Scam identification ability, confidence and the use of digital financial services
Pre-Analysis Plan

Jana Cahlíková[1], Lucy Kaaria[2], Elif Kubilay[3], Eva Raiber[4], and Lisa Spantig[3,5]

[1]Max Planck Institute for Tax Law and Public Finance
[2]University of Nairobi
[3]University of Essex
[4]Aix-Marseille University
[5]RWTH Aachen University

January 2022

1 Introduction

The recent expansion of digital financial products in developing countries led to issues related to consumer protection including fraud and scams. Therefore, the ability to identify scams and confidence in this ability is very important especially in environments where there is low trust in financial institutions. The objective of the study is to better understand how individuals in Kenya react to phone scams. We investigate this using a novel measure of scam identification ability (SIA), which will be implemented in an online survey. The initial findings of the survey will shed light into the correlates of scam identification ability and confidence in this ability. Moreover, we will test whether providing information on how to identify scams increases this ability and confidence to inform future interventions.

2 Experimental Design

In a cross-randomized, 2x2 design, we vary whether participants receive 1) information about how to identify scams and 2) incentives for correctly identifying scams. The control group receives neither information nor incentives.

The measure of SIA consists of 12 example messages (8 scams and 4 non-scams) based on common scam messages in Kenya. Survey participants will be asked for each message whether it is a scam and how confident they are in their assessment.

We will test the causal effect of information about how to spot scams on SIA and confidence in this ability, which will help us to gauge the potential effects of an educational/information campaign on the SIA and related confidence.

Specifically, the SIA measure consists of two independent parts (with 6 messages consisting of 4 scams and 2 non-scams), which will be presented to participants in a random order. The order of messages within the part is also randomized at the individual level. A randomly selected half will receive information on how to identify scam messages in between the two parts. The visuals for the information treatment are provided in the Appendix. An additional, cross-randomized treatment will assess whether paying incentives for correct answers enhances SIA and how incentives interact with information. Around 50% of the sample will be randomized to the incentives treatment in which participants earn 10 Kenyan Schillings for each correctly classified message.

3 Data

Data will be collected in an online survey (coded in Qualtrics) with a sample recruited by GeoPoll. We will aim for 1,000 respondents. We will implement gender, age and location quotas to diversify the respondents. In particular, half of the sample will consist of females. In terms of age, 32%, 27% and 33% of the sample will be in 18-24, 25-34 and above 35 age categories, respectively. Finally, to determine the location composition of the sample, we will rely on the official quotas from GeoPoll based on the population distribution across counties in Kenya. It should be noted that given the quota implementation in Qualtrics, we might receive slightly more respondents in some quotas, such that the overall sample size can be slightly larger than 1,000 individuals.

Treatments will be randomized at the individual level, such that we will have around 250 individuals per treatment arm.

4 Outcomes

In this section, we define and primary and secondary outcomes.

4.1 Primary Outcomes

4.1.1 Scam Identification Ability

We will measure SIA by looking at the answers of respondents to different messages that are either scams or non-scams. Specifically, the sum of correctly identified messages will be our main measure of scam identification ability. Additionally, we will construct two variables that to identify respondents who are i) "overly cautious" and ii) respondents who are "not cautious enough." Over caution is associated with a tendency to avoid non-scam messages, which consequently lowers trust and participation to digital financial market. Therefore, "overly cautious" variable will be constructed by looking at the number of non-scam messages identified as scam. We will also create a binary indicator which takes the value of 1 for respondents who are above median split and 0 otherwise. Similarly, we will construct a variable which captures being "not cautious enough" by looking at the number of scams that are identified as non-scam. Then, we will construct a dummy variable based on the median split. We expect this measure to identify individuals who are likely to fall for scams and suffer direct monetary costs.

4.1.2 Confidence in Scam Identification Ability

After respondents identify a message as scam or non-scam, they specify their level of confidence in their answer from a 5-point likert scale. We will use the overall average confidence across all messages. Additionally, we will construct a dummy variable "high confidence" , which is equals to 1 if the average confidence level is above the median and zero otherwise.

