AMERICAN JOURNAL OF BUSINESS MANAGEMENT
ISSN: 2996-5098 (online) | ResearchBib (IF) = 10.61 IMPACT FACTOR
Volume-4| Issue-4| 2026 Published: |30-04-2026|

THE IMPACT OF THE AGE FACTOR ON PLASTIC CARD FRAUD: A SWOT ANALYSIS ACROSS AGE GROUPS

https://doi.org/10.5281/zenodo.19730192

Imomov Jamshidkhon Odilovich
Tashkent State University of Economics
Associate Professor, Department of Economic and Financial Security, PhD
E-mail: jamshidkhon@gmail.com
Tel: +998983601283
Toshpulatova Mohizodakhon Latifkhon qizi
Student of Tashkent International University
Tel: +998508892588

Abstract

This paper examines the role of the age factor in plastic card fraud in Uzbekistan through SWOT analysis. The study draws on a survey conducted in Tashkent in 2024 (n=391, 44 Likert-scale items, Cronbach a=0.745-0.919) and international academic literature. Cybersecurity knowledge, digital skills, practical application of protective measures, and trust in the banking system were assessed for five age groups: 18-25, 26-35, 36-45, 46-55, and 56 and above. The SWOT matrix identified the strengths, weaknesses, opportunities, and threats specific to each group. The key finding is that the relationship between age and fraud risk is non-linear. The 18-25 age group demonstrated the highest knowledge level (M=3.91), yet showed the largest gap between knowledge and practice (+0.64). Older respondents scored lower on knowledge (M=2.83), but face fewer attacks due to lower online activity. Trust in the banking system was low across all groups (M=1.54-1.81), indicating a systemic problem.

Keywords

plastic card fraud, age factor, SWOT analysis, cybersecurity, digital literacy, age groups, Uzbekistan.

1. INTRODUCTION

The widespread adoption of plastic cards and mobile payments has significantly simplified access to financial services in everyday life. However, this convenience has also introduced new risks. According to Kaspersky Lab (2025), the data of over 2 million bank cards were stolen through malicious software (stealer malware). The Nasdaq Global Financial Crime Report (2024) estimated total losses from financial fraud worldwide at 485.6 billion dollars. In Uzbekistan, the CERT-

AMERICAN JOURNAL OF BUSINESS MANAGEMENT
ISSN: 2996-5098 (online) | ResearchBib (IF) = 10.61 IMPACT FACTOR
Volume-4| Issue-4| 2026 Published: |30-04-2026|

CBU Cybersecurity Center reports that social engineering — deception via phone, SMS, and the internet — remains the most prevalent method of plastic card fraud.

Financial literacy is widely recognized as a key protective factor against fraud. However, the relationship between age and fraud risk is frequently misunderstood. A common assumption holds that older individuals are more vulnerable due to poor technology skills, while younger people can better protect themselves owing to their digital competencies. Ruiz (2026), in a large-scale study of over 14,000 individuals across 10 European countries, challenged this assumption: the 18-29 age group exhibited the highest victimization rate among all age groups. This finding warrants testing within the Uzbekistan context.

The aim of this paper is to assess cybersecurity indicators across age groups among plastic card users using SWOT analysis — identifying the strengths, weaknesses, opportunities, and threats specific to each group — and to provide practical recommendations. SWOT analysis (Strengths, Weaknesses, Opportunities, Threats) enables systematic and comprehensive assessment without complex statistical calculations, making it widely applicable in social research.

2. LITERATURE REVIEW

The relationship between age and financial fraud has been studied repeatedly in international literature, yet findings are often contradictory. Kieffer and Mottola (2017) identified older adults as the primary target group — attributing this to their greater accumulated savings and less cautious financial decision-making. However, Ruiz (2026), in a comprehensive study across 10 European countries, reached the opposite conclusion: the 18-29 age group showed the highest scam victimization rate (12.1%), while those aged 70 and over showed the lowest (7.4%). Ruiz attributed this difference to young people spending more time online, making faster decisions, and showing greater interest in new offers.

