give | grants

The Financial Haemorrhage

HOW INDIA'S DIGITAL REVOLUTION IS LEAVING ITS MOST VULNERABLE BEHIND

Author:
Prateek Bhandula

June 2026

SECTION 1

Connected but Unprotected: The Human Cost of India's Digital Boom

In a single decade, India built one of the most ambitious digital economies in history. Hundreds of millions of people who had never held a bank account now receive government payments directly on their phones. A street vendor in a Tier-3 town accepts UPI on a cup of tea. A farmer in rural Bihar withdraws wages without travelling 30 kilometres to a branch. These are real, consequential gains.

But the speed of that transformation has come at a cost. The infrastructure that brought people online arrived years ahead of the knowledge and safety systems needed to protect them once they got there. That gap is now costing India's most vulnerable citizens thousands of crores every year — and the losses are accelerating.

MACRO LANDSCAPE

₹22,845 Crore
Total Cyber Fraud Losses (2024)

A severe crisis eroding the economic benefits of digital inclusion.

+206% increase
Year-over-Year Loss Escalation

Threatens to systematically dismantle decades of grassroots development.

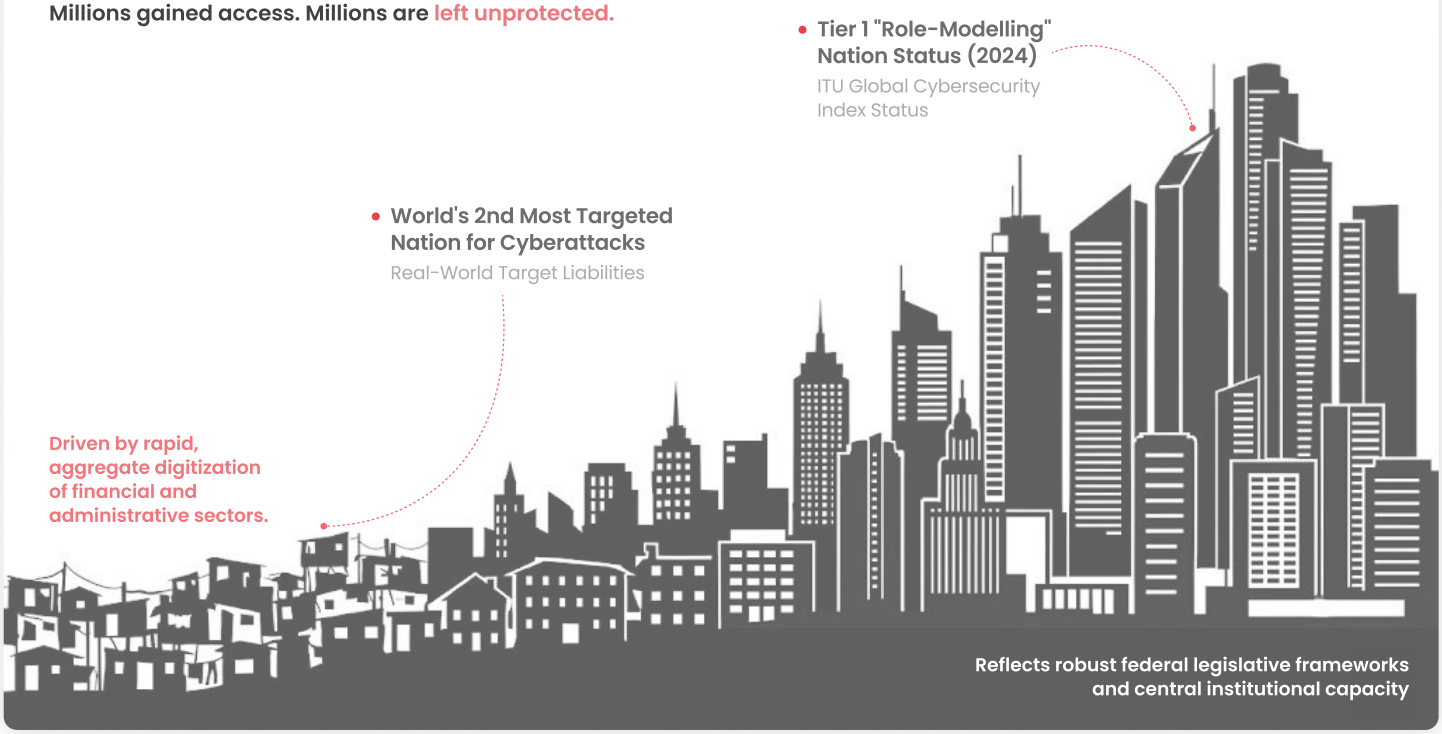
~49%
Global Real-Time Payment Footprint

Creates an expansive, target-rich ecosystem for criminal syndicates.

Sources:
1. https://www.iimb.ac.in/iimb-protean-release-state-dpi-india-report,
2. https://www.irejournals.com/formatedpaper/1707111.pdf,
3. https://timesofindia.indiatimes.com/business/cybersecurity/indias-cyber-fraud-epidemic-rs-22845-crore-lost-in-just-a-year-206-jump-from-previous-year-says-government/articleshow/122840099.cms
4. https://www.researchgate.net publication/400430909_MICROFINANCE_AND_POVERTY_REDUCTION_IN_RURAL_INDIA_A_CRITICAL_EVALUATION_OF_IMPACT_AND_LIMITATIONS,
18. https://www.weforum.org/stories/2026/02/ai-supercharging-global-cyber-fraud-crisis-could-also-solve-it/

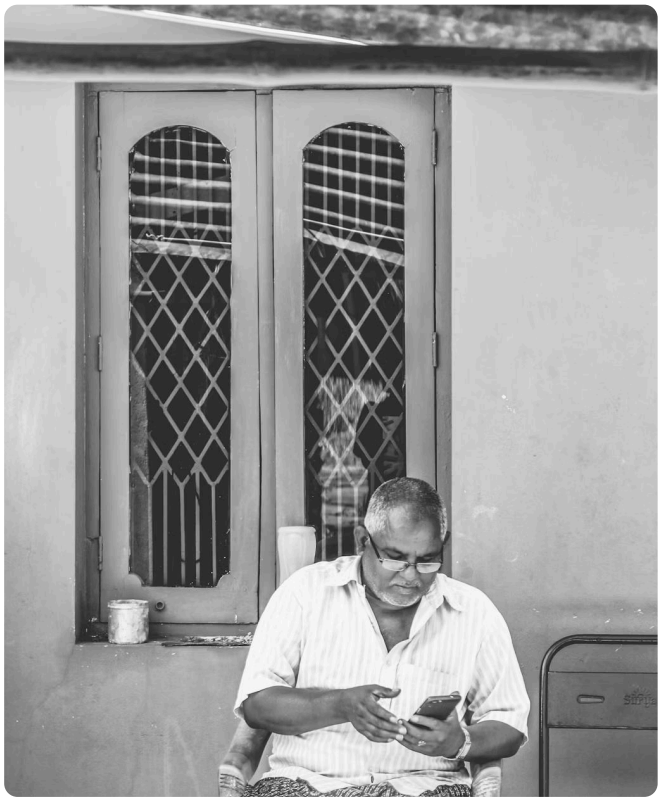
The Price of Progress

Millions gained access. Millions are left unprotected.



