DECODIS

HENRY J. LEIR INSTITUTE
ADVANCING HUMAN SECURITY

Digital Portfolios of the Poor

Philosophies of Trust in Digital Channels

India

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. In India, this pattern manifests itself in digital payment solutions, especially among women.
- 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 939 Indian men and women across a range of northern and southern Indian 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.
- Half of this Indian sample were revealed to be Assurance Seekers, the least aware and confident users of digital tools; 12% were Control Seekers, the most aware but also the most confident. The remaining 38% were Protection Seekers, aware of digital risks but unsure of how to protect themselves.
- 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 India, a particular feature of the results was a difficulty articulating a perspective about risk mitigation or responsibility, especially among the Assurance Seekers. These respondents speak as though they might have heard something but could not provide their own perspective.
- Another key differentiator in India was, across all archetypes, Convenience was cited as the most common benefit, as opposed to market reach, for example, in Nigeria and Kenya.

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

On this skit, Rajeev gets an SMS saying he won INR 10,000 in a lottery prize. His uncle warns him the message is a scam.

CTRL+click on the image to see online

Listen to the Indian Cybersecurity Scenario in Hindi

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

RESPONSE EXAMPLE

See example of a response in Hindi.

If I were Rajeev, I would first check that message and ask knowledgeable people whether this message is fake or there is something true about it. Only after that I would have taken some action, and I might not even take any action. This is because money is not available for free, so I would only believe it if I could check that it is true. (Woman)

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 939.
- Long, meaningful answers. 3x longer responses than in a typical in person interview.[1]

939 people interviewed in India

8 survey modules

340 hours
of voice data collected

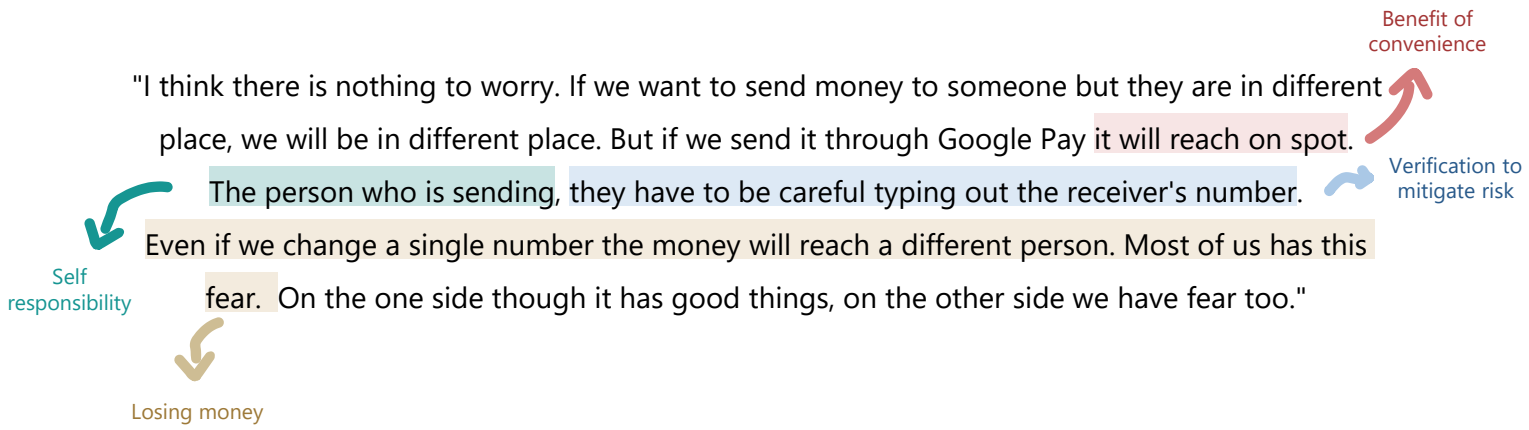
191 voice response questions

113 keypad response questions

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

Data analysis: Inductively identifying themes using grounded theory

Example of response Decodis gets and how we categorize



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 the prompt for a machine learning model to search the data.

