Research Article
2026, Vol. 02, Issue 01, 1-17
https://doi.org/10.xxxx/xxxxx

Journal of Innovations in
Social and Applied Sciences

Socioeconomic Inequalities in Mobile Scam Exposure in AI Era

Mohamed Abdel Alim Saber[1], Mirsat Yesiltepe[2]

[1]Higher Institute of Commercial Sciences, Abu Qir, Alexandria, Egypt
[2]Department of Computer Engineering, Istanbul University, Istanbul, Turkey

abdel.alim@hics-unv.com; yesiltepemirsat@istanbul.edu.tr

Corresponding Author: *yesiltepemirsat@istanbul.edu.tr*

Abstract

Scam calls and fraudulent text messages now reach large numbers of mobile phone owners in low- and middle-income economies, yet evidence on who receives them relies mostly on complaint registers, bank records, and single-country surveys that are difficult to compare. This study describes how self-reported receipt of a scam call or text is distributed across socioeconomic groups, using respondent-level microdata from the Global Findex Database 2025. The analytical sample comprises 64,509 mobile phone owners across the 75 economies where the digital connectivity module was fielded. Weighted prevalence, percentage-point gaps, and prevalence ratios were estimated by gender, age, education, within-economy income quintile, workforce participation, and rural or urban residence, with survey weights rescaled so that each economy carried equal influence and uncertainty clustered by economy. Adjusted prevalence and average marginal effects were estimated using a weighted logistic model with economy fixed effects. Overall, 21.9% (95% CI 18.7–25.1) of phone owners reported receiving a scam call or text. Reported exposure was higher among tertiary-educated respondents than among those with primary education or less (27.4% versus 19.4%), among workforce participants than non-participants (25.0% versus 16.5%), and in the richest than in the poorest income quintile (25.2% versus 18.9%). Exposure peaked between ages 25 and 44 and was lowest at 65 and older (15.6%). Women reported 2.8 percentage points less exposure than men. After mutual adjustment, the education (+8.0 points) and workforce (+4.6 points) differences remained the largest, while the income difference narrowed to 2.6 points. Exposure to scam attempts, therefore, follows economic and communicative activity more closely than conventional markers of disadvantage, which suggests that awareness measures should reach economically active and more educated users as well as groups usually labeled vulnerable.

Article History

Manuscript Received
January 21, 2026

First Revision
June 19, 2026

Final Acceptance
July 02, 2026

Keywords: mobile scams; fraud exposure; socioeconomic inequality; digital financial inclusion; consumer protection

1 Introduction

Mobile phones have become the main point of contact between many households and the wider economy. In 2024, phones carried wage and benefit payments, remittances, loan applications, and government notices, and in many low- and middle-income economies they did so for people who had never held a bank card [1]. The same channel that makes these services reachable also makes their users reachable. Anyone with a number can be called or sent a message by someone they have never met, and a share of those unsolicited contacts are attempts to obtain money or credentials by deception.

Fraudulent calls and text messages are not new, but their volume has grown with the spread of phones and mobile money. Survey evidence from very different settings points in the same direction. In Australia, 65% of people aged 15 and over reported being exposed to a scam in 2021–22, and phone calls and text messages were the two most frequent routes [2]. In the United States, 68% of adults said they received scam calls at least weekly and 61% received scam texts at least weekly [3]. In a 12-country online survey that included Egypt, Indonesia, Mexico and South Africa, phone calls were the initial point of contact in 14% of the most recent scam attempts that respondents described [4]. The Global Findex 2025 report adds that nearly one in five phone owners in low- and middle-income economies received a message from an unknown person asking for money [1].

Exposure of this kind matters for consumer finance and not only for crime statistics. Scam messages frequently impersonate banks and mobile-money providers, and in doing so they target the trust on which digital financial inclusion depends [5, 6]. Even when no money is lost, each attempt imposes a screening burden on the recipient and can discourage use of legitimate services. How that burden is spread across the population is a question about inequality. If attempts are concentrated among people with few resources and little formal education, exposure adds to existing disadvantage. If they are concentrated among people who are more active in the digital and cash economy, the pattern says something different about where fraudsters look for returns and where prevention should be directed.

Answering that question from administrative evidence is difficult. Police complaints, bank fraud files, and consumer-protection registers record the minority of incidents that someone chose to report, usually after a loss. In Spain, fewer than one in twenty card frauds detected by banks appeared in police statistics [7]. Dutch panel respondents who experienced cybercrime reported only 13.1% of incidents to the police [8], and more than a third of scam victims in a 12-country survey reported the incident to no one [4]. Complaint systems such as the one maintained by the U.S. Federal Trade Commission are valuable for tracking tactics and losses, but they describe people who reached the reporting system and not the population that was targeted [9]. Failed attempts are almost never recorded. Population surveys are, therefore, the main way to observe exposure itself.

A second distinction runs through this paper. Receiving a scam communication is not the same as being defrauded. Studies that separate the two stages find that the characteristics associated with being targeted differ from those associated with responding or losing money [10, 11, 12]. In China, for example, only 2.35% of older adults who reported exposure to fraud also reported a financial loss [13]. This study examines exposure only. It asks who receives scam calls and messages, not who is deceived by them.

The existing evidence on socioeconomic patterns in exposure is fragmented. Most studies cover a single country, often a high-income one, and many are limited to older adults, students, or online panels [14, 15, 12, 16]. Definitions range from any unsolicited fraudulent approach to specific scam types, and data sources range from national statistical surveys to complaint registers. Findings on income, education, and gender are consequently inconsistent, and the few multi-country surveys do not report exposure by socioeconomic group [4]. What remains limited is harmonized individual-level evidence, collected with a common question across many low- and middle-income economies, on how exposure to mobile scams differs across socioeconomic groups.

The objective of this study is to provide descriptive evidence using the respondent-level Global Findex 2025 microdata [17]. The single research question is: *How is exposure to mobile scam calls and messages distributed across socioeconomic groups?* Gender, age, education, within-economy income, workforce participation, and rural or urban residence are treated as dimensions of this one question. The study makes the following contributions:

- It provides survey-weighted estimates of self-reported scam-call and scam-text exposure for 64,509 mobile-phone owners in 75 economies, all measured with the same question in the same survey round.

- It reports prevalence, absolute gaps, and prevalence ratios for six socioeconomic dimensions, using a weighting scheme that keeps populous economies from dominating the pooled estimates.
- It examines four pre-specified intersections (age by gender, education by income, workforce participation by gender, and income by residence).
- It estimates adjusted prevalence and average marginal differences with economy fixed effects, and tests their robustness to weighting, connectivity controls, age coding, and item nonresponse.
- It draws implications for the targeting of awareness campaigns and consumer-protection measures by telecommunications providers, financial institutions, and regulators.

The rest of the paper is organized as follows. Section 2 reviews research on mobile scams, exposure measurement, and socioeconomic differences in exposure. Section 3 describes the data, variable construction, weighting, and estimation. Section 4 presents the sample profile, the socioeconomic distribution of exposure, and the intersecting and adjusted results. Section 5 interprets the findings against the literature and discusses their limitations, and Section 6 concludes.

2 Literature Review

2.1 Mobile Scams and Consumer Exposure

Much of the research on fraud draws on routine activity theory, which holds that victimization requires a motivated offender, a suitable target, and the absence of capable guardianship to converge in time and space [18]. Applied to fraud, the theory directs attention to the everyday activities that bring people into contact with offenders. Holtfreter, Reisig, and Pratt found among 922 Florida adults that remote purchasing, such as buying by telephone, mail, or internet, raised the likelihood of being targeted for fraud [10]. A later analysis of the same sample showed that the association between sociodemographic characteristics and online fraud targeting was fully accounted for by indicators of routine online activity [19]. The implication for the present study is direct: groups that communicate and transact more are expected to receive more fraudulent approaches, whatever their susceptibility to them.

