DECODIS

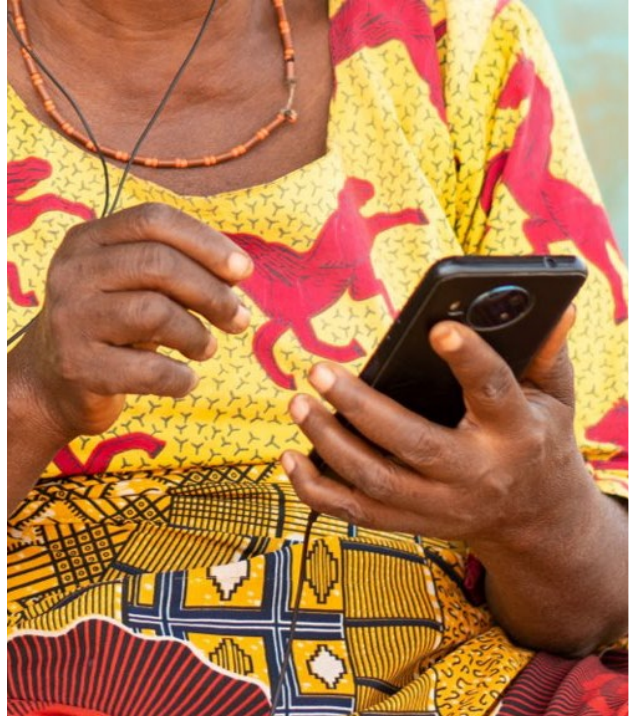
HENRY J. LEIR INSTITUTE
ADVANCING HUMAN SECURITY

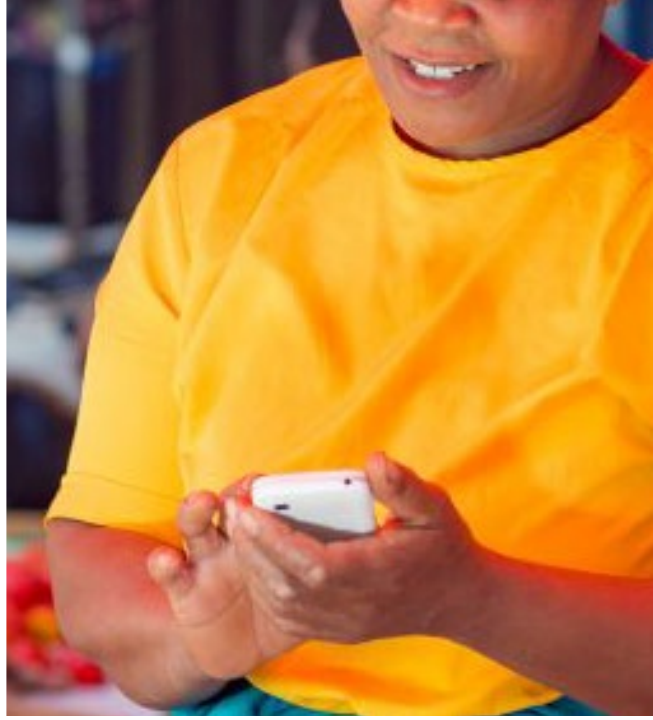
Digital Portfolios of the Poor

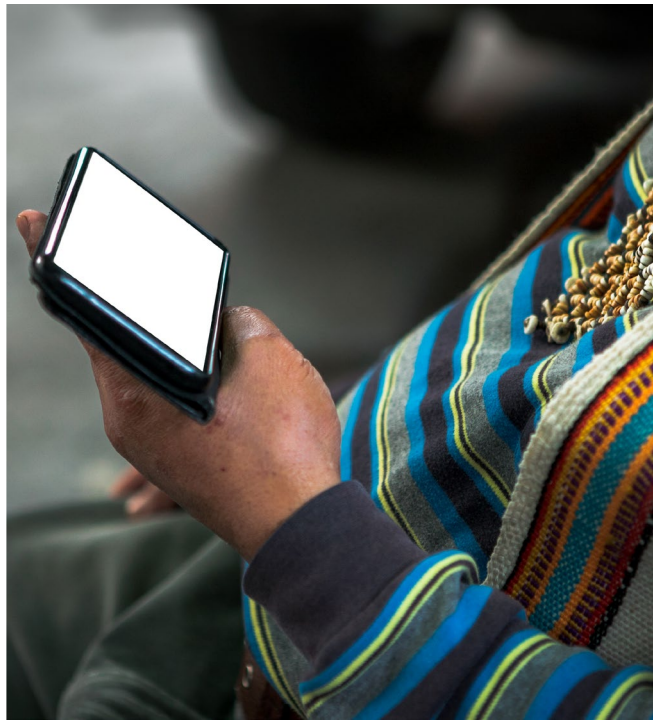
Digital Trust Philosophies

Cross Country Results Across Kenya, Nigeria, Pakistan and India

May 2026







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.

