Based on National Cyber Crime Portal & Official Safety Rules

LATEST 2026 EDITION

How to Stay Safe from WhatsApp Scams

A complete, easy pocket guide for everyday smartphone users to stay safe on WhatsApp

12	100%	4
Detailed Chapters	Verified Rules	Golden Rules

OTP Scam • Fake APK • Part-Time Job • AI Voice Fraud

Safe WhatsApp • Aware Family • Strong India

2026 Mobile Pocket Edition • Published in Public Interest

LEGAL NOTICE • DISCLAIMER

Legal Terms and Rules of Use

1. Public Awareness Purpose

This eBook is an independent guide created solely to raise cyber safety awareness among everyday citizens. Its goal is to warn readers about scams and frauds happening on WhatsApp. It is not legal or financial advice.

2. No Affiliation with Any Organization

This eBook is not sponsored, endorsed, or approved by Meta, WhatsApp LLC, Reserve Bank of India (RBI), NPCI, the Telecom Department, or any agency of the Government of India. It is an independent digital guide.

3. Limitation of Liability

Cyber safety rules, app settings, and government website addresses can change over time. Neither this eBook nor its author is responsible for any online fraud, technical issue, or financial loss faced by any reader. Always check the official website of the concerned authority for the latest updates.

4. Trademarks and Brand Names

'WhatsApp' and 'Meta' are registered trademarks of Meta Platforms. 'UPI' is a registered trademark of NPCI. All other names mentioned in this book (such as Google Pay, PhonePe, Telegram, etc.) belong to their respective owners and are used only for identification under Fair Use.

5. Description of Methods (No Real Names)

All examples and case studies in this book use fictional names solely to explain how scams work. No real person, company, or organization is called a fraudster; only the methods of fraud are exposed.

6. Single-User Digital License

This eBook is strictly for the buyer's personal reading. Unauthorized printing, re-uploading on the internet, or reselling of this eBook is strictly prohibited.

© 2026 All Rights Reserved • Independent Guide Based on 100% Verified Facts

EDITORIAL • PREFACE

Preface: Why Do You Need This Guide?

Today in India, **over 50 crore people** use WhatsApp every day. From morning wishes to family chats, children's schoolwork, and office tasks—everything runs on this one app.

Because we stay connected with friends and relatives on WhatsApp, our trust here is the deepest. Cyber scammers take unfair advantage of this exact trust. Every day we hear about someone sending money after seeing a familiar profile photo, installing a virus disguised as a wedding card, or losing lakhs in a fake part-time job.

> **A scammer never hacks WhatsApp's servers—they play with human trust and panic. They trick us into sharing our own OTP or clicking a fake link by mistake.**

Most frauds succeed only because everyday users do not know 2–3 basic WhatsApp security settings. Millions still do not know the biggest rule: *"Never*

share your 6-digit WhatsApp registration code with anyone, not even someone you know."

Purpose of This eBook:

This eBook is written in **simple, everyday language**, not hard technical jargon. Through 12 chapters filled with real-world case studies, actual scammer dialogues, and verified rules from the Cyber Crime Portal, its sole aim is to keep you and your family completely safe.

Read this guide yourself and share it with your family, parents, and friends. A little awareness from you is the strongest shield for your family's hard-earned savings.

TABLE OF CONTENTS

Complete Chapter List

1. **Chapter 1: How WhatsApp Scams Happen**
   The game of fear and greed, 4 main traps, and the truth about encryption
2. **Chapter 2: Secure Your WhatsApp Account**
   Two-Step Verification, Linked Devices, and Privacy Settings
3. **Chapter 3: The OTP Account Takeover Scam**
   How your 6-digit registration code is stolen and how to recover your account
4. **Chapter 4: Fraud Links and APK Files**
   Protection from wedding card, e-challan, and electricity bill viruses
5. **Chapter 5: Fake Jobs and Work-from-Home Offers**
   Spotting YouTube Like and part-time task job traps
6. **Chapter 6: Asking for Money Using a Known Person's Name**
   Stolen profile photos, fake relative excuses, and emergency fraud
7. **Chapter 7: WhatsApp UPI Payment and QR Scams**
   You never need a PIN to receive money — chat payment safety
8. **Chapter 8: Fake Investment and Tip Groups**
   Staying safe from stock market and crypto Ponzi groups
9. **Chapter 9: Unknown Groups and Fake Profiles**
   Stopping frauds from international numbers
10. **Chapter 10: AI Voice and Video Fraud on WhatsApp**
    Protection from voice cloning and video call blackmail
11. **Chapter 11: What to Do After a Scam & How to**

Complain
Golden 2 Hours, Cyber Crime Portal, and WhatsApp reporting

12 **Chapter 12: WhatsApp Safety Checklist**
Master pocket safety checklist and quick rules

• **Appendix:** Printable Safety Card, Cyber Safety Glossary & Back Cover

CHAPTER 1 • BASICS

How WhatsApp Scams Happen

The game of fear and greed, the 4 main paths scammers use, and the truth about encryption.

WhatsApp: Everyday Convenience and a Scammer's Playground

Today, there is hardly a smartphone in India without WhatsApp. From sending 'Good Morning' messages to family chats, school updates, and office work—everything happens on this single app.

Because we talk to friends and family on WhatsApp, our guard is naturally down. Scammers exploit this trust ruthlessly. They know you might ignore a shady website, but if the same trap arrives on WhatsApp under a familiar name, you are far more likely to trust it.

Key Point to Remember

Hackers Don't Break Through Your Screen!

Most people imagine a hacker using magic software to pull money straight from their bank. **That is completely false.**

The scammer's real trick: They don't break into your phone—they play with your mind. They get you to make the mistake yourself, like tapping a fake link or sharing your OTP in a rush.

A Scammer's 2 Biggest Weapons: Greed and Fear

Whenever a scammer messages you, they target two human weak spots—greed and panic:



1. Greed (The Bait Trap)

"Earn ₹3,000 daily from home", "Get 3 months of free recharge", or "Congrats! You won a ₹25 lakh lottery."

Goal: To sell you the dream of easy money so you click without thinking.

⚡

2. Fear and Panic (The Rush Trap)

"Your electricity will be cut tonight", "Your SIM card is getting blocked", or "Your son is in the hospital, send money now."

> **Goal:** To leave you no time to think or ask anyone, pushing you to transfer money in sheer panic.

