WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Critical Analysis on Cyber Crime Against Women in India with Special References to Phishing

Vasagan. S [a], Krishna R [b] *

[a] vasagan2k01@gmail.com *Student, Saveetha School of Law, SIMATS, Chennai 600077, India*
[b] krishnar1131@gmail.com, *Student, Saveetha School of Law, SIMATS, Chennai 600077, India*
DOI: https://doi.org/10.55248/gengpi.5.0624.1626

A B S T R A C T

Phishing is a type of cybercrime that involves obtaining sensitive data for malicious purposes. This is the most direct approach for evaluating confidential information on a large scale. A vast multitude of online vulnerabilities necessitate the provision of information in order to mitigate the risk of falling victim to phishing attacks. The consequences of phishing range from denial of access to communication to substantial financial loss. Although the mistreatment of women is increasing in all areas, being a victim of cybercrime can be the most distressing ordeal for a woman. Especially in India, where society often looks down upon women and the legal system does not effectively celebrate cybercrimes. In this work, I aim to discuss the various types of phishing that might target women and the negative implications they have on them. I will provide a brief analysis of the regulations that specifically pertain to women in similar situations, such as the Information Technology Act (2000) and the local legislation on this matter. Whenever there is a digital crime involving someone's private property or belongings, the accused can be charged with a violation of Article 21 of the Indian constitution, which guarantees the right to privacy. In such cases, the specified remedy can be invoked against the accused. I also intend to provide some strategies to combat the escalating issue of phishing targeting women in India. We will examine the options available to victims of cybercrime, specifically focusing on phishing, and the necessary changes in legislation to effectively address the increasing activities of cybercriminals. In general, through the use of ridicule or communication, it consistently guides individuals who use marijuana to provide specific details on the fraudulent website.

Keywords: Sensitive, Women, Phishing, Cyber culprits, Right to Privacy

1. Introduction

The term " phishing " happened during the 1990's the place where the developers began using underhanded messages to " fish for " information from dark purposes. Since these early software engineers were ceaselessly suggested as " phreaks ", the term came to be known as phishing, with a " ph ". Phishing messages to trap people in and motivate them to take the bait. Regardless, the client and the affiliation are in a tough spot, if they are trapped. In present day India and women being as a matter of fact educated and revived, phishing can be set as a diagram of a social planning combination of ways that cheat experts use to control mortal cerebrum science. Phishing is the bogus undertaking to get sensitive information intently looking like as usernames, watchwords and Mastercard nuances by making a fake dispatch in much the same way as the principal bones. Regardless, in ultramodern times women are seen and portrayed as lovemaking fights, she's managed unacceptable contrasted with men in striking social circles and works; this has made a monster direction inclination between individuals where without a doubt the men surmise that their terrible ways of behaving towards women can not be repelled. Phishing and web irritating works in an intently looking like manner where the violators aren't insane of any power that can address. The computerized world in itself has a PC produced reproduction where anyone can hide away or to be certain fake his character, this gift of the web is used by the criminally arranged to complete unlawful shows and moreover disguise under the cover gave by the web. High level India is the substance of different advancements and mechanical turn of events. farther than partial people are in the everyday act of using PC, web and other inclination which are most normally used are online amusement spots near as Facebook, talk lofts, Instagram, skype, WhatsApp, Dating spots, etc. At one side of the coin the digitalization has support the game plan of India in all terms tantamount as tutoring, control, organization, etc, but on the contrary side it brought computerized infringement in like manner in India at a truly enormous number. As a result of the continuation extension in the use of PC, web, Figures of new bad behaviors have surfaced and those infringement are fundamentally assigned as computerized infringement, especially phishing among women . These bad behaviors could zero in on any get-together of society, yet women are the most assigned pack. In Indian culture women are the real setback from computerized infringement. To help what is happening of phishing and unlawful entering ordered informationAnti-phishing programming and PC programsaredesigned.One of the wash promising styles to avoid Phishing is " Zeko-Zero Information Validation " which immunes the client from phishing attacks. This incorporates recognizing phishing attacks, how to help and make an effort not to exist pranksters, how to answer when you suspect or uncover a phishing attack and how you could help with ending phishers. " AOL on phishing " was nearly associated with the warez neighborhood changed unlicensed programming and the dull headpiece hacking scene that executed charge card blackmail and other web based infringement. Necessity of AOL

perceives words used in AOL chitchat lofts to suspend the records of individuals related with misrepresenting programming and trading taken accounts. Phishing issue arises in a general sense because of desperation and severance. In Lucknow, the locale has transformed into a weak goal for Nigerian computerized lawbreakers who as well as phishing, lottery and occupation draws, are reevaluating deceiving with bogus masterful courses of action. Against only two cases declared in 2014-2015, the amount of cons including Nigerian occupants has reached 10 of each and every 2018-19. The completion of the disquisition is to have a fundamental report on phishing as a huge wellspring of computerized bad behavior against women. The mark of the assessment is to know about phishing and its critical loss.

2. Objectives

* To allure an unknowing internet stoner into telling information similar as bank account Figures or watchwords

* To subscribe druggies to paid SMS- mailing and to infect computers in order to turn them into bother bumps

* To produce strong security for accounts in social networking spots

* To get by doing fraudulent workshops like playing disbenefit cards and so on

2.1 Review of Literature

Jakobsson and Myers (2006) They send mails on behalf of banks asking for some vital information, asking the target to click on a link which redirects to a banking website. These banking websites ask target to provide sensitive data such as username, password or credit card details etc. . How scammers target women., Dating and romance scams.

Joshi, n.d. (Melad Mohamed Al-Daeef(2000)This often takes place through online dating websites, but scammers may also use social media or email to make contact. They have even been known to telephone their victims as a first introduction.Hybrid anti-phishing systems such as client-side toolbars that combine two or more of such methods can mitigate bad effects on gadgets.

Shashidhar, n.d (1997) To evaluate this crime, they review different research perspectives and approaches and investigate the gaps. It is significant to generate attentiveness about phishing in order to boost thoughts and actions to improve cyber security and gain internet user's confidence. January 2016 DOI: 10.1109/SKIMA.2016.7916190.