Consequently, these vulnerable demographics have been thrust into a highly sophisticated, predatory digital ecosystem without the cognitive tools, technical safeguards, or institutional support required to navigate it safely. While metropolitan populations and corporate entities frequently dominate the discourse on cybersecurity investments, the most insidious, irreversible damage is being inflicted at the grassroots level.

The transition from a cash-heavy economy to a digitally fluid marketplace has created an environment where organized cybercriminal networks—operating out of parallel economic hubs termed "cybercrime villages"—have industrialized financial fraud into a lucrative model.



Sources:
16. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2057035
17. https://carnegieendowment.org/research/2025/09/mapping-indias-cybersecurity-administration-in-2025
19. https://www.theguardian.com/technology/2025/oct/30/scamming-became-the-new-farming-inside-india-cybercrime-villages

SECTION 2

Who Is Now Online & Who Is Most at Risk

India's internet is no longer urban. More than half of the country's 958 million active internet users now live in rural areas, and they are joining the digital economy at four times the pace of their urban counterparts. At the same time, 68% of India's elderly population have adopted digital platforms — WhatsApp, YouTube, UPI — most of them for the first time, without training, and without support.

These are the two groups at the centre of this report. Not because they are careless. But because they were brought into a complex, high-risk digital environment faster than anyone built the systems to protect them.

The Changing Internet Demographics

TOTAL ACTIVE INTERNET USERS

958 Million (8% YoY Growth)

Massive expansion of the overall digital attack surface requiring population-scale security.

RURAL INTERNET BASE

548 Million (57% of total base)

The majority of users reside in areas with the lowest institutional support and literacy.

4X FASTER THAN URBAN CENTERS

4x faster than urban centers

Infrastructural deployment vastly outpaces educational and defensive interventions.

SENIOR CITIZEN PLATFORM ENGAGEMENT

68% active on WhatsApp/YouTube

Post-pandemic isolation has placed significant wealth onto accessible endpoints.

Sources:
24. https://yourstory.com/2026/01/indias-internet-user-base-crosses-950-million-2025-iamai-report
26. https://www.quickheal.co.in/knowledge-centre/guarding-our-elders-a-comprehensive-report-on-the-elder-fraud-epidemic-in-india/

Access Without Protection

Physical Penetration Metrics	Defensive Literacy Deficits
99.5% Rural 4G Coverage: Telecommunications and BharatNet initiatives successfully push optical fiber and low-cost data to the hinterlands.	**86% Elder Literacy Deficit:** Older adults lack basic computer or digital technology skills, rendering them susceptible to social engineering.

This rapid onboarding is characterized by a severe asymmetry between physical access and critical digital literacy. While network pipelines reach the hinterlands, the cognitive frameworks required to evaluate digital threats have not followed.

Similarly, the elderly population in India—projected to reach 193 million by 2031—has undergone an accelerated digital shift. The National Crime Records Bureau (NCRB) documented an 86% surge in cybercrimes explicitly targeting senior citizens between 2020 and 2022, highlighting a deliberate focus on this demographic's accumulated life savings.

SECTION 3

Three People This Is Actually Happening To

The data in this report describes millions of people. These are three of them. Each represents a distinct fraud mechanism, a distinct demographic, and a distinct systemic failure. Together, they show what the haemorrhage looks like at the level of a single household.

Sources:
26. https://www.quickheal.co.in/knowledge-centre/guarding-our-elders-a-comprehensive-report-on-the-elder-fraud-epidemic-in-india/
27. https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=153358&ModuleId=3®=3&lang=1

Mr. Sharma (72), Digitally Migrated Senior

Another senior citizen isolated in the digital crowd

Lacking immediate proximity to digitally native family members to verify claims, and intimidated by forged Supreme Court arrest warrants sent via WhatsApp, he complies with orders to transfer assets to a "safe government escrow account," resulting in complete financial obliteration.

CORE ASSET RISK

Liquid wealth, fixed deposits, accumulated life pensions.

PRIMARY THREAT VECTOR

"Digital Arrest" and Tech Support Extortion: Long video-call psychological isolation.

SYSTEMIC BEHAVIORAL VULNERABILITY

Culturally conditioned to comply with state authority figures; locks up under technical errors.

Asha Devi (35), First-Gen Rural User

Single scam stripped away a woman's financial autonomy

Shares a single device with her husband and son. When scammers trick her into sharing an OTP, the secondary impact is punitive: her husband blames her incompetence, confiscates the phone, and bars her from participating in digital financial activities, effectively erasing her digital identity.

CORE ASSET RISK

Domestic cooking gas subsidies, local SHG pool assets.

PRIMARY THREAT VECTOR

Welfare-Entitlement Fraud: Delivery of fake subsidy links or lottery allocations.

SYSTEMIC BEHAVIORAL VULNERABILITY

Severe text literacy deficit; relies entirely on visual icon recognition over text.

Ramesh (40), Rural Entrepreneur

The invisible theft of a farmer's savings

Relies entirely on the honesty of the local BC agent to withdraw cash. A compromised agent, exploiting system loopholes or utilizing cloned silicone thumbprints, authorizes multiple background transactions. Ramesh absorbs the devastating loss, permanently loses faith in the formal banking system, and retreats to high-interest, exploitative informal moneylenders to survive the crop season.

CORE ASSET RISK

Seasonal crop sale returns, immediate seed purchasing capital.

PRIMARY THREAT VECTOR

Last-Mile Intermediary Fraud: Biometric spoofing via rogue agents.

SYSTEMIC BEHAVIORAL VULNERABILITY

Total geographic dependency on local BC nodes; unable to parse English alert alerts.

SECTION 4

A System Built for the Wrong User

India's digital infrastructure was designed by urban, English-speaking, technically fluent teams — and it shows. The fraud warnings arrive in English. The grievance portals require English. The banking alerts, OTP confirmations, and security protocols all assume a user who can read a Roman-script SMS and navigate a multi-step web form.

98% of India's internet users consume content in Indic languages. The system protecting them does not speak their language — and that gap is not a minor inconvenience. It is a structural exclusion from protection.

