RBI, NPCI व सरकारी नियमों पर आधारित

नवीनतम 2026 संस्करण

UPI Safety Guide

आम लोगों के लिए Fake UPI Request, QR Code और PIN Fraud से बचने की पूरी और आसान Pocket Guide

13	100%	4
विस्तृत अध्याय	सत्यापित नियम	पॉकेट चेकलिस्ट

सुरक्षित डिजिटल भुगतान • सजग नागरिक • सशक्त भारत

कानूनी सूचना • LEGAL NOTICE

कानूनी बातें और इस्तेमाल के नियम

1. जन-जागरूकता उद्देश्य

यह eBook केवल आम नागरिकों और दुकानदारों में Digital Payment की समझ और Cyber Safety जागरूकता बढ़ाने के उद्देश्य से तैयार की गई एक स्वतंत्र Guide है। इसका उद्देश्य सुरक्षित Payment के तौर-तरीके सिखाना है। यह कोई कानूनी (Legal) या Financial सलाह नहीं है।

2. किसी भी संस्था से कोई संबंध नहीं

यह eBook Reserve Bank of India (RBI), NPCI, भारत सरकार, किसी भी Bank अथवा UPI Payment App (जैसे PhonePe, Google Pay, Paytm) द्वारा प्रायोजित, समर्थित या Approved नहीं है। यह एक स्वतंत्र Digital Guide है।

3. ज़िम्मेदारी की सीमा (Limitation of Liability)

UPI और Banking सुरक्षा 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 पैसे के नुकसान के लिए यह eBook या इसके लेखक किसी भी रूप में ज़िम्मेदार नहीं होंगे। ताज़ा जानकारी के लिए हमेशा संबंधित Bank की Official Website या शाखा से संपर्क करें।

4. Trademarks और Brand Names

'UPI', 'BHIM', और 'NPCI' NPCI के पंजीकृत Trademarks हैं। पुस्तक में उल्लिखित अन्य सभी नाम (जैसे Google Pay, PhonePe, Paytm, HDFC, SBI आदि) उनके संबंधित मालिकों की संपत्ति हैं। इनका उपयोग केवल पहचान, जन-जागरूकता 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, दुकान, 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% RBI व NPCI के सार्वजनिक नियमों पर आधारित स्वतंत्र Guide

संपादकीय • EDITORIAL PREFACE

प्रस्तावना: यह गाइड आपके लिए क्यों आवश्यक है?

आज भारत में प्रतिदिन 40 करोड़ से अधिक UPI लेनदेन होते हैं। सब्जी के ठेले से लेकर बड़े शॉपिंग मॉल तक, UPI ने हमारे जीवन को बेहद आसान, तेज और कैशलेस बना दिया है।

लेकिन सुविधा का यह विशाल पहिया अपने साथ साइबर अपराध की नई चुनौतियां भी लेकर आया है। हर दिन अखबारों और टीवी में हम पढ़ते हैं कि किसी सेवानिवृत्त बुजुर्ग की जीवन भर की जमा पूंजी एक लिंक पर क्लिक करते ही साफ हो गई, या किसी युवा के साथ नौकरी और कैशबैक के नाम पर हजारों की ठगी हो गई।

> **साइबर ठग कभी बैंक के कंप्यूटर सर्वर को हैक नहीं करते, वे इंसानी मनोविज्ञान (Human Psychology) को हैक करते हैं — हमारे लालच, घबराहट और जल्दबाजी का फायदा उठाकर हमसे खुद हमारा पासवर्ड या PIN डलवाते हैं।**

अधिकांश ठगी केवल इसलिए सफल हो पाती है क्योंकि आम नागरिकों को UPI के 2-3 बुनियादी नियमों की स्पष्ट जानकारी नहीं होती। सबसे बड़ा नियम आज भी लाखों लोगों को नहीं पता: *"पैसे पाने के लिए कभी PIN या OTP की आवश्यकता नहीं होती।"*

इस ई-बुक का उद्देश्य:

यह ई-बुक जटिल तकनीकी भाषा में नहीं, बल्कि **साधारण बोलचाल की हिंदी** में लिखी गई है। इसमें 13 अध्यायों के माध्यम से वास्तविक केस स्टडीज, वास्तविक स्क्रीनशॉट्स और रिज़र्व बैंक (RBI) व NPCI के प्रमाणित नियमों के जरिए आपको डिजिटल रूप से आत्मनिर्भर और अभेद्य बनाना ही इसका एकमात्र लक्ष्य है।

इस गाइड को स्वयं पढ़ें, अपने माता-पिता, बुजुर्गों और बच्चों के साथ साझा करें। आपकी 10 सेकंड की सतर्कता आपकी जीवन भर की गाढ़ी कमाई की सबसे बड़ी रक्षक है।

विषय सूची • TABLE OF CONTENTS

अध्यायों की विस्तृत सूची

1 **अध्याय 1: UPI को समझना**
UPI क्या है, 2FA सुरक्षा चक्र और पैसे ट्रांसफर होने की प्रक्रिया

2 **अध्याय 2: UPI और आपका Bank**
RBI Zero Liability नियम, 3 दिन की समय-सीमा और ग्राहक अधिकार

3 **अध्याय 3: UPI PIN की सुरक्षा**
स्वर्णिम नियम: पैसे पाने के लिए कभी PIN नहीं लगता, सुरक्षित रीसेट

4 **अध्याय 4: Payment करने से पहले**
10 सेकंड का सुरक्षा विराम, CBS सत्यापित नाम और भौतिक QR जांच

5 **अध्याय 5: UPI के आम Scams**
Collect Request, फर्जी रिफंड और AnyDesk स्क्रीन शेयरिंग के जाल

6 **अध्याय 6: दुकान, घर और रोज़ की ठगी**
बदले हुए QR कोड, फर्जी कूरियर OTP और बिजली बिल धमकी संदेश

7 **अध्याय 7: जब Payment में समस्या आए**
T+1 ऑटो-रिवर्सल, ₹100 प्रतिदिन मुआवजा और UDIR शिकायत निवारण

8 **अध्याय 8: UPI Fraud की शिकायत कैसे करें**
गोल्डन ऑवर (2-3 घंटे), cybercrime.gov.in और 12-अंकों का UTR नंबर

9 **अध्याय 9: नकली आवाज़ और Video Call (AI)**
AI Voice Cloning, Deepfake और 'Digital Arrest' के फर्जीवाड़े का सच

10 **अध्याय 10: AI से बने नकली Screenshot और Website**
Spoof Apps, फर्जी Green Tick और 6-अक्षरों वाले बैंक SMS हेडर

11 **अध्याय 11: नकली Link और Message**
Smishing, खतरनाक .apk फाइलें और DoT चक्षु पोर्टल पर रिपोर्ट

12 **अध्याय 12: अपना Phone सुरक्षित रखें**
Device Hardening, Accessibility सर्विस जोखिम और CEIR मोबाइल ब्लॉकिंग

13 **अध्याय 13: UPI Safety Checklist**
4 मास्टर पॉकेट कार्ड्स, आधिकारिक निर्देशिका और सम्पूर्ण सुरक्षा सारांश

• **परिशिष्ट:** डिजिटल बैंकिंग पारिभाषिक शब्दकोश (Glossary) एवं अंतिम बैक कवर

अध्याय 1 • बुनियादी समझ (Basics)

UPI को समझना

UPI क्या है, पैसे एक Bank Account से दूसरे खाते में कैसे पहुंचते हैं और यह तकनीक साधारण उपयोगकर्ताओं के लिए सुरक्षित क्यों है।

UPI क्या है और इसकी शुरुआत कैसे हुई?

आज भारत के हर शहर, गाँव, नुक्कड़ की चाय की दुकान से लेकर बड़े मॉल तक हर जगह आपको काले-सफेद चौकोर **QR Code** लगे दिखते हैं। लोग जेब से फोन निकालते हैं, कैमरा खोलते हैं और कुछ ही सेकंड में बिना किसी कागजी नोट के भुगतान हो जाता है। इस पूरी क्रांति के पीछे जो तकनीक काम कर रही है, उसका नाम है **UPI**।

UPI का पूरा नाम **Unified Payments Interface** है। इसे भारत सरकार के **RBI** (Reserve Bank of India) की देखरेख में **NPCI** (National Payments Corporation of India) ने तैयार किया है।

याद कीजिए पुराना दौर

UPI से पहले पैसे भेजना कितना मुश्किल था?

UPI आने से पहले यदि आपको किसी रिश्तेदार या दुकानदार को बैंक से पैसे भेजने होते थे, तो आपको:

• सामने वाले का पूरा 16-अंकों का **Bank Account Number** मांगना पड़ता था।

• उसकी बैंक शाखा का 11-अंकों का **IFSC Code** ढूंढना पड़ता था।

• फिर अपने NetBanking ऐप में जाकर उसे **Beneficiary** के रूप में जोड़ना होता था।

• बैंक 30 मिनट से लेकर 2 घंटे तक उसे एक्टिव करने का समय लेता था।

• और रात में या रविवार के दिन बैंक बंद होने पर **NEFT** का पैसा कई घंटों तक अटका रहता था।

UPI ने इस पूरी झंझट को हमेशा के लिए खत्म कर दिया: अब न तो किसी को बैंक खाता नंबर देने की जरूरत है, न IFSC कोड की और न ही घंटों इंतजार करने की। पैसा 24 घंटे, 365 दिन, सेकंडों में सीधे बैंक खाते में ट्रांसफर हो जाता है।

केस स्टडी: शर्मा जी का पहला UPI अनुभव (व्यावहारिक उदाहरण)

58 वर्षीय रमेश शर्मा जी हमेशा नकद (Cash) में लेन-देन करते थे। वे ऑनलाइन पेमेंट को लेकर काफी डरे रहते थे कि कहीं उनका फोन कोई देख ले तो उनका पूरा बैंक खाता खाली न हो जाए।

> **शर्मा जी:** "बेटा प्रिया, अगर मैं सब्जी वाले को अपना मोबाइल नंबर या UPI ID दे दूँ, तो क्या वह मेरे खाते से पैसे निकाल सकता है?"

> **बेटी प्रिया:** "पापा, बिल्कुल नहीं! UPI ID या फोन नंबर केवल आपका पता (Address) है, चाबी नहीं। जैसे किसी को घर का पता देने से वह घर का ताला नहीं खोल सकता, वैसे ही UPI ID जानने से कोई आपके पैसे नहीं निकाल सकता। पैसे निकालने के लिए आपका गुप्त **UPI PIN** चाहिए, जो केवल आपके दिमाग में होता है।"

> **शर्मा जी:** "और अगर मेरा फोन कहीं गिर गया तो?"

> **बेटी प्रिया:** "फोन गिर भी जाए तो भी कोई कुछ नहीं कर सकता, क्योंकि पहले तो आपके फोन पर **Screen Lock** है, और ऐप खोलने के बाद भी पैसे भेजने के लिए आपका **UPI PIN** चाहिए। साथ ही, UPI आपके सिम कार्ड से बंधा होता है।"

शर्मा जी ने उस दिन पहली बार ₹120 की सब्जी का UPI पेमेंट किया। जैसे ही सब्जी वाले के **Soundbox** से आवाज आई — *"Paytm पर 120 रुपये प्राप्त हुए"*, शर्मा जी के चेहरे पर विश्वास और सुकून की मुस्कान आ गई।

पैसे कैसे ट्रांसफर होते हैं? (Behind the Scenes)

अक्सर लोगों के मन में यह गलतफहमी होती है कि उनका पैसा Google Pay, PhonePe या Paytm जैसी कंपनियों के पास जमा रहता है। **यह**

बिल्कुल गलत है।

UPI कोई ई-वॉलेट (Wallet) नहीं है। UPI केवल एक सुरक्षित डिजिटल पाइपलाइन है। आपका पैसा हमेशा आपके अपने **Bank Account** में ही रहता है। जब आप पेमेंट करते हैं, तो पैसा एक बैंक से निकलकर सीधे दूसरे बैंक में जाता है।

कदम 1

आपने QR Code स्कैन किया या UPI ID डाला

आपके फोन का **UPI App** (जैसे BHIM, PhonePe, Google Pay) सामने वाले के बैंक का पता पहचान लेता है।

↓ सुरक्षित एन्क्रिप्शन

कदम 2

आपने अपना गुप्त UPI PIN दर्ज किया

यह PIN आपके फोन से सीधे एक सुरक्षित कोड में बदलकर आपके बैंक को भेजा जाता है। इसे ऐप कंपनी भी नहीं देख सकती।

↓ NPCI स्विच

कदम 3

NPCI नेटवर्क ने दोनों बैंकों को जोड़ा

भारत सरकार का **NPCI** सिस्टम आपके बैंक को पैसे काटने (Debit) और सामने वाले के बैंक को पैसे जोड़ने (Credit) का सुरक्षित निर्देश देता है।

↓ रियल-टाइम सेटलमेंट

कदम 4

पैसा तुरंत खाते में जमा और पुष्टि

सामने वाले के खाते में पैसे जुड़ जाते हैं, दोनों पक्षों को बैंक से SMS आता है और दुकान पर लगे **Soundbox** से आवाज आ जाती है।

UPI ID (VPA) और QR Code क्या होते हैं?



UPI ID (VPA - Virtual Payment Address)

यह आपके बैंक खाते का एक उपनाम (Nick Name) या ईमेल जैसा पता होता है। उदाहरण के लिए: `ramesh@oksbi` या `username@ybl` ।

> **फायदा:** सामने वाले को आपका खाता नंबर नहीं दिखता, जिससे आपकी बैंकिंग प्राइवेसी 100% सुरक्षित रहती है।

📷

QR Code (Quick Response Code)

QR Code कुछ और नहीं, बल्कि UPI ID और बैंक विवरण का एक मशीन द्वारा पढ़ी जाने वाली तस्वीर (चित्र) होता है।

> **फायदा:** आपको 10 अंकों का फोन नंबर या लंबी UPI ID टाइप करने की जरूरत नहीं होती। कैमरा खोलकर स्कैन करते ही सही पता अपने आप आ जाता है।

UPI की सुरक्षा के दो मजबूत ताले (Two-Factor Authentication)

भारतीय रिज़र्व बैंक (RBI) के नियमों के अनुसार, UPI को इस तरह बनाया गया है कि कोई भी धोखेबाज केवल दूर बैठकर आपके खाते से पैसे नहीं निकाल सकता। इसके लिए दो तालों का एक साथ खुलना जरूरी है:

पहला ताला (Something You Have)

आपका फोन और रजिस्टर्ड SIM कार्ड

जब आप पहली बार किसी फोन में UPI ऐप चालू करते हैं, तो ऐप आपके फोन में लगे SIM कार्ड से बैंक को एक गुप्त SMS भेजता है। इसे **Device Binding** कहते हैं।

यदि कोई धोखेबाज अपने कंप्यूटर या दूसरे फोन में आपका नंबर डालकर ऐप चालू करना चाहे, तो वह कभी नहीं कर पाएगा क्योंकि असली सिम कार्ड आपके फोन के अंदर मौजूद है।

दूसरा ताला (Something You Know)

आपका गोपनीय UPI PIN

पैसे भेजने के लिए हर बार 4 या 6 अंकों का UPI PIN डालना अनिवार्य है। यह PIN कभी किसी सर्वर पर सादे अक्षरों में सेव नहीं होता। यह सिर्फ आपके दिमाग में रहता है।

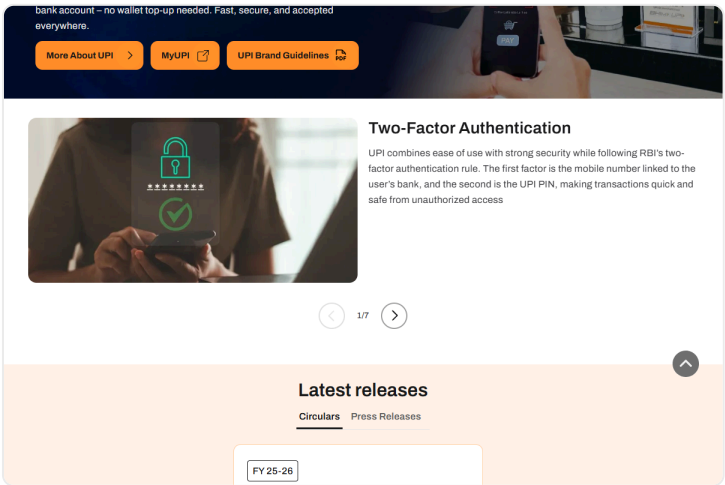
जब तक आप खुद अपनी उंगलियों से यह PIN नहीं डालते, दुनिया की कोई भी ताकत आपके बैंक खाते से एक भी रुपया नहीं काट सकती।

आधिकारिक पोर्टल पर UPI की जानकारी

भारत में UPI का संचालन करने वाली संस्था **NPCI** अपनी आधिकारिक वेबसाइट पर आम नागरिकों के लिए UPI की पूरी जानकारी उपलब्ध कराती है:

npci.org.in/product/upi

आधिकारिक स्रोत



📌 NPCI पोर्टल के आधिकारिक पेज से 2 जरूरी बातें:

1. **आधिकारिक डोमेन की जांच:** हमेशा ब्राउज़र में देखें कि वेबसाइट का पता `npci.org.in` है या नहीं। सरकारी व आधिकारिक संस्थाओं के अंत में `.org.in` या `.gov.in` होता है।

2. **Two-Factor Authentication का नियम:** NPCI ने स्पष्ट लिखा है कि सिम कार्ड और UPI PIN का दोहरा सुरक्षा चक्र हर नागरिक के पैसे को सुरक्षित रखता है।

अध्याय 1: बुनियादी UPI से जुड़े महत्वपूर्ण सवाल

(Basics FAQs)

Q1: क्या किसी को अपनी UPI ID या फोन नंबर बताने से खाता खाली हो सकता है?

उत्तर: बिल्कुल नहीं। UPI ID या मोबाइल नंबर केवल पैसे प्राप्त करने का पता है। जब तक आप किसी को अपना UPI PIN या OTP नहीं बताते, तब तक कोई भी व्यक्ति आपके खाते से पैसे नहीं निकाल सकता।

Q2: क्या UPI इस्तेमाल करने के लिए Debit Card (ATM कार्ड) होना जरूरी है?

उत्तर: पहली बार UPI PIN सेट करने के लिए Debit Card की जरूरत होती है। लेकिन अब NPCI ने **Aadhaar OTP** के जरिए भी UPI PIN सेट करने की सुविधा शुरू कर दी है, जिससे बिना ATM कार्ड वाले लोग भी आधार से UPI चला सकते हैं।

Q3: Google Pay, PhonePe और Bank App में क्या अंतर है?

उत्तर: ये सभी थर्ड-पार्टी ऐप्स (TPAP) हैं। ये सिर्फ आपके बैंक खाते तक पहुँचने का एक सुंदर जरिया हैं। आपका पैसा इन कंपनियों के पास नहीं, बल्कि आपके असली बैंक (जैसे SBI, PNB, HDFC) में सुरक्षित रहता है।

Q4: क्या किसी को अपनी UPI ID या मोबाइल नंबर देने से बैंक खाते से पैसे कट सकते हैं?

उत्तर: बिल्कुल नहीं। अपनी UPI ID (जैसे `name@okhdfcbank`) या मोबाइल नंबर किसी को देना पूरी तरह सुरक्षित है। यह केवल पैसे पाने का एक डिजिटल पता है। आपके बैंक खाते से पैसे केवल और केवल तब कट सकते हैं जब आप खुद अपने फोन पर अपना 4 या 6 अंकों का गुप्त **UPI PIN** दर्ज करें। बिना PIN डाले दुनिया का कोई भी व्यक्ति आपके खाते से एक रुपया भी नहीं निकाल सकता।

Q5: क्या UPI से पैसे भेजने की कोई दैनिक सीमा (Daily Limit) होती है?

उत्तर: हाँ। NPCI के नियमों के अनुसार साधारण व्यक्ति प्रति दिन अधिकतम ₹1,00,000 (एक लाख रुपये) तक भेज सकता है। कुछ बैंकों और नए खातों के लिए पहले 24 घंटे में यह सीमा ₹5,000 से ₹25,000 तक रखी जाती है ताकि कोई बड़ा नुकसान न हो सके।

UPI इस्तेमाल में क्या करें और क्या न करें (Dos and Don'ts)

✅ क्या करें (Do's)

- हमेशा बैंक में रजिस्टर्ड सिम कार्ड को फोन के सिम स्लॉट-1 में रखें।
- पेमेंट करने से पहले स्क्रीन पर दिखने वाले नाम की दोबारा जांच करें।

• केवल Google Play Store या Apple App Store से ही आधिकारिक UPI ऐप डाउनलोड करें।

• बैंक से आने वाले हर SMS को ध्यान से पढ़ें कि उसमें डेबिट (पैसे कटना) लिखा है या क्रेडिट (पैसे आना)।

❌ क्या न करें (Don'ts)

• पैसे पाने (Receive करने) के लिए कभी भी UPI PIN दर्ज न करें।

• अपना UPI PIN किसी डायरी, फोन के बैक-कवर या सोशल मीडिया पर न लिखें।

• किसी अनजान व्यक्ति के कहने पर अपने फोन में AnyDesk या TeamViewer जैसे ऐप न डालें।

• किसी को भी फोन पर बैंक का OTP या कार्ड का CVV नंबर न बताएं।

Google पर UPI की सही आधिकारिक जानकारी कैसे खोजें? (Safe Search Guide)

जब भी आपको NPCI या UPI के बारे में आधिकारिक जानकारी लेनी हो, तो Google पर सर्च करते समय इन 4 सावधानियों का पालन करें:

1

चरण 1: सटीक Google Search Keyword टाइप करें

सर्च बार में केवल यह लिखें: `NPCI official UPI product overview`

2

चरण 2: "Sponsored" या "Ad" लिखे लिंक को छोड़ दें

सर्च रिजल्ट में सबसे ऊपर अगर किसी लिंक के आगे **Sponsored** या **Ad** लिखा हो, तो उस पर क्लिक न करें। ठग अक्सर पैसे देकर अपने फर्जी लिंक ऊपर लगवाते हैं।

3

चरण 3: वेबसाइट के डोमेन पते (URL) की जांच करें

हमेशा देखें कि नीले लिंक के नीचे छोटा पता `https://www.npci.org.in` लिखा है या नहीं। अगर किसी पते में `.xyz`, `.online` या `free-pay` जैसा कुछ दिखे, तो उसे न खोलें।

4

चरण 4: फोन नंबर पर सीधे कॉल न करें

Google सर्च पेज पर दिखने वाले किसी भी अनजान मोबाइल या टोल-फ्री नंबर पर सीधे कॉल न लगाएं। हमेशा आधिकारिक वेबसाइट के भीतर दिए गए "Contact Us" पेज से ही नंबर लें।

🔍 अध्याय 1 के सत्यापित आधिकारिक स्रोत (Official Sources):

- **NPCI आधिकारिक UPI ओवरव्यू:** `https://www.npci.org.in/product/upi`
- **RBI डिजिटल भुगतान सुरक्षा फ्रेमवर्क:** `https://www.rbi.org.in`
- **BHIM UPI आधिकारिक पोर्टल:** `https://www.bhimupi.org.in`

अध्याय 2 • खाता और सुरक्षा (Bank & User Role)

UPI और आपका Bank

Bank Account से UPI का क्या रिश्ता है, आपकी क्या जिम्मेदारी है और RBI के 3-दिन के Zero Liability नियम के तहत पैसे वापस पाने का आपका कानूनी अधिकार क्या है।

Bank Account और UPI App का असली रिश्ता

कई लोगों के मन में यह भ्रम रहता है कि PhonePe, Google Pay या Paytm जैसे **UPI Apps** कोई बैंक हैं, जहाँ उनके पैसे रखे होते हैं। **यह बिल्कुल सच नहीं है।**

असली सच्चाई यह है कि आपका पैसा 100% आपके अपने **Bank Account** (जैसे SBI, PNB, Bank of Baroda, HDFC) में सुरक्षित रहता है। UPI App केवल आपके फोन पर लगी एक डिजिटल खिड़की (Window) है, जो आपको बैंक जाए बिना लेन-देन करने की सुविधा देती है।

आसान समझ

UPI ID और Bank Account का उदाहरण

मान लीजिए आपका बैंक खाता आपके घर की तरह है और **UPI ID** (जैसे `ramesh@oksbi`) आपके घर के बाहर लगा नेमप्लेट या लेटरबॉक्स है।

• जब कोई आपकी UPI ID पर पैसे भेजता है, तो वे सीधे आपके **Bank Account** में क्रेडिट (जमा) होते हैं।

• जब आप किसी को पैसे भेजते हैं, तो वे सीधे आपके **Bank Account** से डेबिट (कटते) हैं।

• किसी को अपनी UPI ID देने पर उसे आपका 16-अंकों का खाता नंबर या IFSC कोड नहीं दिखता, जिससे आपकी बैंकिंग सुरक्षा बनी रहती है।

केस स्टडी: सुनील का खोया फोन और 3-दिन का सुरक्षा नियम

सुनील एक प्राइवेट कंपनी में काम करते हैं। एक शाम ऑफिस से घर लौटते समय बस में उनका फोन चोरी हो गया। घर पहुँचकर जब उन्होंने पत्नी के फोन से अपना बैंक बैलेंस चेक किया, तो उनके होश उड़ गए — उनके बैंक खाते से ₹25,000 कट चुके थे।

सुनील ने क्या कदम उठाए?

