An Analysis of Social Media Deception Among the Youth in South Kerala

Arya Ajith
Department of Commerce & Management, Amrita Vishwa Vidyapeetham, Amritapuri, India

Kavya P.
Department of Commerce & Management, Amrita Vishwa Vidyapeetham, Amritapuri, India

Durgalashmi C.V.
Department of Commerce & Management, Amrita Vishwa Vidyapeetham, Amritapuri, India

Abstract

The 21st century aka the "Digital era" has been witnessing the biggest uprisal of social media platforms, such as Meta, YouTube, Instagram, Twitter and goes on the list. These platforms are used for multi-dimensional purposes such as e-commerce, social interactions, and communications and they also serve as mega platforms for various talents ranging from artistic ones to critical reviewing. Therefore, the beneficiaries of these social media platforms are extensively high in number, as the same act as a major platform for monetary earnings and benefits. Hence, the same also has in-to fractions where a tremendous number of consumers rely on the aforementioned social media platforms to access products, services, job opportunities, relationships, and other reliant sources and purposes since high involvement can lead to other scams and frauds. Hence, it is no matter of surprise that the possibility of fraudulent approaches by social media users and account holders is high. Social media are now becoming part of every youngest's lifestyle which is a gold mine for the scammers who trap the users. People who are highly involved in social media are witnessing a high number of scams and frauds which even losing the users' data and emptying their bank accounts. social media sites are one of the most platforms where more frauds are happening and where you will find fake people and its influence leads to other scams and frauds for the users.

Keywords: *social media, social media fraud, southern Kerala.*

I. INTRODUCTION

The paper discusses the social media fraud of this time exclusive to the geography and demography of Southern Kerala. As per our Surveys and studies, we have found a startling number of social media frauds on the platform Meta, then referred to as Facebook, is the most popular social media platform with an approximate number of 2.6 B monthly active users according to reports[1]. As the population dependent on the platform rises, the possibilities of cyber scams also increase. The COVID-19 pandemic staged a huge rise in the total users of social media and every single related platform as "online" has become the new normal of the Z generation. The fraudsters are considering misusing the vulnerable users of social media by seeking advantage of the existent influencers. The brands and other advertising aspects are major examples of this. A recent YouTuber who has become prey to

this scam revealed that the fraudsters in disguise of companies of prominent products and services approach the influencers, gather their information on accounts and details, and end up hacking the very same. There have been numerous examples from different parts of the country of similar nature.

Recently, in southern Kerala, women influencers were similarly invited to be a part of Instagram lives randomly by this user, and thereby ended up stating abusive allegations against those who refused to the identification of the fraud[2]. Major types of social media fraud include fake friends, free app downloads, quizzes, hidden URLs, gathering of account-sensitive information, and going on the list. This is unending with the penultimate intention of fraud. Now as the paper is focused on, the alarming reports of social media scam/ fraud from the southern part of Kerala. Recently, a youth from Kollam posed as an Army Officer and fraudulently trapped a female social media user followed by fleecing the money, he wanted from her. He used photos of army officers and used them as his profile pictures on both Facebook and Instagram for this identity disguise and fraud.

Also, it has not been long since another resident of Thiruvananthapuram managed to scam gold ornaments amounting to 10 Lakh Rupees from a 10-year-old girl by feigning financial crisis after creating a linkage via social media[3]. Another alternate manner of social media fraud was identified in the form of crowdfunding. The charitable requests on social media significantly impact the viewers and users who generously contribute to resolving major pleas. However, when crowdfunding frauds have become a usual sight people often are put into a perplexed state regarding the genuineness of these requests. [4] Technology plays a crucial role in the banking sector and India has been the second largest telecom market in the world. (Akhil B Nair et.al 2020) banks have also tried to promote mobile banking by showing tutorials and expanding customers can carry out remotely