Chowdhury et al. (2026), in a study conducted in Bangladesh, identified a "digitally literate but financially inexperienced" group — primarily young adults — who scored high on digital skills but struggled to accurately assess financial risk, remaining vulnerable to phishing schemes. They also documented the overconfidence phenomenon: a knowledgeable individual feels safe and fails to take precautionary measures. Ruiz (2026) similarly found that overconfidence increases fraud victimization risk by 29-37%.

Isaia, Oggero, and Sandretto (2024) found that practical digital security skills — such as protecting passwords and recognizing suspicious links — rather than traditional financial knowledge, constitute the primary protective factor. This conclusion applies equally to age groups: whichever group demonstrates higher practical skills tends to experience lower victimization rates.

AMERICAN JOURNAL OF BUSINESS MANAGEMENT
ISSN: 2996-5098 (online) | ResearchBib (IF) = 10.61 IMPACT FACTOR
Volume-4| Issue-4| 2026 Published: |30-04-2026|

SWOT analysis is a structured method for evaluating the internal strengths and weaknesses of a subject, alongside external opportunities and threats. Originally developed for strategic management, it has since been widely adopted in social and economic research. In the context of financial literacy, SWOT analysis allows one to assess not only the current state of age groups, but also their development potential and the threats they face. This approach generates clear, visual, and policy-relevant conclusions without reliance on complex mathematical methods.

3. RESEARCH METHOD

The study employed SWOT analysis. Data were obtained from a survey conducted in Tashkent in 2024 (n=391). The questionnaire comprised 44 items, all rated on a 5-point Likert scale (1=strongly disagree, 5=strongly agree). Nine thematic blocks were covered: general financial literacy, digital skills, cybersecurity knowledge, personal fraud experience, trust in the banking system, practical application of protective measures, attitudes toward social engineering, use of digital payments, and overall satisfaction. Cronbach alpha values ranged from 0.745 to 0.919, indicating satisfactory to high reliability.

Respondents were divided into five age groups: 18-25 (n=112), 26-35 (n=136), 36-45 (n=83), 46-55 (n=44), and 56 and above (n=16). Mean scores were calculated for four key indicators per group: cybersecurity knowledge (S5), digital skills (S7), practical application of protective measures (S12), and trust in the banking system (S19). A separate SWOT matrix was constructed for each age group based on survey results and international literature.

4. KEY SURVEY INDICATORS

Table 1. Key indicators by age group (5-point scale, n=391)

Indicator	18-25	26-35	36-45	46-55	56+
Cybersecurity knowledge (S5)	**3.91**	3.84	3.72	3.41	2.83
Digital skills (S7)	**4.12**	3.87	3.41	2.94	2.31
Practical application (S12)	3.48	**3.51**	3.18	2.87	2.28
Trust in banking system (S19)	1.62	1.74	**1.81**	1.68	1.54
Knowledge-practice gap	**+0.64**	+0.36	+0.23	+0.07	+0.03

Source: author, based on 2024 Tashkent survey (n=391).

AMERICAN JOURNAL OF BUSINESS MANAGEMENT
ISSN: 2996-5098 (online) | ResearchBib (IF) = 10.61 IMPACT FACTOR
Volume-4| Issue-4| 2026 Published: |30-04-2026|

Table 1 reveals several important trends. First, cybersecurity knowledge and digital skills decline steadily with age. Second, trust in the banking system is low across all groups, never exceeding 2.0 — indicating a systemic problem. Third, the knowledge-practice gap is largest among younger groups (+0.64) and narrows with age, reflecting a pattern where young adults know but do not act, while older adults do what they know (though both scores remain low). These indicators form the empirical foundation of the SWOT matrices.

5. SWOT ANALYSIS RESULTS

A separate SWOT matrix is presented for each age group below. Each matrix comprises four elements: Strengths (S), Weaknesses (W), Opportunities (O), and Threats (T), populated on the basis of survey data and international literature.

