Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 5 Issue 2(2025)

An Exploratory Study amongst Gen Z, X and Y on Awareness and Perception about Cyber Scams with Special Reference to Plastic Money

Dr. Vira Bharat

Assistant Professor, Lala Lajpatrai Institute of Management, Mumbai, India

Dr. Jennie Prajith

Assistant Professor, Pillai College of Arts Commerce and Science Autonomous, Mumbai, India

Dr. Shakti Awasthi

Associate Professor, Lala Lajpatrai Institute of Management, Mumbai, India

Abstract:

Cyber scams have become an increasingly prevalent threat in the digital era, impacting individuals across different generational cohorts. This study explores the awareness and perception of cyber scams among Generation Z, Generation Y (Millennial), and Generation X, highlighting the differences in their experiences, knowledge, and susceptibility. The research utilizes a mixed-method approach, incorporating surveys and interviews to assess how each generation perceives online fraud, phishing, identity theft, and financial scams. The findings indicate that while younger generations (Gen Z and Millennial) are more technologically savvy, they may still fall victim to scams due to overconfidence. In contrast, Gen X exhibits cautious online behavior but may lack the latest cyber security knowledge. The study emphasizes the need for targeted awareness programs and adaptive security measures to enhance cyber safety across age groups.

Keywords: *Cyber scams, Generational awareness, Digital fraud, Cyber security, plastic money frauds, Gen Z, Gen Y, Gen X*

1. Introduction

The rapid advancement of digital technology has provided unparalleled convenience in communication, financial transactions, and online services. However, it has also given rise to sophisticated cyber scams, targeting individuals based on their digital behaviors and vulnerabilities. Different generations exhibit varying levels of cyber security awareness, shaped by their exposure to technology, online habits, and risk perceptions. Generation X, born between 1965 and 1980, grew up in a pre-digital era but adapted to the rise of the internet. They tend to be cautious but may struggle with evolving cyber threats. Millennial (Gen Y), born between 1981 and 1996, witnessed the transition from analog to digital and are generally comfortable with technology. However, their trust in digital platforms may make them vulnerable to online fraud. Gen Z, born between 1997 and 2012, is the first truly digital-native generation, highly engaged with social media and e-commerce but potentially prone to cyber risks due to oversharing and reliance on technology. This study aims to

analyze the awareness and perception of cyber scams across these generational cohorts, identifying gaps in knowledge and areas where enhanced cyber security education is required. Understanding these differences can inform policy recommendations, cyber security training programs, and digital safety initiatives to mitigate the growing threat of cyber fraud.

2. Literature Review:

The increasing reliance on digital platforms has led to a surge in cyber scams, including phishing, identity theft, financial fraud, and social engineering attacks. Cybercriminals exploit human vulnerabilities rather than just technological loopholes, making awareness and perception crucial factors in preventing cyber fraud (Smith & Jones, 2021). As cyber scams become more sophisticated, individuals must adapt by improving their digital literacy and security practices (Kumar et al., 2020). Different generations exhibit distinct behaviors concerning cyber security awareness and risk perception. Research suggests that while digital literacy plays a significant role, psychological factors such as trust, caution, and risk-taking tendencies also influence susceptibility to cyber scams (Holtfreter et al., 2021). Understanding these generational differences can help tailor cyber security awareness programs to target specific vulnerabilities.

Generation X grew up during a time of technological transition, making them more cautious users of digital platforms (Mills, 2022). They tend to be skeptical of unsolicited online requests but may lack familiarity with emerging cyber threats, such as crypto currency scams and deep fake fraud (Patel & Singh, 2023). Studies indicate that while Gen X users often prioritize security, they may struggle with evolving digital threats due to a reliance on traditional scam detection strategies (Roberts et al., 2021).

