Kubilay, Elif; Raiber, Eva; Spantig, Lisa; Cahlíková, Jana; Kaaria, Lucy

Research Report

Financial fraud in developing countries: Common scam detection tips do not help distinguish scam from non-scam messages

ECONtribute Policy Brief, No. 056

Provided in Cooperation with:
Reinhard Selten Institute (RSI), University of Bonn and University of Cologne

Suggested Citation: Kubilay, Elif; Raiber, Eva; Spantig, Lisa; Cahlíková, Jana; Kaaria, Lucy (2023) : Financial fraud in developing countries: Common scam detection tips do not help distinguish scam from non-scam messages, ECONtribute Policy Brief, No. 056, University of Bonn and University of Cologne, Reinhard Selten Institute (RSI), Bonn and Cologne

This Version is available at:
https://hdl.handle.net/10419/279765

ECONtribute
MARKETS & PUBLIC POLICY

VoxEU

ECONtribute
Policy Brief No. 056

Financial fraud in developing countries: Common scam detection tips do not help distinguish scam from non-scam messages

Elif Kubilay
Jana Cahlíková
Eva Raiber
Lucy Kaaria
Lisa Spantig

November 2023

www.econtribute.de

UNIVERSITÄT BONN
UNIVERSITÄT ZU KÖLN

Funding by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC 2126/1-390838866 is gratefully acknowledged.

Financial fraud in developing countries: Common scam detection tips do not help distinguish scam from non-scam messages

Elif Kubilay, Eva Raiber, Lisa Spantig, Jana Cahlíková, Lucy Kaaria

8 November 2023

The expansion of digital financial services raises serious consumer protection concerns, including fraud, especially in developing countries. This column reports findings from an online experiment in Kenya which suggest that conventional scam detection tips do not improve individuals' ability to distinguish between scams and genuine messages. Rather, they make people over-cautious – a result partly driven by official communication often including scam markers.

Lack of access to finance has long been identified as holding back the poor from making productive investments (Karlan and Morduch 2010, Claessens 2006). Mobile money and digital financial services are thus a source of optimism for policymakers and development economists (Suri et al. 2023). Digital financial services do not rely on infrastructure investment – in contrast to the traditional banking system – and can be rolled out together with access to phone and internet networks. Increasing phone and internet connectivity in developing countries and the development of user-friendly text or internet-based financial services have the potential to 'bank the unbanked'

The expansion of digital financial services increases access to financial services but also leads to consumer protection issues

Digital financial services have increased access to financial services in both developed and developing countries (e.g. Pazarbasioglu et al. 2020, Balyuk 2022). Yet, there are negative side effects: consumer protection issues are on the rise, and one major issue is fraud (Garz et al. 2021). The literature on fraud – estimating its effects and testing methods for fraud prevention – has long focused on developed countries. Fraud can be detrimental to consumers not only due to the direct money loss, but also by eroding trust in financial services (Guiso et al. 2008, Gurun et al. 2017, Johnson et al. 2019), by decreasing confidence in financial matters (Brenner et al. 2020), and by leading to mental health problems such as depression and stress (DeLiema et al. 2020, Financial Institution Regulatory Authority 2015).

These 'indirect' costs might be even higher in developing countries, where levels of trust are generally lower, as a high level of mistrust can result in people ignoring information received by phone messages. In contexts where text messages are one of the main channels of communication, this can have important implications for the functioning of markets, the provision of information, and public service delivery. For example, SMS-based communication has been used to reduce frictions in rural labour and agricultural markets (Fabregas et al. 2019). Messages have also been used to enhance individuals' knowledge and health behaviors (Holst et al. 2021, He et al. 2023), and to motivate bureaucrats (Dustan et al. 2023). In addition to ignoring information, the fear of being defrauded may also lead to people avoiding the usage of DFS (Koyama et al. 2021).

