National Cyber Crime Portal व सुरक्षा नियमों पर आधारित

नवीनतम 2026 संस्करण

WhatsApp Scam से कैसे बचें

आम Smartphone Users के लिए Fake Link, APK File और Account Hack से बचने की पूरी और आसान Pocket Guide

12	100%	4
विस्तृत अध्याय	सत्यापित नियम	सुरक्षा नियम

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

सुरक्षित WhatsApp • सजग परिवार • सशक्त भारत

2026 Mobile Pocket Edition • जनहित में प्रकाशित

कानूनी सूचना • LEGAL NOTICE

कानूनी बातें और इस्तेमाल के नियम

1. जन-जागरूकता उद्देश्य

यह eBook केवल आम नागरिकों में Cyber Safety जागरूकता बढ़ाने के उद्देश्य से तैयार की गई एक स्वतंत्र Guide है। इसका उद्देश्य पाठकों को WhatsApp पर होने वाले Scams और Fraud के तरीकों से सावधान करना है। यह कोई कानूनी (Legal) या Financial सलाह नहीं है।

2. किसी भी संस्था से कोई संबंध नहीं

यह eBook Meta, WhatsApp LLC, Reserve Bank of India (RBI), NPCI, Telecom Department, या भारत सरकार की किसी भी एजेंसी द्वारा प्रायोजित, समर्थित या Approved नहीं है। यह एक स्वतंत्र Digital Guide है।

3. ज़िम्मेदारी की सीमा (Limitation of Liability)

Cyber Safety के नियम, App Settings और सरकारी Websites के पते समय के साथ बदल सकते हैं। किसी भी पाठक के साथ होने वाले Online Fraud, तकनीकी समस्या या आर्थिक नुकसान के लिए यह eBook या इसके लेखक किसी भी रूप में ज़िम्मेदार नहीं होंगे। ताज़ा जानकारी के लिए हमेशा संबंधित संस्था की Official Website देखें।

4. Trademarks और Brand Names

'WhatsApp' और 'Meta' Meta Platforms के पंजीकृत Trademarks हैं। 'UPI' NPCI का पंजीकृत Trademark है। पुस्तक में उल्लिखित अन्य सभी नाम (जैसे Google Pay, PhonePe, Telegram आदि) उनके संबंधित मालिकों की संपत्ति हैं। इनका इस्तेमाल केवल पहचान और Fair Use के तहत किया गया है।

5. तरीकों का विवरण (No Real Names)

इस किताब में दिए गए सभी उदाहरण और Case Studies केवल ठगी के तरीकों को समझाने के लिए काल्पनिक नामों से दिए गए हैं। किसी भी असली व्यक्ति, कंपनी या संस्था को ठग नहीं कहा गया है; केवल अपराध के तरीकों को उजागर किया गया है।

6. Single-User Digital License

यह eBook केवल खरीदार के व्यक्तिगत पढ़ने के लिए है। इस eBook का अनधिकृत मुद्रण, Internet पर दोबारा Upload करना या Resale करना पूर्णतः प्रतिबंधित है।

© 2026 सर्वाधिकार सुरक्षित • 100% सुरक्षित और जाँचे हुए तथ्यों पर आधारित स्वतंत्र Guide

संपादकीय • EDITORIAL PREFACE

प्रस्तावना: यह गाइड आपके लिए क्यों आवश्यक है?

आज भारत में **50 करोड़ से अधिक** लोग रोज़ाना WhatsApp का इस्तेमाल करते हैं। सुबह की 'शुभकामना' से लेकर परिवार की बातचीत, बच्चों की पढ़ाई और Office का काम—सब कुछ इसी एक App पर चलता है।

हम अपने दोस्तों और रिश्तेदारों से WhatsApp पर जुड़े रहते हैं, इसलिए यहाँ हमारा भरोसा सबसे गहरा होता है। Cyber Scammers इसी भरोसे का सबसे गलत फ़ायदा उठाते हैं। हर दिन हम सुनते हैं कि किसी परिचित की DP देखकर पैसे भेज दिए, किसी ने शादी के कार्ड के नाम पर Virus Install कर लिया, या पार्ट-टाइम नौकरी के नाम पर लाखों गँवा दिए।

> “ **Scammer कभी WhatsApp के सर्वर को हैक नहीं करता, वह इंसानी भरोसे और हड़बड़ी से खेलता है — हमसे खुद हमारा OTP माँगता है, या धोखे से गलत Link पर Click करवाता है।**

अधिकांश ठगी केवल इसलिए सफल हो पाती है क्योंकि आम नागरिकों को WhatsApp की 2-3 बुनियादी सुरक्षा Settings की जानकारी नहीं होती। सबसे बड़ा नियम आज भी लाखों लोगों को नहीं पता: *"WhatsApp का 6-Digit Registration Code कभी किसी अपने को भी नहीं बताना चाहिए।"*

इस ई-बुक का उद्देश्य:

यह ई-बुक कठिन तकनीकी भाषा में नहीं, बल्कि **साधारण बोलचाल की हिंदी** में लिखी गई है। इसमें 12 अध्यायों के माध्यम से वास्तविक Case Studies, Scammer के असली Dialogues और Cyber Crime Portal के प्रमाणित नियमों के ज़रिए आपको और आपके परिवार को पूरी तरह सुरक्षित बनाना ही इसका लक्ष्य है।

इस गाइड को स्वयं पढ़ें और अपने परिवार, माता-पिता और दोस्तों के साथ साझा करें। आपकी थोड़ी-सी जागरूकता आपके परिवार की जीवन भर की कमाई की सबसे बड़ी रक्षक है।

विषय सूची • TABLE OF CONTENTS

अध्यायों की विस्तृत सूची

1 **अध्याय 1: WhatsApp पर Scam कैसे होते हैं**
डर और लालच का खेल, 4 रास्ते और Encryption का सच

2 **अध्याय 2: अपना WhatsApp Account सुरक्षित करें**
Two-Step Verification, Linked Devices और Privacy Settings

3 **अध्याय 3: Account Hack होने का OTP Scam**
6-Digit Registration Code चोरी की चाल और Recovery

4 **अध्याय 4: Fraud Link और APK File**
शादी का Card, E-Challan और बिजली Bill वायरस से बचाव

5 **अध्याय 5: Fake Job और घर बैठे कमाई के Offer**
YouTube Like और Part-Time Job के जाल की पहचान

6 **अध्याय 6: जान-पहचान वाले के नाम से पैसे माँगना**
DP चोरी, रिश्तेदार का बहाना और Emergency Fraud

7 **अध्याय 7: WhatsApp पर UPI Payment और QR Scam**
पैसे पाने के लिए PIN नहीं चाहिए — Chat Payment सुरक्षा

8 **अध्याय 8: Fake Investment और Tip Group**
शेयर बाज़ार और Crypto Ponzi Groups से बचाव

9 **अध्याय 9: अनजान Group और Fake Profile**
International Numbers से होने वाली ठगी की रोकथाम

10 **अध्याय 10: WhatsApp पर AI Voice और Video Fraud**
Voice Clone और Video Call Blackmail से सुरक्षा

11 **अध्याय 11: Scam हो जाए तो Complaint कैसे करें**
Golden 2 Hours, Cyber Portal और WhatsApp Reporting

12 अध्याय 12: WhatsApp Safety Checklist

Master Pocket Safety Checklist व त्वरित नियम

• **अंतिम भाग:** Printable Safety Card, पारिभाषिक शब्दकोश एवं बैक कवर

अध्याय 1 • BASICS (शुरुआती समझ)

WhatsApp पर Scam कैसे होते हैं

डर और लालच का खेल, Scammers के 4 मुख्य रास्ते और Encryption का असली सच।

WhatsApp: सुविधा भी और Scammers का अड्डा भी

आज भारत में शायद ही कोई ऐसा SmartPhone होगा जिसमें WhatsApp न हो। सुबह उठकर 'सुप्रभात' भेजने से लेकर, परिवार की बातचीत, बच्चों के School का काम और Office का लेन-देन—सब कुछ इसी एक App पर चलता है।

हम अपने दोस्तों और रिश्तेदारों से WhatsApp पर जुड़े रहते हैं, इसलिए यहाँ हमारा भरोसा सबसे पक्का होता है। Scammers इसी भरोसे का सबसे गंदा फ़ायदा उठाते हैं। वे जानते हैं कि अगर वे किसी अनजान Website पर जाल बिछाएँगे तो शायद आप बच निकलेंगे, लेकिन अगर वही जाल WhatsApp पर किसी अपने के नाम से आएगा, तो आप एक बार ज़रूर भरोसा कर लेंगे।

याद रखने वाली बात

Hacker आपकी Screen तोड़कर नहीं आता!