Research on scams delivered by phone reinforces this view but also shows how much measurement shapes the results. National statistical surveys that ask about any unsolicited scam invitation produce high prevalence figures. The Australian Personal Fraud Survey defines exposure as receiving an unsolicited invitation, request, notification, or offer, and found that 65% of the population were exposed in 2021–22 while only 2.7% responded [2]. The Pew Research Center's 2025 survey measured frequency instead, finding that most U.S. adults received scam calls and texts every week [3]. By contrast, the 12-country survey by Houtti and colleagues recorded the most recent scam attempt and its vector among 8,369 internet users, and found that scam exposure and scam loss were uncorrelated across countries while losses were strongly and inversely correlated with national income [4]. These studies are not directly comparable, because they differ in their reference periods, in whether they count attempts or people, and in whether offline populations are covered. They agree, however, that attempts are far more common than losses, and that phone calls and text messages are leading delivery channels.

Survey measures of exposure rest on recognition. A respondent can only report a scam call if they identified it as one. Experimental work in Kenya, where 96% of a consumer panel said they had been contacted by a scammer, found that the ability to classify SMS messages as scams or genuine was modest and that simple tips increased the flagging of real scams at the cost of more false alarms [20]. Qualitative work in the United States shows that people judge text messages largely by whether they expected them and whether the sender appeared familiar [21]. Eye-tracking evidence suggests that people misreport the cues they actually rely on [22]. Victims also differ in whether they acknowledge an experience as fraud at all [23]. Self-reported exposure should therefore be read as exposure that was noticed and labelled as a scam, a point that becomes important when comparing groups that may differ in recognition.

Administrative data face the opposite problem, recording too little rather than too much. Kemp and colleagues combined police, bank, and survey data for Spain and showed that police records captured only a small fraction of fraud and that fraud reporting rates across European victimization surveys were around 20–25% [7]. In the Netherlands, the gap between intended and actual reporting of cybercrime was large, and many victims believed the police would not act [8]. Complaint databases, such as the U.S. Consumer Sentinel Network, record millions of fraud reports each year and track contact methods, but they are shaped by who knows how and where to report [9]. In lower-income settings, providers' fraud logs and regulator complaint systems are the main sources, and they focus on losses associated with specific services such as mobile money [5, 6]. Houtti and colleagues found that residents of less affluent countries were also less likely to know how to report a scam [4]. Taken together, these studies suggest that the geography and demography of recorded fraud reflect reporting as much as targeting. A harmonized population survey that asks everyone the same exposure question avoids this selection, even though it introduces the recognition issue discussed above.

2.2 Socioeconomic Inequalities in Scam Exposure

Age is the most studied dimension, and it shows how important the distinction between exposure and victimization is. Research and policy have long focused on older adults. A meta-analysis of U.S. studies estimated that about 5.4% of cognitively intact older adults experience fraud or scam victimization each year [14]. Studies of exposure rather than loss, however, rarely find that the oldest groups are the most targeted. In the Australian survey, exposure rose from 53.3% among 15–24-year-olds to 69.4% at ages 35–44 and then declined to 61.6% among those aged 65 and over [2]. U.S. data show younger adults reporting losses more often than older adults (25% of 18–29-year-olds against 15% of those 65 and over) [3], and Parti found higher online-fraud victimization among younger than older respondents in a national U.S. panel [16]. Whitty's analysis of nearly 12,000 survey respondents, on the other hand, associated cyber-fraud victimhood with older age alongside impulsivity and risky online behaviour [24]. The age pattern therefore seems to depend on whether the outcome is contact or loss, and on the scam type.

Evidence on gender is thinner and less consistent. The Australian survey found no meaningful difference between men and women in either exposure or victimization [2]. Japanese survey data showed higher overall victimization among men [25]. In the Kenyan experiment, women were 3 percentage points less accurate in identifying scam messages [20]. DeLiema, Li, and Mottola found that gender was among the characteristics related to responding to and losing money in some, but not all, scam categories, and that the risk factors for responding differed from those for victimization [11]. None of these studies examines whether gender differences in exposure reflect differences in phone use, workforce participation, or public visibility. This matters in low- and middle-income economies, where women are 14% less likely than men to use mobile internet [26].

Findings on education and income are the most counterintuitive for policy debates that treat fraud risk as a function of disadvantage. Using the 2015 China Household Finance Survey, Yu, Kuo, and Tseng found that higher financial literacy and greater risk tolerance were associated with more fraud exposure as well as more victimization among 22,121 adults aged 50 and over [15]. In a multilevel analysis of 10,010 older CHARLS respondents, higher education, internet use, urban residence, and residence in more developed regions were all associated with greater exposure [13]. Mao and Liu found no direct association of education or urban residence with victimization, but a positive association with household financial assets, partly operating through financial literacy and interest in financial matters [27]. In the United States, greater non-housing wealth was associated with investment fraud among adults aged 50 and older [28], while in Japan lower household income was associated with fictitious billing fraud and higher assets with refund fraud [25]. Evidence on losses points the other way in some places. Pew reported more frequent losses among lower-income U.S. adults [3], and Li, Li, and Du found that digital literacy was associated with lower victimization in eastern China, especially among rural, older, and female residents [29]. A plausible reconciliation is that resources and education increase the number of approaches a person receives, while low resources and low digital skills make a given approach more costly when it succeeds.

Evidence on employment and residence is scattered across studies that were designed for other purposes. Cohen and Felson's original argument used rising labour-force participation to explain changing opportunities for crime [18]. Among older U.S. adults, those in full-time work reported more victimization than retirees for several scam types [16]. Chinese college students whose routines involved more telecommunication and online activity were more likely to be targeted for telecom and cyber fraud, although those routines did not predict completed loss [12]. Urban residence was associated with higher exposure among older Chinese adults [13], and the Findex 2025 report indicates that exposure is common among phone owners in Sub-Saharan Africa, where much of the population is rural [1]. Few studies examine these dimensions jointly, and almost none estimates how they intersect.

Three limitations follow from this body of work. First, most evidence on socioeconomic patterns comes from single high-income or upper-middle-income countries, older-adult samples, students, or online panels, which exclude people without internet access. Second, exposure and loss are often combined or measured with different instruments, so that a finding about who is defrauded is read as a finding about who is targeted. Third, comparative surveys that cover low- and middle-income economies have focused on national differences and channels rather than on differences between socioeconomic groups within countries [4]. The Global Findex 2025 digital-connectivity module asks one exposure question of phone owners in 75 economies, collected face to face in the same period, which allows socioeconomic differences to be described within a common framework. Because the evidence reviewed here does not support a clear directional hypothesis for every dimension, the analysis is organized around the single descriptive research question stated in the Introduction.

3 Materials and Methodology

3.1 Materials and Data Preparation

The data come from the Global Findex Database 2025, produced by the World Bank's Development Research Group with fieldwork by Gallup, Inc. as part of the Gallup World Poll (reference WLD_2024_FINDEX_v02_M) [17, 1]. The survey measures how adults save, borrow, make payments, and manage financial risk. Interviews took place between May and December 2024 in 141 economies. The public respondent-level file contains 144,090 respondents aged 15 and older in 140 economies and 199 variables. The unit of analysis is the individual respondent. In low- and middle-income economies, samples were drawn with a stratified, clustered area-frame design and interviews were conducted face to face; in most high-income economies, random-digit dialling and telephone interviews were used. Within households, one eligible adult was selected at random. The final survey weight combines a base sampling weight with a post-stratification adjustment to national population figures on gender, age, education, and, where available, socioeconomic status, so that each national sample is designed to be representative of the adult population [17].

