An Initiative of CollCom

Collcom
Empowering Youth through Community Service

ISSN: 2583-9969

Vol 18, Issue September 2024

CYBER संस्कार

साइबर अपराध के खिलाफ एक कदम

प्रीतेश मिश्रा
डॉ गौरव कुमार

Digital Arrest Scam!

साइबर संस्कार : Digital Arrest Scam!

प्रीतेश मिश्रा, डॉ गौरव कुमार

प्रकाशक : कॉलकम

1043/2, मेहरावाली अपार्टमेंट,
महरौली नई दिल्ली, 110030, भारत

संपर्क: +91 -9868189955

ईमेल: pr@collcom.org

वेबसाइट: www.collcom.org

प्रथम संस्करण : सितम्बर 2024

मूल्य : ₹ 49

मुद्रक : कॉलकम, भारत

ISSN : 2583-9969

Abstract(सारांश)

इस विशेषांक में "डिजिटल अरेस्ट स्कैम" जैसे खतरनाक साइबर अपराध का विश्लेषण किया गया है, जो भारत में तेजी से फैल रहा है। इसमें दो केस स्टडीज के माध्यम से दिखाया गया है कि कैसे ठग फर्जी पुलिस स्टेशन, सरकारी अधिकारी बनकर वीडियो कॉल्स और धमकियों का इस्तेमाल करके पीड़ितों को जाल में फंसाते हैं। एक केस में लखनऊ की महिला डॉक्टर से 2.8 करोड़ रुपये की ठगी की गई, जबकि दूसरे में एक युवक से 70 लाख रुपये ऐंठे गए। मैगज़ीन में इन ठगों की कार्यप्रणाली (modus of operandi) को उजागर किया गया है और उनसे बचने के लिए सुरक्षा सुझाव दिए गए हैं। इसे पढ़कर हम ये जानेंगे कि ऐसे जालसाजों से कैसे बचें और अपने डिजिटल जीवन को सुरक्षित रखें। इस विशेषांक का उद्देश्य जागरूकता बढ़ाना और साइबर अपराधों से बचाव के उपायों को समझाना है।

विषय-सूची

Digital Arrest Scam!

Contents

Empowering Youth through Community Service

Page No.

- डिजिटल अरेस्ट ठगी की भयावह स्थिति (Media Report) 05-06
- Digital Arrest Scam एवं Working 07
- डिजिटल अरेस्ट स्कैम की कार्यप्रणाली 08-09
  - पार्सल घोटाले के रूप में 08
  - परिवार के सदस्यों की संलिप्तता दिखा कर 08
  - आधार या फ़ोन नंबर का दुरुपयोग करके 09
  - पोर्नोग्राफिक सामग्री देखने पर डिजिटल गिरफ्तारी 09-10
- साइबर ठग कैसे तय करते हैं अपना शिकार 10
- Case Study के माध्यम से फ्रॉड को समझना 11-15
- डिजिटल अरेस्ट से बचने के उपाय और सत्यता की जाँच के तरीके 17
- अनधिकृत(unauthorised) जारी मोबाइल नंबरों को हटाने की प्रक्रिया 18
- UPI Payment Tips 19-21
- फ्रॉड होने पर शिकायत कहाँ करें 19
  - Cyber Fraud Complaint 20
  - UPI के माध्यम से हुए फ्रॉड की शिकायत 22
- निःशुल्क साइबर संस्कार प्रशिक्षण के बारे में 23-25
- संस्था के कार्यकारणी सदस्य 26
- मैगजीन के पिछले संस्करण 27
- संस्था से जुड़ने का तरीका 28

Hindustan Times Subscribe

Home HT Premium Loan ₹10 Lakh Cricket

Kolkata Rape Case Live Updates Paralympics 2024 Liv

Another doctor in Lucknow falls prey to digital arrest scam, duped of ₹48 lakh

By HT Correspondent

Aug 30, 2024 06:32 AM IST

INDIA TODAY AAJ TAK GNTTV LALLANTOP BUSINESS TODAY BANGLA MALAYALAM NORTHEAST BT BAZAAR HAR

INDIA TODAY

Home / Technology / News / Fake digital arrest scam: Man loses Rs 1.2 crore after receiving a call

Fake digital arrest scam: Hyderabad man loses Rs 1.2 crore after receiving calls from scammers

A Hyderabad resident lost Rs 1.2 crore over 20 days to scammers posing as police officers in a fake digital arrest scam. The victim was manipulated into believing he was in serious legal trouble, leading to severe mental strain and isolation.

जागरण

होम ताज़ा ब्रेकिंग राष्ट्रीय शेयर बाजार दुनि

जागरण एग्री पंचायत जागरण बदलाव EICHER TRACTORS

HINDI NEWS NOIDA

रेलवे से रिटायर जीएम की डिजिटल गिरफ्तारी, घर बैठे गंवाए 52.50 लाख रुपये; ठगी से बचने को आप भी बरतें ये सावधानियां

Hindustan Times Subscribe

Home HT Premium Loan ₹10 Lakh Cricket

Kolkata Rape Case Live Updates Paralympics 2024 Liv

Chandigarh: Senior citizen loses ₹1 crore in digital arrest scam

By HT Correspondent, Chandigarh

Aug 26, 2024 10:56 AM IST

अमर उजाला एप डाउनलोड करें

Noida News: दो दिन तक डिजिटल अरेस्ट कर महिला से ठगे 9.70 लाख

नोएडा ब्यूरो

Updated Sat, 10 Aug 2024 10:41 PM IST

Hindustan Times Subscribe

Home HT Premium Loan ₹10 Lakh Cricket Games & Puzzles Real Estate India World HTCit

Powered By 99acres.com

Kolkata Rape Case Live Updates Paralympics 2024 live updates Reliance AGM 2024 Live Videos Photos W

Retired major general put under 'digital arrest' for five days, duped of ₹2 crore by fraudsters

OPEN APP

By Arun Singh

Aug 29, 2024 07:14 AM IST

Exclusive

THE TIMES OF INDIA OPEN APP

Lucknow SGPGIMS Professor Duped Of Rs 2.81 Crore In 'Digital Arrest' Scam

CITY | Pathikrit Chakraborty | TNN | Aug 14, 2024, 15:32 IST

UP NEWS LUCKNOW NEWS VARANASI NEWS UP

ETV BHARAT उत्तर प्रदेश Uttar Pradesh

डॉक्टर डिजिटल अरेस्ट केस: 2.81 करोड़ में सिर्फ 27.88 लाख ही होंगे रिकवर, जानिए क्यों - cyber fraud with PGI Doctor

5 Min Read

By ETV Bharat Uttar Pradesh Team

Published : Aug 16, 2024, 9:15 PM IST

google.com/amp/s/www.aajtak.in/amp/technology/tech-news/story/noida

फेक कोरियर वाले की कॉल, 5 दिन डिजिटल अरेस्ट, नोएडा की बुजुर्ग महिला से ऐसे ठगे 1.3 करोड़

Delhi-NCR से साइबर ठगी का नया केस सामने आया है, जहां एक बुजुर्ग महिला को 1.3 करोड़ रुपये का चूना लगाया है. दरअसल, महिला को एक शख्स का कॉल आया. कॉल करने वाले ने खुद को कुरियर कंपनी का कर्मचारी बताया. यहां से साइबर ठगी की शुरुआत हुई. इस केस में महिला को 5 दिन तक डिजिटली अरेस्ट भी रखा. आइए इस केस के बारे में डिटेल्स में जानते हैं.

