Shikshan Sanshodhan : Journal of Arts, Humanities and Social Sciences ISSN(o): 2581-6241
Monthly, Peer-Reviewed, Refereed, Indexed Journal Impact Factor: 9.134
Volume - 9, Issue - 8, August - 2026

DOIs:10.2018/SS/202608002 --:-- Research Paper / Article / Review

Cyber fraud against women in digital India : a multidimensional study of risk, awareness and financial vulnerability

[1] Pradip Kalsariya, [2] Nimisha Shukla,
[1] Ph.D. scholar, Department of Rural Economics, Gujarat Vidyapith, Ahmedabad, India
[2]Head and Professor, Department of Rural Economics, Gujarat Vidyapith, Ahmedabad, India
Email – [1]kalsariya.pradip.3343@gmail.com, [2]nimisha63@gujaratvidyapith.org

Abstract: *With digitalization and the increasing use of online financial services, incidents of cyber fraud have increased significantly in India. It is often believed that due to limited digital literacy, lack of cyber awareness, over-trusting nature, and limited technical skills; probability of Cyber fraud among women would be high. Hence, this study aims to test this belief and to analyse demographic, economic, digital usage, and security-related factors that affect vulnerability among women for fraud. The study is based on total of 56 women victims from Ahmedabad and Surat cities selected through purposive sampling method, from 2020 to 2022. Data were collected through direct interviews and questionnaires and analysed using descriptive statistics and Spearman's Rho correlation . According to the study, the age group of 36 to 55 was found to be the most vulnerable, while the incidence of fraud was also significant among highly educated women. Women working in private jobs, students, and housewives were found to be at higher risk. Both income and liquid assets were positively correlated with the amount of fraud. Online shopping, credit/debit card, and task-based frauds were the most commonly reported. Most women in the study used Unified Payments Interface (UPI), while awareness about One-Time Password (OTP)s and strong passwords was found to be good. However, the ability to identify fraudulent links and awareness of the cyber helpline 1930 were limited. The study shows that vulnerability to cyber fraud among women is result of combined influence of social, economic, and digital factors. Therefore, it becomes necessary to develop digital literacy, cyber awareness, and safe online behaviour among women.*

Key Words: *Cyber Fraud, Women Victims, Cyber Awareness, Online Fraud, Cyber Vulnerability, UPI, Digital Security, Socio-Economic Factors, Cybercrime.*

1. INTRODUCTION

With the global trend towards digitalization and online financial systems, the use of technology has increased significantly across all sectors. A similar trend can also be observed in India. Initiatives such as "Digital India[1]", "[2]Make in India," and "Skill India[3]," along with the Aadhaar ecosystem, nationwide internet connectivity, and UPI, have led citizens to rapidly adopt the process. As a result, UPI in India has become largest real-time digital payment network in the world. With 22.64 billion UPI transactions worth an estimated ₹29.53 lakh crore recorded in March 2026 (National Payments Corporation of India- NPCI, 2026), India is emerging as one of the world's largest digital economies.
However, the story of technological and financial achievements has its negative side, too. Number of challenges have emerged and one is about digital crime in general, and cyber fraud in particular. Cyber fraud refers to the intentional

[1] Digital India is a flagship programme of the Government of India, launched on July 1, 2015 to transform India into a digitally empowered society and knowledge economy. https://www.digitalindia.gov.in
[2] Make in India, launched on September 25, 2014, aims to facilitate investment, foster innovation, build world-class infrastructure, and position India as a global hub for manufacturing, design, and innovation. static.pib.gov.in
[3] Skill India or the National Skills Development Mission of India is a campaign managed by the National Skills Development Corporation of India. incorporated on July 31, 2008 by Ministry of Finance as Public Private Partnership model. www.skillindiadigital.gov.in

use of digital devices or platforms to illegally obtain financial or personal gain through the internet (Carter, 2025). Following the Covid-19 pandemic, dependence of population on digital platforms increased significantly. Taking advantage of this growing dependence, both national and international fraudsters began exploiting users, leading to a rise in cyber-crimes and digital fraud. In India, more than 3 lakhs cyber-crime cases were reported during 2019 to 2023 with National Payments Corporation of India, out of which 63.23 per cent, i.e., approximately 1.90 lakh cases, were related to cyber fraud. Similarly, in Gujarat, a total of 7,015 cyber-crime cases were reported during the same period, of which 59.7 per cent, i.e., 4,188 cases were related to cyber frauds according to the reports of National Crime Records Bureau.