4.2 Secondary Outcomes

We will collect a number of secondary outcomes to explore the correlates of SIA and confidence.

- Trust in digital financial products: It is measured on a 4-point Likert scale.
- Response times to SIA questions: The average of time respondents take to complete the SIA measure.
- Scams correct: A binary indicator for having identified all scams correctly.
- Non-scams correct: A binary indicator for having identified all non-scams correctly.

5 Hypotheses

In this section, we explain the main hypotheses regarding our treatments are as follows.

1. Information increases SIA.
2. Incentives increase SIA.

5.1 Information Treatment

We will test the null hypothesis that there is no difference in scam identification ability between respondents who receive the information and respondents who do not receive the information treatment. We expect the information treatment to increase scam identification ability. Moreover, we expect information on how to identify scams to increase respondents' confidence in SIA.

We will also look at the effect of information on respondents who are identified as "overly cautious" and "not cautious enough." We predict information to make respondents to better able to spot scams in messages, therefore, decrease the share of respondents who are "not cautious enough." However, the effect of information on overly cautious individuals is ambiguous. By making respondents to differentiate scam from non-scam, information might decrease the share of "overly cautious." On the other hand, information might make respondents too sensitive about scams and consequently increase the share of "overly cautious."

Finally, we will estimate the effect of information on response times. The direction of the effect is ambiguous, if information helps respondents to pay attention to the right details, we would expect respondents to be quicker in differentiating scams from non-scams, which would ultimately decrease response times. However, it might also increase response times of respondents who were not taking their time to differentiate scams from non-scams in the absence of information.

5.2 Incentives Treatment

As we freshly developed a measure of SIA, it is important to understand how incentives affect the outcome of SIA. First, we predict that incentives will increase the number of correctly identified messages by making them exert more effort. Second, we expect incentives to either increase or have no effect on confidence levels. Finally, we expect incentives to increase respondents' response times, again by making them exert more effort to spot scams.

Our cross randomized design allows us to look at the effect of interaction between information and incentives on scam identification ability. We predict that providing both information and incentives to increase correctly identified messages in comparison to the control group. Additionally, we will look at how interacting these two treatments will perform in comparison to only information and only incentives treatment. This will help us understand whether incentives and information are substitutes or complements in our context. For example, in comparison to only information or only incentives, we expect that the combination of the two either increases SIA further or does not have an additional effect. The effects here are rather ambiguous, however, it will have implications on i) the future implementation of our novel measure and ii) future interventions which aim to increase SIA. We will perform similar analyses for other outcomes.

6 Additional Analyses

We will also explore correlates of SIA and confidence in SIA by looking at i) basic demographics, ii) the use of digital financial services and trust in these services, and iii) scam experience. In what follows we give a detailed account of measures in each category.

6.1 Basic Demographics

- Age
- Gender
- Urban versus rural area
- Education level (no education, primary education, secondary education, post-secondary education): We expect a negative correlation between the level of schooling and the number of correctly identified messages. This will internally validate our novel measure of SIA.
- Income level (6 income bands)

6.2 Use of Digital Financial Services

- Recent use of digital financial services (within past 90 days; constructed as a dummy variable which equals to 1 if the respondent used digital financial services within past 90 days and zero otherwise).
- Diversity of the use of digital financial services (constructed as a dummy which equals to 1 for respondents who have above median use of different digital financial services)
- Trust in digital financial services (a great deal, quite a lot of trust, not very much trust and none at all)

6.3 Scam Experience

- A dummy variable which indicates whether the respondent has been contacted by a scammer
- A dummy variable which indicates if the respondent has recently (within the last 4 weeks) been contacted by a scammer
- A dummy variable which indicates if the someone known by the respondent has been victim of a scammer

Finally, we included a question which serves as an "attention check" to understand whether the respondents pay attention to the survey questions. We will control for attention (binary indicator for passing the attention check) in all our main analyses and will conduct robustness checks in which we include inattentive respondents.

