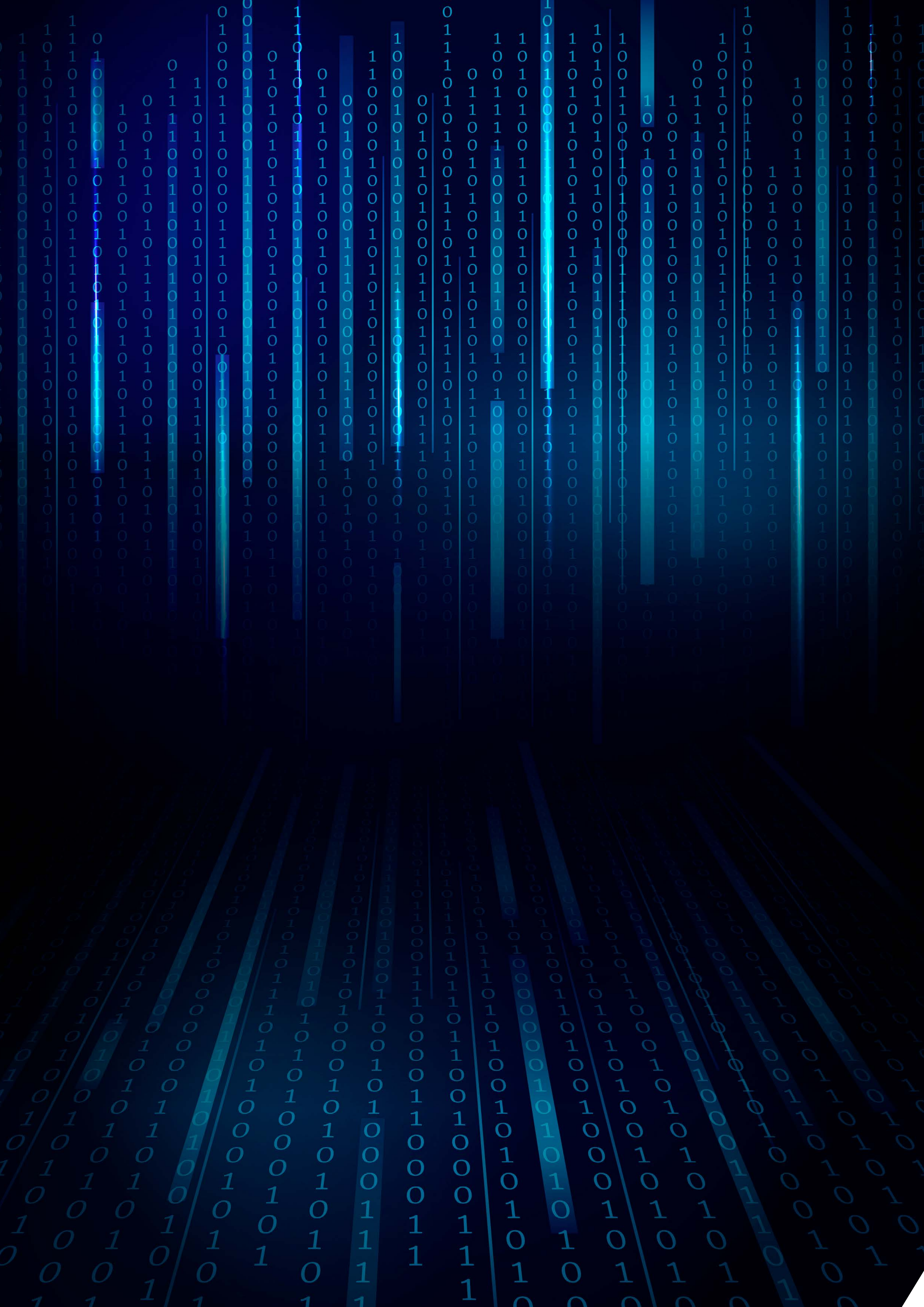
The Federation of Telangana Chambers of Commerce and Industry - FTCCI

protiviti®
Global Business Consulting

Citizens Handbook on Digital Fraud Awareness and Prevention

A Practical Guide to Staying Safe in the Digital World

Face the Future with Confidence®



MESSAGE FROM
THE COMMISSIONER OF POLICE

Sri V.C. Sajjanar, IPS
Commissioner of Police
Hyderabad City

Hyderabad City Police

Cybercrime today has moved well past the individual scammer working alone. What we encounter on the ground are organised, layered criminal networks — recruiters, mule account handlers, technical operators, and money-laundering chains often spanning multiple states and, increasingly, operating from beyond our borders. These groups function with the discipline of an enterprise: defined roles, shift patterns, and the ability to redeploy the moment one channel is blocked. Meeting that scale of organisation requires an equally coordinated response.

No single institution can address this alone. Effective citizen protection today depends on banks maintaining vigilant transaction monitoring and acting swiftly on freeze requests; the Indian Cyber Crime Coordination Centre (I4C) and the Ministry of Home Affairs providing the national coordination, intelligence-sharing, and policy direction that connect city-level investigations to the wider picture; telecom providers acting on SIM fraud and spoofed numbers; and law enforcement translating all of this into cases that are actually investigated, chargesheeted, and prosecuted. Hyderabad City Police continues to invest in this coordination — with banks on transaction trails, with I4C and state cybercrime cells on cross-jurisdictional cases, and with the public through sustained awareness efforts. We also have the C-Mitra service which enables victims to prefer FIR from the comfort of their homes.

This handbook, brought together by FTCCI and Protiviti, adds an equally essential piece: an informed citizen. Awareness at the point of the first phone call or the first QR code is often the only intervention available before a fraud is set in motion — no institutional response, however fast, recovers a transaction as effectively as one that never happened.

This partnership is a welcome example of the multi-stakeholder effort this problem demands — industry, consulting expertise, banking, and law enforcement working toward one shared goal. I hope this handbook reaches every household, workplace, and classroom it can.

Pause. Verify. Report. And should you need us, the National Cyber Crime Helpline 1930 and your nearest police station remain within reach.

