A Study On Customers' Experience On Cybercrimes And Its Protection Measures In Chennai

S. Sudha[1], A. Meera[2]
R. Aarthi Alamelu[3]
[1& 2] Assistant Professor, School of Management Studies,
Sathyabama Institute of Science and Technology, Semmancheri, Chennai

[3] Assistant Professor, Department of Commerce – Accounting and Finance

SRM University, Faculty of Science and Humanities, Vadapalani Campus, Chennai
lncs@springer.com

Abstract. The most common crime that is wreaking havoc in modern World is cybercrime. In addition to causing the government and society to suffer greatly, criminals are also able to keep a large portion of their identity a secret. Numerous unlawful actions exist that are carried out by technically proficient crooks via the internet. It is the need of the hour to know the e-crimes happening around us and how to safeguard us from those e-crimes. The present study focuses on the experience of the customers on cybercrimes and the measures taken by them to protect against those crimes. The author discusses the experiences on cybercrimes and the protection measures taken by the respondents in Chennai, Tamil Nadu. The author also gives suggestions for safeguarding from cybercrimes.

Keywords: Cybercrimes, Cybersecurity, E-crimes

1 Introduction

The global network of interconnected computer networks is termed as internet that connects billions of devices globally using the common internet protocols. These days, one of the most vital aspects of daily living is the Internet. The development in information technology has brought about two primary works via the cyberspace. The internet has given the positive values across the globe. Inspite of those benefits, there are many issues that affects the societal system and additionally cause a fresh surge of global crime.

2 Review of Literature

[7] have discussed about the theoretical background, forms and aggression of e-crimes in this study. It has also focused on the regulations that various countries have in place

M. Rani Nimmagadda et al. (eds.), *Proceedings of the 3rd International Conference on Reinventing Business Practices, Start-ups and Sustainability (ICRBSS 2023)*, Advances in Economics, Business and Management Research 277,
https://doi.org/10.2991/978-94-6463-374-0_76

to combat cybercrimes. The study also includes cyber security and ways to look for security.

Crimes have increased in frequency and propagation through a variety of channels, such as malicious software designed to compromise corporate or personal computer networks in order to steal sensitive data or wipe out entire systems. Hacking, Cyber terrorism, Phishing, Cyber stalking Spamming, Cyber defamation and Malware are the most famous methods as per the studies made [3, 2]

[11] explained about the cybercrime safety mechanism followed by Indian Bank. The safety and security measures to be made by the banks at their core level itself in order to protect the people. The use of technology is very vital in this regard. The different issues faced by the Indian Banking System are also discussed in this article.

According to [6], it should be prohibited to use computers and the internet for any kind of illegal conduct, including downloading music and games illegally and millions of dollars have been looted from online accounts.

3 Research Methodology

3.1 Need for The Study

Cybercrimes are a global menace to individuals, governments, and organizations. Billions of people worldwide are victims of cybercrimes. Given the gravity of crimes, their global scope, and their ramifications, it is obvious that, in order to combat them effectively, there is a critical need for a shared understanding of this kind of criminal behavior on a global scale.

3.2 Objectives of The Study

1. To know the customers' perception and experience on cybercrimes in Chennai
2. To analyze the nature of cybercrimes affected by the customers
3. To understand the level of protection measures against cybercrimes

3.3 Data Collection

The data is collected through primary and secondary data. The sample size is 150 respondents from in and around Chennai. A structured questionnaire is given to the respondents to collect the primary data. Pilot study from 30 respondents was made in order to test the validity of the questionnaire and data. Convenient sampling method is applied by the author for the collection of data. The study is made using statistical tool of descriptive analysis. Conclusions are made from the frequency distribution analysis.

4 Data Analysis and Interpretations

Table 1. – Users of Online Banking

S. No.	Using Online Banking	No Of Respondents	Percentage
1.	Yes	127	85
2.	No	23	15
		150	

Source: Primary Data

Inference

It is referred from the above Table 6.1 that the 85% of the responders are using online banking and 15% are not using online banking.