ज़्यादातर लोग सोचते हैं कि Hacker कोई जादुई Software चलाकर सीधे Bank से पैसा उड़ा लेता है। **यह बिल्कुल गलत है।**

Scammer का असली खेल: वह आपके Phone में नहीं घुसता, बल्कि आपके दिमाग से खेलता है। वह आपसे खुद गलती करवाता है—चाहे वह गलत Link पर Click करना हो, या हड़बड़ी में अपना OTP बताना हो।

Scammers के 2 सबसे बड़े हथियार: लालच और डर

Scammer जब भी Message करता है, वह दो इंसानी कमियों (हड़बड़ी और लालच) का फायदा उठाता है:

🎁

1. लालच (Greed का जाल)

"घर बैठे रोज़ ₹3,000 कमाएँ", "मुफ़्त 3 महीने का Recharge पाएँ", या "बधाई हो! आपको ₹25 लाख की Lottery लगी है।"

> **मकसद:** आपको बिना मेहनत के जल्दी अमीर बनने का सपना दिखाना, ताकि आप बिना सोचे Click कर दें।

⚡

2. डर और हड़बड़ी (Panic का जाल)

"आज रात बिजली कट जाएगी", "आपका SIM Card Block हो रहा है", या "बेटा Hospital में है, तुरंत पैसे भेजो।"

> **मकसद:** आपको सोचने और किसी से सलाह लेने का समय न देना। आप डर में तुरंत पैसे Transfer कर दें।

Case Study: जयपुर के सुमित की एक छोटी-सी चूक

जयपुर में काम करने वाले 34 वर्षीय सुमित के साथ जो हुआ, वह किसी के साथ भी हो सकता है। एक शाम उनके WhatsApp पर अचानक यह Message आया:

💬 **WHATSAPP CHAT (अनजान NUMBER पर BOSS की DP)**

> **Director (DP चुराकर):** "सुमित, मैं एक Client के साथ बहुत ज़रूरी Meeting में हूँ। मेरा Online Banking Login नहीं हो रहा। तुरंत इस Vendor को ₹45,000 Transfer कर दो। मैं 1 घंटे में Office पहुँचकर तुम्हें Cash दे दूँगा।"

> **सुमित:** "जी सर, मैं अभी भेज देता हूँ।"

सुमित ने Boss की DP देखी और बिना Phone मिलाए तुरंत ₹45,000 Transfer कर दिए। आधे घंटे बाद जब असली Director Office पहुँचे, तो पता चला कि उन्होंने ऐसा कोई Message भेजा ही नहीं था! वह DP Internet से चुराई गई थी।

सबक: किसी भी Photo (DP) को देखकर सच न मानें। पैसे भेजने से पहले उस व्यक्ति के असली Phone Number पर सामान्य Call करके आवाज़ ज़रूर सुनें।

Scam का चक्र: कैसे फँसाया जाता है?

WhatsApp पर होने वाला लगभग हर Fraud इन 4 कड़ियों से होकर गुज़रता है:

कदम 1

अनजान Number से Message आना

सुंदर Profile Photo, शानदार Job Offer या डराने वाला बिजली बिल का नोटिस भेजा जाता है।

↓ लालच या डर पैदा करना

कदम 2

आपसे कोई Action करवाना

Scammer कहता है: "नीचे दिए Link पर Click करें", "शादी का Card खोलें", या "अपना 6-Digit Code बताएँ।"

↓ Phone में Malware या OTP चोरी

कदम 3

Bank या Account तक पहुँच बनाना

गलत File से Phone में Spyware घुस जाता है या आपका WhatsApp किसी दूसरे Phone पर चालू हो जाता है।

↓ आर्थिक नुकसान

कदम 4

पैसे गायब और Number Block

खाते से पैसे कट जाते हैं और Scammer तुरंत आपको हर जगह से Block करके गायब हो जाता है।

एक बड़ा भ्रम: "WhatsApp तो Encrypted है, फिर Fraud कैसे?"

बहुत से लोग सोचते हैं: *"WhatsApp पर तो लिखा रहता है कि सब कुछ End-to-End Encrypted है, फिर कोई हमें कैसे ठग सकता है?"*

सरल उदाहरण

ताला और चाबी की सच्चाई

End-to-End Encryption का मतलब: आपके और सामने वाले के बीच की बातचीत को बीच रास्ते में कोई तीसरा इंसान नहीं पढ़ सकता। यह एक मज़बूत तिजोरी के ताले जैसा है।

लेकिन याद रखें: अगर आप खुद उस तिजोरी की चाबी (अपना OTP या PIN) चोर के हाथ में सौंप दें, तो तिजोरी का ताला आपको नहीं बचा सकता। Scammer तकनीक को नहीं, आपको धोखा देता है।

अध्याय 1: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• पैसों की माँग आने पर पहले असली Number पर सामान्य Call करके बात करें।

• अनजान Numbers से आए Links को खोलने से पहले दो बार सोचें।

• Fake Messages को WhatsApp पर ही **Report** और **Block** करें।

❌ यह कभी न करें (DONTs)

• केवल DP देखकर किसी भी Number को अपना दोस्त या Boss न समझें।

• अपना 6-Digit WhatsApp Code कभी किसी के साथ Share न करें।

• मुफ़्त Recharge या घर बैठे कमाई वाले झाँसों पर भरोसा न करें।

Official शिकायत और मदद कहाँ पाएँ?

अगर आपके साथ कोई Cyber Fraud हो जाए या कोई Fake Message आए, तो केवल Official सरकारी Portals पर जाएँ:

1. **National Cyber Crime Portal**
   Cyber Fraud और पैसे की ठगी की तुरंत शिकायत के लिए Website: `cybercrime.gov.in`
2. **Chakshu Portal (Telecom Department)**
   Fake WhatsApp Calls और Fraud Messages की Report के लिए: `sancharsaathi.gov.in`
3. **Google Search का सही तरीका**
   सीधे यह सुरक्षित Keyword खोजें: `cybercrime reporting portal`

Official सत्यापन स्रोत

- Cyber Crime Coordination Centre (I4C), गृह मंत्रालय: `cybercrime.gov.in`
- Telecom Department (Sanchar Saathi Chakshu): `sancharsaathi.gov.in`
- WhatsApp Security Guidelines: `faq.whatsapp.com`

अध्याय 2 • SECURITY SETTINGS (SECURITY SETUP)

अपना WhatsApp Account सुरक्षित करें

5 मिनट की 5 आसान Settings जो आपके WhatsApp को Hackers से 100% सुरक्षित बनाती हैं।

फ़ोन नया हो या पुराना: यह 5 मिनट की सुरक्षा बहुत ज़रूरी है

ज़्यादातर लोग WhatsApp को केवल Install करते हैं और चलाना शुरू कर देते हैं। वे इसकी Security Settings को कभी नहीं देखते।

नतीजा यह होता है कि आपका Account Default रूप से पूरी तरह खुला रहता है। कोई भी अनजान व्यक्ति आपको किसी भी Fake Group में जोड़ सकता है, आपकी Profile Photo Download कर सकता है, और अगर किसी ने आपका Phone 30 सेकंड के लिए ले लिया, तो वह जासूसी भी शुरू कर सकता है।

सुनहरा नियम

WhatsApp का सबसे बड़ा ताला: Two-Step Verification

जब भी आप किसी नए Phone पर WhatsApp शुरू करते हैं, तो एक 6-Digit SMS OTP आता है। लेकिन अगर आपने **Two-Step Verification** चालू किया है, तो SMS के बाद एक दूसरा गुप्त PIN भी माँगा जाता है।

सबसे बड़ा फ़ायदा: अगर कोई चोर आपका SIM या SMS OTP चुरा भी ले, तब भी वह आपके 6-Digit PIN के बिना आपका WhatsApp कभी नहीं खोल पाएगा!

Two-Step Verification कैसे चालू करें? (Step-by-Step)

अपने WhatsApp में अभी ये 4 आसान कदम उठाएँ:

1 **Settings में जाएँ**
WhatsApp खोलें, ऊपर दाईं तरफ 3 Dots पर Click करें और **Settings** चुनें।

↓ Account पर जाएँ

2 **Two-step verification चुनें**
Account → Two-step verification पर Click करके **Turn on** दबाएँ।

↓ 6-Digit PIN बनाएँ

3 **अपना गुप्त PIN दर्ज करें**
अपनी पसंद का 6-अंकों का PIN डालें। (123456 या जन्मतिथि जैसा आसान PIN कभी न रखें)।

↓ Email जोड़ें

4 **सुरक्षित Email Address जोड़ें**
अपना सुरक्षित Email जोड़ें ताकि अगर आप कभी PIN भूल जाएँ, तो उसे आसानी से Reset कर सकें।

4 अन्य ज़रूरी Settings जो आज ही बदलनी चाहिए



1. Linked Devices की जाँच (WhatsApp Web की जासूसी से बचें)

कई बार कोई व्यक्ति 1 मिनट के लिए आपका Phone लेकर WhatsApp Web से अपने Laptop पर Link कर लेता है।

> **क्या करें:** 3 Dots ➔ **Linked devices** खोलें। अगर कोई अनजान Computer दिखे, तो तुरंत **Log out** दबाएँ।



2. Silence Unknown Callers (अनजान Video Call बंद करें)

International Numbers (+92, +84, +62) से आने वाले अश्लील Video Calls और Blackmail से बचने के लिए यह सबसे बढ़िया तरीका है।

> **चालू करें: Settings ➔ Privacy ➔ Calls ➔ Silence unknown callers** को Turn on करें।



3. Groups Privacy (अनजान Groups में जुड़ने पर रोक)

Scammers आपको बिना पूछे Fake Job या Investment Groups में न जोड़ सकें।

> **Settings बदलें: Settings ➔ Privacy ➔ Groups** को **Everyone** से बदलकर **My contacts** करें।



4. Profile Photo व About (DP चोरी से सुरक्षा)

ताकि Scammer आपकी Photo Download करके किसी दूसरे Number पर आपकी Fake DP न लगा सके।

> **Settings बदलें: Privacy** में जाकर **Profile photo** और **About** दोनों को **My contacts** पर सेट करें।

अध्याय 2: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• Two-Step Verification का 6-Digit PIN और Email तुरंत सेट करें।

• महीने में एक बार Linked Devices खोलकर अनजान Browsers को Log out करें।

• Phone की सुरक्षा के लिए WhatsApp में **Fingerprint / App Lock** चालू रखें।

❌ यह कभी न करें (DONTs)

• किसी अनजान व्यक्ति को 1 मिनट के लिए भी अपना Phone अनलॉक करके न दें।

• Group Privacy को **Everyone** पर खुला न छोड़ें।

• Two-Step Verification में 111111 या 123456 जैसा आसान PIN न रखें।

Official सत्यापन स्रोत

• WhatsApp Security & Two-Step Verification Guide: `faq.whatsapp.com`

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

अध्याय 3 • खाता चोरी (ACCOUNT TAKEOVER)

Account Hack होने का OTP Scam

6-Digit Registration Code चोरी की चाल, Call Forwarding का सच और 10 मिनट में Account वापस पाने का तरीका।

एक Code और WhatsApp आपके हाथ से बाहर!