Case Study: One Small Mistake by Sumit from Jaipur

What happened to 34-year-old Sumit in Jaipur can happen to anyone. One evening, he suddenly received this message on WhatsApp:

💬 WHATSAPP CHAT (BOSS'S DP ON AN UNKNOWN NUMBER)

> **Director (using stolen DP):** "Sumit, I'm stuck in an urgent client meeting and my online banking isn't logging in. Transfer ₹45,000 to this vendor right away. I'll reach the office in an hour and give you cash."

> **Sumit:** "Yes sir, sending it right now."

Sumit saw his boss's photo and transferred ₹45,000 without calling to check. Half an hour later, when the real Director walked into the office, Sumit learned he had never sent any such message! The photo had been stolen from the internet.

Lesson: Never trust a message just because of a profile photo (DP). Before sending money, always make a normal phone call to the person's real number and hear their voice.

The Scam Cycle: How They Trap You

Almost every WhatsApp fraud follows these 4 steps:

Step 1

Message from an Unknown Number

A flattering profile photo, a great job offer, or a scary electricity bill notice arrives.

↓ Creating greed or fear

Step 2

Making You Take an Action

The scammer says: "Click the link below", "Open this wedding card", or "Tell me your 6-digit code."

↓ Malware on phone or OTP stolen

Step 3

Gaining Access to Your Bank or Account

A fake file installs spyware on your phone, or your WhatsApp opens on the scammer's device.

↓ Financial loss

Step 4

Money Gone and Number Blocked

Money disappears from your account, and the scammer immediately blocks you everywhere and vanishes.

A Big Myth: "WhatsApp Is Encrypted, So How Can Fraud Happen?"

Many people ask: *"WhatsApp says everything is End-to-End Encrypted—how can anyone still scam us?"*

Simple Example

The Lock and Key Truth

What End-to-End Encryption means: No third party can read your messages while they travel between you and the other person. It works like a strong safe lock.

But remember: If you hand the key to that safe (your OTP or PIN) directly to the thief, the lock cannot save you. Scammers trick you, not the technology.

Chapter 1: Do's and Don'ts

✅ Always Do This (DOs)

• If someone asks for money, call their real saved number on a normal phone call first.

• Think twice before opening any link sent from an unknown number.

• **Report** and **Block** fake messages right inside WhatsApp.

❌ Never Do This (DONTs)

• Never assume a number belongs to your friend or boss just by looking at the DP.

• Never share your 6-digit WhatsApp code with anyone.

• Never fall for free recharge or easy work-from-home promises.

Where to Report and Get Official Help

If you face cyber fraud or receive a fake message, visit only official government portals:

1. **National Cyber Crime Portal**
   To immediately report cyber fraud and financial loss, visit: `cybercrime.gov.in`

2. **Chakshu Portal (Telecom Department)**
   To report fake WhatsApp calls and fraud messages, visit: `sancharsaathi.gov.in`

3. **Safe Way to Search on Google**
   Search directly with this safe keyword: **`cybercrime reporting portal`**

Official Verification Source

- Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs: `cybercrime.gov.in`
- Telecom Department (Sanchar Saathi Chakshu): `sancharsaathi.gov.in`
- WhatsApp Security Guidelines: `faq.whatsapp.com`

CHAPTER 2 • SECURITY SETTINGS

Secure Your WhatsApp Account

5 easy settings in 5 minutes that protect your WhatsApp 100% from hackers.

Old Phone or New: These 5 Minutes of Safety Are Essential

Most people install WhatsApp and start chatting right away without ever opening its security settings.

As a result, your account stays wide open by default. Any stranger can add you to fake groups, download your profile photo, or even spy on your chats if they hold your unlocked phone for 30 seconds.

Golden Rule

WhatsApp's Strongest Lock: Two-Step Verification

Whenever you set up WhatsApp on a new phone, a 6-digit SMS OTP arrives. But if you turn on **Two-Step Verification**, WhatsApp also asks for a second secret PIN after the SMS.

Biggest benefit: Even if a thief steals your SIM or SMS OTP, they can never open your WhatsApp without your secret 6-digit PIN!

How to Turn On Two-Step Verification (Step-by-Step)

Take these 4 easy steps inside WhatsApp right now:

1 **Open Settings**
Open WhatsApp, tap the 3 dots at the top right, and choose **Settings**.

↓ Go to Account

2 **Select Two-step verification**
Tap **Account → Two-step verification** and press **Turn on**.

↓ Create a 6-Digit PIN

3 **Enter Your Secret PIN**
Set a 6-digit PIN of your choice. (Never use easy numbers like 123456 or your birth date.)

↓ Add an Email

4 **Add a Safe Email Address**
Link your personal email so you can easily reset the PIN if you ever forget it.

4 Other Must-Change Settings Today



1. Check Linked Devices (Stop WhatsApp Web Spying)

Sometimes someone borrows your phone for 1 minute and links your WhatsApp Web to their laptop.

> **What to do:** Open 3 dots ➔ **Linked devices**. If you see any unknown computer, tap **Log out** right away.

🔇

2. Silence Unknown Callers (Block Stranger Video Calls)

This is the best way to stop obscene video calls and blackmail from international numbers (+92, +84, +62).

> **Turn it on:** Go to **Settings ➔ Privacy ➔ Calls ➔** Turn on **Silence unknown callers**.

👥

3. Groups Privacy (Stop Stranger Group Invites)

Stop scammers from adding you to fake job or investment groups without your permission.

> **Change setting:** Go to **Settings ➔ Privacy ➔ Groups** and switch from **Everyone** to **My contacts**.

🖼️

4. Profile Photo & About (Prevent DP Theft)

Stop scammers from downloading your photo and setting up a fake profile in your name.

> **Change setting:** Open **Privacy** and set both **Profile photo** and **About** to **My contacts**.

Chapter 2: Do's and Don'ts

✅ Always Do This (DOs)

• Set your 6-digit Two-Step Verification PIN and recovery email right away.

• Open Linked Devices once a month and log out any unknown browsers.

• Keep **Fingerprint / App Lock** turned on in WhatsApp for extra phone safety.

❌ Never Do This (DONTs)

• Never hand over your unlocked phone to a stranger, even for 1 minute.

• Never leave Group Privacy open to **Everyone**.

• Never use an obvious PIN like 111111 or 123456 for Two-Step Verification.