Anjum Shaikh and Antesar (1999) Approach is a combination of white list and visual similarity based techniques. They use computer vision technique called detector to extract discriminative key point features from both suspicious and targeted websites. Then they are used for computing similarity degrees between the legitimate and suspicious pages. Our proposed solution is efficient, covers a wide range of websites phishing attacks and results in less false positive rate.

Syed Taqi Ali(1999), April 2015 DOI: 10.1109/CSNT.2015.68. The current anti-phishing approaches that have seen significant deployments over the internet can be classified into eight categories. Also, the different approaches proposed so far are all preventive in nature. A Phisher will mainly target the innocent consumers who happen to be the weakest link in the security chain.

Swapan Purkait November (2012). Approach offers online information about the risks of phishing attacks, and how to keep away from this attack. These materials are frequently published by the governments, non-profit organizations from trading platforms, such as eBay,Amazon etc. After such training, users can able to detect phishing emails.

Jagruti Patel , Sheetal Mehta Patel(1998) March, 2015, Training system provides a warning along with active items using text and graphics says.The Anti-Phishing Working Group published a preliminary report in 2008 that looked at the cost of a phishing attack in particular to an organisation.

Hadnagy and Fincher (2015) The study found that the "duration of the phishing attack is a key factor" in determining the cost of the attack but that "most costs are incurred during the first 24 hours of the attack" URL phishing against phishing content by using phish-STORM.

Matthew Marx (13 March 2006) For this a few relationship between the register domain rest of the URL are considered also intra URL relentless is consider which help to dusting wish between phishing or non phishing URL says in Vol. 5, Issue 4, April 2016.

Pratik Patil (2000) States that people showed distinct and robust tendencies for phishing susceptibility and false positives. (**Sabina Kleitman)** 26 oct'18, **Vines (2005)** A series of regression analyses looking at the accuracy of both phishing and false positives detection revealed that human-centred variables accounted for a good degree of variance in phishing susceptibility (about 54%), with perceptions of maliciousness, intelligence, knowledge of phishing, and on-task confidence contributing significantly etc.

Himani Thakur ,Dr. Supreet Kaur ,Volume 7, No. 4, July-August (2016) Defence against phishing attacks is one of the hardest confronts faced by the network security these days.Blacklisting techniques have negligible FP rates but consume a lot of bandwidth and should be avoided if there is a risk of zero-hour attacks .

Gehr (1998) The success of a phishing attack through distributed emails is deter- mined by the response of the unsuspecting recipients.As observed by Kavianto, the overall security risk in an organization depends on its individuals' behavioural decisions to respond to security threats such as phishing attacks.

Nurul Akbar(1999) , unique phishing reports were submitted to APWG,they not only target system end- users, but also technical employees at service providers, and may deploy sophisticated techniques.

Mahmoud Khonji(2000),VOL. 15, NO. 4, FOURTH QUARTER 2013. it is possible to detect phishing web pages by evaluating the visual similarity of web pages. Visual assessment approach, semantic assessment approach, human computer interaction enforcement, and web page originality verification.

Van Nguyen ,Aug(2013) By the same token, the complex nature of an attack of this type often leaves ample opportunity for one to recover, at least in part, the digital trail left behind by the attacker.

According to **Hanaa Alghamd(2017),** . doi:10.21427/D7DK8T, Multiple usability studies reckon and conclude that neither client side warnings and toolbars nor server side security pointers can be completely successful when it comes to preventing susceptible from deception.

Lata Ragha (2012),In heuristic technique we are using textual analysis and URL analysis of e-mail. Since most of the phishing mails have similar contents, our proposed method will increase the performance by analysing textual contents of mail and lexis I ical URL analysis.(2009). Phishers spoof these email and websites of banks with similar looking logos. They use the web addresses that resemble the names of banks but are slightly altered. This is why you should never click on a link in an email from bank or your credit card company. Unfortunately, many people fall victim to bank phishing scams and inadvertently give out sensitive information to cyber criminals.

Ankit Kumar Jain and B.B. Gupta (2001), 10 Jan '17. According to Internet world stats , total numbers of Internet users worldwide are 2.97 billion in 2014; that is, more than 38% of the world population uses the Internet. Phishing email is used to defraud both individuals and financial organizations on the internet .

Sanchari Das(1999) 16 Aug 2019, says ,we found that of the total number of papers on phishing (N = 367) only 13.9% (n = 51) focus on users by employing user study methodologies such as interviews, surveys, and in-lab studies. Even within this small subset of papers, we note a striking lack of attention to reporting important information about methods and participants along with crucial recruitment biases in some of the research.

Gaurav Varshney(2006) 26 October 2016, Phishing prevention schemes try to prevent phishing attacks by providing an extra layer of security to the authentication schemes and user interaction platforms ,prevention techniques can be further classified as watermarking based, RFID based, external authentication devices based, dynamic security skin based smart card based 30, and QR Code based techniques 31, and so on.

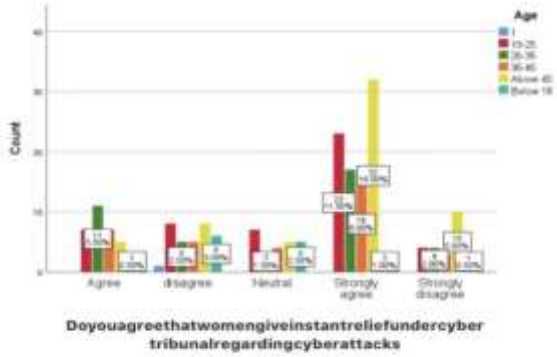
Chuenchujit N Thasphon(2001) Characteristics of phishing emails and web pages were thoroughly analysed, but not enough emphasis was put on exploring alternate attack vectors. Samuel Marchal Considering effectiveness as a combination of detection performance, temporal resilience, deployability and usability. We point out practices to avoid and provide recommendations on the design and implementation of phishing detection techniques.

