National Cyber Crime Portal व RBI सुरक्षा नियमों पर आधारित

माँ-बाप और बुज़ुर्गों की Safety • 2026 Edition

The Parents Shield

माँ-बाप और बुज़ुर्गों को Fake Call, Pension Scam और UPI Fraud से बचाने की पूरी और आसान Pocket Guide

14	बड़े अक्षर	100%
आसान अध्याय	Senior Friendly	सरल बोलचाल हिंदी

Pension & Life Certificate

Fake Police & Digital Arrest

UPI PIN & QR Scam

AI Voice Clone Scam

WhatsApp Fraud Links

ATM Card Swapping

⚠ **Golden नियम:** पैसे आने के लिए दुनिया में कभी कोई UPI PIN या OTP नहीं डालना पड़ता। PIN केवल पैसे भेजने (कटने) के लिए होता है।

नागरिक जागरूकता Cyber Safety श्रृंखला

Mobile Pocket Size Edition • 120mm × 190mm

कानूनी सूचना • LEGAL NOTICE

कानूनी बातें और इस्तेमाल के नियम

1. जन-जागरूकता उद्देश्य (Awareness Only)

यह eBook केवल आम नागरिकों और बुज़ुर्गों में Digital सुरक्षा की समझ बढ़ाने के उद्देश्य से बनाई गई एक स्वतंत्र Guide है। इसका मकसद पाठकों को Phone Calls, Bank Scams और Pension Fraud के तरीकों से सावधान करना है। यह कोई कानूनी या Financial सलाह नहीं है।

2. किसी भी संस्था या सरकार से संबंध नहीं (No Affiliation)

यह eBook Reserve Bank of India (RBI), Telecom Department, National Cyber Crime Portal, NPCI, जीवन प्रमाण, किसी भी Bank या भारत सरकार के किसी मंत्रालय द्वारा प्रायोजित, समर्थित या अनुमोदित नहीं है। यह पूरी तरह से एक स्वतंत्र Digital Guide है।

3. ज़िम्मेदारी की सीमा (Limitation of Liability)

Cyber Safety नियम, सरकारी Portals के Links और काम करने के तरीके समय के साथ बदल सकते हैं। किसी भी पाठक के साथ होने वाले Fraud, पैसे के नुकसान या किसी समस्या के लिए यह eBook या इसके लेखक/प्रकाशक किसी भी रूप में कानूनी तौर पर ज़िम्मेदार नहीं होंगे। ताज़ा जानकारी के लिए हमेशा सरकारी विभाग या Bank की Official Website पर जाएँ।

4. Trademarks और Brand Names (Fair Use)

'UPI' NPCI का पंजीकृत Trademark है। 'WhatsApp' Meta Platforms का Trademark है। पुस्तक में बताए गए अन्य सभी नाम (जैसे PhonePe, Google Pay, SBI, AnyDesk, Airtel, Jio आदि) उनके असली मालिकों की संपत्ति हैं। इनका नाम केवल पहचान और लोगों को समझाने के लिए Fair Use के तहत लिया गया है।

5. केवल तरीकों की जानकारी (No Real Names)

इस Guide में दी गई सभी Case Studies और उदाहरण केवल समाज में चल रहे ठगी के तरीकों को समझाने के लिए काल्पनिक नामों से दिए गए हैं। इसका मकसद किसी असली कंपनी, संस्था या व्यक्ति पर आरोप लगाना नहीं है; केवल अपराध के तरीकों को उजागर किया गया है।

6. Single-User Digital License (इस्तेमाल का अधिकार)

यह PDF केवल व्यक्तिगत और पारिवारिक इस्तेमाल के लिए एक Single-User License के तहत दी गई है। इसे बिना लिखित अनुमति के सार्वजनिक रूप से Re-upload करना, बेचना या व्यावसायिक उपयोग में लाना कॉपीराइट कानून के तहत वर्जित है।

संपादकीय • EDITORIAL PREFACE

हमारे माँ-बाप की डिजिटल ढाल

आज की तेजी से बदलती डिजिटल दुनिया में हमारे बुजुर्ग (माता-पिता और दादा-दादी) सबसे ज्यादा भरोसेमंद और सीधे होते हैं। ठग उनकी इसी मासूमियत, डर और तकनीकी झिझक का फायदा उठाते हैं।

> “
> ठग कभी तकनीक को Hack नहीं करते, वे इंसान के **डर (Panic)**, **मुसीबत के नाटक** और **अत्यधिक विश्वास** को निशाना बनाते हैं।

माँ-बाप के 3 मूल सुरक्षा सूत्र:

1. पैसे लेने के लिए PIN नहीं चाहिए: जब भी कोई कहे कि आपके खाते में Pension या पैसे भेज रहा हूँ इसलिए PIN या OTP डालो — तुरंत समझें कि वह 100% Fake है।

2. Video Call पर कोई Police नहीं होती: असली पुलिस, CBI या कोर्ट कभी WhatsApp या Skype पर Digital Arrest नहीं करती।

3. बच्चों से बात किए बिना कभी Transfer न करें: मुसीबत या गिरफ्तारी के नाम पर कोई भी फोन आए, पहले अपने बच्चों के असली नंबर पर फोन करके सच पता करें।

इस Pocket Guide का उद्देश्य: हर परिवार के बुजुर्गों को बड़े अक्षरों में, बिना किसी कठिन अंग्रेजी शब्द या तकनीकी उलझन के, रोजमर्रा के 14 सबसे खतरनाक Scams से पूरी तरह सुरक्षित और आत्मनिर्भर बनाना।

विषय सूची • COMPLETE TABLE OF CONTENTS

The Parents Shield: सभी 14 अध्याय

01 **बुज़ुर्गों के साथ Fraud क्यों ज़्यादा होता है**
मासूमियत, तकनीकी झिझक और डर का फायदा

02 **UPI क्या है, बिल्कुल आसान भाषा में**
बैंक खाते से सीधे पैसे भेजने का सुरक्षित तरीका

03 **UPI PIN और OTP: कभी किसी को न बताएँ**
PIN केवल पैसे कटने के लिए — पैसे आने के लिए नहीं

04 **Fraud Call: Bank, KYC और Digital Arrest**
नकली पुलिस, CBI और कोर्ट के डर का सच

05 **WhatsApp के Fraud Message और Link**
बिजली बिल, लॉटरी और APK फाइल का खतरा

06 **Fake Payment और QR Scam**
फर्जी SMS और पैसे भेजने के नाम पर QR स्कैन कराना

07 **"बेटा, मैं मुसीबत में हूँ": AI Voice Scam**
बच्चों की आवाज में एक्सीडेंट और जेल का नाटक

08 **Pension और सरकारी Scheme के नाम पर Fraud**
Life Certificate अपडेट और खाते में पेंशन रुकने का डर

09 **रिश्तेदार या बच्चे बनकर पैसे माँगना**
नया नंबर बताकर इमरजेंसी में UPI ट्रांसफर माँगना

10 **"मैं मदद कर दूँ" कहने वाले अनजान लोग**
ATM मशीन, बैंक लाइन और फोन में AnyDesk ऐप

11 **पैसे भेजने से पहले ये ज़रूर पूछें**
3 सेकंड का ठहराव और परिवार से फोन पर पक्का करना

12 **Fraud हो जाए तो क्या करें**
Golden 2 Hours, बैंक खाता ब्लॉक और Cyber Crime रिपोर्टिंग

13 **घर वालों के लिए: माँ-बाप को ये कैसे सिखाएँ**
प्यार से समझाना, फोन सेटिंग्स और दैनिक सुरक्षा नियम

14 **बुज़ुर्गों की Master Safety Checklist**
5 सबसे बड़े नियम — अलमारी और फोन के पास चिपकाने योग्य

अध्याय 1 • माता-पिता की DIGITAL सुरक्षा

बुज़ुर्गों के साथ Fraud क्यों ज़्यादा होता है

इंसानी भरोसा, SmartPhone की नई दुनिया और Scammer के डर की पूरी सच्चाई।

Phone की घंटी और मीठी बातें: Scammer कैसे जाल बिछाता है?

सोचिए, घर में बैठे आपके पिताजी या माताजी के Phone पर एक Call आती है। सामने वाला बहुत ही आदर से बोलता है: *"प्रणाम बाबूजी, मैं आपके Pension Office से बोल रहा हूँ। आपके Bank खाते में जीवन प्रमाण पत्र (Life Certificate) का काम रुका हुआ है। अगर 10 मिनट में ठीक नहीं हुआ, तो इस महीने की Pension रुक जाएगी।"*

बुज़ुर्ग व्यक्ति घबरा जाता है। वह सोचता है कि सामने वाला सच बोल रहा है और उसकी मदद करना चाहता है। Scammers अक्सर नौजवानों के मुकाबले घर के बड़े-बुज़ुर्गों को ही अपना सबसे आसान शिकार बनाते हैं।

सच्चाई समझें

Scammers बुज़ुर्गों को ही क्यों चुनते हैं?

हमारे माता-पिता ने अपनी पूरी ज़िंदगी मेहनत करके बचत की है। उनके Bank खाते में Pension या Retirement का पैसा होता है। साथ ही, वे दूसरों की बातों पर जल्दी विश्वास कर लेते हैं और SmartPhone की बारीक जानकारियों से अनजान होते हैं।

> **सीधी बात:** जब कोई अनजान व्यक्ति Call पर ज़रूरत से ज़्यादा आदर दिखाए या अचानक बड़ी मुसीबत का डर पैदा करे, तो समझ जाइए कि दाल में कुछ काला है।

Case Study: Pension बंद होने का झूठा डर

देखें कैसे Scammer मीठी बातें करके और डर दिखाकर बुज़ुर्गों को फँसाता है:

📞 PHONE CALL SIMULATION (FAKE PENSION OFFICER)

Scammer (बहुत ही मीठी और आदर भरी आवाज़): "नमस्ते Uncle जी, मैं मुख्य Pension Office से बात कर रहा हूँ। आपकी Pension File में एक तकनीकी कमी आ गई है। अगर इसे आज ठीक नहीं किया तो खाता Freeze हो जाएगा।"

सीधे-सादे बुज़ुर्ग: "अरे बेटा, ऐसा कैसे हो गया? मुझे क्या करना होगा? मेरी तो दवाइयों का खर्च भी इसी से चलता है।"

Scammer: "Uncle जी आप बिल्कुल चिंता मत कीजिए, मैं आपकी पूरी मदद करूँगा। आपके Phone पर अभी 6 अंकों का एक Security Code (OTP) आया होगा, बस वह बता दीजिए, मैं यहीं से सब ठीक कर देता हूँ।"

सच्चाई: *(वह Code असल में Bank से पैसे निकालने का OTP था! जैसे ही बुज़ुर्ग ने Code बताया, उनके Bank खाते से जीवन भर की जमा पूँजी साफ़ हो गई।)*

Scammer का 4-Step Trap: बुज़ुर्गों को फँसाने की चाल

1 **आदर से बातचीत की शुरुआत**

Scammer "प्रणाम चाचाजी" या "नमस्ते बाबूजी" कहकर बात शुरू करता है ताकि बुज़ुर्ग को लगे कि सामने वाला कोई भला इंसान है।

↓ अचानक बड़ी मुसीबत का नाटक

2 **Pension, Bank या बिजली कटने का डर**

कहा जाता है: "आज रात SIM बंद हो जाएगा", "Pension रुक जाएगी" या "बिजली का बिल तुरंत भरें वरना कनेक्शन कटेगा।"

↓ सोचने या बच्चों से पूछने का मौका न देना

3 **Code (OTP) या App Download का दबाव**

Scammer कहता है: "किसी को बताने का समय नहीं है, बस Phone पर आया Code बताएँ या यह Link दबाएँ।"

↓ पैसा गायब और Call Block

4 **Bank खाता खाली और पछतावा**

जैसे ही Code बताया या Link दबाया, Bank से सारे पैसे कट जाते हैं और सामने वाला तुरंत Phone काट देता है।

असली अधिकारी vs Fake Caller: 3 सबसे बड़े फर्क



1. असली Bank कभी Code (OTP) नहीं माँगता

RBI का साफ़ नियम है: कोई भी असली Bank कर्मचारी कभी भी Call पर आपसे OTP, UPI PIN, या ATM Card के पीछे का Number नहीं माँगता।

> **नियम:** जो भी Call पर Code या OTP माँगे, वह 100% Scammer है।

🏛️

2. Pension Office कभी हड़बड़ी नहीं मचाता

सरकारी विभागों में किसी भी काम के लिए समय दिया जाता है। Call पर कोई भी सरकारी काम 10 मिनट में बंद नहीं होता।

📱

3. असली कंपनी कभी App Install नहीं कराती

कोई भी Bank या सरकारी विभाग Phone ठीक करने के नाम पर AnyDesk या TeamViewer जैसा Screen Sharing App Download नहीं कराता।

Official Portal: नागरिक सुरक्षा और शिकायत का केंद्र

भारत सरकार के गृह मंत्रालय ने नागरिकों की सुरक्षा के लिए **National Cyber Crime Reporting Portal** बनाया है। यहाँ किसी भी Online Fraud की सीधे शिकायत दर्ज की जाती है:

cybercrime.gov.in

Official सरकारी Portal



📌 **सरकारी Portal से 2 ज़रूरी बातें:**

1. **तुरंत Online शिकायत:** अगर किसी अनजान व्यक्ति ने धोखाधड़ी की है, तो `cybercrime.gov.in` पर जाकर सीधे शिकायत दर्ज कराई जा सकती है।
2. **Official Address की पहचान:** हमेशा Browser में देखें कि Website के पते के अंत में `.gov.in` लिखा हो। सरकारी Website की यह सबसे पक्की पहचान है।

सुरक्षित संपर्क का 3-Step नियम

कभी भी SMS, WhatsApp Message या Google Ad में दिखने वाले अनजान Numbers पर सीधे भरोसा न करें। हमेशा इस 3-Step रास्ते को अपनाएँ:

1. **Google पर सही सरकारी Website खोलें**
   अपने Browser में जाकर सीधे Official URL (जैसे `cybercrime.gov.in`) Type करें। किसी अनजान Link पर दबाकर कभी न जाएँ।
2. **Official Contact Us सेक्शन पर जाएँ**
   Official Website के मुख्य Menu में जाकर 'Contact Us' या 'Helpline' विकल्प पर Click करें।
3. **Official Number सीधे Website से लें**
   Website पर दिए गए Verified Helpline Number को देखकर ही अपने Phone से मिलाएँ।

अध्याय 1: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• अनजान Call पर डर या दबाव महसूस होते ही सीधे **Call काट दें**।

• कोई भी फैसला लेने से पहले अपने बेटे, बेटी या परिवार के सदस्यों से बात करें।

• Bank से जुड़ा कोई भी काम हो तो सीधे अपनी नज़दीकी Bank शाखा (Branch) में जाकर बात करें।

❌ यह कभी न करें (DONTs)

• Phone की Screen पर आया Code (OTP) या UPI PIN कभी किसी को न बताएँ।

• किसी अनजान व्यक्ति के कहने पर Phone में कोई नया App Download न करें।

• Pension या बिजली कटने की धमकी से घबराकर कभी तुरंत पैसे न भेजें।

OFFICIAL स्रोत व नियम

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

• Telecom Department (Sanchar Saathi Portal): `sancharsaathi.gov.in`

• Reserve Bank of India (RBI Senior Citizen Awareness): `rbi.org.in`

अध्याय 2 • UPI की आसान समझ

UPI क्या है, बिल्कुल आसान भाषा में

नकद पैसे रखने की चिंता खत्म: सीधे Bank से Bank पैसे भेजने और पाने का आसान तरीका।

Phone से पैसे कैसे जाते हैं?

