

WOMEN PERCEPTION TOWARDS AWARENESS AND PREEMPTIVE MEASURES OF CYBER SECURITY: A STUDY

Dr. J VR GEETANJALI

Assistant Professor,
Department of Commerce
Bhavan' s Vivekananda College,
Sainikpuri, Secunderabad.
Email: geetanjali.commerce@bhavansvc.ac.in

Ms. Gulnaz, B.Com

Bhavan' s Vivekananda College
Sainikpuri, Secunderabad
Phone 9704517798, naazrmgs786@gmail.com

ABSTRACT

The world is now a global city and the internet is in a lot way responsible for that. The internet, as a worldwide communication network, has changed our daily life in many ways especially after COVID -19 crisis, there is a rapid increase in internet users. A social impact investment firm, Omidyar Network India had predicted that at least half a billion new users will log into internet between 2017 and 2020 and these new users will largely be women.

Cybercrime is a kind of illegal and unethical and unauthorized behavior in a system which process information automatically or transfer data. A study had found that a total of 10 million users could be at risk of being stalked, robbed, and harassed or worse. Centre for Strategic and International studies (CISS) reported that every year there is a financial loss of 445 billion dollar in world economy due to cybercrime. The cyber security implies to the process and the technologies which are designed to protect networks, computers, and the data from the unauthorized access, attacks, and vulnerabilities delivered via the internet by cyber criminals. Though various security measures are available people are not fully aware of it.

The present study is focused to understand the scenario of cybercrimes and cyber security and aimed to analyze the perception of the women towards awareness of cyber security. The study made an attempt to compare the level of awareness among home makers, working women and students as well as to identify the preemptive measures adopted to reduce cyber threats.

A Structured questionnaire was administered among 120 respondents to estimate their level of awareness and preemptive measures taken towards cyber security. The study proved through statistical analysis that there is no significant difference in respondents in their awareness levels and also in adopting preventive measures.

(key words: cyber security, women, awareness, security measures)

INTRODUCTION

The world is now a global city and the internet is in a lot way responsible for that. The internet, as a worldwide communication network, has changed our daily life in many ways. A new paradigm of commerce allows individuals to shop online. The World Wide Web (WWW) allows people to share information. E-mail technology connects people in far-flung corners of the world. This inevitable evolution has also created a dependency on the internet. The powers of the web and smart phones had now helped us in connecting anyone, anytime from anywhere. The rise of the internet and smart phone penetration even in rural areas has increased the consumption of technology. The digital way has fundamentally changed the way of life of all human beings from shopping, banking, and government affairs to meetings, connecting with people, and even playing games. In the Asian region, India ranks among the top two internet users, as it is the very fastest-growing country. Today the internet becomes the backbone of the social and economic world. Users can access the internet anytime from anywhere however, over the internet, many unlawful acts are done. The present scenario proved surfing involves threat for digital privacy.

A research report that is conducted by social impact investment firm Omidyar Network India (2020) had predicted that at least half a billion new users will log into the internet between 2017 and 2020 and these new users are largely women.

The internet is considered as a great boon. But everything has a cost to pay. With the advent of time, data has become more valuable and for someone who wants to make money in various ways, it had become as precious as diamonds. Though now we can access any information through the internet, the data and security of people are always at risk of being stolen or misused in other ways and it becomes easy for fraudulent people to barge into the digital privacy of others. The internet as an open forum has created some security problems. Confidentiality, integrity, and authentication are needed. People need to be sure that their internet communication

is kept confidential. When they shop online, they should ensure that the vendors are authentic and their transaction requests to their banks, they want to be certain that the integrity of the message is preserved. We are living in the information age. We need to keep information about every aspect of our lives. In other words, information is an asset that has to be secured from attacks. To be secured, information needs to be hidden from unauthorized entity when it is needed.

Cyber security awareness is critical for survival in industry dominated by growing virtual crimes. 95% of cyber security rifts are due to human error besides, only 38% of global organizations states that they are able to handle a cyberattacks. People have consistent behaviors in locking their homes or putting their valuables in safe deposit box of a bank or at home. They now must learn to do the same for their digital assets. It is essential for women to possess the cyber security knowledge and protect themselves from cybercrimes.