The 2025 round introduced a digital-connectivity module, fielded in person in 75 economies in the second half of 2024 [1]. The outcome item, `con21`, is labelled "Received scam text or call" in the data dictionary and is described in the Findex report as receipt of a message from someone the respondent did not know asking for money [1]. The coding of every variable was checked against the value labels in the labelled release. The skip pattern was also checked empirically. In the 75 module economies, `con21` is non-missing for every respondent who reported owning a mobile phone (`con1` = 1) and missing for every respondent who did not, including the 12,198 non-owners. The item therefore measures exposure among phone owners, and all prevalence figures in this paper refer to that population. Respondents in the 65 economies without the module are treated as not asked, never as unexposed.

Sample selection proceeded in four steps. Restricting the complete file to the 75 module economies left 76,898 respondents, of whom 64,663 were phone owners asked the scam item. Answers of "don't know" (130) and refusals (24) were excluded rather than coded as "no", leaving an analytical sample of 64,509 respondents in 75 economies with a valid yes or no answer. The descriptive analyses use every respondent with a valid value for the dimension concerned (available-case analysis). The adjusted models require complete information on all six socioeconomic variables and use 63,209 respondents in 74 economies. One economy drops out of these models because its release does not include the income quintile. Table 1 summarizes the variables and their coding.

Table 1: Dataset, variables, and analytical sample

Construct	Variable	Operational definition	Original coding	Analytical coding	Valid obs.	Role
Scam exposure	`con21`	Received a scam text or call	1 Yes; 2 No; 8 DK; 9 Refused; blank = not asked	1 = Yes; 0 = No; DK/refused excluded	64,509	Outcome
Gender	`female`	Respondent is female	1 Female; 2 Male	Women; Men (ref.)	64,509	Dimension
Age	`age`	Age in completed years	15–100	15–24 (ref.) ... 65+	64,509	Dimension
Education	`educ`	Highest level completed	1 Primary or less; 2 Secondary; 3 Tertiary	Three levels; primary (ref.)	64,248	Dimension
Income	`inc_q`	Within-economy household income quintile	1 Poorest ... 5 Richest	Q1 (ref.) ... Q5	63,646	Dimension
Workforce	`emp_in`	In the workforce	1 In; 2 Out	In; Out (ref.)	64,509	Dimension
Residence	`urbanicity`	Rural or urban residence	1 Rural; 2 Urban	Urban; Rural (ref.)	64,319	Dimension
Internet use	`internet_use`	Used internet in past 3 months	0 No/DK/Ref; 1 Yes	Binary	64,509	Sensitivity
Smartphone	`con9`	Type of phone owned	1 Smartphone; 2 Basic; 8/9 DK/Ref	Binary; DK/Ref missing	64,231	Sensitivity
Economy	`economy`	Economy of interview	75 economies	Fixed effects; clusters	75	Adjustment
Weight	`wgt`	Survey weight	Base × post-stratification	Rescaled to sum to 1 per economy	64,509	Weighting

Note: Valid observations are counts in the analytical sample of 64,509 mobile-phone owners in 75 economies. DK = don't know; ref. = reference category in comparisons and models. The survey weight is rescaled within each economy as described in Section 3.

The socioeconomic variables were used in their harmonized form. Gender is recorded as female or male. Exact age, which ranges from 15 to 100 in the analytical sample, was grouped into six bands (15–24, 25–34, 35–44, 45–54, 55–64, and 65 and older). Education follows the dataset's three-level classification (primary or less, secondary, tertiary or more). Income is the respondent's household-income quintile within their own economy. It therefore measures relative position within a national distribution, and the richest quintile in one economy cannot be equated with the richest quintile in another in absolute terms. Workforce participation distinguishes respondents in the workforce from those outside it; the release does not separate employment from unemployment. Residence is coded rural or urban. Two connectivity variables were used only in a sensitivity analysis: internet use in the past three months, and ownership of a smartphone rather than a basic phone, with "don't know" and refused answers treated as missing. Item nonresponse was low: 261 respondents (0.4%) lacked education, 863 (1.3%) lacked an income quintile, 190 (0.3%) lacked residence, and none lacked gender, age, or workforce status. The released file does not contain interview-mode, primary sampling unit, or stratum identifiers.

Pooling 75 national samples requires a decision about how much each economy should count. The Findex weights sum to the number of respondents within each economy, so pooling them directly would give each economy influence roughly in proportion to its sample size. Weighting by adult population would instead let a few very large economies dominate the pooled estimate. Because the question concerns socioeconomic differences within the covered economies rather than the global headcount of exposed people, the primary analysis rescales the survey weight v_i of respondent i in economy c so that the weights sum to one within each economy:

$$w_i = \frac{v_i}{\sum_{j \in c} v_j}, \qquad i \in c. \tag{1}$$

Each economy thus contributes equally, and within each economy respondents keep their design-based relative weights. As a sensitivity analysis, a second weight scales each respondent's survey weight by the economy's adult population, so that pooled estimates represent phone owners in proportion to national population size. Preparation was carried out in a scripted pipeline that never modifies the downloaded file. The pipeline asserts the skip pattern and the code sets, checks that each economy's rescaled weights sum to one, and writes an exclusion log. An independent script reproduces the subgroup prevalences with a different estimator and confirms that subgroup counts and missing values sum to the analytical total. All 19 validation checks passed. The analysis used Python 3 with `pandas` 3.0, `statsmodels` 0.15, `scipy` 1.17, and `matplotlib` 3.10.

3.2 Analytical Methodology

Let $Y_i = 1$ if respondent i reported receiving a scam call or text and $Y_i = 0$ otherwise. The weighted prevalence in group g is

$$\hat{P}_g = \frac{\sum_{i \in g} w_i Y_i}{\sum_{i \in g} w_i}, \tag{2}$$

and differences between a group a and a reference group b are summarized both as an absolute gap in percentage points and as a prevalence ratio:

$$\Delta_{ab} = \hat{P}_a - \hat{P}_b, \qquad PR_{ab} = \frac{\hat{P}_a}{\hat{P}_b}. \tag{3}$$

The reference group for each dimension is men, ages 15–24, primary education or less, the poorest quintile, respondents outside the workforce, and rural residents. Variances were obtained by Taylor linearization of the ratio estimator in Equation (2), with influence functions summed within economies and a small-sample factor $G/(G-1)$, where G is the number of economies. Because the prevalences in a dimension are estimated jointly, their covariances were used to compute the standard errors of the gaps and, through the delta method on the log scale, the confidence intervals of the prevalence ratios. Clustering by economy is conservative. It treats economies as the independent units and absorbs both sampling error and the substantial variation in prevalence between economies. Primary sampling units and strata are not released, so within-economy design effects from clustering could not be represented separately.

Adjusted patterns were estimated with a weighted logistic model that includes all six dimensions and a full set of economy fixed effects:

$$\Pr(Y_{ic} = 1) = \Lambda\left(\alpha_c + \boldsymbol{\beta}_1'\mathbf{Gender}_{ic} + \boldsymbol{\beta}_2'\mathbf{Age}_{ic} + \boldsymbol{\beta}_3'\mathbf{Educ}_{ic} + \boldsymbol{\beta}_4'\mathbf{Inc}_{ic} + \boldsymbol{\beta}_5'\mathbf{Work}_{ic} + \boldsymbol{\beta}_6'\mathbf{Res}_{ic}\right), \tag{4}$$

where $\Lambda(\cdot)$ is the logistic function, α_c is a fixed effect for economy c, and each bold term is a set of indicator variables for the non-reference categories. The fixed effects absorb every economy-level difference in prevalence, including differences in telecommunications regulation, scam activity, and question interpretation. The adjusted comparisons are therefore within economies and are not affected by where each group happens to be concentrated. Country identifiers are used only for this adjustment and for clustering; no economy is ranked or compared. The model was estimated by weighted maximum likelihood with the equal-economy weights, and its covariance matrix was computed with a sandwich estimator clustered by economy.