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

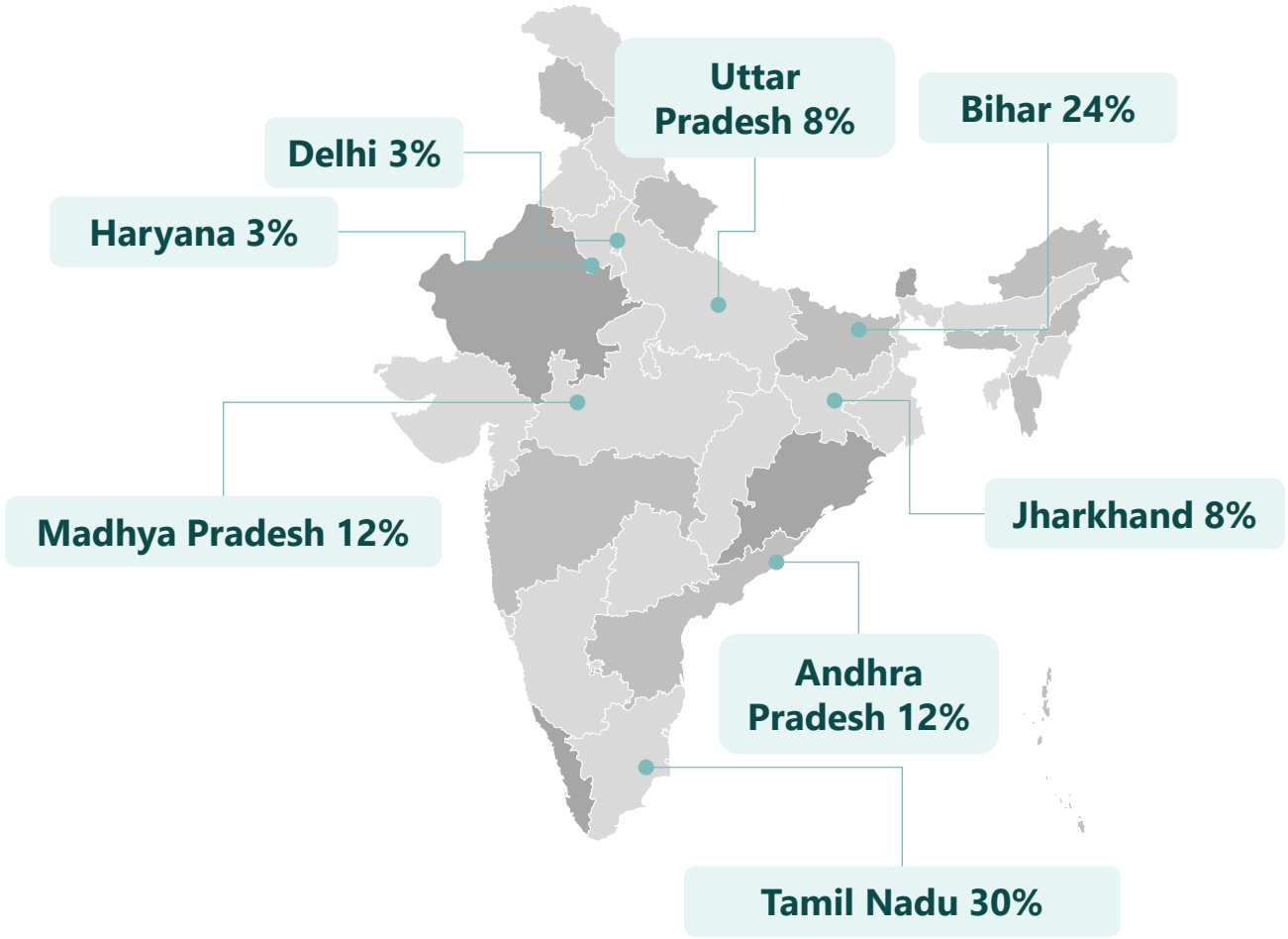
We do extensive iteration, improving the prompt and specificity of theme-tagging.

