Scope of a Study on the Awareness about Preventive Measures towards Online Financial Frauds

Dr. M. Bhuvaneswari[1] and K. G. Rigzin[2]
Professor, Department of Management Sciences[1]
Student II MBA, Department of Management Sciences[2]
Hindusthan College of Engineering and Technology, Coimbatore, India
Corresponding author: Dr. M. Bhuvaneswari

Abstract: *Online financial fraud has become a major concern for individuals and organizations worldwide. With the increasing use of technology, cybercriminals have found new ways to deceive people into revealing sensitive personal and financial information or making unauthorized transactions. Thus, it becomes necessary to raise awareness among people about online financial frauds and preventive measures. The modern era is the era of technology; the internet has penetrated every part of our lives, and online banking and finance are no exception.*

Keywords: financial crime, fraud, cyber-crime, forgery, theft

I. INTRODUCTION

Although technology has made our lives more comfortable, it has also exposed us to new types of crimes. Financial fraud is one of those crimes that have become common in the online world. With this background, the present study aims to assess the awareness of people regarding preventive measures against online financial fraud. Online financial fraud has become a significant problem in the digital world. Fraudsters are utilizing advanced technologies to deceive people to share their financial information, which they then use to steal money from their accounts. The consequences of online financial fraud can be devastating, resulting in severe financial losses and mental stress. Preventive measures, such as creating awareness and educating people, can reduce the number of online financial frauds.

1.1 Statement of the Problem

Online financial frauds is to deceive individuals or organizations to obtain access to their financial information or money. This can be achieved through various methods, including phishing, identity theft, fake websites, credit card fraud, and investment scams. Cybercriminals use these tactics to steal personal and financial information, and in some cases, take over bank accounts or make unauthorized transactions, resulting in significant financial losses for the victim. The ultimate goal of online financial frauds is to use the stolen information or money for personal gain, often leaving the victim in a vulnerable and helpless position.

1.2 Objective Of The Study

- To study the awareness level of people on financial crimes occurring on online
- To study about the place where the crimes are occurring more
- To analyse to create a safer and more trustworthy online environment for all users.

1.3 Scope of the Study

- **Identification of cyber financial frauds** – The study should cover the various types of online financial frauds such as phishing, identity theft, credit card frauds, fraudulent investment schemes, and cryptocurrency scams, among others.
- **Awareness levels of the public** – The study should analyse the extent to which the public is aware of these frauds and the measures that can be taken to prevent them. This can be done through surveys, interviews, and focus group discussions.

Copyright to IJARSCT
www.ijarsct.co.in

DOI: 10.48175/IJARSCT-10398

527

ISSN
2581-9429
IJARSCT

- **Sources of information** – The study should identify the primary sources of information that people use to learn about these frauds. Electronic sources such as social media, emails, and websites, and traditional sources such as newspapers, radio, and television should be included.
- **Measures taken by businesses** – The study should also examine the preventive measures taken by financial institutions such as banks, payment platforms, and other businesses to protect their customers from online financial frauds.
- **The impact of online financial frauds** – Finally, the study should explore the impact of online financial frauds on the victims, the economy, and the society. This includes the financial losses suffered by victims, the impact on consumer trust and confidence, and the broader social and economic implications.

II. RESEARCH METHODOLOGY

The primary data collection is done with questionnaire technique. The number of respondents includes both the male and female.

2.1 Research Design

A research which is used here is "Descritive research". This study uses Survey methods with closed ended question.

Information Required:
- Demographic profiles of the respondents
- On which schemes they are well aware about. Whether they will get the respective benefits.

Research Plan:
- Data source: primary
- Research Approach: Survey method
- Research Instrument: Questionnaire

Sampling method

KYC (Know Your Customer) – this method requires financial service providers to collect information about their customers' identity, source of funds, and other necessary details to ensure that they are not involved in money laundering or terrorist financing. Transaction monitoring – financial institutions use various software to monitor transactions regularly and identify any suspicious activities. These technologies help in identifying and reporting any suspicious transactions to regulatory authorities. Financial institutions are required to submit SARs to regulatory authorities whenever they detect any suspicious transaction or activity. This method helps in identifying potential financial crimes and preventing them. Risk assessment – financial institutions conduct regular risk assessments to identify potential threats, vulnerabilities, and risks that might lead to financial crimes. Based on the results, they implement effective strategies to prevent any such activities. Training and awareness – financial institutions educate their employees and customers about the different types of financial crimes and how to prevent them. This method helps in creating awareness and ensuring that everyone is on the same page while preventing financial crimes.

2.2 Limitation of the Study
- Limited sample size
- Lack of standardization
- Lack of user feedback
- Time-bound nature of the study
- Inaccessibility of proprietary information

III. METHODS OF COLLECTION

This study uses both primary data and as well as secondary data.

Primary data

The data collected through the surveys and interviews will be analysed using qualitative and quantitative methods, depending on the type of data collected. The analysis will be guided by the research objectives and the specific

research questions being investigated. The findings will be presented in a report that will include both descriptive and inferential statistics, as well as qualitative analysis of the open-ended responses.

