| Volume 7 | Issue 1 | NOV. 2024

MAKTABAH JAFARIYAH
Knowledge & Research Academy

The International Journal
ISSN 2581-4354

UNDERSTANDING AND PREVENTING CYBER SCAMS: A STUDY ON INIDAN POPULATIONS

Mr. Sirajbhai Abbasbhai Nagalpara*
Dr. Bhavesh M. Patel**
Mr. Ahesanali Shabbirali Dadavala***

**Department of Computer Science, Hemchandracharya North Gujarat University, Patan, Gujarat.*
*** Department of Computer Science, Hemchandracharya North Gujarat University, Patan, Gujarat.*
**** Department of Computer Science, Hemchandracharya North Gujarat University, Patan, Gujarat.*

Abstract — Social media's widespread effect on contemporary life has made it easier to communicate, share experiences, and do business. However, internet fraud has increased as a result of this widespread usage, especially for people living in rural regions. The purpose of this study is to investigate how rural populations perceive cyber scams and how cybersecurity awareness might aid in averting them. The "Internet generation," a group recognized for its significant dependence on social media platforms in day-to-day activities, is the focus of this study. According to earlier studies, more than one-third of people living in rural areas have fallen victim to social media fraud. The inquiry explores a number of online frauds, such as hoaxes about account termination, healthcare-related scams, gossip-based fraud, lottery and gift card schemes, and catfishing. This study will also examine characteristics like greed, curiosity, and credulity that render rural communities vulnerable to these frauds. According to this study, one important independent factor influencing the frequency of cyber scams is cybersecurity knowledge. This awareness extends beyond online computer protection to cover hardware, software, data, and information security in digital systems. It also includes comprehending security hazards and taking appropriate steps to reduce risks. The ultimate goal of this study is to provide information for the creation of practical plans for raising rural communities' understanding of cybersecurity.

Keywords - Cyber Scams, Social Media, and Cybersecurity.

Background:

Since social media makes it possible to communicate, share experiences, and even conduct business, it has become an essential part of many people's everyday life.

Significance:

Online fraud has increased in parallel with the widespread use of social networking sites, especially among Indian rural populations.

Current Understanding:

Research has indicated that over one-third of rural people in India are victims of social media-based scams.

Research Gap:

This investigation seeks to examine people's understanding of cyber fraud and the impact of digital security education on preventing such occurrences.

Research Inquiry:

How much do people know about cyber scams, and how does cybersecurity awareness affect how often these fraudulent acts occur?

Aim/Objective:

With the ultimate objective of reducing the frequency of online frauds, this study aims to help develop practical strategies to raise cybersecurity awareness among Indian rural residents.

Hypothesis:

According to this study, those who are more knowledgeable about cybersecurity are less likely to become victims of fraudulent schemes that use social media.

I. INTRODUCTION

In recent years, social media platforms have become widely used, revolutionising everyday routines, communication, and information access. Geographical distances have been overcome by this digital revolution, but it has also made some communities more vulnerable to new online threats. Social media frauds have made rural populations more vulnerable, which highlights the urgent need for better cybersecurity education in these areas. Cyber fraud has increased in the digital age, with many frauds aiming to defraud both people and businesses. Due to their lack of technical knowledge, older adults—particularly those over 60—are more vulnerable to fraudulent operations (Sugunaraj et al., 2022).

The purpose of this study is to assess rural communities' awareness of cyber scams and look into how important cybersecurity education is in averting such occurrences. The focus of the research is the "Internet generation," a demographic that primarily relies on social media for many facets of their lives. This study aims to offer important insights into the developing fields of cybersecurity and digital literacy by examining the intricate link between rural communities and social media frauds. The capacity of Internet users to recognise and steer clear of fraudulent transactions can be enhanced by consumer education (Berzins 2010).

An examination of the several social media scams that commonly target rural communities is one of the main topics covered in this study. These scams range from lottery and gift card schemes to more sophisticated types of deception including catfishing and account cancellation scams. Additionally, the study investigates psychological aspects like trust, curiosity, and greed that make rural residents susceptible to these frauds.