Where the Communication Breaks Down

Information Trust Vector

- 64% rely on social media as primary news
- Creates an unverified environment ripe for the spread of malicious payment links.

Device Sharing Concentration

- 18% overall use shared devices; 80% are in rural areas
- Compromises personal data security, privacy, and individual autonomy.

Vernacular Fact-Checking

- <15% of initiatives focus on vernacular dialects
- Regional language users have virtually no mechanisms to cross-verify fraud or deepfakes.

Language Preferences

- 98% of users consume Indic content
- Security protocols, SMS warnings, and banking apps index on English, alienating users.

Sources:
25. https://www.ibef.org/news/india-s-internet-users-to-exceed-900-million-in-2025-driven-by-indic-languages
8. https://www.defindia.org/wp-content/uploads/2025/05/Rural-Fact-Checkers-for-Community_Narrative-Report-1.pdf
26. https://www.quickheal.co.in/knowledge-centre/guarding-our-elders-a-comprehensive-report-on-the-elder-fraud-epidemic-in-india/

Modern digital interfaces are predominantly designed by and for an urban, English-speaking, technically proficient demographic. For the rural poor, the primary barrier is linguistic and contextual. Current safety warnings, dynamic security protocols, and grievance portals heavily index on English, alienating the vast majority of the user base.

Consequently, rural users operating in regional dialects have virtually no accessible mechanisms to cross-verify the authenticity of forwarded messages, deepfakes, or fraudulent payment links. This creates an environment where malicious actors can distribute fake UPI screenshots or phishing links through trusted peer-to-peer networks like WhatsApp, which accounts for nearly 70% of the misinformation spread in rural sectors.

SECTION 5

How the Scams Actually Work

Cybercrime in India is not a technical problem. It is a psychological one. Fraudsters are not breaking into systems. They are breaking into people — exploiting fear, authority, loneliness, and economic desperation with precision.

Understanding how these scams work is essential to understanding why the standard advice — "don't share your OTP", "don't click unknown links" — fails so consistently for the people most at risk.

Who Gets Targeted and How

URBAN / SEMI-URBAN SENIORS		RURAL POOR	
Psychological Weaponization Method	**Real-World Scenario**	**Psychological Weaponization Method**	**Real-World Scenario**
			
Generational respect/fear of institutional authority, combined with deep social isolation.	**"Digital Arrest" Scams:** Scammers spoof official numbers and send forged warrants via WhatsApp.	Economic desperation, shrinking agricultural wages, and rising household indebtedness.	**Entitlement Fraud:** Distribution of fake lottery notifications, loan offers, and fake subsidy plans.

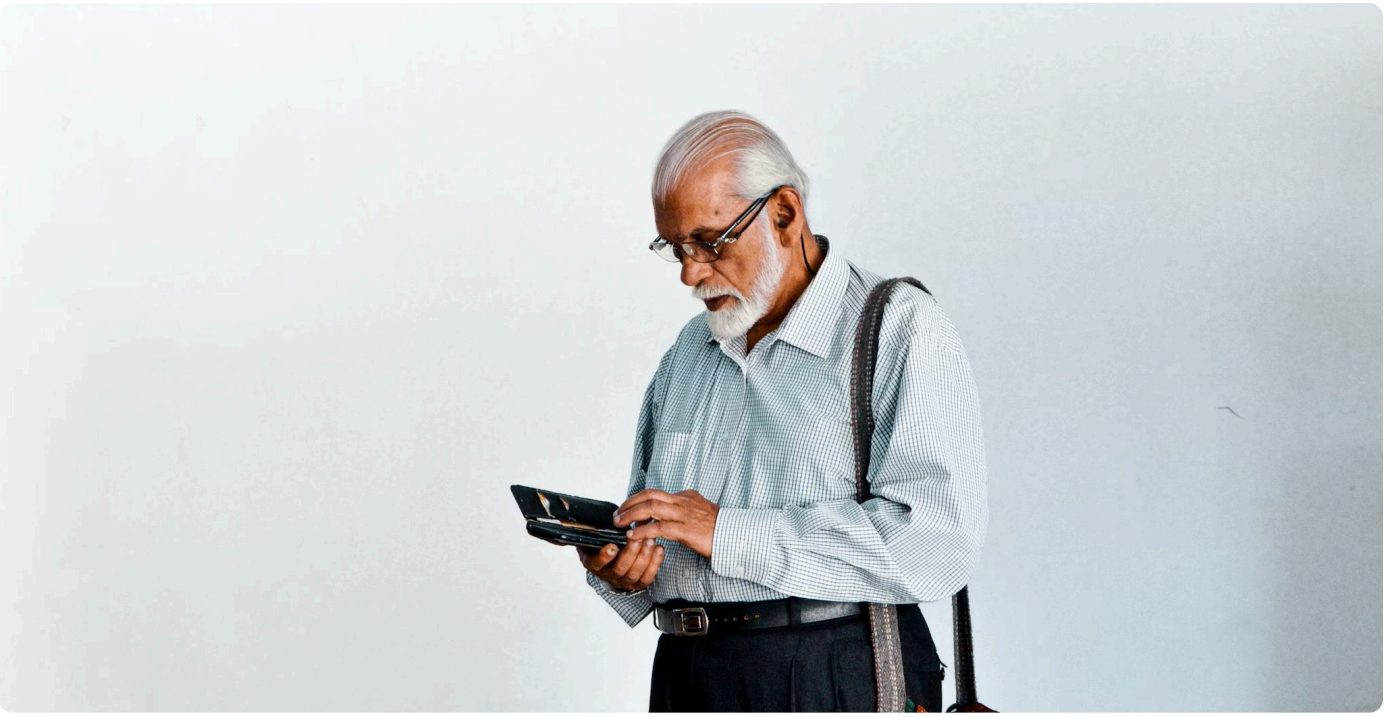
Sources:
20. https://www.niti.gov.in/node/1642
26. https://www.quickheal.co.in/knowledge-centre/guarding-our-elders-a-comprehensive-report-on-the-elder-fraud-epidemic-in-india/
8. https://www.defindia.org/wp-content/uploads/2025/05/Rural-Fact-Checkers-for-Community_Narrative-Report-1.pdf

How a Digital Arrest Scam Unfolds, Step by Step

	Phase 01 ISOLATION	Phase 02 COERCION	Phase 03 LIQUIDATION
Action Taken by Fraudsters	Victims are isolated and monitored via long video calls.	Scammers threaten fabricated legal action over fake contraband parcels.	Victims are forced to transfer funds to a "safe government escrow account".
Victim's Experience & Vulnerability	Induced panic removes logical checking mechanisms.	Intimidated by forged official state emblems and Supreme Court documents.	Results in total financial obliteration of life savings and severe psychological trauma.

