Journal of Analysis and Computation (JAC)
(An International Peer Reviewed Journal), www.ijaconline.com, ISSN 0973-2861
Volume XVIII, Issue II, July-December 2024

STUDY ON CYBER CRIME AWARENESS

[1]Ms. Rama Bhardwaj, [2]Aayush Bansal, [3]Akash Dagur, [4]Akshat Chaurasia

[1]Assistant Professor, Department of Information Technology, JECRC College
[2]B. Tech Student, Department of Information Technology, JECRC College
[3]B. Tech Student, Department of Information Technology, JECRC College
[4]B. Tech Student, Department of Information Technology, JECRC College

ABSTRACT:

Internet use has become part of everyday life for most people. The number of internet users has increased enormously, as has the number of cybercrimes. Cybercrime is a crime committed using a computer and a network. The threat of cybercrime is an ever-present and growing reality in both personal and professional lives. With the advent of the Internet, old crimes have taken on a new face. The purpose of this study is to raise awareness about cybercrime in the modern world and raise awareness about greater cybersecurity. The article attempts to analyze cybercrime awareness among Internet users of different ages and education levels. A linear regression model was used to analyze both objectives. The article showed that there was a connection between age groups and education among respondents. Therefore, it is the responsibility of every internet user to be aware of cybercrime and security and help others by educating them.

Keywords: Cyber-crime, Cyber criminals, Cyber security, Internet, IT Act, Awareness.

[1] INTRODUCTION

The Internet in India is growing rapidly. This has created new opportunities in entertainment, business, sports, education and much more. With the advent and increasing use of the Internet, companies have overcome the barriers of local markets and reached customers around the world. Computers are widely used in businesses, not only as a tool for processing information, but also for gaining strategic and competitive advantages. Computers can be used for both constructive and destructive purposes. Misuse of the Internet has given rise to new age crimes that fall under the Information Technology Act, 2000. As information has become more accessible around the world, it has also become more vulnerable to misuse. India is in the crosshairs of cybercriminals due to the growing number of cyberattacks against the Indian establishment. India ranks third after the US and China in terms of sources of

malicious activity on the Internet, second in terms of sources of malicious code, and fourth and eighth in terms of sources or origins of attacks on the Internet and networks. According to the Computer Emergency Response Team of India (CERT-In), 27,482 cases of cybercrime were reported between January and June 2017.These include phishing, viruses or malicious code, corruption, scanning or probing, website hijacking, ransomware and denial of service attacks.

It found that at least one cybercrime was reported every 10 minutes in India in the first half of 2017, compared to every 12 minutes in 2016. A total of 1 cybercrime was reported in India. There have been 71,000,000 cybercrimes in the last 3.5 years, and the number of crimes this year was 27,482, indicating that the total is expected to exceed 50,000 by December. Analysis of data from 2013 to 2016 shows that 6.7% of all cases were network analyses. and surveys, while viruses or malware accounted for 17.2%. According to the latest report of the National Crime Records Bureau (NCRB), a total of 11,592 cybercrime cases have been registered (including cases under the Information Technology Act, offenses under related sections of the IPC and offenses under the Special and Local Laws (SLL)). compared to the 9,622 cases registered the previous year (2014), representing an increase of 20.5% compared to the previous year. Uttar Pradesh reported the highest number of such crimes at, followed by Maharashtra and Karnataka. Increasing internet usage poses a problem for people who spend long hours surfing the cyber world. In 2017, the number of mobile internet users increased by 12. Compared to the previous year, 49% and 23.93% of the population used the Internet via mobile phone. In 2022, this value is expected to rise to 34.85%. (Statista.com, 2017). Thus, increased internet usage has opened the gate of cyber-crime to flood in. Lack of awareness on such issues will lead to the damage of financial, emotional, moral or ethical grounds. Under such alarming scenario, besides tackling the cybercrimes, another issue that needs to be focused on higher priority is – creating awareness on "cybercrimes and security" among the internet users. Thus, the current study focuses in finding out the answers to alarming questions I. Volume. "Are people aware that they are vulnerable to various cybercrimes? "If they are conscious, to what extent? and "If they don't know, what steps can be taken to raise their awareness and bring them up to speed."