CYBER CRIME

Computer crime or cyber-crime or hi-tech crime basically is a criminal activity where a network or computer is the target, source or place of crime. It is a term for any illegal activity, an offence that is committed against individuals or group of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks like internet.

MAJOR CYBER CRIME AGAINST WOMEN

1. Cyber stalking
2. Cyber pornography
3. Cyber defamation
4. Cyber Harassment
5. Morphing
6. Email spoofing
7. Phishing and Trolling

Therefore, the present study is carried out with an aim of examining the level of awareness and the perception of women towards cyber security and preemptive measures of cyber security.

Sreehari A. et.al (2018) studied the awareness of cybercrimes among college students with a special reference to Kochi. The ratio of awareness among the respondents regarding cybercrime

is high for hacking when compared to other types. The study has found out that most of the respondents occasionally receive spam messages and spam calls but hardly anyone of these respondents failed to report to cybercrime police. Animesh Sharma.et.al (2017) focused to study on cybercrimes and cyber laws of India. The study covered the history, evolution and classifications of cybercrimes along with the cyber laws to protect ourselves from cybercrimes. Jigar shah (2016) emphasized in his study about awareness of cyber laws for Indian youth and proved that internet users are not thoroughly aware of cybercrimes and cyber security that are prevailing. The study recommended that ignorance of the issue of cyber crimes will lead to further damage, if the government fails to take serious attempts in implementing the rules and regulations in this regard.

“Qualified people commit crime more, so there is need to know about principles and computer ethics for their use in proper manner” was stated by Shubham Kumar (2014) in research paper on present scenario of cybercrime in India and its prevention. Stated through his study that India has taken a lot of steps to stop cybercrime but the cyber law cannot afford to be static, it has to change with the changing time. Anuraj singh (2017) had made a report on cyber law in India and cybercrime security. The reports consist of some of its law and security issues, threats, Trojans and attacks over internet.

METHODOLOGY

Primary data was collected through structured questionnaires from 120 respondents. Sample selected from twin cities of Hyderabad and Secunderabad. However, the study also included secondary data such as internet resources, journals, and books. Sample includes only female internet users only. Female users are also categorized as home makers, working women and students.

OBJECTIVES OF THE STUDY

1. To analyze the perception of the women towards awareness and preemptive measures adopted towards cyber security.
2. To compare the level of awareness among homemakers, working women, and students.

Overview on Cyber security

Cyber security is to protect the electronic devices such as smart phones, laptops, tablets, computers and the services rendered/availed, both online and at work from theft or damage. The cyber security implies to the process and the technologies which are designed to protect networks, computers, and the data from the unauthorized access, attacks, and vulnerabilities delivered via the internet by cyber criminals. Cyber security is important because smart phones, computers and the internet are now such a fundamental part of modern life, that it's difficult to imagine functioning without them. From online banking , shopping to email and social media, it's more important take steps that can prevent cyber crimes. Social media plays a huge role in cyber security and will contribute a lot to cybercrimes. Social media has become an enormous platform for the cyber criminals for hacking private information and stealing valuable data. In a world where we are quick to give up our personal information, companies have to ensure they are just as quick in identifying threats, responding in real time and avoiding a breach of any kind. Since people are easily attracted by these social media the hackers use them as a bait to get information and the data they require. Hence people must take appropriate measures especially in handling with social media so as to reduce the loss of their personal data.

Cyber security techniques

1. Access control and password security
2. Anti-virus software
3. Anti-spam mail server
4. Firewall services
5. Anti-spy software

NETWORK SECURITY ASESSMENT TOOLS such as, wire shark, Metasploit, Nmap and Enter soft apps can also protect devices from vulnerabilities.

INFORMATION TECHNOLOGY ACT

The information technology act 2000 provides legal recognition to the transaction done via electronic exchange of knowledge and other electronic means of communication or electronic commerce transactions. The act made provisions for punishment for cyber offences and established authority for investigation and adjudication of cyber offense. It primarily defined

offense as hacking with computer systems, tampering with the source code publication of information which is obscene in electronic form and penalty for damage to computer system.