WhatsApp की सबसे बड़ी कमी तकनीक नहीं, बल्कि हमारा भरोसा है। जब भी आप किसी नए Phone पर WhatsApp शुरू करते हैं, तो एक 6-अंकों का Official SMS Code आता है।

Scammer आपके Phone को छुए बिना आपका WhatsApp चुराना चाहता है। इसके लिए वह आपके किसी दोस्त का पहले से Hack हुआ WhatsApp इस्तेमाल करके आपको एक बहुत ही मासूम Message भेजता है।

खतरे की घंटी

Code भेजते ही क्या होता है?

जैसे ही आप वह 6-Digit Code सामने वाले को बताते हैं, अगले ही सेकंड आपकी Screen पर लिखा आता है: *"Your phone number is no longer registered with WhatsApp on this phone."*

नतीजा: आपका WhatsApp बंद हो जाता है और Hacker आपके पूरे दोस्तों और रिश्तेदारों से आपके नाम पर पैसे माँगना शुरू कर देता है!

Case Study: "यार, मेरा Code गलती से तुम्हारे पास आ गया"

देखें कैसे एक पक्के दोस्त के नाम से Scammer जाल बिछाता है:

💬 WHATSAPP CHAT (दोस्त का HACK हुआ ACCOUNT)

दोस्त (Hacker के कब्ज़े में): "अरे भाई! गलती से मेरा 6-Digit Verification Code तुम्हारे Mobile पर SMS से चला गया है। ज़रा जल्दी देखकर बता दो, मेरा बहुत ज़रूरी काम रुका है।"

आप: "हाँ भाई, 482-195 आया है। क्या हुआ था?"

Hacker: *(Code डालते ही आपका WhatsApp बंद और Hacker का Two-Step PIN चालू!)*

पहचानें: WhatsApp का Code कभी किसी दूसरे के Phone पर गलती से नहीं जा सकता। अगर आपके Phone पर Code आया है, तो इसका मतलब है कि कोई आपके Number से Login करने की कोशिश कर रहा है!

ख़तरनाक चाल: Call Forwarding Code (*401* या *21*)

कई बार Scammer आपसे Code भी नहीं माँगता। वह सामान्य Phone Call करके Telecom Company या Bank का कर्मचारी बनकर बोलता है:

धोखे का बहाना

"5G Speed के लिए यह Number Dial करें"

*"सर, आपका 5G Network चालू करने के लिए अपने Phone के Dialer में जाकर *401*<Number> Dial करें।"*

असली सच: *401* दरअसल **Call Forwarding** का गुप्त Code है। जैसे ही आप इसे Dial करते हैं, आपकी सारी Calls Scammer के Phone पर जाने लगती हैं। इसके बाद Scammer WhatsApp से Voice Call OTP मँगवाकर आपका खाता Hack कर लेता है।

अगर Account Hack हो जाए, तो क्या करें? (10-Minute Recovery)

बिल्कुल घबराएँ नहीं! WhatsApp के Official नियमों के अनुसार तुरंत ये कदम उठाएँ:

1 **दोबारा Login करने की कोशिश करें**
अपने Phone में WhatsApp खोलें, अपना Mobile Number डालें और **Next** दबाएँ।

↓ SMS से नया Code मँगवाएँ

2 **नया 6-Digit SMS Code दर्ज करें**
जादुई सुरक्षा नियम: जैसे ही आप SMS Code डालेंगे, Hacker उसी सेकंड आपके Account से **तुरंत Log out** हो जाएगा!

↓ अगर Hacker ने PIN लगा दिया है?

3 **7 दिन का इंतज़ार करें (Hacker पहले ही बाहर है)**
Hacker भी अब आपका WhatsApp नहीं चला सकता। 7 दिन बाद आप बिना PIN के अपना WhatsApp फिर से चालू कर सकेंगे।

↓ अपनों को सावधान करें

4 **दोस्तों को तुरंत Phone Call करके बताएँ**
सामान्य Call या SMS करके सबको बता दें: *"मेरा WhatsApp Hack हो गया है, कोई भी पैसों की माँग पर पैसे न भेजे।"*

अध्याय 3: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• Phone पर आए किसी भी 6-Digit Code को Secret रखें।

• Call Forwarding की जाँच के लिए `##002#` Dial करें (इससे सारी Forwarding रद्द हो जाती है)।

• आज ही अपना Two-Step Verification PIN चालू करें।

❌ यह कभी न करें (DONTs)

• सगे भाई या दोस्त के Message पर भी अपना WhatsApp Code कभी न भेजें।

• अनजान व्यक्ति के कहने पर Phone Dialer में `*401*` या `*21*` Dial न करें।

• Hack होने पर चुप न बैठें, तुरंत अपनों को Call करके चेतावनी दें।

Official सहायता स्रोत

• 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`

अध्याय 4 • वायरस और खतरनाक FILES (MALWARE)

Fraud Link और APK File

शादी का Card, चालान और बिजली बिल के नाम पर आने वाली खतरनाक Files से अपने Phone और Bank को कैसे बचाएँ।

शादी का Card या Bank खाता खाली करने वाला वायरस?

आजकल WhatsApp पर एक नया ट्रेंड चल रहा है। किसी रिश्तेदार या अनजान Number से एक File आती है, जिस पर लिखा होता है: `Wedding_Card.apk` या `Bijli_Bill.apk`।

लोग सोचते हैं कि यह कोई शादी का Card या निमंत्रण पत्र है, या बिजली बिल की रसीद है। वे बिना सोचे उस पर Click कर देते हैं। लेकिन Click करते ही शादी का Card खुलने के बजाय, Phone में एक छिपा हुआ खतरनाक Spyware Install हो जाता है।

याद रखें

APK File क्या होती है?

APK का मतलब है Android Package Kit। यह Android Phone में किसी भी नए App को Install करने की मुख्य File होती है।

सीधा नियम: असली शादी के Card हमेशा PDF File या Photo (जैसे JPG/PNG) होते हैं। किसी भी असली Card के नाम के आगे कभी `.apk` नहीं लिखा होता!

Case Study: WhatsApp पर आने वाला शादी का Card

देखें कैसे Scammer एक मासूम Message के ज़रिए Phone में वायरस घुसाता है:

💬 WHATSAPP MESSAGE (शादी के CARD का झाँसा)

अनजान Number (रिश्तेदार की DP): "हमारे बेटे की शादी में आपका सपरिवार स्वागत है। कृपया नीचे दी गई File खोलकर शादी का पूरा कार्यक्रम देखें: 📄 `Wedding_Invitation_2026.apk`"

उपयोगकर्ता: *(सोचता है कि शादी का Card है, Click कर देता है... Screen पर 'Install unknown app' आता है और Allow दबा देता है!)*

नतीजा: *(Card नहीं खुला, लेकिन Phone के सारे SMS और Bank OTP सीधे Scammer तक पहुँचने लगे!)*

Scammers के 4 सबसे बड़े APK बहाने



1. शादी का Card (Wedding Card APK)

रिश्तेदार की चोरी की हुई DP लगाकर भेजा जाता है ताकि कोई शक न करे।

फ़ाइल का नाम: `Shadi_Card.apk` या `Wedding_Card.apk`



2. Traffic E-Challan APK

"आपके वाहन का ₹2,000 का चालान कटा है, तुरंत भरें नहीं तो कोर्ट का नोटिस आएगा।"

> **फ़ाइल का नाम:** `Vehicle_Fine_Challan.apk`



3. बिजली बिल Update APK

"रात 9:30 बजे बिजली कनेक्शन कट जाएगा। तुरंत इस App से Bill Check करें।"

> **फ़ाइल का नाम:** `Electricity_Bill_Pay.apk`



4. सरकारी योजना / PM Kisan APK

"मुफ़्त ₹5,000 पाने के लिए तुरंत यह Form भरें।"

> **फ़ाइल का नाम:** `PM_Yojana_Kisan.apk`

अगर गलती से APK Install हो जाए, तो तुरंत क्या करें?

