PREDICTING CYBER CRIME ISSUES IN DIGITAL ENVIRONMENT – AN ANALYTICAL STUDY

Dr. R. Sujatha[1], Dr. B. Navaneetha[2]
[1]Assistant Professor, Department of Computer Science, PSG College of Arts & Science, Coimbatore - 14
[2]Assistant Professor, Department of B.Com (PA), PSG College of Arts & Science, Coimbatore- 14

ABSTRACT

Cybercrime issues are an emerging severe hazard in digital world. Cybercrime is one of the crime involving through internet by harm someone's security or finances. Usage of internet has become a daily routine for majority of people for day-to-day transactions. The number of internet users has grown tremendously and so does cyber-crimes. Worldwide governments, police departments and intelligence units have started to react. Initiatives to curtail cyber threats are taking shape. Indian police has initiated special cyber cells across the country and have started educating the personnel. The digital environment is continually evolving, presenting numerous challenges and vulnerabilities that cybercriminals exploit for their illicit activities. Predicting cybercrime issues in this dynamic landscape is essential for proactive prevention and mitigation efforts. The research focuses on the main issues in cybercrime activities. This paper attempts to analyze the awareness of cyber-crime issues among internet users with different age groups, educational qualifications and also the problems faced by them.

KEYWORDS: ***Cybercrime issues, Hacking, Stalking, Regression***

INTRODUCTION

The internet in India is growing rapidly. Usage of internet has become a daily routine for majority of people for day-to-day transactions. The number of internet users has grown tremendously and so does cyber-crimes. The Digital India initiative is driving our country towards a digitized life where the existence will highly depend on elements like cloud computing, 5G in telecom, e-Commerce etc. Cyber-crime is the crime that is done using computer and network. The threat of cyber-crime is an ever present and increasing reality in both the private and professional sectors. Cybercrime is an important issue for research as it affects many mainstream sectors such as defense, social media, government, industry, private, military and scientific sectors etc. Internet criminals use distorted or hacked data to capture their actions. Several laws and methods have been introduced in order to prevent cybercrime and the penalties are laid down to the criminals. Illegal formations and various intelligent methods in illegal business use the latest technologies to the full extent for the following issues.

(a) Money laundering,

(b) Distributing of false information,

(c) Unauthorized access to information systems and other violations like,

Online identity theft, Financial fraud, Stalking, Bullying, Hacking, Email spoofing, Information piracy and forgery and intellectual property crime.

Categories of Cyber Crimes

The major categories of cyber-crimes can be broadly classified under the following four groups on the basis of their target and impacts:

1. Crimes against Individuals

This type of crime is done to harm particular individuals. These includes hacking , cracking, harassment via emails, cyber-stalking, cyber bullying, defamation, dissemination of obscene material, email spoofing, SMS spoofing, carding, cheating and fraud, child pornography, assault by threat, denial of service attack, forgery, and phishing.

2. Crimes against Property:

There are cybercrimes done to harm the property of an Individual. They can be classified as Intellectual property crimes, cyber-squatting, cyber vandalism, hacking computer system, computer vandalism, computer forgery, transmitting viruses and malicious software to damage information, Trojan horses, cyber trespass, Internet time thefts, robbery o stealing money while money transfers ,etc.

3. Crimes against Government /Firm /Company /Group of individuals:

These types of crimes include cyber terrorism, possession of unauthorized information, distribution of pirated software, web jacking, salami attacks, logic bombs, etc. The criminal in these wants to terrorize the citizens of the country.

4. Crimes against Society:

All the above mentioned crimes have their direct or indirect influence on the society at large. Therefore, all such crimes are included in this such as pornography, online gambling, forgery, sale of illegal articles, phishing, cyber terrorism, etc.

LITERATURE REVIEW

To examine the relationship between various age groups of the respondents and the awareness of cyber-crime and security and to find out the internet usage of the respondents Anupreet Kaur Mokha has undertaken a study on "Awareness of Cyber Crime and Security". A structured questionnaire was administered for the purpose of this research on 160 respondents. Linear Regression technique was performed using SPSS Software version 23 to analyse the data. The findings of the study reveal that the people are not aware of all such types. Majority of the people know only about hacking and virus/worms. They are not aware of phishing, defamation, identity theft, cyber stalking etc. Few suggestions have been given that people should be aware of the basic cyber securities such as Install a security suites such as Avast Internet Security, Kaspersky antivirus, McAfee antivirus, Norton Antivirus, etc. to protect the computer against threats such as viruses and worms, Activate Network Threat Protection, Firewall, and Antivirus and Always use strong passwords preferably alphanumeric etc.

