IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Digital Deception:An Exploration Of Online Fraud Schemes And Prevention Strategies

[1]Dr. Kudshiya Raza, [2]Dr. Surbhi Jain, [3] Dr. Ekta Mukar
[1]Assistant Professor , [2] Assistant Professor, [3] Assistant Professor
[1]Department of Commerce,
[1]St.Aloysius College(Autonomous)Jabalpur, India

Abstract:
The quick rise in digital interactions and online transactions has made it easier for online fraud schemes to flourish, leading to large financial losses and compromised personal information. The purpose of this study is to investigate how internet fraud methods, such as phishing, identity theft, and social engineering attempts, are changing. To investigate the strategies, techniques, and procedures (TTPs) utilized by online fraudsters, a mixed-methods approach comprising surveys and Questionnaire will be utilized. Data was collected from a sample of 295 respondents, selected through random sampling to ensure diversity in age, education, and digital exposure Furthermore, this study will examine the efficacy of current preventative measures such digital literacy initiatives, anti-phishing software, and two-factor authentication. This paper aims to show internet awareness and Literate rate among users. It's also covered effective preventive strategies related to online frauds. The results of the study also help to create a thorough framework for stopping online fraud, offering guidance to legislators, law enforcement, and anybody else looking to safeguard oneself against online fraud

Index Terms - Cyber Fraud, Internet literacy, Digital Security and Prevention Strategies

I. Introduction

The international community has serious concerns regarding India. Illicit activities have increased in tandem with the introduction, development, and use of information and telecommunications technology. Cybercriminals use phony websites, compromised emails, and anonymous servers as tools and media for fraud. Large sums of money to participate in business proposals are not the only crimes that fall under this category; romances, lotteries, and charity scams are also included. Diverse estimates exist for the overall losses resulting from this scenario. Therefore, worldwide collaboration is required to stop illegal activities and safeguard Internet users. While legislation and new methods are continuously being adopted to combat and remove various types of fraud, cyberspace is also offering new tools and means to make it easier to commit these scams. considering this, we discuss and examine a few topics on the methods employed by cybercriminals to commit fraud, particularly financial fraud. Using India as a case study, it also analyzes the effectiveness of the current legal and regulatory framework in preventing this type of cross-border crime. This essay discusses the historical roots of financial scams and provides a brief overview of some of the most well-known ones that have occurred recently in India. Digital banking has become more important in the present digitalization era as a result of India's most recent demonetization

Review of Literature

Cyber Attack on online Banking

1. **D. M. M., & Nalawade, M. P. J. D. K. (June 2023)** - "A Review of Cyber-attacks on Online Bank Accounts." In this they outline about the situation related to Online banking as in the twenty-first century it has become a necessary part of life. Finding the source of the crime, shortages in training, and the growth of the underground economy all play a role in decreasing cybercrime. Volume 2 Issue7, **ISSN: 2582-6433.**

Fraud in Banking Sector

2. **Sharma, N., & Sharma, D. (2017)** – According to "Banking Fraud in India: An Empirical Study of the Impact of Employee Education Cryptographic" research has checked barriers like multipoint inquiries which can help banks to keep their customers' confidence. **Swain, S., & Pani, L. K. (2016)** - "Bank fraud in India", it has witnessed a rise in recent years. This research has highlighted the compliance with the Reserve Bank of India's KYC regulations is not being adequately upheld and there is a lack of dedication among bank employees towards their responsibilities.

Economic and Global Perspective on Fraud

Yego, J. K. (2016) - According to his research on 'Fraud has risen to the level of a major global issue"and is not likely to diminish any time soon. This study shows that many businesses lose their trust and money too.

Jagtap , (2014) a survey conducted amongst the educated respondents shows that 38% of the customers are still non user of online banking because of low security level, risk of fraud and no guidance for operation. It is concluded that despite being educated customers are reluctant to use online banking as they feel it is unsafe to use.

previous studies on cyber fraud or digital fraud revealed a significant research gap regarding the prevention of cyber fraud, including government initiatives, policies, and prevention strategies.

Objectives of the study

II. To assess the level of digital literacy among internet users and its relationship with online fraud vulnerability.

III. To evaluate the effectiveness of preventive strategies such as two-factor authentication and password updates in reducing fraud incidents.