Table 2. SWOT matrix: 18-25 age group (n=112)

	Element	Content	Evidence
S	**Strengths**	– Highest cybersecurity wledge (M=3.91) – Most developed digital skills 4.12) – Rapid adaptation to new nologies – Active sharing of security rience among peers	– S5=3.91 — highest across all ps – S7=4.12 — highest across all ps – Chowdhury et al. (2026): ng adults lead in technological otability – Active information sharing ocial networks
W	**Weaknesses**	– Largest knowledge-practice (+0.64) – Overconfidence: "I cannot be ived" – Very low trust in banking em (M=1.62) – Habit of making quick sions without verification	– S12=3.48, S7=4.12 — gap of the largest – Ruiz (2026): overconfidence eases risk by 29-37% – S19=1.62 — second lowest ng all groups – Isaia et al. (2024): knowledge e is insufficient for protection
O	**Opportunities**	– Converting knowledge into tice through interactive formats eo, games, quizzes) – Peer influence — spreading a ure of security among friends – Social media campaigns for d, wide-reach awareness building	– Young adults respond better ideo and interactive content than – Peer influence is effective in nging behavior – Instagram, TikTok, Telegram: t effective delivery channels
T	**Threats**	– Phishing sites and fake offers ad via social media – Investment schemes	– Ruiz (2026): young adults are primary target for phishing and hs

AMERICAN JOURNAL OF BUSINESS MANAGEMENT
ISSN: 2996-5098 (online) | ResearchBib (IF) = 10.61 IMPACT FACTOR
Volume-4| Issue-4| 2026 Published: |30-04-2026|

	Element	Content	Evidence
		nising rapid wealth – SMS and calls demanding ediate decisions	– Ponzi schemes are actively noted to young people via social orks – "Act now or it will be too late" me pressure tactic

Source: author, based on 2024 survey and international literature.

The SWOT analysis for the 18-25 age group reveals a paradoxical situation: the group with the highest knowledge and digital skills simultaneously exhibits the largest knowledge-practice gap. The core problem for this group is that knowledge does not translate into effective protection — and the primary reason is overconfidence.

Table 3. SWOT matrix: 26-35 age group (n=136)

	Element	Content	Evidence
S	**Strengths**	– High knowledge and digital s (M=3.84 and 3.87) – The largest group of card s — practical experience lable – Relatively small knowledge-tice gap (+0.36) – Established experience in ing with banks	– Largest group in the survey 36, 34.8%) – Majority have 3+ years of card experience – 26-35 year-olds are paratively more experienced in king relations – Practical and theoretical wledge are relatively balanced
W	**Weaknesses**	– Vulnerability to fake stment and job offers – Low trust in banks (M=1.74) voidance of filing complaints – Financial pressure (credit, sing costs) undermines decision ity	– Investment interest and ncial risk are high at this age – S19=1.74 — low, with a eption that banking support is eliable – Middle-income group shows er financial vulnerability (Ruiz,)
O	**Opportunities**	– Cybersecurity training ugh the workplace – Developing skills to verify stment offers – Building trust through roved banking services	– The workplace is a convenient nel for reaching a large audience – Awareness of investment d is especially important for this up – Banks can offer tailored rity services for this ographic

AMERICAN JOURNAL OF BUSINESS MANAGEMENT
ISSN: 2996-5098 (online) | ResearchBib (IF) = 10.61 IMPACT FACTOR
Volume-4| Issue-4| 2026 Published: |30-04-2026|

	Element	Content	Evidence
T	Threats	– Fake investment platforms "get rich quick" schemes – Fraudulent offers circulated elegram and WhatsApp groups – Social engineering calls ersonating bank employees	– This age period involves ve financial and investment sion-making – Messenger-based fraud is easing (CERT-CBU, 2024) – Fake bank employee — the t frequently recorded method by T-CBU

Source: author, based on 2024 survey and international literature.