Table 2. - Experience Regarding Cybercrime

Experience Regarding Cybercrime	**Yes**	**No**	**Prefer Not To Answer**	**Total**
I've had a virus on one of my device	48	93	9	150
Someone's hacked or tried to hack into my devices	21	117	12	150
I've been the victim of a fraud online and lost money	21	120	9	150
I had received sexual images/videos	24	108	18	150
Someone has threatened me to share sexual content/ image of me	15	123	12	150
I have met up someone who knew only online	12	123	15	150

Source: Primary Data

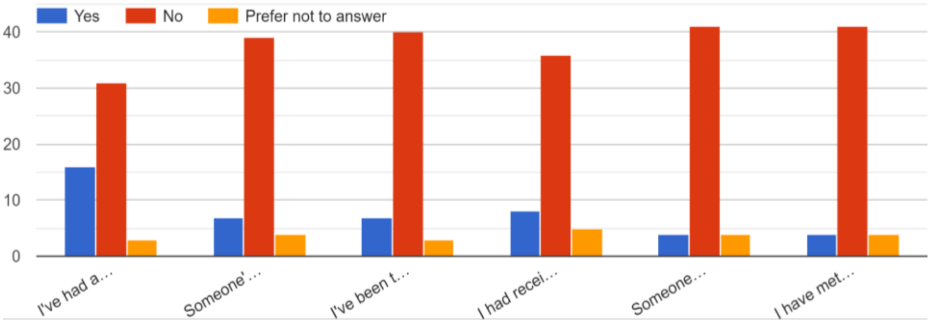

Fig. 1. – Experience Regarding Cybercrimes

Inference:

It is inferred from the above Table 2 and Figure 1 that maximum of the responders said "no" - 62% for virus issues, 78 % for hacking issues, 80 % for online frauds in payments, 72 % for receiving sexual images or videos, 82 % for threatening to share sexual contents, 82 % for someone knowing only online. Less than 20 % of the respondents are only victims of various cybercrimes. Around 32 % were victims of virus attacks. Minority people didn't prefer to answer their experience on cybercrime.

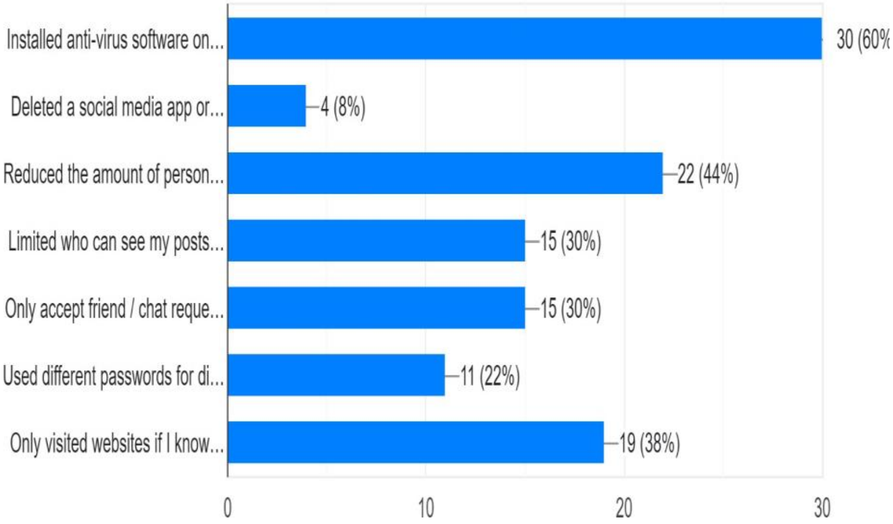

Fig. 2. - Protection Measures Taken by Respondents against Cyber Crimes

Inference:
From the Figure 2, it is interpreted that out of total 150 responders, 60% have installed anti-virus, 8% deleted social apps, 44% reduced amount of personal information, 30% limited others seeing their posts, 30% accept friends who only they know, 22% use different passwords, 38% visited websites only they know. Majority of the respondents have installed anti-virus in order to protect them e-crimes or viruses.

Table 3. - Sharing Password/PIN/OTP With Others

S. No.	Sharing Password/PIN/OTP With Others	No of Respondents	Percentage
1.	Yes	23	15%
2.	No	105	70%
3.	Sometimes	22	15%
		150	

Source: Primary Data

Inference:

From the above Table 6.3 and Figure 6.4, it is interpreted that 15% of the responders share their password/PIN/OTP, 70% don't share, 15% share their password sometimes. Majority of the respondents don't share their PIN.