7 Empirical Model

7.1 Benchmark Model

The main regression specification will be ANCOVA regressions, where we control for baseline SIA level, as well as other individual characteristics.

To test the null hypothesis that i) information, ii) incentive and iii) information and incentive treatment had no effect on our main outcome variables, we will estimate the following model controlling for individual characteristics that are likely to predict our outcome of interest.

$$y_i = \alpha_0 + \alpha_1 Inf_i + \alpha_2 Inc_i + \alpha_3 Inf_i * Inc_i + X_i'\gamma + Other_i + \epsilon_i \quad (1)$$

, where Inf_i is a dummy variable which equals to 1 if individual i received the information treatment and zero otherwise. Inc_i is a dummy which equals to 1 if individual i received the incentives. X_i is a set of individual characteristics for respondent i. These include gender, age, income and education level and outcome variables collected in the first part. $Other_i$ captures other variables that might be added for specific regressions, such as the order of the two parts. We will also present our results without these covariates, or without including respondent characteristics. The estimated $\hat{\alpha_1}$ is the average treatment effect of information treatment, $\hat{\alpha_2}$ is the average treatment effect of incentive treatment and $\hat{\alpha_1} + \hat{\alpha_2} + \hat{\alpha_1} * \hat{\alpha_2}$ is the average treatment effect of interaction between information and incentives treatment. The standard errors ϵ_i will not be clustered but robustly estimated.

Additionally, we will explore treatment effect heterogeneity with respect to gender, age, education level, income level, rural/urban, the use of digital financial products, and scam experience.

7.2 LATE estimation

We expect some respondents to pay less attention to the information than others. Therefore, we will estimate the local average treatment effects (LATE) by looking at the time spent on information, which will proxy treatment intensity. The model we will estimate is as follows:

$$y_i = \beta_0 + \beta_1 InfTime_i + \beta_2 Inc_i + \beta_3 InfTime_i * Inc_i + X_i'\gamma + Other_i + \delta_m + \epsilon_i \quad (2)$$

, where $InfTime_i$ is the intensity of information treatment measured by time spent on looking at information. This variable will take zero by design for respondents who will not receive information. Here, we will use treatment assignment (Inf_i) as an instrument and the estimate β_1 will give us LATE.

7.3 Additional Models

We will also estimate the effects of our treatments at the individual and message level controlling for individual characteristics as follows:

$$y_{im} = \alpha_0 + \alpha_1 Inf_i + \alpha_2 Inc_i + \alpha_3 Inf_i * Inc_i + X_i'\gamma + Other_i + \delta_m + \epsilon_{im} \quad (3)$$

, where y_{im} denotes the outcome of interest for individual i and message m and δ_m denotes the message fixed effects. We expect this model to provide us with more insight regarding the implementation of our measure by taking into account of different types of messages used to test respondents' scam identification ability. For example, without message fixed effects, this model allows testing whether information that is relevant for a given vignette increases correct classification of this particular message.

Appendix

A Online Survey

Online Survey

Welcome!

You will normally see the questions in English. If you prefer, you can switch most parts to Swahili (and back to English) in the top right corner.

Project Title: The Use of Digital Financial Services
Research Team: Dr. Lisa Spantig, Dr. Jana Cahlikova, Lucy Kaaria, Dr. Elif Kubilay and Dr. Eva Raiber

The following statements need to be agreed to before participants can take part in the online survey.

The following survey is part of the study jointly conducted by Nendo Limited and researchers from the University of Essex. You have agreed to take part in this study, and you can read more about the study here [link to participant information sheet].