Examining cybersecurity awareness as an independent variable that affects the prevalence of cyber scams is a key component of this research. This entails assessing how well rural people comprehend security issues, how capable they are of taking responsible action to reduce hazards, and how capable they are of extending protection beyond internet computers to encompass equipment, software, data, and information in online systems. Raising internet users' understanding of cybersecurity is crucial to thwarting cyber frauds. Web-based applications that allow users to report instances of cybercrime and offer instructional materials to safeguard gadgets, social media accounts, and private data might be created (Sun and Hassan, 2022). More than one-third of rural inhabitants have been the victims of social media frauds, according to earlier studies, underscoring the frequency and gravity of this problem. This study sought to aid in the creation of practical plans for raising cybersecurity awareness in rural communities by examining these patterns and their root causes.

II. A. LITERATURE REVIEW

Cyber fraud is a major obstacle to digital financial inclusion, especially in rural areas. While digital banking technology use in rural India encourages financial inclusion, it also makes people more susceptible to cybercrime (Afzal et al., 2024).

Implementing strong cybersecurity measures and educating rural communities about possible hazards are essential to combating growing cyber threats (Shabiya & Alkar, 2023).

As demonstrated in Nigeria, digital forensic accounting has the potential to lower cyber fraud instances (Awodiran et al., 2023).

To overcome these issues, specific cybersecurity education and awareness initiatives are desperately needed in rural communities (Koshy, 2022).

A recurring problem, the "419 scam" or Nigerian scam has spread from postal mail to online and includes a variety of frauds, including advance fee schemes, phoney lotteries, and blackmail (Falade, 2023).

Data analytics and machine learning algorithms can be used to help antifraud activities (Zhu et al., 2023).

Understanding and responding to cyber fraud and scams requires a more efficient and victim-centered strategy, which includes investigating victim support networks and new countermeasures (Button & Cross, 2017).

While cyber security knowledge among payment banking users should assist protect rural digital banking users from cyber fraud, the structural model shows that growing cyber fraud has become a significant barrier to digital financial inclusion in rural regions (Afzal et al., 2024).

Due to their lack of knowledge and education about cybersecurity, rural communities are more vulnerable to numerous cyberthreats as a result of the rising availability of internet services (Koshy, 2022).

A. Scam Types

1. Phishing scam

Phishing is a dishonest cyberattack that mimics trustworthy websites in order to obtain personal information (Khan, 2021).

These communications, which frequently come in the form of emails, texts, or even phone calls, usually include harmful files or links to phoney websites.

The goal is to trick unwary victims into divulging their financial or personal information so that it may be used maliciously for identity theft, financial fraud, or other crimes.

The top types include:

1.1 Email

1.2 Spear

1.3 SMS

1.4 Voice

1. Investment Scam

A Ponzi scheme is a dishonest investment plan that promises investors large returns. The promised rate of return is frequently unrealistically high in practice. Instead of making a real profit from economic activity, the plan makes returns for previous investors using their own money or money from later investors. In recent years, investment cyber frauds have grown more common and complex, presenting serious hazards to people and businesses everywhere (Suela, 2024). Unreasonably high return promises, pressure to make decisions right now, unclear business justifications, and opaque management structures are all common signs of investment frauds (Chariri et al., 2018). Additionally, they use technology and rich media to make their schemes seem more legitimate and to help them build extremely intimate connections with their victims (Anderson et al., 2024).

2. Romance Scam

There are many examples of online romantic interests and pals that appear to be trustworthy but are actually scammers on the Internet. To safeguard oneself from psychological harm and monetary losses, Internet users must be alert and cautious when interacting online.

Cybercriminals fabricate love relationships on dating sites as part of romance cyberscams in order to take advantage of victims emotionally and financially (Bilz et al., 2023). Married and educated people are more susceptible to these frauds, which usually target people between the ages of 25 and 45 (Saad et al., 2018). These frauds remain a serious risk, frequently leaving victims with long-term psychological consequences in addition to financial losses (Tandana, 2022).