The financial toll of these operations is unprecedented; in the first ten months of FY25 alone, digital financial frauds involving ₹4,245 crore across 2.4 million incidents were reported. The Supreme Court of India recently noted that over ₹3,000 crore had been scammed predominantly from the elderly through digital arrest methodologies alone.

For the elderly, the User Interface (UI) and User Experience (UX) of banking applications pose insurmountable cognitive and physical barriers. Age-related declines—such as reduced contrast sensitivity, presbyopia, and diminished motor control due to arthritis—make navigating cluttered screens, small fonts, and executing precise touch-gestures frustrating, error-prone, and highly vulnerable to interception.



SECTION 6

The Infrastructure Being Used Against Its Own Users

For millions of rural Indians, the Business Correspondent (BC) agent is the bank. The nearest branch is 30 kilometres away. The BC is local, known, and trusted. That trust is exactly what makes the BC network a target.

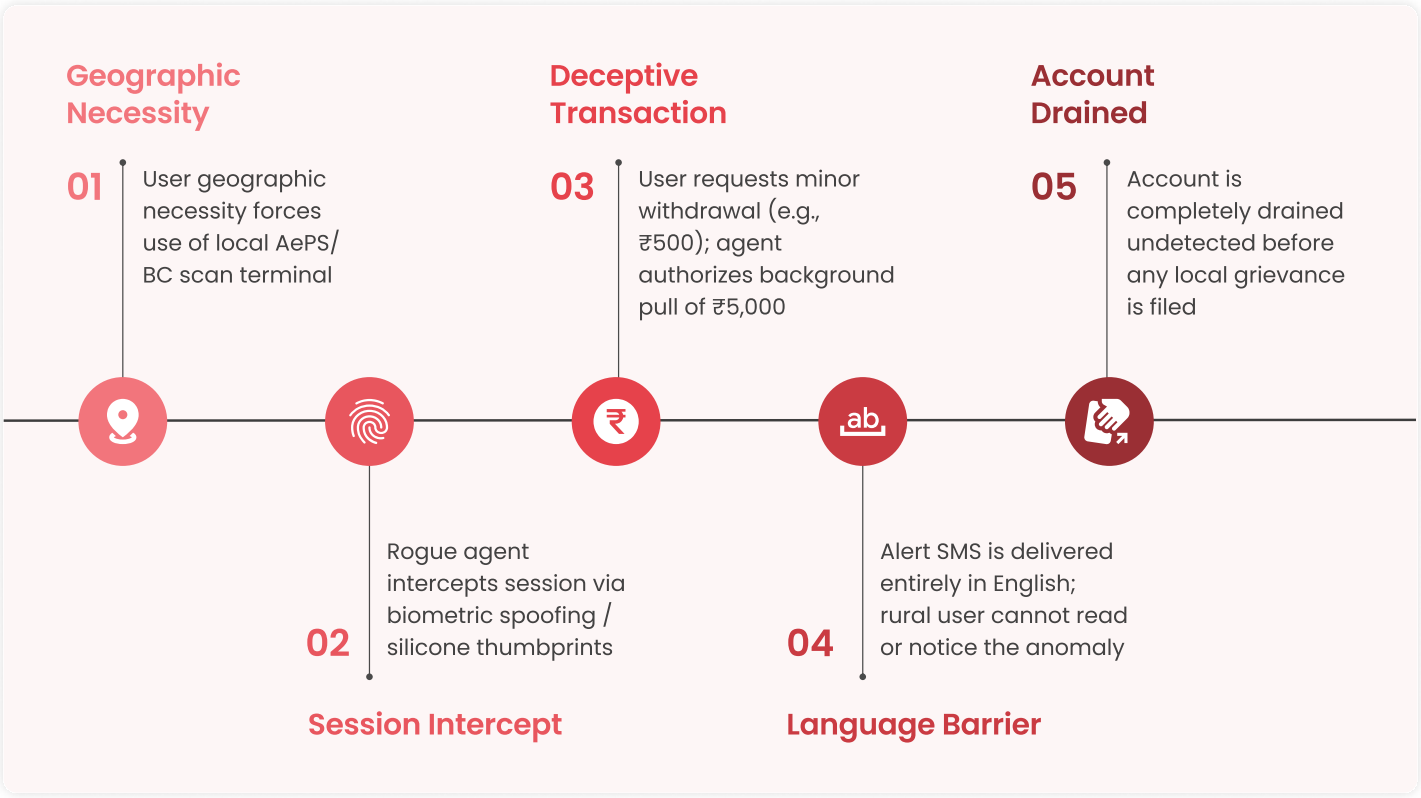
The same last-mile infrastructure built to bring financial inclusion to rural India has become a point of exploitation — through weak agent vetting, biometric vulnerabilities, and a notification system that alerts users to fraud in a language they cannot read.

Three Ways the System Fails at the Last Mile

	Agent Vetting	Biometric Interception	Linguistic Notification Black Hole
Operational Weakness	Weak agent screening processes and an absolute lack of centralized fraud tracking.	Users are forced to share endpoints and biometric access out of geographic necessity.	Automated transaction alerts and SMS bank confirmations are broadcast exclusively in English.
Fraud Method Deployed	Rogue agents exploit technologically illiterate populations at physical transaction points.	**Biometric Spoofing:** Creating silicone thumbprints to bypass device verification.	**Dual-Transaction Authorization:** Authorizing a deep siphoning of funds without user knowledge.

Sources:
3. https://timesofindia.indiatimes.com/business/cybersecurity/indias-cyber-fraud-epidemic-rs-22845-crore-lost-in-just-a-year-206-jump-from-previous-year-says-government/articleshow/122840099.cms
34. https://gfsi.in/unmasking-financial-fraud-in-indias-bc-industry-a-wake-up-call-for-financial-inclusion/
36. https://f1studioz.com/blog/designing-for-the-elderly-the-overlooked-demographic-in-digital-accessibility/

The Last-Mile Fraud Trajectory



Because the user cannot read the English SMS alert, the fraud goes completely undetected until the account is completely drained. Lacking the specialized knowledge to read automated alerts and entirely unaware of how to file a digital grievance, the rural user is forced to absorb the devastating financial blow in silence.

SECTION 7

When Fraud Takes More Than Money

For most victims, the financial loss is only the beginning. What follows — shame, silence, loss of access, family punishment — often inflicts more lasting damage than the original fraud.