The study titled "Cyber Crime Awareness Among Higher Education Students From Haryana with Respect To Various Demographical Variables" was done by Dr. Menka Choudhary focused with the objectives to know the awareness of the respondents. At the end, we can conclude that there is Average Cyber Crime Awareness among the college students from Haryana state. The result revealed that cyber-crime awareness is affected by stream, means professional students show more awareness as compare to their counterparts. It also showed that cyber-crime awareness is same in boys and girls.

Cyber-attacks such as distributed denial of service attacks by sending malicious packets (Kaur Chahal, Bhandari & Behal 2019, phishing attacks to banking and shopping sites that deceive the user (Sahingoz et al., 2019) have increased significantly. In addition, attackers have been using malicious attack software (virus, worms, trojans, spyware and ransomware) that is installed into the user's computer without any consent of the user (Biju, Gopal & Prakash, 2019) increasingly. Again, the most common of these attacks and one of the attacks that are most difficult to be prevented is the social engineering attacks. They are based on technical skill, cunning and persuasion, made by taking advantage of the weakness of the victim.

PROPOSED WORK

The objective of this research is to predict and examine various crime issues in digital environment. To predict and analyse the issues various intelligent methods from statistical techniques is utilized. The analysis is done using SPSS statistical tools.
The following are the few objectives of the study

- To understand the socio economic profile of the respondents
- To analyze the awareness of cybercrime among the respondents
- To explore the issues faced by respondents in digital environment
- To predict and provide the analysis to the respondents

METHODOLOGY

This research study aims to identify the Evaluation on Cyber Crime issues in Digital Environment. To achieve the accurate result, the data are to be collected on two basis such as Primary and secondary data.

Here, the primary data is collected with the help of a structured questionnaire on the basis of survey method. The questionnaire contains questions relating to the awareness and satisfaction Issues faced in digital environment.

Secondly, the secondary data will be gathered with the help of various public documents such as journals, magazines, newspapers, periodicals and websites which relates to the Cyber Crime issues in Digital Environment.

Primary data was collected from 236 respondents. Data collected was edited and coded by using SPSS version 16.0. This helps in converting the gathered data into a tabulated grouped data. The following relevant tools and techniques are applied. Since the Simple random sampling has been adopted, the questionnaires have been collected from different respondents of Coimbatore city. The responses collected were analysed using the SPSS.

PERCENTAGE ANALYSIS

Percentage analysis is applied to find out the distribution of frequencies between variables in this study. It is applied to find out

- Socio-economic profile of the respondents.
- Information on awareness and satisfaction.

ANOVA

Analysis of variance is a statistical model where the significant difference can be tested between means. Here, the distribution will be analysed based on the group of variables. ANOVA will split the data into two parts; they are systematic factors and random factors. This test has analysed to determine the results that independent variables have on the dependent variables.

In this study the following groups were compared to find out the degree of satisfaction of the respondents on various cybercrime activities: Gender, Age, Marital Status, Educational Qualification, Residential Status, Occupational Status, Earnings Of The Family and Monthly Income.

MEAN RANKING

Mean ranking is one of the non- parametric tests which is used to identify the differences between ten set of values in the problems of packaged milk brands which statistically significant in this study. The ordinal numbers of a value will be arranged in a specified order in a decreasing manner.

LIMITATIONS OF THE STUDY

- The study was confined to 236 respondents only.
- The study has been restricted to Coimbatore city only.

The present study is based on both primary and secondary data. The primary data will be collected through questionnaires.

- Step 1: The Dataset is collected
- Step 2: Preprocessing is applied to the dataset. (collected using questionnaire)
- Step 3: Statistical Techniques (Percentage Analysis, ANOVA and Mean Ranking) is applied to predict and analyze the data.
- Step 4: Based on the result analysis is done.

METHODS OF DATA COLLECTION

Primary Data was collected from 236 respondents through questionnaire to analysis whether the people really are aware that they are vulnerable to various cyber-crimes or not.

