DECODIS

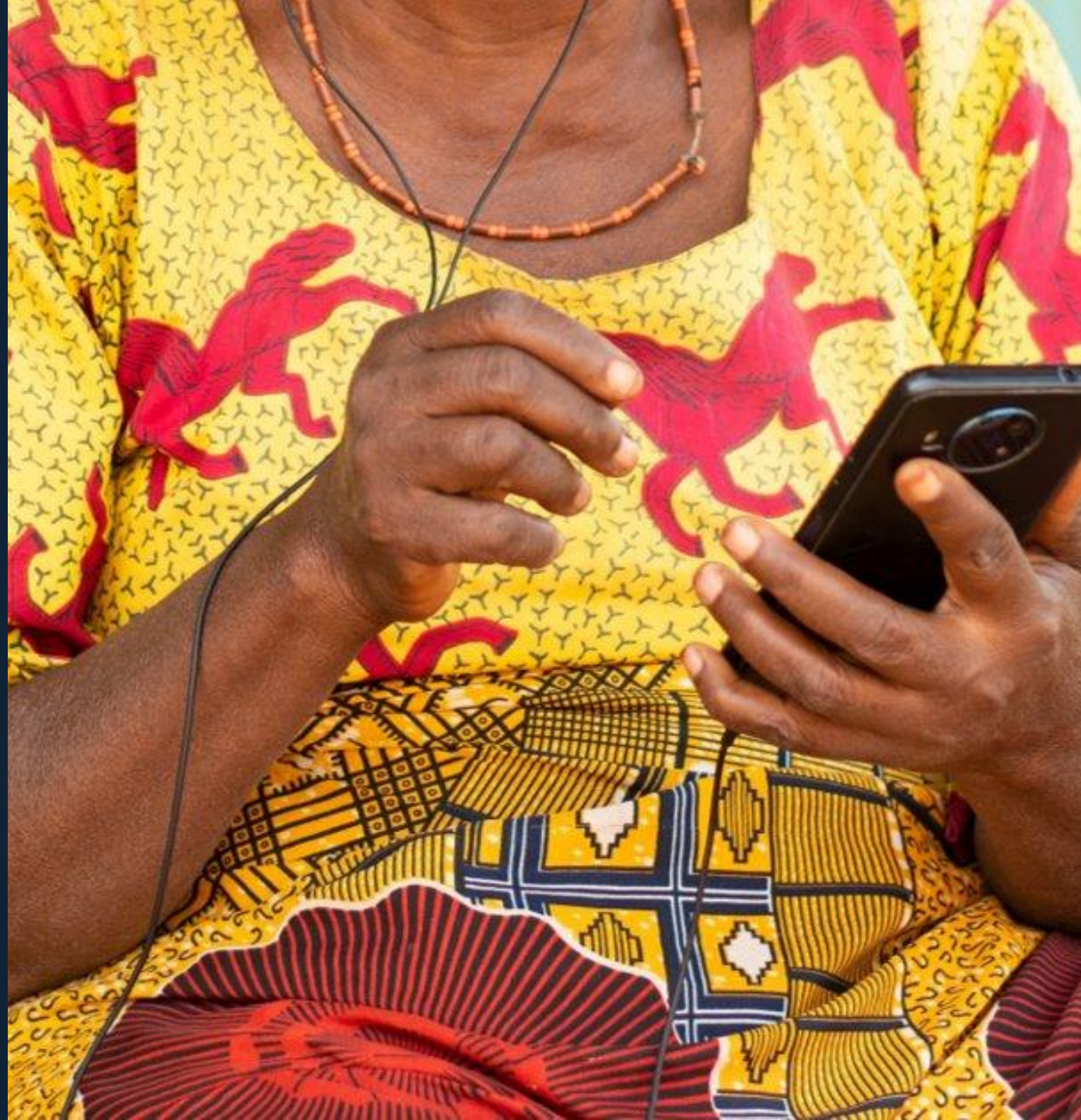
HENRY J. LEIR INSTITUTE
ADVANCING HUMAN SECURITY

Digital Portfolios of the Poor

Digital Philosophies of Trust

Nigeria

May 2026



Executive Summary

Uneven patterns in digital financial usage

- The most recent financial and digital inclusion data shows weakness in digital financial use despite widespread access to digital devices and broad use of digital applications. We asked ourselves, does this low uptake reflect different patterns of digital trust across applications and segments?

Measuring and using digital trust philosophies

- We leveraged automated voice interviews and AI-powered text analysis with 960 Nigerian men and women across a range of northern,eastern and southern states.
- The responses collected were largely open-ended voice responses, surfacing qualitative perspectives often drowned out in traditional quantitative surveys.
- For this study, it was important to have this type of "qualitative data at quantitative scale" to allow for an inductive analysis of how respondents voiced their own perspectives without pre-specification of responses. Yet it was also important to have a large sample to test where a type of response was idiosyncratic across a few respondents or across the entire sample.

Tested with digital providers

- Digital providers effectively leveraged user segments. We used Digital Trust Philosophy segments in workshops with three diverse digital service providers to stimulate action to ensure they are serving all types of customers.

What we found

- Across the four countries covered in this study – Nigeria, Kenya, India and Pakistan – there were three archetypes of digital trust philosophies: Assurance seekers, Protection seekers and Control seeker.
- For Nigeria: Protection Seekers 17%; Assurance seekers 47%; Control seekers 36%
- These archetypes were formulated based on four common pillars: Types of digital risk perceived, how that risk is mitigated, who is responsible for keeping users safe, and the benefits associated with digital usage.
- However, these pillars manifested themselves differently in each country.
- In Nigeria, there is a bifurcation between Assurance seekers and Control seekers are the largest archetypes, similar to Kenya.
- Interestingly, these two archetypes share many features:
    - Similar percentages with access to smartphones (approx. 71%-78%)
    - Similar percentages that need to share the phone (approx. 50%-56%).
    - Both concerned about account hacking and transaction failure, a particular concern in Nigeria compared to other countries.
    - Both mitigate risk by simply being cautious.
    - Both value digital access for income generation.
- However, they differ critically in who they hold responsible for protecting them online. Control seekers balance responsibility between themselves, platforms and institutions (banks), while Assurance seekers are unclear who they hold responsible for protecting them.