SHARE TWEET WHATSAPP

EDITION IN

THE TIMES OF INDIA

SIGN IN

City Jaipur Mumbai Delhi Bengaluru Hyderabad Kolkata Chennai Agra Agartala Ahmedabad Ajmer Allahabad Amaravati Amritsar

CIVIC ISSUES CRIME POLITICS SCHOOL AND COLLEGES RAJASTHAN ELECTIONS VIDEOS PHOTOS WEATHER

NEWS / CITY NEWS / JAIPUR NEWS / Senior Citizen Loses ₹12L In 'Digital Arrest' Fraud

TRENDING Badlapur Sexual Assault Kannada Actor Darshan Shivaji Statue Collapse Anil Deshmukh Snake Bites Bengaluru Teen Gujarat Flood

Senior citizen loses ₹12L in 'digital arrest' fraud

TNN / Aug 30, 2024, 05:01 IST

SHARE AA FOLLOW US

पढ़ें अपने शहर की रियल टाइम खबरें

कभी भी, कहीं भी डाउनलोड करें दैनिक भास्कर ऐप

दैनिक भास्कर

लखनऊ PGI की महिला डॉक्टर से 2.8 करोड़ की ठगी: CBI अफसर बनकर फंसाया, 6 दिन डिजिटल अरेस्ट रखा, 7 खाते में ट्रांसफर कराए पैसे

लखनऊ 15 दिन पहले

DIGITAL ARREST SCAM!

आज के डिजिटल युग में, साइबर हमले और ऑनलाइन धोखाधड़ी एक गंभीर चुनौती बन गए हैं। इन्हीं समस्याओं में से एक महत्वपूर्ण समस्या **"डिजिटल अरेस्ट"** है, जो न केवल वित्तीय नुकसान का कारण बनती है, बल्कि पीड़ितों की मानसिक स्थिति और उनके विश्वास को भी बुरी तरह प्रभावित करती है। डिजिटल सुरक्षा की अनदेखी के कारण समाज में एक गहरे संकट की स्थिति उत्पन्न हो रही है। अनपढ़ तो छोड़िए **इस स्कैम के शिकार डॉक्टर और इंजीनियर्स भी हो रहे हैं।** इस मैगज़ीन के इस अंक में, हम "डिजिटल अरेस्ट" के विभिन्न पहलुओं का विश्लेषण करेंगे और स्वयं को सुरक्षित रखने के लिए प्रभावी उपायों पर चर्चा करेंगे। आइए, मिलकर डिजिटल सुरक्षा की दिशा में एक महत्वपूर्ण कदम बढ़ाएं।

Cyber Crime Index

Ranking countries by cybercrime threat level

Ranking	Country	WCI Score	Ranking	Country	WCI Score
1	Russia	58.39	11	Iran	4.78
2	Ukraine	36.44	12	Belarus	3.87
3	China	27.86	13	Ghana	3.58
4	USA	25.01	14	South Africa	2.58
5	Nigeria	21.28	15	Moldova	2.57
6	Romania	14.83	16	Israel	2.51
7	North Korea	10.61	17	Poland	2.22
8	UK	9.01	18	Germany	2.17
9	Brazil	8.93	19	Netherlands	1.92
10	India	6.13	20	Latvia	1.68

Source: Market Brew by TATA Fintech

जनवरी से अप्रैल 2024 के बीच साइबर अपराधों के कारण भारतीय नागरिकों को **1,750 करोड़** रुपये से अधिक का नुकसान हुआ है। यह आंकड़ा गृह मंत्रालय द्वारा संचालित राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल पर दर्ज की गई **7,40,000 से अधिक शिकायतों** से सामने आया है, जो देश में साइबर अपराधों की बढ़ती समस्या को दर्शाता है।

2024 के शुरुआती चार महीनों में, सिर्फ **"डिजिटल गिरफ्तारी" के 4,599 मामलों** के कारण भारतीय नागरिकों को 120 करोड़ रुपये से अधिक का नुकसान हुआ है।

दिल्ली पुलिस के अनुसार, देश भर में **हर महीने "डिजिटल गिरफ्तारी"** के लगभग **200 मामले** दर्ज किए जाते हैं, जो इस बढ़ती साइबर अपराध की गंभीरता को उजागर करता है।

हाल ही में शोधकर्ताओं की एक टीम द्वारा किए गए एक नए अध्ययन के अनुसार, भारत वैश्विक स्तर पर साइबर अपराध के सबसे अधिक जोखिम वाले क्षेत्रों में 10वें स्थान पर है।

Digital Arrest Scam क्या है ?

डिजिटल अरेस्ट एक प्रकार की साइबर धोखाधड़ी है जहां अपराधी खुद को सरकारी अधिकारी, जैसे कि CBI, पुलिस, या कस्टम अफसर, के रूप में पेश करते हैं। ये अपराधी फर्जी दस्तावेज़, वीडियो कॉल, और नकली गिरफ्तारियों के माध्यम से पीड़ित को डराते हैं और उन्हें फर्जी मामलों में फंसाने की धमकी देते हैं।

कैसे काम करता है यह स्कैम?

- **पहला संपर्क: ठग फोन, ईमेल, या मैसेज के माध्यम से** पीड़ित से संपर्क करते हैं, खुद को सरकारी अधिकारी के रूप में प्रस्तुत करते हैं, और दावा करते हैं कि पीड़ित के खिलाफ आपराधिक मामला है।

- **डर का माहौल बनाना:** ठग फर्जी दस्तावेज़, वीडियो कॉल, और नकली गिरफ्तारी वारंट दिखाकर डर पैदा करते हैं। वे दावा करते हैं कि पीड़ित के खिलाफ मनी लॉन्ड्रिंग या अन्य गंभीर आरोप हैं।

- **लंबी निगरानी:** पीड़ित को यह विश्वास दिलाया जाता है कि उन्हें **'डिजिटल अरेस्ट'** पर रखा गया है, जहां उनके हर कदम की निगरानी की जा रही है। वे पीड़ित को लंबी वीडियो कॉल पर जोड़े रखते हैं, कभी-कभी उन्हें सोने तक नहीं देते, ताकि उनका मानसिक दबाव बढ़े।

- **भुगतान की मांग:** ठग पीड़ित से जल्दी से जल्दी पैसे ट्रांसफर करने के लिए कहते हैं, ताकि वे "कानूनी कार्रवाई" से बच सकें। आमतौर पर, वे बैंक खातों, गिफ्ट कार्ड्स, या क्रिप्टोकरेंसी का उपयोग करने के लिए कहते हैं ताकि भुगतान ट्रैक न किया जा सके।

- **विश्वास पैदा करने के लिए जानकारी का उपयोग:** ठग पहले से ही पीड़ित के बारे में व्यक्तिगत और वित्तीय जानकारी जुटा लेते हैं, जैसे कि बैंक खातों की डिटेल, पारिवारिक विवरण, और सरकारी कागजात, ताकि वे भरोसेमंद लगें। इससे पीड़ित को लगता है कि अपराधी वास्तव में सरकारी अधिकारी हैं।

- **फर्जी वीडियो और सेटअप: ठग पहले से नकली थाने, नकली पुलिस अधिकारी, या अन्य सरकारी सेटअप तैयार** रखते हैं और वीडियो कॉल के दौरान इन्हें दिखाते हैं ताकि पीड़ित को लगे कि वे असली अधिकारी से बात कर रहे हैं।

डिजिटल अरेस्ट स्कैम की कार्यप्रणाली

1. पार्सल घोटाले के रूप में (As a parcel scam)

- डिजिटल अरेस्ट धोखाधड़ी में, साइबर अपराधी पार्सल घोटाले जैसी तकनीक का उपयोग करते हैं। इसमें, पीड़ित को एक फर्जी कॉल या संदेश भेजा जाता है, जिसमें दावा किया जाता है कि उनके नाम पर अवैध सामग्री वाला एक पार्सल पकड़ा गया है।

- अपराधी खुद को कस्टम अधिकारी या कानून प्रवर्तन एजेंट के रूप में पेश करते हैं और पीड़ित से जुर्माना या शुल्क के रूप में पैसे की मांग करते हैं ताकि उन्हें कानूनी परेशानी से बचाया जा सके।

2. परिवार के सदस्यों की संलिप्तता दिखा कर
(Make false claims of involvement of family members)

