DECODIS

HENRY J. LEIR INSTITUTE
ADVANCING HUMAN SECURITY

Digital Portfolios of the Poor

Philosophies of Trust in Digital Channels

Pakistan

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 406 Pakistan men and women
- 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.

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.
- Forty percent of this Pakistani sample were revealed to be Assurance Seekers, the least aware and confident users of digital tools; 22% were Control Seekers, the most aware and 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.
- In Pakistan, a particular feature was the difficulty articulating a perspective about risk mitigation or responsibility, especially among Assurance Seekers, who were entirely unable to identify who is responsible for protecting them and could only describe their approach to risk as learning slowly over time.
- Another key differentiator in Pakistan was that across all archetypes, convenience was cited as the most common benefit among Protection and Control Seekers, while Assurance Seekers were primarily motivated by easy communication, as opposed to market reach, for example, in Nigeria and Kenya.
- Last, in Pakistan, more than in other countries, agents were seen as a key party responsible for protection, especially among Protection Seekers, while Control Seekers stood apart in their strong belief in personal responsibility, with the majority also denying that any significant digital risk exists.

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

In this skit Zara, confides in her friend Asma about a shopkeeper exploiting her by charging unauthorized fees and pressuring her during stipend collection, and Asma urges her to file a formal complaint despite her fear of retaliation.

Listen to the Pakistan Cybersecurity Scenario in Urdu

RESPONSE EXAMPLE

Listen to a response in Urdu.

I think that when a person does this kind of work, they should have privacy on their account. If you have privacy, then you won't have any issues, and you can work online as well. However, privacy on your account is very important.

GP_urd_u0609

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 406.
- Long, meaningful answers. 3x longer responses than in a typical in person interview.[1]

406 people interviewed in Pakistan

4 survey modules

356 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

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 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

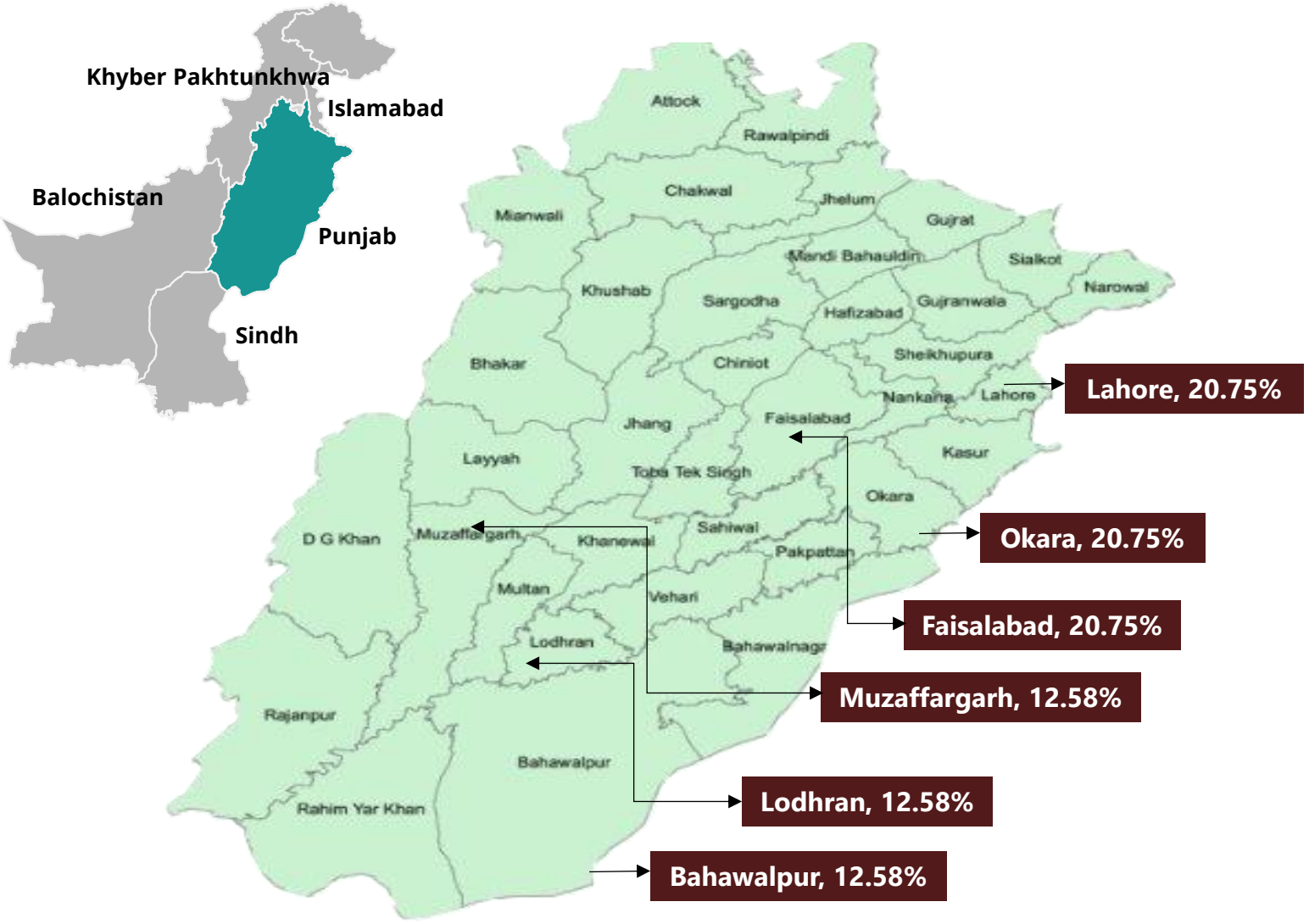
We do extensive iteration, improving the prompt and specificity of theme-tagging.