Table 4. SWOT matrix: 36-45 age group (n=83)

	Element	Content	Evidence
S	Strengths	– Long-standing relationship experience with banking – Increased caution in financial sion-making – Relatively highest trust in ks among all groups (M=1.81) – Knowledge and practice are ively aligned (+0.23)	– Years of card use experience – Life experience enhances ncial caution – S19=1.81 — the highest king trust score among all groups – Knowledge-practice gap is ller compared to younger groups
W	Weaknesses	– Digital skills have declined to age level (M=3.41) – Outdated security habits may address new threats – Many have experienced tisfactory outcomes when raising k issues	– S7=3.41 — noticeably lower younger groups – New phishing methods and fake calls render old knowledge fficient – Unresolved complaints have ed trust in the system
O	Opportunities	– In-person seminars and face-ce learning formats are effective – Bank SMS notifications for ly alerts on new threats – Updating digital skills ugh children in the household	– This group actively icipates in seminars and meetings – SMS notifications are an ctive channel for this ographic – Reverse technology learning ugh children is a viable route
T	Threats	– Phone calls impersonating k employees – Deepfake technology enabling ption using familiar voices – High-value financial rations as primary target	– CERT-CBU: fake phone calls he most widely recorded method – Kaspersky (2025): deepfake cks are on the rise – Higher savings balances in group make them high-value

	Element	Content	Evidence
			ets

Source: author, based on 2024 survey and international literature.

The 46-55 age group (n=44) shows declining digital skills (M=2.94) and very low trust in the banking system (M=1.68). The main strength of this group is more cautious financial behavior and a small knowledge-practice gap (+0.07). Weaknesses include falling behind on new technologies and deep skepticism toward the banking system. The primary threats are proxy fraud (someone attempting to withdraw money in their name) and fake social benefit notifications. Opportunities include face-to-face instruction at bank branches and SMS notifications.

The 56 and above group (n=16) scored the lowest across all indicators: cybersecurity knowledge M=2.83, digital skills M=2.31, trust in banks M=1.54. However, a key distinction is that their knowledge-practice gap is nearly zero (+0.03) — because both knowledge and practice are low, meaning they do what they know. Their key strength is that low online activity provides relative protection from attacks. The primary threat is phone-based fraud and family-context exploitation schemes. Opportunities lie in family-based education channels, community meetings, and simplified written instructions.

6. DISCUSSION

The SWOT analysis clearly showed that cybersecurity knowledge declines with age across all groups: from M=3.91 among 18-25 year-olds to M=2.83 among those aged 56 and above. This is an expected trend. However, an important qualification must be noted: lower knowledge does not always mean higher risk. The 56+ group scores low on knowledge, but their online activity is also low, meaning they encounter fewer fraud attempts. Ruiz (2026) reached the same conclusion in the European context: older adults were less likely to be victimized than younger groups.

The most significant weakness identified in the SWOT analysis for the 18-25 age group is the +0.64 knowledge-practice gap. They are knowledgeable (S7=4.12), yet do not apply protective measures in daily life (S12=3.48). Overconfidence — the mindset of "I cannot be deceived" — is the primary cause. Chowdhury et al. (2026) identified the same phenomenon in Bangladesh: the correlation between knowledge and practice was found to be below 0.10, confirming that knowledge alone does not change behavior.

AMERICAN JOURNAL OF BUSINESS MANAGEMENT
ISSN: 2996-5098 (online) | ResearchBib (IF) = 10.61 IMPACT FACTOR
Volume-4| Issue-4| 2026 Published: |30-04-2026|

The most consistent finding across all SWOT matrices is that trust in the banking system is low in all five age groups, never exceeding 2.0. This is not a characteristic specific to one age group. The 36-45 group scored relatively higher (M=1.81), but this remains objectively low. Chowdhury et al. (2026) found that institutional trust is a stronger predictor than financial knowledge. Accordingly, education programs targeted at age groups must be paired with improvements to bank compensation mechanisms and complaint procedures.

7. PRACTICAL RECOMMENDATIONS

Table 5. Age-targeted recommendations (based on SWOT results)

Age group	Key weakness	Recommendation	Delivery channel
18-25	Knowledge-practice gap (+0.64); overconfidence	Simulation-based exercises to convert knowledge into practice; "test yourself" format; awareness of overconfidence risk	Instagram, TikTok, YouTube short videos; peer influence campaigns
26-35	Vulnerability to investment fraud; low trust in banks	Developing skills to verify investment offers; simplifying bank complaint procedures	Workplaces and trade unions; online webinars; bank information services
36-45	New technological threats; fake phone calls	Timely alerts on new fraud methods; exercises for recognizing fake calls	Bank SMS notifications; local seminars; branch staff interactions
46-55	Declining digital skills; reluctance to file complaints	Simple, repeated rules: never share PIN; always verify bank number; complaining is allowed	Television and radio; bank branches; community meetings
56+	Technological illiteracy; vulnerability to phone fraud	Three core rules: do not share PIN; do not share card number; always call the bank yourself	Children and grandchildren; community activists; simple printed leaflets

Source: author's SWOT analysis.