Table of Contents

I. Objectives of the Study

Why did we embark on this research?

Digital Trust Deficits and Digital Financial Management

Daily mobile phone use has grown substantially across the Global South along with social media, videos, voice and text messages.

But use of digital financial tools has lagged.

There are differentiating patterns across countries:

Kenya
High uptake of digitally-enabled accounts and payment use cases; lower use of storing money digitally.

Nigeria
Growth in uptake of digitally enabled accounts; payments well behind Kenya but storing money is higher.

India
Uptake in digitally enabled accounts and payment use is weaker; storage is higher.

Pakistan
Uptake in digitally-enabled accounts, payments and storage are weak across the board.

Can these uneven patterns be explained by a digital trust deficit?

Digital financial services providers often lament that customers lack trust.
But digital trust remains poorly defined.

All data from Findex, 2024.

Our objectives

01 Develop a globally relevant framework of digital trust philosophies as described from the perspective of the actual and potential users.

02 Determine if there are commonalities across countries, segments, phone ownership or other digital service use.

03 Test whether these frameworks help digital service providers to generate ideas about how to increase trust

II. Qualitative Data at Scale

A new research method

Trust is a qualitative notion but to meet our objectives we need scale

We need qualitative data because:

- Trust is a nebulous, qualitative idea which needs to be described in an open-ended response.
- Quantitative questions ask respondents pre-conceived answers - we want to be open to new perspectives.

We need to ask open-ended questions like:

- **Whose responsibility** is it to make sure that users don't experience privacy breaches or security risks?
- **How do you think** security and privacy breaches happen?
- **What do you see** as pros and cons of using digital financial services?

But we need a large sample size because:

- We want to know if trust deficits differ systematically across segments.
- We want a large enough sample to have segments relevant to a wide range of digital financial service providers.

Data collection: Asynchronous surveys using IVR

What we do
- Asynchronous interviews
- Pre-recorded local language-speaking voice actors not AI generated audio questions

But don't you need to probe?
- Well-tested questions turns what might sound as a disadvantage into a benefit.
- Not having a live interviewer meant no interruption or social desirability bias.[2]

The benefit
- Open-ended responses across 1000 people in four countries.
- Long, meaningful answers. Much longer than a typical live interview average.[1]

We also use skits to increase qualitative depth

What we do

We record fictional audio skits that respondents listen to, then asking questions about their thoughts about the scenario.

Benefits:

- Skits let people discuss sensitive or abstract topics like trust in a depersonalized way.
- Nebulous concepts are made concrete.

[1]See Decodis and Brac University paper about enumerator interruptions in live phone interviews in Bangladesh. Link here

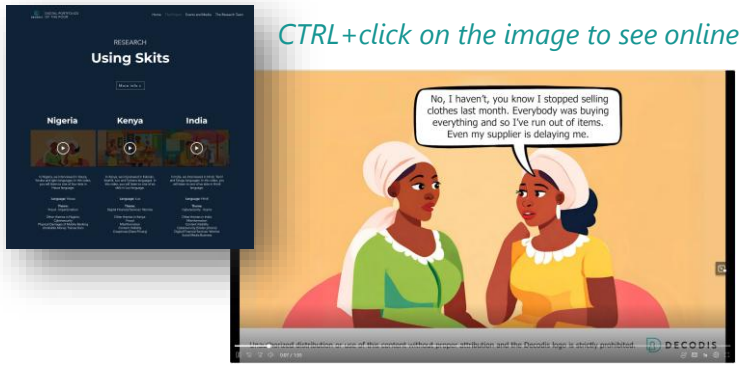
[2]See Bergen and Labonte. 2020. "Detecting and Limiting Social Desirability Bias in Qualitative Research." *Qualitative Health Research* April 30 (5)

Data collection: Using skits

SKIT EXAMPLE

We use 4-6 skits, each followed by 8 questions

A fraudster impersonates Adeola's WhatsApp business account to scam customers, prompting her friend Hawa to advise securing the account with two-step verification and registering it as a WhatsApp business account.



CTRL+click on the image to see online

Listen to the Nigerian WhatsApp Fraud Scenario in Hausa

Note: Videos are for illustration and translation purposes. Respondents are only exposed to skits via phone call.

RESPONSE EXAMPLE

Listen to a response in Yoruba.

"If I see a product advertised on WhatsApp and I'm interested, I call the person directly to make an inquiry. I know all the contacts on my WhatsApp, so I prefer talking to them to confirm it's really them. This is because in the past, I've received messages asking me to send 10,000 or 20,000 naira, so I always call to verify before taking any action."
(Man)

Data collection: Asynchronous surveys using IVR and web links

What we do

- Asynchronous interviews
- Pre-recorded local language-speaking voice actors (not AI generated voice questions)

But don't you need to probe?

- Well-tested questions turn what might sound as a disadvantage into a benefit.
- Not having a live interviewer meant no interruption or social bias.

The benefit

- Open-ended responses across 960.
- Long, meaningful answers. 3x longer responses than in a typical in person interview.[1]

[1]See Decodis & Brac University paper about enumerator interruptions in live phone interviews in Bangladesh. Link here

960 people interviewed in Nigeria

4 survey modules

275 hours
of voice data collected

133 voice response questions

94 keypad response questions

Data analysis: Inductively identifying themes using grounded theory

Example of response Decodis gets and how we categorize

RISK MITIGATION

"I think Onyango's father is someone very informed because it should be that when you are being called from Safaricom office there is a number that they use to call you. And if there is a number different from that of Safaricom then you should not suppose to receive the call. It is your personal duty because Safaricom daily sends messages they announce do not accept: do not accept any number that calls you apart from the one that we tell you. That is why I don't know they are which people, but we were told they once worked with Safaricom but were fired, or someone can trace your number. I can tell people to have awareness on such kind of people by telling someone that."

PERSONAL RESPONSIBILITY

TYPE OF RISK

With hundreds of hours of open-ended response in hands, we begin to understand the data by looking at a subsample of the responses and creating categorical themes based on how respondents answer. We create categorical themes until "saturation," i.e. when no new themes are emerging from looking at additional data.