2.2 Methodology

The research is done on an empirical study on the topic " Critical study and analysis of the impact of cyber crime with special reference to phishing ". Dependent variables are- are people aware about phishing and are people aware about SMSishing .Independent variables are age and gender. Here a random and convenient sampling method is used and the results are given through SPSS .The primary information for the research is collected through surveys from 200 randomly selected respondents which included the general public of different age groups with a well framed and structured survey questionnaire.

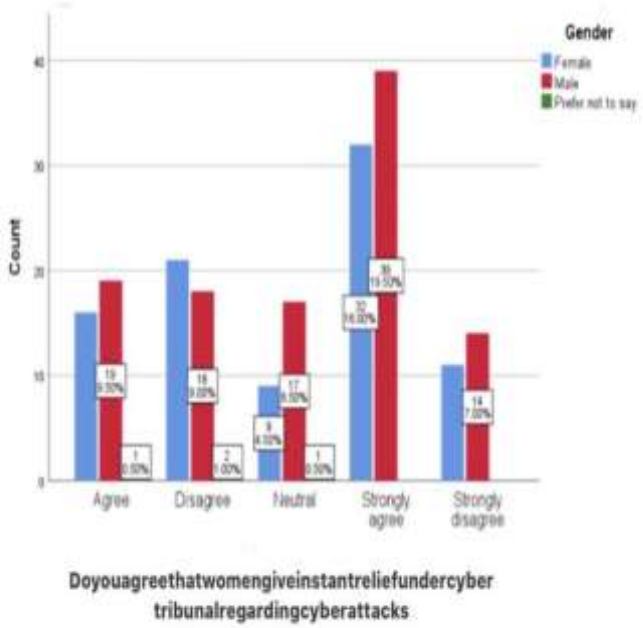
2.3 Analysis

Figure 1



Legend: The graph is between age and instant relief from cyber tribunal for cyber crime

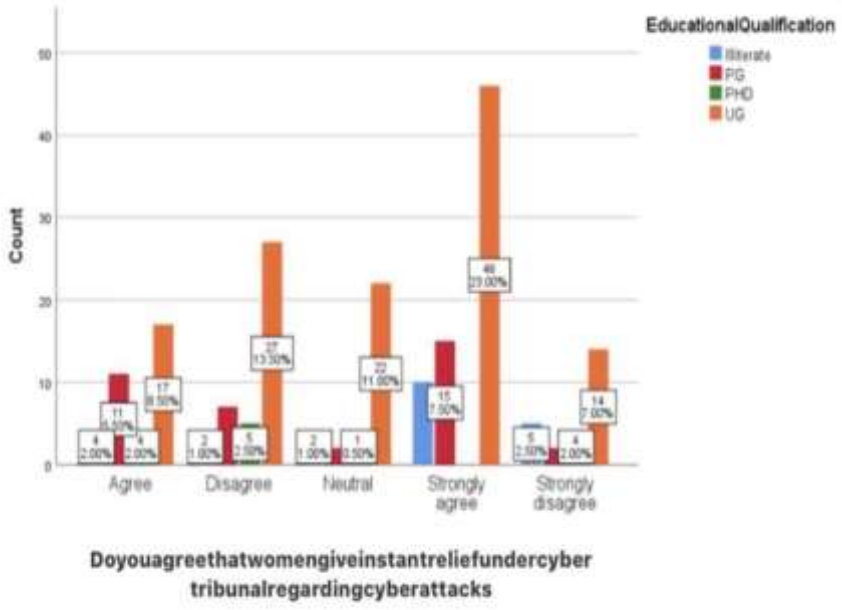
Figure 2



Legend:

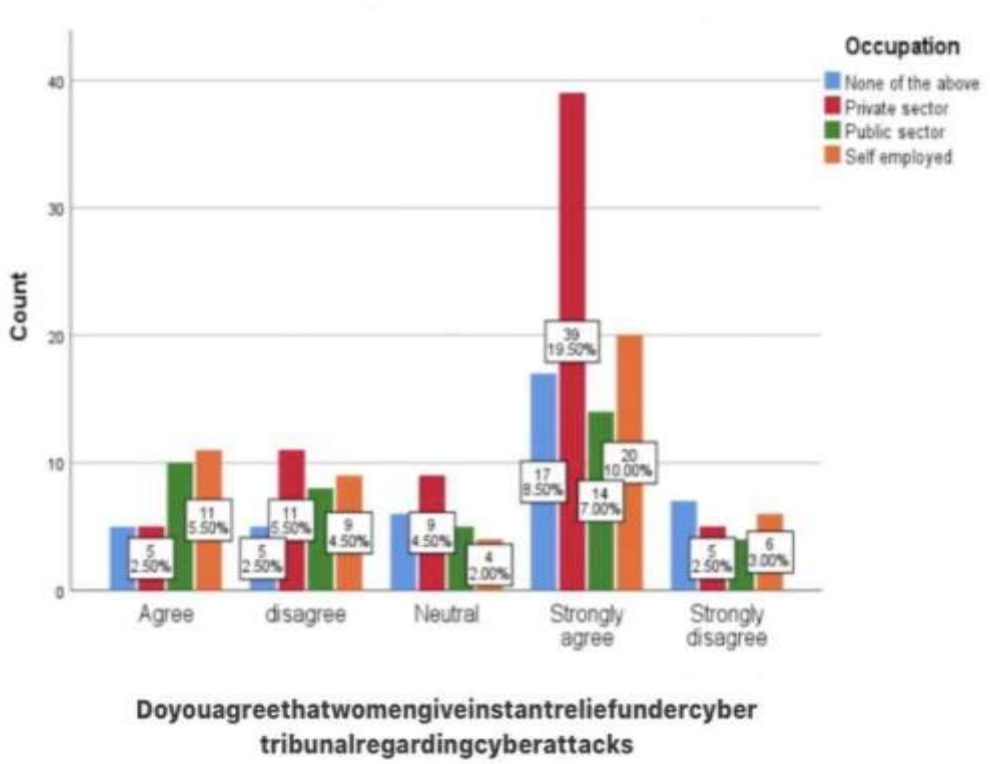
The graph is between gender and instant relief from cyber tribunal for cyber crime