- डिजिटल अरेस्ट धोखाधड़ी में, अपराधी पीड़ितों के परिवार के सदस्यों (बेटा या बेटी या किसी नजदीकी रिश्तेदार के नाम) की संलिप्तता (False Claim of Involvement) का झूठा प्रमाण देकर उन्हें मानसिक दबाव में डालते हैं। ये अपराधी फोन कॉल, ईमेल, या मैसेज के जरिए संपर्क करते हैं और दावा करते हैं कि उनके किसी परिवार के सदस्य को आपराधिक गतिविधि में पकड़ा गया है या उन पर गंभीर आरोप लगे हैं। वे कहते हैं कि तुरंत जुर्माना या फीस चुकाने पर ही कानूनी कार्रवाई से बचा जा सकता है।

- अपराधी पीड़ित को विश्वास में लेने के लिए परिवार के सदस्यों के नाम, स्थान, या अन्य व्यक्तिगत जानकारी का उपयोग करते हैं। इसके अलावा, वे पीड़ित को डराते हैं कि अगर तुरंत कार्रवाई नहीं की गई, तो परिवार के सदस्य की गिरफ्तारी या अन्य गंभीर परिणाम हो सकते हैं।

- इस प्रकार की धोखाधड़ी के दौरान, अपराधी बार-बार कॉल या मैसेज के जरिए संपर्क में रहते हैं, पीड़ित को मानसिक रूप से दबाव में रखते हैं, और उन्हें भयभीत कर देते हैं ताकि वे जल्द से जल्द पैसे का भुगतान कर दें।

- अपराधी इस प्रक्रिया में नकली दस्तावेज़, वीडियो कॉल, और अन्य तकनीकों जैसे किसी बड़े अधिकारी से बात करवाकर पैसे से केस सेटलमेंट की बात करते हैं ताकि पीड़ित को लगे कि वे वास्तव में किसी सरकारी एजेंसी से बात कर रहे हैं। उनका उद्देश्य यह है कि पीड़ित पूरी तरह से भ्रमित हो जाएं और उनकी मांगी गई राशि का भुगतान कर दें।

3. आधार या फ़ोन नंबर का दुरुपयोग करके

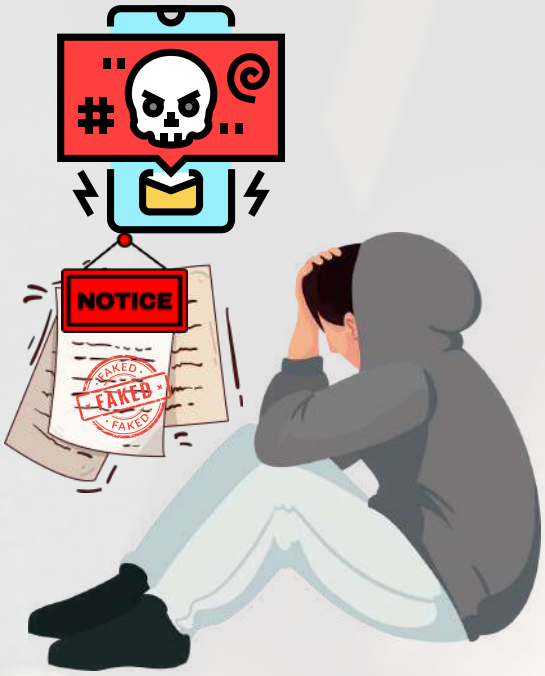
- डिजिटल अरेस्ट धोखाधड़ी में, अपराधी पीड़ित के आधार कार्ड या फोन नंबर का भी दुरुपयोग कर उन्हें अवैध गतिविधियों में फंसा देते हैं।
- अपराधी पीड़ित से संपर्क कर दावा करते हैं कि उनके आधार या फोन नंबर का इस्तेमाल मनी लॉन्ड्रिंग, आतंकवादी फंडिंग, या अन्य आपराधिक गतिविधियों के लिए हुआ है।
- पीड़ित को डराने के लिए नकली दस्तावेज़, गिरफ्तारी वारंट, या वीडियो कॉल का सहारा लिया जाता है, जिससे वे मानसिक दबाव में आ जाते हैं और तुरंत पैसे का भुगतान करने के लिए मजबूर हो जाते हैं।
- अगर कोई कॉल पर जुड़ने से मना करता है तो ठग उनके घर पुलिस भेजने की बात करते हैं। वीडियो कॉल पर जुड़ने पर ठग पहले से तैयारियां करके रखते हैं। ऐसे अपराधी पहले से थाने का सेटअप, नकली एसपी, दरोगा, नारकोटिक्स और सीबीआई जैसे अधिकारियों से बात कर पीड़ित को पूरी तरह फंसाने की कोशिश करते हैं।

4. पोर्नोग्राफिक सामग्री देखने पर डिजिटल गिरफ्तारी धोखाधड़ी

(Digital Arrest Fraud for Viewing Pornographic Content)

डिजिटल गिरफ्तारी धोखाधड़ी का यह तरीका जिसमें साइबर अपराधी पीड़ितों पर पोर्नोग्राफिक सामग्री देखने या डाउनलोड करने का झूठा आरोप लगाते हैं। इसमें अक्सर किशोर या अश्लील सामग्री देखने वाले लोगों को निशाना बनाया जाता है। यह सेक्सटॉर्शन (sextortion) का एक रूप है, जहां ठग खुद को पुलिस या साइबर क्राइम अधिकारी बताकर पीड़ित को गिरफ्तार करने या उनके परिवार को जानकारी देने की धमकी देते हैं। वे पीड़ित के भय और सामाजिक शर्मिंदगी का फायदा उठाते हैं, जिससे पीड़ित मानसिक दबाव में आकर धन देने के लिए मजबूर हो जाता है।

पोर्नोग्राफिक सामग्री देखने पर धोखाधड़ी की प्रक्रिया



- **निशाना चुनना:** अपराधी सोशल मीडिया, चैट रूम्स, ऑनलाइन गेमिंग या अन्य ऑनलाइन प्लेटफ़ॉर्म से नाबालिगों या युवाओं को निशाना बनाते हैं।

- **फर्जी नोटिस:** अपराधी पीड़ित के डिवाइस पर फर्जी नोटिस भेजते हैं, जिसमें सरकारी एजेंसी, पुलिस, या साइबर विभाग का नाम इस्तेमाल किया जाता है। इसमें लिखा होता है कि पीड़ित ने अवैध पोर्न सामग्री देखी है या डार्क वेब से कुछ डाउनलोड किया है।

- **धमकी देना:** अपराधी पीड़ित को डराते हैं कि अगर वे तुरंत जुर्माना या "फाइन" नहीं भरते, तो उन्हें गिरफ्तार किया जाएगा या उनके परिवार को इस बात की सूचना दी जाएगी इत्यादि।

साइबर ठग कैसे तय करते हैं अपना शिकार ?