This is an example of how we manually code responses before the prompt-writing process.

Data analysis: Using prompt-writing to tag themes to each question

Using this method across a large sample tells us whether themes are prevalent and not isolated incidents.

Step 1

We write prompt for AI to extract themes from open-ended transcribed responses.

Context
The following texts are responses to questions about the risks and benefits of WhatsApp for business, online banking, POS transactions

Task
Based on the context, tag the response to the appropriate category based on what the respondent says about the risks of using online banking, POS transactions or platforms like WhatsApp for business.

Categorization Scheme
UnauthorizedPlatformAccess* – Hacking of WhatsApp or bank accounts due to lack of 2FA, malware, or SIM swap.
CyberFraud* – Fears of hackers, phishing, impersonation calls, and information theft through digital channels. Identity&ProfileTheft* – Impersonation on platforms like WhatsApp, with fake profiles used to scam others. ConnectivityFailures* – Frequent loss of signal, network downtime, or poor internet disrupting transactions, causes anxiety.

Output Instructions
Label the response with the relevant category name as listed in the categorization scheme

Step 2

The model tags responses that allude to trust themes. In this case, tens of thousands of open-ended responses are tagged.

Step 3

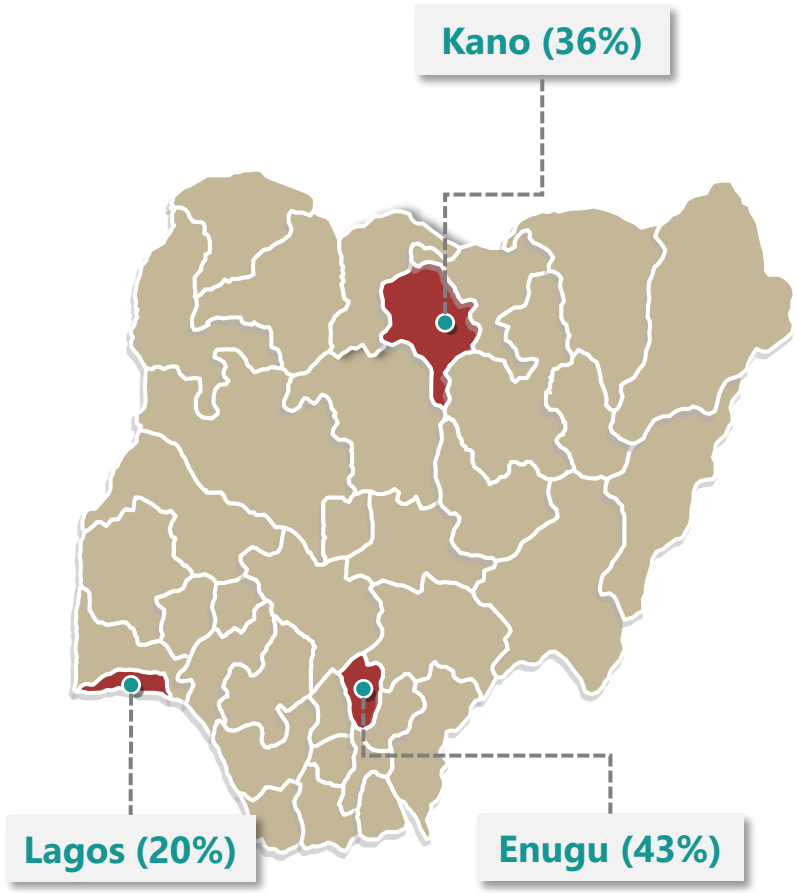
We do extensive iteration, improving the prompt and specificity of theme-tagging.

Resp ID	Transcription of response	Tags
Resp_001	**Someone has to be very careful while making online transactions or filling of forms.**	"Personal Responsibility"

III. Digital Portfolios Sample

Device and application use results for Nigeria

Nigerian sample: Geographies and Languages

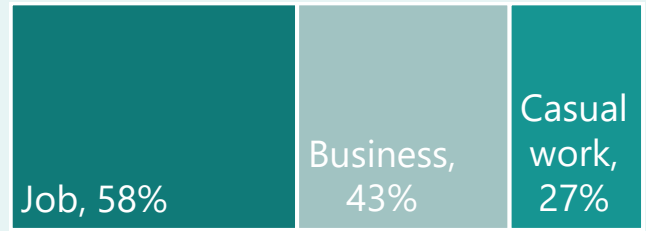


Key survey facts

- **Sample size**: 960 people
- **Languages**: Hausa, Yoruba and Igbo
- **Data collection**: May 2024

57%

Women



Nigeria: Phone access and ownership

Reportedly high ownership.

Reported Access v. Ownership	Smartphone	Feature phone	Basic phone
N	726	126	94
Access to each type of phone	76%	13%	10%
Ownership of each type of phone	72%	11%	9%
|→ Owners who need to share phone	55%	50%	44%