Millennials (Gen Y) are highly engaged in digital banking, social media, and e-commerce, making them prime targets for cyber scams (Chaudhary et al., 2021). While they demonstrate relatively high digital literacy, their trust in digital services can make them vulnerable to sophisticated scams such as business email compromise (BEC) fraud and fake investment schemes (Taylor & Brown, 2022). Studies highlight that Millennials often fall for scams that appear legitimate due to their familiarity with online transactions and digital communication channels (Williams & Cooper, 2023).

Gen Z, as digital natives, are highly proficient with technology but are also heavily exposed to cyber risks through social media interactions (Lee et al., 2022). Research shows that despite their familiarity with cyber security concepts, they frequently fall victim to social engineering scams, influencer fraud, and data breaches due to oversharing personal information online (Garg & Sharma, 2023). Additionally, their reliance on emerging digital payment platforms has increased their susceptibility to financial fraud (Smith et al., 2023).

Behavioral studies indicate that overconfidence in digital skills, impulsive decision-making, and social influence contribute to cyber scam susceptibility (Garg & Sharma, 2023).

Generational differences in skepticism, financial literacy, and digital etiquette also play a role in shaping scam vulnerability (Roberts et al., 2021). Research further suggests that those who frequently engage in online transactions without verifying sources are at a higher risk of falling for fraudulent schemes (Johnson & Carter, 2020).

Experts emphasize the need for targeted cyber security education tailored to different generations (Johnson & Carter, 2020). While Gen X may benefit from simplified fraud detection strategies, Millennials require awareness campaigns focusing on financial scams. Meanwhile, Gen Z needs education on privacy protection, social media security, and responsible online behavior (Smith et al., 2023). Studies advocate for integrating cyber security education into academic curricula to enhance generational preparedness against online threats (Williams & Cooper, 2023). Existing literature highlights significant generational differences in cyber scam awareness and perception. While technological proficiency varies, psychological disposition, online habits, and exposure to cyber threats influence the likelihood of falling victim to scams. Further research is needed to develop tailored interventions that address the specific vulnerabilities of each generational cohort, ensuring a safer digital environment for all users.

3. Objectives of Study:

- To measure the impact of age over the awareness about the fraud of plastic money
- To measure the impact of age over the Perceived Security about the fraud of plastic money
- To measure the impact of age over the Customer Satisfaction about the fraud of plastic money
- To measure the impact of age over the Fraud Type Experienced about the fraud of plastic money
- To measure the impact of age over the Preference of Cash about the fraud of plastic money

4. Research Methodology:

Source of Information and Tools & Techniques of Research

Source of Information: This research is based on both **primary and secondary data** to ensure a comprehensive analysis of cyber scams awareness and perception among different generational cohorts.

- **Primary Data**:
  - Collected through **questionnaires**, both manually and via **Google Forms**.
  - **Personal interviews** conducted with professionals from banks and cyber cells in the Mumbai Metropolitan Region, ensuring insights from individuals who directly deal with cyber fraud cases.
- **Secondary Data**: Gathered from various credible sources, including Bulletins, Reports from the Reserve Bank of India (RBI), Reports from various commissions and committees on money and finance, Bank reports from India and abroad**,** Articles, journals, newspapers, and books on cyber fraud and digital financial crimes

This combination of primary and secondary data ensures a **holistic and well-supported analysis** of cyber scams and their impact on different generational groups.

Tools and Techniques of Research

*Sample Size and Duration: Sample Size**:** The study includes 223 participants selected from Mumbai; Sample Duration**:** Data from the past five years (2018–2023) is analyzed.*

Sampling Technique: A convenience sampling method is used, allowing easy access to individuals actively using digital financial platforms. This ensures the inclusion of plastic card (debit/credit card) users and online banking users**.**

Area Coverage: The research is focused on Mumbai, a major metropolitan hub where digital financial transactions and cyber fraud cases are prevalent.

Questionnaire Design: A well-structured 22-item questionnaire is used to collect primary data. The questionnaire includes close-ended questions to ensure uniform responses for statistical analysis.