Each crime has its own niche that creates group within society making more vulnerable to fraud. Women are also one such section of society, as they are supposed to be more likely to become victims of cyber fraud due to factors such as limited digital literacy, lack of awareness, economic dependency, an over-trusting mindset, and limited technological skills and usage. Hence, there is a need to understand fraud against women not only from perspective of technical crime, but also from economic, gender, and other demographic perspectives.

2. Literature review

In present study; relevant literature, previous studies, research articles, and reports have been reviewed to identify factors related to vulnerability of women. The objective of this review is to understand major factors, methodologies, and research gaps identified in previous studies. The information obtained from these studies has been systematically compiled and analysed, and their major findings, approaches, and identified factors have been briefly presented through the following literature review table.

Table 1 : Brief Review of Literature Related to Study

Serial Number	Reference	Study Area	Main Factors	Methodology	Conclusion
1	Balakrishnan et al. (2025)	Study on Cyber Fraud Victims	Age, Gender	Survey + Logistic Regression	Higher risk among women; overconfidence and social influence were major factors, with differences in age-related awareness. Gender was identified as the most significant risk factor.
2	Chen et al. (2021)	Geographical Factors of Cyber Fraud	Age, Income, Occupation	Case Data Analysis + GAM Analysis	Areas with higher income, urban occupations, and a larger young population reported more cyber fraud cases.
3	Isaia et al. (2024)	Study on Online Fraud	Gender, Age, Education, Income	Survey-based Quantitative Analysis	Only age was found significant: the risk of fraud decreases with increasing age. No significant effect of gender, education, or income was found.
4	Kasturi & Dar (2024)	Cyber Crimes and Cyber Security	Age, Income, Gender, Education	Survey + Legal Analysis	Women and weaker sections were found more vulnerable; low education, low awareness, and digital illiteracy were the major risk-enhancing factors.
5	Kumar & Patel (2025)	Cyber Fraud among Elderly People	Age, Gender, Digital Behaviour	Interview Schedule + Purposive Sampling	Elderly men and individuals spending more time online were more vulnerable; digital

					behaviour was identified as a major risk factor.
6	Macaulay et al. (2020)	Review Study on Fraud Victims	Age, Gender	Literature Review	Differences in risk were observed according to age and gender; fraud was more common among the elderly, while young women faced higher sexual harassment risks.
7	Routiya & Vaishnav (2025)	Cyber Fraud (Mule Accounts and Loan Scams)	Income, Education, Gender	Qualitative Case Study and Content Analysis	Low-income, less educated individuals, and women were more vulnerable. Women were major victims of loan scams, with digital illiteracy identified as the primary cause.
8	Ueno et al. (2021)	Vulnerability to Fraud among the Elderly	Age, Cognitive Decline, Gender	Survey + Cognitive Testing + Regression Analysis	Mild cognitive decline was identified as a major risk factor; men were more vulnerable, while older age and low education were associated with cognitive aspects.
9	Ueno et al. (2022)	Study on Specific Fraud among the Elderly	Age, Education, Gender, Loneliness	Cross-sectional + Questionnaire-based Analysis	Women, elderly individuals, less educated people, and those living alone were found to be at greater risk.
10	Whitty (2019)	Study on Cyber Fraud Victims	Age, Education	Survey + Logistic Regression	Older and highly educated individuals were found more vulnerable; online behaviour was identified as a major factor.
11	Zhang & Ye (2022)	Study on Online Fraud	Age, Education	Questionnaire Survey + Logistic Regression	Younger age and lower education were associated with higher risk; a positive relationship was found between education and awareness.