In many ways, it is not surprising that cybercrime has increased in recent years. As technology becomes more sophisticated, cybercriminals also become more sophisticated, targeting individuals, businesses, healthcare organizations, educational institutions and governments. As more people engage in more diverse online activities and more companies conduct business online, cybercrime is expected to increase. To use the colloquial language of routine operations theory (Cohen and Felson, 1979): We have much more suitable targets in an understaffed space that is falling prey to increasing numbers of motivated criminals. It is also not surprising that as researchers strive to understand these evolving phenomena, a growing literature on cybercrime is emerging. Entire journals are now devoted to studying this disease, and new academic disciplines have been created to combat it. Although our knowledge of cybercrime has increased rapidly and impressively,it remains largely unknown. This special issue of the American Journal of Criminal Justice contains nine new articles that

will help fill this knowledge gap. The articles in this issue reflect three main areas of cybercrime research: victimization of cybercrime, commission of cybercrime, and techniques and tools that facilitate cybercrime. Although there is some thematic overlap, the issue contains three articles in each of these three areas. The first area covered in this special issue concerns cybercrime victimization. This area has been the subject of the most extensive research to date. Additionally, since cybercrime victims are relatively easy to find, extensive research has been conducted on cybervictimization in various cybercrimes. The three articles in this special issue focus on cyber victimization and contribute to the literature in interesting ways by presenting cross-national perspectives, building on theoretical traditions, or providing systematic syntheses of current knowledge. The first article in this section, written by Michelle Wright and a team of colleagues, examines how young people in China, Cyprus, the Czech Republic, India, Japan and the United States describe their experiences with cyberbullying. The study compared whether the ways in which youth explained victimization varied by location (private or public), medium (offline or computer), and severity, and whether cultural differences altered these relationships. Their findings suggest that the role of context, environment, severity, and cultural values must be considered for prevention and intervention efforts to be successful. The second article, focusing on victimization, builds on the general finding that problematic social media use is associated with negative life experiences and provides empirical support for the theoretical link between problematic social media use and cybervictimization. The analysis by colleagues Eetu Marttila, Aki Koivula and Pekka Räsänen is based on the theory of routine activities/lifestyles and exposure. The results suggest that problematic social media use is not only strongly related to cyber victimization in the between-subjects analysis, but it is also clear in the within-subjects analyzes that problematic social media use has a cumulative effect who has cyber victimization.

[2] RELATED WORK

The following methodology was used to study cybercrime and security awareness:

a) Objectives of the study:1. Examine the relationship between respondents' education levels and their awareness of cybercrime and security. 2. Examine the relationship between different age groups of respondents, cybercrime and security awareness. 3. Find out how respondents use the Internet.4. To study the level of awareness of Internet users about the safety of using personal computers and the Internet in the field of cybercrime.

I believe these nine papers speak to the current state and future promise of cybercriminal. Currently, we are building a large body of empirical studies that speak to patterns of victimization andperpetration. With respect to victimization, we have learned a lot about who is likely to be victimized and how the patterns of victimization vary by type of cybercrime. We also have a good understanding of the activities that increase the likelihood of victimization, the emotional and financial costs of being a victim, and how people view victims depending on the setting and type of victimization. The body of evidence supporting

a slightly modified version of Routine Activity Theory/Lifestyle-Exposure Theory is increasingly impressive, and the papers by Marttila, Koivula, and Räsänen as well as the article by Marcum and Higgins offer additional support for aspects of this theoretical approach.

Similarly, our understanding of cybercrime perpetration has expanded exponentially in recent years. While finding samples of cybercriminals is always a challenge, the growing body of evidence suggests that the behavior of cybercriminals is largely explained by the same set of factors that can account for the behavior of more traditional criminals. That is, cybercriminals tend to have low levels of self and social control, are largely unsupervised, experience strains, and learn the how, when, and why of their crimes from their associates. The papers in this issue offer additional support for techniques of neutralization, social learning theory, and self- control theory. While there are nuanced differences in how some criminogenic factors play out in the virtual and offline worlds, our existing theories appear to be robust as many of our theories apply to both online and offline criminal behavior. A few of the differences that exist largely relate to the asynchronous nature of many online interactions. The fact that online interactions can occur synchronously as well as asynchronously expands our networks and provide additional opportunities for others beyond our immediate environment to influence us and for us to commit crimes. The full ramifications of these changes in social networks, criminogenic forces, and criminal opportunities are not understood; however, we understand these far better today than we did even just a few years ago.