सोचिए जैसे पुराने ज़माने में डाकिया आपकी चिट्ठी सही पते पर पहुँचाता था, वैसे ही **UPI** आपके Bank से पैसे निकालकर सीधे सामने वाले के Bank खाते में पहुँचा देता है।

इसके लिए आपको न तो Bank की लाइन में खड़ा होना पड़ता है और न ही जेब में खुले पैसे रखने की चिंता होती है। बस अपने Phone में BHIM, Google Pay, PhonePe या Paytm जैसा कोई भी सुरक्षित App खोलना होता है।

सुनहरा नियम

पैसे आने और जाने का सबसे बड़ा फर्क

जब आप बाज़ार में फल या दवाइयाँ ख़रीदते हैं और दुकानदार को पैसे देते हैं, तब आपको अपना **UPI PIN** डालना पड़ता है।

लेकिन जब आपका बेटा या बेटी आपके खाते में पैसे भेजती है, तो आपको **कोई भी PIN या Button नहीं दबाना होता**। पैसा सीधे आपके खाते में जमा हो जाता है और Bank से Message आ जाता है।

> **सीधी बात:** PIN सिर्फ पैसे कटने के लिए होता है। पैसे आने के लिए दुनिया में कभी कोई PIN नहीं डालना पड़ता।

Case Study: "पैसे भेज रहा हूँ, PIN डालिए" वाली चाल

देखें कैसे Scammer सीधे-सादे बुज़ुर्गों को पैसे भेजने के नाम पर लूटता है:

📞 PHONE CALL SIMULATION (FAKE PAYMENT SENDER)

> **Scammer (घबराया हुआ नाटक करते हुए):** "अरे चाचाजी, आपके दामाद जी ने मुझे आपके खाते में ₹15,000 भेजने को कहा था। मैंने आपके Phone पर एक Link भेजा है, उस पर Click करके अपना UPI PIN डाल दीजिए ताकि पैसे आपके खाते में आ जाएँ!"

> **समझदार बुज़ुर्ग:** "बेटा, पैसे लेने के लिए PIN क्यों डालना? मेरे Bank ने मुझे सिखाया है कि पैसे आने पर कोई PIN नहीं लगता। मुझे कोई PIN नहीं डालना।"

> **सच्चाई:** *(सामने वाले ने असल में पैसे भेजने का नहीं, बल्कि पैसे काटने का Collect Request भेजा था! जैसे ही बुज़ुर्ग ने मना किया, Scammer ने तुरंत Call काट दिया और बुज़ुर्ग की मेहनत की कमाई बच गई।)*

UPI से सुरक्षित खरीदारी: 3 आसान Step

1

दुकान पर QR Code Scan करें

अपने Phone का UPI App खोलें और दुकान पर लगे QR Code के सामने Phone का Camera लाएँ।

↓ दुकान का नाम और रकम की जाँच

2

Screen पर नाम और रुपये देखें

देखें कि जितनी रकम आपको देनी है, Screen पर वही लिखी है और दुकानदार का नाम सही है।

↓ अपना Secret PIN डालें

3

UPI PIN डालें और Payment पूरा

अपना Secret PIN Screen पर छुपाकर डालें। Payment होते ही हरे रंग का सही (✓) का निशान आ जाएगा।

UPI के 3 फायदे और 1 बड़ी सावधानी



1. 24 घंटे तुरंत पैसा पहुँचना

रविवार हो या कोई छुट्टी, UPI हमेशा चालू रहता है। पैसे तुरंत सामने वाले के खाते में जमा हो जाते हैं।



2. हर लेन-देन का पक्का हिसाब

आपके Phone के App में हर Payment की तारीख और रकम दर्ज रहती है, जिससे हिसाब रखना आसान हो जाता है।



3. Bank खाते की जानकारी सुरक्षित

सामने वाले को आपके Bank का Account Number या Password नहीं पता चलता, केवल Mobile Number या UPI ID ही दिखती है।

⚠️

सबसे बड़ी सावधानी: PIN किसी को न दिखाएँ

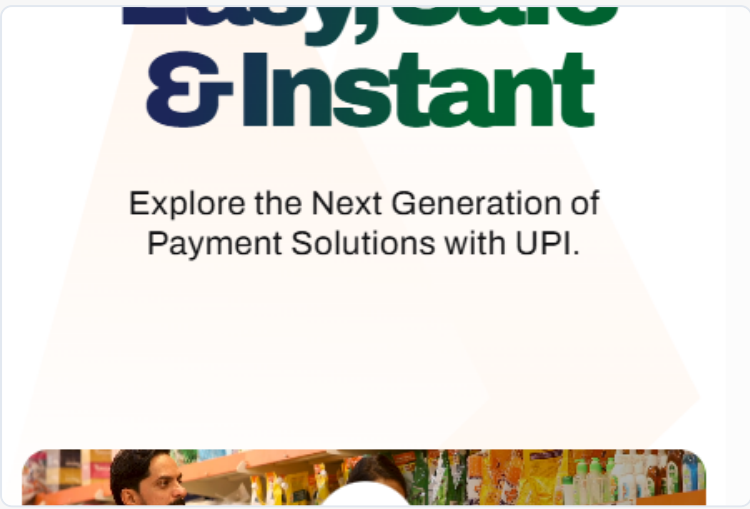
> जैसे घर की तिजोरी की चाबी सिर्फ आपके पास होती है, वैसे ही UPI PIN सिर्फ आपको पता होना चाहिए।

Official Portal: भारत सरकार और NPCI की देखरेख

भारत में UPI की पूरी व्यवस्था **National Payments Corporation of India (NPCI)** और **Reserve Bank of India (RBI)** की देखरेख में चलती है:

🌐 upichalega.com / npci.org.in (UPI Guide)

Official संस्था



📌 **NPCI की Official सलाह:**

1. **पैसे पाने के लिए कोई PIN नहीं:** NPCI का स्पष्ट नियम है कि किसी भी व्यक्ति से पैसे Receive करते समय UPI PIN दर्ज करने की आवश्यकता नहीं होती।
2. **Official App का ही उपयोग:** हमेशा Google Play Store या Apple App Store से जाँचे हुए Bank App ही Download करें।

Bank से संपर्क का सुरक्षित 3-Step नियम

अगर UPI लेन-देन में कोई समस्या आए, तो कभी Google पर Customer Care Number न ढूँढें। हमेशा यह 3-Step रास्ता अपनाएँ:

1. **अपने ATM Card का पिछला हिस्सा देखें**
   हर Debit Card या Passbook पर आपके Bank का असली Toll-Free Number लिखा होता है।
2. **Google पर सीधे Bank की Official Website खोलें**
   Browser के Address Bar में सीधे Bank का पक्का पता टाइप करें। Ads वाले Links से बचें।
3. **Website के Contact Us से Number लें**
   Bank की Official Website पर दिए गए जाँचे हुए Helpline Number पर ही Call मिलाएँ।

अध्याय 2: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• पैसे भेजते समय हमेशा Screen पर दुकानदार का नाम और रकम दोबारा जाँचे।

• UPI PIN डालते समय अपने हाथ की ओट बनाकर Screen को छुपा लें।

• लेन-देन पूरा होने के बाद अपने Bank से आए SMS को पढ़कर Confirm करें।

❌ यह कभी न करें (DONTs)

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

• किसी अनजान व्यक्ति के कहने पर अपने Phone का Lock या PIN न खोलें।

• Phone Call पर किसी को भी अपना UPI PIN या OTP बोलकर न बताएँ।

OFFICIAL स्रोत व नियम

• National Payments Corporation of India (UPI Safety Rules): `npci.org.in`

• Reserve Bank of India (RBI Kehta Hai - UPI Guidelines): `rbi.org.in`

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

अध्याय 3 • DIGITAL चाबी की सुरक्षा

UPI PIN और OTP: कभी किसी को न बताएँ

तिजोरी की चाबी आपके हाथ में: समझें क्यों Phone पर आया Code किसी को बताना सबसे बड़ा खतरा है।

छोटा सा Code, लेकिन जीवन भर की कमाई का पहरेदार

जब भी आप किसी अनजान व्यक्ति से Phone पर बात करते हैं, तो वह बहुत ही चालाकी और प्यार से कहता है: *"Uncle जी, आपके Phone पर एक छोटा सा 6 अंकों का Code आया होगा, बस वह बता दीजिए, मैं आपकी Pension File Update कर देता हूँ।"*

बुज़ुर्ग सोचते हैं कि सिर्फ एक Code बताने से क्या नुकसान हो सकता है? लेकिन सच्चाई यह है कि वह Code ही आपके Bank खाते का मुख्य ताला है।

सच्चाई समझें

UPI PIN और OTP में क्या अंतर है?

1. UPI PIN: यह 4 या 6 अंकों का वह Secret Code है जो आप खुद बनाते हैं। यह आपके घर की तिजोरी की मुख्य चाबी जैसा है। यह केवल पैसे भेजते समय डाला जाता है।

2. OTP (One Time Password): यह 6 अंकों का वह अस्थाई Code है जो Bank आपके Mobile Number पर SMS के ज़रिए भेजता है। जब भी खाते से पैसे निकलते हैं, Bank यह Code भेजकर पूछता है कि क्या सच में आप ही पैसे निकाल रहे हैं।

> **सीधी बात:** जैसे आप घर की चाबी किसी राह चलते अजनबी को नहीं सौंपते, वैसे ही OTP और PIN कभी किसी को मुँह से नहीं बताना चाहिए।

Case Study: "Account Block हो जाएगा, OTP दीजिए"

देखें कैसे Scammer डर पैदा करके OTP निकलवाने की कोशिश करता है:

📞 PHONE CALL SIMULATION (FAKE BANK MANAGER)

Scammer (सख्त और रौबदार आवाज़): "मैं State Bank के Head Office से बोल रहा हूँ। आपका ATM Card आज रात 12 बजे Block कर दिया जाएगा। इसे चालू रखने के लिए आपके Phone पर एक Verification Code भेजा है, तुरंत बताइए!"

सतर्क माता-पिता: "अगर Card में कोई समस्या है तो मैं कल सुबह खुद Bank Branch जाकर बाबूजी से मिल लूँगा। Phone पर मैं कोई Code नहीं बताऊँगा।"

Scammer (गुस्से में): "अगर अभी नहीं बताया तो ₹10,000 जुर्माना लगेगा और खाता कभी नहीं खुलेगा!"

सच्चाई: *(माता-पिता ने तुरंत Call काट दी। जब अगले दिन Bank जाकर पता किया, तो खाता पूरी तरह सुरक्षित था।*

Scammer सिर्फ झूठा डर दिखाकर पैसे चुराना चाहता था।)

OTP चुराने का 4-Step जाल

1 **अचानक डराने वाली Call**

Scammer कहता है: "Debit Card बंद हो गया", "बिजली कट जाएगी", या "गलती से आपके खाते में पैसे आ गए हैं।"

↓ मदद करने का झूठा दिखावा

2 **Phone पर SMS आने की बात कहना**

Scammer अपने Computer पर आपके Bank का Portal खोलता है और Forgot Password या Money Transfer दबाता है।

↓ आपके Phone की Screen पर Code आना

3 **हड़बड़ी में Code माँगना**

Scammer कहता है: "जल्दी बताइए सिर्फ 30 Second का समय है, वरना सब कुछ बंद हो जाएगा।"

↓ Code डालते ही खाता खाली

4 **पैसा उड़ाया और Call Disconnect**

जैसे ही आपने Code बताया, Scammer के खाते में सारा पैसा चला जाता है और उसका Number तुरंत Switch Off हो जाता है।

RBI का स्पष्ट नियम: जो हर नागरिक को जानना चाहिए

1. कोई असली Bank कर्मचारी OTP नहीं माँगता

RBI के नियमों के अनुसार किसी भी Bank अधिकारी को ग्राहक से OTP, PIN या CVV माँगने का अधिकार नहीं है।

> **नियम:** जो भी Call पर Code या OTP माँगे, वह 100% धोखेबाज़ है।



2. SMS में साफ़ लिखा होता है सच

जब भी OTP आए, Message को ध्यान से पढ़ें। उसमें लिखा होता है: *"Do not share this OTP with anyone for payment of ₹..."*



3. PIN को हमेशा गुप्त रखें

अपने UPI PIN को कभी Phone के Cover पर, डायरी के पहले पन्ने पर या Passbook पर लिखकर न रखें।

गलती से पैसे कट जाएँ या Fraud हो जाए तो क्या करें?