TABLE OF CONTENTS

FOREWORD

Sri R.Ravikumar
President, FTCCI

"The future of Digital India will not be determined by how connected we become, but by how confidently every citizen can participate in the digital economy with trust, security, and resilience.

Bala Peddigari
Chair, ICT and Startups Committee
FTCCI

In an era where nearly every interaction between citizens and institutions carries a digital footprint, trust has become both our most valuable currency and our greatest vulnerability. This white paper reflects our organization's commitment to addressing that reality head-on.

Digital transformation has brought extraordinary convenience to public life — from online government services to digital identity systems and real-time data sharing. But with this progress comes a responsibility we cannot afford to overlook: protecting the citizens who place their trust in these systems every day.

We have seen firsthand how breaches of data, lapses in cybersecurity, and gaps in digital literacy can erode public confidence and leave vulnerable populations exposed to fraud, surveillance overreach, and misinformation. Building digital trust is not a technical challenge alone; it is a societal one, requiring collaboration between policymakers, technologists, businesses, and communities.

FTCCI is proud to present this white paper in association with Protiviti. This represents our effort to bring clarity to that challenge. It examines the frameworks, safeguards, and shared responsibilities necessary to build a digital ecosystem where citizens can engage confidently — knowing their data is secure, their rights are respected, and their voices matter in shaping the policies that govern their digital lives.

I want to thank the ICT Committee of FTCCI who have been working relentlessly alongside researchers, policy experts, and community stakeholders who contributed their insight to this work. Their dedication reflects a shared belief: that digital innovation and citizen protection are not competing priorities, but complementary goals that must advance together.

As we move forward, I invite readers — whether policymakers, industry leaders, or engaged citizens — to see this paper not as a final word, but as an invitation to dialogue. The future of digital trust will be shaped by all of us, and it is our collective responsibility to ensure that future is safe, equitable, and empowering for every citizen.

PREFACE

Sandeep Gupta

Managing Director

Protiviti Member Firm for India

India's digital journey has transformed the way we live, work, transact, and connect. From online banking and digital payments to e-governance and commerce, technology has brought unprecedented convenience and opportunities to millions of citizens.

Yet, as our digital economy grows, so do the risks. Cyber fraudsters are no longer targeting only systems; they are increasingly targeting people—exploiting trust, fear, urgency, and even the promise of quick rewards. A single careless click, an unexpected phone call, or a deceptive message can lead to significant financial and emotional loss.

In this evolving landscape, awareness is our first line of defense. Every citizen must stay informed, think critically, and exercise caution while sharing personal or financial information online. Digital trust can only thrive when technology is matched by responsible behavior and collective vigilance.

The National Round Table on **Digital Trust & Citizen Protection** is a timely and important initiative that brings together policymakers, law enforcement agencies, industry leaders, cybersecurity experts, and citizens to discuss practical solutions to emerging digital threats.

Let us work together to build a safer, more secure, and trustworthy digital ecosystem where innovation flourishes and citizens remain protected. A digitally empowered India must also be a digitally aware and cyber-resilient India.

Together, let us stay alert, stay informed, and stay secure.


Mobile Banking Alert
Suspicious Activity
Potential Fraud
Potential Fraud
Spam
Security Warning

EXECUTIVE SUMMARY

India's digital transformation has been remarkably fast. UPI, Aadhaar-linked services, digital banking, e-commerce, and a mobile app for nearly everything have given citizens a level of convenience that simply didn't exist a decade ago. That same speed has created new openings for people who would rather steal money and identities than earn either.

Criminals have kept pace with the shift. They now combine old-fashioned social engineering with newer tools — artificial intelligence, deepfakes, voice cloning, and personal data lifted from breaches or careless sharing — to convince ordinary people to hand over money, OTPs, and account access.

The fraud citizens face today looks very different from the phishing emails and lottery SMS messages of a few years ago. Digital arrest calls, cloned voices pretending to be a relative in trouble, fake investment platforms, SIM swap attacks, identity theft, and loan apps that were never legitimate to begin with — these are now common enough that most people know someone who has been targeted, if not affected directly.

This handbook exists to give citizens something practical: how to recognise these frauds before money changes hands, what protections Indian law actually provides, which agencies to contact, and what to do in the hours immediately after realising something has gone wrong.

If there is one message worth taking from all of this, it's short enough to remember under pressure:

Pause. Verify. Report.

That pause even thirty seconds before scanning a QR code or reading out an OTP is often the only thing standing between a citizen and a loss that is very hard to reverse.

1 India's Digital Economy and Fraud Landscape

India's Digital Revolution

Over roughly the last decade, India has built one of the more ambitious digital public infrastructures anywhere in the world. Aadhaar, UPI, Digi Locker, FASTag, and a steady expansion of e-governance have changed how citizens deal with banks, government offices, and each other's money.

The scale involved is genuinely large — UPI alone processes an enormous number of transactions every minute of the day. That kind of throughput brings real benefits: faster payments, wider financial inclusion, less paperwork. It has also, inevitably, given fraudsters a much bigger surface to work with.

Digital fraud isn't really a side effect of this growth. At this point, it's one of the central risks that comes bundled with it.

The Cost of Digital Fraud

Money is the most visible cost, but rarely the only one. People who have been defrauded often describe a mix of:

01 Financial strain that can take months, sometimes years, to recover from

02 Real emotional distress – shame, anxiety, and in some cases a lasting wariness of anything digital

03 A loss of confidence in banking apps and digital payments generally

04 Reputational fallout, particularly in mule account cases where a victim's name gets tied to a crime they didn't knowingly commit

05 Legal complications that can drag on well after the money itself is gone

Certain groups tend to be targeted more often — senior citizens, students, homemakers, first-time digital users, and small business owners. Not because they're less intelligent, but because fraudsters read them, rightly or wrongly, as less likely to double-check before acting.

Understanding the Fraud Lifecycle

Most digital fraud, however different it looks on the surface, tends to follow a similar arc.