Official Verification Source

- WhatsApp Security & Two-Step Verification Guide: `faq.whatsapp.com`
- National Cyber Crime Reporting Portal: `cybercrime.gov.in`

CHAPTER 3 • ACCOUNT TAKEOVER

The OTP Account Takeover Scam

How your 6-digit registration code is stolen, the call forwarding trick, and how to recover your account in 10 minutes.

One Code Shared, and Your WhatsApp Is Gone!

WhatsApp's weakest link is not technology—it is human trust. Whenever you register WhatsApp on a new phone, an official 6-digit SMS code arrives.

A scammer wants to steal your WhatsApp without touching your phone. So they use a friend's already-hacked WhatsApp account to send you a very innocent-sounding message.

Danger Bell

What Happens the Moment You Share the Code?

As soon as you tell them that 6-digit code, the very next second your screen shows: *"Your phone number is no longer registered with WhatsApp on this phone."*

Result: Your WhatsApp stops working, and the hacker starts messaging all your friends and relatives asking for money in your name!

Case Study: "Bro, My Code Came to Your Phone by Mistake"

See how a scammer uses a close friend's name to trap you:

WHATSAPP CHAT (FRIEND'S HACKED ACCOUNT)

Friend (under hacker's control): "Hey bro! My 6-digit verification code went to your mobile by SMS by mistake. Please check and send it quickly, my urgent work is stuck."

You: "Sure bro, it says 482-195. What happened?"

Hacker: *(Enters the code—your WhatsApp logs out and the hacker sets their own Two-Step PIN!)*

Spot the lie: A WhatsApp code can NEVER go to someone else's phone by mistake. If a code arrived on your phone, someone is trying to log into YOUR number!

Dangerous Trick: Call Forwarding Codes (*401* or *21*)

Sometimes the scammer doesn't even ask for an OTP. They make a regular phone call pretending to be from your telecom company or bank:

The Fake Excuse

"Dial This Number for 5G Speed"

"Sir, to activate your 5G network, open your phone dialer and dial `*401*<Number>`."

The real truth: `*401*` is actually a secret **Call Forwarding** code. As soon as you dial it, all your incoming calls go straight to the scammer's phone. Then the scammer requests a WhatsApp Voice Call OTP and steals your account.

What to Do If Your Account Gets Hacked (10-Minute Recovery)

Don't panic! Follow these official WhatsApp recovery steps right away:

1 **Try Logging Back In**
Open WhatsApp on your phone, enter your mobile number, and tap **Next**.

↓ Request a New SMS Code

2 **Enter the New 6-Digit SMS Code**
Magic safety rule: The moment you enter the SMS code, the hacker is **automatically logged out** of your account that very second!

↓ What If the Hacker Set a PIN?

3 **Wait 7 Days (The Hacker Is Already Out)**
The hacker can no longer use your WhatsApp either. After 7 days, you can unlock and start your WhatsApp again without their PIN.

↓ Warn Your Contacts

4 **Call Your Friends and Family Immediately**
Make normal calls or send SMS to warn everyone: *"My WhatsApp was hacked—please don't send money to anyone asking in my name."*

Chapter 3: Do's and Don'ts

✅ Always Do This (DOs)

• Keep every 6-digit code that arrives on your phone completely secret.

• Dial `##002#` to check and cancel any hidden Call Forwarding.

• Turn on your Two-Step Verification PIN today.

❌ Never Do This (DONTs)

• Never send your WhatsApp code even if a sibling or close friend asks by message.

• Never dial `*401*` or `*21*` in your phone dialer on any stranger's instructions.

• Don't stay silent if hacked—call your contacts immediately to warn them.

Official Support Sources

• WhatsApp Stolen Accounts Recovery Guide: `faq.whatsapp.com`

• WhatsApp Official Support Email: `support@whatsapp.com` (Subject: Lost/Stolen: Please deactivate my account)

• National Cyber Crime Portal: `cybercrime.gov.in`

CHAPTER 4 • VIRUSES AND DANGEROUS FILES (MALWARE)

Fraud Links and APK Files

How to protect your phone and bank account from dangerous files disguised as wedding cards, challans, and electricity bills.

A Wedding Card or a Virus That Empties Your Bank Account?

A new trend is spreading fast on WhatsApp. A file arrives from a relative or an unknown number named `Wedding_Card.apk` or `Bijli_Bill.apk`.

People assume it's a wedding invitation or an electricity bill receipt and tap it without thinking. Instead of opening a card, it silently installs dangerous spyware on their phone.

Remember

What Is an APK File?

APK stands for Android Package Kit. It is the installation file used to install apps on an Android phone.

Simple rule: Real wedding cards are always PDFs or photos (JPG/PNG). No real card ever ends with `.apk`!

Case Study: The Wedding Card Sent on WhatsApp

See how a scammer slips a virus into a phone using an innocent-looking message:

💬 WHATSAPP MESSAGE (THE WEDDING CARD BAIT)

Unknown Number (Relative's DP): "You and your family are warmly invited to our son's wedding. Please open the file below to view the full wedding schedule: 📄 `Wedding_Invitation_2026.apk`"

User: *(Thinks it's a wedding card, taps it... 'Install unknown app' pops up on screen and they tap Allow!)*

Result: *(No card opens—instead, every SMS and bank OTP on the phone starts going straight to the scammer!)*

Scammers' 4 Biggest APK Excuses



1. Wedding Card APK

Sent using a relative's stolen DP so nobody suspects a thing.

File name: `Shadi_Card.apk` or `Wedding_Card.apk`



2. Traffic E-Challan APK

"A ₹2,000 traffic challan has been issued on your vehicle—pay now or face a court notice."

> **File name:** `Vehicle_Fine_Challan.apk`



3. Electricity Bill Update APK

"Your power connection will be cut at 9:30 PM tonight. Check your bill immediately using this app."

> **File name:** `Electricity_Bill_Pay.apk`



4. Government Scheme / PM Kisan APK

"Fill out this form right now to get ₹5,000 free."

> **File name:** `PM_Yojana_Kisan.apk`

What to Do Immediately If You Install an APK by Mistake

Don't waste a single minute! Take these 4 steps right away:

1 **Put Your Phone in Airplane Mode Immediately**
Turn off Wi-Fi and Mobile Data right away so the virus cannot send your bank OTPs to the scammer.

↓ Delete the App Offline

2 **Find and Uninstall the App from Settings**
Go to **Settings → Apps → Manage apps**. Select the fake app and tap **Uninstall** immediately.