- डिजिटल अरेस्ट करने वाले गैंग ऐसे लोगों को निशाना बनाते हैं जो वित्तीय रूप से मजबूत होते हैं, जैसे रिटायर अधिकारी, डॉक्टर, शिक्षक, और इंजीनियर। ये अपराधी डार्क वेब (वो साइटों जो सामान्य सर्च में नहीं दिखती) से ऐसे समूहों का डेटा खरीदते हैं, जिसमें बैंक खातों की जानकारी, निवेश विवरण, और पेंशन की जानकारी शामिल होती है।

- साइबर अपराधी अपने टारगेट ग्रुप का भरोसा बनाने के लिए सेविंग अकाउंट से लेकर एफडी तक में जमा राशि की पूरी डिटेल बताते हैं। मामला असली लगे, इसके लिए वो जिले के प्रशासनिक अफसरों के नाम का इस्तेमाल करते हैं। इन चालबाजों से सामने वाला इंसान अपराधियों पर भरोसा कर बैठता है। पीड़ित को लगता है कि वह सच में किसी मुसीबत में फंसने वाला है।

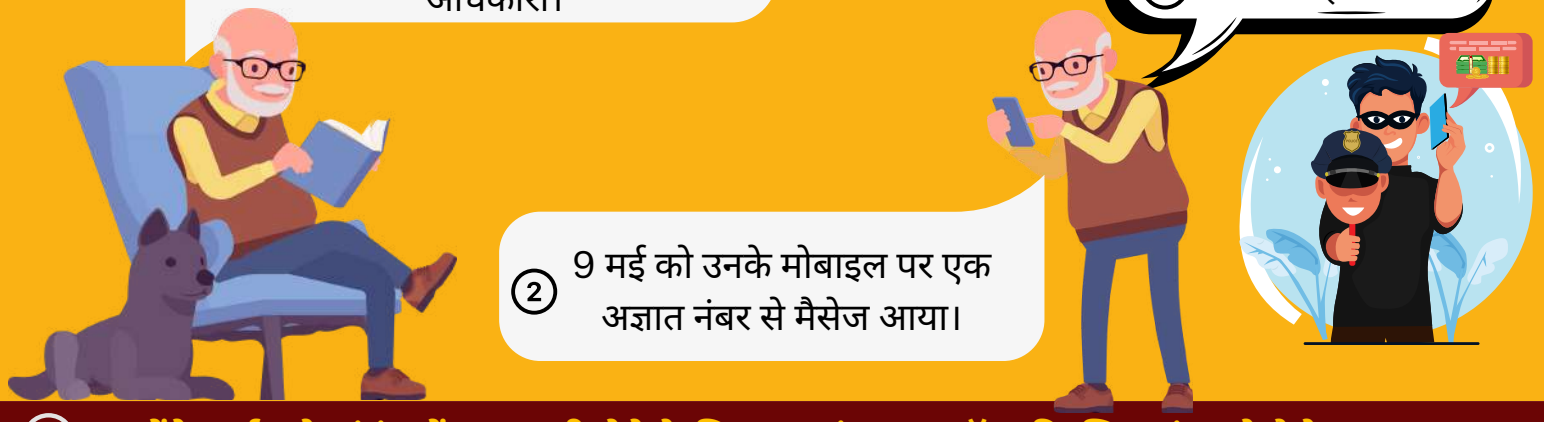
- इसके अलावा, ठग यह भी ध्यान रखते हैं कि उनके टारगेट में वे लोग शामिल हों, जिन्हें किसी भी धोखाधड़ी का संदेह न हो। वे अक्सर बुजुर्ग लोगों या तकनीकी जानकारी से अनभिज्ञ व्यक्तियों को निशाना बनाते हैं, जिन्हें आसानी से धोखा दिया जा सके।

केस स्टडी -1

सच्ची घटना के माध्यम से फ्रॉड को समझना

यह घटना भारतीय रेलवे में जीएम के पद से सेवानिवृत्त एक अधिकारी की है, जिन्हें साइबर अपराधियों ने "डिजिटल अरेस्ट" के जाल में फंसा कर 52.50 लाख रुपये की ठगी का शिकार बनाया। इस कहानी के माध्यम से हम समझेंगे कि उन्होंने किन गलतियों के कारण ठगी का सामना किया और आप कैसे इन गलतियों से बच सकते हैं। यह जानना आवश्यक है कि साइबर अपराधी कैसे मानसिक दबाव, फर्जी पहचान, और कानूनी धमकियों का उपयोग करते हैं ताकि हम जागरूक रहकर खुद को सुरक्षित रख सकें।

पढ़ने के लिए पोस्टर पर क्लिक करें।



④ **उन्होंने पार्सल के संबंध में जानकारी लेने के लिए उस नंबर पर कॉल की, जिस नंबर से मैसेज आया था।**

⑦ अपराधी ने पीड़ित को बताया कि उनके पार्सल में चार पासपोर्ट, तीन क्रेडिट कार्ड, कपड़े, और 100 ग्राम ड्रग्स थे। इसके अलावा, उन्होंने आरोप लगाया कि पीड़ित के तीन बैंक खातों की केवाईसी विभिन्न शहरों में की गई है और इन खातों का उपयोग मनी लॉन्ड्रिंग के लिए किया जा रहा है, जिसे दाऊद और नवाब मलिक जैसे लोगों द्वारा आतंकी गतिविधियों के लिए इस्तेमाल किया गया है। (अपराधी का उद्देश्य पीड़ित को डराकर उनसे धन की मांग करना था।)

⑧ सहमे हुए प्रमोद कहते हैं, "मेरा उन लोगों से कोई लेना-देना नहीं है, मैंने यह सब नहीं किया है।" (वे अपराधियों द्वारा लगाए गए आरोपों से घबराए हुए हैं और स्पष्ट करते हैं कि उनके किसी भी अवैध गतिविधियों से कोई संबंध नहीं है।)

(अपराधी का उद्देश्य पीड़ित को धमकाकर डराना और मनोवैज्ञानिक दबाव बनाकर उन्हें चुप रखने का था, ताकि वे आसानी से धोखाधड़ी के जाल में फंस सकें।)

⑨ "मैं मुंबई क्राइम ब्रांच का अधिकारी बोल रहा हूँ। अगर तुमने इस बातचीत के बारे में किसी को भी बताया, तो तुम्हें जेल भेज दिया जाएगा। ध्यान रहे, तुम्हारा परिवार भी 24 घंटे की निगरानी में है।"

⑩ इसके बाद आरोपी ने वीडियो कॉल के माध्यम से संपर्क किया, ताकि पीड़ित को यह विश्वास दिलाया जा सके कि वे वास्तव में एक सरकारी अधिकारी से बात कर रहे हैं।

⑪ वीडियो कॉल का उपयोग करके, अपराधी ने अपने झूठे दावे को और अधिक विश्वसनीय बनाने की कोशिश की और पीड़ित को मनोवैज्ञानिक दबाव में रखा ताकि वे उनकी मांगों को मान लें और किसी को भी इस बातचीत के बारे में न बताएं।

प्रमोद डर के कारण आरोपियों के दबाव में आ जाते हैं और उनकी बातों में आकर तीन बार में कुल 52.50 लाख रुपये ट्रांसफर कर देते हैं। अपराधियों द्वारा दी गई धमकियों और झूठे आरोपों से भयभीत होकर, प्रमोद ने उनकी मांगों का पालन किया, जो कि साइबर ठगों का उद्देश्य था।

⑫

⑬ जब तक प्रमोद जी को यह समझ में आता कि उनके साथ धोखाधड़ी हो चुकी है, तब तक बहुत देर हो चुकी थी। साइबर अपराधियों ने उन्हें इतनी अच्छी तरह से भ्रमित और भयभीत किया कि उन्होंने तीन बार में 52.50 लाख रुपये ट्रांसफर कर दिए। बाद में, उन्हें एहसास हुआ कि वे एक सुनियोजित जाल में फंस गए थे।

⑭ ध्यान रखें, मेरी तरह किसी अनजान व्यक्ति के बहकावे में न आएं, संदेह होने पर तुरंत शिकायत करें।

⑮ **ऐसी स्थिति में तुरंत 1930 पर कॉल करें या नजदीकी साइबर सेल में रिपोर्ट करें। सतर्क रहें और अपनी व्यक्तिगत जानकारी को सुरक्षित रखें। साइबर ठगों के खिलाफ यह सबसे प्रभावी तरीका है।**

केस स्टडी -2

सच्ची घटना के माध्यम से फ्रॉड को समझना

यह कहानी नोएडा के जयराज शर्मा की है, जो एक प्राइवेट बैंक में मैनेजर हैं। जालसाजों ने उन्हें "डिजिटल अरेस्ट" के नाम पर सात दिनों तक मानसिक दबाव में रखा और 52 लाख रुपये की ठगी कर ली। इस कहानी के माध्यम से हम समझ सकते हैं कि कैसे धोखाधड़ी करने वाले ठग लोगों को डर और भ्रम में डालते हैं, और ठगी से बचने के लिए क्या उपाय किए जा सकते हैं ।