8. CONCLUSION

This paper examined the impact of the age factor on plastic card fraud in Uzbekistan through SWOT analysis across five age groups. The study reached four independent conclusions.

First conclusion. The relationship between age and fraud risk is non-linear. Cybersecurity knowledge declines with age (3.91 at 18-25; 2.83 at 56+), but

knowledge level alone does not determine fraud risk. Online activity, psychological factors, and financial experience all play decisive roles. Lower online activity among older adults provides relative protection.

Second conclusion. The primary problem for young adults is the knowledge-practice gap (+0.64). Despite showing the highest knowledge and digital skills, the 18-25 group does not apply this knowledge to daily protective behavior. Overconfidence is the primary cause, found to increase fraud victimization risk by 29-37% (Ruiz, 2026). Education programs should be oriented toward changing behavior rather than simply transferring knowledge.

Third conclusion. Trust in the banking system is low across all groups (M=1.54-1.81) — this is a systemic problem. Regardless of age group, all respondents lacked confidence in receiving adequate support from their bank in the event of fraud. Without improving the transparency of compensation mechanisms and simplifying complaint procedures, financial literacy programs cannot achieve their full potential.

Fourth conclusion. Each age group has a distinct type of vulnerability and requires a tailored approach. Young adults need interactive simulations and peer influence; middle-aged groups need bank notifications and investment literacy; older adults need simple, repeated rules and family-based channels. A single educational format will not produce equal results across all groups.

REFERENCES:

2. Chowdhury, T. A., Chowdhury, M. A. H., Rahman, M. T., Ahmed, I., Ahmed, N., Tuhin, M. A. I., & Kafy, A. A. (2026). Modeling financial literacy through explainable machine learning and behavioral segmentation in emerging economies. Computers in Human Behavior Reports, 21, 100926. https://doi.org/10.1016/j.chbr.2025.100926

3. European Central Bank & European Banking Authority. (2024). 2024 Report on payment fraud. Frankfurt: ECB/EBA. https://www.ecb.europa.eu

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. https://doi.org/10.1016/j.jbef.2024.100977

5. Kaspersky. (2025). Stealer malware leaked over 2 million bank cards. https://www.kaspersky.com/about/press-releases

6. Kieffer, C. N., & Mottola, G. R. (2017). Understanding and combating investment fraud. In O. S. Mitchell, P. B. Hammond & S. P. Utkus (Eds.), Financial

decision making and retirement security in an aging world. Oxford University Press.

7. Li, J., Wei, X., & Zhao, H. (2024). Digital literacy and fraud vulnerability: Evidence from rural China. China Economic Review, 85, 102156.

8. Lusardi, A., & Mitchell, O. S. (2014). The economic importance of financial literacy: Theory and evidence. Journal of Economic Literature, 52(1), 5-44. https://doi.org/10.1257/jel.52.1.5

9. Nasdaq. (2024). Global Financial Crime Report 2024. Nasdaq Verafin.

10. Ruiz, J. R. (2026). Who gets scammed? The roles of financial literacy, digital financial security, and overconfidence in Europe. International Review of Economics and Finance, 106, 104913. https://doi.org/10.1016/j.iref.2026.104913

11. Soriyev, S., & Tuychiyeva, N. (2022). Improving financial literacy of the population and the factor of economic development of regions. STARS International University Conference Proceedings, 5, 435-438.

12. Vahobov, A. V., & Dusmuhamedov, O. S. (2022). Improving the theoretical foundations of the concept of financial literacy. Economics and Finance, 5(153), 21-28.