Sources:
8. https://www.defindia.org/wp-content/uploads/2025/05/Rural-Fact-Checkers-for-Community_Narrative-Report-1.pdf
24. https://yourstory.com/2026/01/indias-internet-user-base-crosses-950-million-2025-iamai-report

For rural women, a single scam can end their participation in the digital economy entirely. For elderly victims, the psychological aftermath of a digital arrest scam — the humiliation, the fear of being judged by their children — frequently leads to withdrawal, depression, and accelerated cognitive decline. The fraud takes the money. The social response takes everything else.

What Happens After the Fraud

RURAL FEMALE USERS

Immediate Post-Fraud Impact

Victimization is viewed as proof of her inherent "ignorance" and technological unfitness.

Long-Term Systemic Regression

Patriarchal Device Confiscation: Male family members permanently lock her out of digital assets.

URBAN / SEMI-URBAN ELDERS

Immediate Post-Fraud Impact

Deep feelings of shame, humiliation, self-blame, and extreme fear of adult child judgment.

Long-Term Systemic Regression

Social Isolation & Churn: Complete silence breeds depression, accelerating cognitive decline.

The Gendered Cyber Punishment Loop

Fraud

01 Rural woman falls victim to entitlement fraud on shared family device

Technological Ignorance

02 Incident interpreted by household as proof of female incompetence / technological ignorance

Punitive actions

03 Male family members permanently confiscate the shared device

Digital Exclusion

04 Woman is barred from participating in Self-Help Group (SHG) digital financial networks

Gender Digital Divide

05 Complete regression into financial dependency, widening the gender digital divide

Sources:
8. https://www.defindia.org/wp-content/uploads/2025/05/Rural-Fact-Checkers-for-Community_Narrative-Report-1.pdf
5. https://pmc.ncbi.nlm.nih.gov/articles/PMC6014157/
4. https://www.researchgate.net/publication/400430909_MICROFINANCE_AND_POVERTY_REDUCTION_IN_RURAL_INDIA_A_CRITICAL_EVALUATION_OF_IMPACT_AND_LIMITATIONS

When a rural woman falls victim to a scam on a shared family device, it is rarely viewed as a sophisticated cyberattack ; it is viewed as proof of her inherent unfitness to manage technology. This forces an immediate regression into total financial dependency, widening the gender digital divide and nullifying years of women's empowerment initiatives.

SECTION 8

What a ₹7,000 Loss Actually Means to a rural household

On a corporate balance sheet, ₹7,000 is a rounding error. For a rural micro-entrepreneur or an SHG member, it is an entire season's savings. It is the seed capital for next month's inventory. It is the buffer that stands between a household and an informal moneylender.

When that money disappears to a scam, it does not simply disappear. It triggers a cascade — debt, asset liquidation, school withdrawal — that can take years to recover from. And critically, it directly reverses the poverty reduction impact of the very welfare programmes that put the money there in the first place.

The Household Loss Spectrum

Loss Value	Household Context	Real-World Coping Implication
₹5,000-₹7,000	Equates to an entire agricultural season's savings or total operational capital for a micro-enterprise.	Forces a complete extraction of wealth out of the local rural economy.
Systemic Result	Households employ highly damaging negative coping habits to secure survival.	**The Debt Trap:** Households liquidate productive assets, pull kids from school, or borrow from loan sharks.

Sources:
8. https://www.defindia.org/wp-content/uploads/2025/05/Rural-Fact-Checkers-for-Community_Narrative-Report-1.pdf
7. https://pmc.ncbi.nlm.nih.gov/articles/PMC9214770/

How Cybercrime Transfers Wealth in the Wrong Direction

Cybercrime Targeting

01 Predator Cybercrime Operations Target Low-Income Demographics

02 Extraction of Small Operational Capital / Savings Blocks (e.g., ₹7,000)

Capital Extraction

Forced Adoption of Catastrophic Domestic Coping Mechanisms

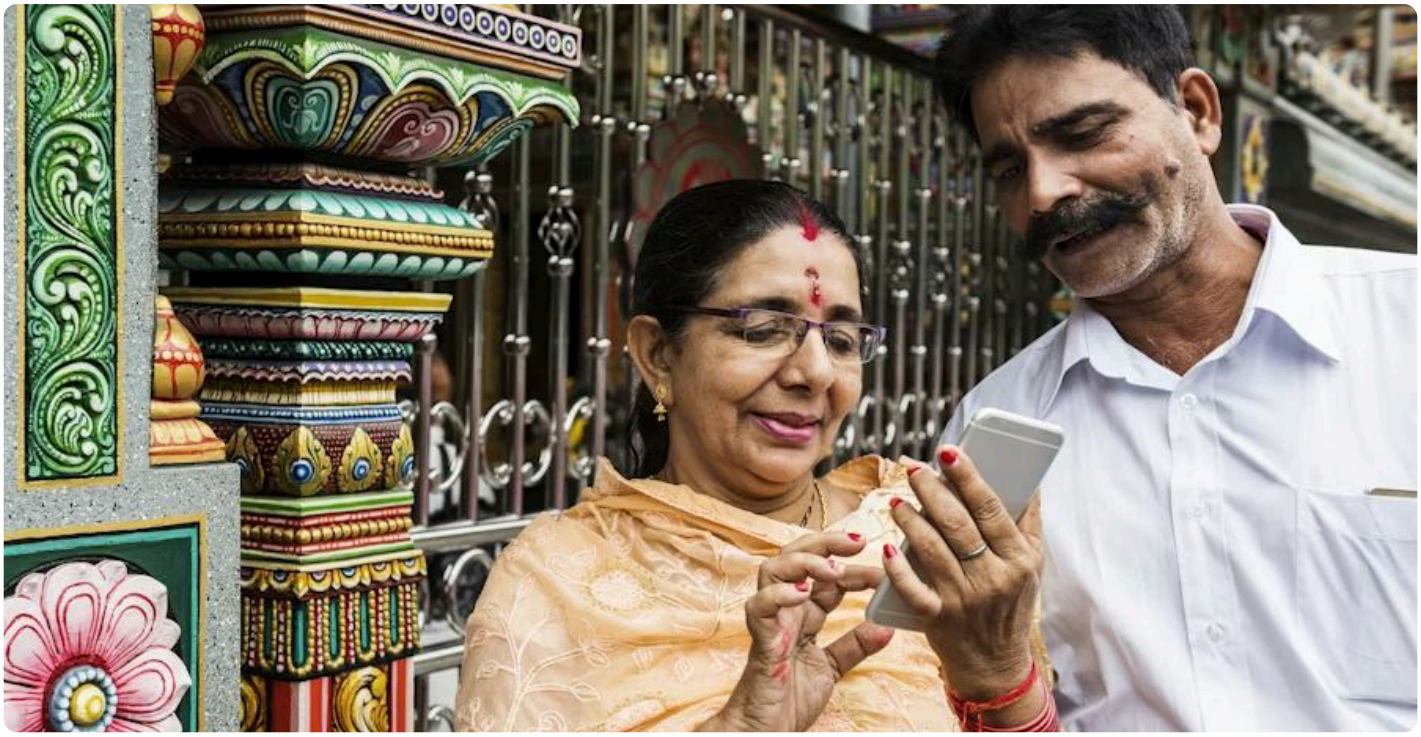
03

- Liquidation of Productive Family Assets
- Immediate Withdrawal of Children from Education
- High-Interest Indebtedness to Informal Local Loan Sharks

04 Complete Neutralization of Welfare Programs, DBTs, and Microfinance Gains

Welfare Loss

Cybercrime acts as a highly efficient, regressive mechanism for transferring wealth from the poorest citizens directly to organized criminal syndicates. This capital destruction directly neutralizes the poverty-alleviation impacts of state welfare programs, Direct Benefit Transfers (DBT), and local microfinance initiatives.