[6]The Cyber dome also recently booked account holders who had been managing accounts that carried fake identity details of police officers to deceive the public in Kochi and most of these fraudsters were identified to be from other states. Cybercrime is remaining as a growing challenge in terms of security and privacy practices. Working and deep learning about cyber security and crimes have been improving daily due to the increase in related cases. Cyber security experts have recently made significant advances in the fields of intrusion detection, malicious code analysis, and forensic identification. As many survey results from many online media users to people were going negative experiences as part of their social media interactions. Although the Kerala Police Cyber dome works coherently, the rise in these fraud cases does not intend to go down. police recorded crime does not generally distinguish between online and offline offenses. Whether or not the offense was committed online or offline is cyber-enabled or cyber-dependent as these offenses were recorded based on the offense in law. These viewpoints explain the depth of understanding of the word cyber crime

II. REVIEW OF LITERATURE

[7] (Santanam et al, 2011)as per their study, the recent upgrade in cyberspace has generally increased time, and forensics has attracted researcher and practitioner interests from technological, organizational, and policy-making pinpoints. These Technological advances address challenges in information sharing, surveillance, and analysis,

organizational advances are needed to encourage abortion between federal, state, and local agencies as well as some private sectors

[8] (Prasid Banerjee,2021)Over 59% of Indian adults have been becoming a victim of the growing number of cyber-crimes in the past years, as per research by the cybersecurity software company. cyber security interconnected incidents have seen a general hike in the past few years which have been aided by some cases of remote working tools. Nowadays India was also the country witnessing a rise in these cyber-crimes. Social media influencers and crypto influencers are also becoming the most wanted victims of these hackers.

[9] (Paul Sandle,2013) has been costing the global economy about $445 billion every year, and damages to businesses from the theft of intellectual property exceed $160 billion in loss to individuals from hacking.

[10] David S. Wall, 2007)is a refreshing look at new forms of crime in the world as we have entered a world that has low impact, multiple-victim crimes in which bank robbers, and nowadays we no longer have to meticulously plan the theft of millions of dollars. New technological capabilities at their disposal now mean that one person can effectively commit millions of robberies of one dollar each.

[11](Izzat Alsmadi, 2019)admits that there is no clear definition of cybercrime within the academic milieu and some quotas have been mentioned as an electronic crime or computer crime," or "computer-related crimes." There are different classifications and types of cybercrimes.

[12] Vinayakumar R, Soman KP, and Prabaharan Poornachandran (Center for Cyber Security Systems and Networks, 219 Soman KP, and Prabaharan Poornachandran (Center for Cyber Security Systems and Networks, 219: have stated theater fraud-related issues on ICT systems are all around in cyberspace and it has existed since the birth of computers from years back. Even though ICT systems continued to develop, cyber-crimes have also started to change accordingly. A certain class of cybercrimes issues and methods are discussed in detail. These cyber-crime issues and further forensic investigation require a need of detailed research and study for possible solutions systems too. For the past few years, one major area has been studied by many industries and organizations which is intrusion detection.ID systems are now becoming a popular method of theft and it is the area of great success in identifying different kinds of complex and diverse malicious foreseen threats. Major work, studies, and research are been concentrated on computer ID theft monitoring, and surveillance, and it has been a major area of study till now.

Ram Sandesh Raachandruni, Prabaharan Poornachandran (2015): Today many industries and organizations are using this SCADA (Supervisory control and data acquisition)systems, so it is a major critical area to protect the systems and the attack on these systems and PCs is causing significant damage to the infrastructure, these systems are been ten unreported which means that they are under real threat and cybercrime attacks to these can huge loss to infrastructure and other business world and ch can be a threat to human life.

[13](J.M.Drew) has described how strategies must be implemented and taken by cyber fraud victims while facing it. And how People have to be provided with effective crime prevention education and awareness campaigns to reduce cyber victimization to reduce the number of

victims in the country. Analyzing previous criminal records can be helpful to implement better solutions to stop further cybercrimes in the future.