उसी शाम

सुनील ने बिना घबराए तुरंत अपने बैंक की आधिकारिक शाखा/कस्टमर केयर को सूचना दी और अपना **UPI व**

NetBanking ब्लॉक करवाया।

अगली सुबह

सुनील ने बैंक जाकर लिखित में **Unauthorized Transaction** की शिकायत दर्ज कराई और **Complaint Reference Number** लिया।

7 दिन बाद

चूंकि सुनील ने किसी के साथ अपना **UPI PIN** या **OTP** शेयर नहीं किया था और बैंक को **3 दिन के भीतर** सूचित कर दिया था, इसलिए **RBI के Zero Liability नियम** के तहत बैंक ने उनके पूरे ₹25,000 खाते में वापस (Refund) जमा कर दिए!

सीख: अगर कभी बिना आपकी गलती के खाते से पैसे कट जाएं, तो रोने या समय गंवाने के बजाय तुरंत बैंक को सूचित करना ही पैसे वापस पाने की सबसे बड़ी कुंजी है।

RBI का 3-दिन का Zero Liability नियम: आपके पैसे की कानूनी सुरक्षा

भारतीय रिज़र्व बैंक (RBI) ने आम जनता के हितों की रक्षा के लिए एक ऐतिहासिक सर्कुलर (*Customer Protection – Limiting Liability*

of Customers) जारी किया है। इसके अनुसार, अगर डिजिटल लेन-देन में धोखाधड़ी होती है, तो नुकसान की भरपाई इस तरह होती है:

स्लैब 1: शून्य नुकसान (Zero Liability) 3 कार्यदिवसों में सूचना

नियम: अगर बैंक के सिस्टम की गलती से पैसे कटे हैं, या किसी थर्ड-पार्टी फ्रॉड में आपका पैसा कटा है और आपने अपना PIN/OTP किसी को नहीं दिया था — और आप **3 Working Days** के भीतर बैंक को शिकायत दर्ज करा देते हैं:

🎯 **ग्राहक का नुकसान = ₹0 (शून्य)!** बैंक पूरा पैसा आपके खाते में वापस लौटाने के लिए बाध्य है।

स्लैब 2: सीमित नुकसान (Limited Liability)

4 से 7 दिनों में सूचना

नियम: अगर धोखाधड़ी की सूचना देने में आपसे 4 से 7 कार्यदिवसों की देरी हो जाती है, तो भी आपका पूरा पैसा नहीं डूबता।

⚠️ **सीमित देनदारी:** साधारण सेविंग्स बैंक खाते पर ग्राहक का अधिकतम नुकसान ₹10,000 तक सीमित रहता है। बाकी बची हुई राशि बैंक को वहन करनी होती है।

अपवाद: जब ग्राहक ने खुद PIN या OTP दिया हो

लापरवाही की स्थिति

कड़वा सच: अगर ग्राहक ने किसी अनजान कॉलर, फर्जी लॉटरी या रिफंड के लालच में आकर खुद अपना **UPI PIN** या **OTP** सामने वाले को बता दिया है:

❌ जब तक ग्राहक बैंक को सूचना देकर खाता ब्लॉक नहीं करवा देता, तब तक होने वाला सारा नुकसान ग्राहक को ही झेलना पड़ेगा। बैंक को सूचित करने के बाद होने वाले किसी भी नए नुकसान की जिम्मेदारी बैंक की होगी।

आपकी जिम्मेदारी बनाम Bank की जिम्मेदारी

सुरक्षित डिजिटल बैंकिंग के लिए दोनों पक्षों के कर्तव्य स्पष्ट रूप से तय हैं:

ग्राहक के रूप में आपकी 3 जिम्मेदारियां:

• अपना **UPI PIN**, **OTP**, पासवर्ड या कार्ड का CVV किसी के साथ साझा न करें।

• बैंक खाते में चालू मोबाइल नंबर हमेशा अपडेट रखें ताकि हर लेन-देन का **SMS Alert** तुरंत मिले।

• बैंक स्टेटमेंट की नियमित जांच करें और कोई भी अनजान कटौती दिखने पर तत्काल बैंक को सूचित करें।

Bank के 3 कानूनी कर्तव्य:

• हर पैसे के कटने (Debit) और आने (Credit) का तत्काल **SMS व Email Alert** ग्राहक को भेजना।

• अनधिकृत लेन-देन की त्वरित शिकायत दर्ज करने के लिए 24/7 टोल-फ्री चैनल, SMS व पोर्टल उपलब्ध कराना।

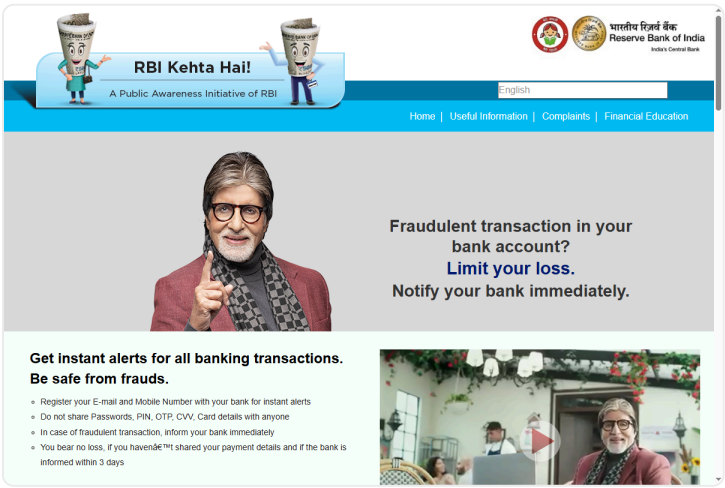
• वैध शिकायत दर्ज होने के 10 कार्यदिवसों (Working Days) के भीतर ग्राहक के खाते में प्रोविजनल क्रेडिट (पैसा) वापस करना।

RBI Kehta Hai: आधिकारिक जागरूकता पोर्टल

भारतीय रिज़र्व बैंक अपने आधिकारिक पोर्टल **'RBI Kehta Hai'** पर नागरिकों को अपने नुकसान को सीमित रखने का यह नियम साफ-साफ दिखाता है:

rbikehtahai.rbi.org.in

आधिकारिक RBI जागरूकता



📌 RBI लिमिट लॉस (Limit Loss) नियम से 2 मुख्य सीख:

1. **तुरंत बैंक को बताएं:** *"Fraudulent transaction in your bank account? Limit your loss. Notify your bank immediately."* (अनधिकृत कटौती होते ही तुरंत बैंक को सूचित करें)।

2. **3 दिन में शून्य नुकसान:** *"You bear no loss, if you haven't shared your payment details and if the bank is informed within 3 days."* (यदि आपने अपनी गोपनीय जानकारी साझा नहीं की है और 3 दिनों में बैंक को बता दिया, तो आपका कोई नुकसान नहीं होगा)।

अध्याय 2: बैंक खाते और देनदारी से जुड़े महत्वपूर्ण

सवाल (Bank Liability FAQs)

Q1: अगर बैंक में शिकायत करने के बाद भी बैंक पैसे वापस न करे तो क्या करें?

उत्तर: यदि बैंक 30 दिनों के भीतर आपकी शिकायत का संतोषजनक समाधान नहीं करता है, तो आप रिज़र्व बैंक के **Banking Ombudsman** (बैंकिंग लोकपाल) के पोर्टल `cms.rbi.org.in` पर ऑनलाइन निशुल्क शिकायत दर्ज कर सकते हैं। लोकपाल बैंक को पैसा वापस करने का आदेश दे सकता है।

Q2: क्या एक ही UPI App में एक से ज्यादा बैंक खाते जोड़े जा सकते हैं?

उत्तर: बिल्कुल हाँ। आप PhonePe, Google Pay या BHIM जैसे किसी भी ऐप में अपने कई बैंक खाते जोड़ सकते हैं। आप चुन सकते हैं कि किस खाते को **Primary Account** बनाना है, जिससे पेमेंट कटेगा।

Q3: क्या बैंक का कोई अधिकारी या कर्मचारी कभी फोन पर UPI PIN मांग सकता है?

उत्तर: कभी नहीं! RBI और सभी बैंकों का स्पष्ट आदेश है कि बैंक का कोई भी मैनेजर, अधिकारी या कस्टमर केयर एग्जीक्यूटिव कभी भी किसी ग्राहक से उसका UPI PIN, पासवर्ड, OTP या ATM पिन नहीं मांग सकता। जो भी मांगे, वह 100% धोखेबाज है।

Q4: क्या Zero Liability का नियम सरकारी और प्राइवेट दोनों बैंकों पर लागू होता है?

उत्तर: हाँ। यह नियम भारत के सभी शेड्यूल वाणिज्यिक बैंकों (जैसे SBI, PNB, HDFC, ICICI, Axis), क्षेत्रीय ग्रामीण बैंकों और सहकारी बैंकों पर समान रूप से लागू होता है।

Q5: बैंक में धोखाधड़ी की शिकायत दर्ज कराते समय मुझे क्या जानकारी देनी होगी?

उत्तर: आपको अपना खाता नंबर, पैसे कटने की तारीख और समय, कटी हुई रकम और सबसे महत्वपूर्ण — 12-अंकों का **UTR Number** (UPI Transaction Reference) देना होगा जो बैंक से आए SMS में लिखा होता है।

बैंक खाता व UPI सुरक्षा: क्या करें और क्या न करें

✅ क्या करें (Do's)

• बैंक से आने वाले हर SMS अलर्ट को तुरंत खोलकर पढ़ें।

• फोन खो जाने या चोरी होने पर उसी दिन बैंक को फोन करके UPI सेवा बंद करवाएं।

• बैंक में शिकायत दर्ज कराते ही शिकायत संख्या (Complaint Reference Number) अवश्य नोट करें।

• अपने बैंक का आधिकारिक कस्टमर केयर नंबर केवल अपनी बैंक पासबुक या चेकबुक से ही लें।

❌ क्या न करें (Don'ts)

• पैसे कटने की सूचना देने में 3 दिन से ज्यादा की देर कभी न करें।

• किसी भी स्थिति में किसी को अपना बैंक OTP या UPI PIN फोन पर न बताएं।

• Google सर्च में दिखने वाले किसी भी अनजान कस्टमर केयर नंबर पर कॉल न लगाएं।

• किसी अनजान व्यक्ति के कहने पर अपने बैंक खाते में नया मोबाइल नंबर लिंक न कराएं।

Google पर अपने बैंक की सही वेबसाइट कैसे खोजें? (Bank Portal Guide)

जब भी आपको अपने बैंक में अनधिकृत लेन-देन की रिपोर्ट करनी हो या कस्टमर केयर से संपर्क करना हो, तो Google पर इन 4 बातों का ध्यान रखें:

1

चरण 1: बैंक का नाम और आधिकारिक पोर्टल कीवर्ड लिखें

सर्च बार में अपने बैंक का नाम जोड़कर केवल यह लिखें: `[अपने बैंक का नाम] official website report unauthorized transaction`

2

चरण 2: "Sponsored" विज्ञापनों से पूरी तरह दूर रहें

सर्च रिजल्ट में सबसे ऊपर दिखने वाले विज्ञापनों पर क्लिक न करें। धोखेबाज बैंक के नाम से पैसे देकर फर्जी विज्ञापन चलवाते हैं ताकि लोग उनके नंबरों पर कॉल करें।

3

चरण 3: बैंक के आधिकारिक डोमेन पते (URL) की जांच करें

हमेशा देखें कि वेबसाइट का पता बैंक के असली नाम से मेल खाता है (जैसे SBI के लिए `onlinesbi.sbi` या `sbi.co.in`, PNB के लिए `pnbindia.in`, HDFC के लिए `hdfcbank.com`)।

4

चरण 4: Google सर्च पर दिखने वाले फोन नंबर पर कॉल न करें

कभी भी Google सर्च के परिणाम में सीधे दिख रहे किसी मोबाइल नंबर पर फोन न मिलाएं। हमेशा केवल अपनी बैंक पासबुक, डेबिट कार्ड के पीछे लिखे नंबर या बैंक की आधिकारिक वेबसाइट के भीतर दिए गए हेल्प सेक्शन का ही उपयोग करें।

🔍 अध्याय 2 के सत्यापित आधिकारिक स्रोत (Official Sources):

- **RBI ग्राहक सुरक्षा सर्कुलर (Limiting Liability of Customers):** Circular No. `DBR.No.Leg.BC.78/09.07.005/2017-18` (`https://www.rbi.org.in`)
- **RBI Kehta Hai आधिकारिक जागरूकता पोर्टल:** `https://rbikehtahai.rbi.org.in/limit-your-loss.html`

- **RBI Banking Ombudsman पोर्टल:** `https://cms.rbi.org.in`

अध्याय 3 • डिजिटल चाबी (PIN Security)

UPI PIN की सुरक्षा

UPI PIN आपके बैंक खाते की डिजिटल चाबी है। जानिए इसका सबसे बड़ा स्वर्णिम नियम, PIN बदलने का तरीका और धोखेबाजों के झूठे दावों की सच्चाई।

UPI PIN क्या है? आपके बैंक खाते की तिजोरी की चाबी

जब आप बैंक की शाखा में जाते हैं, तो पैसे निकालने के लिए चेक पर अपने हस्ताक्षर (Sign) करते हैं या ATM पर जाकर 4 अंकों का ATM PIN डालते हैं। ठीक उसी तरह, जब आप अपने मोबाइल से **UPI** के जरिए किसी को पैसे भेजते हैं, तो बैंक को यह साबित करने के लिए कि यह पेमेंट आप खुद कर रहे हैं, आपको 4 या 6 अंकों का एक गुप्त कोड डालना होता है। इसे ही **UPI PIN** (Personal Identification Number) कहते हैं।



UPI का सबसे बड़ा स्वर्णिम नियम (Golden Rule)

पैसे भेजने के लिए UPI PIN चाहिए।
पैसे पाने (Receive करने) के लिए UPI PIN कभी

नहीं चाहिए!

इस एक नियम को हमेशा के लिए अपने दिमाग में बैठा लें: जब भी कोई आपके खाते में पैसे ट्रांसफर करेगा, तो पैसा सीधे आपके **Bank Account** में आ जाएगा। आपको स्क्रीन पर कोई भी PIN या OTP दर्ज करने की 1% भी जरूरत नहीं होती।

केस स्टडी: विकास और OLX पर पुराना सोफा बेचने का किस्सा

विकास ने अपने घर का पुराना सोफा बेचने के लिए OLX पर ₹8,000 की फोटो डाली। विज्ञापन डालने के 15 मिनट के भीतर ही एक अनजान व्यक्ति का फोन आया।

धोखेबाज का पैंतरा

"भैया, मैं आर्मी कैंट से बोल रहा हूँ, सोफा तुरंत बुक करना है!"

कॉलर ने बिना मोलभाव किए कहा: *"भैया, सोफा मुझे पसंद है। मैं अभी आपको एडवांस के ₹8,000 Google Pay पर भेज रहा हूँ। मेरा आदमी शाम को गाड़ी लेकर सोफा उठा लेगा।"*

2 मिनट बाद विकास के फोन पर एक नोटिफिकेशन आया: **"Collect Request: Pay ₹8,000 to Army Officer"**। फोन पर कॉलर ने कहा: *"भैया, मैंने आपको पैसे भेज दिए हैं। आप जल्दी से अपना UPI PIN डालिए, ताकि ₹8,000 आपके खाते में क्रेडिट हो जाएं।"*

विकास जैसे ही PIN डालने लगा, उसे याद आया: **"अरे! पैसे पाने के लिए तो कभी PIN नहीं डालना पड़ता!"** उसने तुरंत स्क्रीन ध्यान से पढ़ी — वहाँ लिखा था *"Paying ₹8,000"* न कि *"Receiving"*। विकास ने तुरंत पेमेंट कैंसिल कर दिया और कॉलर को ब्लॉक कर दिया। विकास के ₹8,000 लुटने से बच गए!

तुलना: UPI PIN कब डालना है और कब बिल्कुल नहीं?

❌ **PIN कभी न डालें (100% Fraud)**

- **पैसे प्राप्त करते समय:** कोई कहे कि पैसे लेने के लिए PIN डालो।
- **कैशबैक या लॉटरी क्लेम करने पर:** इनाम या रिवॉर्ड पाने के नाम पर।
- **अनजान Collect Request पर:** किसी अनजान व्यक्ति द्वारा भेजी गई रिक्वेस्ट पर।

• **कस्टमर केयर या बैंक अधिकारी के कहने पर:** फोन कॉल पर कोई PIN पूछे।

• **सरकारी सब्सिडी या योजना का लाभ लेने के नाम पर।**

✅ **केवल यहाँ PIN डालें (असली लेन-देन)**

• **जब आप खुद किसी को पैसे भेज रहे हों:** अपनी मर्जी से ट्रांसफर करते समय।

• **दुकान पर QR Code स्कैन करके सामान खरीदते समय।**

• **बिजली, पानी, गैस या मोबाइल रिचार्ज का बिल भरते समय।**

• **ऑनलाइन शॉपिंग (Flipkart, Amazon आदि) पर ऑर्डर का पेमेंट करते समय।**

• **अपने बैंक खाते का बैलेंस (Balance) चेक करते समय।**

UPI PIN कैसे बदलें या रीसेट करें? (Step-by-Step Guide)

यदि कभी आपको लगे कि आपके किसी दोस्त, रिश्तेदार या दुकानदार ने आपका PIN देख लिया है, तो बिना देर किए 1 मिनट में अपना PIN बदल लें:

1

UPI App खोलें और Bank Account पर जाएं

अपने फोन में **PhonePe**, **Google Pay**, **Paytm** या **BHIM** ऐप खोलें। अपनी प्रोफाइल फोटो पर टैप करके **Bank Accounts** सेक्शन चुनें।

2

'Change PIN' या 'Forgot PIN' पर टैप करें

जिस बैंक खाते का पिन बदलना है, उस पर टैप करें। अगर पुराना पिन याद है तो **Change PIN** चुनें; अगर पुराना पिन भूल गए हैं तो **Forgot / Reset PIN** चुनें।

3

प्रमाणीकरण विधि चुनें (Debit Card या Aadhaar)

• **Debit Card से:** अपने ATM कार्ड के अंतिम 6 अंक और एक्सपायरी डेट दर्ज करें।
• **Aadhaar से:** अपने आधार कार्ड के पहले 6 अंक दर्ज करें (यह सुविधा अब अधिकांश बैंकों में उपलब्ध है)।

4

बैंक से आया OTP और नया PIN दर्ज करें

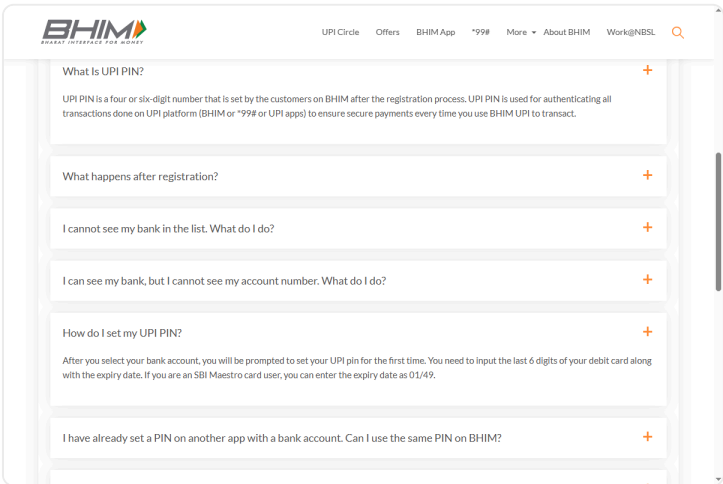
बैंक से आपके मोबाइल पर 6 अंकों का **OTP** अपने आप आ जाएगा। इसके बाद अपना नया मजबूत 4 या 6 अंकों का **UPI PIN** दो बार दर्ज करके सुरक्षित कर लें।

आधिकारिक पोर्टल पर UPI PIN के सुरक्षा नियम

NPCI द्वारा संचालित आधिकारिक **BHIM UPI** पोर्टल पर आम नागरिकों के लिए UPI PIN की सुरक्षा को लेकर स्पष्ट दिशा-निर्देश दिए गए हैं:

bhimupi.org.in/faqs

NPCI BHIM आधिकारिक पोर्टल



📌 **BHIM आधिकारिक पोर्टल से 2 सबसे अहम सीख:**

1. **पिन सिर्फ आपका है:** UPI PIN केवल उपयोगकर्ता की व्यक्तिगत संपत्ति है। बैंक, NPCI या सरकार का कोई भी प्रतिनिधि इसे जानने का अधिकारी नहीं है।
2. **पैसे पाने पर पिन नहीं:** आधिकारिक FAQ में साफ लिखा है कि इनकमिंग पेमेंट (पैसे प्राप्त करने) के लिए पिन दर्ज करने का कोई विकल्प नहीं होता।

अध्याय 3: UPI PIN सुरक्षा से जुड़े महत्वपूर्ण सवाल

(PIN Safety FAQs)

Q1: अगर मैं लगातार 3 बार गलत UPI PIN डाल दूँ तो क्या होगा?

उत्तर: सुरक्षा कारणों से बैंक आपकी UPI सेवाओं को 24 घंटे के लिए अस्थायी रूप से ब्लॉक कर देता है (Cooling Period)। 24 घंटे बाद आप दोबारा सही पिन डाल सकते हैं, या तुरंत अपने Debit Card / Aadhaar OTP से **Reset PIN** कर सकते हैं।

Q2: क्या UPI PIN और ATM PIN एक ही होते हैं?

उत्तर: नहीं। ATM PIN वह होता है जो आप बैंक के ATM मशीन से कैश निकालते समय डालते हैं। UPI PIN वह है जो आप फोन से UPI पेमेंट करते समय डालते हैं। सुरक्षा के लिए इन दोनों को हमेशा अलग-अलग रखना चाहिए।

Q3: क्या आसान PIN रखना ठीक है, जैसे 1234 या 0000 या जन्म वर्ष?

उत्तर: बिल्कुल नहीं! धोखेबाज सबसे पहले `1234`, `0000`, `1111` या आपकी जन्मतिथि (जैसे 1985) का अनुमान लगाते हैं। हमेशा ऐसा पिन बनाएं जिसका कोई दूसरा आसानी से अंदाजा न लगा सके।

Q4: क्या मेरा UPI PIN किसी ऐप कंपनी (जैसे Google Pay / PhonePe) को पता होता है?

उत्तर: बिल्कुल नहीं। जब आप पिन टाइप करते हैं, तो वह सीधे बैंक के सुरक्षित सर्वर पर जाता है। ऐप कंपनी केवल स्क्रीन दिखाती है, वह आपका पिन न तो पढ़ सकती है और न ही सेव कर सकती है।

Q5: क्या बैंक मैनेजर मेरे खाते का UPI PIN बता सकता है या बदल सकता है?

उत्तर: नहीं। बैंक मैनेजर या कोई भी कर्मचारी आपका UPI PIN नहीं देख सकता। इसे बदलने का अधिकार केवल आपके पास है, आपके रजिस्टर्ड सिम कार्ड और डेबिट कार्ड/आधार के जरिए।

UPI PIN की सुरक्षा: क्या करें और क्या न करें

✅ क्या करें (Do's)

• हर 3 से 6 महीने में अपना UPI PIN बदलते रहें।

• पिन डालते समय फोन की स्क्रीन को थोड़ा छुपाकर रखें ताकि कोई पीछे से न देख ले।

• अगर पिन भूल जाएं तो ऐप में 'Forgot PIN' पर जाकर आधार या एटीएम कार्ड से तुरंत रीसेट करें।

• हमेशा याद रखें: पैसे प्राप्त करने के लिए केवल अपना मोबाइल नंबर या QR कोड दिखाना पर्याप्त है।

❌ क्या न करें (Don'ts)

• किसी के कहने पर पैसे पाने, लॉटरी या कैशबैक के लिए कभी UPI PIN न डालें।

• अपना UPI PIN किसी कागज, डायरी या फोन के कवर पर लिखकर न रखें।

• फोन का स्क्रीन लॉक (Screen Lock) और UPI PIN कभी भी एक समान न रखें।

• फोन कॉल पर खुद को बैंक अधिकारी बताने वाले किसी भी व्यक्ति को पिन न बताएं।

Google पर आधिकारिक PIN रीसेट निर्देश कैसे खोजें? (PIN Reset Guide)

यदि आपको UPI PIN या BHIM ऐप से जुड़ी आधिकारिक सुरक्षा गाइड देखनी हो, तो Google पर इन 4 बातों का ध्यान रखें:

1

चरण 1: UPI PIN रीसेट का सटीक कीवर्ड खोजें

सर्च बार में केवल यह लिखें: `BHIM official UPI PIN safety rules`

2

"Sponsored" या "Ad" विज्ञापनों पर क्लिक न करें

सर्च रिजल्ट में सबसे ऊपर दिखने वाले प्रायोजित विज्ञापनों से बचें। साइबर अपराधी अक्सर फर्जी हेल्पलाइन के विज्ञापन लगाते हैं।

3

वेबसाइट के आधिकारिक पते (URL) की जांच करें

हमेशा देखें कि लिंक `https://www.bhimupi.org.in` या `https://www.npci.org.in` का ही हो। किसी अनजान ब्लॉग या वेबसाइट पर न जाएं।

4

सर्च पेज पर दिखने वाले नंबर पर फोन न करें

Google सर्च में दिखने वाले किसी भी फोन नंबर पर कॉल न लगाएं। आधिकारिक पोर्टल के अंदर दिए गए 'Help' सेक्शन से ही संपर्क करें।

🔍 अध्याय 3 के सत्यापित आधिकारिक स्रोत (Official Sources):

- **BHIM UPI आधिकारिक सुरक्षा पोर्टल:** `https://www.bhimupi.org.in/faqs`
- **NPCI UPI सुरक्षा मानक:** `https://www.npci.org.in/product/upi`
- **RBI डिजिटल भुगतान सुरक्षा निर्देश:** `https://www.rbi.org.in`

अध्याय 4 • 10 सेकंड का नियम (Pre-Payment Checks)

Payment करने से पहले

UPI में पैसा 1 सेकंड में ट्रांसफर हो जाता है, लेकिन गलत खाते में जाने के बाद उसे वापस लाना बहुत कठिन होता है। जानिए भुगतान से पहले 10 सेकंड में क्या जांचें।

10 सेकंड का 'सुरक्षा विराम' (Security Pause)

UPI तकनीक की सबसे बड़ी खूबी है इसकी रफ्तार — पैसा पलक झपकते ही सामने वाले के खाते में पहुँच जाता है। लेकिन यही रफ्तार कभी-कभी जल्दबाजी में सबसे बड़ा नुकसान बन जाती है।

एक बार अगर आपने अपना **UPI PIN** डालकर पेमेंट पूरा कर दिया, तो बैंक या ऐप के पास ऐसा कोई 'Undo' या 'Cancel' बटन नहीं होता जिससे पैसा रास्ते में ही रोक लिया जाए। इसलिए भुगतान करने से पहले केवल **10 सेकंड रुककर** स्क्रीन पर दिख रही 4 बातों की जांच करना आपकी सबसे बड़ी सुरक्षा ढाल है।

NPCI का अनिवार्य नियम

CBS Name Verification: असली बैंक नाम का सुरक्षा चक्र

भारतीय राष्ट्रीय भुगतान निगम (NPCI) ने सभी **UPI Apps** (जैसे PhonePe, Google Pay, Paytm, BHIM) के लिए यह अनिवार्य नियम बनाया है कि जब भी कोई यूजर QR कोड स्कैन करे या UPI ID डाले, तो ऐप को स्क्रीन पर प्राप्तकर्ता का असली बैंक खाता नाम (Core Banking System यानी **CBS Name**) दिखाना ही होगा।

💡 **इसका क्या मतलब है?** कोई धोखेबाज ऐप में अपना नाम "Electricity Department" या "Army Officer" लिख सकता है, लेकिन स्क्रीन पर उसके असली बैंक खाते में दर्ज नाम (जैसे *"Mohammad Aslam"* या *"Ramesh Kumar"*) ही दिखेगा। यदि नाम संदिग्ध लगे, तो तुरंत रुक जाएं!