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

Pakistan sample: Geographies and Languages



Key survey facts

- **Sample size**: 406 people
- **Languages**: Urdu and Punjabi
- **Data collected:** December 2025

Pakistan sample: Demographics

66% Women

N = 406

60% 18-34yrs

N = 400

53% Rural

N = 400

As in other countries, the sample in Pakistan was selected to be:

- Two third women and one third men
- In the mid-range of age
- A mix between rural and urban

[1]Asked open-ended question, not all responses were categorizable

Pakistan: Phone access and ownership

75% have significant access to smartphones.

Reported Access v. Ownership	Smartphone	Basic phone
N	299	104
Access to each type of phone	74%	26%
Of those who have access, say they have possession of phone all the time	90%	75%

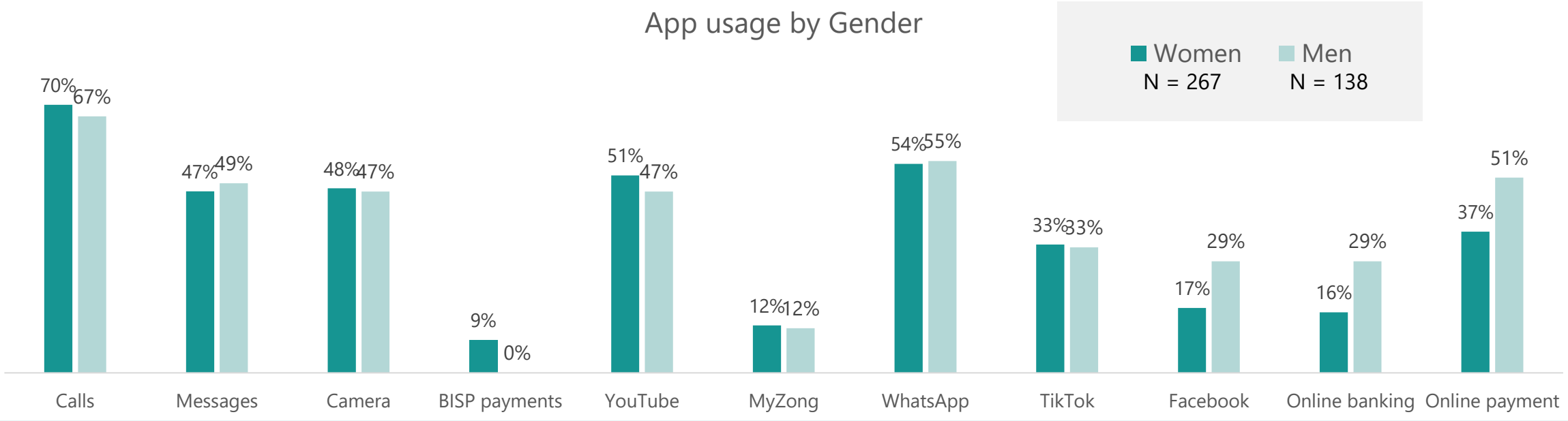
In other studies, we have asked whether women "own" the phone. However, we have found that "ownership" has inconsistent definitions. Many respondents implied that if they can use the phone, they feel a sense of "ownership." We therefore decided in this study to ask whether respondents usually have possession of the phone, which we felt is a more valid indicator of frequent engagement.

In this study, three quarters of the respondents had access to a smartphone, with the last quarter having assess to a basic phone.

Of those with access to a smartphone, most say they have possession of the phone all the time. Of those who have access to a button phone, only 75% have possession of the phone all the time.

This means that we have only a very small sample of three people who have minimal access to a basic phone.

Pakistan sample: Types of digital use by gender



As we found in our other countries, the percent of women use a range of apps is similar to men.

There are two exceptions:

- Social media app, Facebook, which is less well used by both compared to apps like YouTube and TikTok.
- Financial apps, especially online payments.

This pattern suggests once again that, for women, digital financial apps are a different territory compared to the rest of their online lives.

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
Agents	Respondents worry that trusting agents with their phone or account can create risk if those people misuse access.
Data misuse	Users fear their personal information can be misused to commit fraud in their name or to steal from them.