Secondary data

- Academic journals and publications related to the use of financial crimes and financial frauds.
- Industry publications, blogs, and online forums related to financial crimes.
- Company websites and marketing materials related to cyber crime.
- Case studies and success stories of the use of financial crimes.

IV. LITERATURE REVIEW

(Singh, 2013) Fraud exposure is identifying fraud as soon as possible after it has occurred. Once fraud prevention has failed, fraud detection becomes Necessary. Fraud detection must be used continuously since one may not be aware that fraud prevention has failed. Whenever criminal discover a detection method has been implemented, they will change their approaches and try another. Day by day, new criminals are entering the field .many of them are not aware of the fraud detection method that has been very effective in the past and will try an alternative technique. This means that with the latest development, earlier detection techniques and tools are also required to be useful. This is not easy to develop new fraud prevention methods because exchanging thoughts or ideas in fraud detection is very narrow. It may be dangerous to express fraud prevention methods in detail in the public domain, as the criminal can take help from it.

"Factors Influencing the Adoption of Security Measures for Preventing Online Financial Fraud" by S. Zhang and Y. Yang. This study aimed to identify the key factors that influence individuals' adoption of security measures to prevent online financial fraud. The authors found that perceived risk, perceived self-efficacy, and trust in technology were significant predictors of security measures adoption. However, they also identified a lack of awareness and education as a key challenge to improving security measures adoption.

"Cybersecurity Awareness and Preparedness for Small and Medium-Sized Enterprises against Online Financial Fraud: A Study of Nigerian SMEs" by O. Olabode and K. Ogunyemi. This study investigated the cybersecurity awareness and preparedness of small and medium-sized enterprises (SMEs) in Nigeria against online financial fraud. The authors found that most SMEs had low levels of cybersecurity awareness and preparedness, and identified factors such as lack of resources and inadequate training as barriers to improving cybersecurity.

(Murugan, 2012) Fraud is all about identifying and understanding the current situation and selecting prevention strategies based on cracking experience. Back in 2003, we nabbed an international criminal wanted by various Law Enforcement Agencies, including the FBI, and realized the scope of the plastic money fraud and the need for domestic measures. This method describes the nature of a situation at the time of the study and explores the causes and methods of frauds in plastic money to arrive at solutions. They utilize both primary and secondary data. Data from the primary research was obtained through this new study. Using a questionnaire, we were able to collect data to study the behaviour of card users. Researchers also avoided disclosing the participants' names or personal information in this research

"Online Financial Fraud: Risks, Vulnerabilities and Countermeasures" by M. Alazab et al. This study provided an overview of the risks, vulnerabilities, and countermeasures associated with online financial fraud. The authors identified several types of online financial fraud, such as phishing and identity theft, and discussed various countermeasures, such as multi-factor authentication and encryption. They also emphasized the importance of education and awareness in preventing online financial fraud.

"A Study on the Impact of Cybersecurity Education and Awareness Programs on the Prevention of Online Financial Fraud" by M. Alhaji and S. Mohd. This study examined the impact of cybersecurity education and awareness programs on the prevention of online financial fraud. The authors found that such programs could significantly improve individuals' knowledge and awareness of cybersecurity issues, and ultimately reduce the risk of online financial fraud. However, they also identified the need for more effective and targeted education and awareness programs.

(Mudasir Ahmad Wani, 2019) Online Social Networks (OSNs) are an excellent platform to interact, collaborate and share content. OSNs have changed the way people think, express, and socialize with the outside world. Nowadays,

Copyright to IJARSCT
www.ijarsct.co.in

DOI: 10.48175/IJARSCT-10398

529

ISSN
2581-9429
IJARSCT

there are a number of social networking sites like Facebook, Twitter, Flicker, LinkedIn, Research gate, etc., which are used by public to take out their social and professional activities.

V. FINDINGS OF STUDY

PERCENTAGE ANALYSIS
- Majority of **59.6%** respondance are 20 – 30 aged people
- Majority of **55.8%** respondance are male
- Majority of **37.5%** respondance are in Coimbatore
- Majority of **70.2%** respondance are unmarried
- Majority of **42.3%** respondance are UG
- Majority of **26%** respondance income are 30,000 – 40,000 and No work
- Majority of **38.5%** respondance are Online financial fraud are familiar with Investment site
- Majority of **48.1%** respondance are not check and read all the information provided as a disclaimer while conforming that agree options
- Majority of **37.5%** respondance are During fraud calls more financial crimes are occurring
- Majority of **28.8%** respondance are around 5,000 – 10,000 loss money because of frauds
- Majority of **33.7%** respondance are aware about crime occurring online
- Majority of **53.8%** respondance are have heared, happened hacked throw email, social net or blogs
- Majority of **36.5%** respondance are phone pay transaction most financial lost happen
- Majority of **34.6%** respondance are think most of the scam's done throw television and mobile phones
- Most of **40.4%** respondance are allow relationship to use their personal id
- Majority of **42.7%** respondance are put two-step authentication protect their online account from potential fraud
- Majority of **58.3%** respondance are improve securities measures on website and online transaction to prevent online financial fraud
- Majority of **61.2%** respondance are strongly agree that penalties for financial crime should be more severe
- Most of **34%** respondance think that public awareness and education campaign can help prevent financial crime
- Most of **42.7%** respondance think online environment is more safer and more trustworthy