1) I confirm that I have read and understand the Participant Information Sheet dated 25.06.2021 for the study.
    - Yes
2) I understand that my participation is voluntary and that I am free to withdraw from the project at any time without giving any reason. I understand that any data collected up to the point of my withdrawal will be destroyed.
    - Yes
3) I understand that my answers will be anonymous and no personally identifiable information will be collected.
    - Yes
4) I agree to take part in the study.
    - Yes
    - No

PART A: Demographics

1) What is your gender? [Quotas]
    - Male
    - Female

2) In what year were you born? Reply with a four-digit number like 1980. [Text entry; quota]

3) What county do you currently live in? Pick the name of your county below. [Drop-down menu; quota]
    - Baringo
    - Bomet
    - Bungoma
    - Busia
    - Elgeyo-Marakwet
    - Embu
    - Garissa
    - Homa Bay
    - Isiolo
    - Kajiado
    - Kakamega
    - Kericho
    - Kiambu
    - Kilifi
    - Kirinyaga
    - Kisii
    - Kisumu
    - Kitui
    - Kwale
    - Laikipia
    - Lamu
    - Machakos
    - Makueni
    - Mandera
    - Marsabit
    - Meru
    - Migori
    - Mombasa
    - Murang'a
    - Nairobi
    - Nakuru
    - Nandi
    - Narok

- Nyamira
- Nyandarua
- Nyeri
- Samburu
- Siaya
- Taita-Taveta
- Tana River
- Tharaka-Nithi
- Trans Nzoia
- Turkana
- Uasin Gishu
- Vihiga
- Wajir
- West Pokot

4) Do you live in a rural or an urban area?
    - Urban
    - Rural

5) What is the highest level of school you attended?
    - Primary school
    - Secondary school
    - Post-secondary school
    - No School

6) What was the total monthly income for your household in KES for the last month (December 2021)?

    Please include all sources of income including money sent by employers, family or friends. Do not include the value of in-kind items such as food or housing.

    - Below 77,000 KES
    - 77,001 KES - 186,000 KES
    - 186,001 KES - 295,000 KES
    - 295,001 KES - 404,000 KES
    - 404,001 KES - 515,000 KES
    - Over 515,000 KES
    - I do not know
    - I refuse to answer

7) Do you currently have a job with a formal employment contract?
    - Yes
    - No
    - I do not know
    - I refuse to answer

8) Is your phone able to connect to the internet?
    - Yes
    - No
    - I don’t know

9) Is your phone able to access social media like Facebook or Whatsapp or able to download apps?
    - Yes
    - No
    - I don’t know

10) Do you share your phone with someone else?
    - Yes
    - No

11) Do you share a SIM card with someone else?
    - Yes
    - No

12) Are you the one that this SIM card is registered to?
    - Yes
    - No
    - I don’t know

Part B1: Scam Identification Ability (SIA) Measure

You will see several examples of text messages. Some of these messages are scams. Scams try to get your money or personal information to use it for fraud.

Your task is to identify which messages are scams.

[Randomly selected 50% of the sample] For each message that you identify correctly, you will receive 10 Shillings. At the end of the survey, we will let you know how many of the examples you identified correctly.

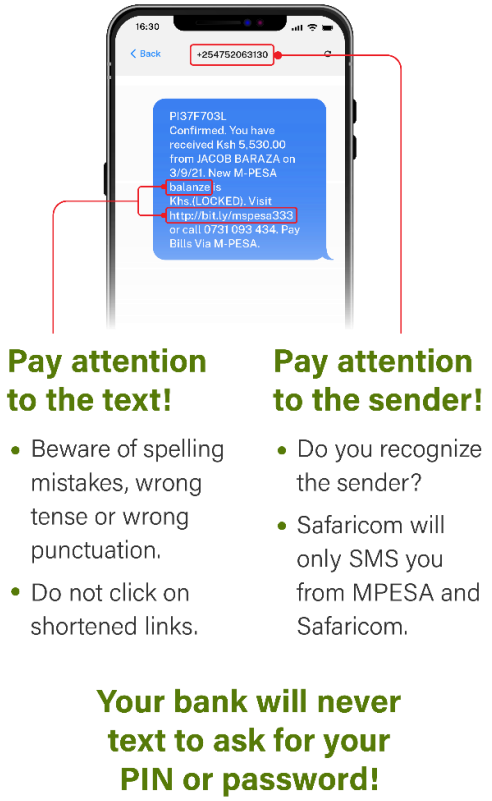
[display vignettes 1-6 or 7-12 here in random order; for each vignette:]

- Is this a scam? (yes/no)
- How confident are you in this answer? (0=not confident at all; 5=completely confident)

Scam identification tips

[for randomly selected 50% of the sample; visualization incl. phone number subject to change.]