Own digital literacy	People do not fully understand digital tools, which makes them worry about losing their money.
No risk	Respondents say they have no concerns. *Note: Because of their speech intonations and the words they use, we believe respondent imply they have no knowledge of risk rather than implying that they know how to handle the risk.*

Though the pillars are consistent across countries, these sub-themes that underpin them are typically different.

This is to be expected, given different products, providers, and regulatory impacts.

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.
"Learn slowly"	Users believe in learning step by step through experience, observation, or guidance helps reduce fear and mistakes over time.
Seeking guidance	Respondents believe relying on trusted family members, especially educated children or relatives, helps protect them from making mistakes.
Cautious behavior	Respondents believe being careful, especially with agents, checking amounts, and watching transactions closely can reduce chances of being cheated.
Security measures	Respondents believe never sharing PINs, OTPs, CNIC numbers, or codes with anyone is the main way to stay safe.

Though the pillars are consistent across countries, these sub-themes that underpin them are typically different.

This is to be expected, given different products, providers, and regulatory impacts.

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
Personal	Respondents believe they themselves are responsible for being careful, protecting information, and avoiding mistakes while using digital services.
Agent	Respondents believe shopkeepers, agents, or service providers should guide users correctly and not misuse people's trust. *Note how agents are intertwined between notions of both trust and distrust.*
Platform	Respondents believe banks, mobile companies, and apps are responsible for keeping systems secure and protecting users from fraud.
Not able to articulate	With unclear ideas and wandering thoughts, respondents are not able to articulate who might be responsible for their digital safety, using intonations and words that suggest they had never thought about it.

Though the pillars are consistent across countries, these sub-themes that underpin them are typically different.

This is to be expected, given different products, providers, and regulatory impacts.