IV. To analyze the association between users' online safety practices and their experience with digital fraud.

V. To suggest practical measures for improving digital security and minimizing online fraud risks.

3.1Population and Sample

This study employed a quantitative, cross-sectional research design to examine the relationship between digital literacy, preventive strategies, and users' vulnerability to online fraud. Data was collected from a sample of 295 respondents, selected through random sampling to ensure diversity in age, education, and digital exposure

3.2 Data and Sources of Data

A structured questionnaire served as the primary data collection tool, featuring a combination of Likert scale questions to assess awareness and behaviors, along with yes/no items to identify experiences with online fraud and use of preventive measures. The key variables studied included digital literacy and preventive strategies (such as two-factor authentication and password changes) as independent variables, and fraud victimization as the dependent variable. Demographic factors such as age, gender, and frequency of internet use were also considered. The collected data were analyzed using descriptive statistics, correlation analysis, and Chi-square tests. Correlation analysis was applied to examine the relationship between digital literacy and fraud vulnerability, while the Chi-square test was used to test the association between preventive strategies and fraud experiences. Hypotheses were tested at a 5% level of significance. The study found no significant correlation between digital literacy and fraud risk, but a statistically significant association between the use of preventive strategies and reduced fraud cases. Limitations of the study include the reliance on self-reported data and a limited range of preventive behaviours considered. Despite these limitations, the methodology provided a clear framework to explore the effectiveness of proactive security behaviours in combating online frau

HYPOTHESES OF THE STUDY:

1. **H_{01} (Null Hypothesis):** There is no significant relationship between users' digital literacy and their vulnerability to online fraud.
   H_{11} (Alternative Hypothesis): There is a significant relationship between users' digital literacy and their vulnerability to online fraud.

2. **H_{02}:** Preventive strategies such as two-factor authentication and regular password changes have no significant impact on reducing online fraud cases.
   H_{12}: Preventive strategies such as two-factor authentication and regular password changes significantly reduce online fraud cases

DATA ANALYSIS AND INTERPRETATION

The collected data from 295 respondents was analyzed to explore patterns of online fraud exposure, preventive behaviours, and demographic influences. Descriptive statistics and cross-tabulations were used to interpret key trends and relationships within the dataset

Table 1: **Fraud Victims by Age Group**

Age Group	Not Victimized	Victimized	Total	% Victimized
Under 18	46	22	68	32.40%
18–24	34	12	46	26.10%
25–34	45	17	62	27.40%
35–44	57	16	73	21.90%
45 and above	33	13	46	28.30%
Total	**215**	**80**	**295**	

Source: Primary Data

Interpretation:

- The Under 18 age group has the highest victimization rate at 32.4%, indicating potential vulnerability due to lack of digital maturity.
- Middle-aged adults (35–44) have the lowest victimization rate (21.9%), possibly due to experience and caution online.
- Across all age groups, fraud is a relevant risk but younger and older users appear more susceptible.

Table 2: **Fraud Victims by Gender**

Gender	Not Victimized	Victimized	Total	% Victimized
Male	86	23	109	21.10%
Female	70	29	99	29.30%
Other	59	28	87	32.20%
Total	**215**	**80**	**295**	

Source: Primary Data

Interpretation:

- Respondents identifying as the 'Other' gender category show the highest victimization rate (32.2%), followed by females.
- Males reported the lowest fraud rate at 21.1%, possibly due to greater self-protection behavior or underreporting.
- Gender disparities may suggest the need for targeted awareness programs, especially for vulnerable or underrepresented groups.

Table 3: **Fraud Victims by Education Level**

Education Level	**Not Victimized**	**Victimized**	**Total**	**% Victimized**
School	48	15	63	23.80%
Graduate	45	15	60	25.00%
Postgraduate	37	17	54	31.50%
Professional/Technical	35	16	51	31.40%
Other	50	17	67	25.40%
Total	**215**	**80**	**295**	

Source: Primary Data

Interpretation:

- **Higher-educated respondents** (Postgraduate, Professional) had **higher victimization rates (~31%)**, possibly due to higher online activity and financial transactions.
- This suggests **education alone doesn't ensure digital safety**; it must be paired with practical awareness and precautions.