III. OBJECTIVES OF THE STUDY

- To find out the pattern of social media fraud.
- To explore various social attributes involved
- To identify the causes in the study area.
- To point out the types that are common in south Kerala.
- To examine the consequences in the study area
- To suggest relevant solutions to the problem.
- To find out if the awareness about cybercrimes and the willingness to report cybercrime cases of the respondents

IV. SCOPE OF THE STUDY

The study focuses on the issues, patterns, s, and consequences of social media fraud in the study area. Another main intention behind this research was to identify how cyber fraud attacks is been affecting people and which social media contributes a lead role in cyber-attacks. The Field of inquiry selected for the purpose is four districts in South Kerala i.e. Ernakulum, Alappuzha, Kollam, and Trivandrum. This investigation can be extremely helpful for Social media users to know more about cyber-attacks and resolve them as well as understand the problems faced by the people and resolve those as well.

V. RESEARCH METHODOLOGY

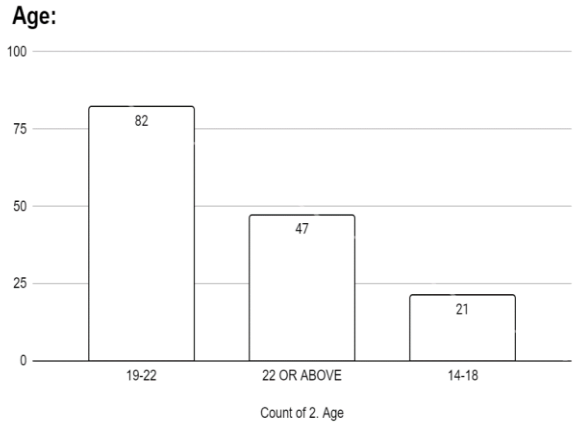
The research has been conducted using primary data collected from 150 respondents in Kerala through a survey containing a structured questionnaire, circulated digitally & secondary data available through documents, journals, magazines, websites, etc. As per our project, we collected data from online platforms like cyber cell websites, newspapers, Articles, etc.

A structured questionnaire was used for the data collection. The tool automatically consolidates all gathered data in the form of a spreadsheet. The data were analyzed using Microsoft Excel. Descriptive statistics were used to summarize the data. Sample Size: 150 Samples were taken for the study. The sampling technique used here is Judgemental sampling. The population under study here are the online media users in the city who is been involved in Social Media Applications for more than 10 years.

VI. DATA INFERENCE.

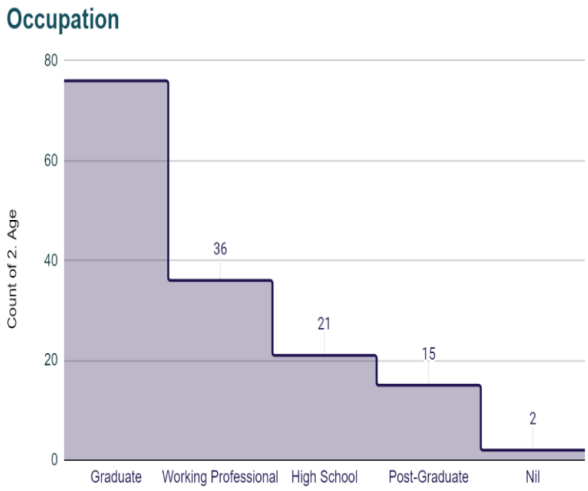
The data collected have been coded and inferred as follows:

Figure 1: Age group of respondents



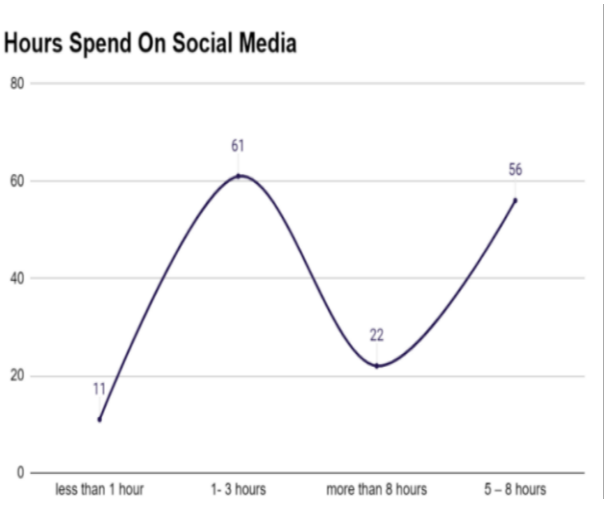
From the above diagram, nearly 14% of respondents are between the age of 14 and 18 years old, 55%of respondents are between 19 and 22 years old, and 31%% of respondents are above 22 years old.