Figure 3



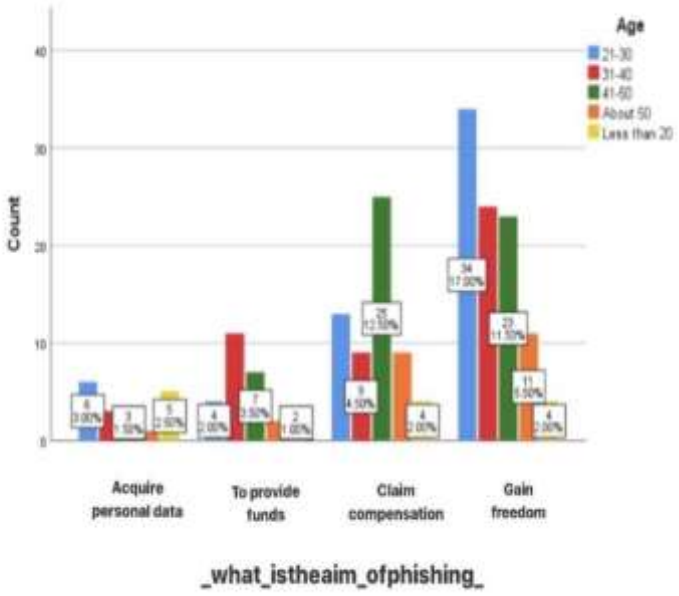
Legend: The graph is between educational qualifications and instant relief from cyber tribunal for cyber crime

Figure 4



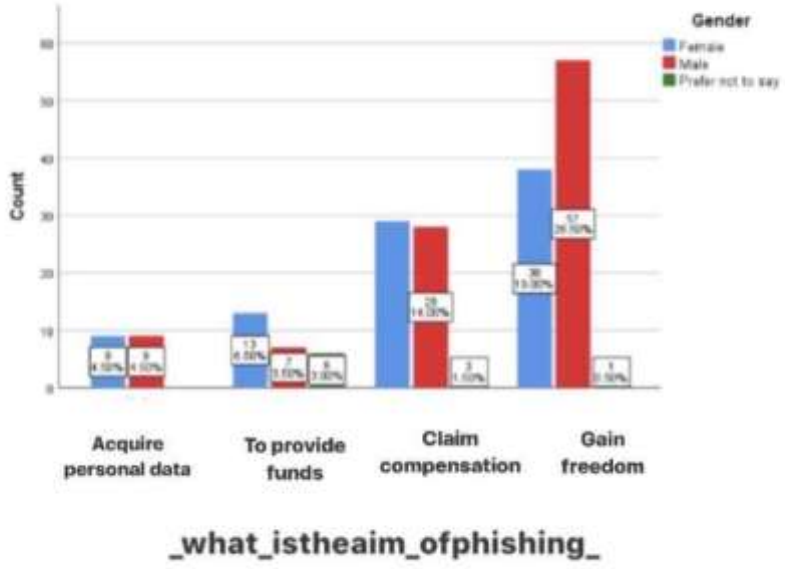
Legend: The graph is between occupation and instant relief from cyber tribunal for cyber crime

Figure 5



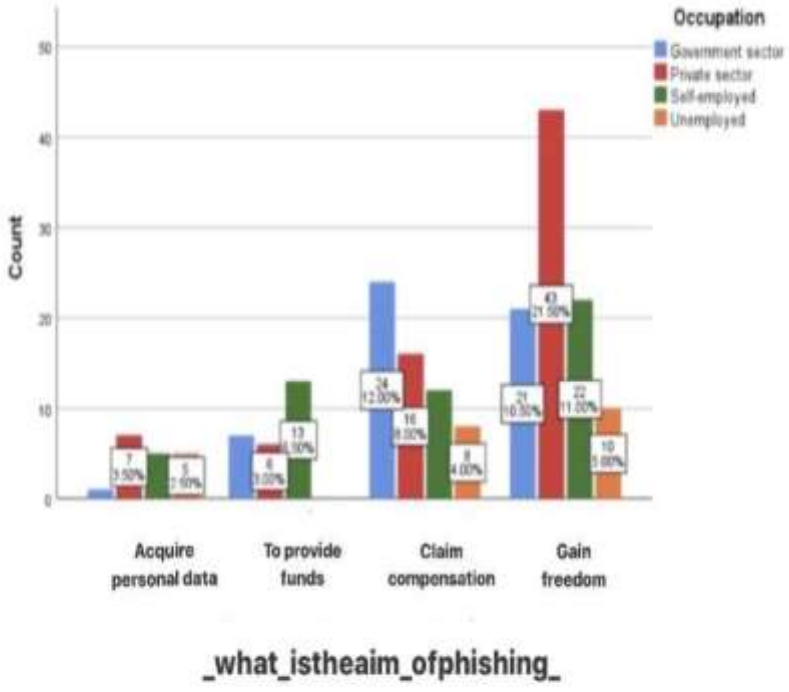
Legend: The graph is between age and what is the aim of phishing

Figure 6



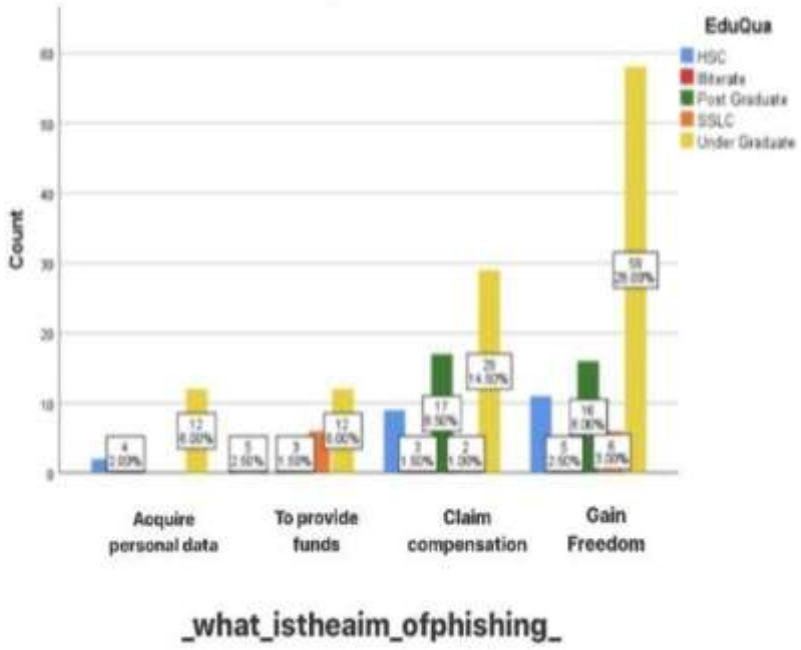
Legend: The graph is between gender and what is the aim of phishing