↓ Run a Security Scan

3 **Run a Google Play Protect Scan**
Open **Google Play Store**, tap your profile icon, and go to **Play Protect → Scan**.

↓ What If the App Won't Uninstall Normally?

4 **Restart in Safe Mode and Remove It**
Hold the power button, long-press **Power off**, restart in **Safe Mode**, and uninstall the app.

Chapter 4: Do's and Don'ts

✅ Always Do This (DOs)

• Install apps only from the official Google Play Store.

• Always keep "Install unknown apps" turned OFF in your phone settings.

• Always check that real government websites end with `.gov.in`.

❌ Never Do This (DONTs)

• Never install any file ending in `.apk`, even by mistake.

• Never click unknown short links like `bit.ly` or `tinyurl`.

• Never forward links promising free phones or recharges to 5 groups.

Official Verification Source

• CERT-In (Indian Computer Emergency Response Team) Advisory: `cert-in.org.in`

• National Cyber Crime Portal: `cybercrime.gov.in`

• Chakshu Fraud Reporting Portal: `sancharsaathi.gov.in`

CHAPTER 5 • PART-TIME JOB TRAPS (TASK SCAMS)

Fake Jobs and Work-from-Home Offers

The multi-crore scam behind liking YouTube videos, the ₹500 initial bait, and the real truth.

"Earn ₹3,000 Daily": Does Anyone Really Give Free Money?

According to the Ministry of Home Affairs Cyber Cell (I4C), the biggest online fraud in India today is the **Task-Based Part-Time Job Scam**.

Scammers know people want extra income from home. So they offer work that needs zero education or experience—just liking YouTube videos or giving 5-star ratings on Google Maps!

The Biggest Trick

You Actually Get Paid at First!

The cleverest part of this scam is that after you finish the first 2–3 tasks, **the scammer actually sends ₹150 to ₹500 to your UPI or bank account!**

Why? To kill 100% of your doubt. It is bait on a fishing hook. Once you trust them, they move you to Telegram and loot lakhs of rupees.

Case Study: The ₹300 Trap for Liking 3 Videos

See how this conversation starts on WhatsApp:

WHATSAPP CHAT (FAKE HR RECRUITER)

Priya (Global HR): "Hello! We have a part-time work-from-home job for you. Just like 3 YouTube videos and send screenshots. You'll earn ₹100 per like. Ready to start?"

User: "Yes, I liked all 3 videos and sent the screenshots."

Priya: "Congrats! ₹300 has been sent to your UPI ID. Join our VIP Telegram group for bigger tasks and earn ₹5,000 daily!"

The Task Scam Cycle: From ₹500 to Losing

Lakhs

1 **First Message on WhatsApp**
A message from an HR profile with a nice photo: "Like videos from home and earn ₹3,000 daily."

↓ Winning your trust

2 **Real ₹300 Payment (The Bait)**
You actually receive ₹300 via UPI for 3 tiny tasks, making you believe the job is genuine.

↓ Moving to Telegram

3 **Adding You to a VIP Telegram Group**
100 fake accounts post forged screenshots of ₹50,000 daily payouts to build excitement.

↓ The Prepaid Tasks Game

4 **Asking You to Deposit Money**
"Deposit ₹1,000 and get ₹1,400 back", then "Deposit ₹10,000 and get ₹14,000."

↓ Money Frozen and Account Emptied

5 **Withdrawal Blocked (The Trap)**
Once you deposit ₹1 lakh, the scammer demands: "Pay 30% tax or your funds stay frozen." In the end, all your money vanishes!

Real Job vs Fake Job Scam



Signs of a Real Job

• Companies pay employees for their work—they never ask employees to pay money.

• Hiring happens through LinkedIn, official websites, or company emails.

> **Golden rule:** You never have to deposit ₹1 to get a job.



Signs of a Fake Job Scam

• Sudden message from an unknown WhatsApp number or international code.

• Asking for money as a "Security Deposit" or "Prepaid Task" to start working.

• Pushing you to leave WhatsApp and move the chat to Telegram.

Chapter 5: Do's and Don'ts

✅ Always Do This (DOs)

• Remember: no real job in the world asks you to pay money to earn money.

• If someone sent you ₹200–₹300 initially, stop right there and never put ₹1 back in.

• **Report** and **Block** such messages directly on WhatsApp.

❌ Never Do This (DONTs)

• Never join Telegram groups on a stranger's recommendation.

• Never transfer money in the name of liking videos or posting reviews.

• Never fall for the lie: "Deposit more money to unlock your stuck funds."

Official Verification Source

• Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs Advisory: `cybercrime.gov.in`

• Chakshu Fraud Reporting Portal: `sancharsaathi.gov.in`

CHAPTER 6 • IMPERSONATION SCAMS

Asking for Money Using a Known Person's Name

Fake emergency dramas using your friend's or boss's DP, the Merchant UPI trick, and the 60-second verification test.

"Bro, Stuck at the Hospital": Is Your Friend Really in Trouble?

Imagine getting a WhatsApp message with the name and DP of a close relative, best friend, or your boss: *"Big emergency, send ₹25,000 to this UPI right now, I'll return it by evening."*

Seeing someone we care about in trouble, most of us send money without thinking. Later we find out the person was sitting safely at home—and the money went straight to a thief!

Know the Truth

A Photo Is Not Proof of Identity!

Today it takes just 5 seconds to download anyone's photo from Facebook, Instagram, or LinkedIn.

Simple rule: Any new number using your friend's photo is NOT your friend until you hear their voice!

Case Study: Boss's Message from a New Number

See how a scammer uses a new number to trick office employees:

WHATSAPP CHAT (FAKE DP OF COMPANY DIRECTOR)

Director (new unknown number): "Amit, this is my new personal number. I'm in an urgent client meeting and my bank app isn't logging in. Send ₹40,000 to this vendor immediately—I'll pay you cash at the office in 1 hour."

Amit: "Sir, I'm sending it, but why does the UPI show 'M/S Quick Enterprise'?"

Director (Scammer): "Yes, that's the client's firm. Hurry up, it's very urgent!"

Before Sending Money: The 60-Second Verification Test

Whenever anyone you know asks for money on WhatsApp, do these 3 checks before paying blindly:

1 **Make a Normal Call to Their Old Saved Number**
Don't call the new number that messaged you—call the original number already saved in your phonebook.

↓ What If They Don't Pick Up?