Figure 2: Status of respondents.



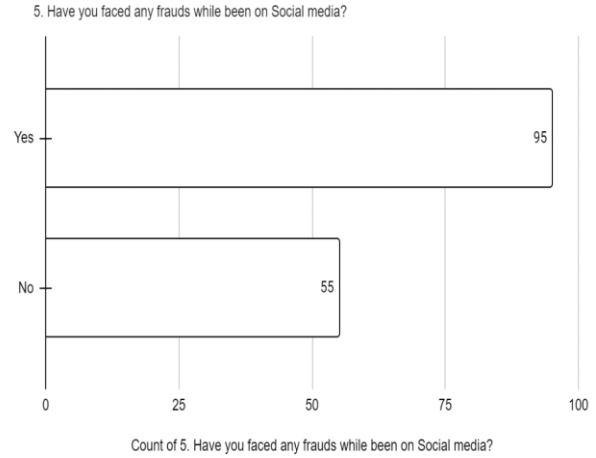
From the above figure, we can understand that majority of the respondents, i.e. 14% of respondents are high schoolers, 51% of respondents are graduates, 10%of respondents are postgraduates, 24% of respondents are working professionals and 1% of the respondents are not been included under any of these options.

Figure 3: Hours spend on social media by respondents.



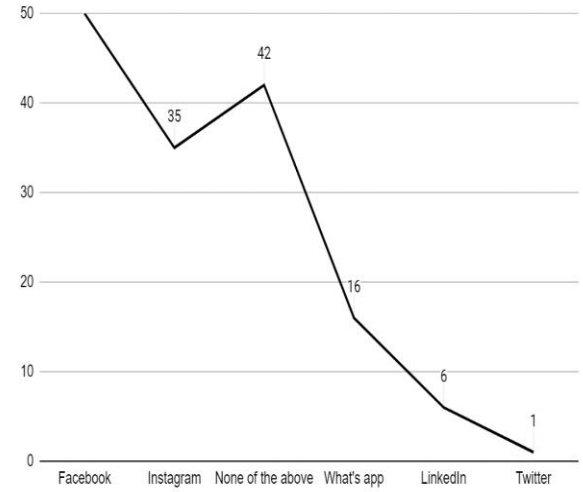
From the above figure, we can see that majority of the respondents around 7% of respondents use social media for less than 1 hour, 41% of respondents use social media for a period of 1-3 hours, 37%of respondents use social media for 5-8 hours and 15% of respondents use social media for more than 8 hours.

Figure 4: Percentage of respondents who faced social media fraud



From the above chart, we can infer that majority of the total respondents i.e.,63% of respondents have faced cyber fraud while they are using social media and 37% of the respondents have not faced any cyber fraud while being on social media.

Figure 5: Percentage of Respondents who have faced cyber fraud through different social media platforms



From the above-given figure, we can see that 33% of the respondents have faced social media fraud through Facebook, 23% through Instagram, 11% through what's an app, and 4% via Linked In. while 28% of the respondents have not faced any kind of cyber fraud through any of the above-mentioned platforms

From the data we collected, 19.3% of respondents know very well about cyber frauds, 53.3% know about it, while 24% of the respondents do not know so well about it and 3.3% don't know about cyber frauds while being on social media

From the data we collected, 49.3% of respondents never lost any money on social media, 14.7% of respondents were overcharged, 9.3% got money deducted from ba an account, 15.3% faced fraud via merchandise and 11.3% don't want to disclose anything about it.