Coefficients were converted into two quantities that are easier to interpret than odds ratios. The adjusted predicted prevalence for category k of a dimension is the weighted average of the model's predicted probabilities when every respondent is assigned category k and all other characteristics keep their observed values. The average marginal effect (AME) of category k is the difference between its adjusted predicted prevalence and that of the reference category, expressed in percentage points. Here it is read as an adjusted difference, not as a causal effect. Standard errors for both quantities were obtained by the delta method from the clustered covariance matrix.

Four intersections were specified before the analysis and no others were examined: age by gender, education by income quintile, workforce participation by gender, and income quintile by residence. For each, weighted prevalence was estimated in every cell, together with the within-stratum gap and its confidence interval. Robustness was assessed by re-estimating the adjusted model (i) without weights, (ii) with adult-population weights, (iii) with internet use and smartphone ownership added as controls, (iv) with a coarser age coding (15–29, 30–49, 50 and older), and (v) after excluding the economies in the top decile of combined item nonresponse on the outcome and socioeconomic variables. Descriptive estimates were also compared with and without weights and between available-case and complete-case samples. Interview-mode adjustment was not needed, because the module was administered face to face in all 75 economies [1]. With more than 60,000 respondents, small differences can reach conventional significance. The interpretation therefore rests on the size of the gaps and their confidence intervals rather than on p-values.

4 Results

4.1 Sample Profile and Overall Exposure

The analytical sample includes 64,509 mobile-phone owners in 75 economies. Thirty-four of these economies are in Sub-Saharan Africa, 16 in Latin America and the Caribbean, 8 in East Asia and the Pacific, 7 in the Middle East and North Africa, 5 in South Asia, 4 in Europe and Central Asia, and 1 is classified as high income. Table 2 describes the sample. With equal economy weighting, the mean age was 36.5 years and 27.2% of respondents were aged 15–24. Just under half (49.4%) were women, 44.6% had primary education or less and 8.8% tertiary education, 63.1% were in the workforce, and 60.2% lived in rural areas. Phone owners were concentrated in the upper part of each economy's income distribution: the richest quintile made up 22.3% of the weighted sample and the poorest 17.3%. Two thirds of respondents had used the internet in the past three months (66.9%), and a similar share owned a smartphone (66.0%). Weighted and unweighted compositions were close for most characteristics. The largest difference was in education, where the unweighted sample contained more respondents with secondary schooling.

Table 2: Weighted characteristics of the analytical sample

Characteristic	n (unweighted)	Weighted %	Unweighted %
Gender			
Men	30,279	50.6	46.9
Women	34,230	49.4	53.1
Age group			
15–24	14,777	27.2	22.9
25–34	16,833	25.2	26.1
35–44	13,178	19.3	20.4
45–54	8,666	13.3	13.4
55–64	6,230	8.7	9.7
65+	4,825	6.4	7.5
Education			
Primary or less	21,902	44.6	34.1
Secondary	35,187	46.6	54.8
Tertiary	7,159	8.8	11.1
Missing	261	–	0.4
Income quintile			
Q1 (poorest)	9,542	17.3	15.0
Q2	10,523	19.0	16.5
Q3	12,045	20.3	18.9
Q4	13,670	21.0	21.5
Q5 (richest)	17,866	22.3	28.1
Missing	863	–	1.3
Workforce status			
Out of workforce	23,767	36.9	36.8
In workforce	40,742	63.1	63.2
Residence			
Rural	37,876	60.2	58.9
Urban	26,443	39.8	41.1
Missing	190	–	0.3

Note: N = 64,509 mobile-phone owners in 75 economies. Weighted percentages use survey weights rescaled to sum to one within each economy and exclude missing values. Unweighted percentages include missing values in the denominator.

Overall, 21.9% of phone owners (95% CI 18.7–25.1) reported receiving a scam call or text. The unweighted estimate was 22.3% (18.8–25.7), and the estimate for the complete-case sample used in the models was 22.1% (18.8–25.3). Weighting by adult population gave a lower pooled figure of 18.7% (12.6–24.9) with a wider interval, because a small number of populous economies then account for most of the weight. Prevalence differed widely between economies, from 2.5% in the lowest to 70.9% in the highest, with an interquartile range of 11.0% to 29.6%. This dispersion is the reason the uncertainty estimates are clustered by economy and the adjusted models include economy fixed effects.

4.2 Socioeconomic Distribution of Scam Exposure

Table 3 and Figure 1 show that exposure increased with socioeconomic position on most dimensions. The widest absolute gaps were for workforce participation and education. Respondents in the workforce reported exposure at 25.0%, compared with 16.5% of those outside it, a gap of 8.5 percentage points (95% CI 6.3–10.7) and a prevalence ratio of 1.52. Exposure rose steadily across education levels, from 19.4% among those with primary education or less to 23.3% with secondary and 27.4% with tertiary education. The tertiary-versus-primary gap was 8.0 points (3.8–12.2), a ratio of 1.41. The income gradient was also monotonic, from 18.9% in the poorest quintile to 25.2% in the richest. The top-to-bottom gap of 6.4 points (4.7–8.0) had a relatively narrow interval, because it is estimated within the same economies. Urban residents reported 3.1 points more exposure than rural residents (23.7% versus 20.6%).

Table 3: Weighted scam-exposure prevalence, confidence intervals, percentage-point gaps, and prevalence ratios by socioeconomic group

Group	*n*	% exposed	95% CI	Gap, pp (95% CI)	PR (95% CI)
Gender					
Men (ref.)	30,279	23.3	20.0–26.6	–	–
Women	34,230	20.5	17.3–23.6	−2.8 (−3.9, −1.8)	0.88 (0.83–0.92)
Age group					
15–24 (ref.)	14,777	21.6	18.3–25.0	–	–
25–34	16,833	23.6	20.0–27.1	+2.0 (0.8, 3.1)	1.09 (1.04–1.15)
35–44	13,178	23.6	20.2–27.0	+2.0 (0.3, 3.7)	1.09 (1.01–1.18)
45–54	8,666	22.0	18.4–25.6	+0.4 (−1.7, 2.5)	1.02 (0.93–1.12)
55–64	6,230	18.4	15.3–21.5	−3.2 (−5.7, −0.7)	0.85 (0.75–0.96)
65+	4,825	15.6	12.6–18.6	−6.0 (−8.7, −3.3)	0.72 (0.62–0.84)
Education					
Primary or less (ref.)	21,902	19.4	15.6–23.1	–	–
Secondary	35,187	23.3	19.8–26.7	+3.9 (1.1, 6.7)	1.20 (1.04–1.38)
Tertiary	7,159	27.4	23.7–31.1	+8.0 (3.8, 12.2)	1.41 (1.17–1.71)
Income quintile					
Q1 (poorest) (ref.)	9,542	18.9	15.8–22.0	–	–
Q2	10,523	21.2	17.9–24.4	+2.3 (1.1, 3.5)	1.12 (1.06–1.19)
Q3	12,045	21.7	18.3–25.0	+2.8 (1.2, 4.3)	1.15 (1.06–1.24)
Q4	13,670	22.6	19.2–25.9	+3.7 (2.2, 5.1)	1.20 (1.11–1.28)
Q5 (richest)	17,866	25.2	21.7–28.8	+6.4 (4.7, 8.0)	1.34 (1.24–1.44)
Workforce status					
Out of workforce (ref.)	23,767	16.5	13.5–19.5	–	–
In workforce	40,742	25.0	21.6–28.5	+8.5 (6.3, 10.7)	1.52 (1.35–1.70)
Residence					
Rural (ref.)	37,876	20.6	17.1–24.2	–	–
Urban	26,443	23.7	20.7–26.8	+3.1 (0.9, 5.2)	1.15 (1.04–1.28)

Note: *n* is the unweighted number of respondents; percentages are weighted with equal-economy weights. Gaps (percentage points, pp) and prevalence ratios (PR) compare each group with the reference category (ref.) of the same dimension. Confidence intervals are clustered by economy (75 clusters). Available-case estimates; missing values: education 261, income 863, residence 190.