The review makes it clear that cyber fraud is a multidimensional phenomenon in which besides gender; technical, social, economic, psychological, and behavioural factors are also involved. Factors such as age, education, digital literacy, income, awareness, tendency to trust, and online behaviour can make people vulnerable to cyber fraud. Some studies have identified risks among both young and elderly individuals with regard to age; however, the risk appears to be more pronounced among the elderly. Low levels of education have been identified as a risk factor, although few studies suggest that higher education may also make individuals vulnerable due to overconfidence or unsafe online behaviour. On the other hand, with regard to gender; both men and women have been reported to be vulnerable to cyber fraud. Most studies indicate that risk is comparatively higher among women, reflecting a gender-based difference. Women may face greater risk due to limited technical knowledge, skills, and cyber awareness, along with other social factors. However, available studies have mainly analysed vulnerability factors of cyber fraud by focusing on general population, while women-centric studies remain limited. In particular, adequate research on vulnerability of women to cyber fraud in the context of Gujarat, is lacking. Therefore, the present study has been undertaken.

3. Research Methodology

For the study, cyber fraud statistics registered in the state of Gujarat during the period from 2020 to 2022 were analysed. According to the data, out of total of 2,638 cyber fraud cases registered, only two districts, namely Surat and Ahmedabad, accounted for 1,334 cases that makes it 50.6 per cent of total. Considering the higher number of cases and better representation in comparison to other districts, the cities of Ahmedabad and Surat were selected as the study area. Using the purposive sampling, total of 56 women was selected for the research. Subsequently, primary data relevant to the study were collected through the direct interview and a structured questionnaire.

4. Analysis of Primary Data

Descriptive statistics, correlation analysis, and tabulation were used to analyse primary data collected during the study. The data were classified and analysed based on variables such as age of respondent, education, income, liquid assets, as well as digital usage and awareness. Tables, percentage analysis, and graphs were also used to present the findings of the study in a simple and clear manner.

4.1. Age Distribution

In various studies, age has been identified as an important factor influencing cyber fraud. Differences are observed among women of different age groups in terms of the use of digital tools, online behaviour, financial decisions, and security levels. The classification of women victims according to age group is presented in the following table.

Table 2 : Classification of Women Victims According to Age Group (in years)

City	18 -25	26 -35	36 - 55	> 55	Total
Surat	5	7	9	2	23
Ahmedabad	5	14	14	0	33
Total	10	21	23	2	56

According to the above table, women aged 36 to 55 years are the most vulnerable age group due to limited security and technical knowledge, while the age group between 26 and 35 years, having greater digital exposure, online activity, and technological usage, also appears vulnerable. Women between 18 and 25 years of age appear comparatively more cautious to some extent due to their greater familiarity with technical matters, whereas the frequency of the elderly age group is comparatively lower due to limited involvement in technology and digital transactions.

4.2. Level of Education

The level of education has an important effect on digital understanding, usage, level of caution, and ability to identify cyber risks. Therefore, education is an important factor in understanding the risks of cyber fraud. The classification is presented as follows.

Table 3 : Classification of Women Victims According to Level of Education

City	Illiterate	Primary	Secondary	Higher Secondary	Graduation	Professional	Total
Surat	1	3	2	5	5	7	23
Ahmedabad	0	2	5	6	13	7	33
Total	1	5	7	11	18	14	56

Proportion of women with higher education is found to be higher among women who have fallen victim to cyber fraud. Particularly, women with graduate/postgraduate and professional education are more engaged with digital services, online transactions, and social media, due to which they may become more vulnerable to cyber risks. On the other hand, the frequency is lower among women with primary education or those who are illiterate, which may mainly be due to their limited online transactions and digital usage. Therefore, it can be said that a higher level of education alone does not ensure cyber security; rather, digital activity, caution, and cyber security awareness are equally important.