How can you spot a scam message? We have collected some tips.



Part B2: SIA Measure (6 messages)

[Introduction] You will see another set of examples of text messages. Some of these messages are scams. Scams try to get your money or personal information to use it for fraud. Your task is to identify which messages are scams.

[Randomly selected 50% of the sample; same as before] For each message that you identify correctly, you will receive 10 Shillings.

[display remaining vignettes 7here in random order; for each vignette:]

- Is this a scam? (yes/no)
- How confident are you in this answer? (0=not confident at all; 5=completely confident)

PART D: The Use of Digital Financial Services

We will now ask you a few questions regarding your use of digital financial services, for example sending mobile money or taking a mobile loan.

1. In the past 90 days, have you made any financial transactions on your phone?
    - Yes
    - No
    - I refuse to answer

2. Which of these financial transactions have you EVER done with your phone? Select all options that apply.

    - Sending or receiving funds with mobile money
    - Accessing a bank account via your mobile phone
    - Paying a bill or paying for something with mobile money
    - Taking a mobile loan
    - Conducting a financial transaction using an agent (includes withdrawing funds)
    - None of the above
    - I refuse to answer

3. **[IF either "Sending or receiving funds with mobile money" or "Paying a bill or paying for something with mobile money" is selected in D2]** What do you use mobile money for? Select all options that apply.

    - Send money to friends or family
    - Receive money
    - Receive salary
    - Receive payments for business
    - Make payments for business
    - Pay bills/purchase items
    - Save or keep money
    - Buy airtime

- Gambling
- Other
- None of the above
- I refuse to answer

4. How much trust do you have in people from your neighborhood?
    - A great deal
    - Quite a lot
    - Not very much
    - None at all

5. How much trust do you have in digital financial services?
    - A great deal
    - Quite a lot of trust
    - Not very much trust
    - None at all

PART E: Scam Experience

We will now ask you some questions about your experiences with scams.
Scammers try to get your money or personal information to use it for fraud.

1. Have you ever been contacted by a scammer?
    - Yes
    - No

[IF E1 = YES]

1.1) Approximately when was the last time you were contacted by a scammer?
- Less than a week ago
- Between 1 week and 4 weeks ago
- Between 1 month and 12 months ago
- More than 12 months ago

1.2) How did you encounter these scams or fraud? Select all options that apply.
- By phone call
- By SMS
- On social media
- Other

1.3) What did the scammers ask you to do? Select all options that apply.
- Send money
- Share my password or PIN
- Share my personal information

- Share account details
- Asked for a payment reversal
- Asked to help relative or a friend in need
- Other

1.4) How did you know that this was a scam? Select all options that apply.

- Regular number
- From others' experiences
- Requested personal information
- No recent transactions
- Personal awareness
- Incorrectly identified me
- Never used the service
- I did not know the caller/sender
- Unusual time
- Poor language or grammar
- Other

1.5) What did you do?

- I fell for it
- I ignored it
- I deleted it
- I reported it

1.6) Have you alerted any of your family members of friends?

- Yes
- No

2. Have you ever been a victim of a scammer?
   - Yes
   - No

[IF E2 = YES]

2.1) Have you alerted any of your family members of friends?

- Yes
- No

3. Has anyone you know ever been a victim of a scammer?
   - Yes
   - No

[for participants in incentive treatment] You have answered ${Score} scam example questions correctly.

[for participants in incentive treatment] Your *bonus earnings* for answering scam example questions is $e{Score} * 10} Schillings.

I confirm that I have completed the survey.

- Yes