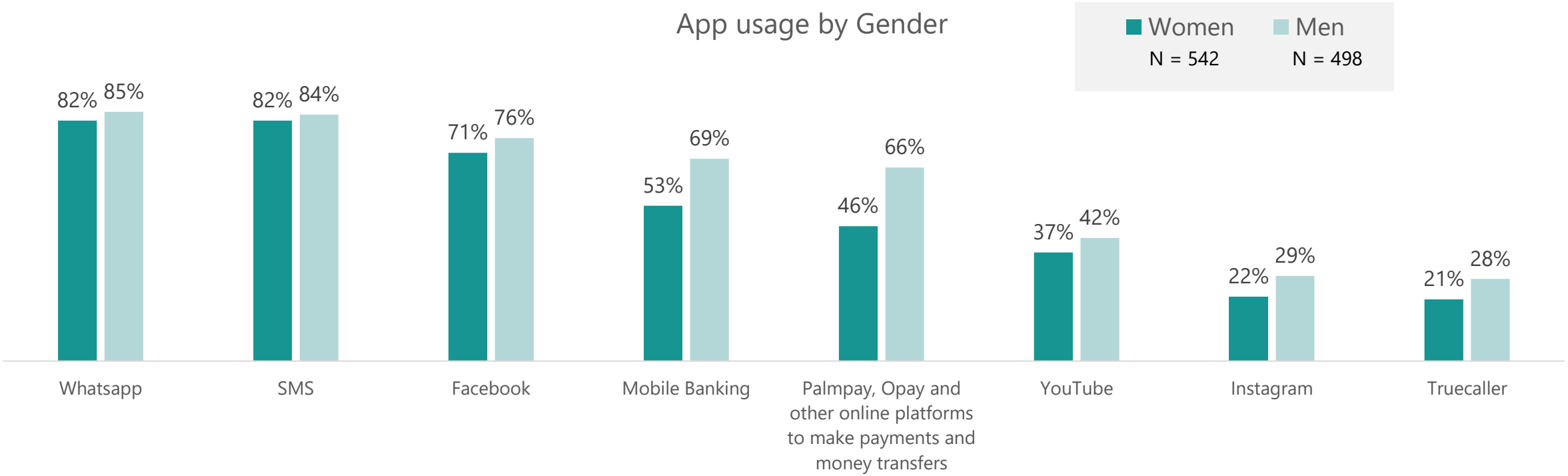
Much access to smartphones, high reported ownership, less sharing than other countries

Of the others, most had access to a smartphone. 72% of the total sample said they owned the phone.

However, we found through other questions in the survey that "ownership" is a broad idea. Many suggest that if they can use it, they feel a sense of "ownership." More importantly, half of those who say they own their phones say they need to share it.

More surprisingly, 57% said they have access two devices and not just one. However, we did not ask respondents to what degree they could access the second device. The responses could have ranged from being able to use it at any time compared to only using it briefly every now and then.

Nigeria: Types of digital use by gender



Generally, a higher percentage of men in this sample used different applications than women. However, a few data point deserve to be called out:

- As in the other countries, the percentage of women using payments or mobile banking is lower than men.
- Apps for communication, social media and digital protection are lower for women than men, but by not as much as digital financial services.

IV. Deriving Philosophies of Trust

in Digital Solutions and Archetypes

Our analytical process

IDENTIFYING **PHILOSOPHIES OF TRUST**	1	1a	Inductively identifying trust themes and sub-themes using grounded theory
		1b	Quantifying themes across the sample using prompt engineering
DERIVING **DIGITAL TRUST ARCHETYPES**	2	2a	Deriving archetypes using cluster analysis
		2b	Describing the archetypes
		2c	Potential “typing tool” to put customers into archetypes

1 1a

Inductively derived pillars of digital trust

A

Risk Perception

"What do people fear?"

B

Risk Mitigation

"How do they act on those fears?"

C

Responsibility Perception

"Who do they hold accountable?"

D

Benefit Perception

"Why take the leap?"

PILLARS OF DIGITAL TRUST

Together, these four pillars reveal **patterns of risk, responsibility, action, and reward** that create and maintain digital trust.

We extract themes of trust "inductively", which means **determined based on what respondents said** and not by forming hypothesis and looking for those in the data.

We derived four key pillars of trust grounded in participants' own words. It also generates a more comprehensive view of how underserved users approach digital engagement.

These pillars of digital trust are the same across all countries in the study.

1 1a

Sub-themes that define Risk Perception

A Risk Perception

People's readiness to trust digital tools depends on what dangers they foresee.

Variable Name	Definitions
Account hacking	Ubiquitous across archetypes. Concerns focus on hackers getting into an account and stealing money.
Middleman distrust	Users are convinced that bank employees know their details and steal their money. This is less about agent.
Transaction failures	Telecom systems in Nigeria can be unstable and users are not sure if a transaction has gone through. They are particularly concerned when they are making a payment and the receiver did not get the money, they are concerned about their reputation.
Physical theft	They worry that taking their phone out to use a digital service in public will attract thieves to steal their phone.

Though the pillars are consistent across countries, the sub-themes that underpin them are different, reflecting the proliferation of products and devices.

1 1a

Sub-themes that define Risk Mitigation

B Risk Mitigation

Variable Name	Definitions
Cautious sharing	This type of risk mitigation comes up in two difference ways. For Assurance seekers, they will limit their transaction only to people they know, or they will use cash. For Control seekers, they will make sure they know how to put digital safeguards in place before using an application or doing a transaction.
External verification	Users will check with someone else to see if they are using the digital service in a safe way.
Identity scrutiny	Users will only accept some sort of digital introduction if they know the person. They will try to verify that the other person is who they say they are.
App verification	Users will use app features to protect themselves.
Transaction monitoring	Users will monitor their translations through the payment app to make sure the incoming and outgoing transactions are what they should be.

Though the pillars are consistent across countries, the sub-themes that underpin them are different, reflecting the proliferation of products and devices.

1 1a

Sub-themes that define Responsibility Perception

C Responsibility Perception

Variable Name	Definitions
Institutional responsibility	Users believe that an institution – most often banks - is responsible for keeping them safe. Unlike India, this is typically not the government.
Unclear	Users are muddled in their answers or state that they do not know.
Platform responsibility	Users will mention a specific platform like a payment app, or WhatsApp, or Facebook. They recognize that the apps they use are distinct from the government, the bank or telcos.
Shared responsibility	Users distinctly mention that they themselves has responsibilities to protect themselves alongside platforms or institutions.
Personal responsibility	Users only refer to themselves as being responsible for keeping themselves safe.

Though the pillars are consistent across countries, the sub-themes that underpin them are different, reflecting the proliferation of products and devices.

1 1a

Sub-themes that define Benefit Perception

D Benefit Perception

The benefits that people receive that pulls them towards digital.

Variable Name	Definitions
Income enabler	Users talk about being able to increase by increasing the reach to sellers beyond foot traffic.
Time efficiency	Users refer to being able to do transactions without going to a bank branch.
Physical safety	Users talk about being able to reach friends and relatives if they are physically unsafe.

Though the pillars are consistent across countries, the sub-themes that underpin them are different, reflecting the proliferation of products and devices.