1 मिनट भी न गँवाएँ! तुरंत ये 4 कदम उठाएँ:

1

Phone को तुरंत Airplane Mode में डालें

Wi-Fi और Mobile Data तुरंत बंद कर दें ताकि वायरस Scammer को आपके Bank OTP न भेज सके।

↓ बिना Internet के App Delete करें

2

Settings से App खोजकर Uninstall करें

Settings → Apps → Manage apps में जाएँ। उस Fake App को चुनें और तुरंत **Uninstall** दबाएँ।

↓ Security Scan चलाएँ

3

Google Play Protect Scan चलाएँ

Google Play Store खोलें, अपनी Profile पर जाकर **Play Protect → Scan** दबाएँ।

↓ अगर App सामान्य रूप से Delete न हो?

4

Safe Mode में Restart करके हटाएँ

Phone का Power Button दबाकर रखें, **Power off** को दबाए रखें और **Safe Mode** में Restart करके App हटाएँ।

अध्याय 4: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• केवल Google Play Store से ही Verified Apps Install करें।

• Phone Settings में "Install unknown apps" को हमेशा बंद (Off) रखें।

• असली सरकारी Websites के अंत में हमेशा `.gov.in` ज़रूर देखें।

❌ यह कभी न करें (DONTs)

• किसी भी `.apk` नाम वाली File को गलती से भी Install न करें।

• `bit.ly` या `tinyurl` वाले किसी अनजान Short Link पर Click न करें।

• मुफ़्त Phone या Recharge का लालच देने वाले Links को 5 Groups में Share न करें।

Official सत्यापन स्रोत

• 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`

अध्याय 5 • पार्ट-टाइम जॉब का जाल (TASK SCAMS)

Fake Job और घर बैठे कमाई के Offer

YouTube Video Like करने के नाम पर हज़ारों करोड़ की ठगी, शुरुआत के ₹500 का चारा और असली सच।

"रोज़ ₹3,000 कमाएँ": क्या सच में कोई मुफ़्त पैसा बाँटता है?

गृह मंत्रालय के Cyber Cell (I4C) के अनुसार, आज भारत में सबसे ज़्यादा Online ठगी **Task-Based Part-Time Job Scam** के ज़रिए हो रही है।

Scammer जानता है कि लोग घर बैठे Extra कमाई करना चाहते हैं। इसलिए वह एक ऐसा काम बताता है जिसमें न किसी पढ़ाई की ज़रूरत होती है और न ही किसी अनुभव की—बस YouTube Videos को Like करना या Google Maps पर 5-Star Rating देना!

सबसे बड़ा धोखा

शुरुआत में सच में पैसे मिलते हैं!

इस Scam की सबसे बड़ी चालाकी यह है कि शुरुआत के 2-3 Tasks पूरे करने पर **Scammer सच में आपके UPI या Bank खाते में ₹150 से ₹500 भेज देता है!**

क्यों? ताकि आपका शक 100% ख़त्म हो जाए। यह मछली पकड़ने के लिए डाला गया काँटा (चारा) है। जैसे ही आप विश्वास कर लेते हैं, वे आपको Telegram पर ले जाकर लाखों रुपये लूट लेते हैं।

Case Study: 3 Videos Like करके ₹300 पाने का जाल

देखें कैसे यह बातचीत WhatsApp पर शुरू होती है:

WHATSAPP CHAT (FAKE HR RECRUITER)

Priya (Global HR): "नमस्ते! हमारे पास आपके लिए Part-time Work From Home Job है। आपको बस 3 YouTube Videos को Like करके Screenshot भेजना है। हर Like का ₹100 मिलेगा। क्या आप तैयार हैं?"

उपयोगकर्ता: "हाँ, मैंने तीनों Videos Like करके Screenshot भेज दिए हैं।"

Priya: "बधाई हो! आपकी UPI ID पर ₹300 भेज दिए गए हैं। आगे के बड़े Tasks और रोज़ ₹5,000 कमाने के लिए हमारे VIP Telegram Group से जुड़ें!"

Task Scam का चक्र: ₹500 से लाखों का नुकसान

1 **WhatsApp पर पहला Message**
सुंदर Photo वाली HR का Message: "घर बैठे Video Like करें और रोज़ ₹3,000 कमाएँ।"

↓ विश्वास जीतना

2 **सच में ₹300 का Payment (चारा)**
3 छोटे काम करने पर आपके UPI पर सच में ₹300 आ जाते हैं। आप मान लेते हैं कि काम असली है।

↓ Telegram पर ले जाना

3 **VIP Telegram Group में जोड़ना**
Group में 100 नकली लोग रोज़ाना ₹50,000 के Payout के Fake Screenshots डालकर माहौल बनाते हैं।

↓ Prepaid Tasks का खेल

4 **पैसे जमा करने की शर्त**
"₹1,000 जमा करें और ₹1,400 पाएँ", फिर "₹10,000 जमा करें और ₹14,000 पाएँ।"

↓ पैसा Freeze और खाता खाली

5 **पैसे निकालने पर रोक (The Trap)**
जब आप ₹1 लाख जमा कर देते हैं, तो Scammer कहता है: "30% Tax जमा करो वरना पैसा Freeze रहेगा।" अंत में सारा पैसा गायब!

असली Job vs Fake Job Scam



असली Job की पहचान

• कंपनी अपने कर्मचारी को काम के बदले वेतन देती है, कभी पैसे नहीं माँगती।

• भर्ती हमेशा LinkedIn, Official Website या Company Email से होती है।

> **सुनहरा नियम:** काम करने के लिए कभी ₹1 भी जमा नहीं करना पड़ता।



Fake Job Scam की पहचान

• अनजान WhatsApp Number या International Number से अचानक Message आता है।

• काम शुरू करने के लिए "Security Deposit" या "Prepaid Task" के नाम पर पैसे माँगे जाते हैं।

• बातचीत को WhatsApp से निकालकर Telegram पर ले जाने का दबाव बनाया जाता है।

अध्याय 5: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• याद रखें: पैसे देकर पैसे कमाने वाला कोई काम दुनिया में नहीं होता।

• अगर किसी ने शुरुआत में ₹200-₹300 भेज भी दिए हैं, तो आगे ₹1 भी न डालें।

• ऐसे Messages को WhatsApp पर ही सीधे **Report** और **Block** करें।

❌ यह कभी न करें (DONTs)

• किसी भी अनजान व्यक्ति के कहने पर Telegram Groups में न जुड़ें।

• Video Like करने या Review देने के नाम पर किसी को अपने पैसे Transfer न करें।

• "फँसे हुए पैसे निकालने के लिए और पैसे जमा करो" वाले झाँसे में न आएँ।

Official सत्यापन स्रोत

• Indian Cyber Crime Coordination Centre (I4C), गृह मंत्रालय एडवाइज़री: `cybercrime.gov.in`

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

अध्याय 6 • पहचान की चोरी (IMPERSONATION SCAMS)

जान-पहचान वाले के नाम से पैसे माँगना

दोस्त या Boss की DP लगाकर मुसीबत (Emergency) का नाटक, Merchant UPI का खेल और 60-Second का Verification Test।

"भाई, Hospital में फँसा हूँ": क्या सच में आपका दोस्त मुसीबत में है?

सोचिए, आपके WhatsApp पर आपके किसी सगे रिश्तेदार, सबसे पक्के दोस्त या Office के Boss की DP और नाम से एक Message आता है: *"बहुत बड़ी Emergency है, तुरंत इस UPI पर ₹25,000 भेज दो, शाम को लौटा दूँगा।"*

हम में से ज़्यादातर लोग अपने इंसान को मुसीबत में देखकर बिना सोचे पैसे Transfer कर देते हैं। बाद में पता चलता है कि वह व्यक्ति तो अपने घर पर आराम से बैठा था, और पैसे किसी चोर के खाते में चले गए!

सच्चाई समझें

Photo पहचान का सबूत नहीं है!

आज के समय में Internet से किसी भी व्यक्ति की Facebook, Instagram या LinkedIn से Photo Download करने में सिर्फ 5 सेकंड लगते हैं।

सीधा नियम: कोई भी नया Number जिस पर आपके दोस्त की Photo लगी हो, वह आपका दोस्त नहीं है जब तक कि आप उसकी आवाज़ न सुन लें!

Case Study: नए Number से Boss का Message

देखें कैसे Scammer एक नया Number लेकर Office के कर्मचारियों को ठगता है:

WHATSAPP CHAT (COMPANY DIRECTOR की FAKE DP)

Director (नया अनजान Number): "अमित, यह मेरा नया Personal Number है। मैं एक क्लाइंट के साथ बहुत ज़रूरी मीटिंग में हूँ और मेरा Bank App Login नहीं हो रहा। तुरंत इस Vendor को ₹40,000 भेज दो, मैं 1 घंटे में Office आकर Cash दे दूँगा।"

अमित: "सर, मैं भेज तो रहा हूँ, लेकिन UPI पर नाम 'M/S Quick Enterprise' क्यों दिख रहा है?"

Director (Scammer): "हाँ, यह उसी क्लाइंट की फर्म है। जल्दी करो, बहुत ज़रूरी है!"

पैसे भेजने से पहले: 60-Second का Verification Test

जब भी कोई अपना WhatsApp पर पैसे माँगे, आँख मूँदकर पैसे भेजने से पहले ये 3 काम ज़रूर करें:

1 **पुराने सुरक्षित Number पर सामान्य Call करें**
जिस Number से Message आया है उस पर नहीं, बल्कि अपनी Phone Book में पहले से Save असली Number पर साधारण Phone Call करें।

↓ अगर Call न लगे तो?