अगर कभी अनजाने में गलत Payment हो जाए या कोई आपसे OTP/PIN लेकर धोखा कर दे, तो घबराएँ नहीं। तुरंत नीचे दिए गए सही और पक्के रास्ते अपनाएँ:

🌐 npci.org.in (Official Complaint Guide) Official सरकारी संस्था

📌 **तुरंत करने वाले 3 आसान काम:**

1. **Bank को तुरंत बताएँ:** सबसे पहले अपने Bank के Official Website पर जाकर Contact Us सेक्शन से Bank का असली Number लें, या पास की Bank Branch में जाकर अपना Account और ATM Card तुरंत Block करवाएँ।
2. **NPCI की Official Site पर Complaint दर्ज करें:** Browser में सीधे `npci.org.in` टाइप करें। वहाँ 'UPI Complaint' / 'Dispute' सेक्शन में जाकर अपनी Transaction Details के साथ शिकायत दर्ज करें।
3. **Cyber Crime Portal पर Report करें:** घर के किसी सदस्य की मदद से `cybercrime.gov.in` पर जाकर तुरंत Online Complaint लिखवाएँ, ताकि ठग के खाते में पैसा Freeze हो सके।

सुरक्षित संपर्क का 3-Step नियम

अगर कोई व्यक्ति Call पर OTP माँगे, तो तुरंत Call काटें और असली Bank से संपर्क के लिए यह 3-Step रास्ता अपनाएँ:

1. **Google पर सही Bank Website खोलें**
   Browser के Address Bar में सीधे Bank का Official URL टाइप करें। किसी अनजान Message के Link पर Click न करें।

2. **Official Contact Us सेक्शन पर जाएँ**
   Website के मुख्य Menu में जाकर 'Contact Us' या 'Customer Care' विकल्प पर Click करें।

3. **Official Number सीधे Website से लें**
   Website पर दिए गए Verified Helpline Number को देखकर ही अपने Phone से मिलाएँ।

अध्याय 3: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• Phone पर कोई Code माँगने पर बिना सोचे तुरंत **Call काट दें**।

• Bank से आए हर Message को शांति से और पूरा पढ़ें।

• कोई भी संशय होने पर सीधे अपने बच्चों या Bank Branch के कर्मचारियों से बात करें।

❌ यह कभी न करें (DONTs)

• Phone Call, WhatsApp या SMS पर किसी को भी अपना OTP न बताएँ।

• अपना UPI PIN कभी किसी डायरी या Phone Cover पर लिखकर न छोड़ें।

• हड़बड़ी या डर में आकर कभी भी अनजान व्यक्ति की बातों में न आएँ।

OFFICIAL स्रोत व नियम

• Reserve Bank of India (Customer Protection & OTP Guidelines): `rbi.org.in`

• National Payments Corporation of India (Dispute Redressal): `npci.org.in`

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

अध्याय 4 • FAKE CALLS की पूरी सच्चाई

Fraud Call: Bank, KYC और Digital Arrest

वर्दी का रौब, नकली अदालत का नाटक और कमरे में बंद करने की धमकी: जानिए कैसे बचें।

Video Call पर Police की वर्दी: एक भयानक नाटक

सोचिए, घर में शांति से बैठे आपके पिताजी के Phone पर एक Video Call आती है। Screen पर सामने Police की वर्दी पहने एक आदमी बैठा दिखता है। उसके पीछे Police Station का बोर्ड और भारत का नक्शा लगा होता है।

वह बहुत ही रौबदार आवाज़ में कहता है: *"आपके आधार Card पर एक Parcel मिला है जिसमें नशीली दवाइयाँ हैं। सुप्रीम कोर्ट ने आपका अरेस्ट वारंट जारी कर दिया है। आप अभी अपने कमरे का दरवाज़ा बंद कर लीजिए, किसी से बात मत कीजिए और Video Call चालू रखिए!"*

कानूनी सच

'Digital Arrest' केवल एक झूठा फरेब है

भारत के कानून में **Digital Arrest** नाम का कोई कानून या नियम नहीं होता। दुनिया की कोई भी Police, CBI या अदालत Video Call पर किसी को गिरफ़्तार नहीं करती और न ही Video Call पर मुक़दमे चलाती है।

Scammers सिर्फ बुज़ुर्गों के सीधेपन और डर का फायदा उठाते हैं ताकि वे घबराकर अपने Bank खाते के सारे पैसे उनके दिए खाते में Transfer कर दें।

> **सीधी बात:** जब भी कोई Video Call पर Police या Court का डर दिखाए, तो 1 Second भी बात न करें —सीधे Red Button दबाकर Call काट दें!

Case Study: कमरे में बंद रहने का दबाव

देखें कैसे Scammer नकली Police बनकर बुज़ुर्गों को मानसिक दबाव में लेता है:

📞 VIDEO CALL SIMULATION (FAKE POLICE OFFICER)

> **Scammer (वर्दी में, सख्त आवाज़):** "यह देश की सुरक्षा का मामला है। अगर आपने कमरे से बाहर पैर रखा या अपने बेटे को बताया, तो पूरे परिवार को जेल भेज दूँगा। अपनी सारी FD और Bank Balance हमारे RBI Verification Account में तुरंत Transfer कीजिए!"

> **जागरूक बुज़ुर्ग:** "अगर मेरे खिलाफ कोई FIR है तो आप मेरे घर के पते पर लिखित नोटिस भेजिए। मैं नज़दीकी Police Station खुद अपने परिवार के साथ जाऊँगा।"

> **सच्चाई:** *(जैसे ही बुज़ुर्ग ने अपने परिवार के साथ स्थानीय Police Station जाने की बात कही, Scammer ने तुरंत Video Call बंद कर दी और उसका Number Block हो गया। बुज़ुर्ग के ₹20 लाख सुरक्षित बच गए।)*

Digital Arrest का 4-Step Trap

1 **Courier या SIM Block का बहाना**

Scammer कहता है: "आपके नाम से भेजे गए Parcel में अवैध सामान मिला है या आपका SIM गैर-कानूनी काम में इस्तेमाल हुआ है।"

↓ तुरंत Video Call से जोड़ना

2 **नकली Police Station का सेट**

Scammer नकली वर्दी, वायरलेस सेट की आवाज़ और सरकारी मुहर वाले Fake Arrest Order Screen पर दिखाता है।

↓ परिवार से अलग-थलग करना

3 **कमरे में अकेले रहने की धमकी**

कहा जाता है: "Camera 24 घंटे ऑन रखिए, बच्चों से बात की तो वे भी जेल जाएँगे।" सोचने का कोई मौका नहीं दिया जाता।

↓ पैसे ट्रांसफर करवाते ही गायब

4 **सुरक्षित खाते के नाम पर लूट**

कहा जाता है: "जाँच पूरी होने तक सारा पैसा इस सरकारी खाते में Transfer करें।" पैसे आते ही

Scammers Call काट देते हैं।

असली कानून vs Fake Call: 3 सबसे बड़े नियम

⚖️

1. कोई Digital Arrest नहीं होता

भारत सरकार के गृह मंत्रालय ने साफ़ कहा है: कानून में Video Call पर गिरफ़्तारी या जाँच का कोई प्रावधान नहीं है।

> **नियम:** Video Call पर Police की बात सुनना 100% गैर-कानूनी और Fake है।

👮

2. Police कभी पैसे नहीं माँगती

कोई भी असली Police अधिकारी कभी भी पैसे किसी खाते में Transfer करने को नहीं कहता। जो पैसे माँगे वह अपराधी है।

📱

3. SIM कभी 2 घंटे में बंद नहीं होता

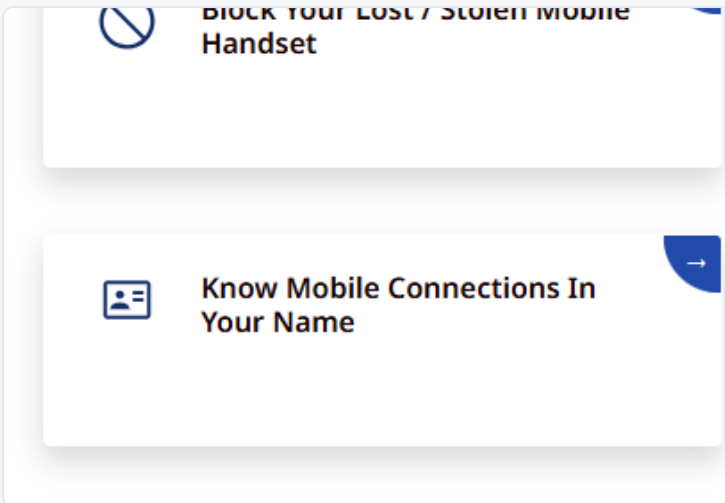
Telecom Department का नियम है कि बिना लिखित नोटिस के किसी भी ग्राहक का SIM अचानक बंद नहीं किया जा सकता।

Official Portal: Telecom Department की नागरिक सेवाएँ

भारत सरकार के Telecom Department ने नागरिकों की सुरक्षा के लिए **Sanchar Saathi** Portal बनाया है:

sancharsaathi.gov.in

Official सरकारी Portal



📌 **सरकारी Portal से 2 ज़रूरी बातें:**

1. **Fake Calls की शिकायत:** इस Portal पर जाकर Chakshu सुविधा के ज़रिए किसी भी Fake Call या Spoofed Number की सीधे Report की जा सकती है।
2. **अपने नाम के SIM की जाँच:** TAFCOP सुविधा से आप देख सकते हैं कि आपके आधार Card पर कितने Mobile Numbers चल रहे हैं।

सुरक्षित संपर्क का 3-Step नियम

अगर कोई Video Call पर Police या Court का डर दिखाए, तो तुरंत Call काटें और यह 3-Step रास्ता अपनाएँ:

1. **Google पर सही सरकारी Website खोलें**
   Browser के Address Bar में सीधे सरकारी Portal (जैसे `cybercrime.gov.in` या `sancharsaathi.gov.in`) Type करें।
2. **Official Contact Us सेक्शन पर जाएँ**
   सरकारी Website के मुख्य Menu में जाकर Contact Us या Help Desk पर Click करें।
3. **Official Number सीधे Website से लें**
   Official Website पर दिए गए जाँचे हुए Helpline Number को देखकर ही अपने Phone से मिलाएँ।

अध्याय 4: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• Video Call पर Police या कोर्ट का डर दिखाते ही तुरंत **Call काट दें**।

• तुरंत कमरे से बाहर निकलें और अपने बेटे, बेटी या परिवार के सदस्यों को पूरी बात बताएँ।

• यदि डर लगे तो सीधे अपने नज़दीकी स्थानीय Police Station में जाकर बात करें।

❌ यह कभी न करें (DONTs)

• किसी अनजान व्यक्ति के कहने पर कभी भी खुद को कमरे में अकेले बंद न करें।

• किसी तथाकथित सरकारी या सुरक्षित खाते में कभी एक भी रुपया Transfer न करें।

• डर या हड़बड़ी में आकर अपने Phone पर आया कोई भी Code (OTP) किसी को न दें।

OFFICIAL स्रोत व नियम

• Ministry of Home Affairs (I4C Advisory on Digital Arrest): `cybercrime.gov.in`

• Telecom Department (Sanchar Saathi Portal): `sancharsaathi.gov.in`

• Reserve Bank of India (Caution against Impersonation): `rbi.org.in`

अध्याय 5 • WHATSAPP संदेशों की सच्चाई

WhatsApp के Fraud Message और Link

बिजली कटने का डर, मुफ्त उपहार का लालच और खतरनाक APK Files: जानिए कैसे पहचानें।

WhatsApp पर नीले रंग का Link: एक छिपा हुआ फंदा

सोचिए, दोपहर के समय आपके WhatsApp पर एक Message आता है: *"बिजली विभाग की सूचना: प्रिय उपभोक्ता, आपका पिछले महीने का बिल Update नहीं हुआ है। आज रात 9:30 बजे आपके घर की बिजली काट दी जाएगी। तुरंत नीचे दिए गए Link पर दबाकर ₹10 का Payment करें!"*

बुज़ुर्ग सोचते हैं कि गर्मी के मौसम में रात को बिजली कट जाएगी तो बहुत मुसीबत होगी। वे बिना सोचे उस नीले Link पर दबा देते हैं। यहीं से धोखाधड़ी शुरू होती है।

खतरे की पहचान

Link दबाते ही क्या होता है?