A set of globally-relevant Digital Trust Philosophy archetypes

AS

Assurance seekers

They have limited understanding of risks and mitigation, building trust through peer assurance.

PS

Protection seekers

They have the widest range of fears, increasing the likelihood of withdrawing from digital tools. They build trust through provider or government protection.

CS

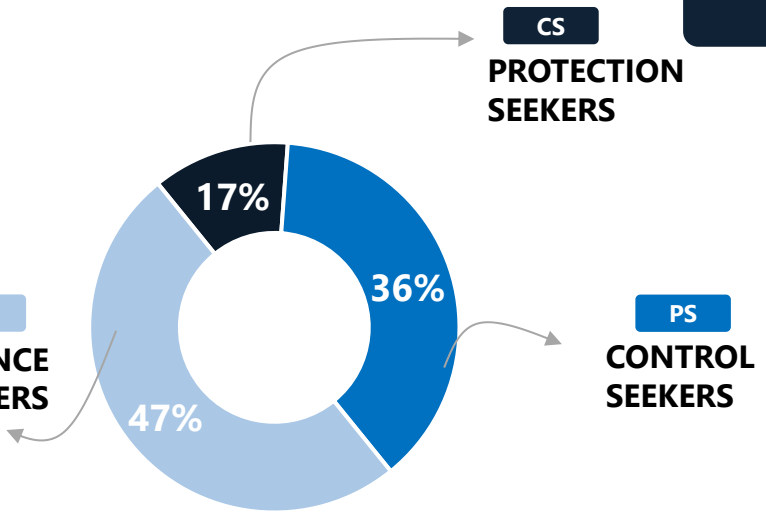
Control seekers

Digitally competent and confident in their ability to self-protect

A set of globally-relevant of Trust Philosophy archetypes

Archetypes in Nigeria

N=960



Online fraud feels rare because platforms like Amazon and Flipkart use cash-on-delivery, and earning money online is generally seen as safe. While harassment and photo misuse worry people, cyber police, helplines like 1930, and trusted apps such as PhonePe, Google Pay, and bank apps make it manageable, and suspicious messages are simply deleted.

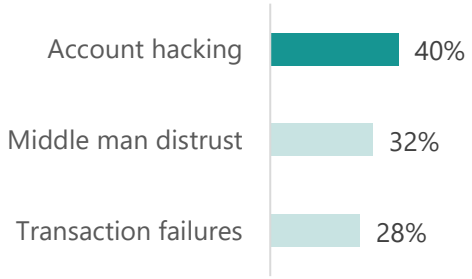
Online risks exist, like data theft or photo misuse, so we must be careful. If something goes wrong, we should act quickly by asking friends first and then going to the bank or cybercrime authorities for help.

Scams and harassment happen on both sides, so we must be careful ourselves. The government should control online abuse, banks should fix server issues, and we should never share IDs or click unknown links, using trusted apps and blocking accounts if something feels wrong.

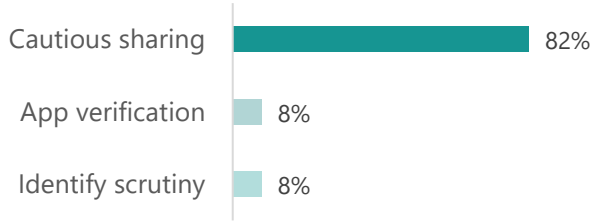
Assurance Seekers: Attributes

Of those who are Assurance Seekers and talking about each pillar,
% who mention this type at least once

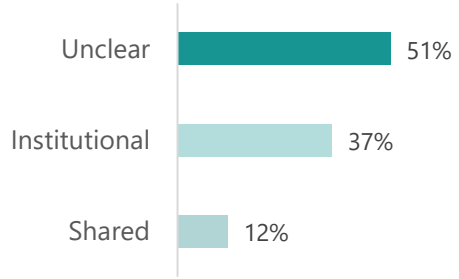
A Risk Perception



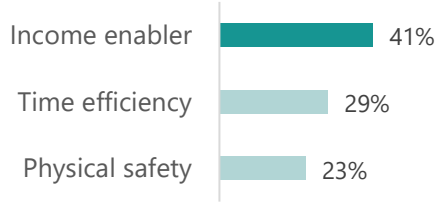
B Risk Mitigation



C Responsibility Perception



D Benefit Perception



AS ASSURANCE SEEKERS
47% of the sample

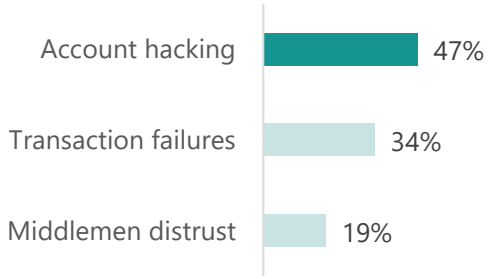
- 58% of Assurance Seekers are women.
- 71% have access to a smartphone.
- 50% need to share a phone.
- Those in this archetype are unclear about how the digital world works.
- They have the highest proportion of people who are unclear about who holds responsibility for digital safety.
- Their chief form of risk mitigation is to use digital financial services as minimally as possible (see quote below)
- They have the highest percent of people who suspect that risk is coming from employees who work at providers who are stealing money, i.e. the middlemen.