Reconnaissance

The fraudster gathers information first, from social media, leaked databases, public records, even a casual reply on a marketplace app. The more they know about you, the more convincing everything that follows becomes.

Trust Building

They then step into a role you're inclined to trust: a bank officer, a police official, a relative, a customer support agent, occasionally even a friend.

Manipulation

Once that trust is in place, they manufacture pressure a deadline, a threat, an opportunity that won't come around again built to stop you thinking too carefully.

Exploitation

This is the point where money actually moves, or credentials get handed over.

Exit

And then they're gone. Numbers get disconnected, accounts vanish, the WhatsApp group goes quiet.

Recognising this shape, reconnaissance, trust, pressure, extraction, disappearance, is often more useful than trying to memorise every individual scam, because new versions of the same pattern turn up every few months under a different name.

2

Understanding Digital Fraud

What is Digital Fraud?

In the simplest terms, digital fraud is any deception carried out through electronic channels to steal money, information, identity, or account access.

It's worth being clear about one thing early on: a fraudster's main tool usually isn't technical skill. It's manipulation. Most scams succeed not because the victim was fooled by clever code, but because they were fooled by a convincing story delivered at the right emotional moment.

Why Digital Frauds Are Increasing

A few things are driving the growth:

01 More of daily life now runs through digital transactions

02 Personal information is easier to find online than most people realise

03 Social media makes it simple to research a target in real detail

04 Data breaches keep surfacing usable information cheaply

05 AI tools have made it far easier to produce a convincing scam at scale

06 Organised groups, not lone individuals, run much of this as an operation, complete with targets and shift patterns

That point about AI is worth dwelling on. It has lowered the skill and cost required to run a convincing scam so much that operations which once needed a dozen people can now be run with a fraction of that.

The Psychology of Fraud

Nearly every scam leans on one or more of five emotional levers.

Fear

"You are under investigation."

Urgency

"Your account will be blocked in 30 minutes."

Authority

A call claiming to be from the police, the RBI, your bank, or customs.

Greed

The promise of returns that sound too good — usually because they are.

Trust

Impersonating someone you already trust: a friend, a colleague, a family member, or an institution you've dealt with for years.

Fraud rarely leans on just one of these. The scams that actually work tend to stack two or three together — fear and authority in a digital arrest call, trust and urgency in a deepfake voice call.

3 Common Types of Digital Frauds in India

Illustrative Cases, Warning Signs and Prevention Measures

3.1 UPI and QR Code Frauds

What Happens?

This one trades on a simple, widespread misunderstanding, that scanning a QR code and entering a UPI PIN is sometimes needed to receive money. It never is. Fraudsters use that confusion to make victims authorise a payment while believing they're about to receive one.

Case Study: The Refund That Became a Payment

A resident of Pune had listed a used smartphone for sale online. A buyer showed interest, agreed on a price, and said he would send ₹20,000 through a QR code. The seller scanned it and, when prompted, entered his UPI PIN ,assuming that was simply how the payment would land in his account. Instead, ₹20,000 left his account within seconds.

Red Flags

01. Receiving money should never require a PIN.

02. Urgent requests to scan QR codes.

03. Buyers insisting on immediate payment confirmation.

Key Lesson

Your UPI PIN is only ever needed to send money — never to receive it.

3.2 Digital Arrest Scam

What Happens?

Fraudsters pose as police officers, cybercrime officials, customs staff, or officials from a central investigating agency. The story usually involves one of a few claims: your Aadhaar has been misused, a parcel in your name contains something illegal, your bank accounts are linked to money laundering, or a warrant has already been issued. Victims are kept on video calls for hours, sometimes days, and pressured into transferring money into accounts described as "safe" or needed for "verification."**Victims are told:**

- Aadhaar has been misused.
- A courier parcel contains illegal goods.
- Bank accounts are linked to money laundering
- Arrest warrants have been issued.

Victims are often forced to remain on video calls for hours and transfer funds into "safe" accounts.

Case Study: The Retired Professor

A retired professor received a call from someone claiming to represent a law enforcement agency, who told her that her Aadhaar number had been used to open bank accounts linked to money laundering. Over the following two days she stayed on video calls with people posing as investigators, believing she was cooperating with a genuine inquiry. She eventually moved more than ₹1 crore across several accounts before mentioning it to a family member — who was the one to tell her it was a scam.

Red Flags

01. Threats of imminent arrest.

02. Being asked to stay on a video call, sometimes for hours at a stretch.

03. Explicit instructions to keep the matter secret, even from family.

04. Any request to transfer money for “verification.”

Key Lesson

There is no such thing as a ‘digital arrest’ under Indian law. No investigation or arrest happens over a video call.

3.3 Deepfake Family Emergency Scam

What Happens?

AI voice cloning is used to imitate the voice of a family member, usually inside a scenario built for panic an accident, a legal problem, a medical emergency abroad.

Case Study: The Son Who Never Called

A businessman received a WhatsApp call that sounded, unmistakably, like his son studying overseas — distressed, describing a road accident, asking urgently for money for treatment and legal costs. The likeness was close enough that verifying didn’t even occur to him, and he transferred ₹5 lakh before calling his son back on a different number and learning that no accident had happened at all..

Red Flags

01. An emergency that needs money transferred immediately.

02. The call itself arriving from an unfamiliar number.

03. Any resistance to you hanging up to check with someone else first.

Key Lesson

Before sending money in response to a family emergency, call back on a number you already have — not the one the call came from.

3.4 Fake Bank Officer Scam

What Happens?

Fraudsters impersonate bank staff, typically over SMS or a phone call, to extract login details or OTPs.

Case Study: The KYC Expiry Message

A bank customer received a text warning that his account would be blocked unless he updated his KYC immediately, along with a link to what looked like his bank’s website. He entered his account number, password, and OTP on the page — all of which the fraudsters used within minutes to clear out the account.

Red Flags

01. KYC “urgently due for renewal” messages.

02. Shortened or unfamiliar-looking links.

03. Any request, however official it sounds, for an OTP.

Key Lesson

No bank will ever ask you for your OTP, password, or PIN — not by call, not by SMS, not by email.