पढ़ने के लिए पोस्टर पर क्लिक करें।

① ये हैं जयराज शर्मा, जो नोएडा के सेक्टर 20 में रहते हैं और यस बैंक में मैनेजर के पद पर कार्यरत हैं।

② **11 जून को जयराज शर्मा के पास एक अज्ञात नंबर से कॉल आई, जिसमें कॉलर ने खुद को ट्राई (टेलीकॉम रेगुलेटरी अथॉरिटी ऑफ इंडिया) का अधिकारी बताया।**

③ कॉलर ने दावा किया, "जयराज, आप जेट एयरवेज के संस्थापक नरेश गोयल के मनी लॉन्ड्रिंग केस की जांच के बाद आरोपी पाए गए हैं। आपके कैनरा बैंक खाते में नरेश गोयल की ओर से 7 करोड़ रुपये भेजे गए और निकाले गए हैं।"

④ जालसाजों ने जयराज को धमकी दी कि यदि वे जांच में ऑनलाइन सहयोग नहीं करते, तो उन्हें तुरंत गिरफ्तार कर लिया जाएगा। उन्होंने यह भी चेतावनी दी कि इस मामले के बारे में किसी को भी जानकारी नहीं दी जानी चाहिए। डर के कारण जयराज ने उनकी सभी बातें मान लीं और निर्देशों का पालन करने लगे।

⑤ जालसाजों ने जयराज को निर्देश दिया, "सुनो, स्काइप ऐप डाउनलोड करो..." इसके बाद उन्होंने कहा कि जांच के लिए स्काइप पर वीडियो कॉल के माध्यम से जुड़ना होगा ताकि वे आगे की 'जांच' में मदद कर सकें।

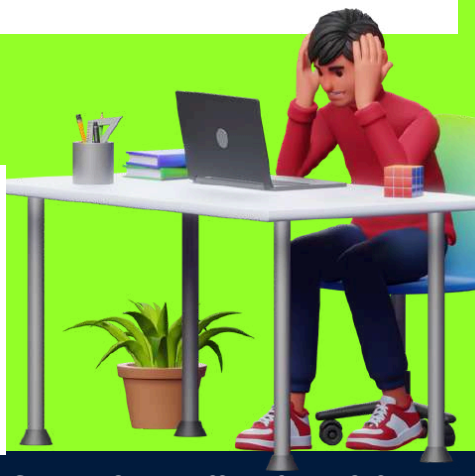
⑥ जयराज ने डरते हुए जवाब दिया, "जी ठीक है, करते हैं।"

⑦ जालसाजों ने स्काइप ऐप डाउनलोड करवाने के बाद जयराज से वीडियो कॉल के जरिए संपर्क किया और उन्हें "डिजिटल अरेस्ट" में डाल दिया। इसके बाद, उन्हें मानसिक दबाव में रखते हुए अगले सात दिनों तक अपराधी लगातार नॉर्मल और वीडियो कॉल के माध्यम से जयराज से बात करते रहे। जयराज ने पूरी तरह से समझे बिना ही उनकी मांगों का पालन करना शुरू कर दिया, जिससे ठगों को और भी अधिक अवसर मिला कि वे उन्हें मानसिक दबाव में रखकर ठगी को अंजाम दे सकें।

⑧ जालसाजों ने जयराज को धमकी दी, "यदि तुमने इन बातों को किसी के साथ भी साझा किया, तो इसे राष्ट्रीय रहस्य उजागर करने का मामला मानते हुए तुम्हें पूरी जिंदगी जेल में बितानी पड़ेगी।"

इस तरह के झूठे दावों और धमकियों का उद्देश्य जयराज को और भी डराना था, ताकि वह ठगों की बातों में आकर उनकी हर मांग को मानें और किसी से भी मदद न मांगें। ठग इस मनोवैज्ञानिक दबाव का उपयोग करते हुए पीड़ित को पूरी तरह से नियंत्रित करने की कोशिश कर रहे थे।

⑨ जालसाजों ने जयराज को धमकाते हुए कहा, "कल तुम्हारी सुप्रीम कोर्ट में ऑनलाइन सुनवाई होगी।"



⑩ इसी बीच, दो ठगों ने खुद को जज और वकील बताते हुए जयराज से संपर्क किया और फर्जी सुप्रीम कोर्ट का नाटक रचते हुए उनकी संपत्ति का पूरा विवरण मांगा, जिसमें बैंक स्टेटमेंट, स्टॉक, और म्यूचुअल फंड निवेश शामिल थे।

⑪ अब सुप्रीम कोर्ट में तुम्हारी "डिजिटल सुनवाई" शुरू हो रही है। अपनी संपत्ति का ब्योरा सांझा करो

⑫ जयराज ने डर के मारे 29 लाख रुपये की संपत्ति का विवरण साझा कर दिया। ये सब मेरे मेहनत की कमाई है।

काफी देर तक पूछताछ करने के बाद जालसाजों ने जयराज से कहा, "आपको इस मामले में पूरी तरह से सहयोग करना होगा, अन्यथा गंभीर कानूनी कार्रवाई की जाएगी। किसी से भी इस बारे में बात न करें, क्योंकि यह एक संवेदनशील मामला है।" अपराधियों का उद्देश्य जयराज को लगातार भयभीत रखना और उन्हें किसी भी प्रकार की मदद लेने से रोकना था ताकि वे अपनी ठगी की योजना को सफलतापूर्वक अंजाम दे सकें।

13 इसके बाद, एक ठग ने खुद को मजिस्ट्रेट बताते हुए कहा कि उनकी संपत्तियों का सत्यापन आरबीआई करेगा और सभी पैसे *12* निर्दिष्ट खातों में भेजने के लिए कहा।

14 "फिलहाल, जितनी भी रकम तुम्हारे खाते में है, उसे तुरंत हमारे द्वारा बताए गए 12 बैंक खातों में ट्रांसफर कर दो।"

15 जयराज ने डर और भ्रम की स्थिति में आकर 52 लाख रुपये ट्रांसफर कर दिए ।

16 सारे पैसे हासिल करने के बाद, अपराधियों ने 17 तारीख को जयराज को "डिजिटल अरेस्ट" से मुक्त कर दिया।

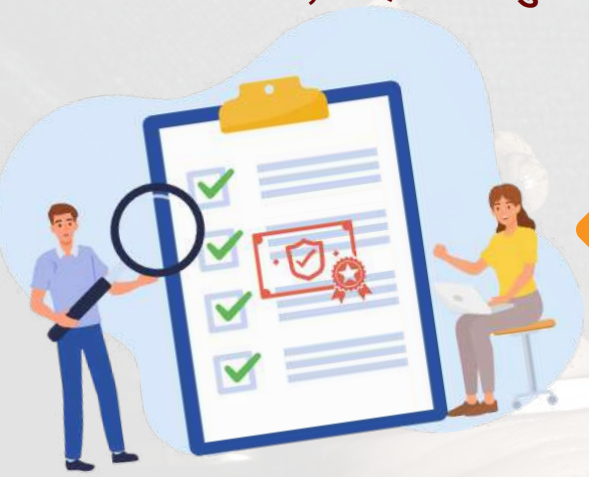
17 **जब जयराज ने अपने पैसे वापस मांगने के लिए उसी नंबर पर दोबारा कॉल की, तो सभी नंबर बंद पाए गए। तभी जाकर उन्हें समझ में आया कि वे एक सुनियोजित ठगी का शिकार हो चुके हैं।**