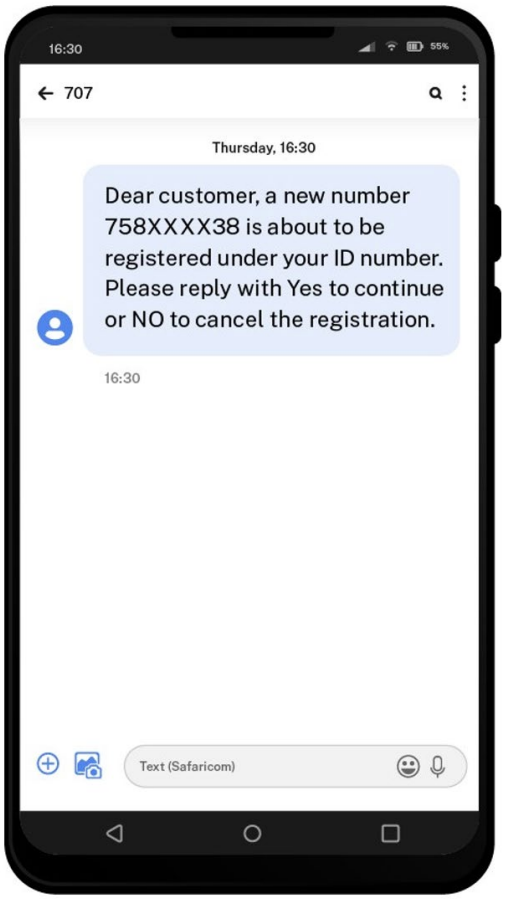
The indirect costs not only occur through direct victimisation but also through exposure to fraud attempts. Yet, people might not be able to recognise all types of fraud or differentiate genuine offers from scams (Chen et al. 2018). So even if only a few individuals are direct victims of fraud, the inability to detect fraud attempts and the lack of confidence in this ability may impede participation in the labour market and hence are relevant measures.

Measuring scam identification ability

We develop a novel measure for an individual's ability to identify a scam – i.e. the ability to distinguish scam messages from non-scam messages – and confidence in this ability (Kubilay et al. 2023). Our focus is Kenya, Africa's leader when it comes to digital infrastructure and mobile money use (Koyama et al. 2021). We first collect actual scams and official communication that circulate in Kenya from different sources: social media (Twitter, now X, and Facebook groups), focus groups and stakeholder interviews. In an online survey (N = 1000), we then show respondents 12 different messages based on the actual messages collected and ask them to indicate whether these messages are a scam or not (see Figure 1 for an example). The share of correctly identified messages measures the respondent's scam identification ability (SIA). We also ask participants to rate their confidence in their answers.

We find that women and less experienced users of digital financial services have lower SIA. Women are also on average less confident in their ability to distinguish scam from non-scam messages. This result corresponds to the findings of a financial literacy gender gap (Lusardi and Mitchell 2014). Surprisingly, having been a victim of a scam is not significantly associated either with SIA or with confidence.

Figure 1 Example vignette



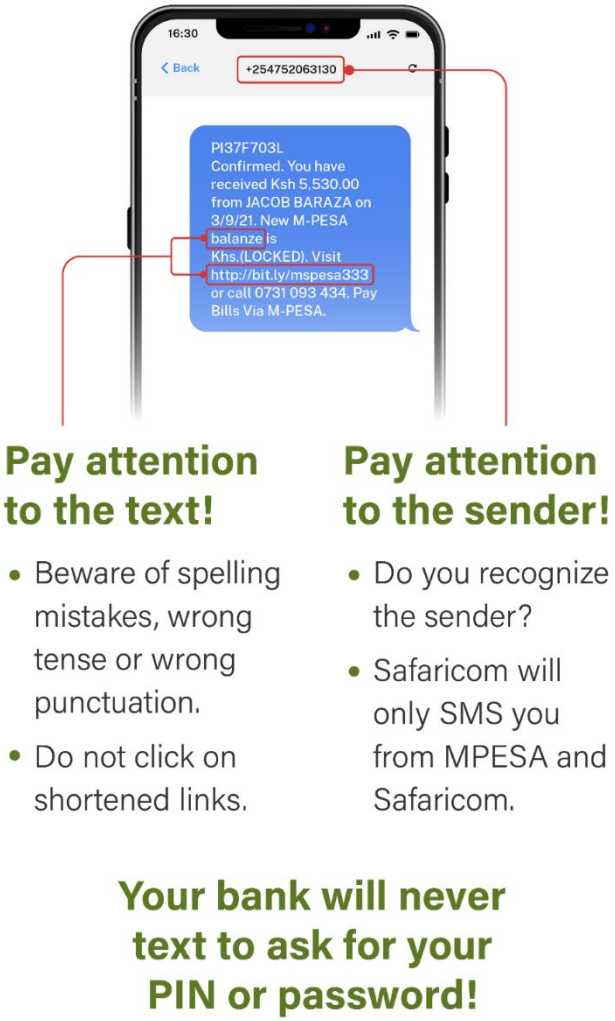
Note: Illustration of a vignette in the style in which messages were shown in the online experiment of Kubilay et al. (2023). Based on an actual official message collected in Kenya in 2021.