Potential causes

Reliance on dating apps like Bumble and Tinder to locate a companion.

phoney profiles on marriage-matching websites.

increased usage of Facebook and other social networking apps. Gleeden is one of the dating and extramarital dating applications.

feelings of isolation-related loneliness or worry, especially during the COVID-19 epidemic.

3. Merchant Fraud

When a fraudster poses as a genuine merchant in order to carry out fraudulent transactions or steal money, this is known as merchant fraud. This may entail tricking real consumers into making pointless transactions or acquiring a merchant account to process payments using stolen cards.

This kind of fraud can involve making phoney websites or ads that look like they are from real vendors, as well as utilising credit or debit cards that have been stolen to make transactions (Malik, 2024). Additionally, as demonstrated by the changing patterns in 419 scam emails, the popularity of cryptocurrencies has given rise to new scam versions (Falade, 2023).

Cybersecurity Awareness

The importance of cybersecurity awareness in protecting people, organisations, and society from online dangers is becoming more widely acknowledged. The need of creating thorough awareness campaigns to address human aspects in cybersecurity has been underlined by several research (Al-Tajer & Ikuesan, 2022). A key component of contemporary information technology is cybersecurity awareness, which aids in shielding private information and systems from potential damage and illegal access (Kumar et al., 2023).

Privacy

Because users frequently reveal private

information without realising it, data privacy on social media platforms is a major worry that can result in both financial and societal concerns (Aghasian et al., 2017). Numerous pieces of personal data, such as user profiles, relationships, and activities, may be found on online social networks (OSNs). According to Wang and Nepali (2015), revealing private information may lead to identity theft, financial loss, and harassment. Users must comprehend the idea of privacy and get an early understanding of the difference between information and secrets in order to improve privacy protection (Alvarez, 2021).

Password Management

A key element of cybersecurity that offers an extra degree of security beyond conventional password-based authentication is two-factor authentication (2FA) (Hossain et al., 2023).

III. RESEARCH METHODOLOGY

A. Introduction

The 2022 report is the most recent one currently accessible. The NCRB reports that 10395, 14007, and 17470 incidents of cybercrime fraud were reported in 2020, 2021, and 2022, respectively. There is no distinct data kept by the NCRB for fraud via phoney websites.

Criminal behaviour on the internet has been rising significantly. The number of victims of cybercrime has increased 16 times since 2001 (from 6 to 91 victims per hour), and the amount of money lost has increased more than 570 times (from ₹166,000 to around ₹99.6 million losses per hour). At least 7,303,267 people were impacted by cybercrime throughout the 22-year period, which also caused losses of ₹3 trillion.

B. Research Design

Amixed-method approach that incorporates both quantitative and qualitative data was used in this investigation. Secondary data sources like the Indian Computer Emergency Response Team (CERT-In), the National Crime Records Bureau (NCRB), cybersecurity reports from major companies like Symantec, Kaspersky, and McAfee, and government agencies like the Ministry of Electronics and Information Technology (MeitY) will be the source of quantitative data. Important information about financial cybercrimes, including digital payment fraud, is also provided by the Reserve Bank of India (RBI).

Interviews and questionnaires were used to gather qualitative data. Various age groups, such as professionals, seniors, and students, will be the focus of surveys to determine their experiences with cybercrime. Thorough insights into new cyberthreats and defence tactics will be obtained through in-depth interviews with cybersecurity specialists, law enforcement officers, and digital security specialists.

C. Data Collection Methods

To give a thorough picture of cybercrime trends, this study collects quantitative data from a variety of secondary sources. An essential resource for tracking the evolution of cybercrime in India is the National Crime Records Bureau (NCRB), which provides historical data on the crime. In order to investigate cyberattack trends, including threat kinds and frequency, the research also used data from the Indian Computer Emergency Response Team (CERT-In). This research examines industry publications from top cybersecurity firms, including Symantec, Kaspersky, and McAfee, to obtain insights into regional and worldwide cybercrime trends as well as new attack techniques and vulnerabilities. The Ministry of Electronics and Information Technology (MeitY) in particular will be the source of data on digital crime statistics and public cybersecurity activities. This study focusses on digital payment fraud, ATM skimming occurrences, and other types of financial cyber fraud, utilising data from financial institutions, including the Reserve Bank of India (RBI), to comprehend the impact of cybercrime on the financial sector. This wide range of data sources will provide a strong basis for examining cybercrime in India.