4.3. Economic Activities

Women victims of fraud were also analysed according to the type of economic activity they undertake. Although occupation-based analysis is found to be limited in cyber fraud related research, occupation can influence factors such as income, digital usage, online financial transactions, time engagement, technical exposure, and awareness. Therefore, an analysis of occupation has been carried out to understand the role of occupation in determining the risks of cyber fraud.

Table 4 : Classification of Women Victims According to Type of Occupation

City	Student / Housewife	Private Job	Govt. Job	Gig Worker	Business/ Service	Retired / Unemployed	Total
Surat	11	6	1	1	3	1	23
Ahmedabad	7	16	1	1	6	2	33
Total	18	22	2	2	9	3	56

Women working in private sector may be the most vulnerable due to their financial independence, digital activity, higher number of digital transactions, greater use of mobile applications, and tendency to respond quickly under work pressure. A higher level of risk is also observed among students and housewives, as they are more connected to social media, online shopping, and other digital platforms, while lack of awareness regarding security measures makes them more vulnerable. Gig workers, due to their constant exposure to online platforms and adherence to security instructions provided in gig work, may be comparatively less vulnerable. Similarly, the lower frequency of fraud among the retired population may be due to their older age and limited use of technology.

4.4. Income

Income affects not only the probability of cyber risk and the extent of financial loss, but also factors such as the standard of living of the population, availability of digital tools, frequency of online transactions, and economic behaviour, such as the tendency to trust attractive offers. Moreover, income has also been identified in other studies as a crucial factor in understanding the risks of cyber fraud.

Table 5 : Classification of Women Victims According to Income (₹ in Lakhs)

City	No Income	<= 4.99	5 - 9.99	>10	Total
Surat	11	9	2	1	23
Ahmedabad	6	24	3	0	33
Total	17	33	5	1	56

Low to middle income group women are at greater risk of cyber fraud. Especially, women with an income less than ₹ 4.99 lakh may become vulnerable due to limited use of resources, lack of awareness about fraud techniques, and a tendency to trust attractive offers. Thereafter, housewives and students with no income may become victims of fraud due to work-from-home opportunities, part-time jobs, and other misleading or fake employment-related advertisements. However, this table only presents the frequency of fraud in relation to income.

4.5. Correlation of Fraud Amount with Economic Factors

As per Table No. 5, the frequency of cyber fraud was analysed based on income, but it is hard to understand the extent of financial loss only on the basis of frequency or number. Victims and amount of financial loss is also an important factor. Therefore, correlation analysis has been carried out to understand the relationship between economic factors and the amount of financial loss among women.

4.5.1. Correlation between Income and Cyber Fraud Amount

Income is an important factor determining the extent of financial loss. Generally, the frequency of fraud may be higher among people with lower income, but since people with higher income are involved in larger financial transactions, the amount lost due to fraud may be higher among them. To understand this relationship statistically, the Spearman's rho correlation results between income and fraud amount are as follows.