Figure 7



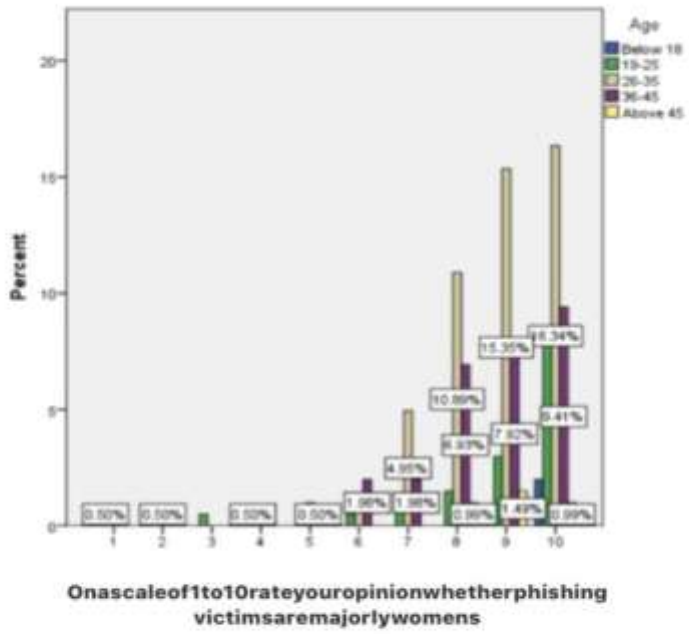
Legend: The graph is between occupation and what is the aim of phishing

Figure 8



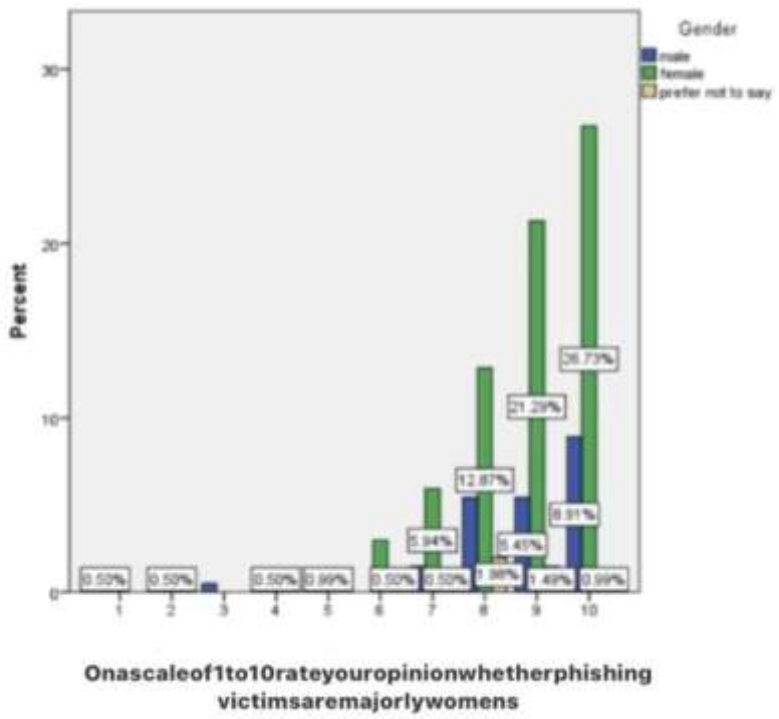
Legend: The graph is between educational qualifications and what is the aim of phishing

Figure 9



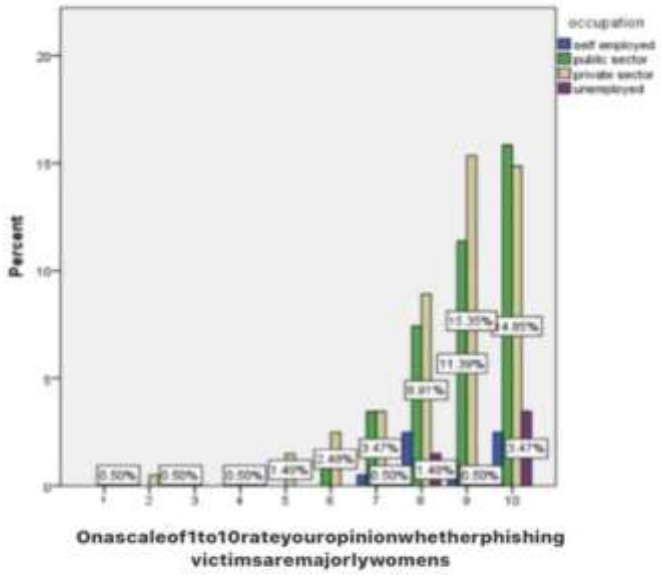
Legend: The graph is between age and whether phishing victims are majorly women