3.5 Fake Customer Care Scam

What Happens?

Fraudsters plant fake customer care numbers in search results or social media ads, so the “helpline” a victim finds is theirs, not the company’s.

Case Study: The Airline Refund

A traveller searching for an airline’s customer care number online ended up calling a fraudster’s number instead of the airline’s. The person on the other end talked him into installing a screen-sharing app to “process the refund faster.” Within minutes his banking credentials were visible on the other end, and the money was gone.

Red Flags

01. Being asked to install AnyDesk, TeamViewer, or similar remote-access apps.

02. A request to share your screen with “support.”

03. Any request for full card details over a call.

Key Lesson

Never install remote-access software at the request of customer support.

3.6 Investment Scam

What Happens?

Victims are lured with promises of unusually high, often guaranteed, returns through stock trading, cryptocurrency, or exclusive investment groups.

Case Study: The WhatsApp Trading Group

A working professional joined a stock-trading group on WhatsApp that regularly posted screenshots of large profits. He was allowed to withdraw small early gains, which built his confidence, so he put in larger amounts. When he tried withdrawing this time, the platform simply stopped responding. His losses came to more than ₹35 lakh..

Red Flags

01. Returns that are guaranteed, or unusually high and consistent.

02. Pressure to invest quickly, before an “opportunity closes.”

03. A platform with no SEBI registration.

Key Lesson

If the returns sound too good to be true, they are no exceptions.

3.7 Job and Task Completion Fraud

What Happens?

Victims are recruited for simple online “tasks”, reviewing products, liking videos, that eventually require a deposit to unlock bigger payouts.

Case Study: Earn ₹5,000 Per Day From Home

A college student took up an offer to review products online. Early tasks paid out small amounts as promised. Later ones asked for a deposit to “unlock” higher-paying assignments. Over a few weeks he deposited more than ₹3 lakh chasing the next payout, before the platform stopped responding altogether.

Red Flags

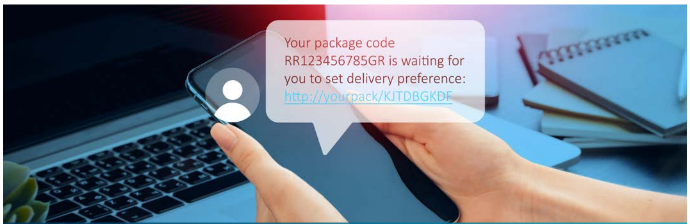
01. Any job that asks you to pay money before you can earn it.

02. Payment requirements that keep growing.

03. Earnings that sound disproportionate to the effort involved.

Key Lesson

Legitimate employers do not require employees to pay money to earn money.



3.8 Courier and Parcel Fraud

What Happens?

Victims are told a parcel sent in their name has been intercepted and found to contain something illegal.

Case Study: The International Parcel Investigation

A man received a call claiming a parcel under his name had been intercepted, allegedly containing passports, narcotics, and foreign currency. The call was passed between several people posing as different agencies, each adding to the urgency, until he transferred money for what he was told was "verification." None of it was real..

Red Flags

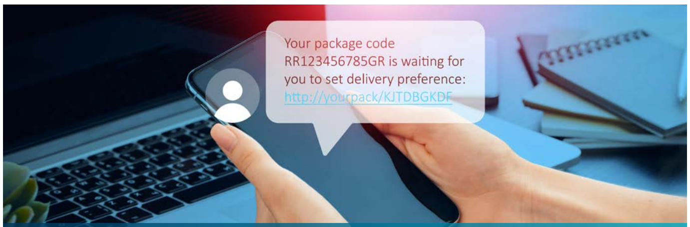
01. Criminal accusations tied to a parcel you never sent.

02. Being transferred between multiple "officials."

03. Any demand to keep the call secret.

Key Lesson

A genuine investigation is never funded by the person being investigated.



3.9 SIM Swap Fraud

What Happens?

Fraudsters obtain a duplicate SIM in the victim's name, using forged documents or insider help at a telecom outlet, and use it to intercept banking OTPs.

Case Study: Overnight Account Drain

A business owner's phone lost network out of nowhere. Within a few hours, several transactions had gone through on his bank accounts. It turned out fraudsters had obtained a replacement SIM using forged identity documents and used the OTPs meant for him..

Red Flags

01. Your phone suddenly losing network for no clear reason.

02. A SIM that deactivates without you requesting it.

03. OTPs that stop arriving

Key Lesson

Immediately contact your telecom provider if your SIM unexpectedly stops working.

3.10 Aadhaar and Identity Theft

What Happens?

Stolen personal details are used to take out loans or open accounts in someone else's name.

Case Study: Loans Never Taken

A salaried employee started getting recovery calls for loans he had never applied for. It turned out fraudsters had used forged documents built around his stolen personal details to take out multiple loans — he only found out once the recovery notices started arriving.

Red Flags

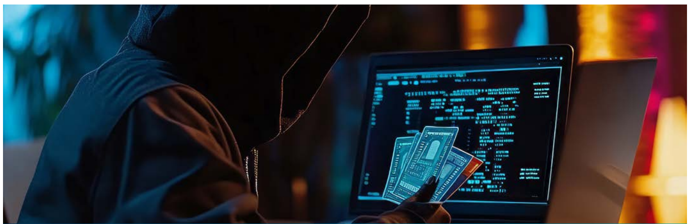
01. Loan offers or confirmations you never applied for.

02. Credit inquiries you don't recognise.

03. Recovery calls for debts that aren't yours.

Key Lesson

Check your credit report periodically — it's often the earliest place identity theft shows up.



3.11 Mule Account Fraud

What Happens?

People are paid to let criminals route money through their bank accounts.

Case Study: Easy Money for Students

A student was offered ₹10,000 a month just to let transactions pass through his account. Months later, investigators traced cybercrime proceeds to that account. He said he didn't know what the money was for — that didn't stop him from being investigated.