1 1a

Sub-themes that define Benefit Perception

D Benefit Perception

The benefits that people receive that pulls them towards digital.

Variable Name	Definitions
Easy communications	Respondents believe that digital tools make it easy to stay in touch with distant family and friends through video calls, chat apps, and other similar ways of communicating easily and instantly.
Convenience	Digital services allow convenient, 24/7 transactions from anywhere, saving travel time and making payments quick and easy.
Work opportunities	Respondents believe that the digital economy offers new ways to earn money or run businesses, for example, online jobs or home-based work.
Education and information	Respondents believe that digital exposure provides easy access to learning and information such as online courses or news. Respondents believe that they can quickly get news, weather or other important information online.

Though the pillars are consistent across countries, these sub-themes that underpin them are typically different.

This is to be expected, given different products, providers, and regulatory impacts.

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

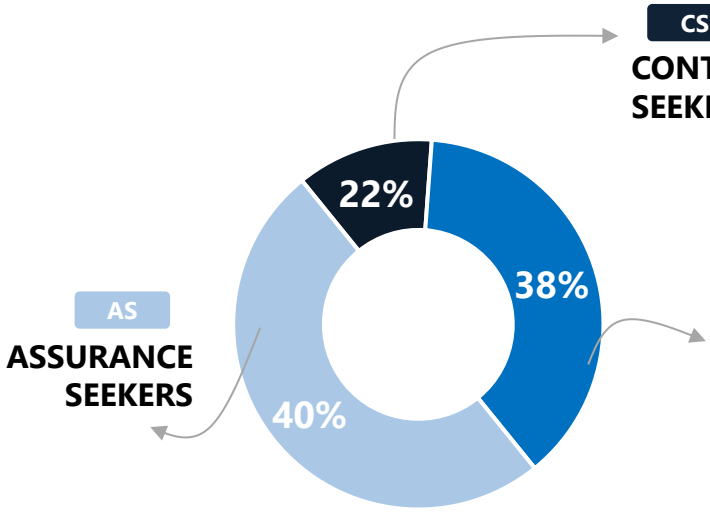
Control seekers

Digitally competent and confident in their ability to self-protect

A set of globally-relevant of Trust Philosophy archetypes

Archetypes in Pakistan

N=406



Respondents feel that they can take more responsibility for mitigating their digital risk. However, unlike other countries, their method is less sophisticated – they rely on manual verification to check about scams or to make sure payments go through. About a third still feel their lack of digital literacy put them at risk.

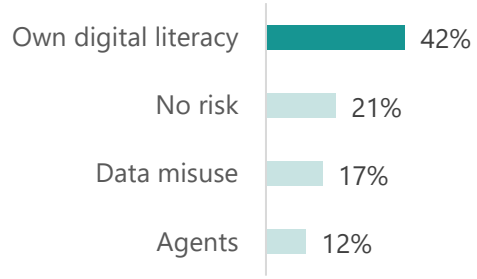
Like all the other archetypes, respondents feel that their own digital literacy is their biggest risk. Respondents try to mitigate that risk by "learning slow" in a step-by-step fashion from others. In terms of who should protect them, respondents' answers reflected confusion and surprise at the question.

Responsibility for keeping them safe is spread between themselves, the platform and agents, rather than mostly on themselves like Control Seekers. They also use verification to mitigate risks but also depend on using cautious behavior and seeking assistance.