We also have a far greater understanding of the techniques of committing cybercrimes. We know considerably more about the use of the Dark Web to find and purchase illegal goods and services, and we have learned that the Surface Web plays a significant role in computer-dependent crimes. Moreover, as the article by Miller and Miller highlights, information technology has helped blur the line between legal, pseudo-legal, and illegal behaviors. What work in this area really highlights is how difficult it is to monitor and police the internet. While there is certainly social control exercised on the internet, there are limits to the effectiveness of this control (see Hawdon et al., 2017). Yet, by understanding the patterns of victimization, the underlying causes of perpetration, and the techniques that facilitate cybercrime, we become better armed in designing strategies to prevent it, defend against it, mitigate its adverse effects, and prosecute those who commit it. All the articles included in this issue further that understanding.

The samples will be collected from different areas of Delhi-NCR.

b) Data collection methods: Primary data was collected from 160 respondents using a questionnaire to find out whether people are actually aware of the likelihood of committing various cyber crimes or not. Secondary Data: Relevant data was collected from various books, published national and international journals, various websites, etc.

c) Research Tools: Linear regression technique was carried out using SPSS version 23 software to obtain the research results.

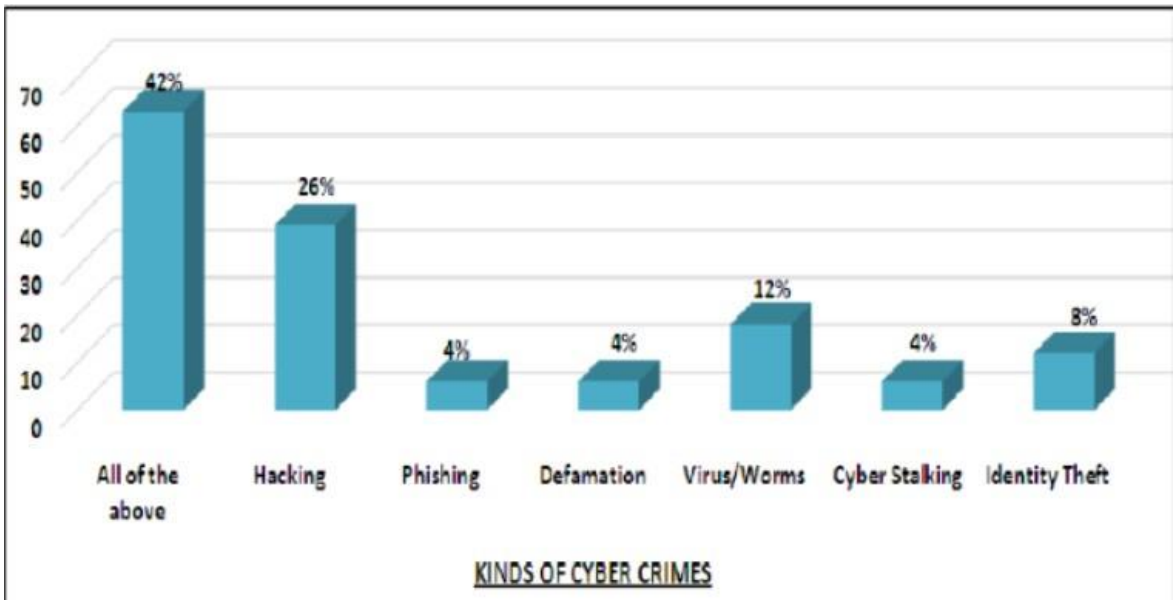
d) Hypothesis: Based on the above objectives, this study aims to test the following hypothesis (null hypothesis):

1)H01: There is a relationship between the respondents' education level and their awareness aboutcybercrime.

2)H02: There is a relationship exists between the various age groups of the respondent and the awareness ofcyber-crimes among them.

[3] ANALYSIS AND INTERPRETATION

A study was conducted on 160 respondents to identify whether they are aware of cyber-crimes or not. Findings of the study are as follows



a)H01: There is a relationship exists between the educational level of the respondent and the awareness ofcyber-crimes among them.