Data Analysis Technique: To analyze the collected data, various statistical tools and techniques are used: Likert Scale – Used to measure respondents' satisfaction and awareness of cybersecurity measures; Percentage Analysis & Chi-Square Test is used to identify the relationship between demographic factors and cyber fraud awareness.

Scope of the Study: This research covers the period 2018–2024, examining major fraudulent cases reported in Mumbai. Since cybercrime is a rapidly evolving field, recent case studies are also incorporated to reflect the latest trends in cyber fraud. This methodology ensures reliable, data-driven insights into the generational differences in cyber scam awareness and perception.

5. Data Analysis:

1. Impact of Age on awareness

To measure the impact of age over the awareness about the fraud of plastic money on the basis of age, for impact of age on awareness after Fraud is measured with the Chi Square test and the results are presented as under:

Table 1.1 : Age * Awareness Cross tabulation

Count							
		Awareness					Total
		Not at all aware	Little aware	Neutral	Aware	Very well aware	
Age	20-30 years	2	15	22	40	48	127

	31-40 years	0	4	6	16	21	47
	41-50 years	1	5	5	3	7	21
	> 50 years	0	8	4	8	8	28
	Total	**3**	**32**	**37**	**67**	**84**	**223**

Table-1.2: Chi-Square Tests

	Value	df	Asymp. Sig. (2sided)
Pearson Chi-Square	14.458[a]	12	.272
Likelihood Ratio	14.252	12	.285
Linear-by-Linear Association	3.107	1	.078
N of Valid Cases	223		
a. 8 cells (40.0%) have expected count less than 5. The minimum expected count is .28.			

The output of the 'chi square test' in the table-1.2, reveals that insignificant gap exists between the hypothesized test value with the calculated sample statistics for measuring the impact of age on awareness for fraud happened with the respondents ($p>0.05$) at 5% level of significance. The respondents have exhibited no differences for the age wise categories.

2. Impact of Age on Perceived Security

To measure the impact of age over the Perceived Security about the fraud of plastic money on the basis of age, for impact of age on Perceived Security after Fraud is measured with the Chi Square test and the results are presented as under:

Table 2.1: Age *Security Level of Cards Cross tabulation

Count							
		Security Level of Cards					Total
		Very poor	Poor	Fair	Good	Very Good	
Age	20-30 years	4	5	50	54	14	127
	31-40 years	2	2	15	23	5	47
	41-50 years	1	2	4	12	2	21

	> 50 years	1	4	6	13	4	28
	Total	**8**	**13**	**75**	**102**	**25**	**223**

Table 2.2: Chi-Square Tests

	Value	df	Asymp. Sig. (2sided)
Pearson Chi-Square	10.266[a]	12	.593
Likelihood Ratio	9.615	12	.650
Linear-by-Linear Association	.002	1	.967
N of Valid Cases	223		

a. 9 cells (45.0%) have expected count less than 5. The minimum expected count is .75.

The output of the 'chi square test' in the table-2.2, reveals that insignificant gap exists between the hypothesized test value with the calculated sample statistics for measuring the impact of age Perceived Security for fraud happened with the respondents ($p>0.05$) at 5% level of significance. The respondents have exhibited no differences for the age wise categories.

3. Impact of Age on Customer Satisfaction

To measure the impact of age over the Customer Satisfaction about the fraud of plastic money on the basis of age, for impact of age on Customer Satisfaction after Fraud is measured with the Chi Square test and the results are presented as under:

Table 3.1 : Age * Customer Satisfaction Cross tabulation

Count							
		Customer Satisfaction					Total
		Highly Dissatisfied	Dissatisfied	Neutral	Satisfied	Highly satisfied	
Age	20-30 years	21	25	34	31	16	127
	31-40 years	16	16	8	5	2	47
	41-50 years	8	7	3	3	0	21

	> 50 years	5	17	1	1	4	28
	Total	**50**	**65**	**46**	**40**	**22**	**223**

Table 3.2: Chi-Square Tests

	Value	df	Asymp. Sig. (2sided)
Pearson Chi-Square	41.146[a]	12	.000
Likelihood Ratio	44.595	12	.000
Linear-by-Linear Association	12.081	1	.001
N of Valid Cases	223		

a. 6 cells (30.0%) have expected count less than 5. The minimum expected count is 2.07.