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 India

Indian sample: Geographies and Languages



Key survey facts

- **Sample size**: 939 people
- **Languages**: Hindi, Tamil and Telugu
- **Data collection:** April 2024

52%
Women

46%
21-30yrs

Research Partner: Gram Vaani

India: Phone access and ownership

Reportedly high ownership[1], but more than half share any type of phone.

Reported Access v. Ownership	Smartphone	Feature phone	Basic phone	No access to a phone
N	832	93	93	27
Access to each type of phone	82%	9%	9%	3%
Ownership of each type of phone	71%	8%	7%	-
|→ Owners who need to share phone	52%	54%	56%	-

[1] Many respondents say they 'owned" their phones, but ownership has different definitions.

Much access to smartphones, high reported ownership, lots of sharing

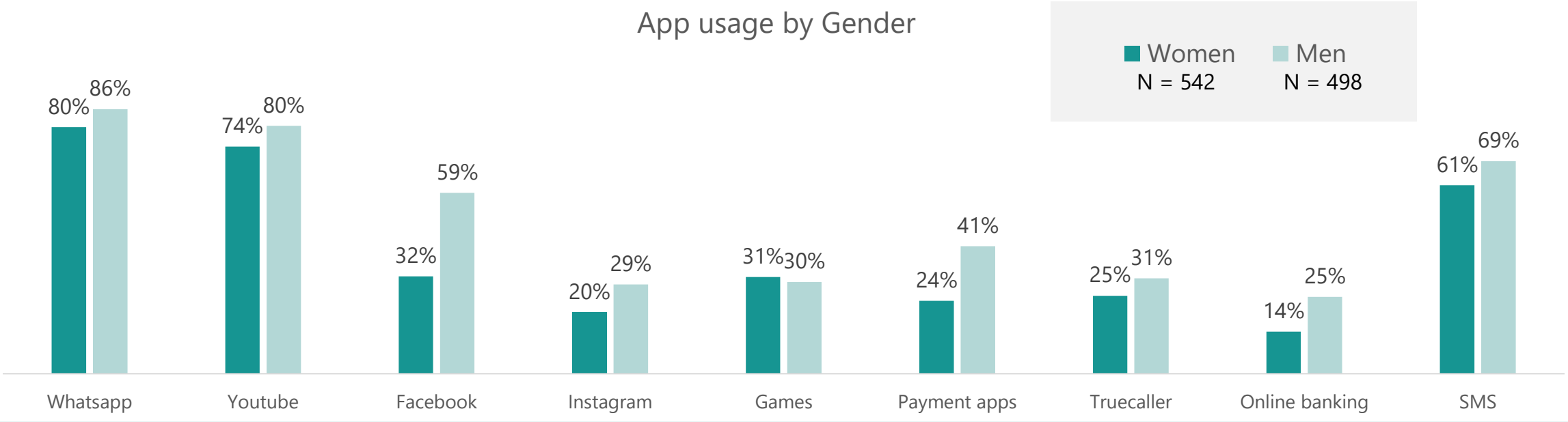
It was not easy to find a household without access any type of phone, but of a sample of 1045, 3% do not have access to a device.

Of the others, most had access to a smartphone. Of those with access to a smartphone, 71% 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.

More surprisingly, 40% 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.

Indian sample: 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 expected, the percentage of men using payments or online banking is low, with the percentage of women even lower, compare to an otherwise robust portfolio of app usage.
- Apps for communication and entertainment (i.e. WhatsApp and YouTube) are used by a similar percentage of women as men.
- However, those apps used for posting, like Facebook, are used by half as many women as men.

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
Scams	Respondents worry about online frauds that could steal their money or information.
Image misuse	Users fear their photos being manipulated or shared without consent for blackmail or humiliation.
Digital literacy	People do not fully understand digital tools, which makes them worry about losing their money.
Cannot articulate risks	No identification of specific risks, feeling no need to worry.