Sources:
14. https://www.fbi.gov/news/press-releases/fbi-highlights-growing-number-of-reported-elder-fraud-cases-ahead-of-world-elder-abuse-awareness-day

SECTION 9

Victims With Nowhere to Turn

A rural woman defrauded of ₹8,000 knows she has been robbed. What she does not know is how to prove it. The reporting system requires her to log transaction hashes, compile digital evidence, and navigate a multi-step English-language portal. She cannot do any of these things — not because she is incapable, but because the system was never designed with her in mind.

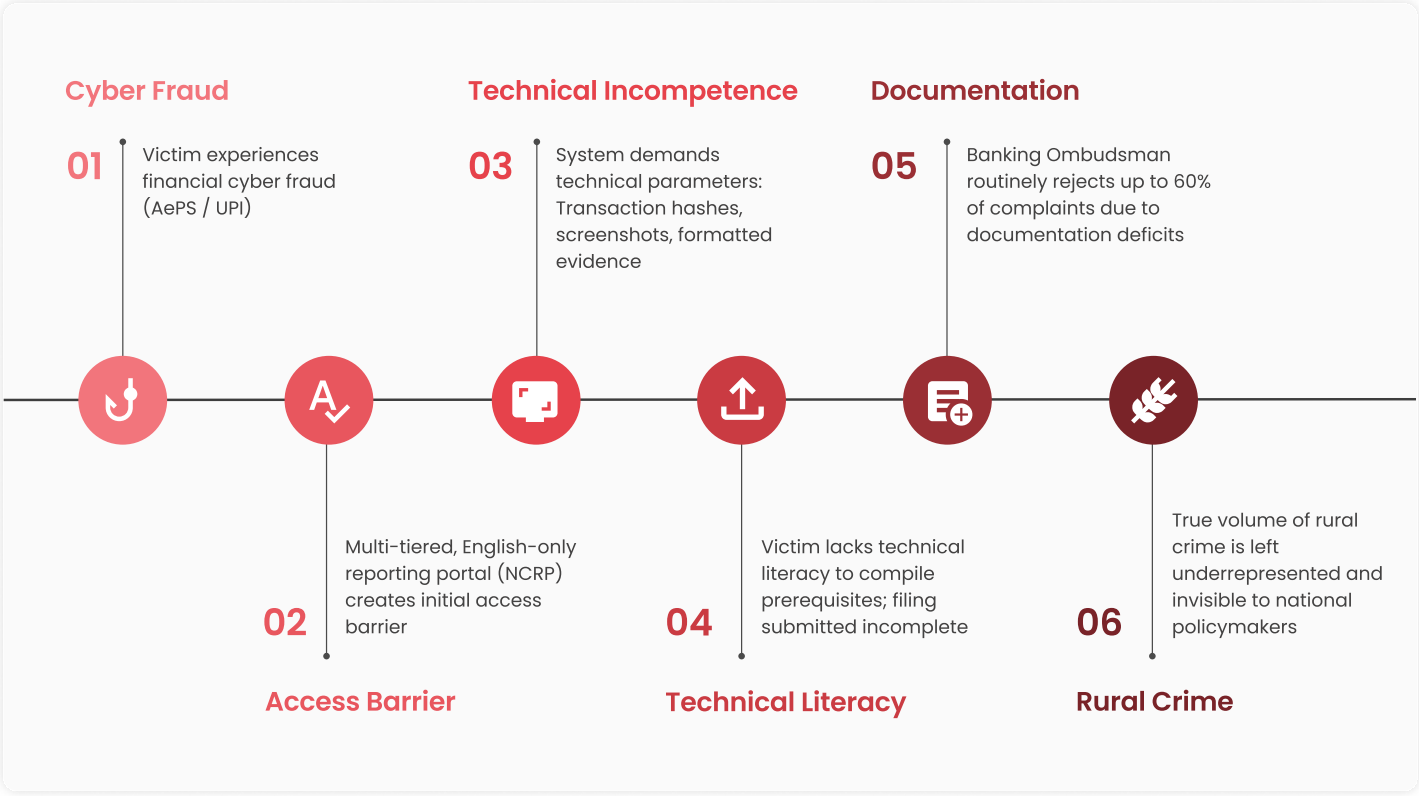
56% of filed cybercrime complaints go completely unresolved. Between 32% and 60% are rejected by the Banking Ombudsman for "lack of useful information." These are not victim failures. They are design failures.

How the System Fails Victims at Every Step

Redressal Point	Data Metric	Structural Failure Cause
Unresolved Complaints	56% of filed cases go completely unresolved	Complex, multi-tiered English web portals are completely inaccessible to dialect users.
Ombudsman Rejection Rate	32% to 60% of complaints are rejected	Banking Ombudsman routinely dismisses filings due to a "lack of useful information".
Grassroots Law Enforcement	High dismissal of small-value frauds (e.g., ₹2,000)	Local police dismiss grassroots claims as jurisdictionally ambiguous or insignificant.

Sources:
10. https://www.microsave.net/wp-content/uploads/2024/12/241211_Mind-the-gap_Closing-the-loopholes-in-consumer-protection-in-digital-financial-services.pdf

Why Most Rural Victims Never Even Report



This structural apathy actively discourages reporting, meaning the true volume of rural cybercrime is vastly underrepresented in official NCRB statistics, rendering the problem entirely invisible to national policymakers.