Secondary Data: Substantial data was collected from various books, published nationals and international journals, various websites, etc.

RESEARCH TOOLS

For the findings of the study, various statistical methods are applied to predict the dataset and the tools SPSS is applied for analyzing the dataset.

HYPOTHESES

On the basis of mentioned objectives, the present study aims at test the following hypothesis (null hypothesis):
H01: There is a relationship exists between the Educational level of the respondents and the awareness about cyber-crimes issues.
H02: There is a relationship exists between the various age groups of the respondent and their awareness of cyber-crimes issues.

ANALYSIS AND INTERPRETATION

For this purpose, a field survey method was employed to collect the first hand information from the respondents are chosen randomly from four different area of Coimbatore city based on the socio-economic profile consists of gender, age, educational qualification, marital status, occupational status, residential status, earning members and monthly income of the respondents. A study was conducted on 236 respondents to identify whether they are aware of cyber-crimes issues 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 of cyber-crime issues among them.

Predictors: Always Constant value, Familiarity with the term "Cyber Crime issues" and Awareness about Cybercrime issues.

In ANOVA Dependent Variable: Educational level of the respondent and Predictors: Familiarities with the term "Cyber Crime issues" and Awareness about Cybercrime issues. In Coefficients Dependent Variable - Educational level is the respondent

To test the hypothesis, is a significant and positive relation exists between Educational level of the respondent and the awareness of cyber-crimes issues among them, Linear Regression Model is used.

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

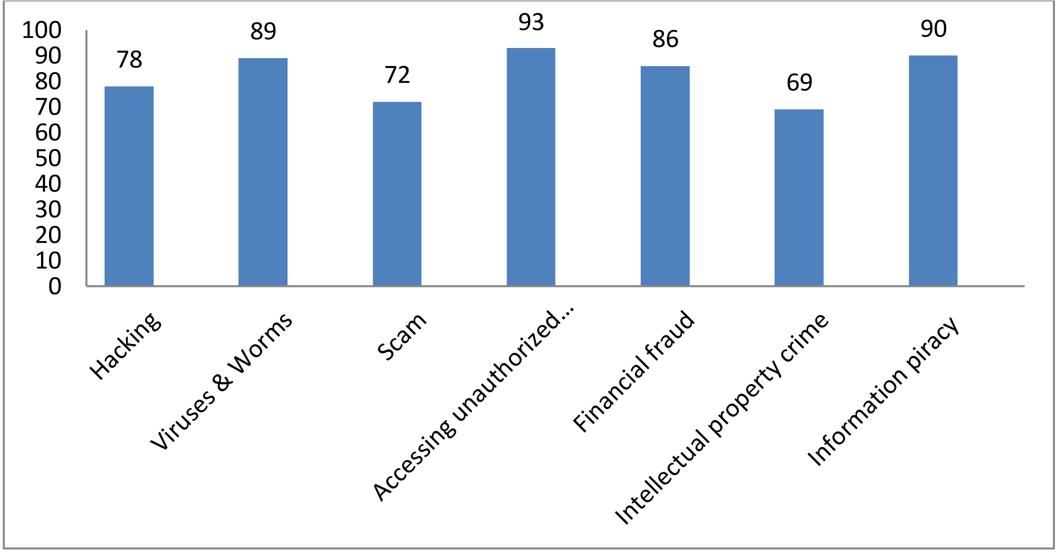
Predictors: Always Constant value, Familiarity with the term "Cyber Crime issues" and Awareness of cyber-crimes issues
In ANOVA Dependent Variable: Age groups of the respondent. Predictors-Constant value, Familiarity with the term "Cyber Crime issues" and Awareness about Cybercrime issues. In Coefficients a. Dependent Variable: Age groups of the respondent. Showing the various kinds of Cyber Crimes issues in day-to-day lives

To test the hypothesis, is a significant and positive relation exists between Educational level of the respondent and the awareness of cyber-crimes issues among them, Linear Regression Model has been used on the two factors i.e. Familiarity with the term "Cyber Crime issues" and Awareness about Cyber Cell. In the hypothesis (H02) is partially accepted for this factor and rejected for Awareness about Cyber Cell.

LEVEL OF AWARENESS ON CYBERCRIME ISSUES

The chart 1 describes the awareness level of respondents on Cybercrime Issues.