"Contact the WhatsApp platform owners; there should be a mechanism that alerts all your contacts immediately if something goes wrong. This could also help in advertising your products. I don't see any risks. **. I don't know bankers, have no idea about hacker risks, and don't know where to go to complain** I prefer cash. People in areas without banks can access money anytime. Sometimes, your card details can be copied."- Female, 35-44, Enugu, Below $33

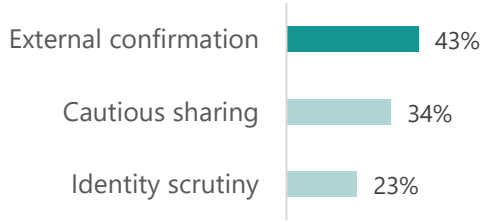
Protection Seekers: Attributes

Of those who are Protection Seekers and talking about each pillar,
% who mention this type at least once

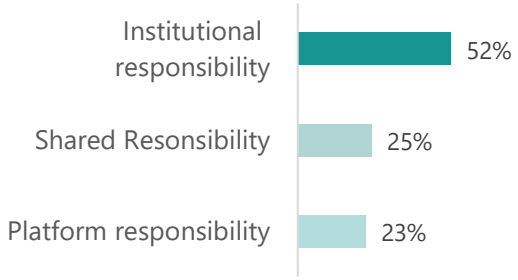
A Risk Perception



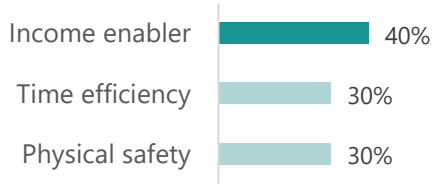
B Risk Mitigation



C Responsibility Perception



D Benefit Perception



PS PROTECTION SEEKERS
17% of the sample

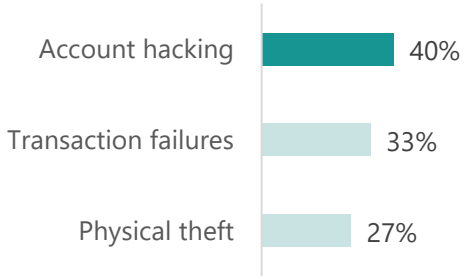
- 55% of Protection Seekers are women.
- 83% have access to a smartphone, the highest of any archetype.
- 50% need to share their phone.
- They speak of external verification as a risk mitigation strategy. This suggests a level of unfamiliarity with digital financial services, but not to the extent that they will curtail their use. See quote below.
- Some reflect some part of their own responsibility alongside institutions and platforms.
- They distinguish between an institution like a bank and digital platforms such as payment apps, WhatsApp and Facebook.

> I trust a WhatsApp Business account only if I know the person or we have mutual friends. Close family can be trusted with account details if they value privacy. Selling on WhatsApp is convenient and safe because you usually know your customers, and you can advertise anything.
> - Male, 25-34, Lagos, Below $33

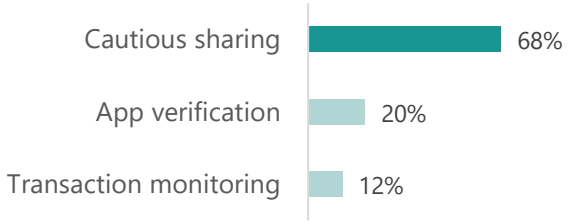
Control Seekers: Attributes

Of those who are Control Seekers and talking about each pillar,
% who mention this type at least once

A Risk Perception

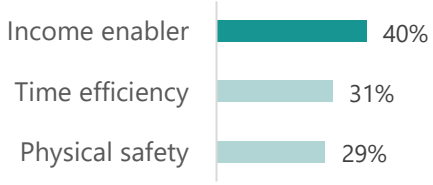


B Risk Mitigation



C Responsibility Perception

D Benefit Perception



CS CONTROL SEEKERS
36% of the sample

- 57% are women.
- 78% have access to a smartphone.
- 56% need to share a phone.
- Similar to Assurance Seekers, Control Seekers are also focused on cautious sharing as a risk mitigation strategy. However, they speak about it differently in that they emphasize being careful about implementing digital safety strategies rather than minimizing use (see below)
- Also reflecting their greater digital capabilities, they are the only archetype to talk about transaction monitoring.
- They are the only archetype to talk about pure personal responsibility, rather than referring to personal responsibility combined with institutional or platform responsibility.

"WhatsApp is safe if you enable two-step verification and stay alert for scams. It's useful for selling products, cheap calls, and private chats. The main risks are unauthorized access and scams, so guard your details closely. "

Female, 25-34,Lagos, Below $33

Key questions institutions could use to type customers into trust archetypes

In order to understand which archetype a customer fits within the most, they could be asked this set of questions. Based on their open-ended response, themes could be extracted using pre-built code.

1. What type of device do you mostly use?
2. What types of digital services do you use?
3. What do you see as risks of digital services?
4. Who do you think is responsible for protecting you from digital risks?
5. What are the greatest benefits of digital channels for you?

V. Workshops in Nigeria

Did this research influence how providers could build trust in digital channels?

Objectives of the workshops

Objective 1

Solve for more than one archetype

- **Identifying customer types easily** - if institutions need to type customers themselves, this would be burdensome
- **Solve for trust archetypes that they already have**, even if not explicitly typified
- **Solve for more than one type of customer** to meet multiple trust needs
- **Solve for a concrete set of attributes.**

Objective 2

Lessons to generate tractable actions across departments

- **Proposing different solutions to earn a slot in the pipeline:** Because there are constant projects and priorities happening across departments, there needs to be a multitude of solutions in order for at least some to enter the project pipeline.
- **Start with low effort to gain traction:** Not all solutions need to be complicated – being able to implement some "low-hanging fruit" provides evidence to invest in more complex solutions
- **Create solutions for different trust needs:** Multiple changes implemented across aspects of customer experience will be more effective at growing customer trust than just one

Keys to success

Attendance

- **Must have senior people** from product development, communications, etc.
- **Must only take half a day** so it is easy for those people to attend

Rotate experience of solutioning for archetypes

- **Work with 2 most prevalent archetypes** in country
- If possible, it is helpful to **have examples of the archetypes** from their customer base
- **The "why" of the workshop**: Your customers are not monolithic in terms of their trust deficits. As you won't know what the trust philosophies are (because they are hidden), you need to "cover all the bases"
- **Workshop participants work with both archetype** to drive home how different archetypes focus on different types of risk.
- An exercise that leads back to normal life – **end with a concrete pitch**

Workshop Process

Framework Introduction

Key outcome: Get situated

We present real data to expose workshop attendees to customer language

Then, we explain the three archetypes and the four trust pillars.

1 Problem Identification

Key outcome: Articulate key pain points of each archetype with respect to their product

We split attendees into small groups, assigning each an archetype. Groups role-play customers and list product pain points and barriers. This allows them to compare how the same problems manifest differently across archetypes.