Though the pillars are consistent across countries, the sub-themes that underpin them are different, reflecting a range of macroeconomic, market and population factors.

1 1a

Sub-themes that define Risk Mitigation

B Risk Mitigation

Variable Name	Definitions
Verify	Users double-check messages and transactions, confirm receipts before sending goods, use passwords and pins, block or delete suspicious contacts and report problems.
Avoid	Users stay away from uses they are nervous about. They prefer not to engage rather than take a chance on suspicious interactions.
Cannot articulate an action	Users find it difficult to articulate risk-management steps or suggest that no action is necessary.

Though the pillars are consistent across countries, the sub-themes that underpin them are different, reflecting a range of macroeconomic, market and population factors.

1 1a

Sub-themes that define Responsibility Perception

C Responsibility Perception

People's readiness to trust digital channels depends on who they believe is protecting them from risks.

Variable Name	Definitions
Self & Community	Protection-seekers feel they must **rely on themselves** and their community to ensure digital safety while assurance-seekers similarly depend on their community but **view family and friends as natural, trusted vetters.**
Government	Respondents believe the government handles catching and punishing digital fraudsters after a report is made.
Platforms	Users express **blind trust in platforms** without any concern.

Though the pillars are consistent across countries, the sub-themes that underpin them are different, reflecting a range of macroeconomic, market and population factors.

1 1a

Sub-themes that define Benefit Perception

D Benefit Perception

The benefits that people receive that pulls them towards digital.

Variable Name	Definitions
Convenience	Digital services allow convenient, 24/7 transactions from anywhere, saving travel time and making payments quick and easy.
Increased income	Digital tools open opportunities to generate income and support their families through work from home.

Though the pillars are consistent across countries, the sub-themes that underpin them are different, reflecting a range of macroeconomic, market and population factors.

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

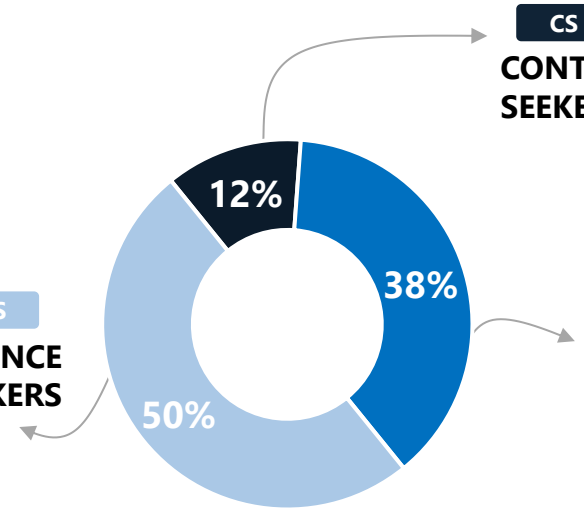
Control seekers

Digitally competent and confident in their ability to self-protect

A set of globally-relevant of Trust Philosophy archetypes

Archetypes in India

N=939



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.

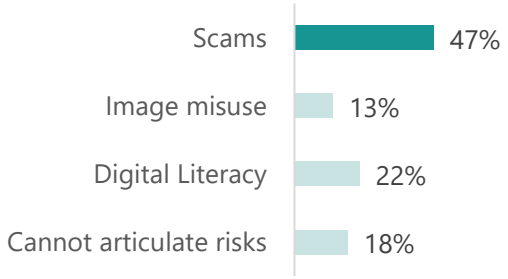
Online risks exist, like data theft or photo misuse, so we must be careful. If something goes wrong, we should act quickly by asking friends first and then going to the bank or cybercrime authorities for help.

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.