Chart No: 1 - Level of Awareness on Cybercrime Issues



Source: Primary data

CONCLUSION

In conclusion, cybercrime issues in the digital environment represent an ever-evolving and multifaceted challenge that affects individuals, organizations, and society at large. The digital landscape provides a breeding ground for various forms of cybercriminal activities, ranging from ransomware attacks and phishing schemes to data breaches and cyber espionage. These issues not only result in financial losses but also threaten data privacy, national security, and the integrity of digital ecosystems.

Addressing cybercrime issues requires a collaborative and proactive approach. Strengthening cyber security measures, enhancing public awareness, and promoting responsible digital behaviour are essential components of mitigating cyber threats. Furthermore, the development and implementation of robust legal and regulatory frameworks, both at national and international levels, are critical to prosecuting cybercriminals and deterring malicious activities.

As technology continues to advance, so too will the tactics employed by cybercriminals. Therefore, on-going research, innovation, and information sharing are vital to staying ahead of emerging threats and vulnerabilities. Ultimately, the battle against cybercrime is an on-going endeavour that demands vigilance, adaptability, and a commitment to securing the digital environment for the benefit of all. The study shows that 45% of the respondents share their personal details with other persons even they don't know them closely 55% of respondents have agreed that their PCs are often damaged by viruses. The internet users must have the awareness about the cybercrime issues and how to handle them. Some of the basic things to be followed to avoid cyber securities issues are as follows,

- Anti-Virus scanning software should be used
- Initiate Firewalls
- Users should use strong passwords preferably alphanumeric.
- Should be more careful while download files or open attachments in emails from unknown senders.
- Beware of links in emails that ask for personal information or popups.

REFERENCES

1. *Anupreet Kaur Mokha, A Study on Awareness of Cyber Crime and Security, , Research Journal of Humanities and Social Sciences (RJHSS) , ISSN 0975-6795 (Online) Vol. 8, Issue 4, P.No. 459-464*
2. *Al-Muhtadi, J., Saleem, K., Al-Rabiaah, S., Imran, M., Gawanmeh, A. and Rodrigues, J. J. (2021) A lightweight cyber security framework with context-awareness for pervasive computing environments. Sustainable Cities and Society, 66, 102610.*
3. *Basit, A., Zafar, M., Liu, X., Javed, A. R., Jalil, Z. and Kifayat, K. A comprehensive survey of ai-enabled phishing attacks detection techniques. Telecommunication Systems, 2021, 76, Pages 139–154.*
4. *Cyber Crime Awareness Among Higher Education Students From Haryana With Respect To Various Demographical Variables, Dr. Menka Choudhary, PalArch s Journal of Archaeology of Egypt / Egyptology 17(7):14454-14461, P.No. 14454 -14461*
5. *, December 2020*
6. *Chen, Q., Islam, S. R., Haswell, H. and Bridges, R. A. (2019b) Automated ransomware behavior analysis: Pattern extraction and early detection. In Science of Cyber Security: Second International Conference, SciSec 2019, Nanjing, China, August 9–11, 2019, Revised Selected Papers 2, 199–214.*
7. *Chayal, N. M. and Patel, N. P. (2021) Review of machine learning and data mining methods to predict different cyber-attacks. Data Science and Intelligent Applications: Proceedings of ICDSIA 2020, 43–51. springer*
8. *Gaurav Gupta has been published A Novel Technique for Detecting And Deciphering Secret Information Communication and presented in 93'd Indian Science Congress, for Young Scientist Award programme held from 3'd-7"t January 2006 in Hyderabad,.*
9. *Handbook of Computer Crime Investigation: Forensic Tools & Technology shan Casey (Editor), Academic Press, 2002.*

10. *Li, Z., Chen, J., Zhang, J., Cheng, X. and Chen, B. Detecting advanced persistent threat in edge computing via federated learning. In Security and Privacy in Digital Economy: First International Conference, SPDE 2020, Quzhou, China, October 30–November 1, 2020, Proceedings 1, Pages 518–532. Springer.*
11. *Zaman, S., Iqbal, M. M., Tauqeer, H., Shahzad, M. and Akbar, G. (2022) Trustworthy communication channel for the iot sensor nodes using reinforcement learning. In 2022 International Conference on Emerging Trends in Electrical, Control, and Telecommunication Engineering (ETECTE), 2022, Pages 1–6. IEEE.*