Table 4: **Fraud Victims by Profession**

Profession	**Not Victimized**	**Victimized**	**Total**	**% Victimized**
Student	45	16	61	26.20%
Service	38	14	52	26.90%
Business	51	15	66	22.70%
Homemaker	40	18	58	31.00%
Other	41	17	58	29.30%
Total	**215**	**80**	**295**	

Source: Primary Data

Interpretation:

- **Homemakers and "Other" professionals** faced higher fraud rates (~30%), possibly due to limited digital training or frequent online shopping/social media use.
- **Business professionals** reported the **lowest victimization rate**, which might reflect greater caution in financial dealings.
- Profession affects exposure to fraud, and tailored training may help reduce risk.

Table 5: **Fraud Victims by 2FA Usage**

2FA Usage	**Not Victimized**	**Victimized**	**Total**	**% Victimized**
Yes	129	54	183	29.50%
No	86	26	112	23.20%
Total	**215**	**80**	**295**	**27.10%**

Source: Primary Data

Interpretation:

- Surprisingly, those using two-factor authentication (2FA) have a slightly higher fraud rate (29.5%) than non-users (23.2%).
- This may suggest:
  - Victims adopted 2FA after being defrauded.
  - False sense of security with 2FA leading to risky behaviour.
- Indicates that 2FA alone is not sufficient—comprehensive security behaviour is necessary.

Table 6.ASSES THE CORRELATION BETWEEN AWARENESS LEVEL AND TRANSACTION SECURITY

This analysis explores the relationship between two important factors: awareness of online fraud schemes and how secure users feel while making digital transactions. The goal is to find out whether people who are more aware of online risks also feel more confident and protected when using the internet for financial activities.

Variables and Mean Score

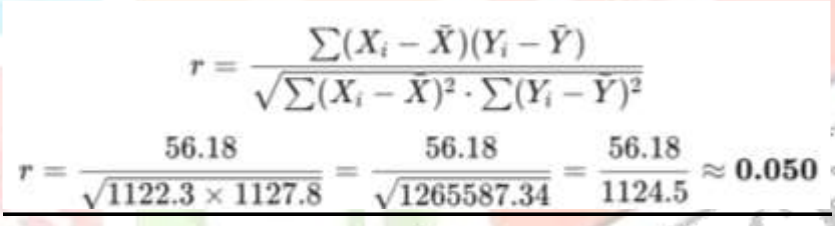
Variables	Mean
X = Awareness Level (rated 1–5)	3.04
Y = Transaction Security (rated 1–5)	2.98

Source: Primary Data

Required Sum for Person’s Formula

Component	Value
∑(X − X̄)(Y − Ȳ)	56.18
∑(X − X̄)²	1122.3
∑(Y − Ȳ)²	1127.8

Pearson Correlation Formula



$$r = \frac{\sum(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum(X_i - \bar{X})^2 \cdot \sum(Y_i - \bar{Y})^2}}$$

$$r = \frac{56.18}{\sqrt{1122.3 \times 1127.8}} = \frac{56.18}{\sqrt{1265587.34}} = \frac{56.18}{1124.5} \approx \mathbf{0.050}$$

Interpretation:

- The correlation coefficient is +0.050.
- This means there is a very weak positive relationship between awareness level and transaction security perception.
- In simple terms, being aware of fraud does not strongly increase how secure people feel during online transactions.
- Although people may be aware of fraud schemes, this awareness **does not significantly change** how secure they feel. More than awareness, real-time practices (like secure platforms, 2FA, alerts) may matter more for confidence.
- Awareness alone is not enough, and other factors like secure technology, platform reliability, and user behaviour may play a more critical role in building trust in digital transactions.

HYPOTHESIS TESTING

Hypotheses 1

- **H_{01} (Null Hypothesis):** There is no significant relationship between users' digital literacy and their vulnerability to online fraud.
- **H_{11} (Alternative Hypothesis):** There is a significant relationship between users' digital literacy and their vulnerability to online fraud.