Chi square
- There is no significance relationship between area they belong online financial fraud
- There is no significance relationship between area they belong check and read all the information provided as a disclaim while conforming that agree option
- There is no significance relationship between area they belong time they notice more financial crimes are occurring.
- There is no significance relationship between area they belong how much money they will lose because of frauds.
- There is significance relationship between area they belong and the aware about crime occurring online.
- There is no significance relationship between area they belong and they ever been hacked through email, social net or blogs.
- There is no significance relationship between area they belong and which transaction platform financial loss often happen.
- There is no significance relationship between area they belong and they think most of the scams done through mobile phones.

- There is no significance relationship between area they belong they allow other to use their personal ID .
- There is no significance relationship between area they belong and how important they feel checking the disclaimer information.
- There is no significance relationship between area they belong they product their online account from potential fraud.
- There is no significance relationship between area they belong that step they think should be taken to prevent online financial fraud.
- There is significance relationship between area they belong they think that public awareness and education campaign can help prevent financial crime.
- There is significance relationship between area they belong they think the online environment is more safer and more trust worthy.

VI. SUGGESTIONS

Conduct a survey: A survey can be conducted among the general public to gather information about the level of awareness of preventive measures for online financial fraud. The survey can consist of questions that focus on the different types of online financial frauds and the best practices to prevent them. Online financial platforms can provide valuable data on the types of online financial frauds that are prevalent and the frequency with which they occur. Analyzing this data can help in identifying patterns and trends, which can be used to develop better preventive measures. Study the psychology of online financial fraudsters: Understanding the psychology of online financial fraudsters can help in developing effective strategies to prevent fraud. This can be achieved by conducting interviews with convicted fraudsters to gain insight into their motives and tactics. Investigate the effectiveness of existing preventive measures: A study can be conducted to evaluate the effectiveness of the existing preventive measures, such as two-factor authentication, encryption, and anti-virus software.

VII. CONCLUSION

our study on the awareness about preventive measures towards online financial frauds has shown that while people are aware of the prevalence of such frauds, their knowledge about how to prevent them is lacking. Participants in our survey showed a general lack of knowledge regarding security measures such as using secure passwords and avoiding public Wi-Fi, which puts them at a higher risk of being targeted by fraudsters. Our findings suggest that there is a need for more effective communication and education about the risks associated with online financial transactions and the measures needed to prevent them. This could include targeted campaigns by financial institutions, governments, and other relevant organizations to increase awareness and educate the public about cybersecurity best practices. To combat the increasing threat of online financial fraud, all stakeholders – including financial institutions, technology companies, and individuals – have a role to play in ensuring that their assets are protected. By improving our knowledge and adopting preventive measures, we can work towards a safer and more secure online financial ecosystem.

BIBLIOGRAPHY

[1]. Chaturvedi, A., & Singh, A. (2020). Online Financial Fraud: Perspective of Banking Companies. Procedia Computer Science, 170, 1156-1162.
[2]. Gupta, H. (2021). Online Banking Fraud: A Review of Trends, Techniques, and Prevention Techniques. Journal of Advanced Research in Social Sciences and Humanities, 6(1), 89-101.
[3]. Kshatriya, N., & Unnikrishnan, S. (2020). Prevention and Detection of Online
[4]. Financial Fraud: A Survey on Techniques and Strategies. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 5(5), 156-166. Marandola, G., & D'Elia, A. (2021). An Overview of Online Financial Fraud: Analysis, Detection, and Prevention Techniques. International Journal of Computer Science and Information Security, 19(2), 1-11.

[5]. Nagy, Z., & Nuijten, N. (2020). Preventing Online Financial Fraud: A Comparative Study of Technological and Behavioral Solutions. Journal of Financial Crime, 27(4), 1056-1071.

[6]. Patel, S., & Patel, A. (2021). Assessing the Awareness of Preventive Measures Against Online Financial Fraud: A Case Study of Gujarat. International Journal of Business Information Systems, 38(1), 56-71.

[7]. Saravanakumar, R., & Devika, S. (2020). Online Financial Fraud: An Analysis of Trends and Preventive Measures. International Journal of Latest Technology in Engineering, Management & Applied Science, 9(1), 37-43.

[8]. Tiwari, V., & Tiwari, R. (2021). Online Financial Fraud: A Study of Awareness and Prevention Among Bank Customers in India. International Journal of Management, Technology, and Social Sciences, 6(1), 57-66.

Copyright to IJARSCT
www.ijarsct.co.in

DOI: 10.48175/IJARSCT-10398

532

ISSN
2581-9429
IJARSCT