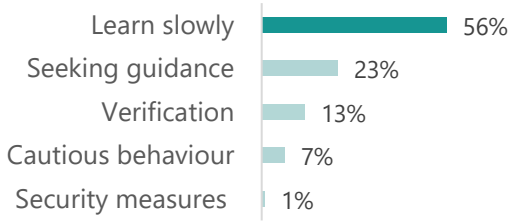
Assurance Seekers: Attributes

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

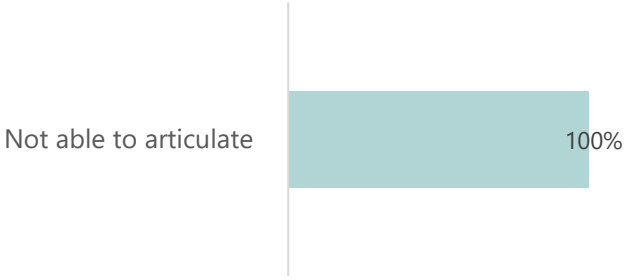
A Risk Perception



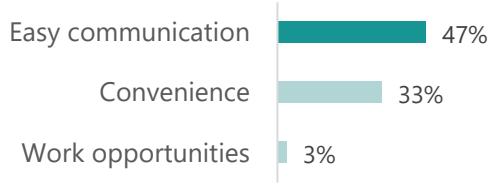
B Risk Mitigation



C Responsibility Perception



D Benefit Perception



AS ASSURANCE SEEKERS
40% of the sample

- 37% of Assurance Seekers have a basic phone, the largest of any archetype.
- 72% of Assurance Seekers are women.
- The biggest perceived risk is their own lack of digital literacy.
- The most common way to mitigate risk is to "learn slowly."
- Assurance Seekers are unable to conceive or articulate who is responsible for protecting them.
- The biggest perceived benefit is easy communication.

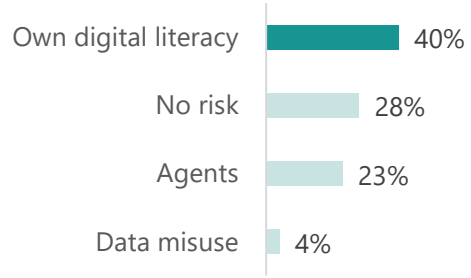
"Take care of yourself and consult someone wise who can understand the solution to this issue, which is development..."

GP_urd_u0633

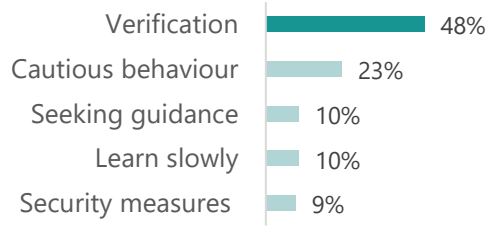
Protection Seekers: Attributes

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

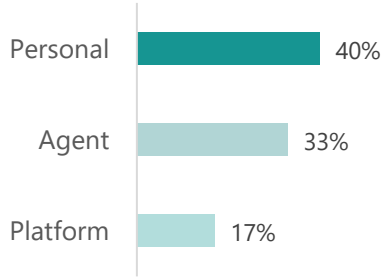
A Risk Perception



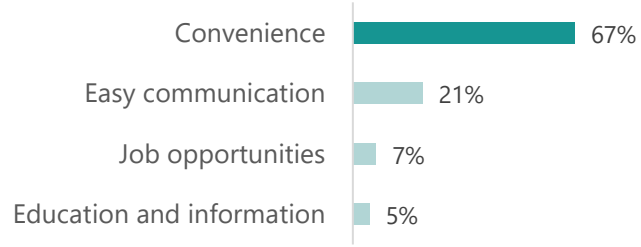
B Risk Mitigation



C Responsibility Perception



D Benefit Perception



PS PROTECTION SEEKERS
38% of the sample

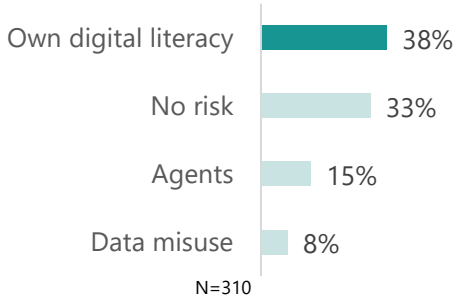
- 84% have access to a smartphone, the largest of any archetype.
- 67% are women.
- Like Assurance Seekers, the biggest perceived risk is still their own lack of digital literacy, but at a lower rate than Assurance Seekers.
- Protection Seekers see agents both a source of risk as well as someone that they need to rely on.
- They tend to mitigate risk through extensive verification behavior (see below).
- Their biggest perceived benefit is convenience.