ऑनलाइन किसी भी अज्ञात व्यक्ति के बहकावे में न आएं, चाहे वह खुद को सरकारी कर्मचारी ही क्यों न बताए, ट्रू-कॉलर एंड कॉलर की व्हाट्सप्प का प्रोफाइल पिक्चर देख कर भ्रमित न हो । ऑनलाइन कभी भी किसी सरकारी कर्मचारी को पैसे न भेजें। किसी भी संदिग्ध स्थिति में संबंधित विभाग या स्थानीय थाने में संपर्क करें और सत्यापित करें। सतर्क रहें और अपनी व्यक्तिगत और वित्तीय जानकारी सुरक्षित रखें।

बताये गए केस स्टडीज से सीखने के मुख्य बिंदु

QUICK TIPS

सतर्कता: जब फोन पर कोई व्यक्ति पुलिस या वीडियो कॉल पर वर्दी पहने खुद को पुलिस या सरकारी अधिकारी या किसी जांच और सुरक्षा एजेंसी का अधिकारी बताए ऐसे किसी भी अज्ञात व्यक्ति के कॉल, मैसेज, या ईमेल पर तुरंत प्रतिक्रिया न दें।



सूचना की पुष्टि: हमेशा संदिग्ध जानकारी की सत्यता को आधिकारिक स्रोतों से जांचें।

ध्यान रखे - किसी भी विभाग का हेल्पलाइन नंबर गूगल या इस जैसे किसी भी सर्च इंजन पर डालकर सर्च न करे। हमेशा उनके आधिकारिक वेबसाइट से ही हेल्पलाइन नंबर ढूंढे।

सुरक्षा उपाय: अपनी व्यक्तिगत और वित्तीय जानकारी को गोपनीय रखें और उसे साझा करने से पहले सोचें।

समय पर कार्रवाई: यदि आपको धोखाधड़ी का संदेह होता है, तो तुरंत 1930 पर कॉल करें या नजदीकी साइबर सेल में शिकायत दर्ज कराएं।

धोखाधड़ी के जोखिम को कम करने के लिए जागरूक रहना और सावधानी बरतना अत्यंत महत्वपूर्ण है।

HELPFUL TIPS

डिजिटल अरेस्ट से सम्बंधित कुछ महत्वपूर्ण बातें

- पुलिस या किसी एजेंसी द्वारा वॉट्सऐप या वीडियो कॉल पर अरेस्ट वारंट जारी नहीं होता; ऐसे संदेशों पर विश्वास न करें।

- अगर कभी कोई फोन पर कहे कि आपके खिलाफ गैर जमानती वारंट या वारंट जारी किया गया है, तो तत्काल नजदीकी पुलिस स्टेशन जाएं। यहां कॉल के बारे में पूरी जानकारी दें, क्योंकि वारंट और गैर जमानती वारंट हमेशा कोर्ट जारी करता है। पुलिस का इसे वॉट्सऐप पर जारी करना नामुमकिन है।

- यदि कोई व्यक्ति फोन या वीडियो कॉल पर खुद को अधिकारी बताता है, तो तुरंत उसका नाम और नंबर गूगल पर सर्च करें। वह खुद को जिस विभाग का अधिकारी या पुलिस बता रहा हो, उस डिपार्टमेंट की वेबसाइट पर जाएं और पोस्टेड अफसरों की लिस्ट देखें।

- ठग खुद को जिस डिपार्टमेंट का बता रहा है, जैसे- नारकोटिक्स कंट्रोल तो वहां के हेल्पलाइन नंबर पर कॉल करें। इसी तरह वो जिस कूरियर कंपनी या सर्विस प्रोवाइडर का नाम ले रहे, वहां फोन कर मामले को जांचें। विभाग की आधिकारिक वेबसाइट पर जाकर अधिकारी की पुष्टि करें और हेल्पलाइन पर संपर्क करें।

- किसी भी संदिग्ध कॉल पर अपनी जानकारी साझा न करें और फर्जी नंबरों से बचने के लिए आधिकारिक स्रोत से ही हेल्पलाइन नंबर प्राप्त करें। किसी भी विभाग का हेल्पलाइन नंबर गूगल या इस जैसे किसी भी सर्च इंजन पर सर्च न करे। दरअसल, साइबर अपराधी गूगल पर इन एजेंसियों के नाम पर फर्जी नंबर अपलोड किए होते हैं।

- अगर आपने कोई पार्सल नहीं भेजा है या कोई कहे कि आपके नाम पर पार्सल मिला है, जिससे आपका मोबाइल नंबर और आधार नंबर मिला। ऐसे फोन कॉल पर भरोसा नहीं करें।

- वॉट्सऐप या वीडियो कॉल पर आपका बैंक अकाउंट देखने के बाद अगर कोई पुलिस क्लीयरेंस सर्टिफिकेट जारी करता है तो तय है कि ठग आपको बहकाने की कोशिश कर रहा। ठग आपका भरोसा जीतकर पैसे अकाउंट में ट्रांसफर करने के लिए ऐसा करते हैं।

- कॉल या वॉट्सऐप ऑडियो-वीडियो कॉल पर कोई कहता है कि आपके अकाउंट में हवाला या मनी लॉन्ड्रिंग का पैसा आया है, तो इस पर विश्वास ना करें। पुलिस या कोई भी सरकारी संस्था ऐसी जानकारी फोन के माध्यम से नहीं देती।

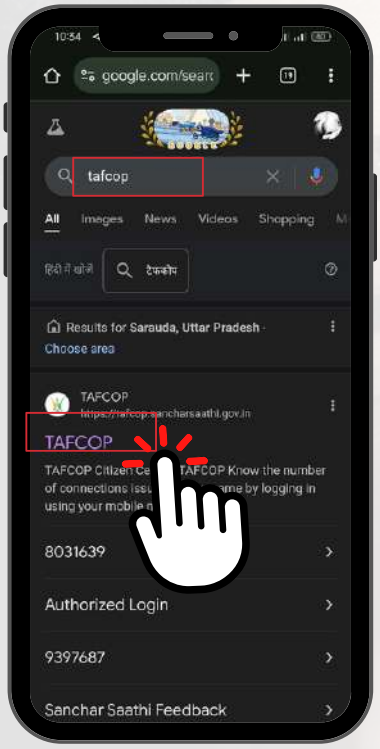
- अगर फोन पर कोई कानूनी कार्रवाई की धमकी देता है तो इस स्थिति में डरें बिल्कुल नहीं। ऐसा कुछ होने पर 1930 पर कॉल करे या अपने नजदीकी पुलिस स्टेशन को सूचित करें।

SPECIAL REPORT

साइबर सुरक्षा टिप्स

यह प्रक्रिया आपको अनधिकृत नंबरों को हटाने और धोखाधड़ी से बचने में मदद करती है।

यदि आपके नाम पर कोई अन्य मोबाइल नंबर जारी किया गया है और आपको इसके बारे में जानकारी नहीं है, तो इसे तुरंत हटाने के लिए निम्नलिखित कदम उठाएं:



Step 1- गूगल पर TAFCOP लिखकर सर्च करे, अथवा वेबसाइट https://tafcop.sancharsaathi.gov.in/telecomUser/ पर क्लिक करें।