2 **Ask a Secret Question Only They Would Know**
Ask: "Where did we meet last time?" or "What is your younger brother's name?" A real friend answers in 2 seconds; a thief makes excuses.

↓ Confirm Their Voice

3 **Ask for a 10-Second Voice Note**
Say: "Bro, send a 10-second voice note saying my name." A scammer can never send a real voice note saying your name.

Check the Name Shown on the UPI ID



Name Mismatch Means Direct Fraud

When you enter a UPI ID in PhonePe, Google Pay, or Paytm, the real bank account holder's name appears.

> If your friend's name is **Rohit Sharma**, but the UPI shows **"M/S Quick Enterprise"** or a stranger's name, don't send even ₹1!

Chapter 6: Do's and Don'ts

✅ Always Do This (DOs)

• Always call the old saved number on a regular phone call before sending money.

• Confirm their identity by asking for a voice note.

• Carefully check the registered name shown on the UPI ID.

❌ Never Do This (DONTs)

• Never transfer money immediately just by seeing a familiar DP and name.

• Never blindly trust excuses like "This is my new number, my old one stopped working."

• Never send money to a stranger's UPI ID even if a friend's message asks you to.

Official Verification Source

• Delhi Police Cyber Cell Advisory on Impersonation Frauds: `cybercrime.gov.in`

• Sanchar Saathi Chakshu Portal: `sancharsaathi.gov.in`

CHAPTER 7 • UPI AND QR CODE SAFETY

WhatsApp UPI Payment and QR Scams

You never need a PIN to receive money — the fake army officer drama, fake QR codes, and collect requests.

"Scan This QR Code to Receive Money": The Biggest Lie!

Suppose you post an ad on OLX or Facebook to sell an old sofa, phone, or bike. Within 10 minutes, a polite buyer messages on WhatsApp: *"I like your item and I'm paying the full amount in advance. Scan this QR code and enter your PIN—the money will land in your account immediately."*

As soon as you scan that QR code and enter your UPI PIN hoping to receive money, ₹15,000 gets deducted from your account instead!

Unbreakable Rule

NPCI and RBI's #1 Rule

Your UPI PIN is used ONLY to send (debit) money from your bank account.

Simple rule: You NEVER need to enter a UPI PIN or OTP to receive money from anyone in the world. QR codes are scanned only to **pay** money, never to receive it!

Case Study: The Fake Army Officer on OLX

See how a scammer uses a uniform photo to gain trust and cheat sellers:

WHATSAPP CHAT (FAKE ARMY OFFICER)

Major Vikram (DP in uniform): "Hello brother! I saw your bike listing. I'm posted at the Army Cantt and I want to buy it. I'm sending ₹30,000 advance right now."

Seller: "Thank you sir, please Google Pay it to my number."

Major Vikram: "Brother, the army's official merchant account can't transfer directly. I'm sending a special QR code—scan it with PhonePe and enter your PIN so the money gets credited to you."

Truth: *(The moment the seller enters their PIN, ₹30,000 gets deducted instead of credited!)*

3-Step Formula to Beat QR Scams

1 **Never Scan a QR Code to Get Paid**

If a buyer asks you to scan a QR code to receive payment, refuse clearly: *"I won't scan any QR—just send the money directly to my mobile number."*

↓ Ring the Alarm Bell in Your Mind

2 **Remember: PIN = Money Leaving Your Account**

Whenever a PIN keypad pops up on your screen, know that money is going OUT of your account.

↓ Check Your Real Balance

3 **Verify Balance in Your Official Bank App**

Never trust WhatsApp payment screenshots or SMS alerts alone. Open your real bank app (like SBI YONO, iMobile, etc.) and check your passbook.

WhatsApp Pay and Collect Request Trap



Never Approve a Payment Request in Chat

Sometimes a scammer sends a **Collect Request** in chat and says: "Tap Approve to get your money."

What to do: Always tap **Decline** on any unknown payment request. If you tap **Pay** and enter your PIN, your money will be deducted instantly.

Chapter 7: Do's and Don'ts

✅ Always Do This (DOs)

• Give only your mobile number or UPI ID when receiving money.

• Always confirm received money by checking your balance inside your official bank app.

• Never trust someone blindly just because of a uniform or canteen card photo.

❌ Never Do This (DONTs)

• Never scan any QR code in the world to receive money.

• Never enter your UPI PIN to receive money.

• Never trust fake SMS messages saying "Sent extra money by mistake, please refund."

Official Verification Source

- NPCI UPI Safety Rules: `npci.org.in`
- RBI Consumer Awareness Portal: `rbi.org.in`
- National Cyber Crime Portal: `cybercrime.gov.in`

CHAPTER 8 • FAKE INVESTMENT TRAPS (STOCK & TIP SCAMS)

Fake Investment and Tip Groups

False dreams of guaranteed stock profits, fake trading apps, and multi-crore scams.

"Double Your Money in 1 Month": Is That Even Possible in Stocks?

Imagine suddenly being added to an unknown WhatsApp group named *"VIP Stock Market Pro Tips"* or *"Institutional Wealth Club"*.

From morning to night, members post screenshots of huge profits—someone claims they made ₹1 lakh today, while another posts a photo of a new luxury car.

Very Important Notice

SEBI's Biggest Warning

According to India's stock market regulator **SEBI** (Securities and Exchange Board of India), educated professionals and retired seniors are losing their life savings to this exact scam.

Simple rule: There is no such thing as 100% guaranteed returns in the stock market. Anywhere someone promises guaranteed profits, it is 100% fraud.

Case Study: The Fake Hype Inside a VIP Stock Group

See how 95% of the people in that group are the scammer's own team or bots:

💬 **WHATSAPP GROUP CHAT (FAKE VIP COMMUNITY)**

Admin (Stock Expert): "Yesterday we gave our VIP members a special Upper Circuit stock—20% profit booked today! Share your screenshots!"

Member 1 (Fake Bot): "Sir! Invested ₹50,000 yesterday, became ₹65,000 today. Your tips are like magic! 🙏"

Member 2 (Fake Bot): "I invested ₹2 lakh and just withdrew ₹40,000 to my bank. Thank you so much sir!"

New User (Trapped by FOMO): *(Thinks everyone is making money—why stay behind? Messages the admin and falls right into the trap!)*

How the Fake Investment Trap Works

1 **Adding You to an Unknown Group**
The group is named after a famous market expert or a big foreign investment firm.