From the data we collected, 53.3% of respondents have been never a victim of any kind of cyber fraud, 35.3% of respondents have been a victim of cyber fraud crime for 1 time, 11.3% faced cybercrime up to 2 to 5 times, and no respondents were been a victim of more than 5 times

From the data we collected, 35.3% of respondents stop using online shopping to some extent because of cyber fraud issues, 25.3% of respondents do online shopping very frequently, 29.3% does on online shopping on highly trusted websites, 4of .7% of respondents don't shop online, while 5.3% respondents completely stopped using the online shopping

From the data we collected, 60% of respondents were told that their friends and relatives have faced cyber issues, 23% of respondents have not faced any cyber issues and 17% may or may not have faced cyber issues

From the data we collected, 55% of respondents may or may not have moved legally against any cyber fraud faced by their friends or relatives, 27% of the respondents have not moved legally and 18% of respondents have legally moved against the issues they faced

From the data we collected, 25.3% have found their photos, profiles, bank details, etc been used by someone else and reported it the to admin website, 61.3%of respondents have not found someone using their ID or details of any kind, while 13.3% of don't know whether their profiles or details are used by someone else

From the data we collected, only 3.3% of respondents feel very safe about sharing their information when there are online, and 24.7% feel safe about the information they share. On the other hand, 59.3% of the respondents are not feeling safe about the information they share and about 12.7% don't know whether they should feel safe about sharing information

From the data we collected, about 5% of the respondents strongly agree that the laws in effect can control cyber fraud occurring, 17% agree 27% of the respondents have a neutral feeling about it. While 28% strongly disagree that the laws are effective and 23% of respondents simply disagree with them.

Descriptive Statistics

	Mean	Std. Deviation	N
Cyber fraud	1.3667	0.48351	150
Online shopping	2.5867	1.32192	150

Correlations

		Cyber fraud	Online shopping
Cyber fraud	Pearson Correlation	1	.386**
	Sig. (2-tailed)		0
	N	150	150
Online shopping	Pearson Correlation	.386**	1
	Sig. (2-tailed)	0	
	N	150	150

**. Correlation is significant at the 0.01 level (2-tailed).

The correlation result is .386 and the p-value is found to be less than .01 showing that it is statistically significant that there is a positive correlation between cyber fraud and online shopping.

X. FINDINGS AND SUGGESTIONS

After analyzing and summarizing the data, and interpretations we have come to know several opinions and findings from the respondents‟ data. And, we mainly came to know that half of the social media users have been receiving online threats and facing cyber fraud issues through Face book one of the world's most admired social media platforms. We have found out that most of the social media users are from the age of 19-22 which shows that youngsters are mainly involved in it about half of the population has been facing cyber fraud in their day-to-day life while being engaged in various social media apps.

We also have certain suggestions to provide after conducting the study that people should follow some security tips which assist an individual to use his/ her PC and related accessories securely and efficiently. Use anti-virus software since Anti-virus software has been designed in such a way to protect you and your computer against known viruses. But the new viruses have been emerging daily, anti-virus programs have to be updated regularly. If you use the Internet then you're a citizen from a global community—a cyber-citizen. Just like being a citizen of the local community is the same as being a cyber-citizen who has responsibilities. Make sure not to open any email or links from unknown sources. You need to store your data information on your computer in a safe place: like locked behind a password in your user account. Citizens must aware of how each site works based on the protection and security the website or social media platforms provide never trust any site at a single site or review and reveal all personal information. Never trust any unnecessary apps on the play store before downloading make sure that they are really useful and safe for your device. And uninstall those apps which are not necessary as they might be the key for the cybercriminals to gain access to one's device and mislead it.

XI. CONCLUSION

The main purpose of this paper is to make citizens realize the threats and potential attacks and to learn from these attacks to protect themselves.

So, we conclude that social media undoubtedly changed each and everyone’s life by connecting people over all the world but on the

other side from our study, we can see that people are been affecting by cyber fraudulent activities while using social media even though they are educated and aware mostly youngsters are victim for these frauds who are highly engaged in social media's.

As per the survey reports most social media users have been taken aback from online shopping up to some extent due to fear of becoming a victim of fraud and also such crimes are reportedly increasing in our society and half of the citizens are active on social media for more than 5 hours which means that they are nearly an active user's and spend more time in social media applications and can affect and trap them into cybercrimes. And we can also see that most people are hesitating to tell truth about the cybercrime they have gone through and they are not taking initiative to legally move forward to stop such malicious activities and completely remove them from society.