जब आप उस Link पर दबाते हैं, तो वह असली बिजली विभाग की नहीं, बल्कि Scammer द्वारा बनाई गई हुबहू नकली Website खोल देता है।

जैसे ही आप वहाँ अपना Bank Card या UPI PIN डालते हैं, Scammer के पास आपकी सारी जानकारी पहुँच जाती है और वह ₹10 की जगह खाते से ₹50,000 साफ़ कर देता है।

> **सीधी बात:** बिजली विभाग या सरकारी Office कभी भी किसी अनजान Mobile Number से WhatsApp पर बिजली काटने की धमकी नहीं भेजते।

Case Study: शादी के Card के नाम पर आया Virus (APK Scam)

देखें कैसे Scammer रिश्तेदार बनकर WhatsApp पर खतरनाक File भेजता है:

💬 **WHATSAPP CHAT SIMULATION (UNKNOWN NUMBER)**

> **अनजान Number (प्यार से):** "प्रणाम फूफाजी, हमारे छोटे भाई की शादी तय हो गई है। शादी का निमंत्रण पत्र नीचे भेज रहा हूँ, कृपया आशीर्वाद देने ज़रूर आएँ! 📎 `Wedding_Card.apk`"

> **सतर्क बुज़ुर्ग:** "अरे बेटा, यह Photo या PDF नहीं है, इसके आगे `.apk` लिखा है। मेरे बेटे ने मुझे सिखाया है कि ऐसी किसी File को कभी Install नहीं करना चाहिए।"

> **सच्चाई:** *(वह कोई शादी का Card नहीं था, बल्कि एक खतरनाक जासूसी App था! अगर बुज़ुर्ग उस पर Click करते, तो उनके Phone के सारे Messages और Bank OTP सीधे Scammer के पास पहुँच जाते।)*

WhatsApp Link Scam का 4-Step Trap

1

डराने या ललचाने वाला Message

Message आता है: "बिजली कटेगी", "₹25 लाख की लॉटरी लगी है" या "मुफ्त राशन Coupon पाएँ।"

↓ नीले रंग का Link दबाने का दबाव

2

अनजान Link पर Click करवाना

कहा जाता है: "तुरंत इस Link पर जाएँ वरना मौका हाथ से निकल जाएगा या जुर्माना लगेगा।"

↓ नकली Form में Bank जानकारी भरना

3

Card Number, PIN या OTP माँगना

खुलने वाली नकली Website पर आपसे आपका Name, Mobile Number, Debit Card और OTP माँगा जाता है।

↓ पैसा चोरी और Message Delete

4

खाता खाली और पछतावा

जैसे ही आपने जानकारी भरी, Bank खाते से तुरंत पैसे कट जाते हैं और भेजने वाला आपको Block कर देता है।

Fake Message की 3 सबसे बड़ी निशानियाँ

⚠️

1. सामान्य Mobile Number से आना

असली कंपनियाँ हमेशा अपने Verified नाम (जैसे VM-HDFCBK या AD-POWER) से SMS भेजती हैं, किसी 10 अंकों के अनजान Mobile Number से नहीं।

> **पहचान: 10 अंकों के Number से आया बिजली बिल का Message 100% Fake होता है।**

📎

2. .apk लिखी हुई File

अगर किसी Message के साथ आई File के नाम के अंत में .apk लिखा हो, तो उसे भूलकर भी न छुएँ। वह एक खतरनाक Virus है।



3. मुफ्त पैसे और लॉटरी का लालच

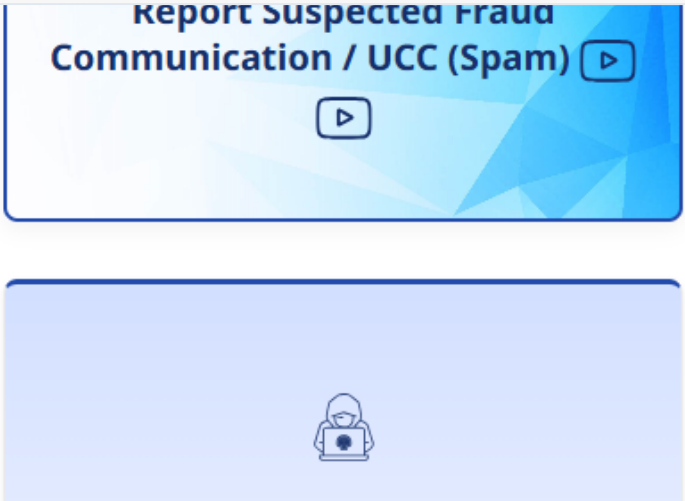
दुनिया में कोई भी कंपनी या सरकार बिना किसी कारण के घर बैठे लॉटरी या मुफ्त नकद पैसे नहीं बाँटती।

Official Portal: Fake Messages की सीधे Report करें

अगर आपको WhatsApp या SMS पर कोई डराने वाला या लॉटरी का Message आए, तो सरकार के **Chakshu Portal** पर उसकी सीधे Report करें:

🌐 sancharsaathi.gov.in/sfc (Chakshu)

Official सरकारी Portal



📌 **Chakshu Portal के 2 बड़े फ़ायदे:**

1. **Fraud Number Block करवाना:** आपके द्वारा Report करते ही Telecom Department उस ठग के Number और पूरे Network की जाँच करके उसे हमेशा के लिए बंद कर देता है।
2. **घर बैठे Report:** इसके लिए कहीं जाने की ज़रूरत नहीं है, सीधे Website खोलकर 2 मिनट में शिकायत दर्ज की जा सकती है।

बिजली बिल या सरकारी सूचना जाँचना: 3-Step नियम

जब भी बिजली या किसी बिल का Message आए, तो कभी Message में दिए Number पर Call न करें। यह सुरक्षित रास्ता अपनाएँ:

1. **अपना पुराना कागज़ी बिल देखें**
   घर में रखे पिछले महीने के असली बिजली बिल पर विभाग का सही Consumer Number और Helpline Number लिखा होता है।

2. **Google पर बिजली विभाग की Official Website खोलें**
   Browser के Address Bar में सीधे विभाग का Official URL टाइप करें। किसी अनजान Link से न जाएँ।

3. **Official Office जाकर बात करें**
   यदि कोई भी संशय हो, तो नज़दीकी बिजली सब-Station या Office में जाकर खुद आमने-सामने Confirm करें।

अध्याय 5: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• किसी भी बिल के Message को पहले अपने घर के बच्चों को दिखाएँ।

• बिजली या पानी का बिल केवल सरकार द्वारा मान्य Official App से ही भरें।

• Fake WhatsApp Messages को तुरंत Block और Report करें।

❌ यह कभी न करें (DONTs)

• WhatsApp पर आए किसी भी अनजान नीले Link पर कभी Click न करें।

• किसी अनजान व्यक्ति द्वारा भेजी गई `.apk` File को कभी Install न करें।

• बिना सोचे समझे किसी भी डर या लॉटरी वाले Message को आगे Forward न करें।

OFFICIAL स्रोत व नियम

• Telecom Department (Chakshu Suspected Fraud Reporting): `sancharsaathi.gov.in`

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

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

अध्याय 6 • QR CODE और FAKE PAYMENT का सच

Fake Payment और QR Scam

पैसे आने के नाम पर QR Code Scan करवाने का जाल और "गलती से पैसे आ गए" की पूरी सच्चाई।

"पैसे लेने के लिए QR Code Scan कीजिए" — सबसे बड़ा झूठ

सोचिए, आपने अपना कोई पुराना सामान बेचने के लिए Internet पर डाला, या किसी रिश्तेदार ने कहा कि वह आपको कुछ पैसे भिजवा रहा है।

तभी एक अनजान व्यक्ति Phone करता है और WhatsApp पर एक QR Code भेजकर कहता है: *"Uncle जी, मैंने आपको ₹10,000 भेज दिए हैं। आप इस QR Code को अपने PhonePe या Google Pay से Scan कीजिए, पैसे सीधे आपके खाते में आ जाएँगे!"*

सुनहरा नियम **QR Code का असली मतलब समझें**

QR Code का केवल एक ही काम होता है—**पैसे काटना (Payment करना)**.

जब आप दुकान पर कोई सामान खरीदते हैं और दुकानदार को पैसे देते हैं, तब आप QR Code Scan करते हैं और अपना PIN डालते हैं। लेकिन जब कोई आपको पैसे देता है, तो आपको **न तो QR Code Scan करना होता है और न ही PIN डालना होता है**।

> **सीधी बात:** पैसे Receive करने के लिए दुनिया में कभी कोई QR Code Scan नहीं करना पड़ता। जो Scan करने को कहे, वह 100% धोखेबाज़ है।

Case Study: "गलती से ₹45,000 ज़्यादा चले गए"

देखें कैसे Scammer दया की भावना का फायदा उठाकर पैसे ठगता है:

📞 PHONE CALL SIMULATION (EMOTIONAL BLACKMAIL)

Scammer (रोते हुए, घबराई आवाज़): "Uncle जी, मुझे किसी और को ₹50,000 भेजने थे, लेकिन गलती से आपके Number पर चले गए! आपके Phone पर ₹50,000 जमा होने का SMS भी आ गया होगा। मेरी माँ ICU में है, कृपया ₹45,000 तुरंत वापस भेज दीजिए वरना मैं बर्बाद हो जाऊँगा!"

समझदार बुज़ुर्ग: "बेटा, पहले मैं अपना Bank App खोलकर असली Passbook Check करूँगा कि सच में पैसा आया है या नहीं। बिना Balance Check किए मैं कोई पैसा नहीं भेजूँगा।"

सच्चाई: *(जब बुज़ुर्ग ने अपना Bank App खोला, तो खाते में एक भी रुपया नहीं आया था! वह SMS असल में Scammer ने किसी Computer Software से भेजा गया Fake SMS था। सतर्कता से बुज़ुर्ग के ₹45,000 बच गए।)*

QR Scam का 4-Step Trap

1 **WhatsApp पर QR Code भेजना**

Scammer कहता है: "मैं आपके खाते में Advance पैसे भेज रहा हूँ, यह सरकारी QR Code Scan कर लीजिए।"

↓ Phone Gallery से Scan करने का दबाव

2 **Scan From Gallery दबाना**

Scammer कहता है: "अपने PhonePe या Google Pay में जाकर 'Upload QR from Gallery' कीजिए।"

↓ Screen पर पैसे कटने की रकम आना

3 **UPI PIN डालने का झाँसा**

Scammer कहता है: "हाँ, अब अपना UPI PIN डालिए ताकि पैसा Receive हो सके।"

↓ PIN डालते ही पैसा गायब

4 **खाते से पैसे कटे और Call Block**

जैसे ही आपने PIN डाला, आपके Bank से पैसे कटकर Scammer के पास चले जाते हैं और उसका Phone बंद हो जाता है।

QR Code का असली गणित: समझें कब पैसा जाता है

🛒 **पैसे भेजना (दुकान पर Payment):**

दुकान का QR Code Scan करें → Screen पर रकम देखें → **अपना UPI PIN डालें** → खाते से पैसे कटे। (यह बिल्कुल सही है)

🛑 **पैसे पाना (Receive करना):**

कोई QR Scan नहीं → **कोई PIN नहीं डालना** → पैसा सीधे आपके खाते में आता है। अगर कोई Scan करने को कहे तो वह **धोखा** है!

Fake SMS vs असली Bank Message: 3 बड़े फर्क



1. Sender Header की पहचान

Bank का असली Message हमेशा 6 अक्षरों के Header (जैसे `AD-SBINB` या `VK-HDFCBK`) से आता है। किसी 10 अंकों के साधारण Mobile Number से नहीं।



2. App में Balance Check करना

जब तक अपने Bank App या Passbook में पैसा जमा न दिखे, तब तक किसी भी SMS को सच न मानें।

3. तुरंत रिफंड करने से इनकार

अगर कोई गलती से पैसे भेजने का दावा करे, तो उससे कहें: *"आप अपने Bank से संपर्क करें, मेरा Bank अपने आप इसे निपटाएगा।"*

सुरक्षित संपर्क का 3-Step नियम

अगर कोई QR Code भेजकर पैसे लेने का दबाव बनाए या Fake SMS भेजे, तो यह 3-Step रास्ता अपनाएँ:

1. **तुरंत अपना Bank App खोलें**
   अपने Phone का Official Bank App खोलें और 'Check Account Balance' या 'View Statement' पर जाएँ।

2. **Google पर सीधे Bank की Official Website देखें**
   किसी भी संशय की स्थिति में Bank के Official URL पर जाकर Contact Us सेक्शन देखें।

3 **अपने Bank Branch से संपर्क करें**

अपनी Bank Branch के शाखा प्रबंधक या परिचित अधिकारी से सीधे बात करके खाते की स्थिति Confirm करें।

अध्याय 6: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• पैसे आने का दावा होने पर हमेशा अपने Bank App में असली Balance Check करें।

• अनजान व्यक्ति की रोने-धोने वाली कहानियों पर बिना Confirm किए भरोसा न करें।

• किसी भी विवाद पर सीधे अपने घर के बच्चों को बताएँ।

❌ यह कभी न करें (DONTs)

• पैसे पाने (Receive करने) के लिए कभी भी QR Code Scan न करें।

• किसी के कहने पर PhonePe या Google Pay में अपना UPI PIN न डालें।

• केवल Phone पर आए SMS को देखकर किसी को भी पैसे वापस न भेजें।

OFFICIAL स्रोत व नियम

• National Payments Corporation of India (QR Safety Rules): `npci.org.in`

• Reserve Bank of India (RBI Kehta Hai - QR Code Safety): `rbi.org.in`

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

अध्याय 7 • AI VOICE CLONES की सच्चाई

"बेटा, मैं मुसीबत में हूँ": AI Voice Scam

अपनों की आवाज़ में रोने-चिल्लाने का नाटक, Accident का डर और AI आवाज़ से बचाव के अचूक नियम।

Phone पर अपने बच्चे की रोती हुई आवाज़

सोचिए, दोपहर के समय आपके Phone पर एक अनजान Number से Call आती है। आप Call उठाते हैं तो सामने से रोते हुए आपके अपने बेटे या बेटी की आवाज़ सुनाई देती है: *"पापा, मुझसे बहुत बड़ी गलती हो गई! मेरी गाड़ी से किसी का Accident हो गया है, Police मुझे लॉकअप में डाल रही है। ये वकील साहब का Number है, इन्हें तुरंत ₹60,000 भेज दीजिए वरना मेरी ज़िंदगी बर्बाद हो जाएगी!"*

किसी भी माता-पिता के लिए अपने बच्चे की रोती हुई आवाज़ सुनना सबसे भारी पल होता है। वे घबरा जाते हैं और बिना सोचे-समझे तुरंत पैसे भेजने के लिए तैयार हो जाते हैं।

तकनीक का सच

AI Voice Cloning क्या है?

आजकल Computer तकनीक (AI) इतनी आगे बढ़ चुकी है कि किसी भी इंसान की केवल 3 Second की आवाज़ सुनकर उसका हूबहू नकली क्लोन बनाया जा सकता है।

Scammers आपके बच्चों के Social Media (Instagram, Facebook या YouTube) से उनकी आवाज़ चुरा लेते हैं और फिर उसी आवाज़ में रोने, गिड़गिड़ाने का नाटक रचते हैं।

> **सीधी बात:** सिर्फ आवाज़ सुनकर यह तय न करें कि सामने सचमुच आपका बच्चा ही है। कोई भी कदम उठाने से पहले उसके असली Number पर दोबारा Call करें।

Case Study: "बेटा थाने में है" वाली झूठी Call

देखें कैसे सतर्क माता-पिता ने एक गुप्त सवाल पूछकर Scammer का भंडाफोड़ किया:

📞 PHONE CALL SIMULATION (FAKE AI VOICE OF SON)

Scammer (हूबहू बेटे की आवाज़ + रोते हुए): "मम्मी, मुझे Police ने पकड़ लिया है! मेरा Phone टूट गया है, इसलिए सिपाही के Phone से Call कर रहा हूँ। तुरंत इस UPI पर ₹40,000 भेजो वरना कोर्ट भेज देंगे!"