↓ Showing Fake Profit Screenshots

2 **Making You Download a Fake Trading App**
The scammer says: "We don't trade on regular apps—download our special VIP app." That app is completely fake.

↓ Fake Profits on Screen

3 **Letting You Withdraw ₹5,000 at First (Trust Bait)**
They let you withdraw a small amount to win your trust, pushing you to invest ₹10–20 lakh out of greed.

↓ Money Frozen and Extortion

4 **Demanding Tax and Fees to Withdraw**
When you try to withdraw your money, the scammer demands: "Pay 20% tax" or "Pay a security deposit." Finally, the group closes and all your money is gone.

Real Investing vs Fake WhatsApp Scam



Signs of Real SEBI-Registered Investing

• Your money always goes into a Demat/Trading account in your own name.

• Money is never transferred to any unknown person's personal savings account.

> **Rule:** No genuine market broker promises guaranteed returns.



Signs of a Fake WhatsApp Scam

• False promises of 200% to 500% guaranteed profits.

• Asking you to deposit money into an individual's or unknown trust's bank account.

• Asking you to download an app from an unknown link outside Google Play Store.

Chapter 8: Do's and Don'ts

✅ Always Do This (DOs)

• Immediately **Exit** and **Report** unknown stock market groups.

• Invest only through official SEBI-registered brokers.

• Check any broker's genuine registration number on `sebi.gov.in`.

❌ Never Do This (DONTs)

• Never invest blindly based on stock tips shared on WhatsApp or Telegram.

• Never transfer investment money into an unknown person's private bank account.

• Never trust ads promising "Guaranteed Returns" or "Risk-Free Profit."

Official Verification Source

• SEBI (Securities and Exchange Board of India) Advisory: `sebi.gov.in`

• National Cyber Crime Portal: `cybercrime.gov.in`

CHAPTER 9 • GROUP PRIVACY AND SAFETY

Unknown Groups and Fake Profiles

The game of foreign country codes, stopping stranger group invites, and the 30-second Group Privacy setting.

Waking Up Inside an Unknown WhatsApp Group?

Have you ever woken up, opened WhatsApp, and seen yourself added to an unknown group called *"Crypto VIP 500X"*, *"Daily Online Earning"*, or *"Part-Time Work India"*?

Hundreds of strangers sit inside, and the group admin from a foreign country code (like +84, +62, +254, or +92) keeps posting long messages and links.

Danger Point

Where Do Scammers Get Your Number?

Scammers pull thousands of phone numbers from leaked databases, old websites, or random number software and dump everyone into new groups at once.

Plain truth: If someone who is NOT in your contacts adds you to an unknown group, it is 99.9% fraud or spam.

Case Study: Inside an Unknown International Group

See how scammers build fake excitement inside stranger groups:

💬 WHATSAPP GROUP (UNSOLICITED ADDITION)

Admin (+84 98...): "Hello all new members! In this group you will get easy daily tasks to earn ₹2,000 from home. Click the link below to start."

Fake Bot 1 (+62 81...): "Sir, I finished today's task and got ₹500!"

Ordinary User (You): *(Thinks: Who added me to this group? I don't know a single person here!)*

4 Biggest Signs of a Fake Profile

Scammers steal or build fake profiles to contact you. Spot them with these 4 clues:

🌐

1. International Country Code

Even though they claim to be in India, their number starts with +84 (Vietnam), +62 (Indonesia), +254 (Kenya), or +1 (USA virtual VoIP).



2. Stolen Attractive DP

They use photos of models, army officers, or attractive people downloaded from Google or social media to look trustworthy.



3. Vague or Strange 'About' Bio

Their bio says "Online Business", "HR Manager", or broken English with zero real identity.



4. Admin-Only Group Settings

Only admins can send messages in the group—normal members are muted so nobody can ask questions or warn others.

The 30-Second Setting to Stop Unknown Groups

Turn on this one WhatsApp setting today so no stranger can add you directly to any group:

1 **Open WhatsApp Settings**
Tap the **3 dots (⋮)** at the top right and open **Settings**.

↓ Choose Privacy

2 **Go to Privacy ➔ Groups**
Tap **Privacy**, scroll down, and select **Groups**.

↓ Choose "My Contacts"

3 **Switch from "Everyone" to "My Contacts"**
By default it is set to **Everyone**. Change it to **My Contacts**.

Benefit

What Changes Now?

Now only people whose numbers are saved in your phone can add you to a group. If a stranger tries to add you, they must send an **Invite Link**—and joining stays 100% your choice.

Chapter 9: Do's and Don'ts

✅ Always Do This (DOs)

• Set Group Privacy to **"My Contacts"** right away.

• If added to an unknown group, immediately tap **Exit Group** and **Report**.

• Keep **"Silence unknown callers"** turned on in Settings.

❌ Never Do This (DONTs)

• Never click any link posted inside an unknown group.

• Never invest money on the advice of any stranger in a group.

• Never answer calls from unknown international numbers (+84, +62, etc.).

Official Verification Source

• WhatsApp Official Help Center (Group Privacy Settings): `faq.whatsapp.com`

• Chakshu Portal (Telecom Department, Govt of India): `sancharsaathi.gov.in`

• National Cyber Crime Reporting Portal: `cybercrime.gov.in`

CHAPTER 10 • DANGER OF AI AND VIDEO CALLS

AI Voice and Video Fraud on WhatsApp

Fake emergency calls using cloned voices of loved ones, stranger video call traps, and stopping blackmail.

"Dad, I Had an Accident!": Is That Really Your Son?

Imagine getting a WhatsApp call or voice note from an unknown number in the afternoon. The voice sounds exactly like your son crying: *"Dad, the police caught me / I had a terrible accident—send ₹50,000 right now or I'll go to jail!"*

Any parent would panic hearing this. Yet in 99% of cases, your child is sitting safely in college or at the office—and that voice is just an **AI Voice Clone**!

New Tech Danger

How Does AI Steal a Voice?

Today, AI tools can copy anyone's voice cleanly using just 3 to 5 seconds of audio from Instagram Reels, YouTube Shorts, or Facebook videos—even adding crying, fear, and panic by computer.

Rule #1: No matter how real the voice sounds, if an emergency money request comes from an unknown number, pause for 10 seconds and call their real saved number first.