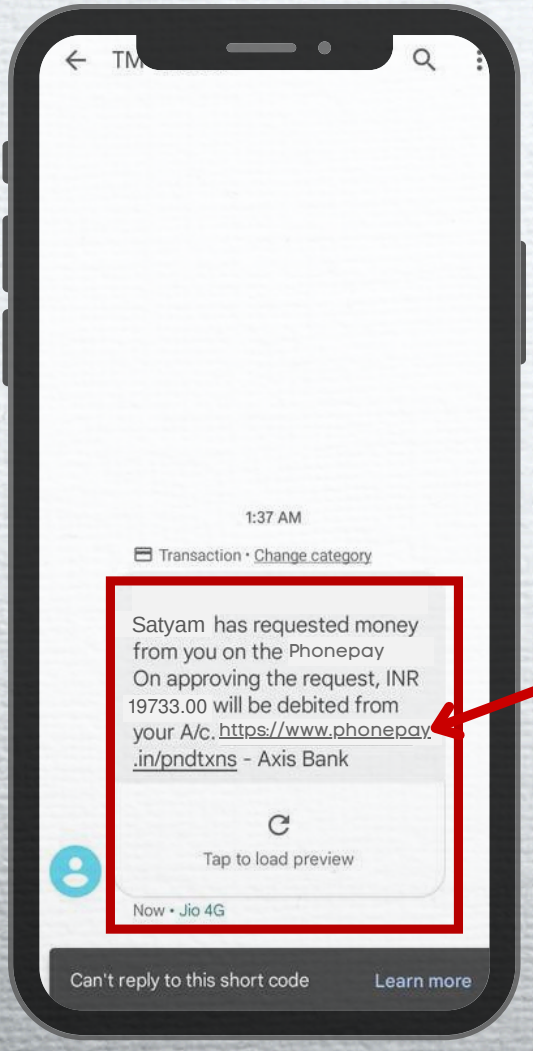
Step 2- अब आप TAFCOP की होम पेज पर है, नीचे स्क्रॉल करे और mobile number दर्ज करें।

Step 3- यहां मोबाईल नम्बर कैप्चा कोड व ओटीपी भरने के बाद लॉगिन पर क्लिक करें।

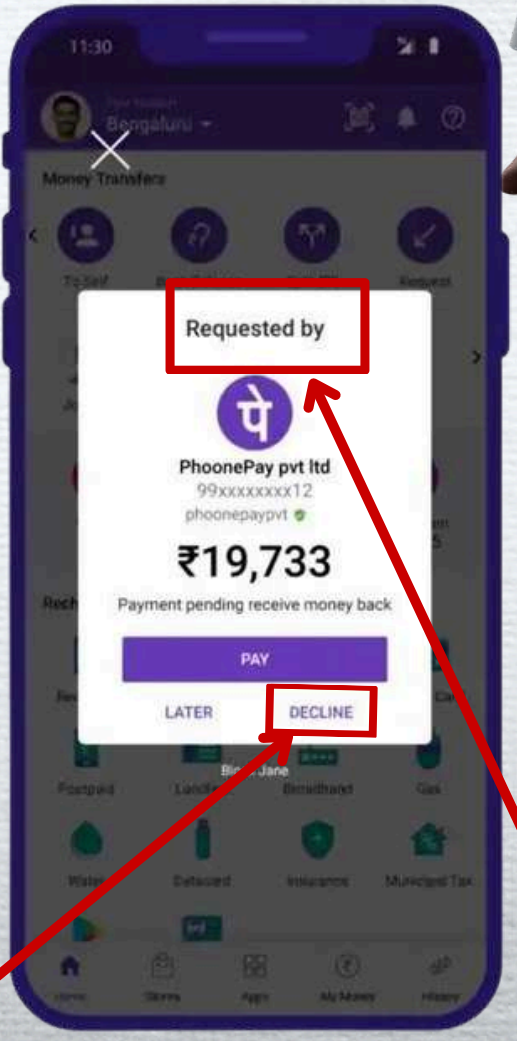
Step 4- अब आपके सामने आपके नाम से जारी सभी मोबाइल नंबरों की सूची दिखाई देगी। यदि इनमें से कोई नंबर आपके उपयोग में नहीं है, तो उस पर टिक करें और "Not My Number" पर क्लिक करके रिपोर्ट करें। इससे टेलीकॉम ऑपरेटर को सूचित किया जाएगा कि यह नंबर आपके नाम पर गलत तरीके से जारी किया गया है, और आगे की कार्रवाई की जाएगी।

साइबर सुरक्षा टिप्स

अगर कोई पैसे प्राप्त करने के लिए आपको लिंक भेजता है, तो उस पर कभी भी क्लिक न करें। ध्यान रखें कि पैसे प्राप्त करने के लिए कभी भी UPI PIN की आवश्यकता नहीं होती है। यह एक सामान्य धोखाधड़ी का तरीका है, जहां साइबर अपराधी लिंक पर क्लिक करवाकर आपकी संवेदनशील जानकारी चुरा सकते हैं।



इस तरह के लिंक को भूलकर भी क्लिक ना करें



इस प्रकार के मैसेज दिखने पर तुरंत Decline button पर क्लिक करें।

Requested By का अर्थ आपसे किसी व्यक्ति ने पैसे लेने की मांग की है जिसमे आपके अकाउंट से पैसे कटेंगे

फ्रॉड होने की स्थिति में क्या करें ?

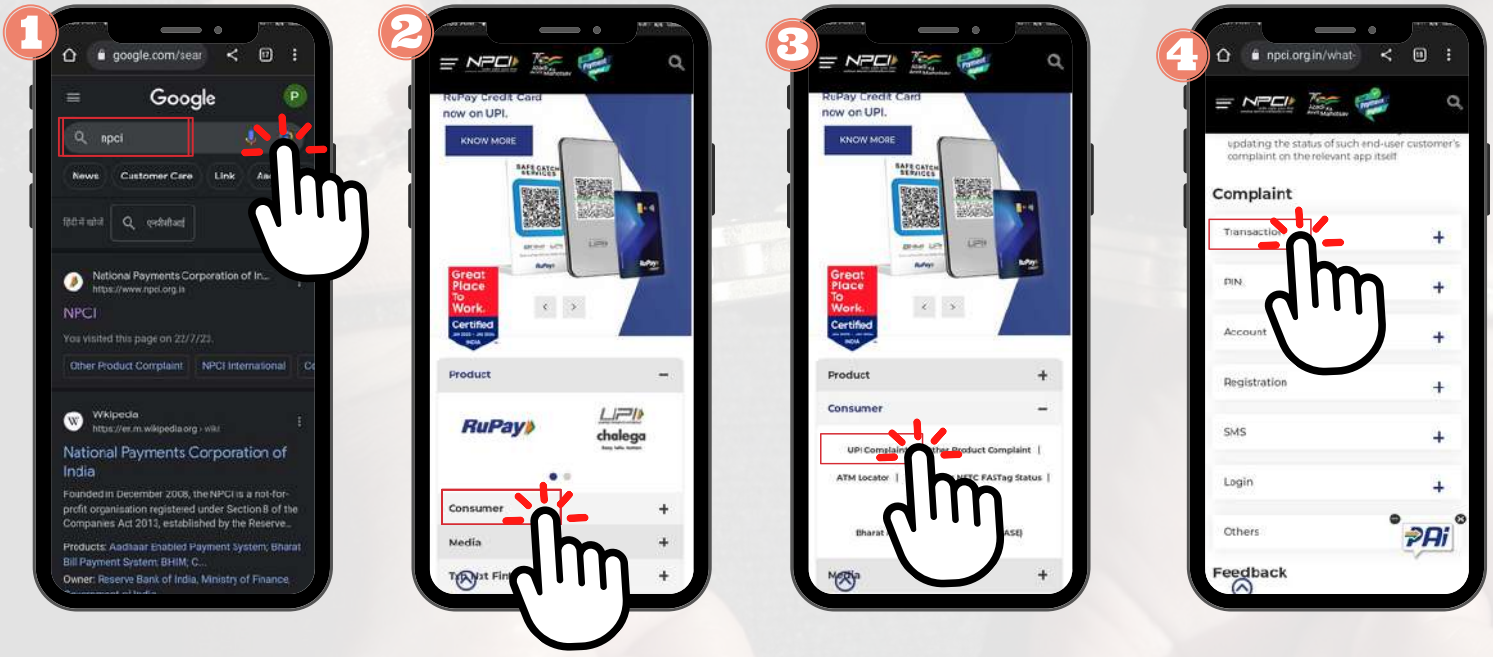
यदि आप इस तरह के फ्रॉड के शिकार हो जाते है तो तुरंत ही आप सभी chat, भेजे गए डॉक्यूमेंट, और भेजे गए पैसों के स्क्रीन शॉट के साथ www.cybercrime.gov.in or 1930 पर संपर्क कर अपनी शिकायत दर्ज करें । ऑनलाइन शिकायत करने के बाद हमे पुलिस स्टेशन जाकर दुबारा शिकायत दर्ज करवाने की जरूरत नहीं होती हैं।

शिकायत दर्ज करने के लिए यहाँ क्लिक करें और आगे के चरण का अनुसरण कर अपनी शिकायत दर्ज करें ।

ध्यान रखें - किसी भी तरह का ऑनलाइन फ्रॉड होने पर हमे डरे बिना ऑनलाइन शिकायत जरूर दर्ज करवानी चाहिए।

फ्रॉड होने की स्थिति में क्या करें ?