A light-tough scam education intervention does not increase scam identification ability

The existing recipe to preventing consumers from falling victim to scams is to pursue education and awareness campaigns. Do they improve people's ability to distinguish scams from genuine communication from banks and telecom providers?

We test the effectiveness of light-touch scam education in our online experiment. After classifying the first block of six vignettes, a randomly chosen half of the participants receive common tips on fraud prevention. These tips warn consumers about 'scam markers' (see Figure 2), which include typos and grammar mistakes, messages coming from an unknown sender, messages including a shortened link, and requests for private information (passwords, pin codes). The tips appear one by one before the overall graphic is displayed. Participants spent on average over one minute reviewing the tips.

Figure 2 Tips treatment



Note: Final graphic of the tips treatment used in the online experiment of Kubilay et al. (2023). The tips were based on commonly communicated tips in Kenya. The pieces of information were shown step by step and participants clicked through them at their own speed before seeing the overall graphic.

We then compare how well participants can distinguish scams from non-scam messages in the second block depending on whether they saw the tips or not. We find that the share of correctly identified messages does not change (see Figure 3, left-hand panel). This implies that our light-touch intervention did not improve respondents' scam identification ability. We find that this average null effect is driven by respondents being more likely to correctly identify scam messages (Figure 3,

middle panel) and less likely to correctly identify genuine messages (Figure 3, left-hand panel). Thus, on average, tips appear to make consumers more cautious - they are more likely to classify any message as a scam.

Figure 3 Effect of the tips treatment on the share of correctly identified messages (left-hand panel), the share of correctly identified scam messages (middle panel), and the share of correctly identified official messages (left-hand panel)

Note: Results of the online experiment of Kubilay et al. (2023) (n=1000). The share of correctly identified messages is based on the classification of six different messages, four of them being scam messages, and two of them genuine official messages.

Taking a closer look, we find a more nuanced picture based on whether a message contains a 'scam marker'. First, offering tips increases the share of correctly identified scams, regardless of whether a scam marker is present in the message. This suggests that tips do indeed make people more cautious. Second, if a genuine message includes a scam marker, it is more likely to be classified as scam. Therefore, official messages resembling scams (including a shortened link or a typo) – which are not unusual in the Kenyan context – seem to partly drive the average null effect.

The way forward: The need for enhanced fraud prevention strategies

While tips have been a popular low-cost measure employed by banks, telecom providers, and public authorities to prevent victimisation, their effectiveness is not only limited in Kenya. For investment fraud (Burke et al. 2022) and telemarketing scams (Scheibe et al. 2014) in developed countries, results are similarly discouraging, showing null or weak effects that are mostly short-lived. The seeming appeal of tips as an easy-to-scale and one-size-fits-all approach rather appears to be a weakness: not all tips apply to all scams, not all consumers can be reached via written tips, and the scammers themselves also receive these tips and take them into consideration when designing their strategies.

For providers, several lessons emerge. First, especially in the Kenyan context, communication should be free of any 'scam markers' that are highlighted by tips or are otherwise commonly associated with scam messages. Yet, this will be a short-lived solution given the dynamic nature of scams and establishing trusted ways of communication may be a more sustainable solution. In a low-tech environment, this could mean inserting an individual-specific word or number in all communication that identifies the provider as the actual communicator. Additional strategies can be based on more advanced technology, ranging from dedicated apps as unique communication channels (see Fu and Mishra 2022 on fraudulent FinTech apps) to biometric identification (if the phone allows).

However, in the end, and irrespective of the technological advances, the human factor will remain a weak spot (see https://retool.com/blog/mfa-isnt-mfa as an example of how a system that was believed to be secured by multifactor authentication was accessed via social engineering). Building digital but also financial capabilities cannot be ignored, even though it will require more than just a few tips.