Figure 10



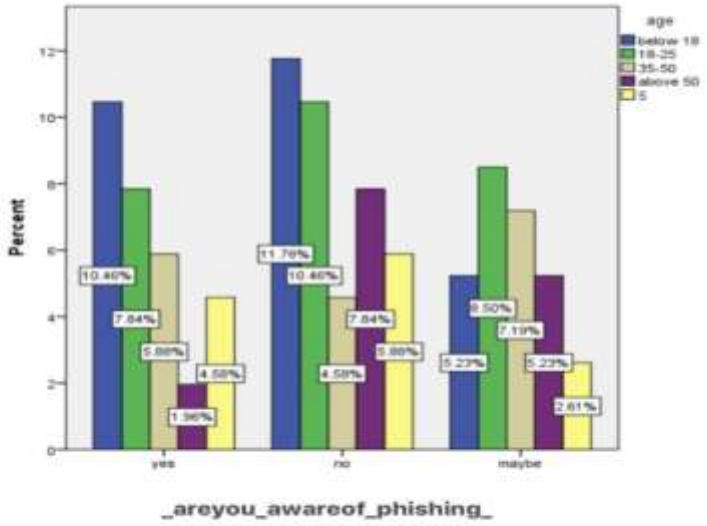
Legend: The graph is between gender and whether phishing victims are majorly women

Figure 11



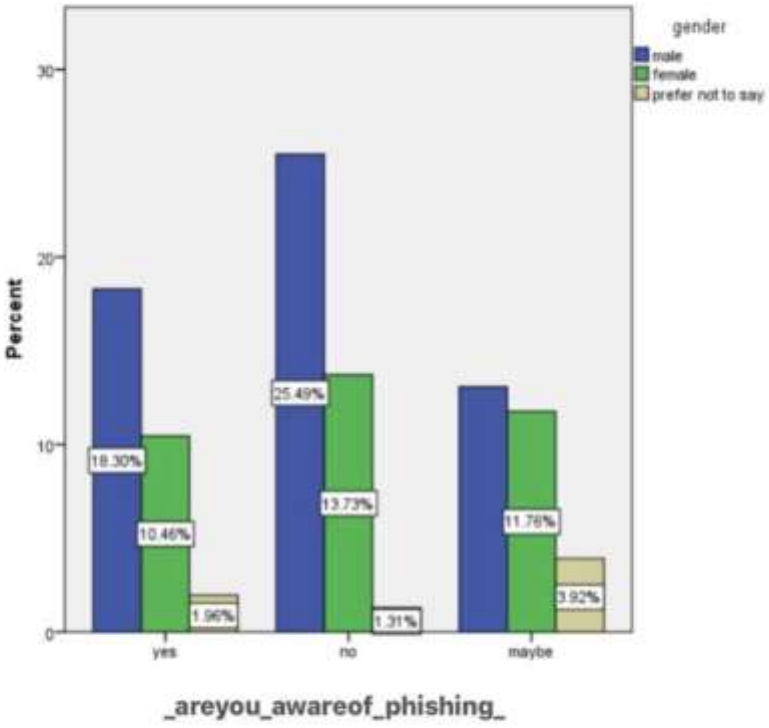
Legend : The graph is between occupation and whether the phishing victims ate majorly women

Figure 12



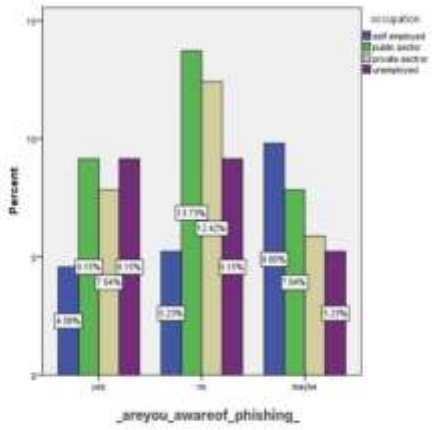
Legend: The graph is between age and awareness about phishing

Figure 13



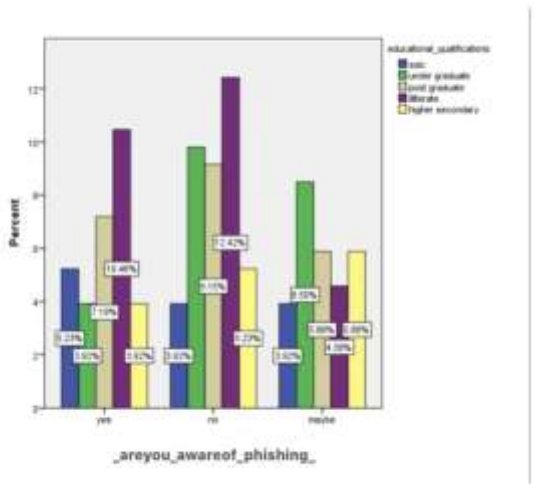
Legend: The graph is between gender and awareness about phishing

Figure 14



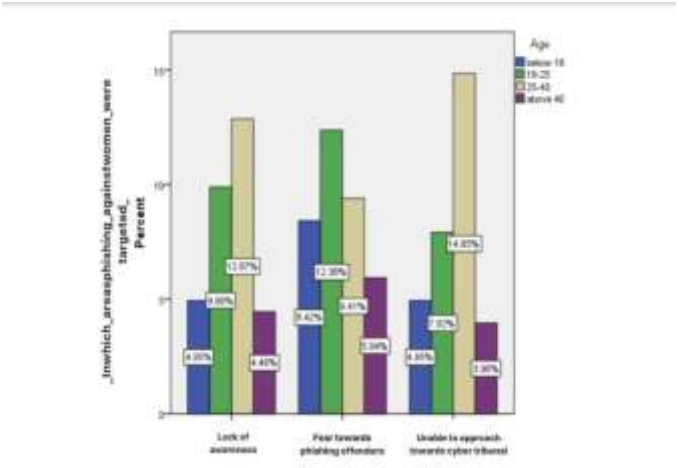
Legend: The graph is between occupation and awareness about phishing

Figure 15



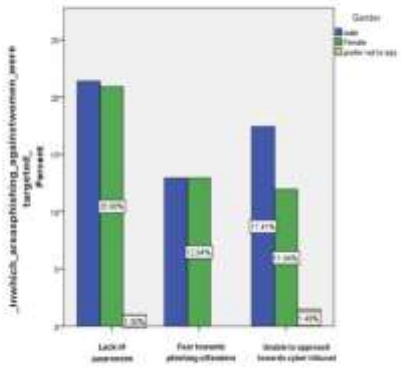
Legend: The graph is between educational qualification and awareness about phishing