होशियार माँ (शांत रहकर): "बेटा, पहले यह बता कि तेरे कमरे की चाबी अलमारी के किस दराज़ में रखी है?"

Scammer (हड़बड़ाते हुए): "मम्मी क्या बकवास पूछ रही हो, मैं मुसीबत में हूँ और तुम चाबी पूछ रही हो!"

सच्चाई: *(माँ समझ गई कि यह नकली आवाज़ है क्योंकि बेटे को चाबी की जगह पता थी। माँ ने Call काटी और बेटे के असली Number पर Phone मिलाया। बेटा Office में शांति से बैठा लंच कर रहा था!)*

AI Voice Scam का 4-Step Trap

1

Social Media से आवाज़ चुराना

Scammer Facebook, Instagram या YouTube Video से आपके बेटे या बेटी की आवाज़ की Recording निकालता है।

↓ AI Software से हूबहू आवाज़ तैयार करना

2

अचानक भयानक Emergency Call

Accident, Police Case या अस्पताल में भर्ती होने का नाटक रचा जाता है ताकि सोचने का समय न मिले।

↓ तुरंत तीसरे व्यक्ति के खाते में पैसे माँगना

3

वकील या Doctor के नाम पर UPI

कहा जाता है: "मेरा खाता काम नहीं कर रहा, तुरंत इस वकील या सिपाही के UPI पर पैसे भेजो।"

↓ पैसे जाते ही Number बंद

4

पैसे चोरी और भयानक सदमा

पैसे Transfer होते ही Call कट जाती है और जब बाद में बेटे से बात होती है, तब धोखे का पता चलता है।

AI Voice पहचानने के 3 अचूक सुरक्षा उपाय



1. पारिवारिक Secret Code (गुप्त सवाल)

घर में एक ऐसा सवाल तय करके रखें जिसका जवाब सिर्फ परिवार वालों को पता हो (जैसे बचपन का उपनाम या पालतू जानवर का नाम)।



2. असली Number पर तुरंत Callback

सामने वाले की Call काटें और अपने Phone की Contact List से अपने बच्चे के असली Mobile Number पर खुद Call मिलाएँ।

3. किसी तीसरे व्यक्ति को पैसे कभी न भेजें

जब भी कोई अनजान वकील, Doctor या सिपाही बनकर पैसे माँगे, तो बिना आमने-सामने मिले कभी पैसे न भेजें।

Official Portal: AI Fraud और Emergency ठगी की शिकायत

भारत सरकार के Cyber Crime Portal पर AI Voice और मुसीबत के नाम पर की जाने वाली ठगी की सीधे शिकायत की जा सकती है:

cybercrime.gov.in

Official सरकारी Portal



Cyber Crime Related Complaint / Women & Children Related Cybercrime

Cybercrime refers to any unlawful activity carried out using computers, digital devices, or the internet. It includes offenses such as data theft, hacking, online harassment, identity misuse, financial scams, spreading malware, and other acts intended to harm individuals, organizations, or digital infrastructure.

Any victim of financial cyber fraud can dial

📌 **सरकारी Portal से 2 ज़रूरी बातें:**

1. **Golden 2 घंटे (Golden Hours):** अगर गलती से पैसे Transfer हो जाएँ, तो तुरंत `cybercrime.gov.in` पर Report करें ताकि Scammer का खाता Freeze कराया जा सके।
2. **Voice Recording और Number सुरक्षित रखें:** जिस Number से ऐसी Call आई हो, उसकी तारीख और समय नोट करके रखें।

Emergency Call की जाँच: 3-Step नियम

जब भी कोई रिश्तेदार या बच्चा बनकर मुसीबत का बहाना बनाए, तो हमेशा यह 3-Step रास्ता अपनाएँ:

1. **तुरंत Call काटें (Panic न हों)**
   सामने वाले की डराने वाली बात सुनते ही तुरंत Red Button दबाकर Call काट दें।
2. **बच्चे या उसके दोस्त को Call मिलाएँ**
   अपने Phone की Contact Diary से अपने बेटे, बहू या उसके Office के साथी को सीधे Phone करें।
3. **सरकारी Portal पर Number Report करें**
   Browser खोलकर `sancharsaathi.gov.in` पर जाएँ और उस Fake Number की Chakshu में शिकायत करें।

अध्याय 7: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• बच्चे की रोती आवाज़ सुनकर भी 10 Second शांत रहें और गहरी साँस लें।

• परिवार में एक Secret Code या सवाल हमेशा तय करके रखें।

• हमेशा अपने बच्चे के पुराने असली Mobile Number पर खुद Call करके जाँचें।

❌ यह कभी न करें (DONTs)

• हड़बड़ी या डर में आकर किसी अनजान UPI ID पर कभी पैसे न भेजें।

• अनजान व्यक्ति द्वारा बताए गए वकील या Doctor की बातों में न आएँ।

• जब तक बच्चे से खुद बात न हो जाए, तब तक किसी भी तीसरे व्यक्ति पर भरोसा न करें।

OFFICIAL स्रोत व नियम

• Ministry of Home Affairs (I4C Advisory on AI Voice Cloning Scams): `cybercrime.gov.in`

• Telecom Department (Sanchar Saathi Portal): `sancharsaathi.gov.in`

• Reserve Bank of India (Public Caution on Imposter Scams): `rbi.org.in`

अध्याय 8 • PENSION और सरकारी योजनाओं की सुरक्षा

Pension और सरकारी Scheme के नाम पर Fraud

जीवन प्रमाण पत्र का बहाना, रुके हुए Arrear का लालच और Phone पर Pension बंद करने की धमकी का सच।

नवंबर का महीना और Pension रुकने की धमकी

हर साल नवंबर में हमारे सेवानिवृत्त माता-पिता को अपना जीवन प्रमाण पत्र (Life Certificate) जमा करना होता है ताकि उनकी Pension बिना रुके आती रहे।

Scammers इसी समय का फायदा उठाते हैं। Phone पर कोई बहुत ही गंभीर आवाज़ में कहता है: *"बाबूजी, मैं मुख्य Pension Office से बोल रहा हूँ। आपका Life Certificate Re-Verify नहीं हुआ है। अगर आज रात तक आधार OTP नहीं बताया, तो अगले महीने से आपकी Pension हमेशा के लिए बंद कर दी जाएगी!"*

सरकारी सच

जीवन प्रमाण पत्र जमा करने का असली नियम

भारत सरकार का स्पष्ट नियम है कि जीवन प्रमाण पत्र कभी भी किसी अनजान Phone Call पर OTP बताकर जमा नहीं होता।

इसे जमा करने के 3 ही कानूनी रास्ते हैं: 1. अपनी Bank Branch में जाकर अंगूठा लगाना। 2. Post Office के डाकिया (Postman) को घर बुलाकर बायोमेट्रिक मशीन पर अंगूठा लगाना। 3. सरकार के Official **Jeevan Pramaan App** से चेहरे का Photo (Face Authentication) खींचना।

> **सीधी बात:** जो भी Phone पर Call करके आपसे Pension चालू रखने के लिए Code या OTP माँगे, वह 100% Scammer है।

Case Study: "आपके ₹85,000 का Arrear पास हो गया है"

देखें कैसे Scammer पुराने Arrear का लालच देकर पैसे ठगने की कोशिश करता है:

📞 PHONE CALL SIMULATION (FAKE TREASURY OFFICER)

> **Scammer (सूट-बूट वाले बाबू की भाषा में):** "प्रणाम Teacher जी, मैं वित्त विभाग की Treasury से बोल रहा हूँ। आपके 7वें वेतन आयोग का ₹85,000 का पुराना Arrear पास हो गया है। सरकार इसे कल आपके खाते में भेज देगी, बस File Charge का ₹1,500 तुरंत इस सरकारी UPI पर जमा कीजिए!"

> **जागरूक शिक्षक:** "बाबूजी, सरकार जब भी कोई Arrear देती है तो वह सीधे Bank खाते में जमा होता है। सरकार कभी Phone पर File Charge नहीं माँगती। मैं कल खुद Treasury Office जाकर पता करूँगा।"

> **सच्चाई:** *(जैसे ही शिक्षक ने खुद Treasury Office जाने की बात कही, Scammer ने तुरंत Call काट दी। सरकार*

कभी भी Pension या Arrear जारी करने के लिए किसी भी नागरिक से अग्रिम पैसे नहीं माँगती।)

Pension Scam का 4-Step Trap

1 **अचानक डराने वाली Call**

Scammer कहता है: "आपका PPO Number और आधार मिसमैच हो गया है, Pension रुक जाएगी।"

↓ घर बैठे ठीक करने का लालच

2 **Phone पर SMS आने की बात कहना**

Scammer अपने Computer पर आधार या Bank का Portal खोलकर Login का OTP जनरेट करता है।

↓ आधार या Bank OTP माँगना

3 **Code बताने का भारी दबाव**

Scammer कहता है: "जल्दी बताइए, Server सिर्फ 2 मिनट के लिए खुला है, वरना फिर कभी Pension नहीं मिलेगी।"

↓ खाता खाली और Number Block

4 **Pension खाते की सारी बचत चोरी**

जैसे ही OTP बताया गया, खाते से जीवन भर की जमा पूँजी साफ़ हो जाती है और Scammer गायब हो जाता है।

असली सरकारी नियम vs Fake Pension Calls



1. कोई भी सरकार Phone पर OTP नहीं माँगती

भारत सरकार के Pension विभाग का स्पष्ट आदेश है कि किसी भी Pensionधारक से Phone पर आधार या Bank OTP नहीं माँगा जाएगा।



2. Arrear के लिए कोई Advance Fees नहीं

Pension या महँगाई भत्ते का सारा पैसा सीधे खाते में जमा होता है। किसी भी File Charge या Processing Fees की कोई कानूनी व्यवस्था नहीं है।



3. डाकिया घर आकर मदद करता है

India Post Payments Bank (IPPB) की सरकारी सेवा के तहत डाकिया मात्र नाममात्र के सरकारी शुल्क में घर आकर Biometric मशीन से Digital Life Certificate जमा करता है।

Official Portal: जीवन प्रमाण पत्र की असली सरकारी Website

भारत सरकार के इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय द्वारा संचालित **Jeevan Pramaan** Portal:

jeevanpramaan.gov.in

Official सरकारी Portal



📌 **Jeevan Pramaan Portal के मुख्य नियम:**

1. **Official App का उपयोग:** जीवन प्रमाण पत्र जमा करने के लिए केवल `jeevanpramaan.gov.in` से ही Official App या Face App Download करें।
2. **Government Domain पहचान:** हमेशा Browser में देखें कि पता `jeevanpramaan.gov.in` हो। किसी Private Link पर कभी भरोसा न करें।

Pension समस्या के समाधान का 3-Step नियम

अगर Phone पर कोई Pension रुकने की धमकी दे, तो कभी भी डर में न आएँ। यह 3-Step सुरक्षित रास्ता अपनाएँ:

1. **सीधे अपनी Bank Branch जाएँ**
   जिस Bank खाते में आपकी हर महीने Pension आती है, वहाँ जाकर Pension डेस्क के अधिकारी से सीधे बात करें।

2. **Google पर Jeevan Pramaan Website खोलें**
   Browser के Address Bar में सीधे `jeevanpramaan.gov.in` Type करें और अपने नजदीकी Center की सूची देखें।

3. **डाकिए की सेवा लें**
   अपने नजदीकी डाकघर (Post Office) में संपर्क करके डाकिया को घर पर Biometric प्रमाण पत्र के लिए बुलाएँ।

अध्याय 8: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• हर साल नवंबर में अपनी Bank Branch या डाकघर जाकर खुद जीवन प्रमाण पत्र दें।

• Pension या Arrear से जुड़ा कोई भी सवाल हो तो अपनी Treasury या Bank में जाकर पूछें।

• घर के बच्चों को अपने PPO Number और Bank Passbook की जानकारी सुरक्षित रखने दें।

❌ यह कभी न करें (DONTs)

• Phone Call पर किसी को भी आधार OTP या Bank Code कभी न बताएँ।

• रुके हुए Arrear को मँगाने के लिए किसी अनजान खाते में Fees कभी न भेजें।

• WhatsApp पर आई किसी अनजान Pension सहायता योजना के Link को न दबाएँ।

OFFICIAL स्रोत व नियम

• Department of Pension & Pensioners' Welfare: `pensionersportal.gov.in`

• Jeevan Pramaan Official Portal: `jeevanpramaan.gov.in`

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

अध्याय 9 • रिश्तों की आड़ में ठगी

रिश्तेदार या बच्चे बनकर पैसे माँगना

"पहचान लिया ना बाबूजी" वाली मीठी बातों का जाल और शर्म-संकोच से परे सुरक्षा के नियम।

"पहचानिए मैं कौन बोल रहा हूँ?" — सबसे पहली चाल

सोचिए, आपके Phone पर एक अनजान Number से Call आती है। सामने वाला बहुत ही बहुत प्यार से बोलता है: *"नमस्ते मामाजी, चरण स्पर्श! पहचान लिया ना? बताइए मैं कौन बोल रहा हूँ?"*

बुज़ुर्ग व्यक्ति शर्म के मारे यह नहीं कह पाता कि उसे आवाज़ समझ नहीं आ रही। वह अपने दिमाग में रिश्तेदारों के नाम सोचता है और कह बैठता है: *"अरे अमित बेटा, तुम?"*

Scammer को बस इसी एक नाम का इंतज़ार होता है। वह तुरंत कहता है: *"हाँ मामाजी, बिल्कुल सही पहचाना! मेरा Phone चोरी हो गया था, इसलिए नए Number से बात कर रहा हूँ।"*

चाल समझें

Scammer रिश्तेदार क्यों बनता है?