Table 6: Correlation between the Income of Women Victims and the Amount Lost

Variable	Spearman's rho	p-Value	N
Income and Cyber Fraud Amount	0.459**	0	56

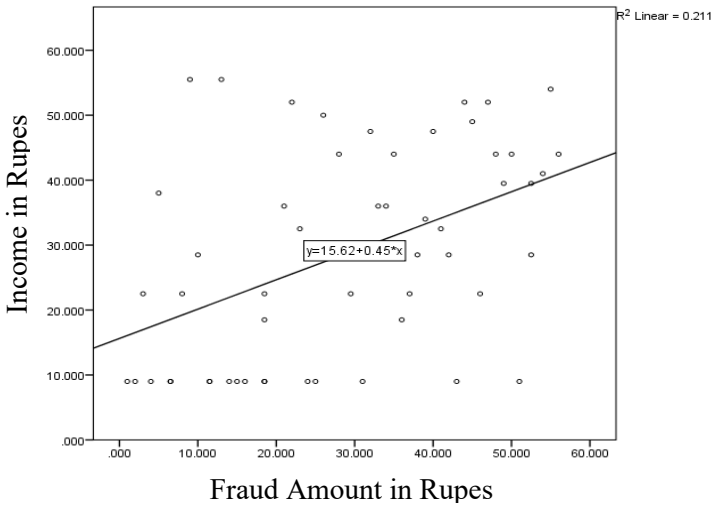

Figure 1: Scatter Plot Showing Correlation

There is moderate positive correlation (Spearman's rho = 0.459) between income and the amount lost in fraud, which is statistically significant (p-value < 0.001). This means that as the income increases, the amount lost in cyber fraud also tends to increase.

The upward slope shown in the figure also supports the positive relationship between income and the amount lost in fraud. It can be said that although the frequency of fraud is comparatively lower among women with higher income, they may suffer greater financial losses due to their involvement in larger financial transactions, investments, and greater digital economic activities.

4.5.2. Correlation between Liquid Assets and Amount Lost in Fraud

It is not possible to fully understand the extent of financial loss based on income alone, as individuals with higher income may have limited available savings due to higher expenses and financial responsibilities. On the other hand, individuals with lower income may have relatively higher cash savings or available assets, due to which they may suffer greater financial losses. Therefore, along with income, the analysis of liquid assets also becomes important in understanding the actual economic losses caused by cyber fraud. The correlation between liquid assets and the amount lost in fraud has been examined as follows.

Table 7: Correlation between Liquid Assets of Women Victims and the Amount Lost

Variables	Spearman's rho	p-value	N
Liquid Assets and Amount Lost	.679**	0	56

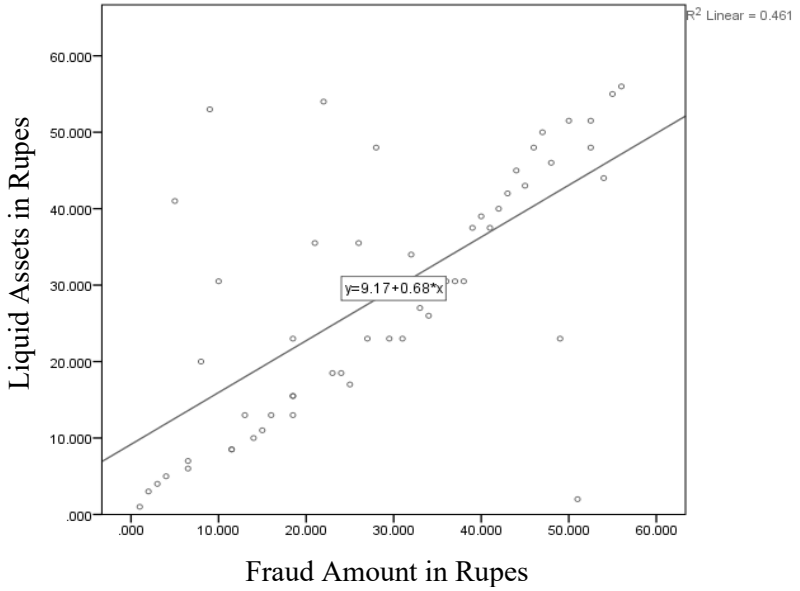

Figure 2: Scatter Plot Showing Correlation

There is strong positive correlation (Spearman's rho = 0.679) between liquid assets and the amount lost in fraud, which is statistically significant (p-value < 0.001). This means that as the liquid assets increase, the amount lost in cyber fraud also tends to increase.

The upward slope shown in the graph also supports this positive relationship. It can be said that women with higher liquid assets may suffer relatively greater financial losses in fraud due to larger financial transactions, major economic decisions, higher savings, and greater digital economic activities.

4.6. Classification of Frauds among Women

Cyber fraud occurs in various forms, and method, purpose, and impact of each type of fraud may differ. To understand the type of fraud women are more vulnerable to, frauds have been classified according to type, which helps in understanding the nature of cyber risks and their major trends.