केस स्टडी: सोनू और पेट्रोल पंप का ₹500 बनाम ₹5,000

सोनू अपने स्कूटर में पेट्रोल डलवाने के बाद जल्दी में था क्योंकि उसे ऑफिस पहुंचने में देर हो रही थी। पेट्रोल ₹500 का डला था।

जल्दबाजी का झटका

एक अतिरिक्त शून्य (0) का फरेब

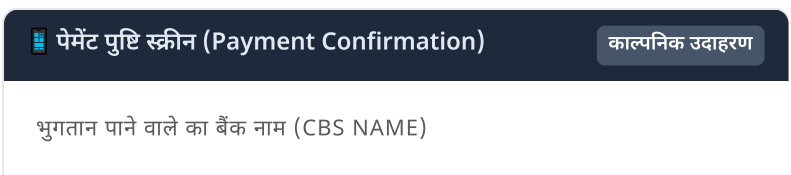
सोनू ने बाइक पर बैठे-बैठे जल्दी में स्कैनर खोला, ₹5000 टाइप कर दिया (गलती से एक शून्य 0 ज्यादा दब गया) और बिना देखे सीधे पिन डालने की स्क्रीन पर बढ़ गया।

लेकिन जैसे ही उसकी उंगलियां पिन डालने लगीं, उसे याद आया: **"10 सेकंड रुककर रकम और नाम देखना है!"** उसने देखा कि स्क्रीन पर **₹5,000.00** लिखा हुआ था, जबकि बिल सिर्फ ₹500 का था!

सोनू ने तुरंत बैक (Cancel) किया और सही ₹500 टाइप करके पेमेंट किया। केवल 5 सेकंड के उस ठहराव ने उसके बैंक खाते के ₹4,500 की अनचाही परेशानी बचा ली।

पेमेंट स्क्रीन पर क्या जांचें? (Interactive Mockup)

जब आप किसी दुकान पर QR कोड स्कैन करते हैं, तो PIN डालने से ठीक पहले स्क्रीन पर यह पुष्टि पृष्ठ (Confirmation Screen) आता है:



Ramesh Kumar Kirana ✓ Verified

जांच 1: क्या यह वही दुकान या व्यक्ति है जिसे आप पैसे भेज रहे हैं?

UPI ID (VPA)

rameshkirana@okaxis

जांच 2: क्या UPI ID सही है? कोई अनजान पता तो नहीं?

रकम (AMOUNT)

₹ 450.00

जांच 3: शून्य (0) ठीक से गिनें। 45 की जगह 450 या 4500 तो नहीं लिख गया?

भुगतान खाता (PAY FROM)

State Bank of India •••• 4021

जांच 4: क्या सही बैंक खाते से पैसे कट रहे हैं?

Proceed to Pay (पिन डालें) →

दुकान के भौतिक QR Code की जांच कैसे करें?

आजकल कई शहरों में धोखेबाज रात के समय या भीड़भाड़ वाली दुकानों में जाकर दुकानदार के असली QR कोड स्टैंडी के ऊपर अपना खुद का फर्जी QR स्टीकर चिपका देते हैं। ग्राहक स्कैन करता है और पैसा दुकानदार के बजाय धोखेबाज के खाते में चला जाता है।



स्टीकर छूकर देखें

जांचें कि क्या असली प्लास्टिक स्टैंडी के ऊपर कोई नया पेपर या स्टीकर अलग से चिपकाया हुआ तो नहीं है।



दुकानदार से नाम की पुष्टि करें

स्कैन करने के बाद दुकानदार से पूछें: *"भैया, स्क्रीन पर 'राजेश जनरल स्टोर' आ रहा है, यही आपका नाम है ना?"*



साउंडबॉक्स की पुष्टि (Voice Alert पर ध्यान दें)

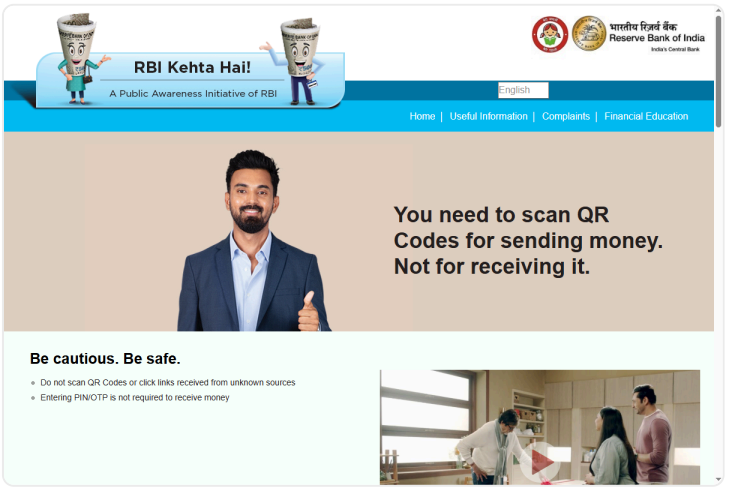
पेमेंट होने के बाद दुकान पर लगे **Soundbox** से आवाज आने का इंतजार करें। यदि आवाज न आए तो दुकानदार को ट्रांजैक्शन की पुष्टि कराएं।

RBI Kehta Hai: आधिकारिक QR Code सुरक्षा निर्देश

भारतीय रिज़र्व बैंक (RBI) अपने आधिकारिक जन-जागरूकता पोर्टल पर QR कोड से जुड़े सबसे बड़े नियम को साफ शब्दों में समझाता है:

rbikehtahai.rbi.org.in

RBI आधिकारिक जागरूकता



📌 RBI क्यूआर कोड (QR Safety) निर्देश से 2 मुख्य सीख:

1. **QR कोड सिर्फ भुगतान करने के लिए:** *"Scan QR code only to make payment, not to receive payment."* (QR कोड केवल पैसे भेजने के लिए स्कैन किया जाता है, पैसे पाने के लिए कभी नहीं)।

2. **पैसे लेने के लिए QR स्कैन न करें:** यदि कोई कहे कि *"यह QR स्कैन करो, तुम्हारे खाते में ₹5,000 आ जाएंगे"*, तो समझ जाएं कि वह ठगी कर रहा है। स्कैन करते ही आपके खाते से पैसे कट जाएंगे।

अध्याय 4: QR कोड और पेमेंट सत्यापन से जुड़े

सवाल (Verification FAQs)

Q1: Static QR Code और Dynamic QR Code में क्या अंतर होता है?

उत्तर: दुकान पर जो प्रिंटेड स्टैंडी लगी होती है, वह **Static QR** होती है, जिसमें रकम आपको खुद टाइप करनी होती है। बड़े मॉल या पेट्रोल पंप की बिलिंग मशीन पर जो स्क्रीन पर QR बनता है, वह **Dynamic QR** होता है, जिसमें बिल की रकम पहले से दर्ज होती है।

Q2: अगर स्क्रीन पर दिख रहा नाम दुकानदार के नाम से अलग हो तो क्या करें?

उत्तर: तुरंत रुकें! दुकानदार से पूछें कि खाते में किसका नाम दर्ज है (कई बार दुकान का नाम और मालिक का व्यक्तिगत नाम अलग हो सकता है)। जब तक दुकानदार पुष्टि न करे, तब तक PIN दर्ज न करें।

Q3: अगर मैंने गलती से किसी गलत नंबर या गलत व्यक्ति को पैसे भेज दिए तो क्या वे तुरंत वापस आ सकते हैं?

उत्तर: UPI में तुरंत वापस पाने का कोई ऑटो-रिवर्सल बटन नहीं होता। आपको तुरंत अपने बैंक को सूचित करना होगा और 12-अंकों के UTR नंबर के साथ शिकायत दर्ज करानी होगी ताकि आपका बैंक प्राप्तकर्ता के बैंक से संपर्क कर पैसे होल्ड करा सके।

Q4: क्या QR Code स्कैन करने से फोन में वायरस आ सकता है?

उत्तर: यदि आप केवल अधिकृत UPI ऐप (जैसे PhonePe, BHIM, Google Pay) के स्कैनर से स्कैन कर रहे हैं, तो केवल पेमेंट स्क्रीन खुलेगी। लेकिन फोन के साधारण कैमरा या किसी अनजान स्कैनर ऐप से संदिग्ध पोस्टर का QR स्कैन करने पर हानिकारक वेबसाइट खुल सकती है। इसलिए हमेशा अपने UPI ऐप के अंदर वाले स्कैनर का ही उपयोग करें।

Q5: क्या पेमेंट करने से पहले मुझे अपने बैंक खाते का बैलेंस जांचना चाहिए?

उत्तर: हाँ। पर्याप्त बैलेंस न होने पर ट्रांजैक्शन डिक्लाइन (Decline) हो सकता है, और कुछ बैंक बार-बार असफल लेन-देन पर मामूली चार्ज लगा सकते हैं।

पेमेंट करने से पहले: क्या करें और क्या न करें

✅ क्या करें (Do's)

• पिन डालने से पहले 10 सेकंड रुककर स्क्रीन पर दिख रहे नाम और रकम की पुष्टि करें।

• दुकान पर QR कोड स्कैन करने के बाद दुकानदार से नाम का मिलान अवश्य करें।

• केवल अधिकृत UPI ऐप के भीतर दिए गए QR स्कैनर का ही उपयोग करें।

• बड़ा भुगतान करने से पहले यदि संदेह हो, तो पहले ₹1 भेजकर सही खाते की पुष्टि कर लें।

❌ क्या न करें (Don'ts)

• कभी भी हड़बड़ी, जल्दबाजी या किसी के दबाव में आकर बिना देखे PIN न डालें।

• किसी अनजान व्यक्ति द्वारा WhatsApp पर भेजे गए QR कोड को पैसे पाने के नाम पर स्कैन न करें।

• दुकान पर किसी मुड़े-तुड़े या ऊपर से चिपकाए गए संदिग्ध QR कोड पर बिना जांचे पेमेंट न करें।

• रकम डालते समय शून्य (0) की संख्या की अनदेखी न करें।

Google पर QR Code सुरक्षा निर्देश कैसे खोजें? (QR Safety Guide)

यदि आपको QR कोड और मर्चेंट पेमेंट की सुरक्षा पर RBI और NPCI के दिशा-निर्देश देखने हों, तो Google पर इन 4 बातों का ध्यान रखें:

1

चरण 1: QR Code सुरक्षा का आधिकारिक कीवर्ड खोजें

सर्च बार में केवल यह लिखें: `RBI Kehta hai QR code scan safety rules`

2

चरण 2: विज्ञापनों को छोड़कर RBI आधिकारिक गाइड देखें

सर्च रिजल्ट में सबसे ऊपर दिखने वाले विज्ञापनों पर क्लिक न करें। साइबर अपराधी अक्सर फर्जी पेमेंट गेटवे के लिंक ऊपर लगवाते हैं।

3

चरण 3: आधिकारिक RBI डोमेन पते (URL) की जांच करें

हमेशा देखें कि लिंक `https://rbikehtahai.rbi.org.in` या `https://www.npci.org.in` का ही हो।

4

चरण 4: Google सर्च पर दिखने वाले नंबरों पर कॉल न करें

सर्च इंजन में सीधे दिख रहे किसी भी मोबाइल नंबर या कस्टमर केयर नंबर पर कभी फोन न लगाएं।

🔍 अध्याय 4 के सत्यापित आधिकारिक स्रोत (Official Sources):

- **RBI Kehta Hai QR कोड सुरक्षा जागरूकता:** `https://rbikehtahai.rbi.org.in`
- **NPCI मर्चेंट पेमेंट और CBS Name वेरिफिकेशन निर्देश:** `https://www.npci.org.in`
- **BHIM UPI मर्चेंट सुरक्षा गाइड:** `https://www.bhimupi.org.in`

अध्याय 5 • धोखे के तरीके (Common UPI Scams)

UPI के आम Scams

धोखेबाज तकनीकी खामियों से नहीं, बल्कि आपकी घबराहट या लालच का फायदा उठाकर पैसे चुराते हैं। जानिए सबसे आम 4 चालें और उनसे बचने के अचूक नियम।

ठग बैंक को नहीं, इंसान के दिमाग को हैक करते हैं

कई लोगों को लगता है कि साइबर अपराधी कंप्यूटर हैकिंग करके सीधे बैंक का सर्वर तोड़ देते हैं। **यह बिल्कुल सच नहीं है।** भारत का UPI सिस्टम इतना मजबूत है कि कोई भी धोखेबाज बाहर से इसे हैक नहीं कर सकता।

इसलिए अपराधी क्या करते हैं? वे सीधे बैंक पर हमला करने के बजाय आपको फोन करते हैं, मैसेज भेजते हैं और आपको इतना डरा देते हैं (जैसे *"बिजली कट जाएगी / खाता बंद हो जाएगा"*) या इतना लालच दे देते हैं (जैसे *"₹5,000 का कैशबैक मिला है"*) कि आप खुद अपनी उंगलियों से अपना **UPI PIN** या **OTP** डाल देते हैं। इसे साइबर सुरक्षा में **Social Engineering** कहते हैं।

केस स्टडी: अनीता जी और कूरियर का ₹5 वाला

झांसा

अनीता जी ने एक ऑनलाइन शॉपिंग वेबसाइट से अपनी बेटी के जन्मदिन के लिए कपड़े मंगवाए थे। डिलीवरी में एक दिन की देरी हो गई थी। दोपहर में उनके पास एक अनजान नंबर से फोन आया।

धोखेबाज की कॉल

"मैडम, आपका पार्सल होल्ड पर है, केवल ₹5 का री-डिलीवरी चार्ज लगेगा!"

कॉलर ने बहुत शालीन आवाज में कहा: *"मैडम, मैं BlueDart कूरियर ऑफिस से बोल रहा हूँ। आपके घर का पता अधूरा है, इसलिए पार्सल रुका हुआ है। मैं आपके WhatsApp पर एक लिंक भेज रहा हूँ, उस पर केवल ₹5 का टोकन चार्ज भर दीजिए, पार्सल आज शाम को डिलीवर हो जाएगा।"*

अनीता जी ने WhatsApp खोला। लिंक पर क्लिक करते ही एक ऐप डाउनलोड होने लगा जिसका नाम था **"Support_Quick.apk"**। कॉलर ने कहा: *"मैडम, ऐप खोलकर 9 अंकों का कोड बताइए और अपना Google Pay खोलिए।"*

अनीता जी को तुरंत शक हुआ: **"सिर्फ ₹5 देने के लिए अलग से ऐप क्यों डाउनलोड करवा रहा है?"** उन्होंने तुरंत कॉल काट दी और डाउनलोड की गई फाइल को इंस्टॉल किए बिना डिलीट कर दिया। बाद में शाम को कूरियर अपने सामान्य समय पर बिना

किसी चार्ज के घर पहुँच गया। केवल एक पल की समझदारी ने उनके खाते के हजारों रुपये बचा लिए।

भारत में सबसे ज्यादा होने वाले 4 बड़े UPI Scams

Scam 1

Collect Request Fraud (पैसे देने के बहाने पैसे काटना)

यह सबसे पुराना लेकिन सबसे ज्यादा लोगों को फंसाने वाला धोखा है। इसमें धोखेबाज आपको पैसे भेजने का नाटक करके आपके फोन पर पैसे मांगने की रिक्वेस्ट भेजता है।

धोखेबाज की चाल: *"सर, मैं आपको एडवांस के ₹10,000 भेज रहा हूँ। आपके PhonePe पर नोटिफिकेशन गया है, जल्दी से 'Accept' दबाकर PIN डाल दीजिए, पैसे क्रेडिट हो जाएंगे।"*

कड़वा सच: UPI में किसी रिक्वेस्ट पर 'Pay' या 'Accept' दबाने और PIN डालने का मतलब होता है — **आपके खाते से पैसे कटकर सामने वाले के खाते में जाना!**

🛡️ **बचाव:** किसी भी अनजान व्यक्ति द्वारा भेजी गई Collect Request को तुरंत **'Decline' (अस्वीकार)** करें और उस यूजर को ब्लॉक करें।

Scam 2

Fake Refund और Cashback Scam (रिवॉर्ड का लालच)

धोखेबाज मैसेज भेजते हैं: *"बधाई! आपने PhonePe पर ₹3,999 का स्क्रैच कार्ड जीता है। तुरंत क्लेम करें।"*

धोखेबाज की चाल: जैसे ही आप उस लिंक पर क्लिक करते हैं, वह आपके फोन के UPI ऐप को खोल देता है। स्क्रीन पर हरा बटन दिखता है: *"Send to Bank"*। आप सोचते हैं कि पैसा आ रहा है, और आप पिन डाल देते हैं।

कड़वा सच: कोई भी असली कैशबैक पाने के लिए किसी बाहरी लिंक या वेबसाइट पर जाने की जरूरत नहीं होती। असली कैशबैक अपने आप बैंक खाते में क्रेडिट हो जाता है।

बचाव: WhatsApp या SMS पर आए किसी भी 'कैशबैक क्लेम' लिंक पर कभी क्लिक न करें।

Scam 3

Screen Share Scam (AnyDesk / TeamViewer का जाल)

जब किसी का पेमेंट अटक जाता है, तो धोखेबाज बैंक का कस्टमर केयर बनकर कॉल करता है।

धोखेबाज की चाल: *"सर, आपका ₹2,000 फंसा हुआ है। हम सर्वर से रिफंड कर रहे हैं। आप Play Store से AnyDesk या TeamViewer ऐप डाउनलोड कीजिए और 9 अंकों का कोड बताइए।"*

कड़वा सच: यह कोड बताते ही आपके फोन की पूरी स्क्रीन धोखेबाज के कंप्यूटर पर लाइव दिखने लगती है। जब आप अपना बैंक ऐप खोलते हैं, तो वह आपके

द्वारा टाइप किया गया पासवर्ड और आने वाला बैंक **OTP** लाइव देखकर आपका पूरा खाता खाली कर देता है।

बचाव: किसी भी व्यक्ति के कहने पर अपने फोन में AnyDesk, TeamViewer या RustDesk जैसे स्क्रीन शेयरिंग ऐप कभी डाउनलोड न करें।

Scam 4

Fake Customer Care (Google Search पर फर्जी नंबर)

लोग Google पर *"Google Pay customer care number"* सर्च करते हैं और ऊपर दिख रहे नंबर पर कॉल लगा देते हैं।

धोखेबाज की चाल: फोन उठाने वाला खुद को सीनियर मैनेजर बताता है और कहता है: *"सर, आपका UPI ब्लॉक हो गया है। इसे चालू करने के लिए इस लिंक पर जाकर ₹1 का टेस्ट पेमेंट कीजिए।"*

कड़वा सच: Google सर्च के परिणामों में दिखने वाले अधिकांश नंबर साइबर ठगों द्वारा पैसे देकर विज्ञापनों में डाले गए होते हैं।

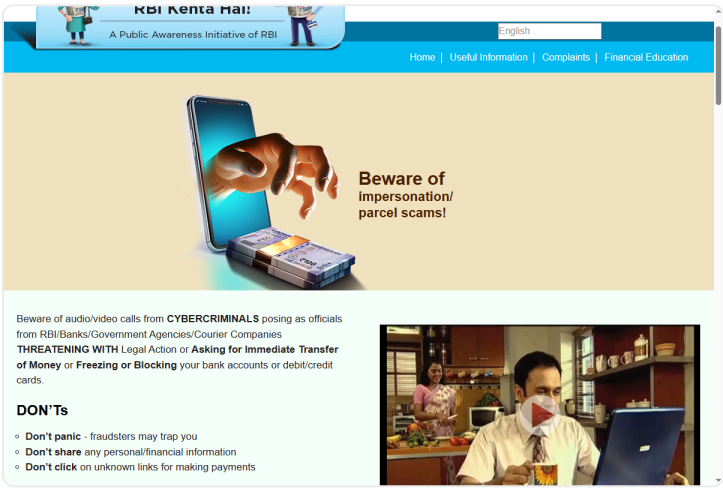
बचाव: कभी भी Google सर्च से हेल्पलाइन नंबर न निकालें। हमेशा केवल अपने बैंक ऐप या पासबुक में दिए गए नंबर का ही उपयोग करें।

RBI Kehta Hai: आधिकारिक जागरूकता निर्देश

भारतीय रिज़र्व बैंक अपने जन-जागरूकता पोर्टल **'RBI Kehta Hai'** पर नागरिकों को फर्जी अधिकारियों और कॉल्स से बचने की साफ सलाह देता है:

rbikehtahai.rbi.org.in

RBI आधिकारिक जागरूकता



📌 RBI प्रतिरूपण (Impersonation Scam) निर्देश से 2 मुख्य सीख:

1. **धमकी देने वालों से सावधान:** बैंक अधिकारी, पुलिस या कूरियर कंपनी बनकर तत्काल पैसे ट्रांसफर करने या खाता ब्लॉक करने की धमकी देने वाले कॉल्स से कभी न डरें।

2. **गोपनीय जानकारी न दें:** अपना बैंक पासवर्ड, पिन, OTP या कार्ड का CVV कभी किसी के साथ शेयर न करें।

अध्याय 5: UPI Scams से बचाव से जुड़े महत्वपूर्ण सवाल (Scam Prevention FAQs)

Q1: अगर मेरे फोन पर अनजान व्यक्ति की Collect Request आए, तो मुझे क्या करना चाहिए?

उत्तर: सीधे लाल रंग का **'Decline' (अस्वीकार)** बटन दबाएं और ऐप में दिए गए *'Report Spam / Block'* विकल्प पर टैप कर दें। इससे वह व्यक्ति आपको दोबारा रिक्वेस्ट नहीं भेज पाएगा।

Q2: अगर गलती से मैंने AnyDesk या स्क्रीन शेयरिंग ऐप डाउनलोड कर लिया हो तो क्या करूँ?

उत्तर: तुरंत 3 काम करें: (1) फोन का इंटरनेट (Mobile Data / Wi-Fi) तुरंत बंद करें, (2) उस ऐप को फोन से अनइंस्टॉल (Delete) करें, और (3) किसी दूसरे फोन से अपने बैंक को फोन करके अपने नेटबैंकिंग व यूपीआई को तुरंत ब्लॉक करवाएं।

Q3: क्या बैंक कभी रिफंड देने के लिए फोन पर संपर्क करता है?

उत्तर: कभी नहीं। यदि किसी लेन-देन का रिफंड आना होता है, तो वह सीधे आपके बैंक खाते में 24 से 48 घंटे में स्वतः क्रेडिट हो जाता है। इसके लिए किसी को कॉल करने या पिन डालने की आवश्यकता नहीं होती।

Q4: क्या फोन पर बात करते समय मेरा बैंक खाता खाली हो सकता है?

उत्तर: नहीं। केवल फोन पर बात करने से पैसे नहीं कटते। पैसे तभी कटते हैं जब आप या तो अपना UPI PIN डालते हैं, या बैंक से आया OTP बता देते हैं, या स्क्रीन शेयरिंग ऐप से उन्हें अपनी स्क्रीन दिखा देते हैं।

Q5: अगर धोखेबाज मुझे पुलिस केस या कानूनी कार्रवाई की धमकी दे तो क्या करूँ?