Scammer जानता है कि हमारे देश में बुज़ुर्ग अपने दामाद, भांजे या भतीजे से पैसे के मामले में कड़े सवाल पूछने में संकोच करते हैं।

वह इसका फायदा उठाकर कहता है कि वह रास्ते में अस्पताल या Police चालान में फँस गया है और तुरंत ₹25,000 किसी तीसरे व्यक्ति के UPI पर मँगवा लेता है।

> **सीधी बात:** जब कोई अनजान Number से Phone करके खुद अपना नाम न बताए और आपसे अंदाज़ा लगवाए, तो समझ जाइए कि वह धोखेबाज़ हो सकता है।

Case Study: "दामाद जी अस्पताल में हैं"

देखें कैसे सतर्क ससुर जी ने एक सवाल से ठग का भेद खोल दिया:

📞 PHONE CALL SIMULATION (FAKE SON-IN-LAW)

> **Scammer (घबराई हुई आवाज़):** "पापाजी, मैं आपका दामाद बात कर रहा हूँ। मेरी कार का चालान कट गया है और Police गाड़ी ज़ब्त कर रही है। अभी इस सिपाही के UPI पर ₹15,000 भेज दीजिए, घर पहुँचकर आपको वापस कर दूँगा!"

> **होशियार ससुर जी:** "अच्छा बेटा, पहले यह बताओ कि तुम्हारी सासू माँ का मायका किस शहर में है?"

> **Scammer (झल्लाते हुए):** "पापाजी, यहाँ Police मुझे पकड़ रही है और आप मायका पूछ रहे हैं! जल्दी पैसे भेजिए!"

> **सच्चाई:** *(ससुर जी ने तुरंत Call काटी और अपनी बेटी के Phone पर मिलाया। बेटी ने बताया कि दामाद जी तो आराम से कमरे में चाय पी रहे हैं! सतर्कता से ₹15,000 बच गए।)*

रिश्तेदार बनने का 4-Step जाल

1

अंदाज़ा लगवाना

Scammer कहता है: "पहचानिए मैं कौन?" ताकि आप खुद अपने किसी रिश्तेदार का नाम बोल दें।

↓ नया Number होने का बहाना

2

Phone चोरी या SIM खोने का दावा

कहा जाता है: "मेरा पुराना Phone गिर गया था, यह मेरा नया Personal Number है, इसे सेव कर लीजिए।"

↓ अचानक पैसे की माँग

3

अस्पताल या Police का झूठा डर

कहा जाता है: "मैं रास्ते में फँसा हूँ, किसी को मत बताइएगा, तुरंत ₹20,000 इस UPI पर भेज दीजिए।"

↓ पैसे मिलते ही Number Switch Off

4

पैसे गायब और पछतावा

जैसे ही आपने पैसे भेजे, वह Number हमेशा के लिए बंद हो जाता है और असल रिश्तेदार को कुछ पता नहीं होता।

पहचानने के 3 सबसे बड़े नियम

❓

1. कभी खुद नाम का अंदाज़ा न लगाएँ

जब कोई कहे "पहचानिए", तो सीधे कहें: *"मुझे आवाज़ समझ नहीं आई, आप अपना पूरा नाम और पिता का नाम बताइए।"*

📖

2. पुराने सेव किए Number पर खुद Call करें

नए Number की बात पर भरोसा न करें। Call काटकर अपनी Phone Book से उस रिश्तेदार के असली Number पर Phone मिलाएँ।

👨‍👩

3. घर के दूसरे सदस्य से बात करवाएँ

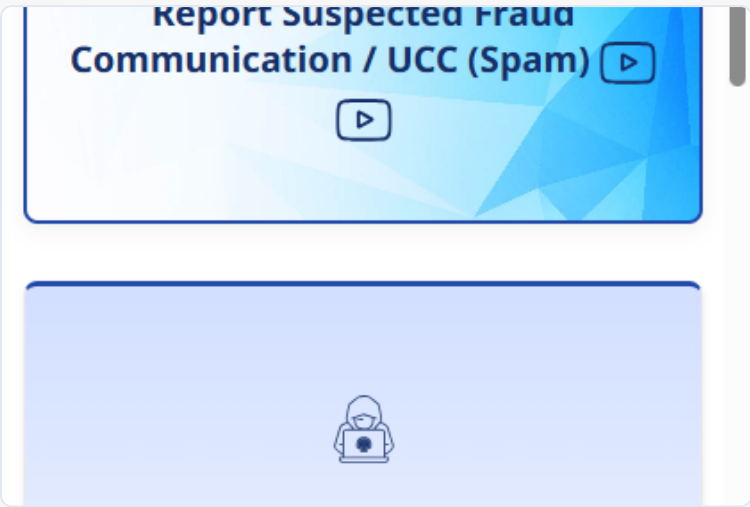
पैसे की बात आते ही कहें: *"रुकिए, मैं घर में बेटे या बहू को Phone देता हूँ, आप उनसे बात कर लीजिए।"* Scammer तुरंत Call काट देगा।

Official Portal: अनजान और Fake Numbers की Report

अगर कोई अनजान व्यक्ति रिश्तेदार बनकर पैसे ऐंठने की कोशिश करे, तो Telecom Department के **Chakshu Portal** पर Report करें:

sancharsaathi.gov.in/sfc (Chakshu)

Official सरकारी Portal



📌 **Chakshu Portal पर Report करने के फ़ायदे:**

1. **देश भर में Number Block:** आपके एक Report से Telecom Department उस Fake Number को हमेशा के लिए बंद कर देता है।
2. **अन्य वरिष्ठ नागरिकों की सुरक्षा:** वह ठग किसी दूसरे परिवार के बुज़ुर्ग को निशाना नहीं बना पाता।

रिश्तेदार की पहचान का 3-Step नियम

जब भी कोई अनजान Number से रिश्तेदार बनकर पैसे माँगे, तो यह 3-Step सुरक्षा नियम अपनाएँ:

1. **सीधे Call काटें**
   सामने वाले की हड़बड़ी वाली बातों में न आएँ और सीधे Red Button दबाकर Call काटें।
2. **परिवार के पुराने Number पर Call मिलाएँ**
   अपनी Phone Diary से उस रिश्तेदार या उसके माता-पिता के असली Mobile Number पर खुद Phone लगाएँ।
3. **घर के बच्चों को पूरी बात बताएँ**
   पैसे भेजने से पहले हमेशा अपने बेटे या बेटी को पूरी बात बताकर Confirm करें।

अध्याय 9: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• अनजान Call पर कभी खुद किसी रिश्तेदार का नाम लेकर अंदाज़ा न लगाएँ।

• रिश्तेदार बनकर आए व्यक्ति से परिवार की कोई पुरानी अंदर की बात पूछें।

• हमेशा उस रिश्तेदार के पुराने असली Mobile Number पर दोबारा Phone करें।

❌ यह कभी न करें (DONTs)

• संकोच या शर्म में आकर कभी किसी अनजान Number पर पैसे न भेजें।

• सामने वाले के कहने पर किसी अनजान दुकानदार या सिपाही के UPI पर पैसे न डालें।

• बिना परिवार से बात किए किसी भी गुप्त मदद का वादा न करें।

OFFICIAL स्रोत व नियम

• Telecom Department (Chakshu Suspected Fraud Reporting): `sancharsaathi.gov.in`

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

• Reserve Bank of India (Advisory on Impersonation Scams): `rbi.org.in`

अध्याय 10 • ATM और BANK में सुरक्षा

"मैं मदद कर दूँ" कहने वाले अनजान लोग

ATM के बाहर खड़े मददगारों का सच, हाथ की सफाई से Card बदलना और PIN चुराने का खेल।

ATM के अंदर बहुत भला दिखने वाला नौजवान

सोचिए, आपके पिताजी ATM से पैसे निकालने गए हैं। उनकी आँखों से थोड़ा कम दिखता है और मशीन का Button समझ नहीं आ रहा। तभी पीछे खड़ा एक बहुत ही सुसज्जित और मीठा बोलने वाला नौजवान आगे आता है:

"लाइए Uncle जी, आप क्यों परेशान हो रहे हैं? मैं आपका Card लगा देता हूँ, आप बस अपना PIN डाल दीजिए, पैसे तुरंत निकल जाएँगे।"

बुज़ुर्ग सोचते हैं कि आजकल के बच्चे कितने संस्कारी हैं, बिना माँगे मदद कर रहे हैं। वे अपना Card उस लड़के के हाथ में दे देते हैं। यहीं से सारा खेल पलट जाता है।

हाथ की सफाई

Card Swapping क्या है?

वह नौजवान Card मशीन में लगाने का नाटक करता है। लेकिन हाथ की सफाई से वह आपके असली Card को अपनी जेब में छुपा लेता है और उसी Bank का एक बंद पड़ा पुराना Card आपके हाथ में थमा देता है।

जब आप Screen पर PIN डालते हैं, तो वह पीछे से आपकी उँगलियाँ देखकर PIN याद कर लेता है। फिर कहता है: *"Uncle जी मशीन में Cash खत्म हो गया है, आप दूसरी मशीन पर चलिए।"*

> **सीधी बात:** आपके बाहर निकलते ही वह आपके असली Card और याद किए गए PIN से खाते के सारे पैसे निकाल लेता है।

Case Study: Passbook मशीन पर मदद का नाटक

देखें कैसे अनजान व्यक्ति की मदद स्वीकार करने पर पूरा खाता साफ़ हो गया:

🏦 BANK BRANCH SIMULATION (FAKE HELPER)

> **अनजान व्यक्ति (आदर से):** "बाबूजी, यह मशीन बार-बार Card रिजेक्ट कर रही है। मैं इसे कपड़े से साफ़ करके ठीक से लगा देता हूँ। आप अपना 4 अंकों का गुप्त Code बोलिए, मैं Feed कर देता हूँ।"

> **साधारण बुज़ुर्ग:** "हाँ बेटा, मुझे थोड़ा कम दिखता है, Code है 4-2-8-0."

> **सच्चाई:** *(लड़के ने Card जेब में डालकर नकली Card वापस कर दिया और 10 मिनट के अंदर पास के दूसरे ATM से बुज़ुर्ग की Pension के पूरे ₹40,000 निकाल लिए।)*

Card बदलने का 4-Step Trap

1. **मदद की मीठी पेशकश**

   नौजवान आदर से आगे आता है और बुजुर्ग की उलझन देखकर खुद मदद करने का नाटक करता है।

↓ Card हाथ में लेना

2 **हाथ की सफाई से Card बदलना**

नौजवान असली Debit Card को अपनी हथेली में छुपाकर उसी रंग का दूसरा बेकार Card थमा देता है।

↓ कंधे के पीछे से PIN देखना

3 **Shoulder Surfing (PIN याद करना)**

जब बुजुर्ग कीपैड पर PIN डालते हैं, तो वह पीछे से उँगलियों की हरकत देखकर 4 अंकों का PIN याद कर लेता है।

↓ मशीन खराब बताकर चलता बनना

4 **असली Card से Cash साफ**

जैसे ही बुजुर्ग ATM से बाहर निकलते हैं, वह असली Card और PIN से तुरंत पैसे निकाल लेता है।

सुरक्षित ATM इस्तेमाल का 3-Point Shield

1. हाथ की ओट बनाकर PIN डालें

जब भी कीपैड पर Number दबाएँ, अपने दूसरे हाथ को ऊपर से छतरी की तरह ढक लें ताकि न तो कोई इंसान और न ही कोई छिपा हुआ Camera आपका PIN देख सके।

2. Card किसी को हाथ न लगाने दें

अपना Debit Card केवल अपने हाथ से मशीन में डालें और तुरंत वापस अपनी जेब में रखें। किसी अजनबी को Card छूने भी न दें।

3. हमेशा अपना नाम जाँचें

ATM से बाहर निकलने से पहले Card पर अपना नाम पढ़कर Confirm करें कि यह आपका ही असली Card है।

मदद चाहिए तो क्या करें: 3 सुरक्षित नियम



1. केवल वर्दीधारी Guard से मदद लें

ATM केबिन में खड़े किसी अनजान ग्राहक से नहीं, बल्कि बाहर खड़े वर्दीधारी Bank सुरक्षा Guard से ही मदद माँगें।



2. Bank Counter पर जाकर पैसे निकालें

अगर ATM में परेशानी होती है, तो Bank Branch के अंदर जाकर विDrawल Form भरकर सीधे Cashier से पैसे लें।



3. हमेशा घर के बच्चों को साथ ले जाएँ

बुज़ुर्ग जब भी बड़ी रकम निकालने जाएँ, तो अपने बेटे, बेटी या परिवार के किसी भरोसेमंद सदस्य को साथ रखें।

Card चोरी या बदल जाने पर 3-Step नियम

अगर कभी लगे कि आपका Card बदल गया है या मशीन में फँस गया है, तो तुरंत यह 3-Step कदम उठाएँ:

1. **तुरंत अपना Card Block करवाएँ**
   Bank App में जाकर 'Block Debit Card' का Button दबाएँ ताकि कोई भी पैसा न निकाल सके।
2. **Passbook पर लिखा Toll-Free Number मिलाएँ**
   अपनी Bank Passbook के पहले पन्ने पर लिखे Official Toll-Free Helpline Number पर तुरंत Phone करें।
3. **नज़दीकी Bank Branch में लिखित शिकायत दें**
   तुरंत अपनी Bank Branch जाकर शाखा प्रबंधक को घटना की जानकारी दें ताकि CCTV फुटेज जाँची जा सके।

अध्याय 10: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• PIN डालते समय हमेशा दूसरे हाथ से कीपैड को ऊपर से ढकें।

• ATM से निकलते समय Card पर अपना नाम ज़रूर पढ़ें।

• लेन-देन पूरा होने के बाद हमेशा लाल रंग का 'Cancel' Button दबाएँ।

❌ यह कभी न करें (DONTs)

• अपना ATM Card कभी किसी अनजान व्यक्ति के हाथ में न थमाएँ।

• किसी के भी पूछने पर अपना 4 अंकों का Secret PIN मुँह से न बोलें।

• जब कोई दूसरा व्यक्ति केबिन के अंदर खड़ा हो, तब पैसे निकालने की कोशिश न करें।

OFFICIAL स्रोत व नियम

• Reserve Bank of India (Safe ATM Usage Guidelines): `rbi.org.in`

• Indian Banks' Association (ATM Safety Best Practices): `iba.org.in`

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

अध्याय 11 • 10 सेकंड का सुरक्षा विराम

पैसे भेजने से पहले ये ज़रूर पूछें

हड़बड़ी में कोई फैसला न लें: समझें 10 सेकंड का विराम और वो 3 सवाल जो हर ठगी को रोक देते हैं।

