DECODIS

Digital Portfolios of the Poor

India Findings

Decodis | May 2026

Summary

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.

Does this reflect a lack of digital trust?

We asked ourselves whether and how digital trust may be driving patterns in digital financial usage and whether it applies across applications and segments. The Digital Portfolios of the Poor project set out to understand the digital trust philosophies of low-income people in India, Kenya, Nigeria, and Pakistan.

For this research, 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.

To achieve this, surveys were collected through automated voice interviews conducted in local languages, with AI-powered qualitative analysis used to surface the motivations, frustrations, and emotions that surveys alone rarely capture.

Key findings are:

- Smartphone access was high at 82%, though more than half of owners reported needing to share their device with others in the household.
- WhatsApp and YouTube were the most widely used apps, with payment app and online banking use notably lower among women (28% and 16%) than men (44% and 30%), and Facebook use less than half as common among women as men.
- Three features distinguished India from the other countries:
    - Nearly 50% of the sample were unable to articulate digital risks or identify who was responsible for protecting them, speaking as if they had heard something about risk but could not form their own perspective.
    - Across the sample, convenience was the primary benefit cited — distinct from Nigeria and Kenya where market reach dominated.

- More than in any other country, respondents looked to the government as the primary party responsible for digital safety.

Sample and Methodology

The Indian findings draw on 939 respondents across eight states — Bihar, Tamil Nadu, Madhya Pradesh, Andhra Pradesh, Jharkhand, Uttar Pradesh, Haryana, and Delhi — surveyed in Hindi, Tamil, and Telugu. The survey comprised 8 modules, covering 191 voice response questions and 113 keypad response questions, with respondents also reacting to audio skits designed to draw out qualitative perspectives on trust in a depersonalized way.

Device Access and Ownership

82% of respondents had access to a smartphone, with 71% reporting ownership — the highest smartphone access rate across the four countries in the study. Feature phone and basic phone access were each at 9%. As in the other countries, ownership was a broad concept: many respondents described feeling a sense of ownership simply by virtue of regular access, and more than half of those who reported owning any type of phone shared it with others in the household. 40% reported access to two devices, though the degree of access to the second device was not measured.

	Smartphone	Feature phone	Basic phone
N	832	93	93
Access	82%	9%	9%
Ownership	71%	8%	7%
→ Owners who share phone	52%	54%	56%

Note: Ownership figures reflect self-reported data. Many respondents equated regular access with ownership. Sharing rates exceed 52% across all device types.

Application Use

WhatsApp and YouTube were the most widely used applications, with broadly similar rates between men and women. The most striking gender gap was in Facebook use — used by 34% of women compared to 58% of men — which may reflect greater concern among women about public visibility and reputational risk online. Payment app and online banking use was notably lower among women (28% and 16%) than men (44% and 30%) despite broadly comparable levels of communication and entertainment app use, suggesting that the gender gap in digital financial services is not primarily a question of device access or general digital confidence.

Application	Women	Men
WhatsApp	76%	84%
YouTube	68%	78%
Facebook	34%	58%
Instagram	22%	32%
Games	18%	36%
Payment apps	28%	44%
Online banking	16%	30%
SMS	55%	62%

Trust Archetypes

The findings revealed three statistically distinct digital trust archetypes, derived from an inductive analysis of how respondents described their own experiences across four pillars: Risk Perception (what dangers people foresee), Risk Mitigation (how they act on those fears), Responsibility Perception (who they hold accountable), and Benefit Perception (why they engage with digital tools at all).

Control Seekers are the most digitally confident group. They are fully aware of digital risks, know how to mitigate them, and express confidence in their ability to do so. They hold themselves primarily responsible for their own protection and tend to believe others should take the same approach. They are the heaviest users of smartphones and a wide range of digital financial services, and value digital tools above all for the market reach and business opportunities they unlock.

Assurance Seekers have the most limited awareness of digital risks and are often unable to articulate specific threats or identify who should be responsible for their protection. They engage with digital tools by habit rather than by informed choice, relying on family, friends, and community networks for guidance when things go wrong. Their engagement with digital tools is anchored in basic financial access and inclusion.

Protection Seekers are aware that digital risks exist — including scams, harassment, and image misuse — but feel uncertain about how to protect themselves. Rather than self-protecting, they look to an institution — a government, regulator, or platform — to bear primary responsibility for their safety online. Despite their concerns, they remain engaged in digital life and value the convenience and opportunities that digital tools provide.