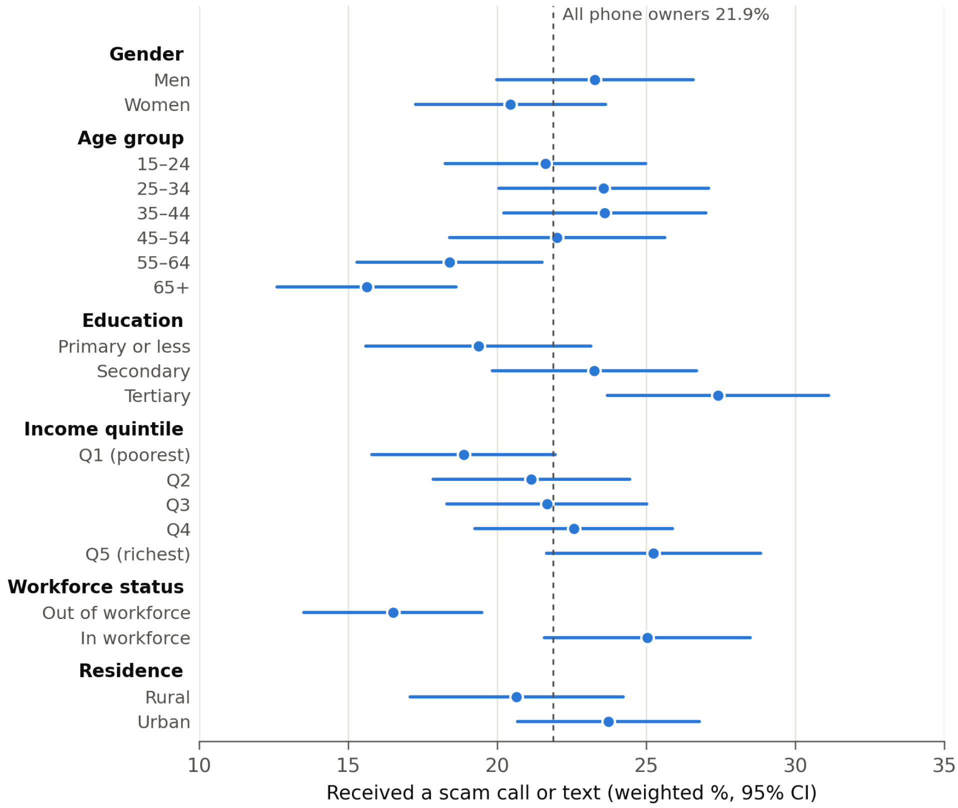

Figure 1: Weighted prevalence of receiving a scam call or text by socioeconomic group, with 95% confidence intervals clustered by economy. The dashed line marks the prevalence among all 64,509 phone owners. Wide intervals reflect between-economy variation; gaps between groups within a dimension are estimated more precisely (Table 3).

Gender and age showed smaller and differently shaped differences. Women reported exposure at 20.5%, against 23.3% for men, a gap of −2.8 points (−3.9 to −1.8) and a prevalence ratio of 0.88. Exposure by age followed an inverted U. It rose from 21.6% at ages 15–24 to about 23.6% at 25–34 and 35–44, was similar to the youngest group at 45–54, and then fell to 18.4% at 55–64 and 15.6% at 65 and older. The oldest group reported 6.0 points (−8.7 to −3.3) less exposure than the youngest. Figure 2 shows that the same shape held for both men and women.

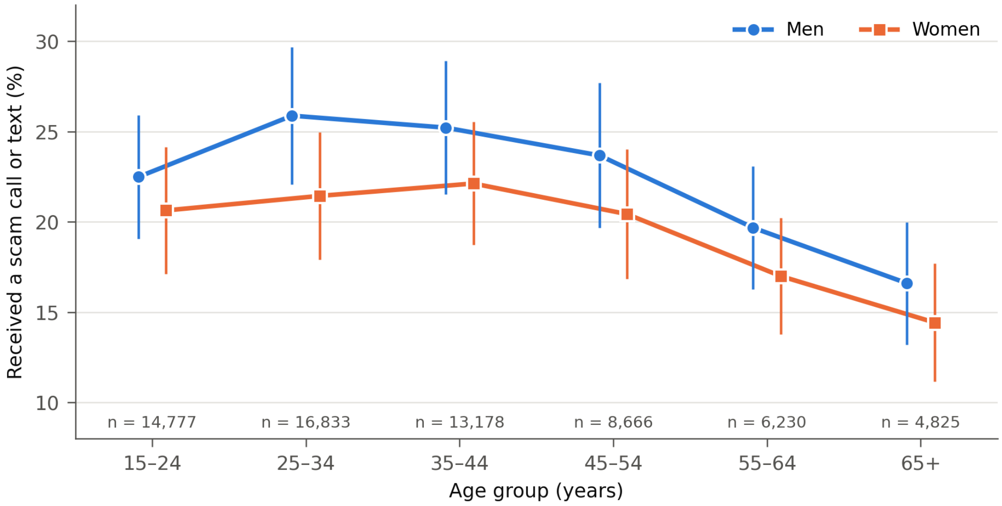

Figure 2: Weighted prevalence of receiving a scam call or text by age group and gender, with 95% confidence intervals clustered by economy. Counts show unweighted respondents per age group.

4.3 Intersecting and Adjusted Inequalities

The age-by-gender breakdown in Figure 2 shows that women reported lower exposure than men in every age group. The gap was widest at ages 25–34 (−4.4 points, −6.4 to −2.5), where men's exposure peaked at 25.9%, and narrowest among the youngest (15–24, −1.9 points) and oldest groups (65 and older, −2.2 points, with an interval that included zero). The workforce-by-gender comparison shows that most of the overall gender gap lies in the difference between participants and non-participants. Among respondents in the workforce, women's exposure was 24.5% and men's 25.4%, a difference of −1.0 point (−2.5 to 0.6). Among those outside the workforce, the figures were 15.9% and 17.6% (−1.7 points, −3.7 to 0.4). The difference between workforce participants and non-participants, by contrast, was about 8 to 9 points for both men and women.

Figure 3 shows that education and income are associated with exposure in the same direction and largely additively. Exposure was lowest (17.3%) among respondents with primary education or less in the poorest quintile and highest (28.4%) among tertiary-educated respondents in the richest quintile. Within the primary and secondary groups, exposure rose with income, by 5.8 points (3.0–8.6) and 4.7 points (2.2–7.3) from the poorest to the richest quintile. Among tertiary-educated respondents, the rise from 23.8% to 28.4% was of similar size but not precisely estimated, because only 458 tertiary graduates were in the poorest quintile. Education appeared to separate groups more sharply than income. Tertiary-educated respondents in the poorest quintile reported slightly more exposure (23.8%) than respondents with primary education or less in the richest quintile (23.1%). The income-by-residence comparison showed that urban respondents reported more exposure than rural respondents in the middle quintiles (by 3.0 to 4.2 points in the second to fourth quintiles). There was no urban–rural difference in the poorest quintile (−0.7 points) or the richest (+1.0 point).