Scammer का सबसे बड़ा हथियार: हड़बड़ी और डर

सोचिए, जब भी कोई अनजान व्यक्ति Call करता है, तो वह कभी यह नहीं कहता कि *"आराम से कल सोचकर बताइएगा"*. वह हमेशा कहता है: *"सिर्फ 5 मिनट का समय है, तुरंत Button दबाइए वरना भारी जुर्माना लगेगा!"*

Scammer ऐसा इसलिए करता है क्योंकि वह जानता है कि अगर आपने 1 मिनट भी शांति से सोच लिया या अपने बेटे-बेटी से पूछ लिया, तो उसका झूठ तुरंत पकड़ा जाएगा।

सुनहरा नियम

10 Second का विराम नियम (10-Second Pause)

जब भी Phone पर कोई डराए, लालच दे या तुरंत पैसे माँगने लगे, तो अपनी उँगली को Phone की Screen से तुरंत हटा लीजिए।

एक गहरी साँस लें और 10 Second तक रुकें। सामने वाले से साफ़ कहें: **"मैं अभी व्यस्त हूँ, 10 मिनट बाद बात करूँगा।"** और Call काट दें।

> **सीधी बात:** दुनिया का कोई भी असली काम 10 सेकंड रुकने से कभी खराब नहीं होता, लेकिन 10 सेकंड की जल्दबाज़ी में जीवन भर की जमा पूँजी ज़रूर जा सकती है।

Case Study: 10 सेकंड रुकने से बची जीवन भर की कमाई

देखें कैसे एक छोटे से विराम ने ₹2 लाख की ठगी रोक दी:

📞 PHONE CALL SIMULATION (HIGH PRESSURE TRAP)

> **Scammer (चिल्लाते हुए):** "बाबूजी, आपकी Pension रुकने में सिर्फ 2 मिनट बचे हैं! Screen पर आया हुआ 6 अंकों का Code तुरंत बताइए वरना File बंद हो जाएगी!"

> **सतर्क बुज़ुर्ग (उँगली रोककर, शांत स्वर में):** "बेटा, मुझे कोई जल्दी नहीं है। अगर Pension रुकेगी तो मैं कल खुद Bank Branch जाकर बाबूजी से मिल लूँगा। मैं Phone पर कोई Code नहीं बताऊँगा।"

> **सच्चाई:** *(Scammer ने झल्लाकर Phone काट दिया। जब बुज़ुर्ग ने अपने बेटे को बताया, तो पता चला कि Pension का कोई काम रुका ही नहीं था। 10 Second के धैर्य से बुज़ुर्ग के ₹2 लाख बच गए!)*

10-Second Family Shield का 4-Step चक्र

1

Screen से उँगली हटाएँ

हड़बड़ी वाली बात सुनते ही तुरंत Screen पर कोई भी Button या Code दबाने से रुक जाएँ।

↓ गहरी साँस लेना

2

सीधे Red Button दबाकर Call काटें

सामने वाले की धमकी या रोने-धोने की आवाज़ पूरी न सुनें, सीधे Call काटें।

↓ कमरे से बाहर निकलना

3

घर के बच्चों को पूरी बात बताएँ

अपने बेटे, बेटी या परिवार के सदस्यों को दिखाएँ कि Phone पर क्या Message या Call आई है।

↓ सुरक्षित फैसला

4

पैसे और मन की शांति सुरक्षित

परिवार की मदद से सच्चाई सामने आ जाती है और ठग का Number तुरंत Block कर दिया जाता है।

पैसे भेजने से पहले 3 सवाल जो खुद से पूछें

सवाल 1: क्या मैं सामने वाले से आमने-सामने मिला हूँ?

अगर सामने वाला केवल Phone, WhatsApp या Internet पर बात कर रहा है—तो उसे ₹1 भी न भेजें।

सवाल 2: क्या पैसे लेने के लिए PIN डालना पड़ता है?

जवाब: कभी नहीं! अगर कोई कहे कि पैसे पाने के लिए अपना UPI PIN डालें, तो वह 100% झूठ बोल रहा है।

सवाल 3: क्या मैंने यह बात अपने परिवार को बताई?

जब तक घर के बच्चों को बात न बता दें, तब तक किसी भी अनजान व्यक्ति के खाते में कोई Payment न करें।

जल्दबाज़ी vs समझदारी



Scammer हमेशा समय सीमा तय करता है

वह कहेगा: "10 मिनट में बिजली कटेगी", "अभी OTP बताइए", "2 मिनट में ऑफर खत्म". यह केवल दिमाग को सुन्न करने का तरीका है।



असली Bank व सरकारी विभाग हमेशा समय देते हैं

कोई भी असली Bank, बिजली विभाग या सरकार हर काम के लिए हफ्तों का समय और लिखित सूचना देती है। Phone पर हड़बड़ी नहीं मचाती।

सुरक्षित संपर्क का 3-Step नियम

जब भी कोई Phone पर जल्दी करने का दबाव बनाए, तो यह 3-Step सुरक्षा नियम अपनाएँ:

1. **Phone का Red Button दबाएँ**
   सामने वाले की बात सुने बिना सीधे Call काट दें और Phone को दूर रख दें।

2. **घर के किसी सदस्य को आवाज़ दें**
   अपने बेटे, बहू या बेटी को बुलाकर बताएँ कि क्या Call आई थी।

3. **Bank की Official Website से Number लें**
   यदि Bank से जुड़ी कोई बात हो, तो केवल Passbook पर लिखे या Bank की Official Website से जाँचे हुए Number पर ही बात करें।

अध्याय 11: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• हर अनजान Call पर 10 Second रुकने की आदत बनाएँ।

• कोई भी फैसला लेने से पहले अपने घर के बच्चों से ज़रूर पूछें।

• शक होने पर सीधे अपने नज़दीकी Bank Branch में जाकर बात करें।

❌ यह कभी न करें (DONTs)

• हड़बड़ी या डर में आकर कभी भी Phone पर कोई Code न बताएँ।

• किसी अनजान व्यक्ति के कहने पर जल्दबाज़ी में पैसे न भेजें।

• "किसी को मत बताइएगा" जैसी बातों पर कभी अकेले फैसला न लें।

OFFICIAL स्रोत व नियम

• Reserve Bank of India (Public Awareness on Financial Frauds): `rbi.org.in`

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

• Telecom Department (Sanchar Saathi Portal): `sancharsaathi.gov.in`

अध्याय 12 • संकट के समय सही कदम

Fraud हो जाए तो क्या करें

पैसे कट जाएँ तो घबराएँ नहीं: समझें शुरुआती 2 घंटे (Golden Hours) की ज़रूरत और पैसे बचाने का पूरा तरीका।

धोखा होने पर खुद को या माता-पिता को दोष न दें

अगर अनजाने में या किसी डरावनी Call के डर में आकर खाते से पैसे कट भी जाएँ, तो सबसे पहली बात याद रखें—**बिल्कुल घबराइए मत और न ही अपनी सेहत खराब कीजिए**।

Scammers बहुत ही बहुत चालाक और शातिर ठग होते हैं। वे बड़े-बड़े अफसरों और युवा इंजीनियरों को भी चकमा दे देते हैं। ऐसी स्थिति में डरने या बात छुपाने के बजाय जितनी जल्दी आप सही कदम उठाएँगे, पैसा वापस लौटने की उम्मीद उतनी ही ज़्यादा होगी।

बहुत ज़रूरी नियम

शुरुआती 2 घंटे (Golden Hours) की ताकत

जब आपके खाते से पैसा कटता है, तो Scammer तुरंत उसे जेब में नहीं डाल लेता। वह उस पैसे को 3-4 अलग-अलग Bank खातों में घुमाता है ताकि कोई पकड़ न सके।

अगर आप घटना के पहले 2 घंटे के भीतर अपने Bank और सरकारी Cyber Crime Portal पर शिकायत दर्ज करा देते हैं, तो कानूनन उस पैसे को रास्ते में ही **Freeze (जकड़)** दिया जाता है।

> **सीधी बात:** बात छुपाने से पैसा कभी वापस नहीं आता। तुरंत अपने बच्चों को बताएँ और शिकायत दर्ज करवाएँ।

Case Study: 30 मिनट में कार्रवाई से वापस मिले ₹60,000

देखें कैसे तुरंत कदम उठाने से फँसा हुआ पैसा सुरक्षित बच गया:

RECOVERY SIMULATION (QUICK ACTION)

घटना: बुज़ुर्ग ने बिजली बिल के झाँसे में आकर ₹60,000 गँवा दिए। खाते से पैसे कटने का SMS देखते ही वे काँपने लगे।

बुज़ुर्ग का सही फैसला: उन्होंने बात छुपाने के बजाय तुरंत अपने बेटे को आवाज़ दी। बेटे ने बिना डाँटे तुरंत Bank App खोलकर Debit Card और Net Banking Block कर दी।

सच्चाई: *(बेटे ने घटना के 25 मिनट के अंदर Official Portal `cybercrime.gov.in` पर Online शिकायत दर्ज की। Cyber Cell ने तुरंत उस खाते को Freeze कर दिया जहाँ पैसा गया था, और 5 दिन बाद पूरे ₹60,000 पिता के खाते में वापस आ गए!)*

Fraud होने पर तुरंत 4-Step एक्शन प्लान

1 **Bank खाता और Card तुरंत Block करें**

Bank App में जाकर या Bank के Official Helpline पर Phone करके Debit Card, UPI और Net Banking बंद करवाएँ।

↓ लेन-देन के सबूत सुरक्षित करना

2 **SMS और UTR Number का Screenshot लें**

पैसे कटने का Message, 12 अंकों का UTR Number, ठग का Phone Number और समय का Screenshot ले लें।

↓ सरकारी Portal पर Report

3 **Cyber Crime Portal पर Report करें**

सीधे सरकारी Website `cybercrime.gov.in` पर जाकर 'Report Financial Fraud' में पूरी जानकारी भरें।

↓ स्थानीय Bank शाखा में जाना

4 **Bank Branch में पावती जमा करें**

अपनी Bank Branch में जाकर लिखित आवेदन दें और Cyber Portal से मिली शिकायत संख्या (Acknowledgement) दर्ज कराएँ।

RBI का ग्राहक सुरक्षा नियम (Zero Liability Rule)



1. 3 दिन के अंदर सूचना देने पर पूरी सुरक्षा

RBI के नियमों के अनुसार यदि किसी तकनीकी कमी या Online Fraud की सूचना 3 दिन के भीतर Bank को दे दी जाए, तो ग्राहक की कोई व्यक्तिगत देनदारी नहीं होती।



2. जितना जल्दी बताएँगे, उतना सुरक्षित

जितनी जल्दी Bank और Cyber Cell को सूचना दी जाएगी, पैसा Scammer द्वारा ATM से निकाले जाने से पहले ही रोका जा सकेगा।

🤝

3. परिवार का साथ सबसे बड़ी ताकत

पैसे से बढ़कर आपके माता-पिता का स्वास्थ्य और सम्मान है। किसी भी नुकसान पर उन्हें प्यार और हिम्मत दें।

Official Portal: Online Fraud की तुरंत शिकायत

भारत सरकार का **National Cyber Crime Reporting Portal** नागरिकों के पैसे को बचाने के लिए 24 घंटे काम करता है:

cybercrime.gov.in

Official सरकारी Portal



Cyber Crime Related Complaint / Women & Children Related Cybercrime

Cybercrime refers to any unlawful activity carried out using computers, digital devices, or the internet. It includes offenses such as data theft, hacking, online harassment, identity misuse, financial scams, spreading malware, and other acts intended to harm individuals, organizations, or digital infrastructure.

Any victim of financial cyber fraud can dial

📌 **सरकारी Portal पर Report के 2 मुख्य बिंदु:**

1. **Citizen Financial Cyber Fraud Reporting System:** यह System सभी Banks और Payment कंपनियों से सीधे जुड़ी है ताकि पैसा तुरंत रोका जा सके।
2. **लिखित शिकायत की रसीद:** शिकायत दर्ज होते ही आपको एक रसीद Number मिलती है जिसे आप अपने Bank में जमा कर सकते हैं।

Bank और सरकार से संपर्क का 3-Step नियम

धोखा होने पर कभी भी Google Search पर दिखने वाले अनजान Numbers पर Call न करें। यह सुरक्षित रास्ता अपनाएँ:

1. **Passbook या Debit Card के पीछे का Number देखें**
   अपने Bank Card के पीछे लिखे Official Helpline Number पर Call करके तुरंत Card Block करवाएँ।
2. **सीधे सरकारी Website पर जाएँ**
   Browser के Address Bar में सीधे `cybercrime.gov.in` Type करें और Contact Us सेक्शन देखें।
3. **नज़दीकी Police Station के Cyber Cell जाएँ**
   अपने शहर के मुख्य Police Station में जाकर लिखित शिकायत दें और पावती रसीद लें।

अध्याय 12: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• पैसे कटते ही बिना संकोच तुरंत अपने घर के बच्चों को बताएँ।

• पहले 2 घंटे के अंदर Bank और `cybercrime.gov.in` पर Report करें।

• Bank से आए पैसे कटने के Message और UTR Number का Screenshot सुरक्षित रखें।

❌ यह कभी न करें (DONTs)

• डर या शर्म के मारे नुकसान की बात परिवार से कभी न छुपाएँ।

• Scammer के कहने पर "पैसे वापस करने के लिए दूसरा OTP बताइए" वाली बात में न आएँ।

• Google पर अनजान Customer Care Number ढूँढने की गलती न करें।

OFFICIAL स्रोत व नियम

• Ministry of Home Affairs (National Cyber Crime Reporting Portal): `cybercrime.gov.in`

• Reserve Bank of India (Customer Protection - Limiting Liability): `rbi.org.in`

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

अध्याय 13 • परिवार के बच्चों के लिए विशेष GUIDE

घर वालों के लिए: माँ-बाप को ये कैसे सिखाएँ

डाँटने या झल्लाने के बजाय प्यार और समझ से अपने माता-पिता को Digital ढाल पहनाने का तरीका।