2 **ऐसा गुप्त सवाल पूछें जो सिर्फ उसे पता हो**
पूछें: "हम पिछली बार किस जगह मिले थे?" या "तुम्हारे छोटे भाई का क्या नाम है?" असली दोस्त 2 सेकंड में बताएगा, चोर बहाने बनाएगा।

↓ आवाज़ Confirm करना

3 **10-सेकंड का Voice Note माँगें**
कहें: "भाई, 10 सेकंड का Voice Note भेजकर मेरा नाम बोलो।" Scammer कभी आपका नाम लेकर आवाज़ नहीं भेज पाएगा।

UPI ID पर दिखने वाले नाम की जाँच करें

🔍

Name Mismatch का मतलब सीधा Fraud

जब आप PhonePe, Google Pay या Paytm में UPI ID डालते हैं, तो असली खाताधारक का नाम दिखता है।

> अगर आपके दोस्त का नाम **रोहित शर्मा** है, लेकिन UPI में नाम **"M/S Quick Enterprise"** या कोई अनजान नाम दिख रहा है, तो 1 रुपया भी न भेजें!

अध्याय 6: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• पैसों की माँग आने पर पहले पुराने असली Number पर Phone Call करके बात करें।

• Voice Note माँगकर आवाज़ Confirm करें।

• UPI ID पर दिखने वाले नाम को ध्यान से Check करें।

❌ यह कभी न करें (DONTs)

• केवल DP और नाम देखकर तुरंत पैसे Transfer न करें।

• "नया Number है, पुराना बंद हो गया" वाले बहाने पर बिना सोचे विश्वास न करें।

• किसी अनजान व्यक्ति की UPI ID पर दोस्त के कहने पर भी पैसे न डालें।

Official सत्यापन स्रोत

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

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

अध्याय 7 • UPI और QR CODE SAFETY

WhatsApp पर UPI Payment और QR Scam

पैसे पाने के लिए कभी PIN नहीं चाहिए — Fake Army Officer का नाटक, Fake QR Code और Collect Request का सच।

"पैसे लेने के लिए QR Code Scan करो": सबसे बड़ा झूठ!

सोचिए, आप OLX या Facebook पर अपना पुराना सोफ़ा, Mobile या गाड़ी बेचने की Post डालते हैं। 10 मिनट के अंदर WhatsApp पर एक बहुत ही सभ्य खरीदार का Message आता है: *"मुझे आपका सामान पसंद है। मैं पूरा पैसा Advance भेज रहा हूँ। यह QR Code Scan करें और PIN डालें, पैसे तुरंत आपके खाते में आ जाएँगे।"*

जैसे ही आप पैसे पाने की उम्मीद में वह QR Code Scan करके अपना UPI PIN डालते हैं, खाते में पैसे आने के बजाय उल्टे ₹15,000 कट जाते हैं!

पत्थर की लकीर

NPCI और RBI का सबसे बड़ा नियम

UPI PIN का उपयोग केवल और केवल आपके Bank खाते से पैसे काटने (Debit) के लिए होता है।

सीधा नियम: दुनिया में किसी से भी पैसे लेने (Receive करने) के लिए कभी भी UPI PIN या OTP डालने की ज़रूरत नहीं होती। QR Code सिर्फ पैसे **भेजने** के लिए Scan किया जाता है, पैसे लेने के लिए नहीं!

Case Study: OLX पर नकली फौजी (Army Officer Scam)

देखें कैसे Scammer वर्दी की Photo लगाकर लोगों को ठगता है:

💬 WHATSAPP CHAT (FAKE ARMY OFFICER)

Major Vikram (वर्दी वाली DP): "नमस्ते भाई! मैंने आपकी बाइक की Post देखी है। मैं Army Cantt में पोस्टेड हूँ और मुझे यह बाइक पसंद है। मैं अभी ₹30,000 Advance भेज रहा हूँ।"

विक्रेता: "धन्यवाद सर, आप मेरे इस Number पर Google Pay कर दीजिए।"

Major Vikram: "भाई, आर्मी का सरकारी Merchant Account सीधे Transfer नहीं कर सकता। मैं आपको एक स्पेशल QR Code भेज रहा हूँ। इसे PhonePe से Scan करके अपना PIN डालें, पैसा आपके खाते में जमा हो जाएगा।"

सच्चाई: *(जैसे ही विक्रेता PIN डालता है, ₹30,000 खाते में आने के बजाय उल्टे कट जाते हैं!)*

QR Scam से बचने का 3-Step Formula

1 **QR Code कभी Scan न करें**
अगर सामने वाला कहे कि पैसे लेने के लिए QR Code Scan करो, तो साफ़ मना करें: *"मुझे कोई QR Scan नहीं करना, सीधे मेरे Mobile Number पर पैसे भेजो।"*

↓ दिमाग की घंटी बजाएँ

2 **याद रखें: PIN = पैसा कटेगा**
जहाँ भी Screen पर PIN डालने का Keypad आए, समझ जाएँ कि आपके खाते से पैसा जा रहा है।

↓ असली Balance Check

3 **असली Bank App में Balance Check करें**
केवल WhatsApp के Photo Screenshot या SMS पर भरोसा न करें। अपने Bank App (जैसे SBI YONO, iMobile आदि) में जाकर Passbook Check करें।

WhatsApp Pay और Collect Request का धोखा

⚠

Chat में आए Payment Request को कभी Approve न करें

कई बार Scammer Chat में **Collect Request** भेजता है और कहता है कि "Approve पर दबाओ, पैसे मिल जाएँगे।"

> **क्या करें:** अनजान व्यक्ति की किसी भी Request पर हमेशा **Decline** (ठुकराएँ) दबाएँ। अगर आपने **Pay** दबाकर PIN डाल दिया तो पैसे तुरंत कट जाएँगे।

अध्याय 7: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

- पैसे लेने के लिए केवल अपना Mobile Number या UPI ID दें।
- पैसा आने का पक्का सबूत हमेशा अपने असली Bank App में Balance देखकर Check करें।
- वर्दी या Canteen Card की Photo देखकर आँख मूँदकर विश्वास न करें।

❌ यह कभी न करें (DONTs)

- पैसे लेने के लिए दुनिया का कोई भी QR Code Scan न करें।
- पैसे लेने के लिए कभी भी अपना UPI PIN दर्ज न करें।
- "गलती से ज़्यादा पैसे चले गए, वापस भेजो" वाले Fake SMS पर विश्वास न करें।

Official सत्यापन स्रोत

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

अध्याय 8 • FAKE INVESTMENT का जाल (STOCK & TIP SCAMS)

Fake Investment और Tip Group

शेयर बाज़ार में पक्के मुनाफ़े का झूठा सपना, Fake Trading App और हज़ारों करोड़ की ठगी का सच।

"1 महीने में पैसा डबल": क्या शेयर बाज़ार में ऐसा मुमकिन है?

सोचिए, आपको अचानक किसी अनजान WhatsApp Group में जोड़ दिया जाता है जिसका नाम होता है: *"VIP Stock Market Pro Tips"* या *"Institutional Wealth Club"*।

उस Group में सुबह से शाम तक बड़े-बड़े मुनाफ़े के Photo Screenshots आ रहे होते हैं: कोई लिखता है कि उसे आज ₹1 लाख का फ़ायदा हुआ, तो कोई अपनी नई लग्ज़री कार की Photo डालता है।

बहुत ज़रूरी सूचना

SEBI की सबसे बड़ी चेतावनी

भारत के शेयर बाज़ार की सरकारी संस्था **SEBI** (Securities and Exchange Board of India) के अनुसार, आज देश में सबसे ज़्यादा पढ़े-लिखे लोग और रिटायर्ड बुज़ुर्ग इसी एक Scam में अपनी ज़िंदगी भर की बचत गँवा रहे हैं।

सीधा नियम: शेयर बाज़ार में 100% Guaranteed Return या "पक्का मुनाफ़ा" नाम की कोई चीज़ नहीं होती। जहाँ भी पक्के मुनाफ़े का दावा हो, वह 100% Fraud है।

Case Study: VIP Stock Group का नकली माहौल

देखें कैसे उस Group में 95% लोग Scammer के ही साथी या Bots होते हैं:

💬 WHATSAPP GROUP CHAT (FAKE VIP COMMUNITY)

Admin (Stock Expert): "कल हमारे VIP Members को हमने स्पेशल Upper Circuit Stock दिया था। आज 20% का Profit Book हुआ। Screenshot Share करें!"

Member 1 (Fake Bot): "सर! कल ₹50,000 लगाए थे, आज ₹65,000 बन गए। आपकी Tips भगवान जैसी हैं! 🙏"

Member 2 (Fake Bot): "मैंने ₹2 लाख लगाए थे, अभी ₹40,000 अपने Bank में निकाल लिए। बहुत-बहुत धन्यवाद सर!"