Objectives of the Digital Philosophies of Trust study

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

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 3,300 respondents.
- 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

3,300 people across 4 countries

Kenya, Nigeria, India and Pakistan

6 survey modules
on avg for each country

1,080 total hours
of voice data collected

188 voice response questions
on avg in each country

120 keypad response questions
on avg in each country

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.

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.

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

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

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 use digital services at all?

PILLARS OF DIGITAL TRUST

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

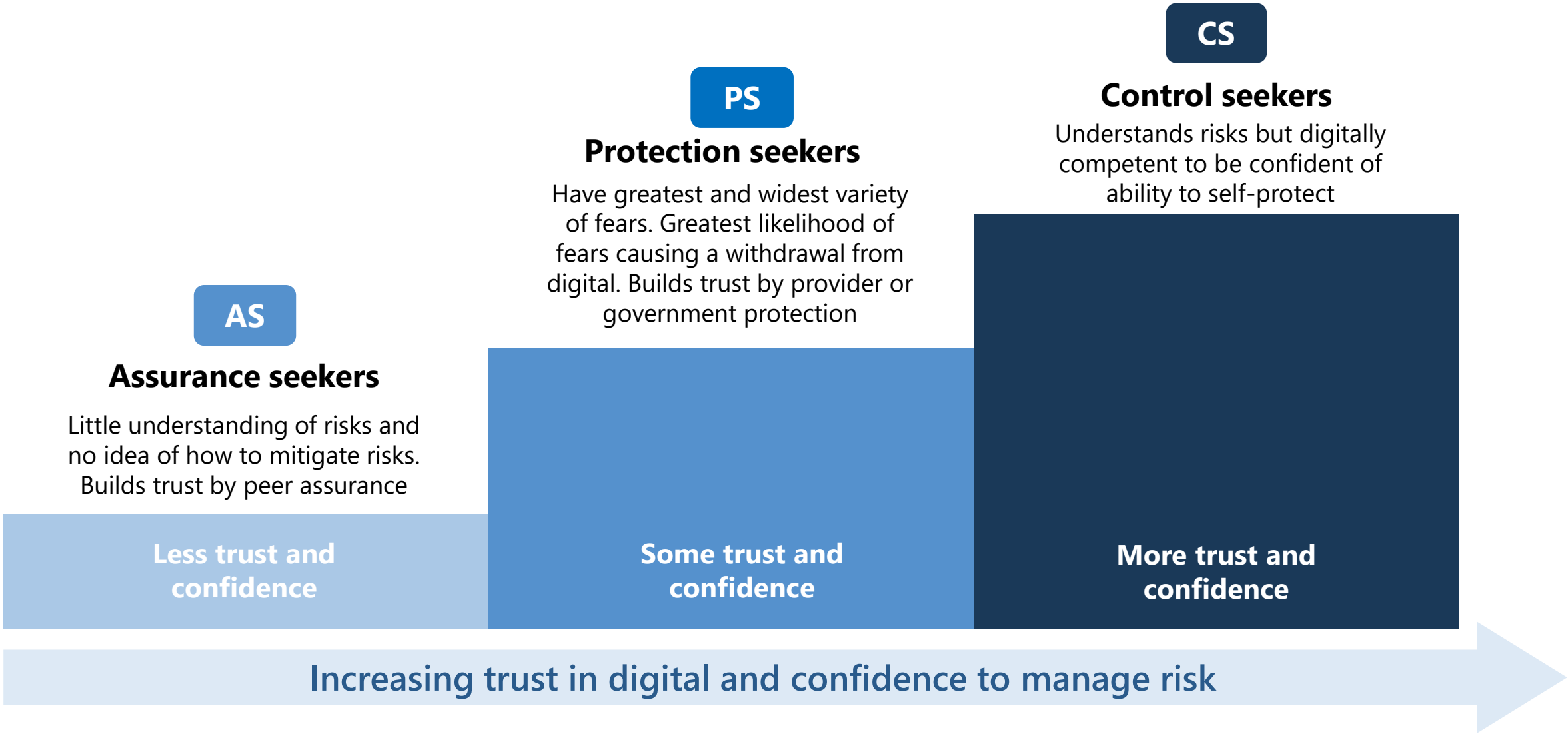
We extract themes of trust "inductively", which means they are **determined based on what respondents said** and not by forming hypothetical themes and looking for those in the data.

We derive four key pillars of trust grounded in participants' own words.

These pillars of digital trust are the same across all countries in the study, though sub-themes can change by country to reflect different market landscapes, demographics, and socio-economics.

Using this data, we perform cluster analysis to generate archetypes.