SECTION 10

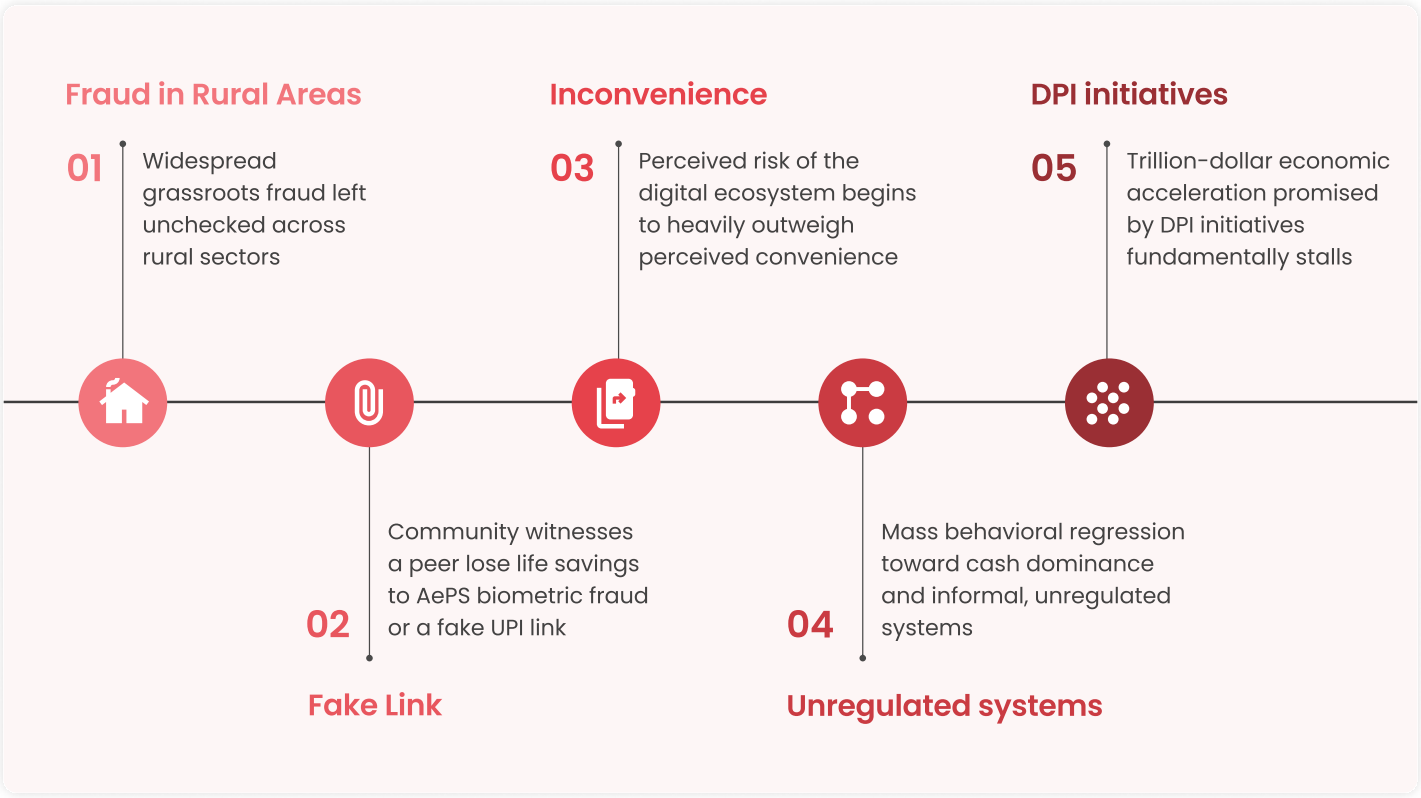
Why the System Cannot Reach the People Who Need It

ndia has invested seriously in cybercrime infrastructure. The I4C helpline, CFCFRMS, Sanchar Saathi, PMGDISHA — these are real programmes with real reach. The problem is not absence of effort. The problem is that every layer of the response system was built for a different user than the one experiencing the most harm.

No single agency owns the end-to-end experience of a grassroots fraud victim. A rural user who has been defrauded is bounced between the police, the bank, the telecom provider, and an English-language portal — each pointing to the next, none completing the loop.

Sources:
52. https://cjp.org.in/cybercrime-and-the-crisis-of-digital-justice-indias-invisible-victims-online/

The Threat to Digital Public Infrastructure (DPI)



On a macroeconomic scale, the most dangerous consequence of unchecked cyber fraud is the systematic erosion of public trust in Digital Public Infrastructure (DPI). Studies indicate that nearly 47% of rural women who actively avoid digital financial tools cite the explicit fear of scams as their primary reason. If the unbanked and underbanked populations lose faith in the security of the ecosystem, the trillion-dollar economic acceleration promised by DPI initiatives will fundamentally stall.

Sources:
17. https://carnegieendowment.org/research/2025/09/mapping-indias-cybersecurity-administration-in-2025

SECTION 11

Who Is Acting & Where the Gaps Are

Government, industry, and civil society are all engaged with this problem. The challenge is not a lack of action — it is that each actor is solving a different part of the problem, with no coordination, and the parts being solved are not the parts that matter most to the people most at risk.

What Each Stakeholder Does — and What It Cannot Reach

Stakeholder Category	Flagship Initiatives & Focus	Structural Limitations & Systemic Gaps
Government & Law Enforcement	• **I4C 1930 Helpline:** Saved ₹5,489 crore via bank fund freezing • **Sanchar Saathi:** Endpoint audits and connection tracking • **PMGDISHA:** Mass rural digital literacy certification	• Reporting portals are highly complex, English-centric, and inaccessible • Central literacy programs focus on basic app usage, not critical cyber resilience.
BFSI & Telecommunications	• **Telcos:** Network-level AI spam and call filtering • **Banks:** Behavioral biometrics, dynamic risk-scoring models, and MFA parameters.	• Interventions are largely reactive and heavily indexed toward urban, high-net-worth customers • MFA parameters create high cognitive friction for elderly users.
Civil Society & NGOs	• **DEF:** Rural 'Infopreneurs' and vernacular fact-checkers • **DSCI:** CyberShikshaa women cybersecurity training • **Cyber Saathi:** Legal advocacy for grassroots victims.	• Chronically underfunded and lacking population-level scalable capital • Poorly integrated with state law enforcement or major banking ombudsmen nodes

Corporate efforts remain largely siloed, focusing on protecting the institutional perimeter rather than educating the vulnerable endpoint user. While civil society organizations are highly effective locally, they chronically suffer from a lack of scalable capital, leaving the defense mechanism porous for the demographics that possess the least capacity to advocate for themselves.