Table 4. – How Often do You Change Your UPI/Card PIN?

S. No.	Change Your UPI/Card PIN?	No. of Respondents	Percentage
1.	Once in a quarter	57	38%
2.	Never changed	76	51%
3.	Change only when prompted by the bank	8	5%
4.	Others	9	6%
		150	

Inference:
The above Table 6.4 and Figure 6.5 clearly denotes that 38% of the respondents have changed the PIN once in quarter, 51% have never changed, 5% change only when prompted by the bank, 6% opted others. Majority of the respondents have never changed their PIN or password.

Table 5. – Opinion About Using PIN/OTP

S. No.	Opinion About Using PIN/OTP	No. Of Respondents	Percentage
1.	Yes, because it makes transactions safe	128	85%
2.	No, it is an inconvenience	22	15%
		150	

Interpretation:

Maximum of 85% of the respondents agreed that using PIN/OTP is good since it makes transaction safe, 15% said that PIN / OTP is an inconvenience.

5 Conclusion

From the present study, the author concludes that cybercrimes have become a vital issue in today's world, since everything has become online and digital. Majority of the respondents in Chennai are using online banking for their financial transactions. Only minority people are affected by cybercrimes. But majority have taken precautionary measures to safeguard themselves from cybercrimes. Maximum respondents don't share their OTP or PIN numbers to anyone and they feel that it is good to use the PIN Numbers.

The people have to use digitalized methods as it is the present trend in all walks of life. Though there is safety and security and high encryption, still there are many hackers and phishers and many unauthorized persons who are stealing our confidential information and indulge in fraudulent activities. It is high time to understand those e-crimes and protect us from those e-crimes. People should be aware of all the cybercrimes. The Government also should take necessary steps to educate the people regarding e-crimes and its safety measures.

References

1. Alansari, M. M., Aljazzaf, Z. M., & Sarfraz, M. (2019). On Cyber Crimes and Cyber security. In M. Sarfraz (Ed.), Developments in Information Security and Cybernetic Wars, pp. 1-41. IGI Global, Hershey, PA, USA. doi:10.4018/978-1-5225-8304-2.ch001.

2. Bhanu Sahu, Neeraj Sahu, Swatantra Kumar sahu, and Priya Sahu. (2013). Identify Uncertainty of Cyber Crime and Cyber Laws . International Conference on Communication Systems and Network Technologies (pp. 450 - 452). Gwalior : IEEE.
3. Bruce S. Schaeffer, Henfree Chan Henry Chan and Susan Ogulnick. (2009). Cyber Crime and Cyber Security:A White Paper for Franchisors, Licensors, and Others. business.cch.com. Chang Yew, Wong. (2002). Malasian Law and Computer Crime. Malaysia: SANS.
4. Chandra, P., 1984, Financial Theory & Practice, Tata McGraw Hill Publishing Co. Ltd, Mumbai.
5. Fathima, S.J., 2020, Digital Revolution in the Indian Banking Sector, Shanlax International Journal of Commerce, 8, 1, 56-64.
6. Gorazd Mesko,and Igor Bernik. (2011). Cybercrime: Awareness and Fear: Slovenian Perspectives. European Intelligence and Security Informatics Conference (EISIC) (pp. 28 - 33). Athens: IEEE.
7. M K Ganeshan and U Arumugam (2022), Impact of E-Commerce in Banking sector, Empirical Economics Letters, 20 (Special Issue 3): (November 2021)
8. Prof. Waghmare G.T. in his Research Paper “A Business Review of Ecommerce in India” has mentioned about the market, 2012
9. Rahman, Rizal. (2012). Legal jurisdiction over malware-related crimes: From theories of jurisdiction to solid practical application. Computer Law & Security Review 28 (2012) 403-415
10. Soegoto, D.S., Ilhamuddin, A.F. and Amirah, P., 2019, Effect of Internet Banking on E Commerce, Advances in Economics, Business and Management Research, 112, 22-24.
11. Stalin, D.C., and Al-Manayseh, M.N., 2020, Economic and Financial Implications of E Banking in India, Shanlax International Journal of Commerce, 8(2), 22-29.Author, F.: Article title. Journal 2(5), 99–110 (2016).