हम नया Phone तो दिला देते हैं, पर सुरक्षा नहीं सिखाते

हम में से ज़्यादातर लोग अपने माता-पिता को जन्मदिन या रिटायरमेंट पर नया SmartPhone लाकर दे देते हैं। लेकिन हम यह भूल जाते हैं कि जिस तकनीक को हम बचपन से इस्तेमाल कर रहे हैं, वह उनके लिए बिल्कुल अनजान और पराई दुनिया है।

जब भी वे गलती से किसी अनजान Link पर दबा देते हैं या Phone के किसी फीचर में उलझ जाते हैं, तो कई बच्चे झल्लाकर बोल पड़ते हैं: *"आपको कुछ समझ नहीं आता, क्यों छेड़ा Phone!"*

याद रखिए, हमारे गुस्से से माता-पिता सहम जाते हैं। अगली बार जब कोई Scammer उन्हें डराता है, तो वे बच्चों के डर के मारे बात छुपा लेते हैं और नुकसान उठा बैठते हैं।

सहानुभूति का नियम

प्यार और सम्मान से सिखाने की कला

बचपन में जब हमने पहली बार चम्मच पकड़ना या साइकिल चलाना सीखा था, तो हमारे माता-पिता ने सैकड़ों बार गिरने पर भी हमें प्यार से उठाया था।

आज जब वे तकनीक की नई साइकिल चलाना सीख रहे हैं, तो उन्हें डाँटने के बजाय उसी धैर्य और स्नेह की ज़रूरत है।

> **सीधी बात:** घर में ऐसा सुरक्षित माहौल बनाएँ कि आपके माता-पिता किसी भी अनजान Call के बाद बिना किसी झिझक के सबसे पहले आपको आवाज़ दें।

Case Study: झल्लाने के बजाय 15 मिनट की बातचीत

देखें कैसे एक समझदार बेटी ने अपनी माँ के Phone को पूरी तरह सुरक्षित बनाया:

❤️ FAMILY SIMULATION (SUPPORTIVE CHILD)

> **बेटी (प्यार से माँ का हाथ पकड़कर):** "माँ, कल से आपके Phone में एक नया नियम है। जब भी कोई अनजान Call आए या कोई डर दिखाए, तो आपको सिर्फ एक काम करना है—सीधे Phone काटकर मुझे आवाज़ देनी है। चाहे मैं Office में होऊँ या काम में, मैं कभी आप पर गुस्सा नहीं करूँगी।"

> **माँ (राहत की साँस लेते हुए):** "बेटा, मुझे लगता था कि मैं छोटी-छोटी बातों के लिए पूछूँगी तो तू चिढ़ जाएगी। अब मुझे कोई डर नहीं है।"

> **सच्चाई:** *(बेटी ने माँ के Phone में ₹3,000 की Daily UPI Limit सेट कर दी और Play Store पर Password लगा दिया। 10 दिन बाद जब Fake बिजली बिल का Call आया, तो माँ ने निडर होकर Call काट दी और बेटी को बताया!)*

माता-पिता के Phone में आज ही करें ये 4 Settings

1

Daily UPI Limit कम करें

उनके Bank App या Google Pay में जाकर रोज़ाना लेन-देन की Limit ₹2,000 से ₹5,000 के बीच सेट कर दें।

↓ अनजान Apps से सुरक्षा

2

Play Store पर Password लगाएँ

Google Play Store की Settings में 'Parental Controls' या 'Require Authentication for Purchases' ऑन कर दें।

↓ Spam Call फिल्टर चालू करना

3

Spam Call Blocker ऑन करें

Phone की मुख्य Calling Settings में जाकर 'Caller ID & Spam Protection' ऑन करें ताकि Fake Calls की पहचान हो सके।

↓ आँखों की सहूलियत

4

Font Size बड़ा करें

Phone की Display Settings में जाकर Font Size और Display Size को 'Large' कर दें ताकि हर Message साफ़ दिखे।

घर में लगाने के लिए 3-Point Family Shield

1. "मुझसे कभी भी पूछ सकते हो" का वादा

अपने माता-पिता को रोज़ाना याद दिलाएँ कि तकनीक के मामले में सवाल पूछना कोई शर्म की बात नहीं है।

2. भारी अंग्रेज़ी शब्दों से बचें

Authentication या Phishing जैसे कठिन शब्दों के बजाय "Phone की गुप्त चाबी" या "मछली का काँटा" जैसी सरल भाषा में समझाएँ।

3. TV या Fridge पर Safety Card चिपकाएँ

इस किताब का अगला अध्याय (Safety Checklist) एक कागज़ पर बड़े अक्षरों में लिखकर उनके कमरे में ऐसी जगह लगा दें जहाँ नज़र पड़ती रहे।

डाँटने के नुकसान vs प्यार से समझाने के फ़ायदे



डाँटने पर क्या होता है?

बुज़ुर्ग खुद को लाचार और अकेला महसूस करते हैं। वे डर के मारे अगली बार कोई समस्या होने पर बच्चों से छुपाने लगते हैं, जिससे बड़ा नुकसान हो जाता है।



प्यार से समझाने पर क्या होता है?

माता-पिता का आत्मविश्वास बढ़ता है। किसी भी अनजान Call या Message के आते ही वे सीधे अपने बच्चों को दिखा देते हैं और ठग नाकाम हो जाता है।

बच्चों के लिए 3-Step सुरक्षा नियम

हर हफ्ते शनिवार या रविवार को 10 मिनट निकालकर यह 3-Step आदत अपनाएँ:

1. **माता-पिता के Phone के Apps Check करें**
   देखें कि कोई अनजान Screen Sharing App (जैसे AnyDesk या QuickSupport) गलती से Install तो नहीं हो गया।

2. **Bank Statement और Balance देखें**
   Bank App में जाकर पिछले 1 महीने का Mini Statement देख लें कि कोई अनजान छोटा-बड़ा लेन-देन तो नहीं हुआ।

3. **प्यार से पूछें कि कोई परेशान तो नहीं कर रहा**
   उनसे पूछें: "पापा, किसी अनजान Number से कोई डराने वाली Call या Pension का Message तो नहीं आया?"

अध्याय 13: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• माता-पिता के Phone में कम Daily Limit और Spam Protection ऑन रखें।

• उनके किसी भी तकनीकी सवाल का जवाब हमेशा शांति और मुस्कान के साथ दें।

• उनके साथ बैठकर हफ्ते में एक बार उनके Phone की सुरक्षा जाँचें।

❌ यह कभी न करें (DONTs)

• गलती होने पर कभी अपने माता-पिता पर चिल्लाएँ या ताना न मारें।

• उन्हें कभी यह महसूस न होने दें कि वे उम्र के कारण तकनीक नहीं सीख सकते।

• उन्हें बिना सुरक्षा Settings सिखाए अकेले पैसे से जुड़ा बड़ा फैसला न लेने दें।

OFFICIAL स्रोत व नियम

• Ministry of Home Affairs (Cyber Hygiene Guidelines for Seniors): `cybercrime.gov.in`

• Reserve Bank of India (Financial Literacy for Senior Citizens): `rbi.org.in`

• Telecom Department (Sanchar Saathi Citizen Safety): `sancharsaathi.gov.in`

अध्याय 14 • 1-PAGE MASTER CHECKLIST

बुज़ुर्गों की Safety Checklist

पूरी किताब का निचोड़: 6 सुनहरे नियम जो हर माता-पिता को जीवन भर सुरक्षित रखेंगे।

याद रखने के 6 सबसे बड़े नियम

माता-पिता और वरिष्ठ नागरिकों के लिए नीचे दिए गए 6 नियम एक सुरक्षा कवच की तरह हैं। इन्हें रोज़ाना याद रखें या Print करके अपने कमरे में चिपका लें:

✓

1. पैसे लेने के लिए कोई PIN नहीं

UPI PIN सिर्फ पैसे भेजने (कटने) के लिए होता है। पैसे आने के लिए दुनिया में कभी कोई PIN नहीं डालना पड़ता।

✓

2. Phone पर आया Code (OTP) किसी को न दें

कोई कितना भी बड़ा अधिकारी या Bank मैनेजर बने, अपने Phone की Screen पर आया 6 अंकों का Code किसी को मुँह से न बताएँ।

✓

3. Video Call पर Police देखते ही Call काटें

कानून में Video Call पर कोई गिरफ़्तारी या जाँच नहीं होती। Video Call पर वर्दी दिखते ही सीधे Red Button दबाएँ।

✓

4. अनजान नीले Link और File को न छुएँ

WhatsApp पर आए बिजली बिल, लॉटरी या शादी के Card के नाम वाली किसी भी अनजान File या Link पर Click न करें।

✓

5. Pension या Bank के लिए सीधे Branch जाएँ

जीवन प्रमाण पत्र या Bank खाते के किसी भी काम के लिए Phone की बजाय सीधे अपनी Bank Branch या Post Office जाएँ।

6. 10 Second रुकें और घर के बच्चों को बताएँ

कोई कितना भी डराए या लालच दे, 10 Second का विराम लें और कमरे से बाहर निकलकर अपने बेटे या बेटी को दिखाएँ।

Bank या सरकार से संपर्क का 3-Step नियम

अगर कभी भी कोई समस्या आए, तो Google पर अनजान Number ढूँढने के बजाय हमेशा इस 3-Step रास्ते पर चलें:

1. **Google पर सही सरकारी Website खोलें**
   Browser के Address Bar में सीधे `cybercrime.gov.in` या `sancharsaathi.gov.in` Type करें।
2. **Official Contact Us सेक्शन पर जाएँ**
   Website के मुख्य Menu में जाकर Contact Us या Helpline विकल्प पर Click करें।
3. **Official Number सीधे Website से लें**

Website पर दिए गए Verified Helpline Number को देखकर ही अपने Phone से मिलाएँ।

अंतिम निष्कर्ष: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

- हर अनजान Call पर शांत रहें और 10 Second रुककर सोचें।
- कोई भी नया कदम उठाने से पहले अपने परिवार से बात करें।
- इस Checklist को Print करके अपने कमरे में चिपका लें।

❌ यह कभी न करें (DONTs)

- किसी अनजान व्यक्ति के कहने पर UPI PIN या OTP कभी न डालें।
- डर या हड़बड़ी में आकर किसी अनजान खाते में पैसे कभी न भेजें।
- Phone पर हुई किसी भी घटना को अपने परिवार से कभी न छुपाएँ।

OFFICIAL स्रोत व नियम

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

• Telecom Department (Sanchar Saathi Portal): `sancharsaathi.gov.in`

• Reserve Bank of India (Senior Citizen Financial Safety): `rbi.org.in`

शब्दावली • SENIOR SAFETY GLOSSARY

बुज़ुर्गों के लिए जरूरी डिजिटल शब्द

UPI PIN (पिन नंबर)

4 या 6 अंकों का आपका सबसे सीक्रेट पासवर्ड। यह **केवल पैसे काटने (भेजने)** के लिए डाला जाता है। पैसे आने के लिए इसकी कभी जरूरत नहीं होती।

OTP (One Time Password) (वन टाइम पासवर्ड)

बैंक द्वारा SMS पर आया अस्थायी कोड। किसी भी फोन कॉल पर, चाहे वह बैंक मैनेजर कहे या पुलिस, कभी किसी को न बताएं।

QR Code (क्यूआर कोड)

काले-सफेद चौकोर बक्सों वाला कोड। इसे स्कैन करने का मतलब हमेशा **पैसे भेजना** होता है। पैसे लेने के लिए कभी QR स्कैन नहीं किया जाता।

Digital Arrest (डिजिटल अरेस्ट)

ठगों द्वारा Video Call पर फर्जी पुलिस स्टेशन का सेट बनाकर डराना। कानून में **Digital Arrest नाम की कोई चीज नहीं होती**।

AI Voice Clone (नकली आवाज)

कंप्यूटर सॉफ्टवेयर से आपके बेटे, बेटी या पोते की हूबहू आवाज बनाकर एक्सीडेंट के नाम पर पैसे मांगना। तुरंत फोन काटकर पुराने नंबर पर बात करें।

Screen Share App (AnyDesk / TeamViewer)

ऐसा ऐप जिसे इंस्टॉल करते ही सामने वाला आपके पूरे फोन की स्क्रीन देख लेता है और आपका बैंक खाता खाली कर सकता है। कभी इंस्टॉल न करें।

Life Certificate (जीवन प्रमाण) (पेंशन सत्यापन)

पेंशन जारी रखने के लिए साल में एक बार दिया जाने वाला प्रमाण पत्र। यह बैंक शाखा, पोस्ट ऑफिस या सरकारी ऐप पर बनता है, किसी अनजान कॉल पर नहीं।

Senior Cyber Safety Pledge

माँ-बाप के 4 अटूट सुरक्षा नियम

घर के हर बड़े-बुजुर्ग को ये 4 बातें हमेशा याद रखनी हैं:

1. **पैसा पाने के लिए PIN नहीं:**
   खाते में पैसा आने के लिए कभी कोई PIN या OTP नहीं लगता।

2. **Video Call पर गिरफ्तारी नहीं:**
   असली पुलिस कभी वीडियो कॉल पर Digital Arrest नहीं करती।

3. **मुसीबत की कॉल पर फोन काटें:**
   बच्चे या रिश्तेदार के एक्सीडेंट की खबर पर पहले उनके पुराने नंबर पर फोन करें।

4. **फोन में कोई ऐप न डालें:**
   अनजान कॉल पर AnyDesk या स्क्रीन शेयरिंग ऐप कभी डाउनलोड न करें।

✓ 14 आसान अध्याय | ✓ Senior Friendly बड़े अक्षर | ✓ 100% मुफ्त नागरिक सुरक्षा

सुरक्षित संपर्क नियम: किसी भी Bank, Pension Office या Police का नंबर Google पर ढूंढने के बजाय सीधे उनकी Official Website खोलकर Contact Us सेक्शन से ही निकालें।

National Cyber Safety Awareness Series • 2026 Edition

Mobile Pocket Format (120mm × 190mm)