Cyber security and cybercrimes are one of the greatest problems faced by everyone. Cybercrimes are proliferating at a higher rate in India. Protection of women has always been a concern especially in a country like India. Women felt insecure in places outside home, but today home is one of the major places for women where they are being victimized. With technology and internet becoming the parallel form of living women don't feel safe anymore, anywhere.

Findings of the study

Out of the total respondents of 120, from twin cities of Hyderabad and Secunderabad, 51% of the internet users are between age group 18-25. More than 50% of the respondents are students and remaining 50% are equally considered from employees and homemakers. Comparisons revealed that 46.7% of the respondents use internet more than 7-8 times in a day. 58.3% of people use internet for social networking such as Facebook, Instagram, WhatsApp, Twitter etc. 73.3% of the users secure their accounts and apps with password. Only 36.7% of the sample respondents agreed that they receive more than 10 spam emails. A maximum of 63% respondents had strongly agreed that they encounter problems as leakage of personal information. Another 55% of users have agreed that loss of money is the common type of loss during cybercrimes. 40% of the users use firewall services while 36.7% of them use anti-virus services and 26.7% of them use none of the services. More than 45% of users do not know about the security tools that can protect their devices from malware, cybercrime. 50% of users agreed that security measures are expensive. Though 40% of users are strongly aware of Information technology Act, and remaining of them aren't aware of Information technology act. In case of facing cybercrimes 33.3% of them agreed to inform the police and 33% of remaining agreed to just ignore it. Wherein 41.7% of them agreed that they report cyber-crime online.

Research Hypothesis 1 (HO1)

There is no significant difference among Students, Home makers and working women in having awareness of Cybercrimes and Cyber security.

Research Hypothesis 2 (HO2)

There is no significant difference among respondents (students, home makers and working women) in adopting Cyber security measures.

To test the hypothesis chi-square test was used to analyze the perceptions of students, homemakers and employees.

Table 1. Awareness of cyber security

| Category | Students | Home makers | Working women | Total |
|-----------------------------|----------|-------------|---------------|-------|
| Aware of cyber security | 46 | 12 | 22 | 80 |
| Not aware of cyber security | 18 | 10 | 12 | 40 |
| Total | 64 | 22 | 34 | 120 |

Research findings

***H01**(research hypothesis 1)

1.Null hypothesis (**H0**): There is no significant difference among Students, Home makers and Working women in having awareness on cyber security

2.Alternate hypothesis(**H1**): There is a difference among Students, Home makers and Working women in having awareness on cyber security.

3.Degree of freedom: $(c-1) (r-1) = (3-1) (2-1) = 2$

4.Level of significance 5% (0.05) = 5.99 (tabulated value)

Table1. Awareness about Cybercrimes and Cyber Security-Comparative Analysis

| Observed | Expected | Chi-square value |
|-----------|----------|------------------|
| 56 | 42.6 | 0.045662928 |
| 18 | 21.4 | 0.214058118 |
| 12 | 14.6 | 0.256360324 |
| 10 | 7.4 | 0.297898054 |
| 12 | 22.8 | 0.39514214 |
| 12 | 11.2 | 0.999959318 |
| Total=120 | 120 | 2.2090 |

Chi-square value =1.134(calculated value)

Tabulated value is greater than calculated value

5.99 > 2.2090

Hence H0 is accepted. i.e There is no significant difference among Students, Home makers and Working women having awareness and not having awareness on cyber security

***HO2**

1.Null hypothesis(H0): There is no significant difference among respondents (students, home makers and working women) in adopting Cyber security measures.

2.Alternate hypothesis (H1): There is a difference among respondents (students, home makers and working women) in adopting Cyber security measures.