To test the hypothesis whether there is a significant and positive relationship between respondents' level of education and their awareness of cybercrime. A linear regression model was used for three factors: knowledge of the term “cybercrime”, awareness of mobile cybercrime, and awareness of cyber law among Internet users. The R value in Table 1 means that the simple correlation is 0.913 (column “R”), indicating a high degree of correlation of . Table 2 shows that the regression model predicts the dependent variable statistically significantly as the p-value is 0.00003., which is less than 0.05 (i.e. the regression model fits the data well). Table 3 provides further clarity by showing the values of the above three factors, namely: knowledge of the concept of “cybercrime”, “awareness of cyber cells”, “awareness of cyber laws among Internet users” and point out that these values are statistically significant at the 0. 05 level for only one factor, namely knowledge of the concept of “Cybercrime” (0.002). Therefore, the hypothesis (H01) was partially accepted

regarding this factor and partially rejected in the case of Cyber Cell Awareness and IT Act Awareness among Internet users.

b) H02: There is a relationship exists between the various age groups of the respondent and the awarenessof cyber-crimes among them.

To test the hypothesis whether there is a significant and positive relationship between the education level of the respondents and cybercrime awareness among them, a linear regression model was used for three factors, namely, knowledge of the term "Crime Cyber" and cybercrime awareness. Cell, raising awareness of Internet users about IT law. The R value in Table 1 means that the simple correlation is 0.903 (column "R"), indicating a high degree of correlation of .Table 2 shows that the regression model predicts the dependent variable in a statistically significant way as the p-value is 0.001, less than 0.05 (i.e. the regression model fits the data well).Table 3 provides more clarity by showing the values for the above three factors, namely awareness of the term cybercrime, awareness of cyber cells, awareness of cyber acts among Internet users and shows that the values are statistically significant at 0.05 level only Level. for one factor, i.e. . Knowledge of the term "cybercrime" (0.00002). Therefore, the hypothesis (H02) was partially accepted regarding this factor and partially rejected in the case of Cyber Mobile Awareness and IT Act Awareness among Internet users.

c) Figure 1 shows a very important part of our research, viz regarding awareness on various types of cybercrimes concluded that (42%) of the respondents are aware of all the types of cyber-crimes whereas 26% are aware of Hacking, 4% are aware of phishing, cyber stalking and defamation, 12% are aware of Virus/Worms and 8% are aware of identity d)40% agreed that Government organizations are more vulnerable to cybercrimes. 63% felt financial institutions, like Banks, finance companies etc. are more vulnerable for cybercrimes.50% said Private sectors are the victims and 10% opted for Educational Research J. Humanities and Social Sciences 2017; 8(4): 459-464 A.K. Mokha 464 institutions, 65% believe there is a threat to law enforcement agencies like police, CBI, courts etc. 32% believe anyone can become a victim of cybercrime.

[4] LITERATURE REVIEW

Aparna and Chauhan (2012): The authors in their paper conducted research in Tricity on cybercrime awareness and revealed that awareness can be increased by giving due importance to cybercrime which can be an efficient tool to decrease or prevent the cybercrimes. They also concluded that it remains the responsibility of the net users as well as the government to ensure a safe, secure, and trustworthy computing environment.

Mehta and Singh (2013): The author conducted a survey to study the awareness about cyber laws in Indian society. He found that there is a significant difference between the awareness level of male and female users of internet services. Male internet users are more aware of cybersecurity regulations than women.

Agarwal (2015): In his article, the author discusses the types of cybercrimes, and the cybercrime laws developed to combat them. The aim was to determine whether internet users are aware of the existence of cybercrime. He also stressed that it is the responsibility of all internet users to be aware of cybercrime and cybersecurity regulations.

Hasan et al., (2015): Conducted a survey to analyze cybercrime awareness in Malaysia and

found that female students are more aware of cybercrime than male students.

Archana Chanuvai Narahari and Vrajesh Shah (2016): The author conducted a survey among 100 respondents to check whether internet users are actually aware of cybercrimes. Respondents were found to have some 3 awareness about cybercrime and cybersecurity, but further awareness is needed. They also proposed a conceptual model on how to maintain and implement cybercrime awareness programs among Internet users.