उत्तर: तुरंत फोन काटें! कोई भी असली पुलिस या जांच एजेंसी फोन पर पैसे ट्रांसफर करने या UPI से जुर्माना भरने को नहीं कहती। यह 100% साइबर अपराधियों की डराने की चाल है।

अनजान कॉल्स व ऑफर्स: क्या करें और क्या न करें

✅ क्या करें (Do's)

• अनजान Collect Request को बिना सोचे तुरंत Decline करें।

• कोई भी समस्या होने पर केवल ऐप के अंदर दिए गए आधिकारिक 'Help & Support' का उपयोग करें।

• अगर कोई फोन पर डराए, तो शांत रहें और परिवार के किसी सदस्य से बात करें।

• किसी भी साइबर ठगी की घटना की तुरंत `cybercrime.gov.in` पर रिपोर्ट करें।

❌ क्या न करें (Don'ts)

• पैसे पाने, लॉटरी या कैशबैक के लिए कभी किसी रिक्वेस्ट पर 'Pay' न दबाएं।

• किसी अनजान कॉलर के कहने पर AnyDesk, TeamViewer या QuickSupport ऐप इंस्टॉल न करें।

• Google सर्च में दिखने वाले किसी भी कस्टमर केयर नंबर पर भरोसा न करें।

• किसी को भी अपने बैंक का OTP या कार्ड का CVV कभी न बताएं।

Google पर आधिकारिक स्कैम एडवाइजरी कैसे खोजें? (Scam Alert Guide)

यदि आपको वित्तीय साइबर ठगी की रिपोर्ट करने के लिए राष्ट्रीय साइबर अपराध पोर्टल खोजना हो, तो Google पर इन 4 बातों का ध्यान रखें:

1

चरण 1: RBI व NPCI स्कैम एडवाइजरी कीवर्ड लिखें

सर्च बार में केवल यह लिखें: `cybercrime gov in report financial fraud`

2

चरण 2: प्रायोजित विज्ञापनों के बजाय rbi.org.in चुनें

सर्च में सबसे ऊपर दिखने वाले प्रायोजित विज्ञापनों पर क्लिक न करें। असली सरकारी लिंक हमेशा सामान्य सर्च रिजल्ट में नीचे होता है।

3

चरण 3: सरकारी व संस्थागत डोमेन पते (URL) की जांच करें

हमेशा देखें कि वेबसाइट का पता `https://cybercrime.gov.in` ही हो। भारत सरकार के पोर्टल्स के अंत में हमेशा `.gov.in` होता है।

4

चरण 4: सर्च पर दिखने वाले नंबरों पर कभी कॉल न करें

सर्च इंजन में सीधे दिख रहे किसी भी मोबाइल नंबर पर कभी भरोसा न करें। केवल आधिकारिक पोर्टल पर जाकर ही ऑनलाइन शिकायत दर्ज करें।

🔍 अध्याय 5 के सत्यापित आधिकारिक स्रोत (Official Sources):

- **गृह मंत्रालय राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल:** `https://cybercrime.gov.in`
- **RBI Kehta Hai impersonation व वित्तीय ठगी निर्देश:** `https://rbikehtahai.rbi.org.in`
- **NPCI फ्रॉड अवेयरनेस सर्कुलर:** `https://www.npci.org.in`

अध्याय 6 • रोज़मर्रा की जिंदगी (Daily Scenarios)

दुकान, घर और रोज़ की ठगी

किराने की दुकान से लेकर घर के दरवाजे तक रोजमर्रा के जीवन में होने वाले 3 सबसे बड़े धोखे, सच्ची कहानियाँ और उनसे बचने के सरल नियम।

ठगी सिर्फ फोन पर नहीं, आपके आस-पास की दुकानों में भी होती है

जब लोग साइबर अपराध के बारे में सुनते हैं, तो उन्हें लगता है कि यह केवल बड़े कंप्यूटर हैकरों का काम है। लेकिन असलियत यह है कि रोजमर्रा की जिंदगी में आपके घर के पास की चाय की दुकान, कूरियर डिलीवरी और मोबाइल पर आने वाले बिजली के बिल में भी ठग घात लगाए बैठे रहते हैं।

आइए 3 सच्ची घटनाओं के जरिए समझें कि सामान्य लोग कहाँ चूक करते हैं और केवल 10 सेकंड की सावधानी कैसे आपकी गाढ़ी कमाई को बचा सकती है।

केस स्टडी 1

दुकान पर बदला हुआ QR Code स्टीकर

सोहन शाम को पास की किराने की दुकान पर ₹320 का सामान लेने गया। दुकान पर बहुत भीड़ थी। सोहन ने काउंटर पर रखे प्लास्टिक के स्टैंडी पर लगे **QR Code** को जल्दी में स्कैन किया, ₹320 टाइप किए और अपना **UPI PIN** डालकर पेमेंट कर दिया।

> **सोहन:** "भैया, ₹320 भेज दिए हैं, चेक कर लीजिए।"
>
> **दुकानदार:** "भाई, मेरे साउंडबॉक्स से तो कोई आवाज नहीं आई और न ही मेरे फोन पर कोई मैसेज आया।"
>
> **सोहन:** "देखिए, मेरे खाते से तो कट गए!" (सोहन ने अपना फोन दिखाया, जहाँ 'Paid ₹320 to Rajesh Kumar' लिखा था)।
>
> **दुकानदार:** "अरे! मेरा नाम तो 'रमेश गुप्ता' है, यह राजेश कुमार कौन है?"

जब दुकानदार ने स्टैंडी को ध्यान से छुआ, तो देखा कि किसी धोखेबाज ने उसके असली QR कोड के ऊपर अपना खुद का फर्जी QR स्टीकर चिपका रखा था! सोहन का पैसा दुकानदार के बजाय उस ठग के खाते में चला गया था।

💡 **सोहन से क्या चूक हुई?** सोहन ने पिन डालने से पहले स्क्रीन पर दिखने वाले बैंक नाम (CBS Name) को दुकानदार के नाम से नहीं मिलाया। अगर वह सिर्फ 2 सेकंड पूछ लेता कि *"भैया स्क्रीन पर राजेश नाम आ रहा है, क्या यह आप ही हैं?"*, तो ठगी तुरंत पकड़ी जाती।

केस स्टडी 2

फर्जी डिलीवरी एजेंट और OTP का खतरनाक खेल

कविता जी दोपहर में घर पर थीं। उनके फोन पर एक कॉल आया:

कॉलर: "नमस्ते मैडम, मैं Amazon डिलीवरी से बोल रहा हूँ। आपका एक पार्सल आया है, लेकिन आपके मकान का नंबर साफ नहीं दिख रहा है। क्या आप घर पर हैं?"

कविता जी: "हाँ, मैं घर पर हूँ, लेकिन मैंने तो कोई पार्सल नहीं मंगाया।"

कॉलर: "मैडम, शायद आपके पति या बेटे ने ऑर्डर किया होगा। अगर आपको पार्सल कैंसिल कराना है, तो कंपनी के नियम के अनुसार आपके फोन पर कैंसिलेशन का 6 अंकों का **OTP** आया है, वह बता दीजिए ताकि पार्सल वापस चला जाए और कोई चार्ज न लगे।"

कविता जी ने सोचा कि पार्सल कैंसिल करने का ही कोड होगा। उन्होंने बिना SMS पढ़े कॉलर को OTP बता दिया। फोन कटते ही 2 मिनट के भीतर कविता जी के बैंक खाते से **₹20,000** साफ हो गए!

> ⚠️ **सच्चाई क्या थी?** वह OTP किसी पार्सल का नहीं था! ठग ने अपने फोन में कविता जी का मोबाइल नंबर डालकर UPI ऐप रजिस्टर करने की कोशिश की थी, और कविता जी ने खुद उसे लॉगिन करने का बैंक OTP दे दिया था।

केस स्टडी 3

बिजली कटने का फर्जी SMS और रात का डर

शर्मा जी रात को 8:45 बजे खाना खा रहे थे, तभी उनके फोन पर यह SMS आया:

> "Dear Consumer, your electricity power will be disconnected tonight at 9:30 PM from electricity office because your previous month bill was not updated. Please immediately call officer on: [10-अंकों का व्यक्तिगत मोबाइल नंबर]"

शर्मा जी घबरा गए कि रात में बिजली कट जाएगी तो बच्चे कैसे पढ़ेंगे और फ्रिज बंद हो जाएगा। उन्होंने तुरंत उस नंबर पर फोन मिलाया।

> **धोखेबाज:** "सर, आपका बिल सर्वर में पेंडिंग दिख रहा है। आप तुरंत अपने Google Pay से केवल ₹10 का री-वेरिफिकेशन पेमेंट इस लिंक पर कीजिए, लाइन चालू रहेगी।"

शर्मा जी ने लिंक खोला, ₹10 का भुगतान करने के लिए PIN डाला। लेकिन लिंक के पीछे ठग ने ₹10 नहीं, बल्कि **₹35,000 की Collect Request** लगा रखी थी। PIN डालते ही शर्मा जी के खाते से ₹35,000 कट गए।

> 🛡️ **बचाव का नियम:** बिजली विभाग कभी भी किसी 10-अंकों वाले मोबाइल नंबर से रात में लाइट काटने की धमकी नहीं देता। अगर बिल का संदेह हो, तो हमेशा अपने बिजली बिल पर लिखे आधिकारिक ऐप या नजदीकी बिजली घर जाकर ही पता करें।

दुकान पर QR Code स्कैन करते समय 4-चरणीय सुरक्षा चेकलिस्ट

बाजार या दुकान पर जब भी आप पेमेंट करें, तो इन 4 कदमों का अनिवार्य रूप से पालन करें:

1. **भौतिक QR कोड की जांच करें**

   दुकान के स्टैंडी को उंगली से छूकर देखें कि क्या उसके ऊपर कोई अलग से स्टीकर या कागज तो नहीं चिपकाया गया है।

2

स्क्रीन पर दिखने वाला CBS नाम पढ़ें

स्कैन करने के बाद स्क्रीन पर जो नाम आए, उसे देखें। अगर आप 'गुप्ता स्टोर' पर हैं और स्क्रीन पर 'संजय सिंह' दिखे, तो तुरंत रुकें।

3

दुकानदार से बोलकर पुष्टि करें

पिन डालने से पहले दुकानदार से पूछें: *"भैया, स्क्रीन पर आपका यही नाम आ रहा है ना?"*

4

दुकानदार के लिए: साउंडबॉक्स की आवाज अवश्य सुनें

पिन डालने के बाद दुकान पर लगे **Soundbox** से आवाज आने का इंतजार करें। आवाज आते ही पेमेंट की 100% पुष्टि हो जाती है।

दूरसंचार विभाग का 'चक्षु' (Chakshu) पोर्टल

भारत सरकार के दूरसंचार विभाग (DoT) ने फर्जी SMS, बिजली बिल की धमकी और फर्जी कॉल्स की शिकायत के लिए **'चक्षु'** पोर्टल शुरू किया है:



📌 संचार साथी पोर्टल से 2 महत्वपूर्ण बातें:

1. **फर्जी संदेशों की सीधी रिपोर्ट:** अगर आपको बिजली कटने, लॉटरी या पार्सल के नाम पर कोई फर्जी SMS या WhatsApp संदेश आए, तो आप सीधे 'चक्षु' पर उस नंबर की रिपोर्ट कर सकते हैं।

2. **नंबर होगा हमेशा के लिए ब्लॉक:** आपकी एक शिकायत से सरकार उस धोखेबाज के सिम कार्ड और फोन को पूरे देश में स्थायी रूप से ब्लॉक कर देती है।

अध्याय 6: दुकानदार व दैनिक लेन-देन से जुड़े सवाल

(Merchant FAQs)

Q1: डिलीवरी एजेंट को कौन सा OTP देना सुरक्षित होता है?

उत्तर: डिलीवरी बॉय को केवल वही OTP बताएं जो डिलीवरी के समय आपके फोन पर आता है और जिसमें साफ लिखा हो: *"Share this OTP with delivery agent only when you receive package"*। और यह OTP केवल तभी दें जब सामान भौतिक रूप से आपके हाथ में आ चुका हो। फोन पर कभी OTP न दें।

Q2: अगर दुकान का साउंडबॉक्स न बोले और मेरे खाते से पैसे कट जाएं तो क्या करें?

उत्तर: अपने ऐप में उस ट्रांजैक्शन को खोलें और दुकानदार को 12-अंकों का **UTR Number** दिखाएं। दुकानदार अपने ऐप के 'History' सेक्शन में वह UTR देखकर पुष्टि कर सकता है।

Q3: क्या बिजली विभाग सच में रात को 9:30 बजे बिजली काट सकता है?

उत्तर: बिल्कुल नहीं! भारत में बिजली आपूर्ति नियमों के अनुसार रात के समय या बिना पूर्व लिखित कानूनी नोटिस के किसी भी उपभोक्ता की घरेलू बिजली नहीं काटी जा सकती। ऐसे सभी SMS 100% साइबर अपराधियों द्वारा भेजे जाते हैं।

Q4: अगर मैंने फर्जी बिजली बिल वाले लिंक पर क्लिक कर दिया हो तो तुरंत क्या करूँ?

उत्तर: यदि केवल लिंक खुला है और आपने PIN नहीं डाला, तो तुरंत पेज बंद करें और फोन के Downloads फोल्डर से कोई भी नई फाइल डिलीट कर दें। अगर PIN डाल दिया था, तो तुरंत अपना UPI PIN बदलें और बैंक को सूचित करें।

Q5: क्या सड़क किनारे ठेले वाले को UPI पेमेंट करना सुरक्षित है?

उत्तर: हाँ, 100% सुरक्षित है। बस नियम वही रखें — स्कैन करने के बाद स्क्रीन पर दिखने वाला नाम ठेले वाले से पूछें और सही रकम टाइप करके ही PIN डालें।

दुकान व डिलीवरी सुरक्षा: क्या करें और क्या न करें

✅ क्या करें (Do's)

• दुकान पर पेमेंट करने से पहले स्क्रीन पर दिखने वाले नाम की दुकानदार से पुष्टि करें।

• डिलीवरी एजेंट को OTP केवल तभी दें जब पार्सल आपके हाथ में मिल चुका हो।

• बिजली या गैस का बिल हमेशा आधिकारिक सरकारी पोर्टल या अधिकृत बिलिंग ऐप से भरें।

• फर्जी संदेश आने पर तुरंत भारत सरकार के 'चक्षु' पोर्टल पर शिकायत दर्ज कराएं।

❌ क्या न करें (Don'ts)

• दुकान पर किसी मुड़े हुए या अलग से चिपकाए गए स्टीकर वाले QR पर बिना जांचे पैसे न भेजें।

• फोन कॉल पर ऑर्डर कैंसिल करने या पता सही करने के नाम पर कभी OTP न बताएं।

• बिजली कटने के किसी भी SMS में दिए गए 10-अंकों वाले नंबर पर कभी कॉल न करें।

• अनजान लिंक पर जाकर कभी भी ₹1 या ₹10 का टेस्ट पेमेंट न करें।

Google पर चक्षु पोर्टल और मर्चेंट सपोर्ट कैसे खोजें? (Merchant Support Guide)

यदि आपको संदिग्ध SMS या फर्जी कॉल्स की शिकायत दर्ज करने के लिए संचार साथी पोर्टल खोजना हो, तो Google पर इन 4 बातों का ध्यान रखें:

1

चरण 1: चक्षु पोर्टल और मर्चेंट सुरक्षा कीवर्ड खोजें

सर्च बार में केवल यह लिखें: `sanchar saathi chakshu report suspected fraud`

2

"Sponsored" या "Ad" लिखे विज्ञापनों को छोड़ें

सर्च में सबसे ऊपर दिखने वाले प्रायोजित विज्ञापनों पर क्लिक न करें। असली सरकारी पोर्टल का लिंक सामान्य सर्च परिणामों में होता है।

3

चरण 3: संचार साथी आधिकारिक सरकारी डोमेन देखें

हमेशा देखें कि वेबसाइट का पता `https://sancharsaathi.gov.in` ही हो। सरकारी पोर्टल्स के अंत में हमेशा `.gov.in` होता है।

4

सर्च पेज पर दिखने वाले नंबरों पर फोन न करें

Google सर्च में सीधे दिख रहे किसी भी मोबाइल नंबर पर कभी फोन न लगाएं। केवल आधिकारिक पोर्टल पर जाकर सीधे ऑनलाइन शिकायत फॉर्म भरें।

🔍 अध्याय 6 के सत्यापित आधिकारिक स्रोत (Official Sources):

- **दूरसंचार विभाग (DoT) संचार साथी पोर्टल:** `https://sancharsaathi.gov.in`
- **चक्षु (Chakshu) संदिग्ध संचार रिपोर्टिंग सुविधा:** `https://sancharsaathi.gov.in/sfc/`
- **NPCI मर्चेंट QR सुरक्षा दिशा-निर्देश:** `https://www.npci.org.in`

अध्याय 7 • समस्या समाधान (Failed Transactions)

जब Payment में समस्या आए

खाते से पैसे कट गए लेकिन सामने वाले को नहीं मिले? घबराएं नहीं — जानिए पैसा कहाँ अटका है, कब तक वापस आएगा और देरी होने पर बैंक से ₹100 प्रतिदिन हर्जाना पाने का आपका अधिकार।

पैसे कट गए पर सामने वाले को नहीं मिले — ऐसा क्यों होता है?

जब आप UPI से किसी को पैसे भेजते हैं, तो यह कोई जादू नहीं है बल्कि इंटरनेट पर 3 अलग-अलग कंप्यूटर सर्वरों का एक तालमेल है:

• **आपका बैंक (Remitter Bank):** जो आपके खाते से पैसे काटता है।

• **NPCI का UPI स्विच:** जो भारत सरकार का केंद्रीय सर्वर है और पैसों को सही दिशा दिखाता है।

• **सामने वाले का बैंक (Beneficiary Bank):** जो सामने वाले के खाते में पैसे जमा करता है।

यदि इन तीनों में से किसी भी एक बैंक का सर्वर धीमा हो, इंटरनेट कमजोर हो या तकनीकी रुकावट आ जाए, तो लेन-देन बीच में रुक जाता है। इसे बैंकिंग की भाषा में **Failed Transaction** या **Deemed Approved Transaction** कहते हैं।

सबसे बड़ा सुकून

आपका पैसा कहीं गायब नहीं होता!

यह बात हमेशा याद रखें: बैंकिंग नेटवर्क में पैसा कभी हवा में गायब नहीं हो सकता। यदि आपके खाते से पैसे कट गए हैं और सामने वाले को नहीं मिले, तो वह पैसा सुरक्षित एस्क्रो/बैंकिंग चैनल में जमा रहता है। या तो वह सामने वाले के खाते में पूरा जमा होगा, या फिर आपके ही बैंक खाते में अपने आप वापस (**Auto-Reversal**) आ जाएगा।

केस स्टडी: मनोज का अटका किराया और ₹300 का मुआवजा

मनोज ने 1 तारीख की शाम को अपने मकान मालिक को ₹4,500 का किराया Google Pay से भेजा। बैंक से पैसे कटने का SMS आ गया, लेकिन मकान मालिक ने कहा: *"भाई, मेरे पास तो कोई पैसा नहीं आया, स्क्रीन पर Pending दिख रहा है।"*

मनोज की समझदारी

मनोज ने दोबारा पैसे नहीं भेजे, बल्कि सही नियम अपनाया

अक्सर लोग घबराहट में तुरंत दोबारा ₹4,500 भेज देते हैं, जिससे उनके ₹9,000 कट जाते हैं। लेकिन मनोज ने शांति रखी। उसने Google Pay में जाकर उसी ट्रांजैक्शन पर **"Raise Dispute"**

का बटन दबाया और अपना 12-अंकों का **UTR Number** नोट कर लिया।

दिन 1 (T) पेमेंट अटका, इन-ऐप कंप्लेंट दर्ज हुई।

दिन 2 (T+1) अगला कार्यदिवस बीता, तकनीकी जांच जारी रही।

दिन 5 4 दिन बाद मनोज के खाते में ₹4,500 का पूरा रिफंड आ गया। और साथ ही, **RBI के TAT नियम** के अनुसार 3 दिन की देरी के लिए बैंक ने बिना मांगे **₹300 का अतिरिक्त हर्जाना (Compensation)** भी मनोज के खाते में स्वतः क्रेडिट किया!

RBI का समय-सीमा नियम (Turn Around Time - TAT)

भारतीय रिज़र्व बैंक ने अपने आधिकारिक सर्कुलर (*Circular No. DPSS.CO.PD No.629/02.01.014/2019-20*) के तहत फेल्ड यूपीआई लेन-देन के लिए कड़े नियम बनाए हैं:

RBI आधिकारिक नियम

T + 1 कार्यदिवस का ऑटो-रिवर्सल नियम

T = Transaction का दिन
T + 1 = अगला कार्यदिवस (Working Day)

यदि आपका पैसा कट गया और सामने वाले को नहीं मिला, तो बैंक के पास उस पैसे को वापस आपके खाते में लौटाने के लिए अधिकतम **T + 1 कार्यदिवस** का समय होता है।

हर्जाने का कानूनी अधिकार

देरी होने पर ₹100 प्रति दिन का हर्जाना (Compensation)

यदि बैंक T + 1 दिन के भीतर आपका पैसा वापस नहीं लौटा पाता है, तो जितने दिन की भी देरी होगी, बैंक को **₹100 प्रतिदिन** के हिसाब से हर्जाना आपके खाते में जमा करना होगा।

🎯 **सबसे खास बात:** इसके लिए आपको अलग से कोई आवेदन नहीं देना होता। RBI के नियम अनुसार बैंक को यह हर्जाना अपने आप (*Suo Motu*) आपके खाते में क्रेडिट करना अनिवार्य है।

पेमेंट अटकने पर 4-चरणीय समाधान प्रक्रिया

जब भी किसी पेमेंट में समस्या आए, तो शांति से इस क्रम का पालन करें:

1

Transaction Status जांचें और इंतजार करें

अपने UPI ऐप के **History** सेक्शन में जाएं। अगर स्टेटस *Pending* या *Processing* है, तो 2 से 3 घंटे इंतजार करें। जब तक अंतिम स्थिति न आए, उसी व्यक्ति को दोबारा पैसे न भेजें।

2

ऐप के अंदर Dispute दर्ज करें (UDIR सिस्टम)

उसी फेल्ड पेमेंट पर टैप करें और **"Having an issue"** या **"Raise Dispute"** चुनें। NPCI का UDIR (Unified Dispute and Issue Resolution) सिस्टम सीधे दोनों बैंकों के सर्वर से जांच शुरू कर देता है।

3

12-अंकों का UTR नंबर लेकर बैंक को लिखित दें

यदि T + 1 दिन बीतने पर भी पैसा न आए, तो बैंक से आए SMS में लिखा 12-अंकों का **UTR Number** लेकर अपने बैंक की आधिकारिक वेबसाइट पर ऑनलाइन शिकायत दर्ज करें।

4

RBI Banking Ombudsman (लोकपाल) में शिकायत

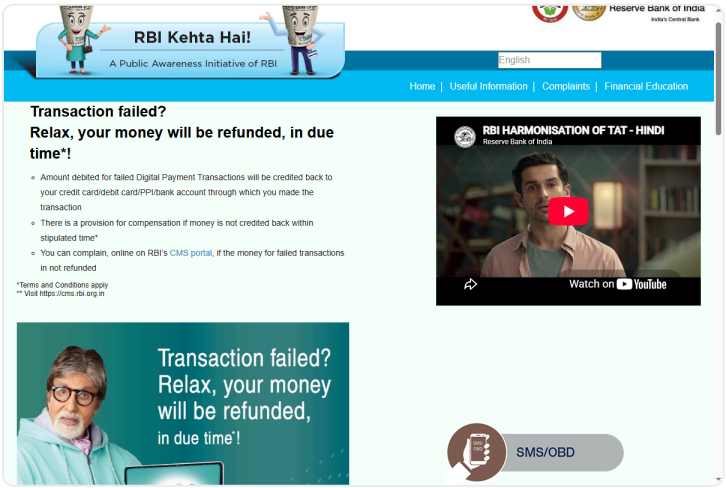
यदि बैंक 30 दिनों के भीतर आपकी शिकायत का संतोषजनक समाधान न करे, तो रिज़र्व बैंक के ऑनलाइन पोर्टल `cms.rbi.org.in` पर मुफ्त बैंकिंग लोकपाल शिकायत दर्ज करें।

RBI Kehta Hai: आधिकारिक समय-सीमा निर्देश

भारतीय रिज़र्व बैंक अपने जागरूकता पोर्टल पर फेल्ड ट्रांजैक्शन और मुआवजे के नियम को साफ शब्दों में समझाता है:

rbikehtahai.rbi.org.in

RBI आधिकारिक जागरूकता



📌 RBI विफल लेनदेन (TAT Compensation) निर्देश से 2 मुख्य सीख:

1. **स्वतः रिफंड का नियम:** फेल्ड ट्रांजैक्शन की स्थिति में पैसा निर्धारित समय में अपने आप ग्राहक के खाते में वापस आ जाना चाहिए।
2. **देरी पर हर्जाना:** निर्धारित समय सीमा से अधिक समय लगने पर ग्राहक को प्रतिदिन ₹100 का हर्जाना पाने का कानूनी अधिकार है।

अध्याय 7: विफल लेनदेन और मुआवजे से जुड़े

सवाल (Failed Payment FAQs)

Q1: क्या T + 1 दिन में शनिवार और रविवार भी गिने जाते हैं?

उत्तर: नहीं। 'T + 1 कार्यदिवस' (Working Day) का मतलब है बैंक खुलने का दिन। यदि आपने शुक्रवार रात को पेमेंट किया और शनिवार/रविवार को बैंक की छुट्टी है, तो सोमवार को T+1 माना जाएगा।

Q2: अगर पेंडिंग पेमेंट 2 घंटे बाद अचानक सफल (Success) हो जाए तो?

उत्तर: कई बार बैंक सर्वर धीरे होने के कारण थोड़ी देर बाद पैसा सामने वाले के खाते में पहुँच जाता है। इसलिए जब तक स्टेटस क्लियर न हो, दोबारा नया पेमेंट न करें ताकि दो बार पैसे न कटें।

Q3: क्या ₹100 का मुआवजा पाने के लिए मुझे बैंक में अलग से आवेदन देना होगा?