नया व्यक्ति (FOMO का शिकार): *(सोचता है कि सब कमा रहे हैं, मैं भी क्यों पीछे रहूँ? वह Admin को Message करता है और फँस जाता है!)*

Fake Investment Trap का पूरा खेल

1 **अनजान Group में जोड़ना**
Group का नाम किसी मशहूर शेयर बाज़ार के Expert या बड़ी विदेशी Company के नाम पर रखा जाता है।

↓ नकली मुनाफ़े का लालच

2 **Fake Trading App Download करवाना**
Scammer कहता है: "हम सामान्य Apps में काम नहीं करते, हमारी स्पेशल VIP App Download करें।" वह App पूरी तरह Fake होता है।

↓ Screen पर नकली मुनाफ़ा

3 **शुरुआत में ₹5,000 निकालने देना (विश्वास)**
ताकि आपका भरोसा पक्का हो जाए। इसके बाद आप लालच में आकर ₹10 लाख या ₹20 लाख तक डाल देते हैं।

↓ पैसे Freeze और वसूली

4 **पैसे निकालने पर Tax और वसूली का खेल**
जब आप पैसा निकालने जाते हैं, तो Scammer कहता है: "20% Tax जमा करो", "Security Deposit दो।" अंत में Group बंद और सारा पैसा डूब जाता है।

असली निवेश vs Fake WhatsApp Scam



असली SEBI Registered निवेश की पहचान

• पैसा हमेशा आपके अपने नाम के Demat/Trading Account में जमा होता है।

• कभी किसी अनजान व्यक्ति के व्यक्तिगत Savings Account में पैसा Transfer नहीं किया जाता।

> **नियम:** असली बाज़ार में कोई Guaranteed Return का वादा नहीं करता।



Fake WhatsApp Scam की पहचान

• 200% से 500% के पक्के मुनाफ़े का झूठा दावा किया जाता है।

• पैसा किसी "Ramesh Kumar" या किसी अनजान ट्रस्ट के चालू खाते में जमा करने को कहा जाता है।

• Google Play Store के बाहर की किसी अनजान Link से App Download करने को कहा जाता है।

अध्याय 8: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• अनजान Stock Market Groups से तुरंत **Exit** करें और उन्हें **Report** करें।

• केवल SEBI Registered Official Brokers के साथ ही निवेश करें।

• किसी भी Broker की सत्यता जाँचने के लिए `sebi.gov.in` पर उनका Registration Number Check करें।

❌ यह कभी न करें (DONTs)

• WhatsApp या Telegram पर मिलने वाली शेयर Tips पर आँख मूँदकर पैसे न लगाएँ।

• किसी अनजान व्यक्ति के निजी Bank खाते में निवेश के नाम पर पैसा Transfer न करें।

• "Guaranteed Return" या "बिना Risk के मुनाफ़ा" वाले Ads पर कभी भरोसा न करें।

Official सत्यापन स्रोत

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

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

अध्याय 9 • GROUP PRIVACY और सुरक्षा

अनजान Group और Fake Profile

विदेशी Country Codes का खेल, अनजान Groups की रोकथाम और 30-Second की Group Privacy Setting।

सुबह उठते ही अनजान Group में आपका Number?

क्या आपके साथ कभी ऐसा हुआ है कि आप सुबह उठकर WhatsApp खोलते हैं और देखते हैं कि आपको *"Crypto VIP 500X"*, *"Daily Online Earning"* या *"Part-Time Work India"* नाम के किसी अनजान Group में जोड़ दिया गया है?

उस Group में सैकड़ों लोग होते हैं और Group का Admin किसी विदेशी Country Code (जैसे +84, +62, +254 या +92) वाले Number से लंबे-चौड़े Messages और Links भेज रहा होता है।

खतरे की बात

Scammers के पास आपका Number कहाँ से आता है?

Scammers Internet पर लीक हुए डेटाबेस, पुरानी Websites या Random Number Generator Software से हज़ारों Phone Numbers की लिस्ट निकालते हैं और बिना किसी रोक-टोक के सबको एक साथ नए Groups में डाल देते हैं।

सीधी बात: अगर कोई व्यक्ति आपकी Contact List में नहीं है और आपको किसी अनजान Group में जोड़ता है, तो वह 99.9% Fraud या Spam का हिस्सा होता है।

Case Study: अनजान International Group का माहौल

देखें कैसे अनजान Groups में लोगों को फँसाने के लिए जाल बुना जाता है:

💬 WHATSAPP GROUP (UNSOLICITED ADDITION)

Admin (+84 98...): "नमस्ते सभी नए Members! इस Group में आपको रोज़ाना घर बैठे ₹2,000 कमाने के आसान Tasks मिलेंगे। शुरू करने के लिए नीचे दिए Link पर Click करें।"

Fake Bot 1 (+62 81...): "सर, मैंने आज का Task पूरा कर लिया और मुझे ₹500 मिल गए!"

साधारण User (आप): *(सोचता है: मुझे इस Group में किसने जोड़ा? मैं तो इनमें से किसी को भी नहीं जानता!)*

Fake Profile के 4 सबसे बड़े लक्षण

Scammer किसी असली इंसान की Profile चुराकर या बनाकर आपसे संपर्क करता है। इन 4 बातों से उसकी पहचान करें:

🌐

1. International Country Code

भारत में रहकर भी Number +84 (Vietnam), +62 (Indonesia), +254 (Kenya), या +1 (USA Virtual VoIP) से शुरू होता है।

👤

2. चुराई हुई सुंदर DP

Google या Social Media से Download की गई किसी मॉडल, फौजी या सुंदर लड़की की Photo लगाई जाती है ताकि भरोसा हो सके।



3. अधूरा या अजीब 'About'

About/Bio में "Online Business", "HR Manager", या टूटी-फूटी अंग्रेजी में लिखा होता है। कोई असली पहचान नहीं होती।



4. Admin-Only Group Settings

Group में केवल Admin ही Message भेज सकता है। बाकी आम Members के लिए Messages बंद रखे जाते हैं ताकि कोई सवाल न पूछ सके।

अनजान Groups को रोकने की 30-Second Setting

WhatsApp में यह एक Setting चालू कर लें। इसके बाद कोई भी अनजान व्यक्ति आपको सीधे किसी Group में नहीं जोड़ पाएगा:

1

WhatsApp Settings खोलें

ऊपर दाईं तरफ **3 बिंदु (⋮)** दबाएँ और **Settings** पर Click करें।

↓ Privacy विकल्प चुनें

2

Privacy ➔ Groups में जाएँ

Privacy पर दबाएँ, फिर नीचे Scroll करके **Groups** वाले विकल्प को चुनें।

↓ "My Contacts" चुनें

3

"Everyone" हटाकर "My Contacts" चुनें

यहाँ पहले से **Everyone** चुना होता है। इसे बदलकर **My Contacts** कर दें।

फ़ायदा

अब क्या होगा?

अब केवल वही लोग आपको Group में जोड़ सकेंगे जिनका Number आपके Phone में Save है। अगर कोई अनजान व्यक्ति आपको जोड़ना चाहेगा, तो उसे पहले आपको एक **Invite Link** भेजना पड़ेगा, जिसे स्वीकार करना पूरी तरह आपकी पसंद होगी।

अध्याय 9: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• Group Privacy को आज ही **"My Contacts"** पर सेट करें।

• अनजान Group में जोड़े जाने पर तुरंत **Exit Group** और **Report** करें।

• अनजान Calls से बचने के लिए Settings में **"Silence unknown callers"** चालू रखें।

❌ यह कभी न करें (DONTs)

• अनजान Group में आए किसी भी Link पर कभी Click न करें।

• Group में आए किसी अनजान व्यक्ति के कहने पर अपने पैसे न लगाएँ।

• अनजान International Numbers (+84, +62 आदि) से आए Calls कभी न उठाएँ।

Official सत्यापन स्रोत

• 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`

अध्याय 10 • AI और VIDEO CALLS का खतरा

WhatsApp पर AI Voice और Video Fraud

अपनों की आवाज़ में Clone Call, अनजान Video Call का फंदा और Blackmail से बचने का तरीका।

"पापा, मेरा Accident हो गया!": क्या वह सच में आपका बेटा है?

सोचिए, दोपहर के समय आपके WhatsApp पर एक अनजान Number से Call या Voice Note आता है। आवाज़ बिल्कुल आपके बेटे की होती है, वह रोते हुए कहता है: *"पापा, Police ने मुझे पकड़ लिया है / मेरा बहुत बड़ा Accident हो गया है, तुरंत इस खाते में ₹50,000 भेजो नहीं तो जेल हो जाएगी!"*

किसी भी माँ-बाप के लिए यह सुनते ही होश उड़ जाना स्वाभाविक है। लेकिन 99% मामलों में आपका बेटा अपने College या Office में सुरक्षित बैठा होता है, और वह आवाज़ सिर्फ **AI Voice Clone** होती है!

नई तकनीक का खतरा

AI आवाज़ कैसे चुराता है?

आजकल Instagram Reels, YouTube Shorts या Facebook Videos से किसी की भी केवल 3 से 5 सेकंड की साफ़ आवाज़ लेकर AI Software हूबहू नकल तैयार कर सकता है। रोने की आवाज़, डर या Panic के भाव—सब कुछ Computer से बनाया जाता है।

पहला नियम: चाहे आवाज़ कितनी भी अपने जैसी लगे, अगर अनजान Number से पैसों की Emergency माँग आए, तो पैसे भेजने से पहले 10 सेकंड रुकें और असली Number पर Call करें।

Case Study: AI Voice Note और डर का माहौल

देखें कैसे Scammer रोने-धोने का नाटक करके माता-पिता को डराता है:

WHATSAPP VOICE CALL / AUDIO MESSAGE

नकली बेटा (AI Clone Voice): "पापा! बचा लो... गाड़ी से एक आदमी टकरा गया है। Police वाले ₹40,000 माँग रहे हैं, नहीं तो FIR कर देंगे। इस UPI ID पर तुरंत पैसे भेजो!"