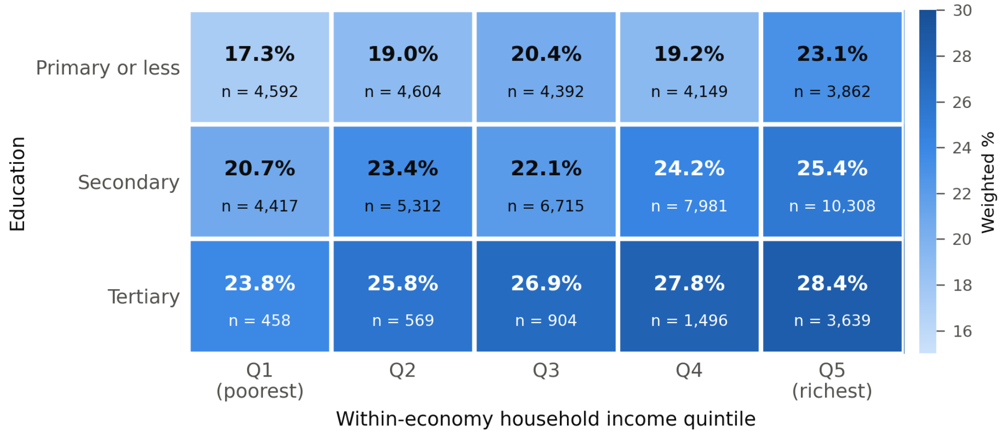

Figure 3: Weighted prevalence of receiving a scam call or text by education and within-economy household income quintile. Each cell shows the weighted percentage and the unweighted number of respondents.

Table 4 reports adjusted differences from the fixed-effects model, and Figure 4 shows the corresponding adjusted predicted prevalence. The education gradient was essentially unchanged by adjustment. Tertiary education was associated with 8.0 points (6.2 to 9.8) more exposure than primary education or less, and secondary education with 4.1 points more. The workforce difference narrowed from 8.5 to 4.6 points (3.6 to 5.7) but remained the second largest. The income gradient narrowed much more. Once education, workforce status, and the other characteristics were held constant, the richest quintile differed from the poorest by 2.6 points (1.1 to 4.0), and the three middle quintiles were within 1.6 points of the poorest. The adjusted gender gap was −2.0 points (−3.1 to −1.0), and urban residence was associated with 1.9 more points. For age, adjustment moved the pattern slightly toward the middle years. Adjusted exposure peaked at 35–44 (23.7%) and was 3.2 points (−5.4 to −0.9) lower at 65 and older than at 15–24. The adjusted prevalence ranged from 17.9% among those aged 65 and older to 27.5% among tertiary-educated respondents.

Table 4: Adjusted average marginal effects on the probability of receiving a scam call or text (percentage points)

Category	AME (pp)	95% CI	*p*
Gender (ref. men)			
Women	−2.0	−3.1 to −1.0	<0.001
Age group (ref. 15–24)			
25–34	+1.6	0.7 to 2.6	0.001
35–44	+2.7	1.1 to 4.2	<0.001
45–54	+2.0	0.4 to 3.7	0.015
55–64	−0.4	−2.3 to 1.5	0.675
65+	−3.2	−5.4 to −0.9	0.006
Education (ref. primary or less)			
Secondary	+4.1	2.7 to 5.5	<0.001
Tertiary	+8.0	6.2 to 9.8	<0.001
Income quintile (ref. Q1, poorest)			
Q2	+1.6	0.4 to 2.8	0.011
Q3	+1.4	−0.1 to 2.9	0.071
Q4	+1.5	0.2 to 2.7	0.023
Q5 (richest)	+2.6	1.1 to 4.0	<0.001
Workforce (ref. out of workforce)			
In workforce	+4.6	3.6 to 5.7	<0.001
Residence (ref. rural)			
Urban	+1.9	0.9 to 3.0	<0.001

Note: Weighted logistic model with economy fixed effects and all six dimensions entered jointly; equal-economy weights; N = 63,209 respondents with complete data in 74 economies. AME = average marginal effect, the difference in adjusted predicted prevalence between the category and the reference (ref.), read as an adjusted difference rather than a causal effect. Confidence intervals use a sandwich covariance clustered by economy and the delta method.

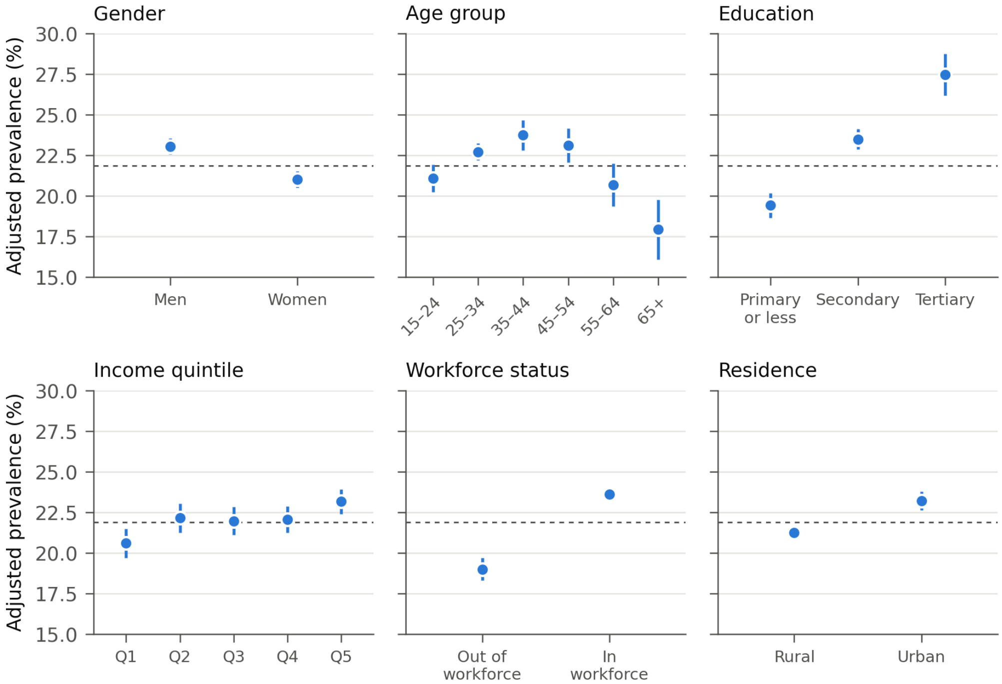

Figure 4: Adjusted predicted prevalence of receiving a scam call or text by socioeconomic group, from a weighted logistic model with economy fixed effects (N = 63,209; 74 economies). Bars are 95% confidence intervals clustered by economy; the dashed line marks the unadjusted overall prevalence (21.9%).

Table 5 summarizes the sensitivity analyses for the key contrasts. The education and workforce differences were the most robust. The tertiary difference stayed between 5.9 and 8.6 points and the workforce difference between 3.9 and 4.9 points in every specification. The gender gap kept its sign and remained significant throughout, ranging from −1.6 to −3.4 points. Three results were more sensitive. First, adding internet use and smartphone ownership reduced the tertiary difference to 5.9 points and the difference for ages 65 and older to −0.7 points, with an interval including zero. Much of the lower exposure of older phone owners therefore coincides with their lower use of smartphones and the internet. Second, with adult-population weights, the richest-quintile difference (+1.5) and the oldest-age difference (−1.6) were no longer distinguishable from zero. The same weighting also changed the descriptive gaps: the tertiary-versus-primary gap widened to 12.6 points and the oldest-versus-youngest gap narrowed to −1.7 points. This indicates that the income and age patterns are less uniform in the most populous economies. Third, with coarser age bands, respondents aged 50 and older did not differ clearly from those aged 15–29 (−1.0 point), because the broader band combines the peak and the decline. Excluding the eight economies with the highest item nonresponse (above 1.9% of phone owners) left all estimates practically unchanged. Available-case and complete-case descriptive gaps differed by at most 0.2 points, and unweighted gaps were within 0.4 points of the weighted ones.