Case Study: AI Voice Note and Panic Pressure

See how scammers use fake crying to scare parents into paying fast:

WHATSAPP VOICE CALL / AUDIO MESSAGE

Fake Son (AI Cloned Voice): "Dad! Save me... our car hit someone. The police want ₹40,000 or they'll file an FIR. Send the money to this UPI ID right now!"

Alert Father (Smart User): "Son, calm down. First tell me—what is your grandmother's name? And which friend are you with?"

Fake Son (Making Excuses): "Dad, ask later, it's an emergency—the police are snatching my phone!"

Truth: *(When the father made a normal call to his son's real number, the son said: "Dad, I'm having tea in the office canteen!")*

Unknown Video Calls and Video Blackmail Trap

Late at night, a WhatsApp video call arrives from an unknown number with an attractive woman's DP.



The Trap Upon Answering

The moment you pick up, an obscene video plays on the other side, and the scammer records your face on screen.

⚖️

Fake Police and CBI Threats

Within a minute, they send back an edited video showing your face and pose as "CBI / Delhi Police", threatening to make it viral unless you pay.

What to Do If Someone Video-Blackmails You

If anyone ever gets trapped like this, follow these 4 steps right away:

1

Never Transfer Even ₹1

If you pay ₹5,000 once, they will keep demanding up to ₹5 lakh. Paying never stops blackmail.

↓ Save the Evidence

2

Keep Screenshots and Number Records

Take screenshots of threatening messages, UPI IDs, and phone numbers for your complaint.

↓ Cut All Contact

3

Block and Report Immediately

Don't argue or beg. Simply **Block** and **Report** the number directly on WhatsApp.

↓ Official Government Complaint

4

Report on the National Cyber Crime Portal

File an online complaint right away at `cybercrime.gov.in`. Police actively help victims in such cases.

Chapter 10: Do's and Don'ts

✅ Always Do This (DOs)

• Agree on a **Family Secret Code** that only your family members know.

• Never pick up unknown video calls; if answered by mistake, cover the camera with your finger right away.

• Whenever someone claims a family emergency, call their old saved number first to verify.

❌ Never Do This (DONTs)

• Never send money to an unknown account in fear or panic.

• Never pay money out of fear if someone tries to blackmail you.

• Never share private photos or videos in chat with any stranger.

Official Verification Source

• National Cyber Crime Reporting Portal: `cybercrime.gov.in`

• Ministry of Home Affairs (I4C Cyber Dost Advisories): `cybercrime.gov.in`

• Telecom Department Chakshu Portal: `sancharsaathi.gov.in`

CHAPTER 11 • EMERGENCY STEPS & COMPLAINTS

What to Do After a Scam & How to Complain

Why the Golden 2 Hours matter, 4 immediate steps, and the right government process to recover money.

Stay Calm If Scammed: The First 2 Hours Are Golden!

If you clicked a wrong link in a hurry or transferred money to a fraudster, stay calm first—anyone can be tricked in a weak moment.

Your biggest weapon right now is **Speed**. In cyber safety, the window right after a fraud is called the **"Golden 2 Hours"**.

Golden Rule

How Do the Golden 2 Hours Save Your Money?

When you report immediately, the Ministry of Home Affairs system (CFCFRMS) puts a **Freeze (hold)** on the scammer's bank account or wallet before they can move the money out.

Plain truth: The faster you report, the higher your chance of getting your money back safely!

4 Immediate Steps to Take the Moment

Money Is Deducted

1 **Never Delete Chats or Evidence**
Don't clear the chat out of fear or anger. Take **screenshots** of the scammer's messages, phone number, UPI ID, and bank SMS right away.

↓ Alert Your Bank

2 **Inform Your Bank Immediately**
Call the official customer care number printed on the back of your ATM card. Mark the transaction as fraud and freeze Net Banking / UPI if needed.

↓ File an Official Portal Complaint

3 **Report on the National Cyber Crime Portal**
Go straight to `cybercrime.gov.in`, select "Report Cyber Crime", and enter the full details and Transaction ID.

↓ Report on WhatsApp

4 **Use WhatsApp's In-App Report**
Open the scammer's chat ➔ tap **3 dots (⋮)** ➔ **More** ➔ **Report** so WhatsApp permanently bans that account.

What Evidence Do You Need for a Complaint?

Keep these 4 items ready when filing your complaint:



1. 12-Digit UTR / Transaction ID

The 12-digit Reference Number shown in your bank SMS or UPI app receipt (PhonePe, GPay, Paytm).



2. WhatsApp Chat Screenshots

Full screenshots of the chat clearly showing the scammer's promises, threats, or links.



3. Scammer's UPI ID & Number

Clear details of the phone number or UPI ID where the money was sent.



4. Bank Account Statement

The bank passbook or Net Banking statement page showing the deducted transaction.

Beware: Fake "Money Recovery" Scams

New Trap

Watch Out for Fake Instagram Hackers

When people post on social media about losing money to fraud, fake accounts comment: *"Contact this Instagram expert—they got my money back in 1 hour."*

Bitter truth: This is a second gang of scammers who steal even more money from victims as a "Processing Fee". In India, only **your Bank, the Police, and the Cyber Crime Portal** have the power to recover funds—no private person can!

Chapter 11: Do's and Don'ts

✅ Always Do This (DOs)

• File your complaint within the first 2 hours as soon as money is deducted.

• Save your UTR number and bank SMS alerts safely.

• Report fraud numbers on the **Chakshu Portal** (`sancharsaathi.gov.in`) as well.

❌ Never Do This (DONTs)

• Never stay silent out of shame or fear—tell your family and bank right away.

• Never delete the WhatsApp chat with the scammer.

• Never pay ₹1 to any unknown "hacker" claiming they can recover your money.

Official Complaint & Support Sources

• National Cyber Crime Reporting Portal: `cybercrime.gov.in`

• Chakshu Fraud Reporting Portal: `sancharsaathi.gov.in`

• Reserve Bank of India (RBI Cyber Fraud Circulars): `rbi.org.in`

CHAPTER 12 • FINAL CHAPTER (MASTER POCKET REFERENCE)

WhatsApp Safety Checklist

A complete one-page safety card for daily use. Save it on your phone, print it out, or share it with family and friends.

Your Complete Pocket WhatsApp Safety Card

WhatsApp is our biggest bridge to family, friends, and work—but one tiny slip can cost a lifetime of savings.

This final chapter packs the most essential rules from all 11 chapters into **4 color-coded Safety Cards**. Whenever you feel unsure, just open this checklist.