Variables and Mean Score

Variables	Mean
X = Digital Literacy (Independent Variable):($\bar{X}$)	3.13
Y = Vulnerability to Online Fraud (Dependent Variable):($\bar{Y}$)	0.25

Source: Primary Data

Required Sum for Person's Formula

Metric	Value
Sum of Product of Deviations $\sum(X-\bar{X})(Y-\bar{Y})$	–0.403
Denominator $\sqrt{[\sum(X-\bar{X})^2 \times \sum(Y-\bar{Y})^2]}$	137.29
Sum of squared deviations in awareness $\sum(X-\bar{X})2$	**1294.54**
Sum of squared deviations in fraud status $\sum(Y-\bar{Y})2$	**14.57**
Pearson Correlation Coefficient (r)	**–0.0029**

IV. RESULTS AND DISCUSSION

Key insights from hypothesis

In Nutsell, Even though it has been assume higher awareness should protect users, this data suggests **knowledge alone does not shield individuals from falling prey to scams**. It could be because many frauds use **emotional or psychological tactics** that bypass rational awareness.**Technical tricks** (phishing links, cloned websites) may be hard to detect even for informed users.People may be **aware**, but still take **risky actions** out of urgency, trust, or lack of attention..digital literacy increases, the likelihood of becoming a victim **barely changes**, and might decrease *slightly*, but **not meaningfully**.

Hypothesis 2

H_{02}: Preventive strategies such as two-factor authentication and regular password changes have no significant impact on reducing online fraud cases.
H_{12}: Preventive strategies such as two-factor authentication and regular password changes significantly reduce online fraud cases.

- ❖ A Chi-square test was conducted to examine the association between preventive strategy usage and online fraud victimization.

Chi-Square Test Contingency Table

Preventive Strategy Level	**Not a Victim (0)**	**Victim (1)**	**Total**
Low (Score 1–2)	18	44	62
Medium (Score 3)	35	44	79
High (Score 4–5)	78	76	154
Total	131	164	295

Source: Primary Data

Chi-Square Calculation Table

Strategy Level	**Victim Status**	**Observed (O)**	**Expected (E)**	**(O−E)²/E**
Low	Not a Victim (0)	18	27.56	3.31
Low	Victim (1)	44	34.44	2.66
Medium	Not a Victim (0)	35	35.07	0.0001
Medium	Victim (1)	44	43.93	0.0001
High	Not a Victim (0)	78	68.37	1.35
High	Victim (1)	76	85.63	1.05
Total χ^2				**≈ 8.37**

Source: Primary Data

Chi-Square Test Formula:

$$\chi^2 = \sum \frac{(O-E)^2}{E}$$

Where:

- OF = Observed frequency
- EF = Expected frequency

Chi-Square Test Results

Statistic	Value
Chi-square (χ^2) value	8.368
Degrees of freedom (df)	2
p-value	**0.0152**

The chi-square test result ($\chi^2 = 8.37$, p = 0.015) is **statistically significant**, as the p-value is less than 0.05. Therefore, the **null hypothesis (H_{02})**—which states that preventive strategies have no significant impact on reducing online fraud cases—is **rejected**. The **alternative hypothesis (H_{12})** is **accepted**, indicating that preventive strategies such as two-factor authentication and regular password changes **significantly reduce** the likelihood of becoming a victim of online fraud.

Key insights from hypothesis

The analysis of Hypothesis 2 revealed that the use of preventive strategies such as two-factor authentication and regular password changes is significantly associated with a lower incidence of online fraud. The chi-square test ($\chi^2 = 8.37$, p = 0.015) confirmed this relationship, leading to the rejection of the null hypothesis. This indicates that individuals who consistently implement these security practices are less likely to become fraud victims. The insight highlights that proactive behavior and practical security measures are more effective in reducing online fraud than awareness alone.

Findings of the study

- Out of 295 respondents, a large portion had **medium to high awareness (digital literacy)**, but many still reported experiences with online fraud, showing that awareness alone may not be enough.
- In the initial analysis tables, it was found that **users with lower awareness or less confidence in digital safety were slightly more likely to become fraud victims**, but the difference was not strong.
- A **correlation test (r = –0.0029)** showed **no meaningful relationship** between digital literacy and online fraud, meaning people who are more aware are **not necessarily safer** from fraud.
- Therefore, **Hypothesis 1** (H_{01}: There is no significant relationship between digital literacy and vulnerability to fraud) was **accepted**, and the **alternative was rejected**.
- A second analysis looked at **preventive strategies** like using **two-factor authentication and changing passwords regularly**.
- Users who followed these practices more often had **fewer cases of online fraud**.
- A **Chi-square test** confirmed this link ($\chi^2 = 8.37$, p = 0.015), meaning the relationship between strategy use and fraud reduction was **statistically significant**.
- As a result, **Hypothesis 2** (H_{02}: Preventive strategies have no impact) was **rejected**, and the **alternative hypothesis (H_{12})** was **accepted**.
- The earlier tables supported this too, showing that **users with low preventive habits were more likely to be fraud victims**, while those with strong habits were safer.