Figure 16



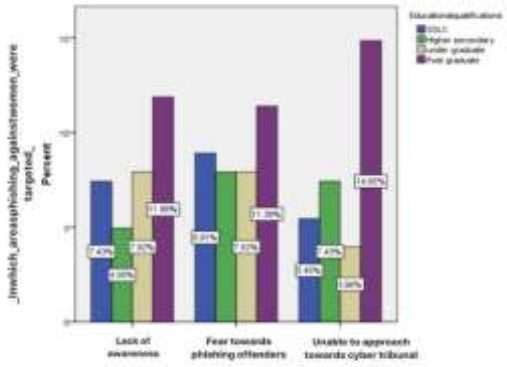
Legend: The graph is between age and in which area phishing against women were targeted

Figure 17



Legend: The graph is between gender and in which area phishing against women were targeted

Figure 18



Legend: The graph is between educational qualification and in which area phishing against women were targeted

RESULT:

Figure 1 - reports that 19-35 and above 45 have highly opted to strongly agree , neutral have been opted by all the age groups to the very least . **Figure 2 -** reports that Male and female have highly opted to strongly agree , agree and disagree whereas prefer not to say have opted only neutral . **Figure 3 -** reports that illiterate PG & UG have highly opted strongly agree , whereas PhD have opted only to disagree . **Figure 4 -** reports that all the occupational ector have highly opted to strongly agree whereas the rest of the options are scattered opted by all the age groups varyingly . **Figure 5 -** reports that all the age group opted highly to gain freedom, claim compensation highly opted by 41-50 , to provide funds highly opted by 31-40 , and 21-30 highly opted to acquire personal data . **Figure 6 -** reports that Male and female have highly opted to gain freedom , claim compensation, prefer not to say opted to provide funds .**Figure 7 -** reports that the private sector , self employed have highly opted to gain freedom, the government sector and unemployed have highly opted to claim compensation. **Figure 8 -** reports that HSc have opted highly to gain freedom, illiterate have opted nothing, PG have opted to claim compensation, SSLC have opted highly to provide funds .**Figure 9 -** reports that below 18 rated 10, above 45 have rated 9 , 19-25 rated 9,10 , 26-35 have rated 8-10 , 36-45 have rated 8-10 . **Figure 10 -** reports that female highly rated 8 -10 , male rated 8-10 , prefer not to say have opted only to 8. **Figure 11 -** reports that the public and private sector have rated from 8-10 ; self employed have rated 8,10 and unemployed have rated 10 the max . **Figure 12 -** reports that all the age groups aren't strongly aware about phishing but still few amounts of below 18 , 35-50 opted yes and maybe is opted by 18-25 the highest. **Figure 13 -** reports that Male and female have highly opted to no , yes whereas prefer not to say have highly opted to maybe . **Figure 14 -** reports that public and private sector have opted highly to no ; self employed opted highly to maybe ; unemployed opted highly to no and yes . **Figure 15 -** reports that illiterate have opted no , PG, UG opted highly to yes , no and maybe; higher secondary opted highly to maybe . **Figure 16 -** reports that 25-40 highly opted to unable to approach towards cyber tribunal the highest , below 18& 18-25 opted fear towards phishing offenders and above 40 opted the highest

to fear towards phishing offenders . **Figure 17 -** reports that male and female have highly opted to lack of awareness and no or least fear towards offenders towards highest area of phishing against women . **Figure 18 -** reports that PG , higher secondary and SSLC have opted unable to uproach towards cyber tribunal the highest , lack of awareness were opted the highest by PG , and the least responses was opted by UG .

DISCUSSION

Figure 1 - shows that all the age groups strongly agree that women are given instant relief under cyber tribunal regarding cyber attacks . **Figure 2 -** Shows that both male and female strongly agree that women are given instant relief under cyber tribunal regarding cyber attacks . **Figure 3 -** shows that all the educational qualifications except PhD strongly agree that women are given instant relief under cyber tribunal regarding cyber attacks. **Figure 4 -** shows that all the occupational sector strongly agree that women are given instant relief under cyber tribunal regarding cyber attacks . **Figure 5 -** Shows that all the age groups think the main aim of phishing is to gain freedom . **Figure 6 -** Shows that all the gender except prefer not to say think the main aim of phishing is to gain freedom . **Figure 7 -** shows that all the occupational sectors think claiming compensation and gain freedom are the main of phishing. **Figure 8 -** Shows that gain freedom is the aim of phishing by all educational qualifications. **Figure 9 -** Shows that all the age groups highly rated for their opinions on phishing victims are majorly women . **Figure 10 -** shows that Male and female have only highly rated for their opinions on phishing victims are majorly women . **Figure 11 -** Shows that as people have highly rated from 8- 10 , they are well aware about the fact the phishing victims are majorly women . **Figure 12 -** Shows that all the age groups aren't much aware about phishing but below 18 is partially aware about it . **Figure 13 -** Shows that both male and female aren't well aware of phishing. **Figure 14 -** shows that the public and sector are the ones who are majorly aware about phishing. **Figure 15 -** shows that illiterates say yes and no majorly for being aware of phishing . **Figure 16 -** shows that fear towards phishing offenders is the highest form of phishing area targeted against women . **Figure 17 -** shows that all gender groups feel lack of awareness towards highest area of phishing against women . **Figure 18 -** shows that PG , UG and SSLC feel that unable to approach towards cyber tribunal is the highest area of phishing against women .