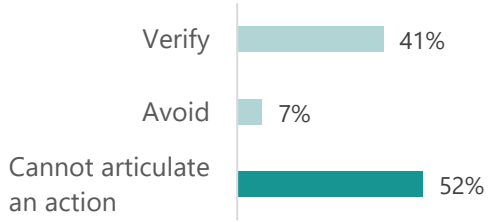
Assurance Seekers: Attributes

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

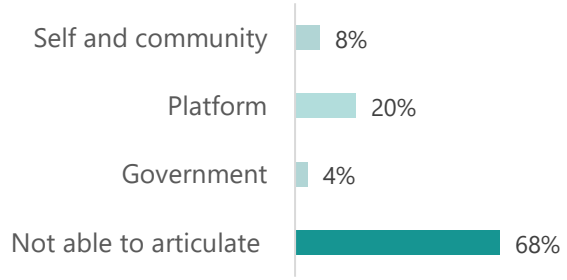
A Risk Perception



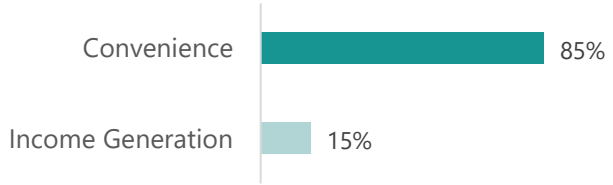
B Risk Mitigation



C Responsibility Perception



D Benefit Perception



AS ASSURANCE SEEKERS
50% of the sample

- 54% of women in the sample are Assurance Seekers, the highest of all archetypes.
- 60% of Assurance Seekers say they must share their phones.
- 76% of Assurance Seekers have access to a smartphone, the lowest of all archetypes.
- Benefits are focused on convenience.
- Trust is tentative, being unsure of who bears the responsibility of protection
- Risk of financial scams is expressed as a fear that someone will steal from their mobile money accounts.

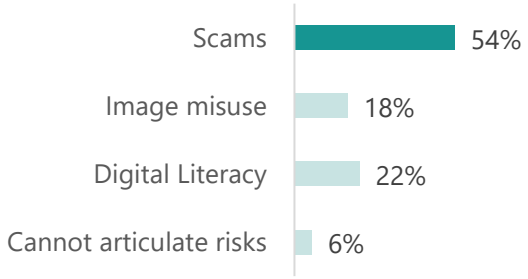
"However, Facebook brings many problems and instances of harassment. We must plan ahead about how to deal with such dangers. Most harassment happens through inappropriate messages or calls. We shouldn't panic; instead, **we should stay brave and seek help from the right people or from cybercrime authorities."**

GI_tam_u0165_QF2_05

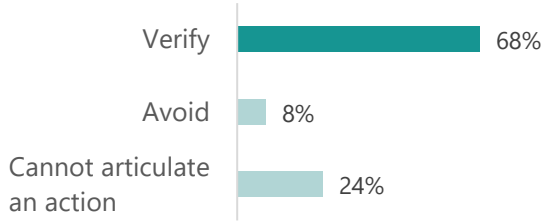
Protection Seekers: Attributes

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

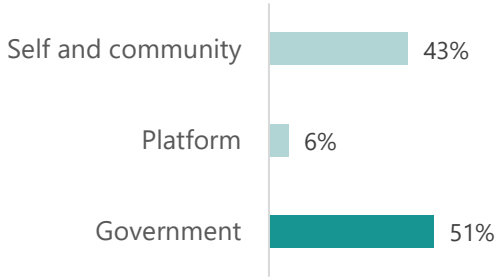
A Risk Perception



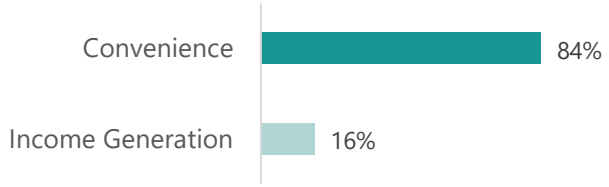
B Risk Mitigation



C Responsibility Perception



D Benefit Perception



PS PROTECTION SEEKERS
16% of the sample

- 38% of women are Protection Seekers.
- 89% have access to smartphones.
- 57% say they need to share the phone.
- They are deeply embedded in their digital lives, especially in using social media for business
- Given their deep engagement in the digital world, they are most concerned about harassment
- They seem confident but many desire the government to protect their safety online.
- They value consistent experiences and low-effort protections that don't interrupt their routines.