Table 8: Types of Fraud and Frequency among Women

Type of Cyber Fraud	Frequency	Percentage
Online Shopping	12	21.43
Investment and Task-based	7	12.50
Credit / Debit Card	6	10.71
OTP / Link	5	8.93
Money Demand through Fake Messages	5	8.93
Matrimonial	4	7.14
Fake KYC and Unauthorized Applications	3	5.36
OLX	3	5.36
Online Job	3	5.36
Fake Customer Care	2	3.57
Electricity Bill and Delivery Related	2	3.57
Others	4	7.14
Total	**56**	100.00

The frequency of online shopping-related fraud is higher among women, which indicates lack of security awareness regarding e-commerce. The proportion of credit/debit card and task-based fraud is also significant. Fraudsters exploit trustful nature of women or use attractive tactics to commit OTP, link-based, fake message, and matrimonial frauds.

4.7. Use and Awareness of Digital Services

Along with social, demographic, and economic factors, use of digital services and cyber awareness among women also play a significant role in shaping their vulnerability. This has been analysed based on their use of banking services, ability to identify OTPs and fraudulent links, knowledge of creating strong passwords, and awareness of the cyber helpline number 1930.

4.7.1. Use of Unified Payments Interface (UPI)

Table 11: Use of UPI According to City

City	Use of UPI		
	NO	YES	Total
Surat	1	22	23
Ahmedabad	0	33	33
Total	1	55	56

As per the table, most of the women victims were using UPI, which shows that UPI is the most widely used among digital banking services. Its use among women may be higher due to its simple process, quick payments, and mobile-based convenience and security. However, its widespread usage may also increase the risks of cyber fraud through methods such as OTPs, links, QR codes, and fake payment requests.

4.7.2. Awareness about OTP

Table 12: Awareness regarding Sharing OTP with Strangers

City	Not Knowledge At All	Partial Knowledge	Complete Knowledge	Total
Surat	2	8	13	23
Ahmedabad	1	9	23	33
Total	3	17	36	56

Most of the women were fully aware of not sharing OTPs with strangers, which indicates that the level of awareness regarding OTP-related cyber security among women is comparatively good. However, the proportion of women with partial knowledge is also significant, which suggests that despite having basic awareness, they may still remain vulnerable to new methods of fraud. On the other hand, the proportion of women with no knowledge at all is comparatively low. In short, it can be said that despite awareness regarding OTPs, limitations still exist in practical caution and the ability to identify risky situations.

4.7.3. Ability to Identify Fraudulent and Unsafe Links

Table 13: Awareness regarding Identifying and Opening Unsafe Links

City	Not Knowledge At All	Partial Knowledge	Complete Knowledge	Total
Surat	8	10	5	23
Ahmedabad	2	24	7	33
Total	10	34	12	56

Majority of the women victims have only partial knowledge regarding the identification of unsafe or fraudulent links. This means that women possess basic awareness about cyber security, but their ability to fully identify suspicious links or websites is still limited. The proportion of women with complete knowledge is comparatively low, while women with no knowledge at all are also found in a significant proportion. In short, methods such as fraudulent links, QR codes, and fake websites may become important causes of cyber fraud among women.

4.7.4. Knowledge of Creating Strong Passwords

Table 14: Knowledge regarding Creating Strong Passwords

City	Not Knowledge At All	Partial Knowledge	Complete Knowledge	Total
Surat	5	8	10	23
Ahmedabad	3	12	18	33
Total	8	20	28	56

Most of the women victims have complete knowledge regarding the creation of strong passwords, which indicates awareness about basic cyber security among them. However, the proportion of women with partial knowledge is also comparatively high, which suggests that despite having knowledge about password security, its practical and consistent use is not always ensured. On the other hand, the proportion of women with no knowledge at all is comparatively low. In short, despite increasing awareness regarding passwords, limitations may still exist in practical cyber security habits.