सतर्क पिता (समझदार User): "बेटा, शांत हो जाओ। पहले यह बताओ कि तुम्हारी नानी का क्या नाम है? और तुम किस दोस्त के साथ थे?"

नकली बेटा (बहानेबाज़ी): "पापा, बाद में पूछना, अभी बहुत Emergency है, Police Phone छीन रही है!"

सच्चाई: *(जैसे ही पिता ने बेटे के असली Number पर सामान्य Call की, बेटा बोला: "पापा, मैं तो Office की Canteen में चाय पी रहा हूँ!")*

अनजान Video Call और Video Blackmail का फंदा

रात के समय WhatsApp पर किसी अनजान Number से अचानक Video Call आता है। DP में किसी सुंदर लड़की की Photo लगी होती है।

Call उठाते ही जाल

जैसे ही आप Call उठाते हैं, सामने कोई अश्लील Video चल रहा होता है। आपकी शक्ल Camera में दिखते ही Scammer Screen Recording

चालू कर देता है।

⚖️

Fake Police और CBI की धमकी

अगले ही मिनट आपकी शक्ल जोड़कर बनाया गया Video भेजा जाता है और "CBI / Delhi Police" बनकर पैसे न देने पर Video Viral करने की धमकी दी जाती है।

अगर कोई Video Blackmail करे तो क्या करें?

अगर कभी गलती से कोई इस जाल में फँस जाए, तो इन 4 कदमों का तुरंत पालन करें:

1

1 रुपया भी कभी Transfer न करें

अगर आपने एक बार ₹5,000 दे दिए, तो वे आपसे ₹5 लाख तक वसूलेंगे। पैसे देने से Blackmail कभी बंद नहीं होता।

↓ सबूत सुरक्षित रखें

2

Screenshots और Number का Record रखें

धमकी भरे Messages, UPI ID और Phone Numbers के Screenshots ले लें। यह शिकायत के समय काम आएँगे।

↓ संपर्क काटें

3

तुरंत Block और Report करें

Scammer से बहस न करें, न ही गिड़गिड़ाएँ। सीधे उस Number को WhatsApp पर **Block** और **Report** करें।

↓ तुरंत सरकारी शिकायत

4

National Cyber Crime Portal पर शिकायत करें

तुरंत National Cyber Crime Portal `cybercrime.gov.in` पर Online शिकायत दर्ज करें। Police ऐसे मामलों में पूरी मदद करती है।

अध्याय 10: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• परिवार के साथ एक **Family Secret Code** तय करें, जो केवल घर वालों को पता हो।

• अनजान Video Call आने पर कभी न उठाएँ; गलती से उठे तो Camera पर तुरंत उँगली रख दें।

• किसी अपने की Emergency Call आने पर हमेशा उसके पुराने असली Number पर Call करके सच्चाई जानें।

❌ यह कभी न करें (DONTs)

• डर या हड़बड़ी में आकर बिना सोचे-समझे किसी अनजान खाते में पैसे न भेजें।

• Blackmail होने पर डरकर कभी पैसे Transfer न करें।

• अपनी निजी Photos या Videos किसी अनजान व्यक्ति के साथ Chat पर Share न करें।

Official सत्यापन स्रोत

• 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`

अध्याय 11 • EMERGENCY कदम और शिकायत

Scam हो जाए तो क्या करें और Complaint कैसे करें

शुरुआती Golden 2 Hours का महत्व, 4 तुरंत कदम, और पैसा वापस पाने की सही सरकारी तरीका।

ठगी हो जाए तो शांत रहें: पहले 2 घंटे सबसे कीमती हैं!

अगर कभी हड़बड़ी में आपसे कोई गलत Link Click हो गया, या किसी धोखेबाज़ के खाते में पैसे Transfer हो गए, तो सबसे पहले खुद को शांत रखें। किसी भी इंसान से धोखे में गलती हो सकती है।

इस समय सबसे बड़ा हथियार है: **तेज़ी (Speed)**। Cyber Safety में घटना के तुरंत बाद के समय को **"Golden 2 Hours"** कहा जाता है।

सुनहरा नियम

Golden 2 Hours में पैसा कैसे बचता है?

जब आप तुरंत शिकायत दर्ज कराते हैं, तो भारतीय गृह मंत्रालय का System (CFCFRMS) उस पैसे को Scammer के Bank खाते या Wallet से आगे निकलने से पहले ही **Freeze (होल्ड)** करवा देता है।

सीधी बात: जितनी जल्दी शिकायत दर्ज होगी, आपका पैसा वापस सुरक्षित मिलने की संभावना उतनी ही ज़्यादा होगी!

पैसे कटते ही उठाने वाले 4 तुरंत उठाए जाने वाले कदम

1 **Chat या सबूत कभी Delete न करें**
डर या गुस्से में आकर Chat Clear न करें। Scammer के Messages, Phone Number, UPI ID और Bank SMS के **Screenshots** तुरंत ले लें।

↓ Bank को Alert करें

2 **अपने Bank को तुरंत सूचित करें**
अपने ATM Card के पीछे लिखे Official Customer Care पर Call करें। उस Transaction को Fraud घोषित करवाएँ और Net Banking / UPI को तुरंत Block करवाएँ।

↓ सरकारी Portal पर शिकायत

3 **National Cyber Crime Portal पर शिकायत दर्ज करें**
सीधे सरकारी Portal `cybercrime.gov.in` पर जाएँ। "Report Cyber Crime" विकल्प चुनकर पूरी घटना और Transaction ID दर्ज करें।

↓ WhatsApp पर Report

4 **WhatsApp In-App Report करें**
Scammer की Chat खोलें ➔ ऊपर **3 बिंदु (⋮)** दबाएँ ➔ **More** ➔ **Report** दबाएँ। इससे WhatsApp उस Account को स्थायी रूप से बंद कर देता है।

Complaint के लिए क्या-क्या सबूत चाहिए?

शिकायत दर्ज करते समय आपके पास ये 4 चीज़ें तैयार होनी चाहिए:



1. 12-Digit UTR / Transaction ID

आपके Bank SMS या UPI App (PhonePe, GPay, Paytm) की रसीद में दिखने वाला 12 अंकों का Reference Number।



2. WhatsApp Chat Screenshots

बातचीत की पूरी Screen Photos, जिसमें Scammer के वादे, धमकियाँ या भेजे गए Links साफ़ दिख रहे हों।



3. Scammer की UPI ID व Number

जिस Phone Number या UPI ID पर पैसे भेजे गए, उसका साफ़-साफ़ विवरण।



4. Bank Account Statement

Bank Passbook या Net Banking से निकाला गया वह पन्ना जहाँ से पैसा कटा हुआ दिख रहा हो।

सावधान: "पैसे वापस दिला दूँगा" कहने वाले Fake Recovery Scam

नया धोखा

Fake Instagram Hackers से बचें

जब लोग Social Media पर लिखते हैं कि उनके साथ Fraud हो गया, तो कई Fake Accounts Comment करते हैं: *"इस Instagram Expert से संपर्क करो, इसने 1 घंटे में मेरे पैसे वापस दिला दिए।"*

कड़वा सच: यह Scammers का दूसरा गिरोह होता है जो पीड़ित लोगों से "Processing Fee" के नाम पर और पैसे ऐंठ लेता है। भारत में पैसे वापस दिलाने का अधिकार केवल **आपके Bank, Police और Cyber Crime Portal** के पास है, किसी Private व्यक्ति के पास नहीं!

अध्याय 11: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

- पैसे कटते ही पहले 2 घंटे के अंदर तुरंत शिकायत दर्ज करवाएँ।
- UTR Number और Bank SMS सुरक्षित रखें।
- Fraud Number की Report **Chakshu Portal** (`sancharsaathi.gov.in`) पर भी करें।

❌ यह कभी न करें (DONTs)

- शर्म या डर के मारे चुप न बैठें, तुरंत अपनों और Bank को बताएँ।
- Scammer के साथ हुई WhatsApp Chat कभी Delete न करें।
- पैसा वापस दिलाने का दावा करने वाले किसी अनजान Hacker को 1 रुपया भी न दें।

Official शिकायत व सहायता स्रोत

- 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`

अध्याय 12 • अंतिम अध्याय (MASTER POCKET REFERENCE)

WhatsApp Safety Checklist

रोज़मर्रा के उपयोग के लिए एक पन्ने का सम्पूर्ण Safety Card। अपने Phone में Save रखें, Print करें या परिवार और दोस्तों के साथ Share करें।

आपकी जेब में पूरी WhatsApp Safety Card

WhatsApp आज हमारे परिवार, दोस्तों और काम-काज से जुड़ा सबसे बड़ा साधन है। लेकिन एक छोटी सी चूक ज़िंदगी भर की बचत पर भारी पड़ सकती है।

इस अंतिम अध्याय में पूरी eBook के 11 अध्यायों के सबसे बहुत ज़रूरी नियमों को **4 रंगीन Safety Cards** में संजोया गया है। जब भी मन में कोई शक हो, बस इस एक Checklist को खोलकर देख लें।