The output of the 'chi square test' in the table-3.2, reveals that significant gap exists between the hypothesized test value with the calculated sample statistics for measuring the impact of age on Customer Satisfaction for fraud happened with the respondents ($p>0.05$) at 5% level of significance. The respondents have exhibited that the respondents with the age of 20-30 years were more satisfied with the efforts of the cyber cell for better control over the recovery process.

4. Impact of Age on Fraud Type Experienced

To measure the impact of age over the Fraud Type Experienced about the fraud of plastic money on the basis of age, for impact of age on Fraud Type Experienced after Fraud is measured with the Chi Square test and the results are presented as under:

Table 4.1: Fraud Situation Experienced * Age Cross tabulation

Count						
		Age				Total
		20-30 years	31-40 years	41-50 years	> 50 years	
Fraud Situation Experienced		1	0	0	1	2
	Auto generated mails to your inbox	44	22	1	10	77

	Calls for disclose my debit card witch was not own by me . It was like they want to disclose my personal details.	1	0	0	0	1
	Confidential reports/information being hacked	12	2	1	1	16
	Hacked my Flipkart account	0	1	0	0	1
	Why other should bother	1	1	2	0	4
	Never experienced such situation	48	16	10	15	89
	Publishing obscure material on your profile	5	1	0	0	6
	Trojan or Malware	15	4	7	1	27
Total		**127**	**47**	**21**	**28**	**223**

Table 4.2: Chi-Square Tests

	Value	**df**	**Asymp. Sig. (2sided)**
Pearson Chi-Square	54.991[a]	33	.010
Likelihood Ratio	46.690	33	.058
N of Valid Cases	223		

a. 37 cells (77.1%) have expected count less than 5. The minimum expected count is .09.

The output of the ‘chi square test’ in the table-4.2, reveals that significant gap exists between the hypothesized test value with the calculated sample statistics for measuring the impact of age on Fraud Type Experienced for fraud happened with the respondents ($p>0.05$) at 5% level of significance. The respondents with the age of 2030 years have exhibited better satisfaction for control over Auto generated mails to their inbox with the efforts of the cyber cell for better control over the recovery process.

5. Impact of Age on Preference of Cash

To measure the impact of age over the Preference of Cash about the fraud of plastic money on the basis of age, for impact of age on Preference of Cash after Fraud is measured with the Chi Square test and the results are presented as under:

Table 5.1: Preference of Cash * Age Cross tabulation

Count						
		Age				Total
		20-30 years	**31-40 years**	**41-50 years**	**> 50 years**	
Preference	More extent	17	7	3	3	30
of Cash	Not at all	13	4	3	2	22
	To an extent	31	6	4	5	46
	To some extent	66	30	11	18	125
Total		**127**	**47**	**21**	**28**	**223**

Table 5.2

Chi-Square Tests			
	Value	df	Asymp. Sig. (2sided)
Pearson Chi-Square	4.664[a]	9	.863
Likelihood Ratio	4.802	9	.851

N of Valid Cases	223		

a. 6 cells (37.5%) have expected count less than 5. The minimum expected count is 2.07.

The output of the 'chi square test' in the table-5.2, reveals that insignificant gap exists between the hypothesized test value with the calculated sample statistics for measuring the impact of age on performance of cash for fraud happened with the respondents ($p>0.05$) at 5% level of significance.