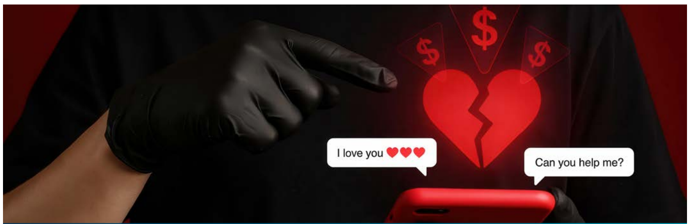
Red Flags

01. Being offered money simply to receive and forward funds.

02. Income with no real explanation for where it's coming from.

Key Lesson

You're legally responsible for all transactions through your bank account.



3.12 Romance Scam

What Happens?

A fraudster builds an emotional relationship online over weeks or months before asking for money.

Case Study: The Overseas Partner

A woman developed an online relationship with someone claiming to work abroad. He repeatedly asked for money, saying he was detained at customs. By the time she stopped, she had lost over ₹20 lakh.

Red Flags

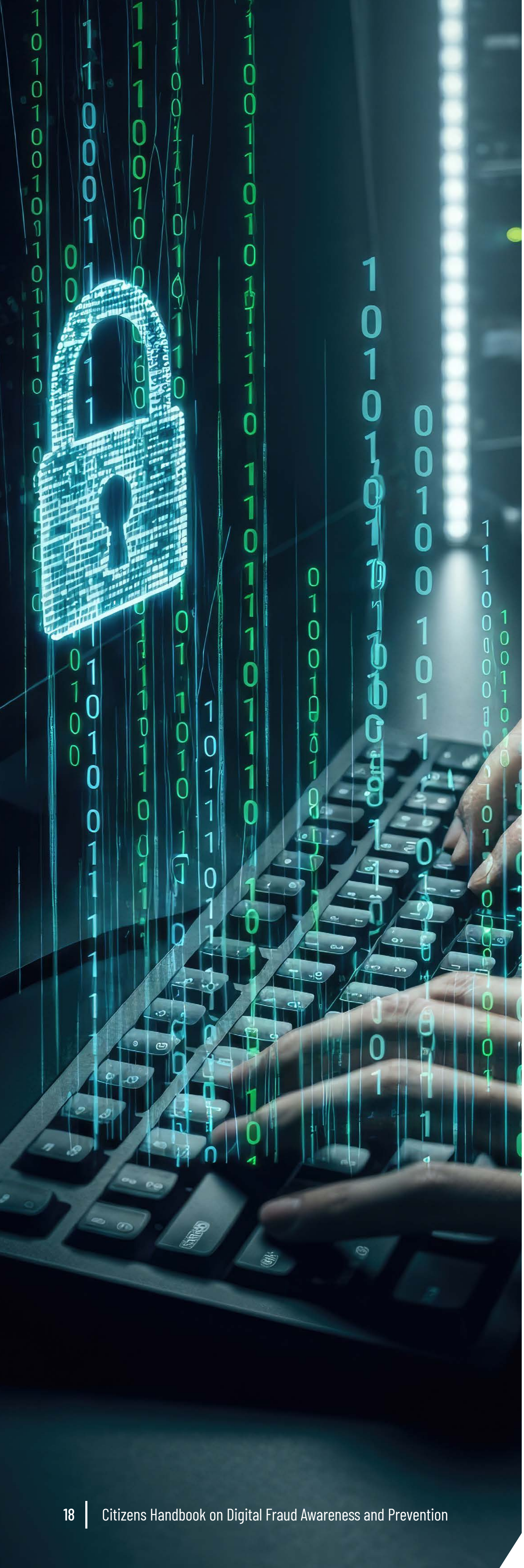
01. A partner who always has a reason not to meet or video call.

02. Any request for money, however small at first.

Key Lesson

However real the relationship feels, financial verification still applies — trust and money are separate questions.


AI-THREAT
DETECTION



4

Protecting Yourself and Your Family

Mobile Security Essentials

A few habits go a long way:

- Keep a lock screen enabled, always
- Install security updates as soon as they're available, not weeks later
- Download apps only from the Play Store or App Store, never sideloaded APKs
- Check what permissions an app is asking for, and say no to anything that doesn't make sense for what it does

Banking Security Practices

- Turn on transaction alerts for every account
- Glance through your statement regularly, not only when something feels off
- Avoid banking over public Wi-Fi
- Stick to your bank's own app rather than third-party apps that claim to "manage" your accounts

Password Security

A strong password is unique to that one account, long enough to be hard to guess, and not built around your birthday or your pet's name. Wherever multi-factor authentication is available, turn it on — it's a small extra step that blocks a large share of account takeovers on its own.

Protecting Senior Citizens

Senior citizens are targeted often, not because they're careless, but because fraudsters bet on unfamiliarity with newer scam formats and a natural instinct to respect authority. Families can help by agreeing on a simple verification habit in advance — a rule that any money request, however urgent it sounds, gets confirmed with another family member first — along with a short list of emergency contacts and the occasional conversation about whatever scam format is currently doing the rounds.

Protecting Children

Children need a different kind of awareness — around gaming scams that ask for in-game purchases or account details, social media contacts who aren't who they claim to be, oversharing personal information, and grooming behaviour that starts out as friendly conversation. These conversations tend to work better as ongoing, low-key check-ins than as a single lecture.

5

AI, Deepfakes and the Future of Fraud

Understanding the New Age of Digital Fraud

Artificial intelligence is changing how healthcare, education, banking, and public services function — mostly for the better. It's also changing how fraud works, and not in a direction that favours citizens.

Scams built on AI are faster to produce, cheaper to run, and far more personalised than what came before. Older scams often gave themselves away — broken English, an odd sender address, a story that didn't quite add up. AI-generated fraud doesn't have those tells anymore. It can sound like a real person, write like a real institution, and hold up under a level of scrutiny that used to be enough to catch a scam.