> "For us, it is not called our own if the name is not shown with the bill. It needs to be verified in a way that when the bill arrives. The name on the bill should also be shown so that we can confirm it is indeed our bill. If the name needs to be confirmed, a notification should also be shown, similar to how it happens before making a payment transfer with OTP verification. If all these things are in place, it becomes easier."
> GP_urd_u0173

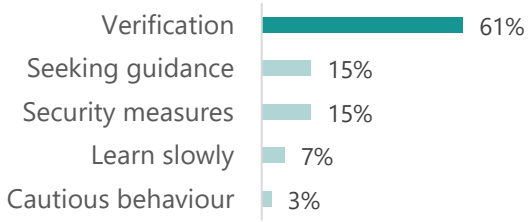
Control Seekers: Attributes

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

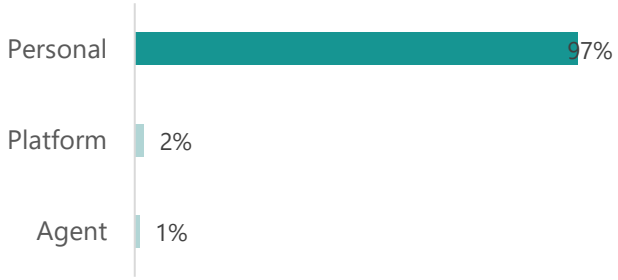
A Risk Perception



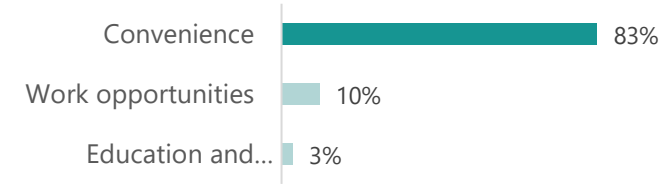
B Risk Mitigation



C Responsibility Perception



D Benefit Perception



CS CONTROL SEEKERS
22% of the sample

- 79% of Control Seekers have access to a smartphone.
- 62% are women, the smallest percent of any archetype.
- The biggest perceived risk is their own lack of digital literacy, though many also deny that any risk exists.
- Control Seekers have a strong sense of personal responsibility when it comes to mitigating risk.
- The biggest way they mitigate risk is through verification. See quote below.
- The biggest perceived benefit is, like Protection Seekers, convenience.

"One should proceed with honesty and not get involved in unnecessary matters [...]One should remember this and avoid unnecessary discussions. They should keep their work organized, update their ID card, and ensure that the necessary documentation is signed. Beyond this, nothing more can be discussed. "
GP_urd_u0182

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?

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 Pakistan sample, 40% were in the Assurance Seekers cluster. These are users who are least aware of digital risks and depend on learning slowly and seeking guidance from others to navigate them. It is striking that Assurance Seekers are entirely unable to articulate who should be responsible for protecting them in their digital lives. These are users 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 22% of this sample. These users are aware of digital risks, rely on verification to mitigate them, and hold themselves personally responsible for their own protection. First and foremost, they hold themselves responsible for protecting themselves, with 97% attributing responsibility to noone but themselves.

- Thirty-eight percent of this sample are Protection Seekers. These users recognize risks but rely on agents and personal responsibility to protect them. They use verification as their primary means of mitigating risk.

- Across all archetypes, the main benefit of digital is felt to be convenience, while the main risk felt is a lack of digital literacy. It is striking that two pillars were consistent across all archetypes. The other countries in this study had more variation.

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