1 WhatsApp Account Settings Checklist

Check These 5 Settings on Your Phone Today

- ✓ **Keep Two-Step Verification ON:**
  Go to Settings ➔ Account ➔ Two-step verification and set a 6-digit PIN so no one can steal your WhatsApp.
- ✓ **Check Linked Devices Regularly:**

Open Settings ➔ Linked Devices. If you spot any unknown browser or computer, tap **Log out** right away.

✓ **Set Group Privacy to "My Contacts":**
Go to Settings ➔ Privacy ➔ Groups and choose **My Contacts** so strangers cannot add you to fake groups.

✓ **Keep "Silence unknown callers" ON:**
Go to Settings ➔ Privacy ➔ Calls and turn it on so unknown foreign calls stay silent automatically.

✓ **Show Profile Photo Only to Contacts:**
In Settings ➔ Privacy ➔ Profile photo, choose "My Contacts" so strangers cannot steal your DP.

2 Never Make These 6 Mistakes (Red Flags Checklist)

Over 95% of cyber frauds happen because of these 6 mistakes

✗ **Never share your 6-digit SMS code:**
Even if a sibling or best friend asks on chat, never share your WhatsApp registration SMS code.

✗ **Never scan a QR code to receive money:**

Remember: a PIN is always for sending money. Never enter your UPI PIN to receive payment.

- ✕ **Never install unknown .APK files:**
  Files named Wedding_Card.apk or Bijli_Bill.apk are dangerous spyware—never open them.
- ✕ **Avoid fake jobs paying to like videos:**
  No genuine company pays money just for liking YouTube videos or posting hotel reviews.
- ✕ **Never trust "Guaranteed Return" stock groups:**
  All WhatsApp groups promising guaranteed stock market profits are 100% fake.
- ✕ **Never answer unknown international video calls:**
  Video calls from foreign codes (+84, +62, etc.) are traps for video blackmail.

3 The 10-Second Verification Test (Verification Card)

Whenever a known person asks for money

- ✓ **Make a direct phone call to their old saved number:**
  If someone asks for money from a "new number", don't WhatsApp-call them—make a normal SIM call

to their old number.

✓ **Ask for a 10-second voice note:**
Tell them: "Bro, send a 10-second voice note saying my name." A scammer will never be able to say it.

✓ **Match the name on the UPI ID:**
If your friend's name is 'Rohit' but the UPI shows an enterprise or stranger's name, don't send even ₹1.

✓ **Use a Family Secret Code:**
Keep a secret code word known only to your family. It is the surest way to beat AI voice clone scams.

4 Emergency Action Checklist (If Fraud Happens)

Do this within the Golden 2 Hours after money is deducted

! **Save chats and screenshots:**
Don't delete the chat out of fear or anger. Screenshot the scammer's number, UPI ID, and bank SMS.

! **Note down the 12-digit UTR / Transaction ID:**
Find the 12-digit reference number in your bank deduction SMS or passbook.

! **Alert your bank's official Customer Care:**
Call the official number on the back of your ATM card, report the transaction as fraud, and secure Net Banking.

! **Report on the National Cyber Crime Portal:**
Visit `cybercrime.gov.in` within 2 hours and file an online complaint.

! **Report the fraud number on Chakshu Portal:**
Submit the scammer's number and links on the official portal `sancharsaathi.gov.in`.

🎉 **Congratulations!**

You Have Completed Book 1: How to Stay Safe from WhatsApp Scams

You now have complete practical knowledge to stay safe on WhatsApp. Share this guide with your parents, elders, and friends so no cyber fraudster can ever steal their hard-earned money.

🤝 **Our Pledge:** "I will never click unknown links blindly, never enter my PIN to receive money, and never share my OTP with anyone."

Back to Table of Contents

Official Verification & Complaint Sources

- National Cyber Crime Reporting Portal: `cybercrime.gov.in`
- Chakshu Portal (Telecom Department, Govt of India): `sancharsaathi.gov.in`
- WhatsApp Official Help Center: `faq.whatsapp.com`
- Reserve Bank of India (RBI Cyber Awareness): `rbi.org.in`

APPENDIX

Cyber Safety Glossary

Registration Code (OTP)
The secret 6-digit code sent by SMS when starting WhatsApp. Sharing it transfers your account to another phone.

Two-Step Verification (2FA)
A double security wall—a secret 6-digit PIN you set yourself. Without it, nobody can hack your WhatsApp.

APK File
Android Application Package — an app file from outside the Play Store. Any APK sent as a wedding card or challan is a virus.

Linked Devices
A WhatsApp Web feature. Check it regularly to make sure no unknown computer or browser is reading your messages.

End-to-End Encryption

A message privacy lock—no third party can read chats in transit. However, if malware enters your phone, your screen can be watched live.

AI Voice Cloning

A modern scam where AI copies a loved one's exact voice and creates a fake emergency to demand money.

Mule Account

A rented bank account opened in someone else's name on commission so fraudsters can move stolen money around.

Chakshu Portal

The Telecom Department's official portal where suspicious WhatsApp fraud numbers and fake SMS messages are reported directly.

Golden 2 Hours

The first 2 hours right after money is deducted—reporting immediately on cybercrime.gov.in helps freeze the fraudster's bank account fast.

Spoof DP / Impersonation

Stealing your boss's or relative's photo from social media and putting it on an unknown number to ask for money.

💡 Keep this glossary handy whenever you want to double-check any technical term.

★ FINAL SECURITY RULES

4 Golden Rules of WhatsApp Safety

1. **Never Share Your Code:** Never send your 6-digit WhatsApp registration code, even if a friend or relative asks.
2. **No PIN Needed to Receive Money:** You never need to scan a QR code or enter a PIN to receive money on WhatsApp or UPI.
3. **Never Install Unknown Files:** Any .apk file sent in chat as a wedding card, challan, or electricity bill is a direct virus.
4. **Verify Voice and Identity First:** Never trust a DP alone. Call the sender on their old saved number before sending any money.

✓ 12 Detailed Chapters ✓ Real-Life Case Studies

✓ DoT & Cyber Portal Verified ✓ Master Pocket Card

🤝 Pledge for a Safe Digital India

Awareness is the strongest protection. When you stay safe, you protect your family and society from cyber crime.

Safe WhatsApp • Safe Family • Safe India

2026 Edition • Independently Published in Public Interest