The sum of the findings of the study about internet banking, mobile banking and awareness about cyber helpline 1930 summarise as follows :

4.7.5. Most of the (91.07 Percent) women victims were not using internet banking services, which indicates limited awareness and low technical knowledge regarding digital banking services. From this, it can be said that becoming a victim of cyber fraud is not caused only by the use of internet banking; women may also become victims through other digital mediums such as OTPs, links, online shopping, social media, and mobile applications. On the other hand, the proportion of women using internet banking is comparatively low.

4.7.6. A total of 28 percent of the female victims used mobile banking, and use of mobile banking among women is higher than net banking. From this, it can be said that although the use of smartphone-based digital services is increasing among women, there is still a lack of adequate cyber security awareness and practical knowledge.

4.7.7. Most of the women victims (96.40) lack awareness about Cyber Helpline 1930, which indicates limited access to cyber support and complaint mechanisms. Only a very small proportion of women were found to be aware of this helpline. From this, it can be said that adequate awareness has not yet developed among women regarding immediate support after cyber fraud, the complaint registration process, and the government mechanisms available to reduce financial losses. However, another reason for this limited awareness may be the non-existence of the cyber helpline during the period of cases reported in 2020–21.

5. CONCLUSION

The present study was conducted to understand the role of various demographic, economic, and security-related factors shaping the vulnerability of women victims of cyber fraud based on their experiences. The findings of the study indicate that cyber fraud is not merely a technical problem, but also a multidimensional issue closely linked with social, economic, psychological, and behavioural factors.

The study found that the age group of 36 to 55 years was the most vulnerable, while the age group of 26 to 35 years also appeared to be at significant risk due to greater digital activity and online exposure. In terms of education, the incidence of fraud was found to be higher among women with higher education, indicating that formal education alone does not guarantee cyber security; awareness, caution, and logical thinking in online transactions are also essential. Women working in private jobs appeared to be at higher risk, while students and housewives were also found to be more vulnerable due to social media usage, online shopping, and misleading employment-related advertisements. In terms of income, the number of cases was higher among women with low to middle income; however, according to the correlation analysis, women with higher income and greater liquid assets may suffer greater financial losses due to their higher economic capacity.

Furthermore, women are more vulnerable to online shopping-related, credit/debit card, and task-based frauds. OTPs, links, QR codes, fake messages, and trust-based methods are widely used to deceive women. Among digital banking services, women use UPI more extensively than other services. Although they are aware of OTP security and the importance of strong passwords, they still have limited knowledge regarding fraudulent links and cyber helplines.

In short, the vulnerability of women to cyber fraud is not only the result of technical ignorance, but also the combined effect of digital activity, economic conditions, online behaviour, trusting tendencies, limited cyber awareness, and

practical digital security skills. Therefore, to protect women from cyber risks, technical security alone is not sufficient; it is essential to develop digital literacy, practical cyber awareness, safe online behaviour, and awareness regarding cyber support services. In this regard, targeted programmes designed for specific groups may increase effectiveness and awareness and help reduce the number of such cases.