Sources:
44. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2146786, 46. https://www.pib.gov.in/PressReleasePage.aspx?PRID=1812277 47. https://askfuzz.ai/discover/news/banking/digital-frauds-drop-to-17-of-complaints-as-banks-strengthen-security, 31. https://bfsi.economictimes.indiatimes.com/news/industry/indians-lose-rs-4245-crore-in-24-lakh-digital-fraud-cases-in-first-10-months-of-fy25/119326470

SECTION 12

Securing the Next Billion: Why digital safety is a strategic imperative

CSR investment in India has historically flowed toward what is visible: school buildings, healthcare camps, sanitation drives. Digital safety is invisible until it fails — and when it fails, it fails catastrophically for the people least able to recover.

There are four reasons why the corporate and philanthropic sector needs to treat grassroots digital safety as a priority investment, not a peripheral concern.

Market Preservation 01

47% of rural women who avoid digital financial tools cite fear of scams as their primary reason.

(Source: Digital Empowerment Foundation)

Widespread fraud drives behavioural regression toward cash and informal finance. A digitally confident rural user is a net-new, loyal participant in the formal economy. Protecting that user is protecting that market.

Brand and Reputational Risk 02

56% of filed cybercrime complaints go completely unresolved.

(Source: MicroSave Consulting 2024)

When fraud occurs on a specific payment platform or telecom network, community distrust attaches to the brand, not the anonymous scammer. Proactive grassroots safety programmes reduce this exposure and reduce the likelihood of regulatory intervention.

ESG and BRSR Alignment 03

SEBI's BRSR mandate requires listed companies to disclose their impact on communities and consumers.

Investments in cyber safety for underserved populations directly strengthen the Social and Governance pillars of ESG frameworks. Corporations investing here satisfy BRSR disclosure requirements with evidence of measurable community impact.

SDG Convergence 04

4 SDGs are directly addressed:

Digital safety initiatives intersect with internationally recognised development benchmarks, giving corporations credible, globally reported impact anchors for their sustainability disclosures.

Sources:
8. https://www.defindia.org/wp-content/uploads/2025/05/Rural-Fact-Checkers-for-Community_Narrative-Report-1.pdf, 42. https://www.fico.com/blogs/scams-india, 10. https://www.microsave.net/wp-content/uploads/2024/12/241211_Mind-the-gap_Closing-the-loopholes-in-consumer-protection-in-digital-financial-services.pdf, 11. https://responsenet.org/business-responsibility-and-sustainability-reporting-impact-investment-india/, 56. https://csrbox.org/Impact-stories_full_Empowering-Communities--L&T-Finance's-'Digital-Sakhi'-Program-Transforms-Lives-of-42-Lakh-Members_683

SECTION 13

What Good Looks Like

The following approaches have produced measurable outcomes across documented programmes. They are not recommendations — they are patterns the evidence has already established. The gap in every case is not proof of concept. It is scale.

01. Peer-Led Threat Recognition

Community-based women ambassadors have consistently outperformed centralised broadcast campaigns. The gap in existing models is curriculum: current programmes teach app usage; what builds resilience is scenario-based threat recognition.

Programme	What It Does	Evidence of Impact
L&T Finance Digital Sakhi	Trains rural women as community digital ambassadors	Documented behaviour change in target villages; culturally trusted delivery
Google Internet Saathi	Women-led digital literacy across rural India	Reached 30 million+ women across 300,000+ villages
The upgrade required	Shift curriculum from "how to use UPI" to "how to identify a fake government call"	Peer-delivered, scenario-based training is the documented gap

Sources: L&T Finance; Google Internet Saathi programme data; CASEL India

02. Assisted Grievance at the Last Mile

The 32–60% Banking Ombudsman rejection rate is a documentation design failure, not a victim failure. Where trained staff sit physically with victims to file complaints, resolution rates improve.

Intervention Point	Current Gap	What Works
Common Service Centres (CSCs)	No cyber grievance function; victims redirected elsewhere	Trained staff assist victims in compiling transaction evidence and navigating NCRP

Intervention Point	Current Gap	What Works
Rural bank branches	Nodal officers exist but are inaccessible to rural victims	Direct linkage between branch nodal officer and victim with support staff
Panchayat offices	No digital grievance infrastructure	Low-cost physical touchpoint with trained community paralegal

Sources: MicroSave Consulting 2024; Citizens for Justice and Peace

03. Vernacular-First Safety Tools

98% of India's internet users prefer Indic-language content. Less than 15% of safety infrastructure operates in vernacular languages. The tools exist - the gap is deployment and scale.

Tool Type	Current Status	Documented Model
WhatsApp fact-checking bots	Fragmented; few operate in regional dialects	DEF's Infopreneur network - vernacular community fact-checkers; behaviour change documented in Rajasthan study
Banking SMS alerts	English-only; unreadable by majority of rural users	No scaled vernacular alternative currently exists
Fraud awareness campaigns	English-first; passive rule-based *("don't share OTP")*	Vernacular, scenario-based delivery proven more effective in pilot programmes

Sources: Digital Empowerment Foundation; IBEF

04. A Financial Buffer for the Uninsured

India has among the lowest cyber insurance penetration in Asia. For a rural household at the margin, a ₹10,000 fraud loss does not stay contained - it triggers debt, asset liquidation, and in documented cases, school withdrawal.

Tool Type	Current Status	Documented Model
Individual cyber insurance	Near-zero penetration at bottom of income distribution	Products exist for corporates; no equivalent for PMJDY account holders
Jan Dhan / microfinance bundling	56.16 crore accounts with no fraud safety net	WIEGO and sector analysts confirm demand and structural feasibility
Recovery mechanism post-fraud	No financial buffer; households absorb full loss	Ultra-low-premium micro-cyber insurance identified as viable; no scaled product exists

Sources: Insurance Asia 2024; WIEGO; Elets BFSI

Acknowledgement

This report draws on the foundational research, on-ground insights, and dedicated work of several key organizations striving to understand and improve India's digital landscape. We would like to explicitly acknowledge and express our deep gratitude to the following entities, whose comprehensive reports significantly informed the narratives, data, and context within this document:

Digital Empowerment Foundation (DEF)

We acknowledge **DEF** for their indispensable research in the **Rural fact checkers for community narrative report**. Their grassroots work provided crucial context regarding digital literacy, vernacular language challenges, and the vital need for community-led resilience mechanisms against misinformation and fraud.

Sources: Rural Fact Checkers for Community Narrative Report

IAMAI and Kantar

We acknowledge **IAMAI and Kantar** for their rigorous demographic tracking and trend analysis in the **Internet in India Report 2025**. Their comprehensive data on active internet users, device sharing, and the accelerated pace of rural digital adoption formed the statistical backbone for understanding who is now online and most at risk.

Sources: Internet in India Report 2025

give | grants

THE FINANCIAL HAEMORRHAGE

How India's Digital Revolution Is Leaving Its Most Vulnerable Behind

"The wound is not inevitable. It is the predictable consequence of building access without building safety."

givegrants.in