What's now possible, cheaply and at scale, includes convincingly human conversations, realistic voice clones, deepfake video, phishing messages tailored to the recipient, fabricated identities, chat interactions run by AI rather than a person, and fake websites or documents good enough to survive a casual glance.

As these tools keep improving, the usual signs of fraud will keep getting harder to spot. The practical response is to build a habit of continuous verification rather than relying on gut feel.

Never Trust Solely Based On

- Voice
- Video
- Social media profiles
- Display names
- Caller IDs
- Screenshots
- Digital documents
- Online reviews

Real trust comes from checking independently, through a channel the other side didn't control.

5.1 Deepfake Voice Scams

What is Voice Cloning?

Voice cloning uses AI to recreate someone's voice from a short audio sample, a few seconds pulled from a YouTube video, a public speech, or even a WhatsApp voice note is often enough. From there, a fraudster can generate entirely new sentences in that voice, saying things the real person never said.

Case Study: "Dad, I Need Help Right Now"

A businessman received a WhatsApp call that sounded, unmistakably, like his son studying abroad distressed, describing a road accident, asking urgently for money for treatment and legal fees. He transferred several lakh rupees before checking. When he reached his son on another number later that day, there had been no accident. The voice had been synthetic.

Warning Signs

01. A crisis that needs money sent immediately.

02. The call arriving from a number you don't recognise.

03. Pressure not to check with anyone else first.

Prevention Tips

- Call back on a saved number before doing anything else.
- Agree on a verification step as a family, in advance.
- Consider a shared code word for genuine emergencies — something a stranger, or an AI, wouldn't know.

5.2 Deepfake Video Scams

What Are Deepfake Videos?

Deepfake video uses AI to generate footage of someone saying or doing things they never did, replicating expressions, lip movement, voice, and mannerisms closely enough to pass a casual watch

Case Study: The CEO Approval

A finance manager took a video call that appeared to be from his company's CEO, instructing him to process an urgent, confidential payment tied to an acquisition. The appearance and voice checked out, so the payment went through. It was only afterward that the video was confirmed to be a deepfake.

Warning Signs

01. Instructions to keep a transaction confidential.

02. Pressure to skip the usual approval steps.

03. Urgency around a large payment.

Prevention Tips

- Stick to approval workflows even when the request looks like it's from the top.
- Confirm through a separate channel before acting.
- Require more than one sign-off for high-value transfers, no exceptions.

5.3 AI-Powered Phishing

The Evolution of Phishing

Old phishing emails often gave themselves away — spelling errors, odd formatting, a tone that didn't quite match the sender. AI-written phishing doesn't have those problems anymore. It reads as grammatically correct, personalised to the recipient, aware of context, and hard to distinguish from something genuine.

Case Study: The Perfect Bank Email

A customer got an email that looked exactly like it came from his bank — correct branding, references to real recent account activity, no errors anywhere. He clicked through and entered his login details on what turned out to be a fake page. The fraudsters had account access within minutes.

Warning Signs

01. Any email asking you to log in through a link rather than the app or website directly.

02. Unexpected security alerts.

03. Urgency around "updating" account information.

Prevention Tips

- Type your bank's website address directly, or use the app — don't click through email links.
- If something feels urgent, verify through the bank's official number before doing anything.

5.4 Synthetic Identity Fraud

What Are Synthetic Identities?

A synthetic identity blends real information with fabricated details to build a person who doesn't actually exist , a real Aadhaar number, say, paired with a stolen PAN, a fake address, and an AI-generated photograph. These constructed identities get used to open accounts, take out loans, and move fraud proceeds through the banking system.

Case Study: The Loan That Never Existed

A salaried employee started getting collection notices for personal loans he hadn't taken. It came out that fraudsters had combined his stolen details with fabricated information to build a synthetic identity and take out loans from several lenders — he only learned about it months after the fact

Prevention Tips

- Check your credit report on a regular schedule, not just when something seems wrong.
- Look over your financial records periodically.
- Report anything unfamiliar the moment you spot it.

5.5 AI Chatbots Used for Fraud

The Rise of Fraud Automation

AI chatbots can now carry on realistic conversations with a victim for weeks, and unlike a human fraudster, the same system can run thousands of these conversations at once.

Case Study: The Investment Advisor

A retired professional signed up on an online investment platform where an AI assistant provided market updates and portfolio advice over several weeks. The conversations felt professional and genuinely personalised, and trust built up gradually. He eventually transferred a significant sum, and the platform disappeared not long after.

Lesson Learned

Trust that builds slowly through repeated conversation can be just as dangerous as trust built through a real relationship, the platform behind it doesn't need to be a real person for the manipulation to work.

5.6 Social Media Deepfake Impersonation

What Happens?

Fraudsters build fake profiles using AI-generated photos and stolen personal details often more polished-looking than a real account.

Case Study: The Fake Army Officer

Someone built an online friendship with a person claiming to be an army officer posted overseas, complete with photos, videos, and supporting documents that all looked genuine. Trust built over months before the request for money came. It later turned out the entire identity — photos, documents, backstory — had been fabricated using AI-generated content..

Warning Signs

- Consistent refusal to meet or video call live.
- A string of emergencies.
- Requests for money.
- A profile with very little verifiable history behind it.

5.7 The Future of Fraud

A few directions this is likely to head in next:

Real-Time Voice Cloning

Impersonating a family member live, mid-conversation, rather than only in a pre-recorded clip.

Autonomous Fraud Agents

AI systems running scams with little to no human involvement at all.

Hyper-Personalized Fraud

Scams built around personal details gathered automatically from across multiple platforms at once.

Deepfake Government Officials

Convincing impersonations of police, regulators, or other authorities.

Fake Evidence Generation

Fabricated documents, screenshots, emails, audio, and video good enough to hold up under a quick check.

6 Citizen Rights and Legal Protections in India

Information Technology Act, 2000

The IT Act is the main law covering cyber offences in India. It provides for action against identity theft, unauthorised access, data theft, and cybercrime more broadly, and gives authorities the power to investigate and prosecute offenders under these provisions.