Suggestions and recommendations

- Individuals should:
  - Enable **two-factor authentication (2FA)** on all important accounts.
  - Use **strong, unique passwords** and avoid reusing them across platforms.
  - **Update passwords regularly** to reduce the risk of long-term exposure.
  - Stay informed about **common online fraud techniques** (e.g., phishing, fake links).
  - **Avoid clicking unknown links** or downloading suspicious attachments.
- Educational institutions should:
  - **Integrate cybersecurity awareness** into the curriculum or orientation programs.
  - Conduct regular **awareness campaigns and workshops** on online safety.
  - **Train peer educators or student volunteers** to promote safe digital habits on campus.
- Organizations should:
  - Implement **mandatory digital safety training** for all employees.
  - Enforce **strong security protocols** like 2FA and access control systems.
  - Conduct **simulated phishing tests** to improve employee fraud detection skills.
- Governments and policymakers should:
  - Run widespread **digital safety awareness campaigns** through TV, radio, and social media.
  - Promote access to **free or subsidized cybersecurity tools** (e.g., password managers).
  - Set up **regional fraud helplines and easy-to-use reporting platforms** in local languages.

Conclusion

This study investigated the relationship between digital literacy, preventive strategies, and users' vulnerability to online fraud using data from 295 respondents. The aim was to understand whether being digitally aware or actively using safety measures like two-factor authentication and password updates could reduce the risk of fraud victimization. Findings from the first hypothesis revealed that digital literacy had no significant correlation with fraud vulnerability ($r = -0.0029$), leading to the acceptance of the null hypothesis. This suggests that awareness alone may not be enough to protect individuals from fraud. In contrast, the second hypothesis showed that preventive strategies were significantly associated with lower fraud cases. The chi-square test ($\chi^2 = 8.37$, $p = 0.015$) confirmed this relationship, resulting in the rejection of the null hypothesis. This indicates that users who actively implement security practices are less likely to fall victim to online scams. The study highlights that while digital education is important, it must be paired with practical behavior changes to be effective. Simply knowing about fraud risks does not necessarily prevent users from becoming victims. Instead, consistent application of security measures plays a more decisive role. These findings suggest a need for a shift in focus from just spreading awareness to promoting hands-on digital safety habits. Institutions, employers, and policymakers must prioritize training, tools, and campaigns that encourage active protection. As cyber threats continue to rise, empowering users to adopt preventive behaviors is essential for reducing online fraud and ensuring a safer digital environment for all.

REFERENCES

REFERENCES

1. Anderson, K. B. (2013). *Consumer fraud in the United States, 2011: The third FTC survey*. Federal Trade Commission. https://www.ftc.gov/sites/default/files/documents/reports/consumer-fraud-united-states-2011-third-ftc-survey/130419fraudsurvey_0.pdf
2. Cross, C., Smith, R. G., & Richards, K. (2014). *Challenges of responding to online fraud victimisation in Australia*. Trends Issues in Crime and Criminal Justice, 474. https://www.aic.gov.au/publications/tandi/tandi474
3. Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346
4. Leukfeldt, E. R., & Jansen, J. (2020). Cybercrime and older adults: How often and why are they victimized? *International Review of Victimology*, 26(1), 49–59. https://doi.org/10.1177/0269758019832220
5. Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46(4), 815–825. https://doi.org/10.1016/j.dss.2008.11.010
6. Reisig, M. D., Holtfreter, K., & Pratt, T. C. (2009). Low self-control and the risk of fraud: A study of older adults. *Journal of Criminal Justice*, 37(6), 653–666. https://doi.org/10.1016/j.jcrimjus.2009.09.008
7. Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, 26(1), 277–292. https://doi.org/10.1108/JFC-10-2017-0095
8. Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, 24(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005