References

Balyuk, T (2022), "FinTech lending and bank credit access for consumers", *Management Science.*

Brenner, L, T Meyll, O Stolper, A Walter (2020), "Consumer fraud victimization and financial well-being", *Journal of Economic Psychology* 76: 102243.

Burke, J, C Kieffer, G Mottola, F Perez-Arce (2022), "Can educational interventions reduce susceptibility to financial fraud?", *Journal of Economic Behaviour and Organisation* 198: 250–266.

Chen, Y, I YeckehZaare, AF Zhang (2018), "Real or bogus: predicting susceptibility to phishing with economic experiments", *PLOS ONE* 13(6): e0198213.

Claessens, S (2006), "Access to financial services: A review of the issues and public policy objectives", *The World Bank Research Observer* 21(2): 207-240.

DeLiema, M, M Deevy, A Lusardi, O S Mitchell (2020), "Financial fraud among older Americans: evidence and implications", *The Journals of Gerontolology* 75(4) : 861–868.

Dustan, A, J M Hernandez-Agramonte, S Maldonado (2023), "Motivating bureaucrats with behavioral insights when state capacity is weak: Evidence from large-scale field experiments in Peru", *Journal of Development Economics* 160: 102995.

Fabregas, R, M Kremer, F Schilbach (2019), "Realizing the potential of digital development: The case of agricultural advice", *Science* 366 (6471): eaay3038.

Financial Institution Regulatory Authority, Investor Education Foundation (2015), *The Non-Traditional Costs of Financial Fraud: Report of Survey Findings,* Technical report, Applied Research and Consulting.

Fu, J and M Mishra (2022), "Combatting fraudulent and predatory fintech apps with machine learning", IPA Policy Brief.

Garz, S, X Giné, D Karlan, R Mazer, C Sanford, J Zinman (2021), "Consumer protection for financial inclusion in low- and middle-income countries: Bridging regulator and academic perspectives", *Annual Review of Financial Economics* 13(1): 219–246.

Guiso, L, P Sapienza and L Zingales (2008), "Trusting the stock market", *Journal of Finance* 63(6): 2557–2600.

Gurun, U G, N Stoffman and S E Yonker (2017), "Trust busting: The effect of fraud on investor behavior", *Review of Financial Studies* 31(4): 1341–1376.

He, D, F Lu and J Yang (2023), "Impact of self- or social-regarding health messages: Experimental evidence based on antibiotics purchases", *Journal of Development Economics* 163: 103056.

Holst, C, G M N Isabwe, F Sukums, H Ngowi, F Kajuna, D Radovanović, W Mansour, E Mwakapejei, P Cardellichio, B Ngowi, J Noll and A S Winkler (2021), "Development of digital health messages for rural populations in Tanzania: Multi- and interdisciplinary approach", *JMIR MHealth UHealth* 9(9): e25558.

Johnson, E J, S Meier, O Toubia (2019), "What's the catch? suspicion of bank motives and Sluggish refinancing", *Review of Financial Studies* 32(2): 467–495.

Karlan, D and J Morduch (2010), “Access to finance”, in *Handbook of Development Economics* 5: 4703-4784.

Koyama, N, S Totapally, S Goyal, P Sonderegger, P Rao and J Gosselt (2021), *Kenya’s Digital Economy: A People’s Perspective,* Technical report.

Kubilay, E, E Raiber, L Spantig, J Cahlíková and L Kaaria (2023), "Can you spot a scam? Measuring and improving scam identification ability", *Journal of Development Economics* 165: 103147

Pazarbasioglu, C, A G Mora, M Uttamchandani, H Natarajan, E Feyenand M Saal (2020), “Digital financial services”, in *World Bank Symposium,* p. 54.

Scheibe, S, N Notthoff, J Menkin, L Ross, D Shadel, M Deevy and L L Carstensen (2014), “Forewarning reduces fraud susceptibility in vulnerable consumers”, *Basic Applications of Social Psycholology* 36(3): 272–279.

Tavneet S, J Aker, C Batista, M Callen, T Ghani, W Jack, L Klapper, E Riley, S Schaner and S Sukhtankar (2023), “Mobile Money”, VoDevLit.