A set of globally-relevant Digital Trust Philosophy archetypes



Globally-relevant Digital Trust Philosophy archetypes

Built on country-specific foundations

	AS Assurance seekers	PS Protection seekers	CS Control seekers
KENYA N=992	**39%** of country sample 	**1%** of country sample 	**60%** of country sample 
NIGERIA N=953	**47%** of country sample 	**17%** of country sample 	**36%** of country sample 
INDIA N=939	**50%** of country sample 	**38%** of country sample 	**12%** of country sample 
PAKISTAN N=406	**40%** of country sample 	**38%** of country sample 	**22%** of country sample 
	A core feature across Assurance Seekers in all four countries is being unclear or unable to articulate who is responsibility for their digital safety. This archetype is the majority in India and Pakistan.	In Kenya and Nigeria, very few of the sample are in the Protection Seeker archetype. In India and Pakistan, there are striking similarities: for both, verification is the key risk mitigation strategy, and convenience is the key benefit.	More than half of the Kenyan sample are in this archetype, with Nigeria with one-third. However, their digital concerns are very different, with Kenyans focused on harassment of women online, while Nigerians are concerned about account hacking.

Workshops with Kenyan and Nigerian DFS providers testing the effectiveness of the Digital Trust Philosophy archetypes to develop solutions

Objective

Help institutions to develop easy solutions to build trust across archetypes and provider teams

Results

A range of solutions:

- **Across the archetypes:** Solutions for all archetypes will be more effective at growing customer trust than catering to only one.
- **Across organizational areas:** Because there are constant projects and priorities happening across provider teams, there needs to be multiple solutions for at least some to enter the project pipeline.

Workshops with Kenyan and Nigerian DFS providers to test the effectiveness of the Trust Philosophy archetypes to develop solutions

Objective

Help institutions to develop tractable solutions to build trust across archetypes.

Foundational principle in these workshops:

Solutions for multiple archetypes increases trust for all.

Earn trust by layering in solutions across the organization.

Kenya

SACCOs

- Bottom of the pyramid savings and loan institutions that are starting to digitize

Nigeria

- A payments product
- A digital-first bank
- A savings group fintech

Examples: Multiple solutions across many teams

Kenya: SACCO

- **Legal/Compliance:**
  - In-app dispute clarity button linked to CRM
  - Members can track/clear loan issues seamlessly
- **Branch/Finance:**
  - Flexible repayment options (daily/weekly)
  - Apple Store-style genius bar for hands-on support
- **Customer Experience**
  - Community Q&A support button
  - App-based loyalty / referral incentives
  - Offline access and local reassurance are essential for vulnerable members

Nigeria: Payments

- **Compliance:** Safety-check prompts after each saving — user feeling is a metric.
- **Leadership:** Track and report a User Trust Index as a board-level priority.
- **Customer Experience:** Weekly feedback pulse ensures smooth, uninterrupted interactions.
- **Business Development:** Leverage everyday trusted networks for distribution and uptake.
- **Product development:** Layered journeys with guidance for new users and safe, simple paths for all.
- **Marketing:** Co-create campaigns with real users, leveraging their lived trust deficits.

Conclusions

- **There is no monolithic digital trust philosophy, even within countries or segments.** Even if countries have a higher proportion of an archetype, all could be found.

- **A new methodology generates qualitatively informed at quantitatively-sized samples.** This format of data was critical to identifying a cross-country set of four trust pillars that still reveal sub-themes that were specific to supply-side and socio-economic differences within countries.

- **Archetypes ranged from confused to confident.** India and Pakistan have the highest percentages of "foggy" users, but even Kenya and Nigeria have sizable shares. Likewise, Kenya and Nigeria have higher percentages of confident users, but India and Pakistan have a small proportion as well.

- **Provider workshops generate multiple tractable solutions across organizations, suitable to serving all archetypes of customers.** Working with concrete archetype examples, audios and other materials galvanize trust-building ideas but also enable shorter workshops where senior people can participate. It is critical to involve senior level managers who have the internal weight to bring ideas to reality.

Annex

A new analytical lens: Assessing trust philosophies

- 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 unearths *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 start 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?
- Benefit perception: 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.

Analysis steps

1. **Multi-dimensional Data Integration:** We systematically synthesize respondents' open-ended responses to questions across four core dimensions: *Risk Perception, Risk Mitigation Behaviors, Responsibility Perception and Benefit Recognition. This ensures a holistic capture of trust-related attitudes and behaviors.*

2. **Thematic Analysis – Systematic Inductive Coding:** Using iterative, grounded coding techniques, we inductively identify thematic categories and subcategories across all four pillars. This qualitative approach unravels not only surface concerns, but also latent, recurrent themes embedded in diverse user experiences.

3. **Latent Profile Derivation through Qualitative Comparative Patterning:** We conduct 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.

4. **Empirical Validation via Agglomerative Cluster Analysis:** To validate and solidify the qualitative typology, we employ agglomerative hierarchical clustering to empirically test the robustness and reproducibility of the emergent clusters along the full suite of coded variables.

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

1. **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.

2. **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.

3. **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.

4. **Benefit Perception:** 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