6. Findings of Study:

a. Impact of age on awareness: Insignificant gap exists between the hypothesized test value with the calculated sample statistics for measuring the impact of age on awareness for fraud happened with the respondents ($p>0.05$) at 5% level of significance. The respondents have exhibited no differences for the age wise categories.

b. Impact of age on Perceived Security: Insignificant gap exists between the hypothesized test value with the calculated sample statistics for measuring the impact of age Perceived Security for fraud happened with the respondents ($p>0.05$) at 5% level of significance. The respondents have exhibited no differences for the age wise categories.

c. Impact of age on Customer Satisfaction: Significant gap exists between the hypothesized test value with the calculated sample statistics for measuring the impact of age on Customer Satisfaction for fraud happened with the respondents ($p>0.05$) at 5% level of significance. The respondents have exhibited that the respondents with the age of 20-30 years were more satisfied with the efforts of the cyber cell for better control over the recovery process.

d. Impact of age on Fraud type: Significant gap exists between the hypothesized test value with the calculated sample statistics for measuring the impact of age on Fraud Type Experienced for fraud happened with the respondents ($p>0.05$) at 5% level of significance. The respondents with the age of 20-30 years have exhibited better satisfaction for control over Auto generated mails to their inbox with the efforts of the cyber cell for better control over the recovery process.

e. Impact of age on Preference of Cash: Insignificant gap exists between the hypothesized test value with the calculated sample statistics for measuring the impact of age on performance of cash for fraud happened with the respondents ($p>0.05$) at 5% level of significance.

7. Conclusion:

The respondents have exhibited no differences for the age wise categories. The respondents have exhibited that the respondents with the age of 20-30 years (Gen Z) were more satisfied with the efforts of the cyber cell for better control over the recovery process. The respondents with the age of 20-30 years (Gen Z) have exhibited better satisfaction for control over Auto generated mails to their inbox with the efforts of the cyber cell for better control over the recovery process.

References:

- Chaudhary, A., Patel, K., & Singh, R. (2021). *Digital fraud and Millennials: Awareness, behavior, and preventive measures.* Cybersecurity Journal, 12(3), 45-60.
- Garg, P., & Sharma, N. (2023). *Understanding social engineering scams among Gen Z and Millennials.* Journal of Cyber Psychology, 9(2), 78-92.
- Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2021). *Risk factors for cyber fraud victimization: A generational perspective.* Journal of Crime & Cybersecurity, 15(4), 112-130.
- Johnson, L., & Carter, S. (2020). *Cybersecurity education: Bridging the generational awareness gap.* Digital Security Review, 18(2), 56-71.
- Kumar, R., Singh, V., & Gupta, M. (2020). *The evolution of cyber fraud: Trends, risks, and prevention strategies.* Cybercrime Review, 20(1), 34-50.
- Lee, H., Brown, T., & Cooper, J. (2022). *Social media fraud and digital natives: An analysis of Gen Z's vulnerability to cyber scams.* Journal of Online Security, 10(3), 99-115.
- Mills, B. (2022). *Generation X and cyber threats: A study on risk perception and awareness.* Cybersecurity & Behavior, 7(1), 23-40.
- Patel, K., & Singh, R. (2023). *The rise of cryptocurrency scams: Are older generations more vulnerable?* Financial Cybersecurity Review, 14(2), 78-95.
- Roberts, P., Anderson, D., & Taylor, J. (2021). *Generational differences in online risk-taking behavior.* Digital Safety Journal, 11(4), 67-82.
- Smith, J., & Jones, M. (2021). *Cybercrime in the 21st century: Trends, challenges, and prevention strategies.* Cyber Security Research, 19(3), 88-105.
- Smith, R., Patel, A., & Kumar, S. (2023). *Cybersecurity habits among Gen Z: Understanding risks and responses.* Journal of Digital Awareness, 15(1), 41-58.
- Taylor, R., & Brown, P. (2022). *Phishing scams and Millennials: Examining susceptibility and prevention.* Journal of Cyber Threats, 13(2), 54-72.
- Williams, C., & Cooper, H. (2023). *Online security challenges for Gen Z: A study of social media fraud and digital literacy.* Journal of Digital Risk Management, 16(2), 103-119.