उत्तर: नहीं। RBI के नियमों के अनुसार बैंक को यह राशि बिना मांगे सीधे आपके खाते में क्रेडिट करनी होती है। यदि बैंक हर्जाना न दे, तो आप बैंक से इसकी मांग कर सकते हैं या लोकपाल में शिकायत कर सकते हैं।

Q4: UTR Number क्या होता है और यह कहाँ मिलता है?

उत्तर: UTR (Unique Transaction Reference) 12 अंकों का एक विशेष नंबर होता है जो हर UPI लेन-देन को पहचान देता है। यह आपके बैंक ऐप की पासबुक, ट्रांजैक्शन हिस्ट्री और बैंक से आए SMS में लिखा होता है।

Q5: क्या गलती से किसी दूसरे के खाते में चले गए पैसे पर भी T+1 नियम लागू होता है?

उत्तर: नहीं। T+1 नियम केवल 'तकनीकी खराबी' से फंसे पैसों पर लागू होता है। अगर आपने खुद गलती से किसी गलत व्यक्ति को पैसे भेज दिए हैं, तो यह बैंक की तकनीकी गलती नहीं है। इसके लिए आपको तुरंत बैंक में लिखित आवेदन देकर रिसीवर के बैंक से पैसे होल्ड कराने का अनुरोध करना होगा।

पेमेंट फंसने पर: क्या करें और क्या न करें

✅ क्या करें (Do's)

- पैसे कटने पर तुरंत दोबारा पेमेंट न दोहराएं; पहले हिस्ट्री में स्टेटस देखें।
- ऐप के अंदर दिए गए 'Raise Dispute' विकल्प से तुरंत कंप्लेंट दर्ज करें।
- हर फेल्ड पेमेंट का 12-अंकों का UTR नंबर अपनी डायरी या फोन में नोट कर लें।
- T+1 दिन के बाद भी पैसा न आने पर अपने बैंक की आधिकारिक शाखा से संपर्क करें।

❌ क्या न करें (Don'ts)

• पैसे अटकने पर Google सर्च में दिख रहे किसी भी अनजान हेल्पलाइन नंबर पर फोन न करें।

• रिफंड पाने के लिए किसी अनजान कॉलर के कहने पर AnyDesk या स्क्रीन शेयर ऐप न डालें।

• रिफंड लेने के नाम पर कभी किसी लिंक पर जाकर अपना UPI PIN न डालें।

• पेंडिंग पेमेंट को नजरअंदाज न करें; जब तक स्टेटस क्लियर न हो, जांच करते रहें।

Google पर T+1 ऑटो-रिवर्सल नियम कैसे खोजें? (TAT Guidelines)

यदि बैंक में 30 दिन तक सुनवाई न होने पर आपको RBI लोकपाल (Banking Ombudsman) में शिकायत करनी हो, तो Google पर इन 4 बातों का ध्यान रखें:

1

चरण 1: विफल ट्रांजेक्शन और ऑटो-रिवर्सल कीवर्ड खोजें

सर्च बार में केवल यह लिखें: `RBI CMS portal file banking ombudsman complaint`

2

चरण 2: विज्ञापनों को छोड़ें और rbi.org.in TAT सर्कुलर देखें

सर्च में सबसे ऊपर दिखने वाले प्रायोजित विज्ञापनों पर क्लिक न करें। असली RBI लोकपाल पोर्टल का लिंक सामान्य सर्च में होता है।

3

चरण 3: रिज़र्व बैंक के आधिकारिक डोमेन की पुष्टि करें

हमेशा देखें कि वेबसाइट का पता `https://cms.rbi.org.in` ही हो।

4

चरण 4: गूगल सर्च पर दिखने वाले फर्जी हेल्पलाइन नंबरों पर कॉल न करें

सर्च इंजन में सीधे दिख रहे किसी भी मोबाइल नंबर पर कभी फोन न लगाएं। केवल आधिकारिक पोर्टल पर जाकर सीधे ऑनलाइन शिकायत फॉर्म भरें।

🔍 अध्याय 7 के सत्यापित आधिकारिक स्रोत (Official Sources):

- **RBI TAT और ग्राहक मुआवजा सर्कुलर:** Circular No. `DPSS.CO.PD No.629/02.01.014/2019-20` (`https://www.rbi.org.in`)
- **NPCI UDIR (Dispute Resolution) फ्रेमवर्क:** `https://www.npci.org.in`
- **RBI CMS ऑनलाइन लोकपाल पोर्टल:** `https://cms.rbi.org.in`

अध्याय 8 • आपातकालीन कार्रवाई (Emergency Action Plan)

UPI Fraud की शिकायत कैसे करें

धोखाधड़ी होने पर घबराने या खुद को कोसने के बजाय इन मिनटों में सही कदम उठाएं। जानिए साइबर अपराध का 'गोल्डन ऑवर', शिकायत के 3 सरकारी रास्ते और पैसे वापस पाने की वास्तविक प्रक्रिया।

साइबर सुरक्षा में 'गोल्डन ऑवर' (Golden Hour) क्या है?

जब किसी व्यक्ति के साथ ऑनलाइन ठगी या अनधिकृत वित्तीय लेनदेन होता है, तो घटना के शुरुआती **2 से 3 घंटे** को सुरक्षा एजेंसियां और बैंक **'गोल्डन ऑवर' (Golden Hour)** कहते हैं।

यह समय इतना महत्वपूर्ण क्यों है? आइए ठगों के पैसे निकालने के तरीके (Modus Operandi) को समझें:

> **0 से 15 मिनट**
>
> **पैसा ठग के पहले खाते में:** आपके बैंक खाते से पैसे कटकर ठग के किराये के खाते (Mule Account) में पहुँचते हैं।

> **15 से 60 मिनट**

पैसों की लेयरिंग (Layering): ठग पकड़े जाने से बचने के लिए उस पैसे को तुरंत 5 से 10 अलग-अलग वॉलेट या खातों में छोटे टुकड़ों में बांट देता है।

2 से 3 घंटे के भीतर

नकद निकासी (ATM Withdrawal): ठग या उसके साथी किसी दूरदराज के ATM या माइक्रो-एटीएम से नकद पैसे निकाल लेते हैं। एक बार नकद निकल जाने के बाद पैसा वापस पाना बेहद कठिन हो जाता है।

यदि आप इस **गोल्डन ऑवर** के दौरान आधिकारिक प्रणाली पर शिकायत दर्ज करा देते हैं, तो भारत सरकार का वित्तीय फ्रॉड सिस्टम (CFRMS) तुरंत हरकत में आता है और ठग के बैंक खाते पर **Lien Mark (फ्रीज)** लगा देता है, जिससे पैसा ATM से नहीं निकाला जा सकता!

केस स्टडी: राजेश जी की 25 मिनट की सतर्कता और ₹45,000 की बचत

लखनऊ के राजेश जी को एक शाम बिजली विभाग के नाम से फर्जी मैसेज आया कि रात 9:30 बजे बिजली काट दी जाएगी। घबराहट में उन्होंने मैसेज में दिए लिंक पर क्लिक किया और ₹10 का रीचार्ज करने के चक्कर में उनके खाते से **₹45,000** कट गए।

केस स्टडी से सीख

राजेश जी ने समय गंवाए बिना 3 सही कदम उठाए:

राजेश जी (मन में): *"मैं घबराकर रोने नहीं बैठूंगा। तुरंत बैंक और साइबर पोर्टल को अलर्ट करना होगा!"*

मिनट 5

राजेश जी ने बैंक के SMS से 12 अंकों का **UTR Number** तुरंत डायरी में लिखा।

मिनट 12

अपने UPI ऐप (Google Pay) के Transaction History में जाकर **"Report Fraud"** दर्ज किया।

मिनट 25

राजेश जी ने तुरंत राष्ट्रीय साइबर अपराध पोर्टल (**cybercrime.gov.in**) पर जाकर *"Report Financial Fraud"* में शिकायत दर्ज की और 12-अंकों का UTR नंबर भर दिया।

नतीजा: शिकायत दर्ज होते ही सिस्टम ने ठग के उस Mule Account को तुरंत फ्रीज कर दिया। ठग केवल ₹5,000 निकाल पाया था, जबकि **₹40,000 बैंक खाते में ही लॉक हो गए**। कानूनी प्रक्रिया पूरी होने के बाद राजेश जी को उनकी बची हुई रकम वापस मिल गई!

शिकायत करने से पहले ये 4 जानकारियां एक कागज पर लिख लें

शिकायत दर्ज करते समय सिस्टम आपसे सटीक विवरण मांगता है। यदि आप पहले से यह जानकारी तैयार रखेंगे, तो आपका कीमती समय बचेगा:



1. 12-अंकों का UTR Number

आपके बैंक से पैसे कटने वाले SMS या UPI ऐप की रसीद में लिखा 12 अंकों का UTR या UPI Ref No सबसे जरूरी पहचान संख्या है।



2. सही समय और तारीख

ट्रांजैक्शन किस तारीख को और किस मिनट पर हुआ (उदा. 08/11/2026 शाम 05:42 बजे)।



3. ठग का UPI ID या मोबाइल नंबर

जिस UPI ID, मर्चेंट नाम या बैंक खाते में पैसे ट्रांसफर हुए, उसका पूरा विवरण और स्क्रीनशॉट।

4. फ्रॉड का स्क्रीनशॉट व साक्ष्य

ठग के साथ हुआ WhatsApp चैट, फर्जी SMS, या फर्जी ऐप का नाम व स्क्रीनशॉट सुरक्षित रखें।

धोखाधड़ी की शिकायत के 3 आधिकारिक रास्ते

UPI ठगी होने पर बिना एक मिनट गंवाए इन तीनों जगहों पर शिकायत दर्ज करें:

रास्ता 1 • तुरंत (पहले 5 से 10 मिनट में)

अपने UPI App में इन-ऐप रिपोर्ट करें

जिस ऐप (PhonePe, Google Pay, Paytm, BHIM आदि) से पैसे कटे हैं, उसी ऐप के अंदर ट्रांजैक्शन रिपोर्ट करने की आधिकारिक व्यवस्था होती है:

1. UPI ऐप खोलें और **History / Transaction History** में जाएं।
2. धोखाधड़ी वाले ट्रांजैक्शन पर टैप करें।
3. नीचे दिए गए **"Report Fraud"**, **"Having an Issue"** या **"Raise Dispute"** पर क्लिक करें।

4. कारण में *"Unauthorized Transaction / Fraud"* चुनें और विवरण दर्ज करें।

🌐 **आधिकारिक पोर्टल:** अपने ऐप की आधिकारिक वेबसाइट के सपोर्ट पेज पर जाएं।

🔍 **सटीक Google Search:** `[App का नाम] official support report fraud`

रास्ता 2 • पहले 24 घंटों में

अपने Bank को लिखित व ऑनलाइन सूचित करें

आपका बैंक आपके खाते का मुख्य संरक्षक है। बैंक को तुरंत सूचित करके आगे का नुकसान रोकें:

1. बैंक की आधिकारिक वेबसाइट या अधिकृत मोबाइल ऐप पर लॉगिन करें।
2. **"Report Unauthorized Transaction"** या **"Debit Freeze"** विकल्प चुनें।
3. यदि आपका UPI PIN लीक हो गया है, तो बैंक से कहकर अपना **UPI Access तुरंत ब्लॉक करवाएं** और डेबिट कार्ड हॉटलिस्ट करें।
4. बैंक से अपनी लिखित शिकायत का **Complaint Reference Ticket Number** अवश्य नोट करें।

🌐 **आधिकारिक पोर्टल:** बैंक की पासबुक या आधिकारिक मोबाइल ऐप में दिया अधिकृत पोर्टल।

🔍 **सटीक Google Search:** `[बैंक का नाम] official website report unauthorized debit`

रास्ता 3 • कानूनी कार्रवाई (National Cybercrime Portal)

राष्ट्रीय साइबर क्राइम रिपोर्टिंग पोर्टल (cybercrime.gov.in)

यह भारत सरकार के गृह मंत्रालय (Ministry of Home Affairs - MHA) का केंद्रीय पोर्टल है जो देश भर के सभी बैंकों, यूपीआई ऐप्स और पुलिस थानों के नोडल अधिकारियों से 24x7 सीधे जुड़ा हुआ है:

1. वेबसाइट खोलें: **https://www.cybercrime.gov.in**
2. होमपेज पर **"Report Financial Fraud"** (वित्तीय धोखाधड़ी रिपोर्ट करें) पर क्लिक करें।
3. अपने मोबाइल नंबर और OTP से लॉगिन करें।
4. घटना की तारीख, समय, 12 अंकों का **UTR Number** और ठग का विवरण भरें।
5. शिकायत सबमिट होने पर मिलने वाला **Acknowledgment Number** सुरक्षित रखें। इस नंबर से आप भविष्य में अपनी जांच की स्थिति ट्रैक कर सकते हैं।

🌐 **आधिकारिक वेबसाइट:** https://www.cybercrime.gov.in

🔍 **सटीक Google Search:** `national cyber crime reporting portal official website report fraud`

अत्यंत जरूरी चेतावनी: Google पर हेल्पलाइन नंबर कभी न खोजें!

धोखाधड़ी का शिकार होने के बाद लोग घबराहट में सबसे बड़ी गलती यह करते हैं कि वे Google पर जाकर *"UPI Customer Care Number"*, *"Google Pay Refund Helpline"* या *"Cyber Cell Helpline Contact"* सर्च करने लगते हैं।

साइबर ठगों का 'सर्च इंजन' जाल:

शातिर ठग Google पर पैसे देकर अपने फर्जी मोबाइल नंबरों के विज्ञापन चलवाते हैं। जब आप उस नंबर पर कॉल करते हैं, तो सामने बात करने वाला व्यक्ति खुद को बैंक या साइबर सेल का बड़ा अफसर बताता है और कहता है: *"सर, आपका रिफंड प्रोसेस हो रहा है, बस आप अपने फोन में AnyDesk ऐप डाउनलोड कर लीजिए या इस लिंक पर ₹1 का टोकन पेमेंट कीजिए।"*

नतीजा यह होता है कि जो बचे-खुचे पैसे आपके खाते में थे, ठग उन्हें भी खाली कर देता है!

नियम याद रखें: कभी भी Google सर्च पर मिले किसी मोबाइल नंबर पर कॉल न करें। शिकायत हमेशा आधिकारिक वेबसाइट के अंदर

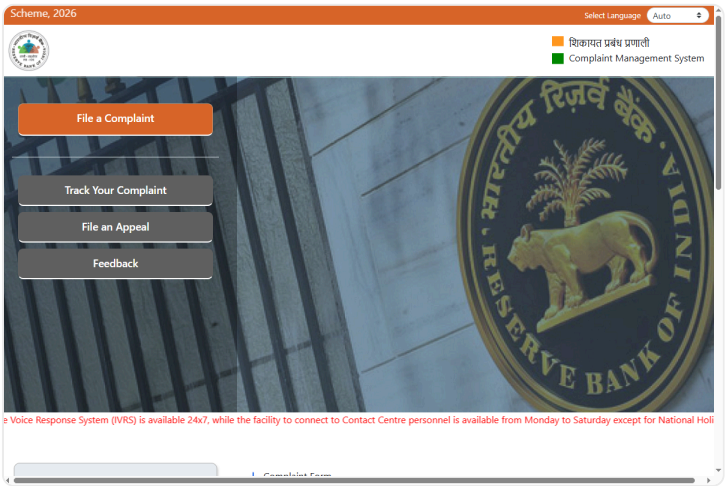
जाकर लिखित फॉर्म में या बैंक की अधिकृत शाखा में ही दर्ज कराएं।

RBI CMS: आधिकारिक एकीकृत लोकपाल शिकायत पोर्टल

यदि बैंक या पेमेंट ऐप द्वारा 30 दिनों के भीतर आपकी धोखाधड़ी की शिकायत पर उचित कार्रवाई न की जाए, तो Reserve Bank of India के आधिकारिक CMS पोर्टल पर ऑनलाइन लोकपाल शिकायत दर्ज की जाती है:

cms.rbi.org.in

RBI आधिकारिक शिकायत पोर्टल



📌 रिज़र्व बैंक के आधिकारिक CMS पोर्टल से 2 मुख्य सीख:

1. **File a Complaint:** इस पोर्टल पर जाकर आप बैंक के खिलाफ मुफ्त में लोकपाल शिकायत दर्ज कर सकते हैं। इसके लिए किसी वकील या दलाल की जरूरत नहीं होती।

2. **Track Your Complaint:** शिकायत दर्ज होने के बाद मिले टोकन नंबर से आप घर बैठे जांच की प्रगति और बैंक के जवाब को ऑनलाइन देख सकते हैं।

अध्याय 8: साइबर क्राइम व पुलिस रिपोर्टिंग से जुड़े

सवाल (Cyber Complaint FAQs)

Q1: क्या साइबर पोर्टल पर शिकायत करने के लिए मुझे पुलिस थाने जाना पड़ेगा?

उत्तर: वित्तीय फ्रॉड (पैसे कटने की ठगी) के लिए तुरंत थाने जाने की जरूरत नहीं होती। आप सीधे `cybercrime.gov.in` पर घर बैठे ऑनलाइन शिकायत दर्ज कर सकते हैं। यह पोर्टल सीधे आपके जिले की साइबर पुलिस और संबंधित बैंकों को डिजिटल सूचना भेज देता है।

Q2: अगर मेरे साथ रात के 2 बजे फ्रॉड हो जाए, तो क्या सुबह तक इंतजार करना चाहिए?

उत्तर: बिल्कुल नहीं! सुबह तक का इंतजार ठग को पैसे निकालने का पूरा मौका दे देगा। `cybercrime.gov.in` पोर्टल 24 घंटे और सातों दिन चालू रहता है। रात को ही तुरंत शिकायत दर्ज करें ताकि सुबह बैंक खुलने से पहले ही ठग का खाता फ्रीज हो जाए।

Q3: क्या बैंक यह कहकर पल्ला झाड़ सकता है कि 'आपने खुद UPI PIN डाला था'?

उत्तर: यदि आपने धोखाधड़ी या सोशल इंजीनियरिंग के तहत धोखे से PIN डाला है, तो भी बैंक को आपकी शिकायत दर्ज करके संबंधित नोडल बैंक को तत्काल लीन मार्क (फ्रीज) का अनुरोध भेजना अनिवार्य है। यदि बैंक सहयोग न करे, तो आप 30 दिन बाद RBI Ombudsman में शिकायत कर सकते हैं।

Q4: अगर ठग ने पैसे तुरंत ATM से नकद निकाल लिए हों, तो क्या होगा?

उत्तर: यदि पैसा नकद निकल चुका है, तो बैंक स्तर पर तत्काल फ्रीज संभव नहीं हो पाता। ऐसे मामलों में साइबर पुलिस ठग के उस Mule Account के मालिक (जिसके नाम पर खाता खुला था) और ATM के CCTV फुटेज के आधार पर कानूनी कार्रवाई और रिकवरी करती है।

Q5: साइबर पोर्टल पर Acknowledgment Number मिलने के बाद मुझे क्या करना चाहिए?

उत्तर: उस Acknowledgment Number की PDF रसीद डाउनलोड करें और उसकी एक कॉपी लेकर अपने बैंक की गृह शाखा (Home Branch) में जाएं। शाखा प्रबंधक (Branch Manager) को एक लिखित पत्र देकर रिसीविंग लें कि आपने सरकारी पोर्टल पर आधिकारिक शिकायत दर्ज कर दी है।

धोखाधड़ी होने पर: क्या करें और क्या न करें

✅ क्या करें (Do's)	❌ क्या न करें (Don'ts)
धोखाधड़ी होते ही **2-3 घंटे के भीतर** साइबर पोर्टल पर शिकायत दर्ज करें।	शर्म या घबराहट के कारण परिजनों से बात छुपाकर समय न गंवाएं।
बैंक SMS और UPI ऐप से 12 अंकों का **UTR Number** नोट करें।	Google सर्च पर कस्टमर केयर नंबर ढूंढकर किसी अनजान को फोन न लगाएं।
अपने UPI ऐप के अंदर **"Report Fraud"** तुरंत दबाएं।	फोन पर रिफंड का झांसा देने वाले के कहने पर AnyDesk या TeamViewer डाउनलोड न करें।
यदि PIN लीक हुआ है, तो बैंक से कहकर अपना UPI तुरंत ब्लॉक करवाएं।	ठग के कहने पर रिफंड पाने के लिए ₹1 का भी नया ट्रांसफर न करें।
दर्ज शिकायत का **Acknowledgment Number** संभाल कर रखें।	बिना आधिकारिक रिसीविंग लिए बैंक से खाली हाथ वापस न लौटें।

Google पर आधिकारिक साइबर अपराध पोर्टल कैसे खोजें? (Cybercrime Portal Guide)

यदि आपको राष्ट्रीय साइबर क्राइम पोर्टल पर जाना है, तो सर्च इंजन पर सुरक्षित रहने के लिए इस प्रक्रिया का पालन करें:

🔍 `"national cyber crime reporting portal official website report fraud"`

1

चरण 1: साइबर पोर्टल को कोट्स (Quotes) में खोजें

ऊपर दिया गया वाक्य कोट्स के साथ सर्च बार में डालें ताकि सर्च इंजन केवल असली पेज दिखाए।

2

'Sponsored' विज्ञापनों को छोड़ दें

सर्च रिजल्ट में सबसे ऊपर दिखने वाले विज्ञापनों पर कभी क्लिक न करें। असली सरकारी पेज बिना विज्ञापन का होता है।

3

gov.in डोमेन की जांच करें

वेबसाइट के पते में हमेशा **cybercrime.gov.in** और बाईं तरफ ताले का निशान (HTTPS) जरूर देखें।

🔍 अध्याय 8 के सत्यापित आधिकारिक स्रोत (Official Sources)

- **National Cyber Crime Reporting Portal:** https://www.cybercrime.gov.in (गृह मंत्रालय, भारत सरकार)
- **RBI एकीकृत लोकपाल शिकायत पोर्टल (CMS):** https://cms.rbi.org.in

• **NPCI आधिकारिक शिकायत निवारण दिशानिर्देश:**
https://www.npci.org.in

अध्याय 9 • नया खतरा (Artificial Intelligence)

नकली आवाज़ और नकली Video Call (AI)

जब फोन पर आपके बेटे या रिश्तेदार की हूबहू आवाज सुनाई दे और सामने पुलिस की वर्दी में अफसर दिखे — जानिए AI ठगी का यह नया चेहरा, 'Digital Arrest' का सच और इससे बचने के अचूक व्यावहारिक उपाय।

AI Voice Cloning: आवाज़ की हूबहू डिजिटल नकल

आज आधुनिक **Artificial Intelligence (AI)** तकनीक इतनी विकसित हो चुकी है कि किसी भी व्यक्ति की सोशल मीडिया वीडियो, रील या साधारण ऑडियो कॉल से केवल **3 से 5 सेकंड** की आवाज़ का नमूना लेकर उसकी हूबहू आवाज़ बनाई जा सकती है।

इसे साइबर सुरक्षा की भाषा में **AI Voice Cloning** कहते हैं। कंप्यूटर सॉफ्टवेयर इंसान की आवाज़ की टोन, पिच, बोलने की गति और यहां तक कि सांस लेने के अंदाज को भी पूरी तरह कॉपी कर लेता है।

⚠ यह तकनीक कैसे काम करती है?

3 चरणों में रची जाती है आवाज की साजिश:

• **आवाज चुराना (Sample Collection):** ठग Facebook, Instagram या YouTube से आपके बच्चों की छोटी-छोटी वीडियो क्लिप्स से आवाज का नमूना डाउनलोड करते हैं।

• **AI में टेक्स्ट डालना (Voice Synthesis):** ठग कंप्यूटर में मनचाहा भावनात्मक वाक्य लिखते हैं, जैसे — *"पापा, मुझे बचा लीजिए, मेरा बहुत बड़ा एक्सीडेंट हो गया है!"*

• **हूबहू कॉल जनरेट करना:** सॉफ्टवेयर उस लिखे हुए वाक्य को बिल्कुल आपके बच्चे की रोती हुई आवाज में बदलकर आपके फोन पर कॉल मिला देता है।

केस स्टडी: शर्मा जी का फोन और 1 सवाल से खुली AI की पोल

भोपाल के 58 वर्षीय रमेश शर्मा जी दोपहर में अपने दफ्तर में बैठे थे। अचानक एक अनजान नंबर से कॉल आई। जैसे ही उन्होंने फोन उठाया, दूसरी तरफ उनके बेटे रोहित की रोती हुई कांपती आवाज आई:

केस स्टडी से सीख

बेंगलुरु में रहने वाले बेटे के नाम पर AI कॉल:

आवाज (बेटे जैसी): *"पापा! मैं बहुत बड़ी मुसीबत में फंस गया हूँ... मेरे दोस्त की गाड़ी से एक बच्चे को टक्कर लग गई है।*

पुलिस ने मुझे पकड़ लिया है। थानेदार साहब बात कर रहे हैं, जो कहें मान लीजिए नहीं तो जेल भेज देंगे!"

नकली पुलिस इंस्पेक्टर (कड़क आवाज): *"शर्मा जी, आपका बेटा हमारे कब्जे में है। केस रफा-दफा करना है तो 10 मिनट के अंदर इस UPI ID पर ₹50,000 भेजिए। फोन काटा तो सीधे जेल में बंद कर देंगे!"*

शर्मा जी के हाथ कांपने लगे। बेटे की आवाज में इतना दर्द और घबराहट थी कि कोई भी पिता तुरंत पैसे भेज देता। लेकिन तभी शर्मा जी को अपने परिवार का सुरक्षा नियम याद आया।

शर्मा जी ने हिम्मत करके पूछा: *"रोहित बेटा, अगर तुम बोल रहे हो, तो बताओ हमारे घर के कुत्ते का क्या नाम है?"*

ठग की तरफ से सन्नाटा: सामने वाला सकपका गया और गालियां देते हुए फोन काट दिया!