REFERENCES

1. Balakrishnan, V., Ahhmed, U., & Basheer, F. (2025). Personal, environmental and behavioral predictors associated with online fraud victimization among adults. PLOS ONE, 20(1), e0317232, 1–17. Retrieved April 28, 2026, From https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0317232
2. Carter, W., (2025). The Economic Impact of Online Fraud: A Review. Preprints.org. Retrieved April 15, 2026, from https://doi.org/10.20944/preprints202507.0436.v1
3. Chen, S., Gao, C., Jiang, D., Hao, M., Ding, F., Ma, T., Zhang, S., & Li, S. (2021). The spatiotemporal pattern and driving factors of cyber fraud crime in China. ISPRS International Journal of Geo-Information, 10(12), 802. Retrieved April 27, 2026, from https://doi.org/10.3390/ijgi10120802.
4. Isaia, E., Oggero, N., & Sandretto, D. (2024). Is financial literacy a protection tool from online fraud in the digital era? Journal of Behavioral and Experimental Finance, 44, 100977. Retrieved April 18, 2026, from https://doi.org/10.1016/j.jbef.2024.100977
5. Kasturi, Y., & Dar, M. A. (2024). Cybercrime in the digital age: Challenges and legal gaps in India's cybersecurity landscape. African Journal of Biomedical Research, 27(6s), 212–224. Retrieved April 22, 2026, from https://doi.org/10.53555/AJBR.v27i6S.5724.
6. Kumar, S., & Patel, M. (2025). Digital habits and cyber vulnerabilities among older victims of cyber fraud. Working with Older People, 29(4), 433–443. Retrieved April 22, 2026, from https://doi.org/10.1108/WWOP-04-2025-0018
7. Macaulay, P. J. R., Steer, O. L., & Betts, L. R. (2020). Factors leading to cyber victimization. In Emerging cyber threats and cognitive vulnerabilities (pp. 1-25). Academic Press. Retrieved April 27, 2026, from https://doi.org/10.1016/B978-0-12-816203-3.00001-0
8. National Crime Records Bureau, 2019 (Volume 2; pp. 751–842). (2019). Ministry of Home Affairs, Delhi. Retrieved on February 02, 2025, From https://www.ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1653730632_CII 202019 20Volume 202.pdf
9. National Crime Records Bureau, 2021 (Volume 2; pp. 785–877). (2021). Ministry of Home Affairs, Delhi. Retrieved on February 02, 2025, From https://www.ncrb.gov.in/uploads/nationalcrimerecordsbureau/post/1679310741CII2021Volume2.pdf
10. National Crime Records Bureau, 2022 (Volume 2; pp. 785–877). (2022). Ministry of Home Affairs, Delhi. Retrieved on February 02, 2025, From https://www.ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1701608364CrimeinIndia2022Book2.pdf
11. National Crime Records Bureau, 2023 (Volume 2; pp. 785–877). (2023). Ministry of Home Affairs, Delhi. Retrieved on February 02, 2025, From https://www.ncrb.gov.in/uploads/files/2CrimeinIndia2023PartII2.pdf
12. National Crime Records Bureau,2020 (Volume 2; pp. 759–850). (2020). Ministry of Home Affairs, Delhi. Retrieved on February 02, 2025, From https://www.ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1653720991_CII 202020 20Volume 202.pdf
13. National Payment Corporation of India. (2026). *Unified Payments Interface (UPI) monthly statistics*. *product statistics.* Retrieved May 7, 2026, from https://www.npci.org.in/product/upi/product-statistics
14. Routiya, V., & Vaishnav, S. (2025). Financial vulnerability in the digital age case studies of cyber frauds in state of Chhattisgarh (SSRN Working Paper No. 5255157). SSRN. Retrieved April 17, 2026, from https://ssrn.com/abstract=5255157
15. Ueno, D., Arakawa, M., Fujii, Y., Amano, S., Kato, Y., Matsuoka, T., and Narumoto, J. (2022). Psychosocial characteristics of victims of special fraud among Japanese older adults: A cross-sectional study using scam vulnerability scale. Frontiers in Psychology, 13, Article 960442. Retrieved April 27, 2026, from https://doi.org/10.3389/fpsyg.2022.960442
16. Ueno, D., Daiku, Y., Eguchi, Y., Iwata, M., Amano, S., Ayani, N., Nakamura, K., Kato, Y., Matsuoka, T., & Narumoto, J. (2021). Mild cognitive decline is a risk factor for scam vulnerability in older adults. Frontiers in Psychiatry, 12, Article 685451, 1–13. Retrieved April 28, 2026, https://doi.org/10.3389/fpsyt.2021.685451
17. Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. Journal of Financial Crime, 26(1), 277–292. Retrieved April 25, 2026, from https://doi.org/10.1108/JFC-10-2017-0095
18. Zhang, Z., & Ye, Z. (2022). The role of social-psychological factors of victimity on victimization of online fraud in China. Frontiers in Psychology, 13, Article 1030670. Retrieve 27 April, 2026, From https://doi.org/10.3389/fpsyg.2022.1030670