SUGGESTIONS

Regulation shouldn't simply cover aggressors; still, it ought to likewise teach and illuminate all gatherings on the best way to practice their correspondence privileges. Simultaneously, distinctions should come shrewd both on the web and disconnected; know how to go to protection lengths in the internet and how to look for convenient activity assuming their freedoms are abused. Phishing against ladies is as yet taken flawlessly in India, considerably in light of the fact that overall the regard towards ladies in our ultramodern culture is on a drop. Likewise a many individuals are ill suited to deal with the way that for sure posting pictures of somebody online is a wrongdoing. Phishing like morphing,e-mail parodying don't have an ethical moving in the public eye and thus are taken without a hitch. This carries us to the main part where social progression is requested, individuals need to fete the freedoms of others and acknowledge what comprises a wrongdoing. They should learn not to barge in with the confidential existences of others; regard towards ladies in the public eye needs to increment. This must be finished in the event that energetic sorts are mentored from a young age to respect ladies.

LIMITATIONS

However there used to be a few troubles in managing phishing and different cybercrimes like loss of validation and absence of digital armed force yet with the Felonious regulation Remedy Bill(2013) most extreme of these issues have been dealt with. In any case, a few changes are as yet requested like phishing shrewd judges.The head issue of phishing lies in the business as usual and the progression of phishing . The police, bar and the analytical offices need to keep up to date with the rearmost improvements in web-grounded tasks so they can snappily recognize the authentic culprit. It's the occupation of the general set of laws and nonsupervisory organizations to stay up with the Innovative turns of events and guarantee that fresher advancements don't become apparatuses of double-dealing and urgency , which they don't stay aware of . Government lingers behind in going to administrative lengths that protect mortal privileges; particularly ladies' freedoms are guarded online similarly as they are actual spaces.

4. Conclusion

Phishing is a form of social engineering that is employed to get targeted information from the intended or designated victim. Phishing has been a persistent and continuously growing threat in various sectors, characterised by complexity and intricacy. It is crucial to stay vigilant about phishing tendencies and ensure that your computer and online browsers are up to date with the latest antivirus and security patches. While these styles may not provide complete protection, they are a fashionable way of attempting to do so. Individuals should be concerned about the fraudulent website and the individuals involved in this criminal activity. The majority of respondents are concerned about phishing. Multiple organisations have collaborated on phishing campaigns and are actively seeking persons who engage in such activities, with the intention of investigating similar misconduct. Engaging in attempts is the intelligent approach to keeping up with trends and sophisticated procedures.Collaboration is necessary in order to collectively implement comparable transformations. Women should receive training to adopt preventive measures, such as being cautious when sharing personal photos and videos online, being careful when communicating with strangers online, and safeguarding passwords and other sensitive information that could jeopardise their safety and privacy. Women who use drugs on the internet in India should be more aware of the importance of improving privacy settings on social networking platforms as a precautionary step. Hence, it is imperative to cultivate mindfulness and understanding among women regarding the cautious use of online

facilities. Additionally, providing them with correct assistance in the event of encountering cybercrime will empower them to raise their voice against such incidents. There is a significant need for information and specialised efforts to prevent the persistence of women's importunity in India.

References

1. "Adding Context to Phishing Attacks: Spear Phishing." n.d. Phishing and Countermeasures. https://doi.org/10.1002/9780470086100.ch6. Akerlof, George A., and Robert J. Shiller. 2016. Phishing for Phools:
2. The Economics of Manipulation and Deception. Princeton University Press.
3. Gehr, Richard. 1998. The Phish Book.
4. Hadnagy, Christopher, and Michele Fincher. 2015. Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails. John Wiley & Sons.
5. Halevi, Tzipora, Nasir Memon, and Oded Nov. n.d. "Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks." SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2544742.
6. Jakobsson, Markus, and Steven Myers. 2006. Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. John Wiley & Sons.
7. James, Lance. 2005. Phishing Exposed. Elsevier.
8. ———. 2006a. "Banking on Phishing." Phishing Exposed. https://doi.org/10.1016/b978-159749030-6/50006-4.
9. ———. 2006b. "Crossing the Phishing Line." Phishing Exposed. https://doi.org/10.1016/b978-159749030-6/50009-x.
10. Joshi, Rushikesh. n.d. "Interactive Phishing Filter." https://doi.org/10.31979/etd.g3pg-f7e7.
11. Lininger, Rachael, and Russell Dean Vines. 2005. Phishing: Cutting the Identity Theft Line. John Wiley & Sons.
12. Puterbaugh, Parke. 2009. Phish: The Biography. Hachette UK.
13. Shashidhar, Sudhir Kapoor. n.d. "Spear Phishing - The New Face of Phishing." SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2905041.
14. "Adding Context to Phishing Attacks: Spear Phishing." n.d. Phishing and Countermeasures. https://doi.org/10.1002/9780470086100.ch6.
15. Akerlof, George A., and Robert J. Shiller. 2016. Phishing for Phools: The Economics of Manipulation and Deception. Princeton University Press.
16. Gehr, Richard. 1998. The Phish Book.
17. Hadnagy, Christopher, and Michele Fincher. 2015. Phishing Dark Waters: The Offensive and Defensive Sides of Malicious Emails. John Wiley & Sons.
18. Halevi, Tzipora, Nasir Memon, and Oded Nov. n.d. "Spear-Phishing in the Wild: A Real-World Study of Personality, Phishing Self-Efficacy and Vulnerability to Spear-Phishing Attacks." SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2544742.
19. Jakobsson, Markus, and Steven Myers. 2006. Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft. John Wiley & Sons.
20. James, Lance. 2005. Phishing Exposed. Elsevier.
21. ———. 2006a. "Banking on Phishing." Phishing Exposed. https://doi.org/10.1016/b978-159749030-6/50006-4.
22. ———. 2006b. "Crossing the Phishing Line." Phishing Exposed. https://doi.org/10.1016/b978-159749030-6/50009-x.
23. Joshi, Rushikesh. n.d. "Interactive Phishing Filter." https://doi.org/10.31979/etd.g3pg-f7e7.
24. Lininger, Rachael, and Russell Dean Vines. 2005. Phishing: Cutting the Identity Theft Line. John Wiley & Sons.
25. Puterbaugh, Parke. 2009. Phish: The Biography. Hachette UK.
26. Shashidhar, Sudhir Kapoor. n.d. "Spear Phishing - The New Face of Phishing." SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2905041.