2 Solution Identification

Key outcome: Create cross-institution

Co-design cross-functional solutions and cluster similar ideas into themes. Teams come up with a prioritized set of archetype-aligned solution themes.

3 Make it Actionable

Key outcome: Create proposals of the business

Produce concrete proposals (short, medium and long term), measures of success and next steps.

7 prompts:

- Tell me about your customer (archetype)
- Tell me about their problem
- How would you solve with $100,000?
- What actions (short/medium/long term)?
- How will you measure success?
- How will you ensure lasting impact?
- Summarize as an evocative story

Workshop institutions

Why we work with microfinance banks and FinTech companies:

- They deepen user trust in savings
- They sustain trust despite unreliable mobile networks
- They build trust with the hard to reach

Source
Microfinance Bank Limited

Source Microfinance Bank Limited is a digital microfinance bank that focuses on low-income clients.

They aim to offer personalized financial solutions and prioritize making these solutions easily accessible to bridge financial inclusion gaps.

esusu.africa is a FinTech company focused on digitizing traditional thrift savings and microcredit systems to enhance financial inclusion across Africa.

They offer digital solutions that automate the processes of thrift savings, collections, and microcredit, thereby addressing challenges associated with manual savings schemes.

AjoCard is a FinTech company focused on making it easy for the underserved and unbanked to manage their money and make payments securely and conveniently.

They have efforts underway to modernize member services through digital channels.

Source Microfinance Bank Limited

Source's objectives

To deepen their users' trust in them - especially in some of their traditional offerings such as digital savings, which are tricky given the high level of requirement of faith from the user.

With strong and growing infrastructure in place, they are **eager to explore how trust could be established and reinforced** in this digital world.

Source Outputs

1 Problem Identification

44% of our female respondents share concerns about **frauds and scams**

2 Solution Identification

Leadership
Reframe messaging from “tech-driven banking” to “community-rooted empowerment” and ensure it resonates through the organization and then to the users

Audit, Compliance
Develop alternative ways of communicating the Terms and Conditions for each product- in ways that the user actually understands instead of the traditional formally worded a lengthy document- while meeting regulatory requirements

Customer Experience
Run awareness campaigns on scam detection, online security, and how Source protects savings—include content on spotting “too-good-to-be-true” offers.

Marketing
Share testimonials from long-term users who overcame trust concerns, highlighting how Source enabled safe savings- using the users' vocabulary as understood through survey insights.

Product Development
Build subtle gamification into the savings journey (e.g.“3 months saved without withdrawal!” badge), rewarding consistency and reinforcing self-trust.

Sales & Partnerships
Launch a “Voices of Trust” referral campaign where loyal customers are rewarded for giving testimonials and referring peers—positioning trust as a shared experience.

esusu.africa

esusu.africa's objectives

To simplify their platform experience (both web and app) for low-income users, particularly those with limited digital literacy.

With a strong product offering and growing demand, they are **eager to understand how prevalent unreliable networks are to building trust** to provide justification to prioritizing revenue to improving their platform optimization. Likewise, they were looking to see if other activities could be used to reassure customers.

As our survey data revealed, network issues are perceived as a trust issue among a sizable portion of women customers, increasing the prioritization.

esusu.africa Outputs

1. Problem Identification

32%

of female respondents who are concerned about using online payment platforms report being concerned about **"unreliable service" issues**

2. Solution Identification

Leadership
Recognize that minor technical disruptions have major emotional consequences for users. Recast them internally as trust risks, not just uptime issues and ensure uptake of the revised messaging across the teams internally.

Product Development
Create a back-end logic that flags users with 3+ failed syncs or exits mid-transaction, then route to support or proactive agent follow-up.

IT
Develop a sustainable back-end architecture plan required for platform optimization, convey the need to the leadership team for an effective re-allocation of resources. This includes running new and necessary API integrations with partners.

Business Development
Help field-facing partners explain connectivity issues as *temporary and fixable*, not mysterious —equipping them to defuse fear of fraud or disappearance.

Customer Experience
Expand receipt messaging channels to include WhatsApp and/or email, in addition to text messages- to further generate confidence in transactions relating to the esusu platform.

Agent Network Management
Build trust assets. Give agents visuals or WhatsApp-forwardable guides showing what a network issue looks like and what to do—users trust visual explanations from familiar agents more than technical terms.

AjoCard

AjoCards's objectives

To strengthen their ability to connect with hard-to-reach users—particularly low-income women navigating complex digital realities.

With a growing Personal Banker network and expansion ambitions, they are **eager to understand how to better communicate value and build user confidence** not just through the PB network, but also directly. They recognized that meaningful engagement requires not just broader outreach, but a deeper, more nuanced understanding of the user's lived digital experience.

The workshop offered a space to rethink communication strategies through the voices of users themselves.

AjoCard Outputs

1 Problem Identification

25% of our female respondents share concerns resulting from a **lack of a physical banking infrastructure**

2 Solution Identification

Leadership
Develop a "User Trust Index" based on referrals, complaints, net savings retained, and support satisfaction and report it at board level alongside revenue and growth.

Marketing & Communications
Co-create marketing content with a panel of 6–8 real users from different regions/language groups which ensure every campaign is co-designed, not imposed.

Customer Experience
Activate a 'weekly pain-point pulse' reporting system through which the CX team approaches every user interaction from the perspective of empathy-centered listening and then shares with the larger team a quick weekly summary of the top 3 recurring user concerns across support —especially those tied to trust, confusion, or fear, making the CX team a real-time feedback provider.

Business Development & Sales
Prioritize BD deals with partners that users already trust: religious networks, women's cooperatives, telecom agents. This trust by association accelerates adoption.

Product Development
Design product journeys for different digital comfort levels, such as a mode with minimal screens for returning users and a different mode with added guidance for new or low-literacy users. Additionally, Many users drop off because they get overwhelmed or need time to decide. Build in safe exit points, reminders, and soft re-entry cues into the savings journey.

Compliance
Add a "Do you feel your savings are safe with us?" prompt after savings transactions, especially in high-risk areas—treat perception as a compliance metric.

VI. Conclusions

What did we learn?