Trust Archetypes in India Compared to Other Countries

India had the highest share of Assurance Seekers of all four countries (50%) and the lowest share of Control Seekers (12%), placing it at the least confident end of the four-country trust spectrum. Its 38% Protection Seeker share — the joint highest alongside Pakistan — reflects a substantial portion of users who are aware of risk but look primarily to external institutions, and especially to government, for protection. Across all countries, the same four pillars underpinned the archetypes, though the specific fears, behaviours, and benefits that defined each pillar differed significantly by country context.

Country	Assurance Seekers	Protection Seekers	Control Seekers
Kenya (N=992)	39%	1%	60%
India (N=939)	**50%**	38%	12%
Nigeria (N=953)	47%	17%	36%
Pakistan (N=544)	40%	38%	22%

Key India-Specific Findings

Risk Perception: Scams, Image Misuse, and Digital Literacy

Indian respondents articulated three primary risk categories. Scams — fraud, fake schemes, and deceptive messages designed to steal money or account information — were the most widely cited concern across all archetypes. Image misuse was a distinctly prominent concern in India compared to other countries: users, particularly women, feared their photos being manipulated or shared without consent for blackmail or humiliation. This risk shaped online behaviour and, for many women, acted as a reason to avoid posting on Facebook or Instagram entirely. A third category — digital literacy anxiety — was particularly prevalent among Assurance Seekers, who described worry about losing money not through fraud but through their own misunderstanding of how digital tools work. Strikingly, a significant proportion of Assurance Seekers could not identify any specific digital risk at all, suggesting an awareness gap rather than an absence of exposure.

Risk Mitigation: Avoidance as a Primary Strategy

Unlike in Kenya, where risk mitigation followed a uniform, institution-scripted pattern, Indian respondents described two distinct mitigation strategies. Verification — double-checking messages and transactions, using passwords and PINs, blocking suspicious contacts — was the approach described by more digitally engaged respondents, particularly Control Seekers.

Avoidance was the more common strategy among Assurance and Protection Seekers: simply staying away from digital uses that felt uncertain, preferring not to engage rather than take a chance. This passive stance was especially pronounced among Assurance Seekers, many of whom found it difficult to articulate any specific risk-management step and defaulted to inaction as a form of self-protection. This has significant implications for digital financial inclusion: many users are not being defrauded — they are simply not participating.

Responsibility Perception: A Government-First Country

India stood apart from all other countries in the degree to which respondents expected the government to be responsible for digital safety. While self and community protection were mentioned across archetypes, government was the dominant frame, particularly among Protection Seekers. This reflects a broader pattern in which Indian respondents — more than those in Nigeria or Kenya — described a relationship with digital financial services mediated by institutional authority rather than individual agency. Convenience was the most commonly cited benefit across all archetypes: the ability to transact without visiting a branch, to send money quickly, to access services at any time. This is a notably different benefit profile from Nigeria and Kenya, where market reach and business opportunity featured more prominently, pointing to a more payment-and-access-oriented digital economy in India.

Conclusion

Understanding how customers think about digital financial services — the risks they perceive, the protections they expect, and the benefits they value — is critical to building services that people will actually trust and use. Trust is not a single thing, and it cannot be addressed with a single intervention. Customers fall into different trust archetypes as an amalgamation of their environment, their experiences, and their own personality traits — including risk tolerance, confidence, and the degree to which they hold themselves or others responsible for their digital safety.

The three archetypes identified in this study — Control Seekers, Assurance Seekers, and Protection Seekers — represent fundamentally different starting points for any trust-building effort. In India, where Assurance Seekers are the majority and avoidance is the dominant mitigation strategy, this has particular urgency: the gap between digital access and digital participation is not primarily a fraud problem — it is a comprehension and confidence problem that requires deliberate design to close. A Control Seeker needs transparency and recourse. An Assurance Seeker needs plain-language guidance and peer-rooted reassurance that makes the system feel navigable. A Protection Seeker needs visible institutional action — from government and platforms alike — that demonstrates accountability rather than simply claiming it.

Data collected from 939 respondents across India using automated voice interviews and AI-powered qualitative analysis. Conducted by Decodis in partnership with the Henry J. Leir Institute at Tufts University.