नतीजा: शर्मा जी ने तुरंत रोहित के असली नंबर पर कॉल मिलाया। रोहित अपने ऑफिस में शांति से लंच कर रहा था और सब कुछ पूरी तरह ठीक था! शर्मा जी के 1 समझदारी भरे सवाल ने उनके ₹50,000 और मानसिक शांति बचा ली।

Deepfake Video Call और 'Digital Arrest' का सच

ठग केवल आवाज ही नहीं, बल्कि **Deepfake Video** तकनीक से किसी भी व्यक्ति का चेहरा लाइव वीडियो कॉल पर बदल सकते हैं। वे नकली वर्दी पहनकर और पीछे पुलिस थाने या सुप्रीम कोर्ट का फर्जी बैकग्राउंड लगाकर लोगों को वीडियो कॉल करते हैं।

⚖️ भारतीय कानून में 'Digital Arrest' का कोई अस्तित्व नहीं है!

भारत के संविधान, CrPC या किसी भी कानून में **"Digital Arrest"** नाम की कोई धारा या व्यवस्था नहीं है।

1. पुलिस कभी Video Call पर अरेस्ट नहीं करती: किसी भी नागरिक की गिरफ्तारी के लिए पुलिस अधिकारी को कानूनी वारंट के साथ शारीरिक रूप से उपस्थित होना पड़ता है।

2. कोई भी जांच एजेंसी UPI से पैसे नहीं मांगती: CBI, ED, Income Tax, कस्टम विभाग या राज्य पुलिस कभी भी केस बंद करने, वेरिफिकेशन करने या जमानत देने के लिए निजी बैंक खाते या UPI पर पैसे नहीं मांगती।

3. कैमरा चालू रखने का दबाव ठगी का सबूत है: ठग कहते हैं *"आप कमरे में अकेले बैठिए और कैमरा 24 घंटे चालू रखिए।"* ऐसा वे केवल

इसलिए करते हैं ताकि पीड़ित अपने रिश्तेदारों या असली पुलिस से बात न कर सके।

तुलना: असली कॉल बनाम AI ठगी की कॉल

जब भी कोई संदिग्ध या डरावनी कॉल आए, तो इन 4 बड़े अंतरों को तुरंत पहचानें:

पहचान का बिंदु	✅ असली आपातकालीन कॉल	❌ AI नकली कॉल (Scam)
कॉल की शुरुआत	सामान्य बातचीत, परिस्थिति को शांत मन से समझाने की कोशिश।	शुरुआत से ही अत्यधिक रोने, चीखने या पुलिस सायरन की आवाज।
कॉल काटने की छूट	कहते हैं: *"हां, आप फोन काटकर 2 मिनट में वापस मिला लीजिए।"*	धमकी देते हैं: *"फोन काटा तो तुरंत जेल भेज देंगे या मार देंगे!"*
पैसों की मांग	सीधे अस्पताल के काउंटर या आधिकारिक प्रक्रिया की बात होती है।	तुरंत किसी अनजान तीसरे व्यक्ति के UPI ID पर पैसे ट्रांसफर करने की जिद।
व्यक्तिगत सवाल	घर की पुरानी बातें और निजी सवालों का तुरंत सही जवाब देते हैं।	पारिवारिक सवाल पूछते ही ठग बहाना बनाने लगता है या गाली देकर फोन काट देता है।

AI ठगी से बचने के 3 अचूक सुरक्षा नियम

1

पारिवारिक सीक्रेट कोड वर्ड (Family Code Word) बनाएं

आज ही अपने परिवार (माता-पिता, बच्चों और जीवनसाथी) के साथ बैठकर एक गुप्त शब्द या सवाल तय करें (जैसे बचपन के किसी पालतू जानवर का नाम या ननिहाल का कोई पुराना किस्सा)। जब भी कोई बच्चा किसी अनजान नंबर से इमरजेंसी कॉल करे, तो सबसे पहले वह कोड वर्ड पूछें। AI आवाज तो बना सकता है, पर आपके घर का सीक्रेट कभी नहीं जान सकता!

2

कॉल तुरंत काटें और असली नंबर पर कॉल बैक करें

चाहे कितनी भी बड़ी मजबूरी या धमकी दी जाए, एक बात गांठ बांध लें: **फोन तुरंत काटें।** फिर अपनी फोनबुक में पहले से सेव किए गए असली नंबर पर सीधे फोन मिलाएं। यदि वह फोन न उठाए, तो उसके हॉस्टल के दोस्त, रूममेट या ऑफिस के सहकर्मी को फोन करें।

3

Video Call में Deepfake के 3 सुराग पहचानें

यदि कोई पुलिस अधिकारी बनकर WhatsApp या Skype पर वीडियो कॉल करे, तो ध्यान से देखें: (1) उसकी पलकें प्राकृतिक रूप से नहीं झपकतीं, (2) होठों का हिलना आवाज के साथ मेल नहीं खाता,

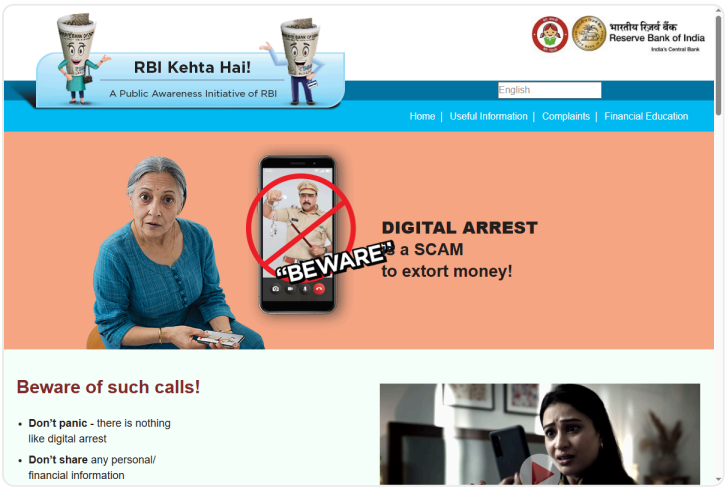
और (3) चेहरा हिलाने पर गालों या कानों के किनारे धुंधले (Blur) हो जाते हैं।

RBI Kehta Hai: डिजिटल अरेस्ट पर रिज़र्व बैंक की चेतावनी

भारतीय रिज़र्व बैंक के आधिकारिक जागरूकता पोर्टल पर डिजिटल अरेस्ट से बचाव के स्पष्ट दिशा-निर्देश दिए गए हैं:

rbikehtahai.rbi.org.in

RBI आधिकारिक जागरूकता



📌 RBI डिजिटल अरेस्ट चेतावनी (Digital Arrest Advisory) से 2 मुख्य सीख:

1. **Digital Arrest एक फ्रॉड है:** रिज़र्व बैंक साफ कहता है कि डिजिटल अरेस्ट केवल जबरन पैसे ऐंठने का एक फर्जी तरीका है। कानून में इसका कोई वजूद नहीं है।

2. **घबराएं नहीं, पैसे न दें:** किसी भी धमकी में आकर अपनी वित्तीय जानकारी साझा न करें और तुरंत आधिकारिक सरकारी पोर्टल पर रिपोर्ट दर्ज करें।

अध्याय 9: AI वॉयस क्लोनिंग और डिजिटल अरेस्ट

से जुड़े सवाल (AI Fraud FAQs)

Q1: AI सॉफ्टवेयर को मेरे परिवार के सदस्यों की आवाज कहाँ से मिलती है?

उत्तर: लोग अक्सर अपने बच्चों के जन्मदिन, वेकेशन या रील्स को सोशल मीडिया (Instagram, Facebook, YouTube) पर 'Public' प्राइवेसी के साथ अपलोड करते हैं। ठग वहां से केवल 3 सेकंड का ऑडियो चुरा लेते हैं। इसलिए अपने सोशल मीडिया अकाउंट को हमेशा 'Private' रखें।

Q2: क्या 'Digital Arrest' की धमकी देने पर सचमुच पुलिस मेरे घर आ सकती है?

उत्तर: बिल्कुल नहीं। असली पुलिस कभी फोन पर चेतावनी देकर पैसे नहीं मांगती। जो लोग फोन पर धमकाते हैं, वे दूर किसी अन्य राज्य या देश के साइबर ठग होते हैं। आप बिना डरे तुरंत नजदीकी पुलिस थाने में जाकर उस फर्जी कॉल की शिकायत करें।

Q3: अगर सामने वाला वीडियो कॉल पर असली पुलिस थाने में बैठा दिखे तो क्या करें?

उत्तर: ठग किराए के कमरों में पुलिस स्टेशन जैसा पर्दा और अशोक स्तंभ की फोटो लगाकर स्टूडियो तैयार करते हैं या AI वीडियो फिल्टर लगाते हैं। उनसे कहें कि *"मैं अभी अपने स्थानीय थाने जा रहा हूँ, आप मेरे शहर के SHO से बात कर लीजिए।"* इतना सुनते ही ठग तुरंत कॉल काट देगा।

Q4: क्या WhatsApp पर अनजान विदेशी कोड (+92, +84 आदि) से आई वीडियो कॉल उठानी चाहिए?

उत्तर: कभी नहीं। अनजान विदेशी नंबरों से आने वाली ऑडियो या वीडियो कॉल को कभी न उठाएं। WhatsApp Settings में जाकर **"Silence Unknown Callers"** (अपरिचित कॉल करने वालों को म्यूट करें) का विकल्प चालू रखें।

Q5: अगर किसी बुजुर्ग ने डर के मारे पैसे ट्रांसफर कर दिए हों, तो क्या करें?

उत्तर: तुरंत अध्याय 8 में बताए गए **'गोल्डन ऑवर'** नियम का पालन करें। घटना के 2 घंटे के भीतर राष्ट्रीय साइबर पोर्टल `cybercrime.gov.in` पर 12-अंकों के UTR नंबर के साथ शिकायत दर्ज करें ताकि ठग का बैंक खाता फ्रीज हो सके।

संदिग्ध वीडियो या वॉइस कॉल: क्या करें और क्या न

करें

✅ क्या करें (Do's)	❌ क्या न करें (Don'ts)
परिवार के साथ एक गुप्त **Family Code Word** तय रखें।	सोशल मीडिया पर बच्चों की आवाज़ वाली लंबी वीडियो पब्लिकली शेयर न करें।
इमरजेंसी कॉल आने पर तुरंत फोन काटकर अपने सुरक्षित नंबर पर मिलाएं।	धमकी देने वाले के दबाव में आकर कभी भी हड़बड़ी में UPI PIN न डालें।
याद रखें कि कानून में **Digital Arrest** जैसी कोई चीज नहीं है।	खुद को अकेले कमरे में बंद करके वीडियो कॉल पर घंटों बैठे न रहें।
संदिग्ध फर्जी कॉल की सूचना तुरंत **cybercrime.gov.in** पर दें।	डर के मारे परिवार या स्थानीय पुलिस से बात छुपाकर पैसे न गंवाएं।
WhatsApp पर *Silence Unknown Callers* सेटिंग ऑन रखें।	अनजान वीडियो कॉल पर अपना कैमरा ऑन करके बातचीत शुरू न करें।

Google पर डिजिटल अरेस्ट एडवाइजरी कैसे खोजें? (Digital Arrest Advisory)

यदि आप रिज़र्व बैंक या सरकार द्वारा डिजिटल अरेस्ट पर जारी आधिकारिक दिशा-निर्देश पढ़ना चाहते हैं:

🔍 `"RBI Kehta hai digital arrest advisory cybercrime official"`

1

चरण 1: डिजिटल अरेस्ट एडवाइजरी को कोट्स में खोजें

ऊपर दिया गया वाक्य कोट्स के साथ गूगल सर्च बार में टाइप करें ताकि सटीक सरकारी पेज ही सामने आए।

2

विज्ञापनों (Sponsored Links) से बचें

सर्च रिजल्ट में ऊपर दिख रहे विज्ञापनों पर क्लिक न करें। केवल `rbi.org.in` या `cybercrime.gov.in` के लिंक पर जाएं।

3

वेबसाइट URL में HTTPS जांचें

पेज खुलने पर एड्रेस बार में ताले का निशान और आधिकारिक डोमेन देखकर ही जानकारी पढ़ें।

🔍 अध्याय 9 के सत्यापित आधिकारिक स्रोत (Official Sources)

• **RBI Kehta Hai आधिकारिक परामर्श (Digital Arrest Scam Advisory):** https://rbikehtahai.rbi.org.in/rbi-digital-arrest.html

• **National Cyber Crime Reporting Portal:** https://www.cybercrime.gov.in (गृह मंत्रालय, भारत सरकार)

• **DoT संचार साथी चक्षु (संदिग्ध कॉल व मैसेज रिपोर्ट):**
https://sancharsaathi.gov.in

अध्याय 10 • तकनीकी धोखे (Spoofing & Phishing)

AI से बने नकली Screenshot और Website

दुकानदार और ग्राहक सावधान: सामने वाले के मोबाइल का स्क्रीनशॉट या फॉरवर्ड किया गया SMS कभी भी पेमेंट का प्रमाण नहीं होता। जानिए Spoof Apps की सच्चाई और असली पुष्टि के नियम।

नकली Screenshot और Spoof Apps का फरेब

आजकल इंटरनेट पर ऐसे कई अनधिकृत **Spoof Apps** और **Fake Pay Generators** मौजूद हैं, जो किसी भी लोकप्रिय **UPI App** (जैसे Paytm, PhonePe या Google Pay) की हूबहू दिखने वाली "Payment Successful" स्क्रीन बना देते हैं।

धोखेबाज केवल 5 सेकंड में दुकानदार का नाम और बिल की राशि टाइप करता है। ऐप तुरंत हरे रंग के टिक (Green Tick), फर्जी UTR नंबर और यहां तक कि साउंडबॉक्स जैसी नकली ऑडियो आवाज के साथ स्क्रीन तैयार कर देता है। धोखेबाज फोन दिखाकर कहता है: *"देखिए भैया, पैसे कट गए, स्क्रीनशॉट आपके WhatsApp पर भी भेज दिया है!"* और सामान लेकर चंपत हो जाता है।

⚠ **कड़वा सच: स्क्रीनशॉट सिर्फ एक तस्वीर है!**

स्क्रीनशॉट केवल मोबाइल स्क्रीन पर दिखने वाली रंगीन इमेज होती है। इसका बैंकिंग नेटवर्क (NPCI या Bank CBS) से कोई संबंध नहीं होता। कोई भी व्यक्ति ग्राफिक टूल या फर्जी ऐप से ₹10 से लेकर ₹10,00,000 तक का फर्जी सक्सेस स्क्रीनशॉट बना सकता है।

केस स्टडी: दुकानदार मोहन और ₹18,000 का फर्जी Green Tick

जयपुर में मोबाइल और इलेक्ट्रॉनिक्स की दुकान चलाने वाले मोहन लाल शाम को दुकान पर अकेले थे। एक सूट-बूट पहने युवक दुकान पर आया और ₹18,000 का महंगा ब्लूटूथ स्पीकर खरीदने लगा।

दुकानदार की सूझबूझ

जल्दबाजी का नाटक और मोहन लाल की शांति:

ग्राहक (जल्दबाजी में): *"भैया, मुझे फ्लाइट पकड़नी है, जल्दी पैक कर दीजिए। मैंने आपके QR पर ₹18,000 ट्रांसफर कर दिए हैं, ये देखिए मेरे PhonePe पर Green Tick आ गया!"*

मोहन लाल: *"सर, 1 मिनट रुकिए। मेरे साउंडबॉक्स से आवाज़ नहीं आई और मेरे मर्चेंट ऐप में अभी बैलेंस नहीं बढ़ा है।"*

ग्राहक (गुस्से में): *"अरे आप मेरा फोन देखिए! क्या मैं झूठ बोल रहा हूँ? आपका सर्वर धीमा होगा, पैसे रास्ते में होंगे। मेरा स्क्रीनशॉट ले लीजिए!"*

मोहन लाल ने ग्राहक के गुस्से की परवाह नहीं की। उन्होंने शांति से अपने बैंक का **Statement / Passbook** ऐप खोला। खाते में कोई नया पैसा जमा नहीं हुआ था। जब मोहन ने कहा कि *"सर, चलिए बगल वाले बैंक एटीएम से चलकर कैश निकाल लेते हैं"*, तो वह युवक फोन जेब में रखकर चुपके से खिसक गया!

सबक: मोहन लाल ने ग्राहक की चमचमाती स्क्रीन के बजाय केवल अपने बैंक खाते और साउंडबॉक्स पर भरोसा किया और एक बड़े वित्तीय नुकसान से अपनी दुकान को बचा लिया।

तुलना: नकली Screenshot बनाम असली बैंक पुष्टि

नीचे दिए गए उदाहरण से समझें कि धोखेबाज की स्क्रीन में क्या कमियां होती हैं और असली पुष्टि कहां होती है:

❌ धोखेबाज का नकली Screenshot (Spoof App)



Paid Successfully

₹3,500

To:	Sharma General Store
UPI ID:	sharmaji@okaxis
UTR / Ref:	**98765432 (अमान्य 8 अंक)**

काल्पनिक उदाहरण

लाल झंडे (Red Flags):

• **काल्पनिक UTR:** असली UPI UTR हमेशा 12 अंकों का होता है, फर्जी स्क्रीन में अक्सर अंक गलत या कम होते हैं।

• **कोई बैंक रिकॉर्ड नहीं:** यह सिर्फ फोन में बनी इमेज है, आपके खाते में ₹0 जमा हुआ है।

• **असंगत फॉन्ट:** अक्षरों की बनावट असली ऐप से हल्की भिन्न होती है।

✅ **असली पुष्टि (केवल आपका अपना फोन / साउंडबॉक्स)**

आधिकारिक Bank Passbook / SMS

Account Credited

+ ₹3,500.00

Bank Header:	VK-HDFCBK
UTR No:	631245897120 (12 अंक)
Available Bal:	₹18,450.00 (खाते में वृद्धि)

असली पुष्टि के 3 लक्षण:

• **अपने Bank App में एंट्री:** अपनी पासबुक या स्टेटमेंट में क्रेडिट स्पष्ट दिखता है।

• **आधिकारिक Soundbox:** साउंडबॉक्स स्पष्ट आवाज में बोलता है कि भुगतान प्राप्त हुआ।

• **Bank SMS:** 6-अक्षरों वाले रजिस्टर्ड बैंक हेडर से तुरंत SMS आता है।

⚠️ *Educational Note: ऊपर दी गई स्क्रीन केवल समझाने के लिए बनाया गया काल्पनिक उदाहरण (educational illustration) है।*

नकली SMS की पहचान: 10 अंकों का नंबर बनाम Bank Header

धोखेबाज अब केवल नकली स्क्रीनशॉट ही नहीं दिखाते, बल्कि वे आपके मोबाइल पर बैंक के नाम से मिलता-जुलता नकली SMS भी भेज देते हैं:

प्रेषक: +91 9XXXX-XXXXX (10 अंकों का व्यक्तिगत नंबर) ❌

"Dear Customer, your A/C ending XX4512 has been credited with INR 3,500.00 on 08-Nov-2026 by UPI/Ref 9876-XXXX-1012 (12-अंकीय UTR). Updated Balance: INR 18,450.00."



TRAI और RBI का आधिकारिक नियम

भारत में किसी भी बैंक या वित्तीय संस्थान को साधारण 10 अंकों वाले मोबाइल नंबर से लेनदेन का SMS भेजने की अनुमति नहीं है।



आधिकारिक SMS Header की बनावट

असली बैंक SMS हमेशा 6 अक्षरों के आधिकारिक हेडर से आते हैं (जैसे `AX-ICICIB`, `VM-SBIPAY`, `BP-HDFCBK`)। यदि किसी 10-अंकों के व्यक्तिगत नंबर से पैसे आने का SMS आए, तो वह 100% फर्जी है।

Phishing Websites: हूबहू दिखने वाली नकली वेबसाइट्स

साइबर ठग बैंकों, UPI ऐप्स और सरकारी पोर्टल्स के हूबहू दिखने वाले नकली वेबपेज (Phishing Sites) तैयार करते हैं। इनका उद्देश्य आपका नेटबैंकिंग पासवर्ड, डेबिट कार्ड नंबर या UPI PIN चुराना होता है।

संस्थान	✅ असली आधिकारिक वेबसाइट	❌ नकली / Phishing वेबसाइट
State Bank of India	`onlinesbi.sbi`	`sbi-netbanking-login.online`
HDFC Bank	`hdfcbank.com`	`hdfc-rewards-points.site`
NPCI (UPI)	`npci.org.in`	`npci-refund-support.club`
RBI (केन्द्रीय बैंक)	`rbi.org.in`	`rbi-governor-fund.top`

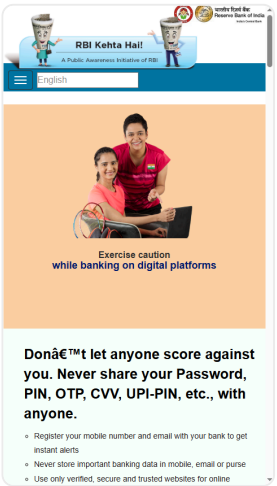
🔍 डोमेन नाम (URL) जांचने का नियम:

हमेशा ब्राउज़र के एड्रेस बार में वेबसाइट का मुख्य डोमेन देखें। भारतीय बैंक कभी भी `.site`, `.online`, `.top`, `.club` या `.free` जैसे मुफ्त या सस्ते डोमेन का उपयोग नहीं करते। आधिकारिक पते के अंत में हमेशा आधिकारिक डोमेन (जैसे `.bank.in`, `.org.in`, `.co.in` या मान्यता प्राप्त `.com`) होता है।

RBI Kehta Hai: सुरक्षित बैंकिंग वेबसाइट्स की पहचान

भारतीय रिज़र्व बैंक (RBI) अपने जन-जागरूकता अभियान में सुरक्षित डिजिटल वेबसाइट्स की पहचान करने के स्पष्ट निर्देश देता है:

rbikehtahai.rbi.org.in RBI आधिकारिक जन-जागरूकता



📌 RBI सुरक्षित बैंकिंग वेबसाइट निर्देश से 2 मुख्य सीख:

1. **आधिकारिक URL टाइप करें:** बैंक की वेबसाइट पर जाने के लिए गूगल पर सर्च करने या अनजान लिंक पर क्लिक करने के बजाय एड्रेस बार में सीधा सही URL खुद टाइप करें।

2. **सुरक्षा पैडलॉक (Padlock) और HTTPS:** वेबसाइट पते के आगे ताले का निशान और 'https://' की पुष्टि अवश्य करें। कभी भी असुरक्षित 'http://' पेज पर अपनी बैंकिंग जानकारी न भरें।

अध्याय 10: नकली स्क्रीनशॉट और फिशिंग से जुड़े

सवाल (Spoofing FAQs)

Q1: क्या कोई मोबाइल ऐप साउंडबॉक्स जैसी आवाज निकाल सकता है?

उत्तर: हां। कुछ शातिर ठग अपने फोन में ऑडियो रिकॉर्डिंग या फर्जी ऐप में ऐसी ध्वनि सेट कर लेते हैं जो बोलती है: *"Paytm/PhonePe पर ₹500 प्राप्त हुए।"* लेकिन ध्यान दें — यह आवाज ठग के फोन से आती है, आपकी दुकान पर रखे आधिकारिक साउंडबॉक्स से नहीं!

Q2: अगर ग्राहक कहे कि "मेरे खाते से पैसे कट गए हैं, आपको शाम तक मिल जाएंगे", तो क्या करें?

उत्तर: विनम्रता से कहें: *"सर, जैसे ही मेरे खाते में पैसे क्रेडिट होंगे, मैं सामान दे दूंगा। यदि आपके पैसे कट गए हैं तो वे RBI के नियम अनुसार 24 घंटे में आपके खाते में स्वतः वापस आ जाएंगे।"* बिना पैसे खाते में आए कभी भी सामान न दें।

Q3: क्या बैंक के नाम से आने वाले हर SMS पर आंख मूंदकर भरोसा किया जा सकता है?

उत्तर: नहीं। केवल 6 अक्षरों वाले अधिकृत बैंक हेडर (जैसे AX-SBIPAY) के SMS ही बैंक से आते हैं। किसी भी 10 अंकों वाले मोबाइल नंबर से आए पैसे जमा होने के SMS पूरी तरह नकली होते हैं।

Q4: अगर किसी वेबसाइट पर ताले का निशान (HTTPS) लगा हो, तो क्या वह 100% सुरक्षित है?

उत्तर: हमेशा नहीं। HTTPS का मतलब केवल यह है कि आपका कनेक्शन एन्क्रिप्टेड है। आज ठग भी अपनी फर्जी वेबसाइट्स पर मुफ्त SSL सर्टिफिकेट लगा लेते हैं। ताले के साथ-साथ वेबसाइट का सटीक स्पेलिंग (जैसे `onlinesbi.sbi`) देखना अनिवार्य है।

Q5: अगर किसी दुकानदार ने गलती से फर्जी स्क्रीनशॉट देखकर सामान दे दिया हो, तो क्या करे?