However, cybercrimes do not always arise from these social media platforms but various other things in cyberspace are also responsible for these attacks since social media is the key and most chosen platform by hackers to trap users to take advantage of them.

Anyone could be attacked by a cybercriminal. Though not all people are victims of cybercrimes, they are still at risk. Serious attacks are been happening every day and we should have at least basic preparation, knowledge, and principles to protect ourselves, so awareness can be the best defense. The government should also make laws against cyber fraud which can be amended to make stringent rules in the current scene where personal data is susceptible to multiple kinds of fraud. And being aware citizens, every person must limit their lifestyle on social media also manage the social media settings, and update the security regularly if you are a constant social media users. be more vigilant during online transactions and perform transactions only through safe and secured websites, avoid scams texts, and emails and educate people around us about the same. make sure that you always use a full-service internet security suite like using some trusted security software. identity theft is also becoming a new age theft by making fake profiles that can scam people and loot money from their friends and acquaintances make sure that if you become a victim alert to authorities about it and never panic in those situations, your report may assist authorities to stop taking advantage of other people in the future. so always make sure that prevention is better than cure.

Reference

[1] Sk. M. B. S. N. Dr. K. Kiran Kumar, “A Survey of Cyber Crimes,” International Journal of Engineering Research & Technology (IJERT), 2016.

[2] Dr. S. S. B. Y. V. Dr. P. M. Teen Jose, “Cyber Crimes in Kerala: A stud,” Advances in Computational Sciences and Technology, vol. 10, no. 5, pp. 1153–1159, 2017.

[3] R. Sivaraman, “Cyber scam involving social media influencers surfaces,” Jun. 2021.

[4] A. A. Anju Mohan, “Impact of Technological Innovation on Bank Employees Stress,” Jour of Adv Research in Dynamical & Control Systems, vol. Vol. 11, 0, no. Special Issue, 2019.

[5] A. S. P. Akhil B Nair, Keerthana S Prabh, B.R. Aditya, C.V. Durgalashmi, “Study on the Usage of Mobile Banking Application during COVID-19 Pandemic,” Webology, vol. Volume 18, no. Volume 18, Special

Issue on Information Retrieval and Web Search, 2020.

[6] A. A. Nandana Gopal R, Akshaya V S and A. A, "A STUDY ON CUSTOMER SATISFACTION TOWARDS SBI YONOWITH SPECIAL REFERENCE TO KOLLAM DISTRICT," International Journal of Psychosocial Rehabilitation, vol. 24, no. 8, 2020.

[7] R. Santanam, M. Sethumadhavan, and M. Virendra, Eds., "Cyber Security, Cyber Crime and Cyber Forensics," 2011, doi: 10.4018/978-1-60960-123-2.

[8] Prasid Banerjee, "Over 59% Of Indian Adults Fell Victim To Cyber Crime Over Past 12 Months," Mint, 2021.

[9] Paul Sandle, "Cyber crime costs global economy $445 billion a year," Reuters, 2013.

[10] David S. Wall, Cybercrime: The Transformation of Crime in the Information Age. Wiley, 2007.

[11] Izzat Alsmadi, The NICE Cyber Security Framework. 2019.

[12] A. S. of E. C. A. V. V. I. Vinayakumar R (Center for Computational Engineering and Networking (CEN), A. S. of E. C. A. V. V. I. Soman KP (Center for Computational Engineering and Networking (CEN), and A. S. of E. A. A. V. V. I. Prabaharan Poornachandran (Center for Cyber Security Systems and Networks, "A Comparative Analysis of Deep Learning Approaches for Network Intrusion Detection Systems (N-IDSs): Deep Learning for N-IDSs," International Journal of Digital Crime and Forensics (IJDCF) 11(3), pp. 1–25, 2019.

[13] J. M. Drew, "A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies," Journal of Criminological Research, Policy and Practice, vol. 6, no. 1, 2020, doi: 10.1108/JCRPP-12-2019-0070.