Conclusions

- **Inductive analysis of digital trust across four countries manifested four common pillars**, which statistically clustered into three archetypes.

- **In this Nigerian sample, 47% were in the Assurance Seekers cluster.** These are users who are the most unclear about who holds responsibility for their digital safety. It is also striking that many Assurance Seekers talk about "cautious sharing" as a risk mitigation strategy. They talk about "cautiousness" in a way that suggests using digital in a minimal way.

- **Conversely are Control Seekers, which are 36% of this sample.** These users are also most concerned about account hacking but more express, more than any other archetype, that they are responsible for their own digital safety. They also talk about "cautious sharing" but, as opposed to Assurance Seekers, "cautious" means making sure they have digital solutions set up to protect them.

- **Seventeen percent of this sample are Protection Seekers.** These users recognize risks but feel an institution, i.e. the provider, should protect them.

- **Across all archetypes, the main benefit of digital is felt to be Income Enabling while the main risk is felt to be Account Hacking.**

- With these three different archetypes dominating the Nigerian landscape, what are digital financial providers to do to grow trust with both? By using details of all three archetypes, each institution was able to brainstorm solutions that would serve each **across their various departments**.

Annex

A new analytical lense: **Assessing trust philosophies**

INDUCTIVE **USAGE**

- **Traditional segmentation**: Measures who is digitally active, and why.
- Most digital inclusion research uses inductive segmentation: grouping users by *who uses what*, *how often*, or *on which channels*—and then crafting interventions to move users "forward" on some digital journey.
- This approach is useful for mapping activity, but it reveals little about the *why* and *how* behind digital behaviors.
- Digital engagement is not only about access or skills. **It's fundamentally about trust**—how users perceive risk, build confidence, and decide to engage or withdraw.
- Inductive "usage" segments miss the *invisible architecture* of trust:
  - Two people might both use mobile money, but one does so only after triple-checking with their bank and friends, while the other simply accepts things as they are.
  - Standard segments would group these two together, missing the *radically different trust philosophies*—and, therefore, the different types of support they need.

INDUCTIVE **ANALYSIS**

- Inductive analysis unearthed *not usage profiles*, but ***trust philosophies*** shaping every digital action, risk, and expectation.
- Inductive segmentation makes the digital landscape look flat**. Trust philosophy segmentation** reveals its contours. Each group looks similar on the surface, but their risk perceptions, barriers, motivators, and intervention needs are fundamentally different.

Our approach is **different**

We started by listening for how users *perceive*, *manage*, and *act upon* trust and risk, capturing responses in four critical areas:

Risk Perception

What are people truly worried about? (e.g., hacking, scams, failure, theft)

Risk Mitigation

What do people *actually do* to protect themselves? (e.g., external confirmation, cautious sharing, monitoring)

Responsibility Perception

Who do they believe should keep them safe—institutions, platforms, themselves, or others?

Risk Mitigation

What makes digital services worth the risk? (e.g., time saved, income, ease, safety)

- By collecting data across these four windows into their lived realities, we ran a cluster analysis that looks beyond what people do and reveals *how* and *why* different people *trust*.
- The method uncovers *natural groupings*—segments are not forced, but emerge based on patterns in how people weigh risk, take precautions, assign responsibility, and see value.
- Each cluster is a **distinct trust profile**: Not just a behavioral group, but a reflection of a deeper, guiding trust philosophy—
  - Some users only trust after actively checking and verifying.
  - Others simply accept digital risk as a fact of life.
  - Another group pursues inclusion on their own terms, by taking personal control.
- By identifying these unique trust and risk management philosophies, practitioners and designers can build interventions, protections, and communications that resonate—"speaking the language of trust" that users actually use.

Annex

Analysis steps

MULTI-DIMENSIONAL **DATA INTEGRATION**

1

We systematically synthesized respondents' open-ended responses to questions across four core dimensions: *Risk Perception, Risk Mitigation Behaviors, Responsibility Perception and Benefit Recognition. This ensured a holistic capture of trust-related attitudes and behaviors.*

THEMATIC ANALYSIS – **SYSTEMATIC INDUCTIVE CODING**

2

Using iterative, grounded coding techniques, we inductively identified thematic categories and subcategories across all four pillars. This qualitative approach unraveled not only surface concerns but also latent, recurrent themes embedded in diverse user experiences.

LATENT PROFILE DERIVATION through **QUALITATIVE COMPARATIVE PATTERNING**

3

We conducted cross-sectional pattern analysis across coded data to qualitatively derive emergent trust profiles, identifying meaningful clusters of respondents based on distinct patterns of trust formation, risk response, and benefit expectation.

EMPIRICAL VALIDATION VIA **AGGLOMERATIVE CLUSTER ANALYSIS**

4

To validate and solidify the qualitative typology, we employed agglomerative hierarchical clustering to empirically test the robustness and reproducibility of the emergent clusters along the full suite of coded variables.

Why did we choose the four factors we did to define our trust philosophies?

Risk Perception

Trust begins with awareness. People's readiness to use digital tools depends on what dangers they foresee, whether that's hacking, scams, or technical failures. Mapping risk perception allows us to capture ***why* some users hesitate while others proceed**—revealing the emotional and cognitive triggers that open or close the door to digital adoption.

Risk Mitigation

Trust is more than belief; it is enacted through daily choices. By examining risk mitigation strategies—like cautious sharing and external verification—we get granular insight into ***how* users translate their fears or confidence into practice.** This dimension reveals not just theoretical trust, but trust-in-action.

Responsibility Perception

Trust is deeply social and institutional. Whether users trust a system often hinges on ***who* they believe is accountable for security**—banks, government, platforms, or themselves. By including responsibility perception, we surface the implicit contracts and expectations that frame people's willingness to engage.

Risk Mitigation

Trust is not only about reducing risk, but about pursuing value. Users weigh risks against perceived benefits: income opportunities, convenience, safety, or cost savings. This dimension grounds trust in lived realities and practical utility—capturing ***why* digital services are worth the leap of faith**.

DECODIS

Social Research. Reimagined.

linkedin.com/company/decodis

@decodisresearch

@decodisresearch

info@decodis.com

www.decodis.com