उत्तर: अपनी दुकान के CCTV कैमरे से उस व्यक्ति का फुटेज निकालें, उसकी गाड़ी का नंबर नोट करें और तुरंत नजदीकी पुलिस थाने व राष्ट्रीय साइबर पोर्टल `cybercrime.gov.in` पर रिपोर्ट दर्ज कराएं।

दुकानदारों व ग्राहकों के लिए क्या करें और क्या न

करें (Dos & Don'ts)

✅ क्या करें (Do's)	❌ क्या न करें (Don'ts)
पेमेंट की पुष्टि के लिए केवल **अपने बैंक ऐप या साउंडबॉक्स** पर भरोसा करें।	ग्राहक के मोबाइल में दिख रहे हरे टिक (Green Tick) या स्क्रीनशॉट को प्रमाण न मानें।
SMS आने पर प्रेषक का **6-अक्षरों का बैंक हेडर** अवश्य जांचें।	10 अंकों के व्यक्तिगत मोबाइल नंबर से आए पैसे जमा होने के SMS पर विश्वास न करें।
बैंक की वेबसाइट का सही URL ब्राउज़र में स्वयं टाइप करें।	गूगल सर्च रिजल्ट में सबसे ऊपर दिखने वाले स्पॉन्सर्ड विज्ञापनों पर क्लिक न करें।
12 अंकों के असली UTR नंबर की पुष्टि अपने बैंक स्टेटमेंट में करें।	जल्दबाजी या दबाव बनाने वाले ग्राहक के आगे झुककर बिना पुष्टि सामान न सौंपें।
संदिग्ध फर्जी ऐप या वेबसाइट की शिकायत तुरंत **cybercrime.gov.in** पर करें।	किसी वेबसाइट पर इनाम या लॉटरी जीतने के झांसे में आकर अपना UPI PIN दर्ज न करें।

Google पर सुरक्षित बैंकिंग वेबसाइट्स कैसे खोजें? (Safe Banking Guide)

यदि आप अपने बैंक की सही और आधिकारिक वेबसाइट खोजना चाहते हैं, तो सर्च इंजन पर इस सुरक्षित तरीके को अपनाएं:

🔍 `"RBI Kehta hai safe internet banking fake websites guidelines official"`

1

चरण 1: आधिकारिक बैंक डोमेन को कोट्स में खोजें

ऊपर दिया गया वाक्य कोट्स के साथ सर्च बार में डालें ताकि गूगल केवल आधिकारिक जागरूकता पेज दिखाए।

2

'Ad' या 'Sponsored' पर कभी क्लिक न करें

सर्च रिजल्ट में सबसे ऊपर दिखने वाले विज्ञापनों में ठगों की फर्जी वेबसाइट हो सकती है। उन्हें छोड़ दें।

3

आधिकारिक डोमेन की जांच करें

लिंक पर क्लिक करने से पहले देखें कि वेबसाइट का डोमेन `.bank.in`, `.org.in` या मान्यता प्राप्त आधिकारिक डोमेन ही हो।

🔍 अध्याय 10 के सत्यापित आधिकारिक स्रोत (Official Sources)

• **RBI Kehta Hai आधिकारिक जागरूकता पोर्टल:**
https://rbikehtahai.rbi.org.in

• **National Cyber Crime Reporting Portal:**
https://www.cybercrime.gov.in (गृह मंत्रालय, भारत सरकार)

• **DoT संचार साथी चक्षु (फर्जी SMS व कॉल रिपोर्टिंग):**
https://sancharsaathi.gov.in

अध्याय 11 • डिजिटल जालसाजी (Smishing & Malicious Links)

नकली Link और Message

SMS और WhatsApp पर बिजली बिल कटने, लॉटरी जीतने, कूरियर पेंडिंग होने या Bank KYC बंद होने का डर दिखाकर भेजे जाने वाले संदिग्ध लिंक की सच्चाई और सुरक्षा के ठोस उपाय।

Smishing क्या है? मैसेज के जरिए ठगी का नया जाल

जब साइबर अपराधी SMS या WhatsApp के जरिए किसी नागरिक को लुभाने या डराने वाला फर्जी संदेश भेजते हैं और उसमें एक हानिकारक वेब लिंक (**Link**) देते हैं, तो इस तकनीक को साइबर सुरक्षा में **Smishing (SMS Phishing)** कहा जाता है।

धोखेबाजों का एकमात्र मकसद आपको घबराहट या लालच में डालकर उस लिंक पर तुरंत क्लिक करवाना होता है। एक बार आपने लिंक पर क्लिक किया, तो वे आपका **UPI PIN**, **OTP** या फोन का पूरा नियंत्रण चुराने का प्रयास करते हैं।

⚠️ भारत में सबसे ज्यादा भेजे जाने वाले 4 फर्जी मैसेज:

1. बिजली बिल डिस्कनेक्शन की धमकी

"Dear Customer, your Electricity power will be disconnected tonight at 9:30 PM from electricity office because your previous month bill was not updated. Please immediately pay your bill by clicking here: bit.ly/power-pay-xyz"

सच्चाई: बिजली विभाग कभी भी किसी व्यक्तिगत 10-अंकों वाले मोबाइल नंबर से रात में लाइट काटने की धमकी भरा SMS नहीं भेजता।

2. Bank A/C या KYC बंद होने का डर

"SBI/HDFC Alert: Your NetBanking account will be suspended today due to pending PAN KYC. Update immediately to keep your account active: sbi-kyc-verify.online"

सच्चाई: कोई भी बैंक SMS में लिंक भेजकर गोपनीय जानकारी या PIN दर्ज करने को नहीं कहता।

3. लॉटरी, इनाम और भारी कैशबैक का लालच

"Congratulations! You have received a scratch card worth INR 4,999 on PhonePe/Paytm. Claim your instant cashback directly in your bank account: paytm-reward-claim.site"

सच्चाई: UPI कैशबैक पाने के लिए किसी बाहरी लिंक पर क्लिक करने की कभी जरूरत नहीं होती।

4. पेंडिंग कूरियर / पार्सल डिलीवरी

"India Post / Courier: Your parcel cannot be delivered due to wrong house address. Please confirm your details and pay INR 5 re-delivery fee here: indiapost-track.top"

सच्चाई: ₹5 के नाम पर लिंक से आपके बैंक खाते का पूरा विवरण और OTP मांग लिया जाता है।

केस स्टडी: सुमन जी का कूरियर मैसेज और बेटी की सतर्कता

दिल्ली की रहने वाली 52 वर्षीय सुमन जी को एक दिन दोपहर में India Post के नाम से SMS आया कि उनका एक पार्सल घर का पता अधूरा होने

के कारण अटका हुआ है। पार्सल दोबारा मंगाने के लिए ₹5 का भुगतान करने का लिंक दिया गया था।

घरेलू सतर्कता की कहानी

₹5 के लिंक के पीछे छिपी जासूसी APK फाइल:

सुमन जी: *"अरे रिया, मैंने पिछले हफ्ते ऑनलाइन साड़ियां मंगाई थीं। डाक विभाग का मैसेज आया है कि ₹5 देकर एड्रेस अपडेट करो, नहीं तो पार्सल लौट जाएगा।"*

बेटी रिया (सॉफ्टवेयर इंजीनियर): *"मम्मी, रुको! डाक विभाग कभी 10 अंकों के साधारण मोबाइल नंबर से मैसेज नहीं भेजता। मुझे लिंक देखने दो।"*

रिया ने जैसे ही मैसेज देखा, लिंक `bit.ly` से छोटा किया गया था। जब उस पर टैप किया गया, तो फोन की स्क्रीन पर एक चेतावनी आई: *"Do you want to download IndiaPost_Service.apk?"*

बेटी का तुरंत एक्शन: रिया ने तुरंत डाउनलोड कैंसल किया। उसने समझाया कि **.apk** कोई वेबपेज नहीं बल्कि एक एंड्रॉयड ऐप फाइल होती है। यदि मम्मी ने इसे इंस्टॉल कर लिया होता, तो यह ऐप फोन के सारे

SMS और OTP चुपचाप ठगों तक पहुंचा देती और बैंक खाता खाली हो जाता!

लिंक के पीछे छिपे 3 बड़े तकनीकी खतरे

अक्सर लोग सोचते हैं कि केवल लिंक खोलने से क्या नुकसान हो सकता है? समझिए कि एक गलत क्लिक आपके फोन और बैंक खाते को कैसे खतरे में डालता है:



खतरा 1: जासूसी APK फाइल का ऑटो-डाउनलोड (Malware / Trojan)

लिंक पर क्लिक करते ही फोन में बिना आपकी स्पष्ट अनुमति के एक `.apk` फाइल (जैसे `Update_Bank.apk`) डाउनलोड हो जाती है। यदि आपने इसे 'Install' कर दिया, तो यह ऐप बैकग्राउंड में आपके सभी SMS और बैंकिंग **OTP** चुपचाप ठगों के सर्वर पर भेज देती है।



खतरा 2: नकली Phishing लॉगिन पेज

लिंक खोलने पर बिल्कुल बैंक जैसी दिखने वाली नकली वेबसाइट खुलती है। यदि आपने वहां अपना यूजरनेम, पासवर्ड या डेबिट कार्ड नंबर भरा, तो वह तुरंत धोखेबाज के डेटाबेस में सेव हो जाता है।

खतरा 3: शॉर्ट लिंक (Shortened URL) का पर्दा

ठग असली फर्जी पते को छिपाने के लिए `bit.ly`, `tinyurl.com` या `is.gd` जैसी सेवाओं का उपयोग करते हैं, ताकि आम नागरिक यह न पहचान सके कि लिंक उसे किस खतरनाक सर्वर पर ले जा रहा है।

निर्णय वृक्ष (Decision Tree): "संदिग्ध Link मिले तो क्या करें?"

जब भी फोन पर कोई अनजान लिंक वाला मैसेज आए, तो इस सरल सुरक्षा मार्गदर्शिका (Flowchart) का पालन करें:

चरण 1: शुरुआत

SMS या WhatsApp पर कोई लिंक प्राप्त हुआ

मैसेज में बिजली बिल, लॉटरी, कैशबैक, कूरियर या बैंक KYC का जिक्र है।

↓

जांच 1: प्रेषक का नंबर

क्या मैसेज 10-अंकों वाले साधारण मोबाइल नंबर से आया है?

हाँ (+91 9xxxx) ➡️ 100% फर्जी संदेश! लिंक पर कभी क्लिक न करें।

नहीं (Bank Header) ➡️ फिर भी लिंक पर क्लिक न करें, हमेशा आधिकारिक ऐप खोलें।

⬇️

जांच 2: यदि गलती से लिंक खुल गया हो

वेबपेज या स्क्रीन पर क्या दिखाई दे रहा है?

1. कोई .apk फाइल डाउनलोड हो रही है?

तत्काल रोकें: डाउनलोड को कैंसल करें और File Manager से उसे तुरंत Delete करें। इंस्टॉल कभी न करें!

2. UPI PIN, OTP या पासवर्ड मांगा जा रहा है?

तुरंत पेज बंद करें: किसी भी वेबपेज पर पैसे पाने के लिए कभी PIN या OTP दर्ज न करें।

⬇️

अंतिम सुरक्षित कदम

मैसेज को ब्लॉक करें और 'चक्षु' पोर्टल पर रिपोर्ट करें

भारत सरकार के `sancharsaathi.gov.in` (Chakshu) पर फर्जी नंबर की रिपोर्ट दर्ज कराएं और मैसेज को फोन से मिटा दें।

तुलना: असली Bank SMS बनाम फर्जी Smishing SMS

इन 4 अंतरों से आप 3 सेकंड में असली और नकली संदेश को पहचान सकते हैं:

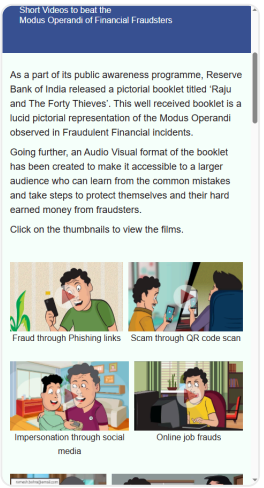
✅ असली बैंक संदेश (Official)	❌ फर्जी Smishing संदेश (Scam)
हेडर: 6-अक्षरों वाला पंजीकृत अल्फान्यूमेरिक कोड (उदा. `AD-HDFCBK`, `VK-SBIPAY`)।	**हेडर:** साधारण 10 अंकों का व्यक्तिगत मोबाइल नंबर (उदा. `+91 9XXXX-XXXXX`)।
मकसद: केवल सूचनात्मक — आपके द्वारा किए गए सफल डेबिट या क्रेडिट की पुष्टि।	**मकसद:** किसी बाहरी वेबसाइट लिंक पर भेजकर गुप्त वित्तीय जानकारी चुराना।
लिंक: कभी भी गोपनीय PIN या पासवर्ड दर्ज करने वाला संदिग्ध लिंक नहीं होता।	**लिंक:** संदिग्ध पते (जैसे `bit.ly/...`, `.online`, `.top` या `.apk`)।
भाषा: सामान्य और संयमित भाषा, तुरंत खाता बंद करने की धमकियां नहीं होतीं।	**भाषा:** अत्यधिक घबराहट पैदा करने वाली भाषा ("आज रात 9:30 बजे बिजली कट जाएगी")।

RBI Kehta Hai: फिशिंग लिंक्स पर रिज़र्व बैंक की सलाह

भारतीय रिज़र्व बैंक (RBI) अपने लोकप्रिय जन-जागरूकता अभियान **'राजू एंड द फॉर्टी थीव्स' (Raju and The Forty Thieves)** में फिशिंग लिंक्स के खतरों पर विशेष रूप से सचेत करता है:

rbikehtahai.rbi.org.in

RBI जन-जागरूकता सीरीज



📌 RBI फिशिंग जागरूकता (Raju & Forty Thieves) से 2 मुख्य सीख:

1. **लिंक का स्रोत जांचें:** अनजान व्यक्ति या अज्ञात नंबर से आए लिंक पर कभी क्लिक न करें। बैंक कभी भी SMS में गोपनीय जानकारी दर्ज करने का लिंक नहीं भेजते।

2. **संदेह होने पर आधिकारिक ऐप खोलें:** यदि बिजली बिल या बैंक अपडेट का मैसेज आए, तो मैसेज के लिंक पर जाने के बजाय सीधे अपने अधिकृत इलेक्ट्रिसिटी ऐप या बैंक ऐप में जाकर स्थिति देखें।

अध्याय 11: संदिग्ध लिंक और Smishing से जुड़े

सवाल (Phishing Link FAQs)

Q1: क्या सिर्फ किसी लिंक पर क्लिक करने से मेरे खाते से पैसे कट सकते हैं?

उत्तर: केवल लिंक खुलने पर सामान्यतः पैसे नहीं कटते जब तक कि आप उस पेज पर अपना UPI PIN न डालें या कोई जासूसी APK ऐप इंस्टॉल करके उसे SMS पढ़ने की अनुमति (Accessibility Permission) न दे दें। फिर भी, कभी भी अनजान लिंक पर क्लिक न करें।

Q2: फोन में .apk फाइल डाउनलोड होने पर क्या खतरा होता है?

उत्तर: .apk फाइल एंड्रॉइड फोन का सॉफ्टवेयर पैकेज होती है। यदि यह इंस्टॉल हो जाए, तो ठग आपके फोन की स्क्रीन देख सकते हैं, आपके बैंक से आने वाले OTP पढ़ सकते हैं और आपकी जानकारी के बिना पैसे ट्रांसफर कर सकते हैं।

Q3: अगर मैंने गलती से किसी फर्जी लिंक पर अपना UPI PIN डाल दिया हो, तो क्या करें?

उत्तर: बिना 1 सेकंड गंवाए अपने फोन का आधिकारिक UPI ऐप (Google Pay, PhonePe, BHIM) खोलें और तुरंत **"Change UPI PIN"** में जाकर अपना नया PIN सेट करें। साथ ही अपने बैंक से संपर्क करके UPI सेवा अस्थायी रूप से बंद करवाएं।

Q4: क्या WhatsApp पर दोस्तों द्वारा भेजे गए 'फ्री रीचार्ज' या 'सरकारी योजना' वाले लिंक सच होते हैं?

उत्तर: बिल्कुल झूठ! साइबर ठग लोगों से लालच देकर *"इस मैसेज को 10 दोस्तों को भेजो तो ₹500 का रीचार्ज मिलेगा"* जैसी फॉरवर्डिंग करवाते हैं। ये पूरी तरह फर्जी होते हैं और वायरस फैलाने का काम करते हैं।

Q5: DoT के 'चक्षु' (Chakshu) पोर्टल पर फर्जी SMS की शिकायत कैसे दर्ज की जाती है?

उत्तर: `sancharsaathi.gov.in` खोलें, 'Chakshu' विकल्प पर क्लिक करें, उस संदिग्ध मैसेज का स्क्रीनशॉट और भेजने वाले का 10-अंकों का नंबर दर्ज करें। दूरसंचार विभाग उस नंबर को तुरंत ब्लॉक कर देता है।

संदिग्ध मैसेज व लिंक मिलने पर: क्या करें और क्या

न करें

✅ क्या करें (Do's)	❌ क्या न करें (Don'ts)
मैसेज में आए लिंक के बजाय संबंधित विभाग की **आधिकारिक ऐप या वेबसाइट** खोलें।	10 अंकों के साधारण मोबाइल नंबर से आए बिजली बिल या बैंक SMS पर भरोसा न करें।
यदि कोई .apk फाइल डाउनलोड हो जाए, तो उसे File Manager से तुरंत **Delete** करें।	डाउनलोड हुई अनजान .apk फाइल पर टैप करके उसे कभी 'Install' न करें।
संदिग्ध नंबर की शिकायत दूरसंचार विभाग के **चक्षु पोर्टल** पर दर्ज करें।	WhatsApp पर आए 'फ्री रीचार्ज' या 'इनाम' वाले लुभावने मैसेज आगे फॉरवर्ड न करें।
ब्राउज़र की सेटिंग्स में *"Warn on dangerous sites"* हमेशा चालू रखें।	शॉर्ट लिंक (bit.ly, tinyurl) पर बिना जाने-समझे कभी क्लिक न करें।
गलती से PIN शेयर हो जाने पर तुरंत आधिकारिक ऐप में जाकर अपना **UPI PIN बदलें**।	SMS में दिए गए किसी भी फोन नंबर पर सहायता के लिए कभी कॉल न लगाएं।

Google पर सुरक्षित सर्च कैसे करें: सरकारी चक्षु व साइबर पोर्टल ढूंढना

यदि आप फर्जी SMS या व्हाट्सएप कॉल की आधिकारिक शिकायत दर्ज करना चाहते हैं:

🔍 `"sanchar saathi chakshu report suspected fraud official portal"`

1

चरण 1: चक्षु पोर्टल को कोट्स में खोजें

ऊपर दिया गया वाक्य कोट्स के साथ गूगल सर्च में टाइप करें ताकि सटीक सरकारी पोर्टल सबसे ऊपर आए।

2

gov.in डोमेन देखें

जांचें कि वेबसाइट का URL `sancharsaathi.gov.in` ही हो। किसी निजी .com या .in पर न जाएं।

3

चरण 3: सर्च विज्ञापनों को छोड़कर असली शिकायत पेज चुनें

रिजल्ट में सबसे ऊपर दिखने वाले 'Sponsored' लिंक पर कभी क्लिक न करें।

🔍 अध्याय 11 के सत्यापित आधिकारिक स्रोत (Official Sources)

• **DoT संचार साथी चक्षु पोर्टल:** https://sancharsaathi.gov.in (दूरसंचार विभाग, भारत सरकार)

• **National Cyber Crime Reporting Portal:** https://www.cybercrime.gov.in (गृह मंत्रालय, भारत सरकार)

• **RBI Kehta Hai जन-जागरूकता (Raju and The Forty Thieves):** https://rbikehtahai.rbi.org.in

अध्याय 12 • डिवाइस सुरक्षा (Mobile Device Hardening)

अपना Phone सुरक्षित रखें

UPI की सुरक्षा केवल आपके PIN से नहीं, बल्कि आपके स्मार्टफोन की बुनियादी सेटिंग्स से तय होती है। जानिए स्क्रीन लॉक और UPI PIN का अंतर, परमिशन ऑडिट और सुरक्षित ऐप डाउनलोड के नियम।

स्मार्टफोन का Screen Lock और UPI PIN: कभी एक न रखें

आपका स्मार्टफोन केवल बात करने का साधन नहीं, बल्कि आपकी जेब में रखा पूरा डिजिटल बैंक है। यदि आपका फोन सुरक्षित नहीं है, तो आपकी बैंकिंग भी कभी सुरक्षित नहीं हो सकती।

भारत में लाखों लोग सुविधा के चक्कर में एक बहुत बड़ी गलती करते हैं: जो 4 अंकों का कोड वे फोन की स्क्रीन खोलने के लिए रखते हैं (जैसे 1234, 2580 या जन्म वर्ष 1985), वही कोड वे अपने **UPI PIN** में भी डाल देते हैं!



स्क्रीन लॉक और UPI PIN हमेशा अलग रखें

यदि कोई अजनबी, सहकर्मी या बस में पास बैठा व्यक्ति आपका फोन अनलॉक होते देख ले, तो वह केवल फोन देख रहा है। लेकिन अगर दोनों

पिन एक हुए, तो वह आपके बैंक खाते का मालिक भी बन जाएगा!

Biometric (Fingerprint / Face ID) का उपयोग

फोन अनलॉक करने के लिए फिंगरप्रिंट या फेस आईडी चालू रखें। इन्हें कोई झांककर चुरा नहीं सकता। लेकिन बैकअप पिन कभी भी आसान न रखें।

Auto Screen-Lock 30 सेकंड रखें

फोन की Display Settings में जाकर स्क्रीन टाइमआउट को 30 सेकंड पर सेट करें। मेज पर अनलॉक फोन छोड़कर जाने की आदत सबसे ज्यादा नुकसान कराती है।

केस स्टडी: आलोक की कैब यात्रा और एक जैसी PIN की भूल

नोएडा में नौकरी करने वाले 28 वर्षीय आलोक शाम को ऑफिस से शेयरिंग कैब में घर लौट रहे थे। कैब में उन्होंने अपना फोन अनलॉक करने के लिए स्क्रीन पर 2580 टाइप किया। बगल में बैठे यात्री ने यह नंबर देख लिया।

लापरवाही की भारी कीमत

कैब में छूटा फोन और ₹25,000 की निकासी:

> **आलोक (जल्दबाजी में उतरते हुए):** *"अरे भैया, मेरी सोसाइटी आ गई, रोकिए!"* (फोन सीट पर ही छूट गया)
>
> **सहयात्री (मन में):** *"स्क्रीन लॉक 2580 था। चलिए PhonePe खोलकर देखते हैं कि इसका UPI PIN क्या है..."*

सहयात्री ने फोन अनलॉक किया, आलोक का PhonePe ऐप खोला और अपने खाते में ₹25,000 ट्रांसफर करने के लिए वही 2580 डाला। पिन बिल्कुल सही निकला और पैसे तुरंत ट्रांसफर हो गए!

बड़ा सबक: यदि आलोक ने फोन लॉक के लिए अलग पासवर्ड और UPI के लिए अलग गुप्त PIN रखा होता, तो फोन खोने पर भी उसका बैंक खाता 100% सुरक्षित रहता!

App Permissions Audit: खतरनाक अनुमतियों की पहचान

जब आप कोई नया ऐप इंस्टॉल करते हैं, तो वह कई परमिशन (Permissions) मांगता है। गलत ऐप को दी गई एक संवेदनशील परमिशन आपके पूरे बैंक खाते को खाली कर सकती है।

🚨 **सबसे खतरनाक परमिशन: ACCESSIBILITY SERVICE**

Android में **Accessibility Service** दिव्यांग नागरिकों की सहायता के लिए बनाई गई है। लेकिन यदि किसी अनजान थर्ड-पार्टी ऐप को यह परमिशन मिल जाए, तो वह ऐप एक रिमोट एक्सेस ट्रोजन (RAT) बन जाता है। वह आपकी स्क्रीन पर टाइप किया गया हर पासवर्ड और बैंक से आने वाला **OTP** चुपचाप पढ़कर खुद पैसे ट्रांसफर कर सकता है!