5 Discussion

Across 75 economies, about one in five mobile-phone owners reported receiving a scam call or text, and exposure was not evenly spread. The most consistent differences were associated with education and workforce participation. Tertiary-educated respondents reported about 8 points more exposure than those with primary education or less, a gap that was unaffected by adjustment. Workforce participants reported about 5 points more than non-participants once other characteristics were held constant. Income showed a monotonic but largely compositional gradient. Exposure was lowest at the youngest and oldest ages, and women reported somewhat less exposure than men, mainly because they are less often in the workforce. These results do not support the idea that scam attempts fall mainly on the poorest, least

Table 5: Sensitivity of adjusted differences (percentage points, 95% CI) to alternative specifications

Specification	N	Econ.	Women	Age 65+	Tertiary	Q5	In workforce	Urban
Main specification	63,209	74	−2.0 [−3.1, −1.0]	−3.2 [−5.4, −0.9]	8.0 [6.2, 9.8]	2.6 [1.1, 4.0]	4.6 [3.6, 5.7]	1.9 [0.9, 3.0]
Unweighted	63,209	74	−1.6 [−2.5, −0.7]	−2.3 [−4.1, −0.6]	8.3 [6.8, 9.8]	1.7 [0.4, 3.0]	4.6 [3.8, 5.4]	1.6 [0.7, 2.5]
Adult-population weights	63,209	74	−3.4 [−6.0, −0.8]	−1.6 [−4.9, 1.7]	8.6 [6.4, 10.8]	1.5 [−1.4, 4.4]	3.9 [1.7, 6.1]	1.7 [−0.1, 3.4]
+ Internet, smartphone	62,948	74	−1.7 [−2.7, −0.7]	−0.7 [−3.1, 1.7]	5.9 [4.1, 7.6]	1.6 [0.1, 3.1]	4.5 [3.5, 5.5]	1.4 [0.3, 2.4]
Alternative age bands[a]	63,209	74	−1.9 [−2.9, −0.9]	−1.0 [−2.5, 0.5]	8.3 [6.4, 10.1]	2.6 [1.2, 4.0]	4.9 [3.9, 6.0]	1.9 [0.9, 2.9]
High nonresponse excluded[b]	57,261	67	−2.1 [−3.2, −1.0]	−3.2 [−5.4, −1.0]	8.1 [6.1, 10.1]	2.3 [0.7, 3.8]	4.5 [3.4, 5.7]	2.0 [1.0, 3.1]

Note: Average marginal effects from weighted logistic models with economy fixed effects, relative to the reference categories in Table 4. Econ. = number of economies. [a]Age bands 15–29 (ref.), 30–49, and 50 and older; the Age 65+ column reports the 50+ contrast. [b]Excludes the eight economies in the top decile of combined item nonresponse on the outcome and socioeconomic variables.

educated, or oldest phone owners. Within economies, the groups that received more attempts were those with more schooling, paid or market work, higher relative income, and urban residence. These are the groups usually considered least vulnerable.

Several explanations are consistent with this pattern, and the data cannot separate them. Routine activity accounts suggest that people who make more calls, send more messages, transact more, and appear in more customer, employer, and service databases present more opportunities to offenders [18, 19]. The narrowing of the education and age differences when internet use and smartphone ownership were added fits this interpretation. Economic visibility may also matter. Fraudsters who impersonate banks, mobile-money providers, or employers may be more likely to target numbers associated with account holders and wage earners, and studies of older adults in China and the United States report similar links between exposure and financial engagement or assets [15, 27, 28, 13]. A third explanation is recognition. Better-educated respondents may identify a message as a scam more readily and so report it, while others may not label the same contact as fraud [20, 23]. Differences in recognition would inflate the education gradient, but they cannot readily explain the workforce gap, which persisted after adjustment for education. The results agree with the Australian age profile of exposure [2] and with studies that separate targeting from victimization [10, 12, 13]. They also fit the finding that exposure and loss are unrelated across countries [4]. They contrast with research that concentrates on losses, where lower income and lower digital literacy are more often associated with harm [3, 29]. The contrast does not imply a contradiction, because a group can be less frequently targeted yet more heavily harmed when an attempt succeeds.

The practical implications follow from treating exposure and harm as separate problems. Because attempts are concentrated among the economically active, awareness efforts that address only older or poorer users will miss the people who receive the most attempts. Mobile-network operators, banks, and mobile-money providers can reach these users through the channels they already use: payroll and account notifications, transaction interfaces, and network-level filtering and warnings for suspicious numbers and messages. Regulators can use exposure measures of this kind alongside complaint data, which undercount attempts that do not lead to losses [7, 9]. At the same time, the lower reported exposure of older, rural, and less educated owners should not be read as lower risk, because these groups may recognize fewer scams and may have fewer resources to absorb a loss [29, 20]. Messages aimed at them should focus on recognition and on safe ways to verify and report suspicious contacts. None of these findings places responsibility on recipients. Exposure is something that is done to people, and the gradients describe where offenders make contact, not who is careless.

The findings have several limitations. The outcome is self-reported and depends on recognition and recall, and the item does not distinguish calls from texts, the number of attempts, or the reference period in detail. It covers only phone owners in the economies where the module was fielded, so it says nothing about adults without a phone, and the sample is mostly from low- and middle-income economies. The design is cross-sectional, and the associations reported here are not causal. The income measure is relative to each economy and cannot be compared in absolute terms across economies. Clustered intervals cannot fully reflect within-economy design effects, because primary sampling units and strata are not released. Some estimates, especially the income and age gradients, depend on whether economies are weighted equally or by population. Finally, the module was administered face to face in all 75 economies, so the results are not affected by interview mode but do not describe the telephone-surveyed high-income economies. The findings apply to phone owners in the covered economies and not to every adult or economy worldwide.

6 Conclusion

Among mobile-phone owners in the 75 Global Findex 2025 economies with a digital-connectivity module, reported exposure to scam calls and texts was higher among more educated, economically active, better-off, urban, and male respondents, and lower at both ends of the age range. After adjustment within economies, education and workforce participation remained the clearest differences. The study shows that, when exposure is measured separately from loss with a common question across many economies, attempted mobile fraud follows economic and communicative activity more than conventional markers of disadvantage. For consumer protection, the main implication is that prevention should be directed at the heavily targeted economically active majority through the operators and financial institutions that serve them, while support for less-exposed but potentially more vulnerable groups continues to focus on recognition and recovery. These patterns are based on self-reported, cross-sectional data from phone owners, so they describe where scam attempts are reported rather than why they occur.