[5] CONCLUSION AND FUTURE WORK

As the number of internet users increases, cybercrime also increases. Different types of cybercrimes occur in daily life. But people don't know all of these guys. Most people only know about hacking and viruses/worms. They ignore cases of phishing, defamation, identity theft, cyber harassment, etc. The modern world needs to be informed about internet-related crimes. The survey shows that 48% of respondents share their personal information with other people, even if they do not know them very well. 55% of respondents believe that their computers are often damaged by viruses. Internet users are faced with spam messages, phishing calls and emails asking for sensitive information such as mobile number, bank account, address, etc. It is the responsibility of each of us to raise awareness of important cybersecurity issues. Cybersecurity refers to technologies and processes that are used to protect computers, networks and data from unauthorized access and attacks by cybercriminals over the Internet. People need to be aware of the basics of computer security because they should: a) Install security packages like Avast Internet Security, Kaspersky Antivirus, McAfee Antivirus, Norton Antivirus, etc. to protect your computer from threats such as viruses and worms. b) Enable network, firewall and virus protection. c) Always use complex passwords, preferably alphanumeric ones. d) Only share personal information over the phone or on secure websites. e) Do not click on links, download files, or open attachments in emails from unknown senders. f) Be wary of links in emails asking for personal information or pop-ups. g) Check that all antivirus software and operating system on your computer are up to date. h) Carefully check the website spelling, URL, HTTP addresses, etc. The government is also working to curb cybercrime. It has enacted cybersecurity laws to help people learn about various cybercrimes and cybersecurity. The Information Technology (IT) Act, 2000 deals with cyber security offences. To stop criminals, not only the government but also citizens must work together. Victims of any of these cybercrimes should come forward and file a report with the Special Cyber Crime Units. This will help in the fight against cybercrimes. Therefore, awareness about cybercrime and security is necessary these days**.**

REFERENCES

[1] Aggarwal, Gifty (2015), General Awareness on Cyber Crime. International Journal of Advanced Research inComputer Science and Software Engineering. Vol 5, Issue 8.
[2] Aparna and Chauhan, Meenal (2012), Preventing Cyber Crime: A Study Regarding Awareness of Cyber Crime in Tricity. International Journal of Enterprise Computing and Business Systems, January, Vol 2, Issue 1.
[3] Archana Chanuvai Narahari and Vrajesh Shah (2016). Cyber Crime and Security – A Study on Awarenessamong Young Netizens of Anand. International Journal of Advance Research and Innovative Ideas in Education.Vol-2 Issue-6. 4. Avais, M. Abdullah et.al. (2014), Awareness regarding cyber victimization among students of University of Sindh, Jamsharo. International Journal of Asian Social Science, Vol. 4(5): 632-641 5. Hasan et al., (2015), Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia. Journal of Social Sciences, Vol. 11 (4): 395.404 6. Jamil D. and Khan M.N.A. (2011), Data Protection Act in India with Compared To the European Union Countries. International Journal of Electrical and Computer Sciences, Vol: 11 No: 06. 7. Mehta, Saroj and Singh, Vikram (2013), A Study of Awareness aboutCyber laws in the Indian Society. International Journal of Computing and Business Research, January, Vol.4, Issue. 1. 8. Parmar, Aniruddhsinh and Patel Kuntal (2016), Critical Study and Analysis of Cyber Law Awareness among Netizens. Conference: International Conference on ICT for Sustainable Development, At http://link.springer.com/chapter/10.1007%2F978-981-10-0135-2_32, Volume: 409 9. Singaravelu, S and Pillai,
[4] K. Perumal (2014), B.Ed. Students Awareness on Cybercrime in Perambalur District. International Journal of Teacher Educational Research (IJTER) Vol.3 No.3 March. Journal of Advance Research and Innovative Ideas in Education.Vol-2 Issue-6.
[5] Avais, M. Abdullah et.al. (2014), Awareness regarding cyber victimization among students of University of Sindh, Jamsharo. International Journal of Asian Social Science, Vol. 4(5): 632-641
[6] Hasan et al., (2015), Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia. Journal of Social Sciences, Vol. 11 (4): 395.404
[7] Jamil D. and Khan M.N.A. (2011), Data Protection Act in India with Compared To the European Union Countries. International Journal of Electrical and Computer Sciences, Vol: 11 No: 06.
[8] Mehta, Saroj and Singh, Vikram (2013), A Study of Awareness aboutCyber laws in the Indian Society. International Journal of Computing and Business Research, January, Vol.4, Issue. 1.
[9] Parmar, Aniruddhsinh and Patel Kuntal (2016), Critical Study and Analysis of Cyber Law Awareness among Netizens. Conference: International Conference on ICT for Sustainable Development, At http://link.springer.com/chapter/10.1007%2F978-981-10-0135-2_32, Volume: 409
[10] Singaravelu, S and Pillai, K. Perumal (2014), B.Ed. Students Awareness on Cybercrime in Perambalur District. International Journal of Teacher Educational Research (IJTER) Vol.3 No.3 March.