किन ऐप्स को परमिशन दें?	किन ऐप्स के लिए तुरंत बंद करें?
SMS Permission: केवल आधिकारिक डिफॉल्ट मैसेज ऐप और बैंक/UPI ऐप को।	कैलकुलेटर, फोटो एडिटर, टॉर्च या गेम ऐप्स को SMS पढ़ने की अनुमति कभी न दें।
Accessibility: केवल फोन की आधिकारिक सिस्टम सेटिंग्स को।	व्हाट्सएप पर मिले किसी भी ऐप या अनधिकृत 'क्लीनर' ऐप को कभी न दें।
Location: केवल मैप्स और कैब ऐप्स को (वह भी "While using app")।	ऑफलाइन गेम्स, म्यूजिक प्लेयर या वॉलपेपर ऐप्स को लोकेशन कभी न दें।
Notification Access: केवल भरोसेमंद ब्रांड की स्मार्टवॉच ऐप को।	अनजान ऐप्स को नोटिफिकेशन पढ़ने का अधिकार न दें, वे OTP चुरा सकते हैं।

मार्गदर्शिका: फोन की App Permissions कैसे जांचें (4 सरल चरण)

हर महीने केवल 2 मिनट निकालकर अपने Android फोन में इन 4 चरणों का पालन करें:

1

Settings में जाएं

फोन की **Settings** खोलें और **Apps / Manage Apps** पर टैप करें।

2

Permission Manager खोलें

वहां दिए गए **Permission Manager** (अनुमति प्रबंधक) विकल्प को चुनें।

3

SMS और Accessibility देखें

सूची में **SMS** पर टैप करें। देखें कि किन-किन ऐप्स को यह अधिकार मिला हुआ है।

4

अनावश्यक ऐप्स से अधिकार हटाएं

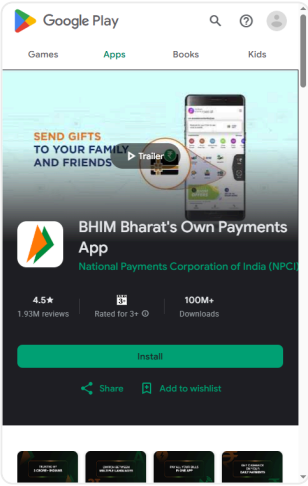
किसी गैर-जरूरी ऐप को SMS की अनुमति हो, तो तुरंत **"Don't Allow"** कर दें या ऐप को अनइंस्टॉल करें।

Google Play Store पर असली और नकली UPI ऐप की पहचान

साइबर अपराधी लोकप्रिय UPI ऐप्स के मिलते-जुलते नाम और लोगो बनाकर फर्जी क्लोन ऐप डाल देते हैं। असली ऐप की पहचान इन 3 बातों से

करें:

🌐 `play.google.com (Official App Store)` **NPCI आधिकारिक ऐप**



📌 Google Play Store आधिकारिक BHIM ऐप से 2 मुख्य सीख:

1. **आधिकारिक डेवलपर का नाम:** ऐप के नाम के नीचे डेवलपर देखें। BHIM ऐप के नीचे स्पष्ट लिखा है: `National Payments Corporation of India (NPCI)`। फर्जी ऐप्स के डेवलपर अज्ञात या अजीब नाम वाले होते हैं।

2. **सत्यापित डाउनलोड संख्या:** असली ऐप के 10 करोड़ से ज्यादा (100M+) डाउनलोड्स और लाखों समीक्षाएं हैं। फर्जी क्लोन ऐप के केवल कुछ सौ या हजार डाउनलोड होते हैं।

पब्लिक Wi-Fi, Juice Jacking और SIM Swap का खतरा

घर से बाहर निकलते समय फोन नेटवर्क और चार्जिंग को लेकर इन 3 बड़े खतरों से हमेशा सावधान रहें:

सार्वजनिक Wi-Fi (Public Wi-Fi)

रेलवे स्टेशन, बस स्टैंड या कैफे के खुले वाई-फाई पर बैठा कोई भी हैकर विशेष सॉफ्टवेयर से आपके इंटरनेट ट्रैफिक की जासूसी कर सकता है।

सुनहरा नियम: जब भी **UPI** से भुगतान करना हो, वाई-फाई बंद करें और केवल अपने सिम के **Mobile Data** का उपयोग करें।

Juice Jacking (सार्वजनिक चार्जिंग पोर्ट)

एयरपोर्ट या मेट्रो स्टेशनों पर लगे अनजान USB चार्जिंग केबल्स में डेटा चोरी की चिप्स लगी हो सकती हैं जो फोन में मालवेयर भेज सकती हैं।

सुनहरा नियम: हमेशा अपना एडॉप्टर (Plug) साथ रखें और सीधे बिजली के 3-पिन सॉकेट में चार्ज करें, न कि अज्ञात USB पोर्ट में।

SIM Swap Fraud (सिम क्लोनिंग)

ठग फर्जी दस्तावेजों से आपके नंबर का डुप्लीकेट सिम जारी करवा लेते हैं। जैसे ही नया सिम चालू होता है, आपके फोन से सिग्नल गायब हो जाता है।

सुनहरा नियम: यदि फोन का नेटवर्क अचानक बिना वजह गायब हो जाए और 'No Service' दिखाए, तो तुरंत ऑपरेटर और बैंक को सूचित करें।

अध्याय 12: स्मार्टफोन और ऐप सुरक्षा से जुड़े सवाल (Device Hardening FAQs)

Q1: क्या फिंगरप्रिंट लॉक चालू करने से UPI PIN की जरूरत खत्म हो जाती है?

उत्तर: नहीं। UPI से पैसे भेजने के लिए NPCI के नियमानुसार 4 या 6 अंकों का UPI PIN डालना अनिवार्य है। फिंगरप्रिंट केवल UPI ऐप को खोलने (App Lock) के लिए इस्तेमाल होता है, पैसे भेजने के लिए नहीं।

Q2: फोन में 'Install Unknown Apps' सेटिंग हमेशा बंद क्यों रखनी चाहिए?

उत्तर: यदि यह सेटिंग On रहती है, तो WhatsApp या Chrome ब्राउज़र से कोई भी खतरनाक वायरस या जासूसी .apk फाइल आपकी अनुमति के बिना

फोन में इंस्टॉल हो सकती है। इसे हमेशा 'Off' रखें।

Q3: क्या फोन खो जाने पर घर बैठे उसे स्थायी रूप से ब्लॉक किया जा सकता है?

उत्तर: हां! भारत सरकार के दूरसंचार विभाग के **CEIR पोर्टल (sancharsaathi.gov.in)** पर जाकर आप अपने 15 अंकों के IMEI नंबर की मदद से खोए हुए फोन को पूरे भारत में पूरी तरह ब्लॉक कर सकते हैं।

Q4: क्या नया फोन लेने पर पुराना फोन बेचते समय फैक्टरी रीसेट काफी है?

उत्तर: पुराना फोन बेचने से पहले सभी UPI और बैंकिंग ऐप्स से लॉग-आउट करें, अपना Google/iCloud अकाउंट हटाएं, और फिर **Factory Data Reset** करें ताकि आपका कोई भी बैंकिंग डेटा पुराने फोन में न रह जाए।

Q5: क्या फोन के ऑपरेटिंग सिस्टम (Android/iOS) को अपडेट करना जरूरी है?

उत्तर: अत्यंत आवश्यक है! हर सिस्टम अपडेट में कंपनियों द्वारा नई सुरक्षा खामियों और वायरस से बचाव के सिक्योरिटी पैच (Security Patches) दिए जाते हैं। पुराना सॉफ्टवेयर हैकर्स के लिए आसान निशाना होता है।

स्मार्टफोन सुरक्षा: क्या करें और क्या न करें

✅ क्या करें (Do's)	❌ क्या न करें (Don'ts)
फोन की स्क्रीन लॉक और **UPI PIN** दोनों को पूरी तरह अलग रखें।	जन्म वर्ष, गाड़ी नंबर या 1234 जैसे आसान पिन का उपयोग न करें।
केवल आधिकारिक Google Play Store या Apple App Store से ही ऐप डाउनलोड करें।	WhatsApp या Telegram पर आई अनजान `.apk` फाइलों को फोन में इंस्टॉल न करें।
हर महीने फोन के **Permission Manager** में जाकर गैर-जरूरी परमिशन बंद करें।	कैलकुलेटर या फोटो एडिटर ऐप्स को SMS या Accessibility परमिशन न दें।
बैंकिंग लेनदेन के लिए केवल अपने सिम के **Mobile Data** का उपयोग करें।	रेलवे स्टेशन या होटल के खुले सार्वजनिक वाई-फाई पर UPI पेमेंट न करें।
फोन खो जाने पर तुरंत **sancharsaathi.gov.in (CEIR)** पर फोन ब्लॉक कराएं।	गूगल पर फर्जी मोबाइल ट्रैकर खोजकर किसी अनजान को पैसे न दें।

Google पर चोरी हुआ फोन ब्लॉक करने का सरकारी पोर्टल (CEIR Guide)

यदि आपका फोन खो जाए या चोरी हो जाए, तो भारत सरकार के आधिकारिक CEIR पोर्टल पर जाने के लिए यह तरीका अपनाएं:

🔍 `"sanchar saathi ceir block lost stolen mobile official portal"`

1

चरण 1: CEIR फोन ब्लॉकिंग पोर्टल को कोट्स में खोजें

ऊपर दिया गया वाक्य कोट्स के साथ सर्च बार में डालें ताकि गूगल केवल आधिकारिक सरकारी पोर्टल दिखाए।

2

चरण 2: sancharsaathi.gov.in डोमेन देखें

दूरसंचार विभाग का एकमात्र आधिकारिक पोर्टल `sancharsaathi.gov.in` है। किसी निजी ट्रैकर साइट पर न जाएं।

3

चरण 3: विज्ञापनों को छोड़कर असली CEIR पेज खोलें

सर्च रिजल्ट में दिखने वाले 'Sponsored' विज्ञापनों को छोड़कर असली लिंक पर ही क्लिक करें।

🔍 अध्याय 12 के सत्यापित आधिकारिक स्रोत (Official Sources)

- **DoT संचार साथी CEIR पोर्टल (खोया मोबाइल ब्लॉक):** https://sancharsaathi.gov.in (दूरसंचार विभाग, भारत सरकार)
- **NPCI आधिकारिक BHIM सुरक्षा निर्देश:** https://www.bhimupi.org.in
- **National Cyber Crime Reporting Portal:** https://www.cybercrime.gov.in (गृह मंत्रालय, भारत सरकार)

अध्याय 13 • अंतिम अध्याय (Master Pocket Reference)

UPI Safety Checklist

रोज़मर्रा के उपयोग के लिए एक पन्ने का सम्पूर्ण सुरक्षा कार्ड। अपने फोन में सहेजें, प्रिंट करें या परिवार और मित्रों के साथ साझा करें। इस एक चेकलिस्ट में पूरी किताब का निचोड़ समाया है।

आपकी जेब में संपूर्ण UPI सुरक्षा कार्ड

UPI आज भारत के 40 करोड़ से अधिक नागरिकों के दैनिक जीवन का अटूट हिस्सा बन चुका है। लेकिन सुविधा के साथ सुरक्षा का अनुशासन ही आपकी गाढ़ी कमाई की असली ढाल है।

इस अंतिम अध्याय में पूरी ई-बुक के 12 अध्यायों के सबसे महत्वपूर्ण व्यावहारिक नियमों को **4 रंगीन सुरक्षा कार्ड्स** में संजोया गया है। जब भी मन में कोई संदेह हो, केवल इस एक अध्याय को खोलकर देख लें।

1

Payment करने से पहले (Before Paying Checklist)

पैसे भेजने से पहले इन 6 बातों की पुष्टि अवश्य करें

- ✓ **10 सेकंड का सुरक्षा विराम (Security Pause):**

  किसी भी व्यक्ति के दबाव, हड़बड़ी या जल्दबाजी के माहौल में आकर कभी भी UPI PIN दर्ज न करें। स्क्रीन को 10 सेकंड ध्यान से पढ़ें।

- ✓ **CBS बैंक नाम का मिलान (Mandatory Verified Name):**

  QR कोड स्कैन करते ही स्क्रीन पर दिखने वाला नाम सामने वाले के बैंक खाते में दर्ज कोर बैंकिंग नाम से मिलाएं। केवल दुकान के बोर्ड पर न जाएं।

- ✓ **दुकान का भौतिक QR छूकर देखें:**

  सुनिश्चित करें कि असली स्टैंडी के ऊपर किसी धोखेबाज ने अपना फर्जी QR कोड स्टीकर तो नहीं चिपका रखा।

- ✓ **रुपये और शून्य (0) ध्यान से गिनें:**

  ₹500 की जगह गलती से ₹5,000 या ₹50,000 टाइप न हो जाए, इसे 'Pay' दबाने से पहले दो बार अवश्य जांचें।

- ✓ **केवल सुरक्षित Mobile Data का उपयोग:**

  रेलवे स्टेशन, बस स्टैंड या कैफे के खुले सार्वजनिक Wi-Fi पर कभी भी UPI से बैंकिंग लेनदेन न करें।

- ✓ **स्क्रीन के नीचे 'Debit' शब्द देखें:**

  सुनिश्चित करें कि स्क्रीन पर "Paying / Sending" लिखा हो, न कि कोई धोखेबाज "Collect Request" भेज रहा हो।

2

ये 7 गलतियां कभी न करें (Never Do This — Red Flags)

इन 7 गलतियों से 95% से अधिक वित्तीय साइबर अपराध होते हैं

पैसे पाने के लिए कभी PIN या OTP न डालें:

अटल नियम: UPI में पैसे प्राप्त करने (Receive) या रिफंड पाने के लिए कभी भी PIN या OTP की जरूरत नहीं होती।

ग्राहक का स्क्रीनशॉट या फोन कभी न मानें:

स्क्रीनशॉट केवल तस्वीर है। भुगतान की पुष्टि के लिए केवल अपने बैंक ऐप की पासबुक या साउंडबॉक्स की आवाज पर भरोसा करें।

स्क्रीन शेयरिंग ऐप (AnyDesk / TeamViewer) कभी न डालें:

बैंक या कस्टमर केयर बनकर कोई भी स्क्रीन शेयर ऐप डाउनलोड करने को कहे, तो तुरंत फोन काट दें।

Google पर 'कस्टमर केयर नंबर' कभी न खोजें:

सर्च इंजन विज्ञापनों में ठग अपने फर्जी मोबाइल नंबर डाल देते हैं। हमेशा बैंक पासबुक या ऐप के अंदर दिए सपोर्ट का उपयोग करें।

SMS में आए अनजान लिंक या .apk फाइलों पर क्लिक न करें:

बिजली बिल कटने, लॉटरी जीतने या कूरियर पेंडिंग होने के फर्जी SMS में दिए गए लिंक को कभी न खोलें।

स्क्रीन लॉक और UPI PIN कभी एक न रखें:

फोन अनलॉक करने का पासवर्ड और बैंक का UPI PIN हमेशा पूरी तरह अलग होना चाहिए।

'Digital Arrest' की धमकी में आकर पैसे न भेजें:

भारतीय कानून में डिजिटल अरेस्ट का कोई वजूद नहीं है। पुलिस कभी फोन या वीडियो कॉल पर पैसे नहीं मांगती।

3

जब Payment में समस्या आए (If Problem Occurs)

पैसे अटकने या गलत खाते में जाने पर सही क्रम

पैसे कटने पर दोबारा पेमेंट न दोहराएं:

यदि पैसा कट गया पर सामने वाले को नहीं मिला, तो तुरंत दोबारा पैसे न भेजें। 2 से 3 घंटे इंतजार करें।

RBI T+1 Auto-Reversal नियम याद रखें:

असफल लेनदेन का पैसा अगले कार्यदिवस (T+1) तक स्वतः आपके खाते में वापस आ जाना अनिवार्य है।

देरी होने पर ₹100 प्रतिदिन का मुआवजा (Compensation):

यदि T+1 दिन के बाद भी पैसा वापस न आए, तो बैंक बिना मांगे ₹100/दिन का मुआवजा आपके खाते में स्वतः जमा करेगा।

ऐप के अंदर UDIR डिस्प्यूट दर्ज करें:

लेनदेन के नीचे 'Raise Dispute' पर टैप करें और SMS से 12-अंकों का
UTR Number
सुरक्षित रख लें।

गलत खाते में पैसे जाने पर बैंक को लिखित दें:

UTR नंबर के साथ अपने बैंक में तत्काल आवेदन दें ताकि लाभार्थी बैंक से राशि होल्ड करने का अनुरोध किया जा सके।

4

यदि Fraud हो जाए (Emergency Protocol)

शुरुआती 'Golden Hour' (2-3 घंटे) में तत्काल करने योग्य 4 कदम

कदम 1: तुरंत अपना UPI PIN बदलें

अपने आधिकारिक UPI ऐप में जाकर तुरंत UPI PIN रीसेट करें और नेटबैंकिंग पासवर्ड बदल दें।

कदम 2: बैंक से UPI सेवा अस्थायी रूप से बंद करवाएं

बैंक की आधिकारिक शाखा या मोबाइल ऐप में जाकर खाते पर UPI सेवा तुरंत फ्रीज करवाएं।

कदम 3: cybercrime.gov.in पर रिपोर्ट दर्ज कराएं

राष्ट्रीय साइबर पोर्टल पर 12-अंकों के UTR नंबर के साथ 'Report Financial Fraud' दर्ज करें ताकि ठग का बैंक खाता फ्रीज हो सके।

कदम 4: Acknowledgment Number लेकर बैंक शाखा जाएं

शिकायत की रसीद डाउनलोड करें और अपनी बैंक शाखा में जाकर लिखित पावती (Receiving) लें।

त्वरित आधिकारिक संदर्भ तालिका (Official Directory)

किसी भी धोखाधड़ी या समस्या की स्थिति में केवल भारत सरकार और रिज़र्व बैंक के इन आधिकारिक पोर्टल्स का उपयोग करें:

पोर्टल 1 **ऑनलाइन वित्तीय ठगी की रिपोर्ट**

आधिकारिक वेबसाइट:

`cybercrime.gov.in`

विशिष्ट सेक्शन:

Report Financial Fraud (नागरिक वित्तीय धोखाधड़ी रिपोर्ट)

सटीक Google Search:

```
"national cyber crime reporting portal official website"
```

पोर्टल 2 फर्जी SMS / संदिग्ध कॉल की शिकायत

🌐 आधिकारिक वेबसाइट:

`sancharsaathi.gov.in`

📌 विशिष्ट सेक्शन:

Chakshu (चक्षु पोर्टल • संदिग्ध फ्रॉड रिपोर्ट)

🔍 **सटीक Google Search:**

```
"sanchar saathi chakshu report suspected fraud"
```

पोर्टल 3 खोया या चोरी हुआ मोबाइल ब्लॉक करना

🌐 आधिकारिक वेबसाइट:

`sancharsaathi.gov.in`

📌 विशिष्ट सेक्शन:

CEIR (Block Stolen/Lost Mobile)

🔍 **सटीक Google Search:**

```
"sanchar saathi ceir block lost mobile portal"
```

पोर्टल 4 RBI डिजिटल सुरक्षा नियम व वीडियो

आधिकारिक वेबसाइट:

`rbikehtahai.rbi.org.in`

विशिष्ट सेक्शन:

Raju & Forty Thieves (राजू एंड द फॉर्टी थीव्स)

सटीक Google Search:

```
"RBI Kehta hai official digital banking awareness"
```

पोर्टल 5 बैंक द्वारा 30 दिन में समाधान न मिलने पर

आधिकारिक वेबसाइट:

`cms.rbi.org.in`

विशिष्ट सेक्शन:

RBI Banking Ombudsman (बैंकिंग लोकपाल)

सटीक Google Search:

```
"RBI CMS portal file banking ombudsman complaint"
```

गोल्डन रूल: इंटरनेट पर कभी 'कस्टमर केयर नंबर' सर्च न करें

सर्च इंजन के विज्ञापनों में ठग फर्जी मोबाइल नंबर डाल देते हैं। हमेशा केवल अपनी बैंक पासबुक या अधिकृत ऐप के भीतर दिए गए मेनू से ही संपर्क विवरण

प्राप्त करें।

ई-बुक के 5 सबसे महत्वपूर्ण सवाल (Final Recap FAQs)

Q1: क्या UPI से पैसे प्राप्त (Receive) करने के लिए कभी भी PIN डालना पड़ता है?

उत्तर: कभी नहीं! यह पूरी किताब का सबसे महत्वपूर्ण नियम है: *"पैसे भेजने के लिए PIN चाहिए, पाने के लिए कभी नहीं।"* यदि कोई पैसे देने के नाम पर PIN डालने को कहे, तो वह 100% ठग है।

Q2: अगर दुकानदार को पैसे ट्रांसफर करने के बाद उसके खाते में न पहुंचे तो क्या करें?

उत्तर: घबराकर तुरंत दोबारा पैसे न भेजें। अपने ऐप में UTR नंबर जांचें और 2-3 घंटे इंतजार करें। पैसा या तो दुकानदार को मिलेगा या आपके खाते में T+1 दिन में स्वतः वापस आ जाएगा।

Q3: अगर कोई पुलिस या CBI अफसर बनकर वीडियो कॉल पर डराए तो क्या करें?

उत्तर: तुरंत कॉल काट दें! भारतीय कानून में 'Digital Arrest' जैसी कोई

चीज नहीं है। देश की कोई भी पुलिस वीडियो कॉल पर पैसे नहीं मांगती।

Q4: अगर फोन चोरी हो जाए तो सबसे पहले क्या करें?

उत्तर: सबसे पहले अपने बैंक को फोन करके UPI सेवा बंद करवाएं, फिर टेलीकॉम ऑपरेटर से डुप्लीकेट सिम लें, और `sancharsaathi.gov.in (CEIR)` पर जाकर चोरी हुए फोन को ब्लॉक करवाएं।

Q5: क्या यह पूरी ई-बुक किसी भी समय ऑफलाइन पढ़ी जा सकती है?

उत्तर: हां! आप इस पूरी ई-बुक की PDF फाइल अपने मोबाइल में सुरक्षित रख सकते हैं और बिना इंटरनेट के कभी भी पढ़ सकते हैं।

🎉 बधाई!

आप एक जागरूक और सुरक्षित UPI नागरिक बन चुके हैं

आपने **UPI Safety Guide** के सभी 13 अध्याय सफलतापूर्वक पूरे कर लिए हैं। डिजिटल भुगतान आज भारत की सबसे बड़ी ताकत और क्रांति है। जब तक आप इन बुनियादी नियमों का पालन करेंगे, कोई भी साइबर अपराधी आपकी गाढ़ी कमाई को नुकसान नहीं पहुंचा सकता।

🤝 **सुरक्षा का संकल्प:** इस गाइड में सीखी गई बातों को अपने माता-पिता, बच्चों, बुजुर्गों और पड़ोसियों के साथ अवश्य साझा करें ताकि भारत का हर नागरिक ऑनलाइन ठगी से सुरक्षित रह सके।

📖 पूरी विषय सूची (Table of Contents) पर वापस जाएं →

कानूनी एवं शैक्षणिक अस्वीकरण (Disclaimer):

यह ई-बुक भारतीय रिज़र्व बैंक (RBI), राष्ट्रीय भुगतान निगम (NPCI), गृह मंत्रालय (MHA) और दूरसंचार विभाग (DoT) के सार्वजनिक दिशा-निर्देशों पर आधारित एक स्वतंत्र जन-जागरूकता पहल है। इसका उद्देश्य नागरिकों को वित्तीय सुरक्षा के प्रति जागरूक करना है। विशिष्ट कानूनी या बैंकिंग विवादों के लिए हमेशा अपने संबंधित बैंक की आधिकारिक शाखा या विधिक सलाहकार से संपर्क करें।

परिशिष्ट • APPENDIX

डिजिटल बैंकिंग पारिभाषिक शब्दकोश (Glossary)

VPA (UPI ID)

Virtual Payment Address — बैंक खाते का उपनाम जो खाता नंबर छिपाकर पैसे भेजने/पाने का सुरक्षित डिजिटल पता बनता है।

UTR Number

Unique Transaction Reference — हर सफल या असफल UPI लेनदेन का 12-अंकों

का विशिष्ट पहचान नंबर जो बैंक जांच में मुख्य साक्ष्य होता है।

2FA

Two-Factor Authentication — सुरक्षा की दोहरी परत (रजिस्टर्ड सिम कार्ड + आपका 4 या 6 अंकों का गोपनीय UPI PIN)।

CBS Name

Core Banking Solution Name — सामने वाले के बैंक खाते में दर्ज आधिकारिक सरकारी नाम, जो QR स्कैन करने पर स्क्रीन पर दिखता है।

UDIR

Unified Dispute and Issue Resolution — NPCI की स्वचालित प्रणाली जिससे फेल्ड पेमेंट की इन-ऐप शिकायत सीधे दोनों बैंकों के सर्वर से हल होती है।

Phishing

बैंक या अधिकृत पोर्टल जैसी दिखने वाली नकली वेबसाइट बनाकर पासवर्ड या कार्ड नंबर चुराने की साइबर साजिश।

Smishing

SMS Phishing — मोबाइल पर बिजली बिल, कूरियर या बैंक KYC के नाम से डराने वाला फर्जी मैसेज भेजकर खतरनाक लिंक पर क्लिक करवाना।

Mule Account

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

RAT (Screen Sharing)

Remote Access Trojan — AnyDesk या TeamViewer जैसे ऐप्स जिनके जरिए ठग दूर बैठकर आपके फोन की स्क्रीन और OTP लाइव देख लेते हैं।

CEIR

Central Equipment Identity Register — भारत सरकार के संचार साथी का आधिकारिक पोर्टल जिससे चोरी हुआ फोन पूरे देश में स्थायी रूप से ब्लॉक होता है।

चक्षु (Chakshu)

दूरसंचार विभाग (DoT) का आधिकारिक पोर्टल जहाँ संदिग्ध कॉल, फर्जी SMS और व्हाट्सएप ठगी की शिकायत सीधे दर्ज की जाती है।

TAT (समय-सीमा)

Turn Around Time — रिज़र्व बैंक द्वारा निर्धारित समय-सीमा (जैसे T+1 कार्यदिवस) जिसके भीतर फेल्ड पेमेंट का पैसा वापस लौटाना अनिवार्य है।

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

★ सुरक्षा का अंतिम संदेश

UPI सुरक्षा के 4 अटल स्वर्णिम नियम

1. **पैसे पाने के लिए कभी PIN नहीं:** UPI में पैसे प्राप्त करने या रिफंड के लिए कभी भी PIN या OTP की आवश्यकता नहीं होती।
2. **स्क्रीनशॉट केवल तस्वीर है:** कभी सामने वाले के फोन पर भरोसा न करें, केवल अपने बैंक ऐप या साउंडबॉक्स पर विश्वास करें।
3. **AnyDesk कभी डाउनलोड न करें:** फोन कॉल पर सहायता के नाम पर स्क्रीन शेयरिंग ऐप डाउनलोड कराने वाला 100% साइबर ठग होता है।
4. **गूगल पर हेल्पलाइन न खोजें:** सर्च इंजन के विज्ञापनों में ठगों के फर्जी नंबर होते हैं। हमेशा आधिकारिक बैंक ऐप का प्रयोग करें।

✓ 13 विस्तृत अध्याय | ✓ वास्तविक केस स्टडीज

✓ RBI व NPCI प्रमाणित | ✓ 48+ व्यावहारिक FAQs

राष्ट्रीय सुरक्षा संकल्प

डिजिटल भारत की शक्ति आपकी उंगलियों में है। जब आप सतर्क रहते हैं, तो आप केवल अपना पैसा नहीं बचाते, बल्कि पूरे भारत को साइबर अपराध से सुरक्षित बनाते हैं।

सुरक्षित UPI • सुरक्षित परिवार • सुरक्षित भारत

संस्करण 2026 • जनहित में जारी स्वतंत्र मार्गदर्शिका