The growing internet usage across all demographics has affected the age distribution of cybercrime victims in India, as seen in Table 1. Based on existing statistics and trends, the approximate number of victims per age group is broken down as follows:

Table 1: Impact of different cybercrimes

Type of Cybercrime	Description	Impact/Statistics
Phishing Attacks	Fraudulent attempts to obtain sensitive information via emails or messages	Over 17 million cases in 2021, with individuals and businesses affected
Financial Fraud	Unauthorized access to bank accounts and credit card information	₹615 crore lost in 2021 due to UPI and digital payment frauds
Identity Theft	Stealing personal information to commit fraud	52,974 cases reported in 2020, leading to personal and financial losses
Online Harassment	Cyberstalking, bullying, and blackmailing	Over 20% of internet users in India have reported harassment

ATM/Debit Card Frauds	Fraud involving the use of ATM or debit cards	13,993 incidents reported in 2020, with significant personal financial loss
Online Child Exploitation	Circulation of child pornography and abuse content	19,000+ reported cases in 2020
Cryptocurrency Scams	Fraudulent schemes involving cryptocurrencies	Significant rise in crypto-related fraud; over ₹1,000 crore lost in 2021

An estimated breakdown of India's cybercrime victim count by age group during the past few years, based on trends and occurrences recorded, is shown in Table 2:

Table 2: Yearly growth of cybercrime costs

Year	Estimated Cybercrime Costs (₹)	Growth Rate (%)	Notable Cybercrime Incidents
2016	₹18,000 crore	-	Significant rise in phishing attacks, data breaches
2017	₹21,000 crore	16.67%	Ransomware (WannaCry, Petya) spread widely
2018	₹25,000 crore	19.05%	Increase in ATM/debit card fraud and cryptocurrency scams
2019	₹29,000 crore	16.00%	Data breaches targeting large companies, mobile malware surge
2020	₹38,000 crore	31.03%	Rise in COVID-19-related phishing and scams
2021	₹50,000 crore	31.58%	Increase in ransomware attacks on businesses
2022	₹68,000 crore	36.00%	Surge in UPI fraud, social engineering, and data theft
2023	₹1.25 lakh crore	83.82%	Rise in targeted ransomware, large-scale data breaches, AI-driven cyber attacks

In Fig. 1. data can be represented in a bar chart format to show the comparison of cybercrime victim counts across different age groups and over the years (Figure-1)

IV. SUGGESTED FRAMEWORK

Users may be protected against online fraud and scams by putting in place a number of procedures that priorities protecting private information, Internet use, and financial transactions. (Figure-2)

V. CONCLUSION

This research underscores the importance of enhancing cybersecurity knowledge among internet generation, especially people in India, to protect them from diverse social media-based fraud.

Future Scope: The results of this investigation can be utilized to create successful approaches for improving cybersecurity education among people in India, potentially leading to a decrease in online scams in the coming years.

REFERENCES

Afzal, M., Meraj, M., Kaur, M., & Shamim Ansari, M. (2024). How does cybersecurity awareness help in achieving digital financial inclusion in rural India under escalating cyber fraud scenario? Journal of Cyber Security Technology, ahead-of-print(ahead-of-print), 1–39. https://doi.org/10.1080/23742917.2024.2347674

Aghasian, E., Gao, L., Garg, S., Montgomery, J., & Yu, S. (2017). Scoring Users' Privacy Disclosure Across Multiple Online Social Networks. IEEE Access, 5, 13118–13130. https://doi.org/10.1109/access.2017.2720187