References

[1] L. Klapper, D. Singer, L. Starita, and A. Norris, *The Global Findex Database 2025: Connectivity and Financial Inclusion in the Digital Economy*. Washington, DC: World Bank, 2025. [Online]. Available: https://doi.org/10.1596/978-1-4648-2204-9

[2] Australian Bureau of Statistics, "Personal fraud, 2021–22 financial year," Australian Bureau of Statistics, Canberra, Feb. 2023. [Online]. Available: https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/2021-22

[3] J. Gottfried, E. Park, and M. Anderson, "Online scams and attacks in America today," Pew Research Center, Washington, DC, Tech. Rep., Jul. 2025. [Online]. Available: https://www.pewresearch.org/internet/2025/07/31/online-scams-and-attacks-in-america-today/

[4] M. Houtti, A. Roy, V. N. R. Gangula, and A. Walker, "A survey of scam exposure, victimization, types, vectors, and reporting in 12 countries," *Journal of Online Trust and Safety*, vol. 2, no. 4, 2024. [Online]. Available: https://doi.org/10.54501/jots.v2i4.204

[5] M. W. Buku and R. Mazer, "Fraud in mobile financial services: Protecting consumers, providers, and the system," Consultative Group to Assist the Poor, Washington, DC, CGAP Brief, Apr. 2017. [Online]. Available: https://www.cgap.org/research/publication/fraud-in-mobile-financial-services

[6] S. Garz, X. Giné, D. Karlan, R. Mazer, C. Sanford, and J. Zinman, "Consumer protection for financial inclusion in low- and middle-income countries: Bridging regulator and academic perspectives," *Annual Review of Financial Economics*, vol. 13, no. 1, pp. 219–246, 2021. [Online]. Available: https://doi.org/10.1146/annurev-financial-071020-012008

[7] S. Kemp, F. Miró-Llinares, and A. Moneva, "The dark figure and the cyber fraud rise in Europe: Evidence from Spain," *European Journal on Criminal Policy and Research*, vol. 26, no. 3, pp. 293–312, 2020. [Online]. Available: https://doi.org/10.1007/s10610-020-09439-2

[8] S. van de Weijer, R. Leukfeldt, and S. Van der Zee, "Reporting cybercrime victimization: Determinants, motives, and previous experiences," *Policing: An International Journal*, vol. 43, no. 1, pp. 17–34, 2020. [Online]. Available: https://doi.org/10.1108/PIJPSM-07-2019-0122

[9] Federal Trade Commission, "New FTC data show a big jump in reported losses to fraud to $12.5 billion in 2024," Press release, Washington, DC, Mar. 2025. [Online]. Available: https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-125-billion-2024

[10] K. Holtfreter, M. D. Reisig, and T. C. Pratt, "Low self-control, routine activities, and fraud victimization," *Criminology*, vol. 46, no. 1, pp. 189–220, 2008. [Online]. Available: https://doi.org/10.1111/j.1745-9125.2008.00101.x

[11] M. DeLiema, Y. Li, and G. Mottola, "Correlates of responding to and becoming victimized by fraud: Examining risk factors by scam type," *International Journal of Consumer Studies*, vol. 47, no. 3, pp. 1042–1059, 2023. [Online]. Available: https://doi.org/10.1111/ijcs.12886

[12] K. Lin, Y. Wu, I. Y. Sun, and J. Qu, "Telecommunication and cyber fraud victimization among Chinese college students: An application of routine activity theory," *Criminology & Criminal Justice*, vol. 25, no. 3, pp. 717–735, 2025. [Online]. Available: https://doi.org/10.1177/17488958221146144

[13] T. Hu, F. C. D. Andrade, and Y.-C. Chen, "Multilevel risk factors for financial fraud in later life: Evidence from China," *Innovation in Aging*, vol. 10, no. 4, 2026. [Online]. Available: https://doi.org/10.1093/geroni/igag004

[14] D. Burnes, J. Henderson, Charles R., C. Sheppard, R. Zhao, K. Pillemer, and M. S. Lachs, "Prevalence of financial fraud and scams among older adults in the United States: A systematic review and meta-analysis," *American Journal of Public Health*, vol. 107, no. 8, pp. e13–e21, 2017. [Online]. Available: https://doi.org/10.2105/AJPH.2017.303821

[15] S.-J. Yu, C.-T. Kuo, and Y.-C. Tseng, "Association of financial literacy and risk preference with fraud exposure and victimization among middle-aged and older adults in China," *Journal of Applied Gerontology*, vol. 42, no. 1, pp. 89–98, 2023. [Online]. Available: https://doi.org/10.1177/07334648221121775

[16] K. Parti, "What is a capable guardian to older fraud victims? comparison of younger and older victims' characteristics of online fraud utilizing routine activity theory," *Frontiers in Psychology*, vol. 14, 2023. [Online]. Available: https://doi.org/10.3389/fpsyg.2023.1118741

[17] Development Research Group, Finance and Private Sector Development Unit, World Bank, "The Global Findex Database 2025: Connectivity and financial inclusion in the digital economy," 2025, reference ID: WLD_2024_FINDEX_v02_M. [Online]. Available: https://microdata.worldbank.org/catalog/7860

[18] L. E. Cohen and M. Felson, "Social change and crime rate trends: A routine activity approach," *American Sociological Review*, vol. 44, no. 4, pp. 588–608, 1979. [Online]. Available: https://doi.org/10.2307/2094589

[19] T. C. Pratt, K. Holtfreter, and M. D. Reisig, "Routine online activity and internet fraud targeting: Extending the generality of routine activity theory," *Journal of Research in Crime and Delinquency*, vol. 47, no. 3, pp. 267–296, 2010. [Online]. Available: https://doi.org/10.1177/0022427810365903

[20] E. Kubilay, E. Raiber, L. Spantig, J. Cahlíková, and L. Kaaria, "Can you spot a scam? measuring and improving scam identification ability," *Journal of Development Economics*, vol. 165, 2023. [Online]. Available: https://doi.org/10.1016/j.jdeveco.2023.103147

[21] S. Tabassum, C. Faklaris, and H. R. Lipford, “What drives SMiShing susceptibility? a U.S. interview study of how and why mobile phone users judge text messages to be real or fake,” in *Proceedings of the Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)*. Philadelphia, PA: USENIX Association, Aug. 2024, pp. 393–411. [Online]. Available: https://www.usenix.org/conference/soups2024/presentation/tabassum-sarah

[22] M. E. Edwards and J. D. Still, “Cyber hygiene of SMiShing: What they know and where they look,” *Computer Standards & Interfaces*, vol. 95, 2026. [Online]. Available: https://doi.org/10.1016/j.csi.2025.104048

[23] C. A. Maher, “Buyer beware, or buyer unaware? examining the correlates of consumer fraud victimization acknowledgment in the United States,” *Crime & Delinquency*, vol. 71, no. 6–7, pp. 2493–2517, 2025. [Online]. Available: https://doi.org/10.1177/00111287231197422

[24] M. T. Whitty, “Predicting susceptibility to cyber-fraud victimhood,” *Journal of Financial Crime*, vol. 26, no. 1, pp. 277–292, 2019. [Online]. Available: https://doi.org/10.1108/JFC-10-2017-0095

[25] Y. Kadoya, M. S. R. Khan, J. Narumoto, and S. Watanabe, “Who is next? a study on victims of financial fraud in Japan,” *Frontiers in Psychology*, vol. 12, 2021. [Online]. Available: https://doi.org/10.3389/fpsyg.2021.649565

[26] GSMA, “The mobile gender gap report 2025,” GSMA, London, Tech. Rep., May 2025. [Online]. Available: https://www.gsma.com/gender-gap-2025/

[27] X. Mao and Y. Liu, “Relationship between socioeconomic conditions and financial fraud victimization among older adults in China: Do financial literacy and financial attitudes matter?” *Research on Aging*, vol. 45, no. 7–8, pp. 503–516, 2023. [Online]. Available: https://doi.org/10.1177/01640275221132195

[28] M. DeLiema, M. Deevy, A. Lusardi, and O. S. Mitchell, “Financial fraud among older Americans: Evidence and implications,” *The Journals of Gerontology: Series B*, vol. 75, no. 4, pp. 861–868, 2020. [Online]. Available: https://doi.org/10.1093/geronb/gby151

[29] P. Li, Q. Li, and S. Du, “Does digital literacy help residents avoid becoming victims of frauds? empirical evidence based on a survey of residents in six provinces of east China,” *International Review of Economics & Finance*, vol. 91, pp. 364–377, 2024. [Online]. Available: https://doi.org/10.1016/j.iref.2024.01.056