of fraud because it will affect the victim's ability to meet other obligations.

6.2 Suggestions

From the analysis done in the challenges section, six major challenges were found through the survey, and this section will discuss the solutions to those challenges.

Training – Organizations and educational institutions should train their employees/students once a month about the recent happenings in the domain of cybercrimes and what precautions they should follow to protect themselves from these attacks.

Awareness- Organizations, media, educational institutions should take enough efforts to spread awareness to help every individual know about cybercrimes. This is the era where every person uses a smartphone, and not being aware of the crimes would make anyone vulnerable to an attack. Media can come up with advertisements depicting how cybercrime will impact an individual, organization, or government.

Internet – It is found that the majority of the respondents do not feel safe giving their information online. It is suggested that individuals give the information only when necessary and read the terms and conditions, privacy policies, etc., before providing their details to any source. It is in the hand of an individual how to use their data, what information to provide, and whatnot.

IT tool usage – From the responses, it is found that people of the age 55-64 and 65 plus find it difficult to handle any IT tool/product/device compared to the remaining age groups. As a solution to this challenge, teenagers and youth at their home can help the senior citizens by teaching the usage of a smartphone.

Laws/Acts- The majority of people are completely unaware of the laws/Acts that protect them against cybercrimes. Organizations in their training sessions can talk about these and make their employees more aware of the laws that protect the victims. Media can apply the same in their advertisements, and educational institutions can take sessions and spread awareness about cybercrime laws.

Rise in cybercrimes – While awareness is one of the reasons the respondents think that the crimes are increasing, knowing about the crimes but being negligent among them stands top among other
reasons. Individuals should take proper care and precautions when giving their information and not be reckless about providing it. Individuals should understand that anyone can be a victim of cybercrime in this digital era, hence be careful with their data.

7. Conclusion
Recent reports on developments in the defense environment and major cyber threats. They present scenarios marked by a steady increase in cybercrime activities. Despite the increasing visibility and worldwide law enforcement actions against cyberattacks, illicit revenues have hit incredible numbers. In view of the global economic downturn, the burden on culture has been unsustainable. We need to work together to prevent the cost to the global economy that we can't maintain. The research conducted analyzed a total of six challenges and four impacts that cybercrimes cause and presented possible solutions to the challenges found through the questionnaire. Cybercrime is increasing day by day, and with the growing technology, we might not be able to completely eradicate cybercrimes but can surely reduce the impact of the crimes by taking necessary precautions and following basic measures that safeguard our data. Also, knowing more about cybercrimes and its laws that protect individuals against such crimes can reduce the impact they cause.

8. Future Scope
The world is seeing a significant rise in cybercrimes, and the victims of these crimes are individuals, organizations, and even states and nations. The study presented the impact and challenges of these crimes. The research can be further extended to studying the impact and challenges of cybercrimes specifically in one domain, for example, IT Organizations, businesses, Government, etc. The vulnerabilities, threats, risks, and impact it imposes on the organizations can be studied.

Acknowledgment
The authors wish to acknowledge Symbiosis Centre for Information Technology for providing the library facility.

Conflict of Interest: There is no conflict of interest among the authors

Funding: Self-funded

Ethical approval: Not applicable

References
[1]. Alalwan, J. A. (2018). Fear of cybercrime and the compliance with information security policies: A theoretical study. ACM International Conference Proceeding Series, 2008, 85–87. https://doi.org/10.1145/3183586.3183590
[2]. Alazab, M., & Broadhurst, R. (2016). Spam and criminal activity. Trends and Issues in Crime and Criminal Justice, 526. https://doi.org/10.2139/ssrn.2467423
[3]. Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns, and Security Countermeasures. Procedia Economics and Finance, 28(April), 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1
[4]. Brar, H. S., & Kumar, G. (2018). Cybercrimes: A proposed taxonomy and challenges. Journal of Computer Networks and Communications, 2018(1). https://doi.org/10.1155/2018/1798659
[5]. Burns, A. J., & Johnson, E. (2018). The evolving cyberthreat to privacy. IT Professional, 20(3), 64–72. https://doi.org/10.1109/MITP.2018.032501749
[6]. Conteh, N. Y., & Schmick, P. J. (2016). Cybersecurity: risks, vulnerabilities, and countermeasures to prevent social engineering attacks. International Journal of Advanced Computer Research, 6(23), 31–38. https://doi.org/10.19101/ijacr.2016.623006
[7]. Creswell, J. W., Hanson, W. E., Clark Plano, V. L., & Morales, A. (2007). Qualitative Research
Designs: Selection and Implementation. *The Counseling Psychologist*, 35(2), 236–264. https://doi.org/10.1177/0011000006287390

[8]. Harsh, K., Singh, T., & Singh, P. K. (2015). *Emerging threats of cybercrimes*. J(1), 21–23.

[9]. Iqbal, Juneed; Beigh, B. M. (2017). Cybercrime in India: Trends and Challenges. *International Journal of Innovations & Advancement in Computer Science*, 6(12), 187–196.

[10]. Kamruzzaman, M., Ashraful Islam, M., Shahidul Islam, M., Shakawat Hossain, M., & Abdul Hakim, M. (2016). Plight of Youth Perception on Cyber Crime in South Asia. *American Journal of Information Science and Computer Engineering*, 2(4), 22–28. http://www.ajise.org/journal/ajisce%5Cnhttp://creativecommons.org/licenses/by/4.0/

[11]. Kumar Goutam, R., & Kumar Verma, D. (2015). Top Five Cyber Frauds. *International Journal of Computer Applications*, 119(7), 23–25. https://doi.org/10.5120/21080-3759

[12]. Leukfeldt, E. R., Kleemans, E. R., Kruisbergen, E. W., & Roks, R. A. (2019). Criminal networks in a digitized world: on the nexus of borderless opportunities and local embeddedness. *Trends in Organized Crime*, 22(3), 324–345. https://doi.org/10.1007/s12117-019-09366-7

[13]. Pathak, P. B. (2016). Cybercrime: A Global Threat to Cybercommunity. *Ijcsset.Com*, 7(03), 46–49. http://www.ijcsset.com/docs/IJCSET16-07-03-002.pdf

[14]. Paul, P. K., & Aithal, P. S. (2018). *Cyber Crime: Challenges, Issues, Recommendation and Suggestion in Indian Context*. 3(1), 59–62.

[15]. Review, B. L., June, A., & Kalra, K. (2017). *EMERGENCE OF CYBER CRIMES: A CHALLENGE FOR THE NEW*. 86–103.

[16]. Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 2(2), 121–135. https://doi.org/10.1093/cybsec/tyw001

[17]. Van Rensburg, & Kennedy. (2018). Online vulnerabilities facing small businesses today. *Governance Directions*, 70(10), 648–651. https://commons.erau.edu/adfsl/2016/thursday/2/

[18]. Wardman, B. (2016). Assessing the Gap: Measure the Impact of Phishing on an Organization. *Annual ADFSL Conference on Digital Forensics, Security and Law*, c. https://commons.erau.edu/adfsl/2016/thursday/2/

[19]. Winkelman, S. B., Early, J. O., Walker, A. D., Chu, L., & Yick-Flanagan, A. (2015). Exploring Cyberharrassment among Women Who Use Social Media. *Universal Journal of Public Health*, 3(5), 194–201. https://doi.org/10.13189/ujph.2015.030504