1 WhatsApp Account Settings Checklist

आज ही यह 5 Settings अपने Phone में Check करें

✓ **Two-Step Verification चालू रखें:**
Settings ➔ Account ➔ Two-step verification में जाकर 6-Digit PIN चालू करें। इससे कोई भी आपका WhatsApp चुरा नहीं पाएगा।

✓ **Linked Devices की नियमित जाँच:**

Settings ➔ Linked Devices में देखें। अगर कोई अनजान Web Browser या Computer दिखे, तो तुरंत **Log out** दबाएँ।

✓ **Group Privacy को "My Contacts" पर सेट करें:**
Settings ➔ Privacy ➔ Groups में जाकर **My Contacts** चुनें, ताकि कोई अनजान व्यक्ति आपको Fake Group में न जोड़ सके।

✓ **"Silence unknown callers" चालू रखें:**
Settings ➔ Privacy ➔ Calls में जाएँ और इसे चालू करें, ताकि अनजान विदेशी Calls खुद ब खुद शांत रहें।

✓ **Profile Photo केवल Contacts को दिखाएँ:**
Settings ➔ Privacy ➔ Profile photo में "My Contacts" चुनें ताकि कोई अनजान आपकी DP न चुरा सके।

2 ये 6 गलतियाँ कभी न करें (Red Flags Checklist)

इन 6 गलतियों से 95% से अधिक Cyber Fraud होते हैं

✗ **6-Digit SMS Code कभी किसी को न बताएँ:**
सगे भाई या पक्के दोस्त के कहने पर भी अपना WhatsApp Registration SMS Code कभी Share न करें।

✗ **पैसे लेने के लिए कभी QR Code Scan न करें:**

याद रखें: PIN हमेशा पैसे भेजने के लिए होता है। पैसे लेने के लिए कभी भी अपना UPI PIN न डालें।

- **अनजान .APK Files कभी Install न करें:**
  Wedding_Card.apk या Bijli_Bill.apk जैसे नाम वाली Files खतरनाक Spyware होती हैं। इन्हें भूलकर भी न खोलें।
- **Like करके पैसे कमाने वाली Fake Jobs से बचें:**
  YouTube Video Like करने या Hotel Review देने के नाम पर कोई भी असली कंपनी पैसे नहीं देती।
- **Guaranteed Return वाले Stock Groups पर भरोसा न करें:**
  शेयर बाज़ार में पक्के मुनाफ़े का वादा करने वाले सभी WhatsApp Groups 100% Fake होते हैं।
- **अनजान International Video Calls कभी न उठाएँ:**
  विदेशी Country Codes (+84, +62 आदि) से आने वाले Video Calls Video Blackmail का फंदा होते हैं।

3 10-Second का Verification Test (Verification Card)

जब भी किसी अपने के नाम से पैसों की माँग आए

- **पुराने असली Number पर सीधे Phone Call करें:**
  नया Number बताकर पैसे माँगे जाएँ, तो कभी WhatsApp Call न करें, सीधे सामान्य SIM Call करके बात करें।
- **10 सेकंड का Voice Note माँगें:**

सामने वाले से कहें: "भाई, 10 सेकंड का Voice Note भेजकर मेरा नाम बोलो।" Scammer कभी आपका नाम नहीं बोल पाएगा।

✓ **UPI ID पर नाम का मिलान करें:**
अगर दोस्त का नाम 'रोहित' है लेकिन UPI में किसी Enterprise या अनजान व्यक्ति का नाम दिख रहा है, तो 1 रुपया भी न भेजें।

✓ **Family Secret Code का उपयोग करें:**
घर में एक ऐसा Secret Code तय रखें जो केवल आपके परिवार के सदस्यों को पता हो। AI Voice Scam से बचने का यह सबसे अचूक उपाय है।

4 Emergency Action Checklist (अगर Fraud हो जाए)

पैसे कटने पर शुरुआती Golden 2 Hours में यह करें

! **Chat और Screenshots सुरक्षित रखें:**
डर या गुस्से में Chat Delete न करें। Scammer का Number, UPI ID और Bank SMS के Screenshots ले लें।

! **12 अंकों का UTR / Transaction ID नोट करें:**
पैसे कटने के SMS या Bank Passbook में दर्ज 12 अंकों का Reference Number निकालें।

! **Bank के Official Customer Care पर सूचित करें:**
ATM Card के पीछे लिखे Number पर Call करें और उस Transaction को Fraud घोषित करवाकर Net Banking सुरक्षित करें।

! **National Cyber Crime Portal पर शिकायत करें:**
2 घंटे के भीतर सरकारी Website `cybercrime.gov.in` पर जाकर Online Complaint दर्ज करवाएँ।

! **Chakshu Portal पर Fraud Number Report करें:**
सरकारी Portal `sancharsaathi.gov.in` पर जाकर Scammer का Number और Links दर्ज करें।

🎉 बधाई!

आपने Book 1: WhatsApp Scam से कैसे बचें पूरी पढ़ ली है

अब आपके पास WhatsApp पर सुरक्षित रहने का पूरी ज्ञान है। यह जानकारी अपने माता-पिता, बुज़ुर्गों और दोस्तों के साथ ज़रूर Share करें, ताकि कोई भी Cyber ठग आपके अपनों की गाढ़ी कमाई न लूट सके।

🤝 **हमारा संकल्प:** "मैं न कभी बिना सोचे अनजान Link खोलूँगा, न पैसे लेने के लिए PIN डालूँगा, और न ही किसी को अपना OTP बताऊँगा।"

📚 मुख्य सूची (Table of Contents) पर वापस जाएँ

Official सत्यापन व शिकायत स्रोत

- 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`

परिशिष्ट • APPENDIX

साइबर सुरक्षा शब्दकोश (Glossary)

Registration Code (OTP)
WhatsApp चालू करने के लिए SMS से आने वाला 6-अंकों का गुप्त कोड, जिसे बताने पर आपका Account दूसरे फोन में Transfer हो जाता है।

Two-Step Verification (2FA)
सुरक्षा की दोहरी दीवार — 6 अंकों का गुप्त PIN जो आप खुद तय करते हैं। इसके बिना कोई भी आपका WhatsApp हैक नहीं कर सकता।

APK File
Android Application Package — Play Store के बाहर से आने वाली फ़ाइल। शादी का कार्ड या चालान के नाम से आई APK फ़ाइल सीधा वायरस होती है।

Linked Devices
WhatsApp Web का फ़ीचर। इसमें समय-समय पर Check करें कि कोई अनजान Computer या Browser आपके Messages तो नहीं पढ़ रहा।

End-to-End Encryption
मैसेज की सुरक्षा का ताला — रास्ते में कोई तीसरा व्यक्ति चैट नहीं पढ़ सकता। लेकिन फोन में वायरस आने पर स्क्रीन लाइव देखी जा सकती है।

AI Voice Cloning
आर्टिफिशियल इंटेलिजेंस से अपनों की हूबहू आवाज़ बनाकर मुसीबत का बहाना बनाकर पैसे माँगने की आधुनिक ठगी।

Mule Account

किराये का बैंक खाता — जिसे ठग कमीशन देकर किसी के नाम पर खुलवाते हैं और चुराया गया पैसा घुमाने के लिए इस्तेमाल करते हैं।

Chakshu Portal

Telecom Department का आधिकारिक पोर्टल जहाँ संदिग्ध WhatsApp Fraud Numbers और फ़र्ज़ी SMS की रिपोर्ट सीधे दर्ज होती है।

Golden 2 Hours

पैसे कटने के तुरंत बाद के शुरुआती 2 घंटे, जब तुरंत cybercrime.gov.in पर शिकायत करने से ठग का बैंक खाता तुरंत Freeze हो सकता है।

Spoof DP / Impersonation

इंटरनेट या सोशल मीडिया से आपके बॉस या रिश्तेदार की फ़ोटो चुराकर अनजान नंबर पर लगाकर पैसे माँगने का फ्रॉड।

💡 किसी भी तकनीकी शब्द पर संदेह होने पर इस शब्दकोश को संदर्भ के रूप में देखें।

★ FINAL SECURITY RULES

WhatsApp सुरक्षा के 4 सुनहरे नियम

1. **Code कभी Share न करें:** 6-Digit WhatsApp Registration Code किसी दोस्त या रिश्तेदार के माँगने पर भी कभी न भेजें।
2. **पैसे पाने के लिए PIN नहीं:** WhatsApp या UPI पर पैसे Receive करने के लिए कभी भी QR Scan या PIN डालने की ज़रूरत नहीं होती।
3. **अनजान File कभी Install न करें:** Chat में आई शादी का कार्ड, चालान या बिजली बिल के नाम वाली .apk फ़ाइल सीधे वायरस होती है।
4. **आवाज़ और पहचान जाँचे बिना पैसे न दें:** DP देखकर भरोसा न करें। पैसे माँगने वाले को पुराने नंबर पर सामान्य Call करके पहले बात करें।

✓ 12 विस्तृत अध्याय ✓ Real-Life Case Studies

✓ DoT व Cyber Portal Verified ✓ Master Pocket Card

🤝 सुरक्षित डिजिटल भारत का संकल्प

सावधानी ही सबसे बड़ा बचाव है। जब आप सुरक्षित रहते हैं, तो आप अपने परिवार और पूरे समाज को साइबर अपराध से बचाते हैं।

Safe WhatsApp • Safe Family • Safe India

2026 Edition • जनहित में स्वतंत्र रूप से प्रकाशित