Al-Tajer, M., & Ikuesan, R. (2022). Cyber Security Threat Awareness Framework for High School Students in Qatar. cornell university. https://doi.org/10.48550/arxiv.2207.00820

Alvarez, T. (2021). Meta-Analysis of Social Networking Sites for the Purpose of Preventing Privacy Threats in the Digital Age. Journal of Applied Data Sciences, 2(3), 64–73. https://doi.org/10.47738/jads.v2i3.36

Anderson, M., March, E., Land, L., & Boshuijzen-Van Burken, C. (2024). Exploring the roles played by trust and technology in the online investment fraud victimisation process. Journal of Criminology. https://doi.org/10.1177/26338076241248176

Awodiran, M. A., Anwana, A., Idem, U. J., Ogundele, A. T., & Emem, O. (2023, January 26). Digital Forensic Accounting and Cyber Fraud in Nigeria. https://doi.org/10.1109/cymaen57228.2023.10050992

Berzins, M. (2010). Online Scams (pp. 561–573). igi global. https://doi.org/10.4018/978-1-60566-368-5.ch049

Bilz, A., Shepherd, L. A., & Johnson, G. I. (2023a). Tainted Love: a Systematic Literature Review of Online Romance

Scam Research. Interacting with Computers, 35(6), 773–788. https://doi.org/10.1093/iwc/iwad048

Button, M., & Cross, C. (2017). Cyber Frauds, Scams and their Victims. https://doi.org/10.4324/9781315679877

Chariri, A., Sektiyani, W., Nurlina, N., & Wulandari, R. W. (2018). INDIVIDUAL CHARACTERISTICS, FINANCIAL LITERACY AND ABILITY IN DETECTING INVESTMENT SCAMS. JURNAL AKUNTANSI DAN AUDITING, 15(1), 91. https://doi.org/10.14710/jaa.15.1.91-114

Falade, P. V. (2023). Trend and Emerging Types of “419” SCAMS. Advances in Multidisciplinary and Scientific Research Journal Publication, 2(1), 105–114. https://doi.org/10.22624/aims/csean-smart2023p13

Hossain, M. N., Zaman, S. F. U., & Sayeed, M. S. (2023, January 23). Adding Knock Code Technology as a Third Authentication Element to a Global Two-factor Authentication System. https://doi.org/10.1109/icssit55814.2023.10060915

Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (2013). Improving Password Cybersecurity Through Inexpensive and Minimally Invasive Means: Detecting and Deterring Password Reuse Through Keystroke-Dynamics Monitoring and Just-in-Time Fear Appeals. Information Technology for Development, 20(2), 196–213. https://doi.org/10.1080/02681102.2013.814040

Khan, M. (2021). Detection of Phishing Websites Using Deep Learning Techniques. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), 3880–3892. https://doi.org/10.17762/turcomat.v12i10.5094

Koshy, R. (2022). Need for Cybersecurity Awareness in Rural Communities: A Socio-Legal Perspective. International Journal of Advanced Research in Science, Communication and Technology, 233–237. https://doi.org/10.48175/ijarsct-7786

Kumar, G., Kumar, M., Pandey, S. K., Kumar, A., Varshney, N., & Singh, K. U. (2023, April 8). Cybersecurity Education: Understanding the knowledge gaps based on cyber security policy, challenge, and knowledge. https://doi.org/10.1109/csnt57126.2023.10134610

Malik, A. A. (2024). Online shopping, Cyber frauds and Fraud prevention Strategies. International Journal for Electronic Crime Investigation, 8(1), 49–56. https://doi.org/10.54692/ijeci.2024.0801186

Medlin, B. D., & Cazier, J. A. (2005). An Investigative Study: Consumers Password Choices on an E-Commerce Site. Journal of Information Privacy and Security, 1(4), 33–52. https://doi.org/10.1080/15536548.2005.10855779

Pratap, M., & Das, A. (2023). Designing a Random Password Generator Using Python Programming Language. International Journal of Scientific Research in Science, Engineering and Technology, 450–454. https://doi.org/10.32628/ijsrset23103138