3.Degree of freedom: $(c-1) (r-1) = (2-1) (2-1) = 1$

4.Critical value: 3.84145

Table 2. Respondents' Preemptive Measures Towards Cyber Security

| Category | Observed | Expected | Chi-square value |
|-----------------------------|----------|----------|------------------|
| Security measures taken | 112 | 120 | 0.3 |
| Security measures not taken | 108 | 120 | 0.3 |
| Total | | | 0.6 |

Chi-square value =0.6(calculated value)

Critical value is greater than calculated value

3.84 > 0.6

Hence accept H0. i.e There is no significant difference among respondents (students, home makers and working women) in adopting Cyber security measures

CONCLUSION

Most of the internet users are young (i.e 51% in our current study) so they must be educated right from school. School curriculum must cover all aspects of cybercrimes. Empowering and educating women and children with adequate knowledge and awareness about the occurrence of cybercrimes in a society is essential. The present study concluded that there is no difference

among Students, Home makers and Working women in having awareness on cyber security and there is no difference among respondents in adopting Cyber security measures. Though our legal system now takes care of cybercrimes, women have to be aware of cyber victimization by self and moreover cyber laws are not universal as they vary from country to country. Today many of the netizens want to browse web privately and safely especially women.

Suggestions to tackle the cybercrimes

Workshops and orientation from experts and ethical hackers are to be encouraged. Government should collaborate with ethical hackers to bring out more practical solutions for the prevailing problems. Government should organize more awareness campaigns in various places where the potential net users are high. A coactive approach involving the initiatives and steps taken by the government and other legislative bodies to address such crimes would be the best way to tackle the cybercrimes. Rules and regulations that affect cybercrimes should be implemented strictly to make sure that no one is taking the safety issues without any consideration. Strict governance is required in order that nobody is inculcating the habit of indulging in illegal download and data theft. Cyber cells have to be increased even in small towns. Every organization should be made aware of the procedure to reach cyber cells, their roles and responsibilities. Need to adopt Uniform Law Worldwide because as cybercrime is an internationally threatening issue, and there is more scope for cross border crimes, certain steps should be seized at the planetary even for preventing the cybercrime and coordination between the government is encouraged. National Crime Records Bureau should assemble all the cases of women and child harassment and other cybercrimes against women and children under separate category so that performance of law enforcement agencies in this regard could be discerned and observed properly. Maximum punishments under the act are bailable thus there is necessity to increase punishment so as to have deterrent effect.

REFERENCES

- https://www.business-standard.com/article/companies/at-least-half-billion-new-users-to-log-in-internet-by-2022-omidyar-report-119112801364_1.html
- <https://www.businessinsider.in/tech/news/biggest-data-breaches-of-2019-to-affect-india/articleshow/72465865.cms>
- <https://yourstory.com/2019/12/data-security-tech-startup-houm-technology-digital-homes>
- <https://www.thehindubusinessline.com/info-tech/children-women-need-awareness-on-cyber-crime-expert/article23160305.ece>
- <https://searchsecurity.techtarget.com/definition/cybersecurity>
- <https://360.shiprocket.in/blog/how-internet-changed-our-lives/>
- <http://www.legalserviceindia.com/legal/article-1344-cyber-safety-and-security-for-women.html>
- <https://us.norton.com/internetsecurity-privacy-cyber-safety-for-women.html>
- <https://www.news18.com/news/buzz/big-win-for-cybersecurity-scientists-are-using-a-new-tool-to-set-trap-for-hackers-2519211.html>
- <http://www.legalserviceindia.com/legal/article-639-cyber-crime-in-india-are-women-a-soft-target.html>
- <https://study.com/academy/lesson/what-is-cyberstalking-definition-examples.html>
- <https://www.indiaforensic.com/cyberstalking.htm>
- <http://www.legalserviceindia.com/legal/article-1278-dimensions-of-cyber-defamation-critical-study.html>
- <https://analyticsindiamag.com/difference-between-cybersecurity-information-security/>
- <https://www.techopedia.com/definition/23142/anti-spyware>
- <https://www.ijeat.org/wp-content/uploads/papers/v8i6S3/F13130986S319.pdf>
- <https://www.irjet.net/archives/V4/i6/IRJET-V4I6303.pdf>
- <https://acadpubl.eu/hub/2018-119-16/1/130.pdf>
- <https://www.ijtsrd.com/papers/ijtsrd18693.pdf>
- <https://www.ijtsrd.com/humanities-and-the-arts/social-science/54/a-study-of-awareness-about-cyber-laws-for-indian-youth/jigar-shah>