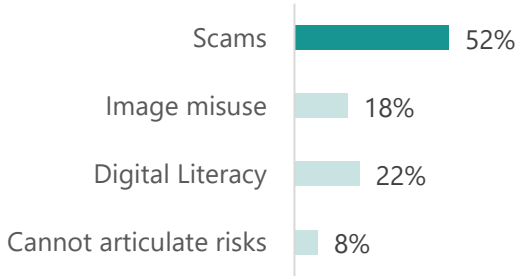
"Yes, sometimes there's uncertainty about whether **customers will actually pay or not. But digital platforms have made things easier and more reliable**. People trust them now. Payments and products are properly recorded through end-to-end messages, which is a great advantage."

GI_hin_u0950_QF2_03

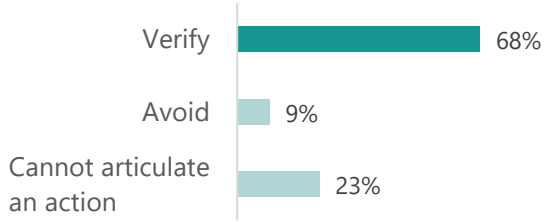
Control Seekers: Attributes

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

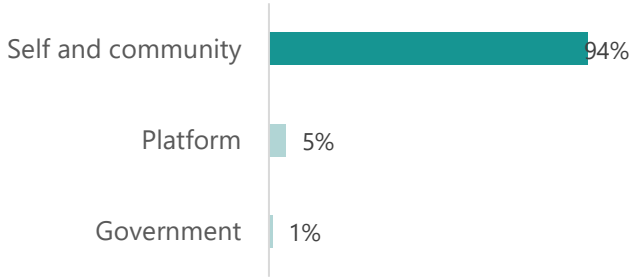
A Risk Perception



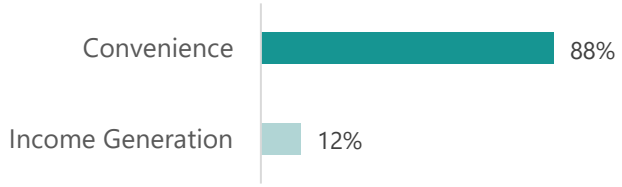
B Risk Mitigation



C Responsibility Perception



D Benefit Perception



CS CONTROL SEEKERS
12% of the sample

- Only 12% of women are Control Seekers
- 88% have access to smartphones
- 52% say they need to share the phone
- High use of mobile payments
- Types of scams are mostly expressed through concern of someone stealing from their mobile wallet
- Many use WhatsApp for business use and use digital loans
- Digitally assertive, highly intentional, they trust only themselves to stay safe.

"Nowadays, **platforms like Flipkart, Amazon, and others offer both prepaid and cash-on-delivery options, which helps ensure customers aren't cheated.** If something goes wrong, full transaction details are available, allowing the police to investigate if needed. Digital banking has progressed, and money transfers through apps are safe, making physical cash less necessary."
GI_hin_u1017_QF2-03

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. 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 Indian sample, about half were in the Assurance Seekers cluster. These are users who are least aware of digital risks and depend on recommendations and help from their community to help them navigate these risks. It is striking that many Assurance Seekers are not able to articulate what risks they feel are prevalent and who should have the responsibility for protecting them in their digital lives. These are users who are engaging in their digital lives by rote action, pressing buttons they know and asking others to help them.
- At the other end of the scale are Control Seekers, which are 12% of this sample. These users are fully aware of digital risks, know how to mitigate them and express confidence about being able to do so. First and foremost, they hold themselves responsible for protecting themselves and suggest that others should learn to do so themselves.
- Thirty-eight percent of this sample are Protection Seekers. These users recognize risks but feel an institution should protect them. In India, this tends to be the government.
- Across all archetypes, the main benefit of digital is felt to be Convenience while the main risk is felt to be Scams.

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