Saad, M. E., Zamri, M., & Norul, S. (2018). Cyber Romance Scam Victimization Analysis using Routine Activity Theory Versus Apriori Algorithm. International Journal of Advanced Computer Science and Applications, 9(12). https://doi.org/10.14569/ijacsa.2018.091267

Shabiya, N. M., & Alkar, H. (2023). A study of cybercrime and cybersecurity. I-Manager's Journal on Digital Forensics & Cyber Security, 1(1), 15. https://doi.org/10.26634/jdf.1.1.19082

Stainbrook, M., & Caporusso, N. (2019). Comparative Evaluation of Security and Convenience Trade-Offs in Password Generation Aiding Systems (pp. 87–96). springer. https://doi.org/10.1007/978-3-030-20488-4_9

Suela, L. C. (2024). Online Fraud Exposed: Tactics and Strategies of Cyber Scammers. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT, 08(04), 1–5. https://doi.org/10.55041/ijsrem31604

Sugunaraj, N., Ranganathan, P., & Ramchandra, A. R. (2022). Cyber Fraud Economics, Scam Types, and Potential Measures to Protect U.S. Seniors: A Short Review. 623–627. https://doi.org/10.1109/eit53891.2022.9813960

Sun, E., & Hassan, N. H. (2022, December 2). Cybercrime Incident Reporting System. https://doi.org/10.1109/icmnwc56175.2022.10031682

Tandana, E. A. (2022). AMID THE THREAT OF CYBERCRIME. QUAERENS: Journal of Theology and Christianity Studies, 4(2), 129–147. https://doi.org/10.46362/quaerens.v4i2.214

Wang, Y., & Nepali, R. K. (2015, June 1). Privacy threat modeling framework for online social networks. https://doi.org/10.1109/cts.2015.7210449

Zhu, C., Zhang, C., Wang, R., Tian, J., Hu, R., Zhao, J., Ke,

Y., & Liu, N. (2023). Building of safer urban hubs: Insights

from a comparative study on cyber telecom scams and early

warning design. Urban Governance, 3(3), 200–210.

https://doi.org/10.1016/j.ugj.2023.05.004

FIGURE:

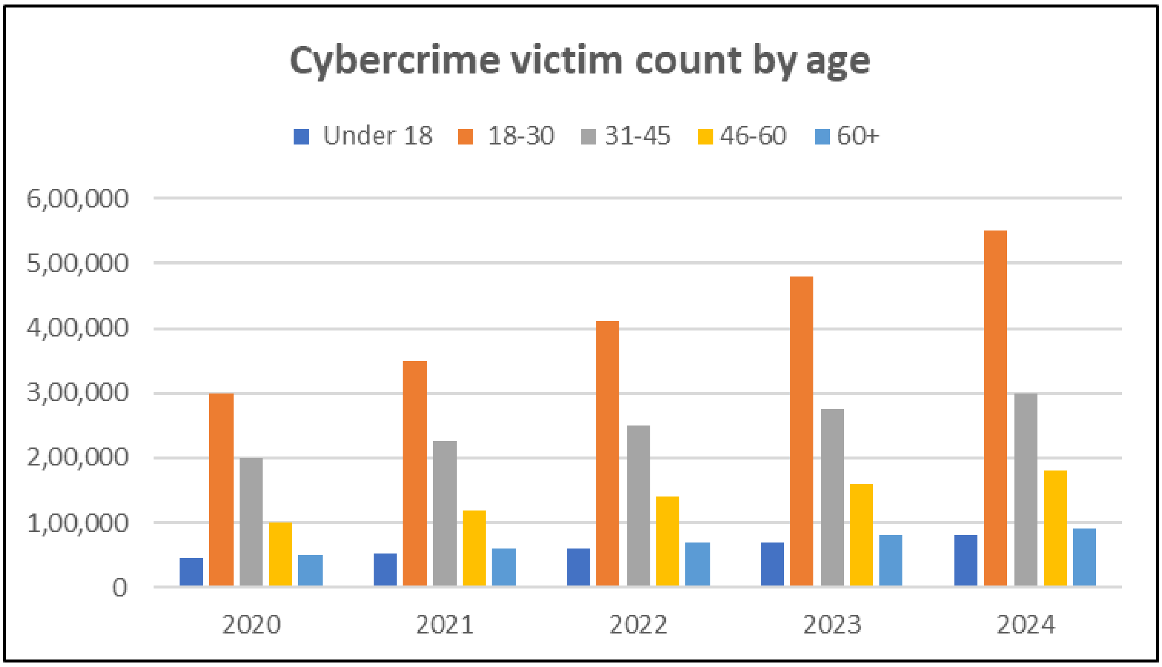
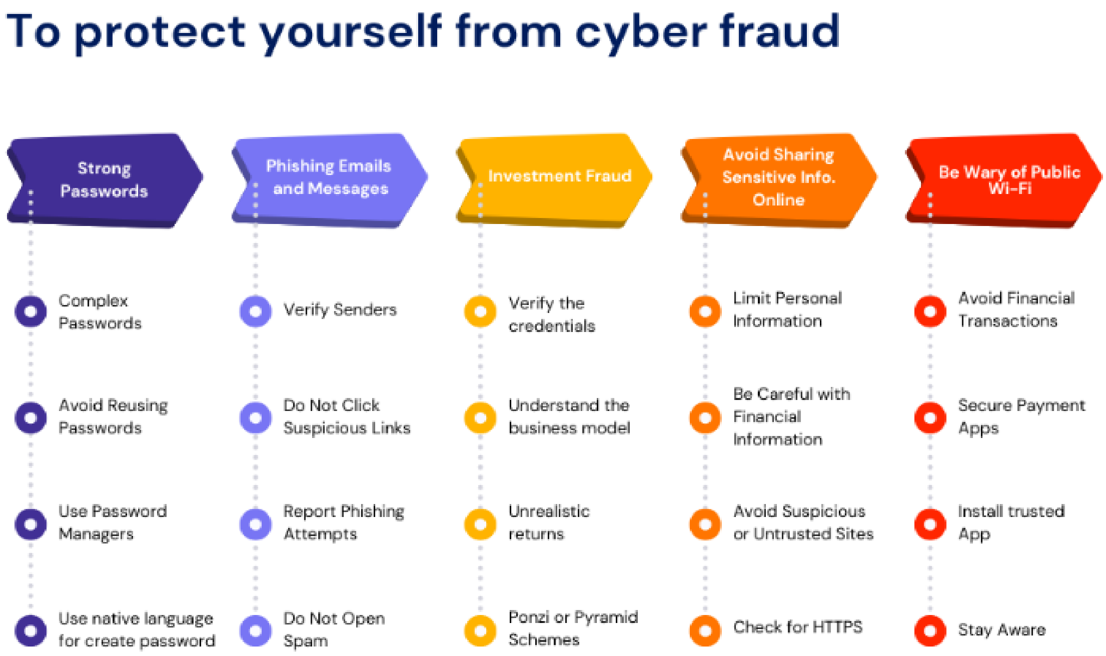


Fig. 1. Cybercrime Victim



To protect yourself from cyber fraud

Strong Passwords
- Complex Passwords
- Avoid Reusing Passwords
- Use Password Managers
- Use native language for create password

Phishing Emails and Messages
- Verify Senders
- Do Not Click Suspicious Links
- Report Phishing Attempts
- Do Not Open Spam

Investment Fraud
- Verify the credentials
- Understand the business model
- Unrealistic returns
- Ponzi or Pyramid Schemes

Avoid Sharing Sensitive Info. Online
- Limit Personal Information
- Be Careful with Financial Information
- Avoid Suspicious or Untrusted Sites
- Check for HTTPS

Be Wary of Public Wi-Fi
- Avoid Financial Transactions
- Secure Payment Apps
- Install trusted App
- Stay Aware

Fig. 2. Proposed Model for preventing Cyber Fraud