Bharatiya Nyaya Sanhita, 2023

The BNS, which replaced the IPC, covers cheating, impersonation, forgery, criminal intimidation, and financial deception. Digital fraud cases are frequently prosecuted under these provisions alongside the IT Act.

Digital Personal Data Protection Act, 2023

The DPDPA strengthens how personal data must be handled and places real obligations on organisations that collect or process it. Citizens now have a clearer right to know how their information is being used — which matters directly, since so much fraud starts with data that shouldn't have been so easy to get hold of.

RBI Customer Protection Framework

RBI guidelines protect customers against unauthorised electronic transactions, and that protection is strongest when the fraud is reported quickly. This is one of the more practical reasons not to sit on a fraud out of embarrassment — reporting fast genuinely improves the odds of both liability protection and recovery.

7 What To Do If You Become a Victim

The First Golden Hour

If you realise something has gone wrong, act immediately:

- Contact your bank.
- Ask them to freeze the affected account.
- Change your passwords.
- Disable or disconnect any device you think has been compromised.
- Tell your family — partly for support, partly because a second person thinking clearly helps

Report the Incident

National Cyber Crime Helpline

1930

Cyber Crime Reporting Portal

File a report as soon as you can. The earlier it's reported, the better the chances of freezing the transaction before the money moves further and becomes harder to trace.

Preserve Evidence

Hold on to whatever you can:

- Screenshots
- SMS messages
- Emails
- Call recordings, if you have any
- Transaction IDs
- UPI reference numbers

This evidence often makes the difference in how quickly an investigation can move.

8 Institutional Ecosystem for Citizen Protection

India has built a fairly layered system to deal with cybercrime, involving:

- The Ministry of Home Affairs
- The Indian Cyber Crime Coordination Centre (I4C)
- The Indian Computer Emergency Response Team (CERT-In)
- The Reserve Bank of India
- State cybercrime cells
- Banks and other financial institutions
- Telecom service providers

It's worth getting familiar with how to reach these before you ever need to. Trying to work out who to call while you're also trying to stop money leaving your account is not the ideal time to be doing that research.

9 Fraud Prevention Checklist

Before you make any payment, run through this quickly:

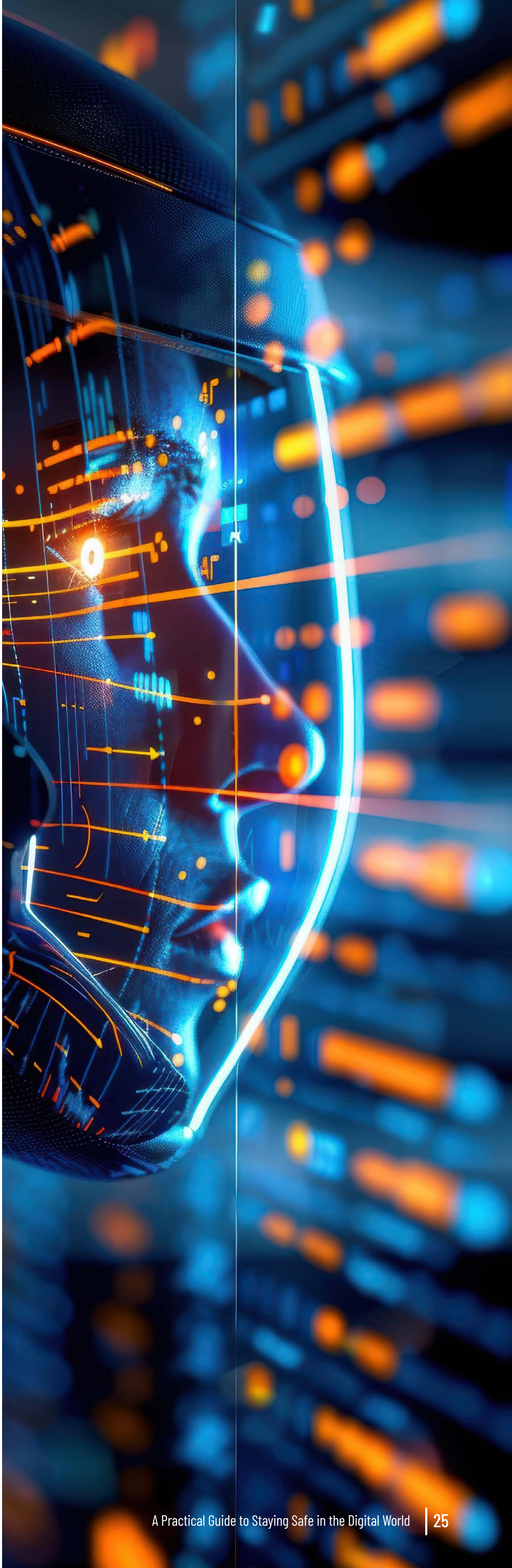
- Verify who you're actually paying.
- Confirm unusual requests independently, through a separate channel.
- Read the transaction details before confirming, not after.
- Treat urgency as a warning sign, not a reason to hurry.
- Never share an OTP with anyone, for any reason.
- Never share a PIN with anyone, for any reason.
- Never give a stranger remote access to your device.
- Verify any claimed law enforcement contact through an official channel, not the number they gave you.

10 Building a Cyber-Aware India

Technology alone won't fix this. It takes awareness, a habit of checking rather than assuming, sensible digital behaviour, and communities that talk about scams openly instead of treating them as something embarrassing to admit to.

Every citizen has some part to play in keeping India's digital systems trustworthy. As fraud gets more sophisticated, public awareness has to keep pace with it — arguably outpace it.

The safest people online usually aren't the most technically skilled. They're the ones who've built the habit of pausing before they act.



CONCLUSION:

Building a Safer Digital India Starts with Every Citizen

India's digital shift has given millions of people real, practical access to banking, payments, government services, healthcare, education, and everyday commerce that simply didn't exist in this form before. UPI transactions that clear in seconds, online investments, digital identity systems, mobile-first services — all of this is now just part of ordinary life.

The same tools that made this convenient have also become useful to people running fraud at scale. Digital fraud isn't limited anymore to phishing emails or the old lottery-winner SMS. Today's fraudsters work with artificial intelligence, deepfakes, social engineering, and personal data pulled from breaches, often as part of an organised operation rather than a lone scammer working alone.

Fraud doesn't discriminate by education or income. Students, homemakers, professionals, business owners, senior citizens, and people who consider themselves tech-savvy have all been caught out at some point. What most of these cases have in common isn't a lack of intelligence — it's a moment where trust, urgency, fear, or emotion got the better of caution.

As fraud keeps evolving, so does the response to it. Banks, telecom providers, regulators, and law enforcement are all tightening safeguards and reporting systems, and that work matters. But none of it fully substitutes for a citizen who knows what to look for and pauses before reacting.

Awareness genuinely is the first line of defence here. Questioning an unexpected request, verifying an identity before trusting it, keeping personal information a little more guarded, and reporting anything that feels off — these habits, practiced consistently, prevent more fraud than any single piece of technology.

AI is going to make this harder before it gets easier. Cloned voices, deepfake video, synthetic identities, and scams built around personal detail will keep chipping away at the usual signs people rely on to spot fraud. Verification can no longer be based only on what you see or hear — it has to become routine, the way locking your front door is routine.

This isn't only an individual responsibility, either. Families should talk to children and older relatives about the scams currently doing the rounds. Schools have room to fold basic digital safety into what they already teach. Workplaces benefit from periodic awareness sessions. Communities do better when reporting a scam is treated as useful information-sharing, not an admission of having been foolish.

A country this digitally ambitious also needs to be digitally cautious — the two go together, not against each other. And what holds the whole system up, ultimately, is trust: trust in digital payments, in online services, in digital identity, in whatever comes next. Keeping that trust intact is a shared job between citizens, businesses, regulators, and government.

Three things are worth carrying forward from this handbook:

Stop before reacting to pressure, fear, urgency, or excitement.

Verify anything involving money, personal information, or account access.

Report suspicious activity immediately — to your bank, your service provider, or the right authority.

Fraud will keep changing shape. An informed citizen — one who's built the habit of pausing and checking — remains the most reliable defence against it, either way.

Stop. Verify. Report.

About FTCCI

The Federation of Telangana Chambers of Commerce and Industry (FTCCI) is a prominent industry body in Telangana, India, established in 1917 to support trade and industry and represent business interests to the government. Originally formed to represent the Hyderabad State under the Nizam, it has evolved over the decades, including a period as the Federation of Andhra Pradesh Chambers of Commerce and Industry, and after the bifurcation of Andhra Pradesh in 2014, it was renamed FTCCI.

FTCCI has been energising industry for a 100 years. They have been engaging with the government to represent their members, and played a key role in enabling change through meaningful interactions for an entire century.

Address:
Federation House
Federation Marg, Hari Nagar, Red Hills,
Hyderabad, Telangana 500004, India

Acknowledgement

Chair, ICT Committee: Sri Bala Prasad Peddigari
Co-Chair, ICT Committee: Sri Pankaj Diwan

Members:
Sri Lalit Sharma, Sri Vidyasagar, Sri Shreeram Iyer,
Sri Paidimarry Vinod Kiran, Sri Sridhar Seshadri,
Smt. P. Sangeetha, Director
have contibuted to this publication.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and its independent and locally owned member firms provide clients with consulting and managed solutions in finance, technology, operations, data, digital, legal, HR, risk and internal audit through a network of more than 90 offices in over 25 countries.

Named to the Fortune 100 Best Companies to Work For® list for the 11th consecutive year, Protiviti Inc. has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with government agencies and smaller, growing companies, including those looking to go public. Protiviti Inc. is a wholly owned subsidiary of Robert Half (NYSE: RHI).

Contacts

Sandeep Gupta
Managing Director
sandeep.gupta@protivitiglobal.in
+91 9702730000

Vaibhav Koul
Managing Director
vaibhav.koul@protivitiglobal.in
+91 9819751715

Sayantan Bose
Managing Director
sayantan.Bose@protivitiglobal.in
+91 9818880941

Sahil Chander
Managing Director
sahil.chander@protivitiglobal.in
+91 8800490154

Nikunj Garg
Managing Director
nikunj.garg@protivitiglobal.in
+91 9818537621

Ajay Malik
Managing Director
ajay.malik@protivitiglobal.in
+91 9987071312

Kishan Malineni
Managing Director
kishan.malineni@protivitiglobal.in
+91 7396484555

Mithilesh Singh
Managing Director
mithilesh.singh@protivitiglobal.in
+91 9029955267

Prashant Singh
Managing Director
p.singh@protivitiglobal.in
+91 9739179111

Sarita Padmini
Senior Director
sarita.padmini@protivitiglobal.in
+91 9953043552

Shobhit Singhal
Senior Director
shobhit.singhal@protivitiglobal.in
+91 9899299539

Nagesh Akula
Senior Director
nagesh.akula@protivitiglobal.in
+91 9866694411

Acknowledgement

Sri Vaibhav Koul - Managing Director (Technology and Digital), Sri Kishan Malineni - Managing Director (Technology and Digital), Sri Nagesh Akula - Senior Director (Technology and Digital) have contibuted to this publication.

NOTES

Face the Future with Confidence®

This publication has been carefully prepared, but should be seen as general guidance only. You should not act or refrain from acting, based upon the information contained in this publication, without obtaining specific professional advice. Please contact the person listed in the publication to discuss these matters in the context of your particular circumstances. Neither Protiviti India Member Private Limited nor the shareholders, partners, directors, managers, employees or agents of any of them make any representation or warranty, expressed or implied, as to the accuracy, reasonableness or completeness of the information contained in the publication. All such parties and entities expressly disclaim any and all liability for or based on or relating to any information contained herein, or error, or omissions from this publication or any loss incurred as a result of acting on information in this presentation, or for any decision based on it.

©2026 Protiviti India Member Private Limited