यदि UPI के माध्यम से फ्रॉड हो जाए या गलती से पैसे किसी गलत UPI पर भेज दिए जाएं, तो आप निम्नलिखित चरणों का पालन कर शिकायत दर्ज कर सकते हैं:



Step 1- गूगल पर NPCI लिखकर सर्च करे, अथवा वेबसाइट www.npci.org.in पर क्लिक करें।

Step 2- अब आप NPCI की होम पेज पर है, नीचे स्क्रॉल करे और consumer पर क्लिक करें।

Step 3- अब UPI पर क्लिक करें।

Step 4- नीचे स्क्रॉल करे और complaint के अंतर्गत Transaction वाले ऑप्शन पर क्लिक करें ।

Step 5- अपने समस्या के अनुसार विवरण भरे । और सबमिट बटन पर क्लिक करें।

*** शिकायत विलम्ब से होने की स्थिति में पैसा वापस मिलना मुश्किल हो सकता है।**

फ्रॉड होने की स्थिति में क्या करें ?

आप अपने शहर के **नजदीकी साइबर सेल** में भी अपनी शिकायत दर्ज कर सकते है ताकि आपको जल्द से जल्द समाधान मिल सके।

उत्तर प्रदेश पुलिस के साइबर थानों के मोबाइल नम्बर एवं ईमेल

CLICK HERE

Delhi District Cyber Cells CLICK HERE

नि:शुल्क ऑनलाइन साइबर प्रशिक्षण

आजकल साइबर अपराध तेजी से बढ़ रहे हैं, जिन्हें रोकने के लिए हमने आपके लिए एक **फ्री साइबर प्रशिक्षण महा-अभियान** शुरू किया है। इस अभियान के माध्यम से, आप विभिन्न साइबर अपराधों से बचने के तरीके सीख सकते हैं। यह प्रशिक्षण आपको न केवल सतर्क रहने में मदद करेगा, बल्कि आपको इन खतरों से सुरक्षित रखने के उपाय भी बताएगा।

इस प्रशिक्षण में स्कैम को समझाने के लिए **कहानी और छोटे-छोटे वीडियो** का भी इस्तेमाल किया गया है, इसे **इंग्लिश और हिंदी दोनों भाषा** में तैयार किया गया, लगभग 30 मिनट्स का समय इसे पूरा करने में लगता है, और अंत में एक प्रमाण पत्र स्कोर कार्ड का साथ दिया जाता है।

इस प्रशिक्षण को एक बार जरूर करें।

- **हिंदी में साइबर प्रशिक्षण**- https://forms.gle/AJajaozGwTjLPExC7
- **Cyber Training in English**- https://forms.gle/8LyAQPWPucn8LHir8

संस्थापक के बारे में

DR GAURAV KUMAR

(Founder and Director of CollCom, Asst Prof at Bennett University, Greater Noida)

डॉ गौरव वर्तमान में बेनेट विश्वविद्यालय (टाइम्स ग्रुप), ग्रेटर नॉएडा, उत्तर प्रदेश में कंप्यूटर इंजीनियरिंग विभाग में सहायक प्रोफेसर के पद पर कार्यरत हैं । वह एक सामाजिक उद्यमी और CollCom (कॉलेज कम्युनिटी सोशल वेंचर) के संस्थापक और राष्ट्रीय सेवा योजना बेनेट विश्वविद्यालय के कार्यक्रम अधिकारी भी है। डॉ कुमार हमारे देश के प्रतिष्ठित संस्थानों में से एक जवाहरलाल नेहरू विश्वविद्यालय, नई दिल्ली से कंप्यूटर विज्ञान में एम.टेक और पीएचडी पूरी की है। अपनी शिक्षा के दौरान, वह सामाजिक गतिविधियों में काफी सक्रिय थे जैसे स्लम बस्ती में बच्चों को पढ़ाना, Waste मैनेजमेंट, वृक्षारोपण अभियान, रक्त दान, स्वास्थ्य, योग और फिटनेस के लिए सभी को जागरूक करना जैसे विषय पर काफी काम किया है ।

उनके इस अथक प्रयास के लिए उन्हें विश्वविद्यालय से स्वर्ण पदक पुरस्कार और मानव संसाधन विकास मंत्रालय, भारत सरकार से सर्वश्रेष्ठ स्वयंसेवी (बेस्ट वालंटियर अवार्ड) का पुरस्कार से भी सम्मानित किया गया है। कोविड के समय में डॉ कुमार शांत नहीं बैठे । उन्होंने प्लाज्मा और ऑक्सीजन सपोर्ट के लिए लोगों की मदद करने का काम शुरू किया। उन्होंने देखा की हर व्यक्ति, बच्चे से लेकर बूढ़े तक, सभी लोग अपने दैनिक कार्य करने के लिए इंटरनेट पर निर्भर होते जा रहे है। जल्द ही, उन्हें इंटरनेट की दुनिया में तेजी से बढ़ रहे साइबर अपराध के बारे में जागरूकता की कमी के महत्व का एहसास हुआ। उन्होंने साइबर अपराध जागरूकता पर एक मेगा अभियान शुरू किया। उन्होंने विभिन्न स्कूलों और कॉलेजों (ऑफ़लाइन और ऑनलाइन) का दौरा करना शुरू किया और साइबर अपराध जागरूकता पर 35 से अधिक कार्यशालाएँ की । उन्होंने एक छोटा और बहुत ही अभिनव ऑनलाइन सेल्फ गाइड साइबर क्राइम अवेयरनेस ट्रेनिंग मॉड्यूल विकसित किया, जिसमें अभी तक **75,000** से अधिक लोगों ने भाग लिया और लाभान्वित हुए ।

उनका लक्ष्य अगले दो वर्षों में हमारे देश के 10 लाख लोगों को इंटरनेट की दुनिया में सशक्त बनाना है।

सलाहकार सदस्य

Dr Anil Kumar Singh
(Asst. Professor, Jawaharlal Nehru University)

Shri Anshumali Sharma
(Ex-State Liaison Officer (SLO) NSS, Uttar Pradesh)

Dr. Sanjeev Sharma
(Associate Professor, JNU, New Delhi)

Shri Gautam Kumar
(Executive Engineer, WRD, Govt of Bihar)

Shri Amrish Kumar Niranjan
(Youth Assistant, NSS, Delhi)

Shri Sintoo Kumar
(TGT Teacher, Govt of Delhi)

Shri OP Mishra
(Entrepreneur and Director of Jetex Infotech)

Shri Ranjan Kumar
(Senior Product Manager, Microsoft)

कार्यकारी सदस्य

Dr Gaurav Kumar
(Asst Prof, Bennett University, Founder CollCom)

Mr Priteesh Kumar
(Asst. Director-Collaboration, CollCom)

Shri Satya Mishra
(Asst. Director-Marketing, CollCom)

Mr Pritesh Mishra
(National Coordinator, CollCom)

Mr Sumit Kumar
(State Coordinator, CollCom)

Ms Shweta Kumari
(Social Media Head, CollCom)

संपादक के संदेश..

MR. PRITESH MISHRA

(National Coordinator, CollCom)

किसी व्यक्ति के साथ फ्रॉड होने का अर्थ ये कदापि नहीं है की वो शिक्षित नहीं है, केवल सीधा सा अर्थ है वो उस बात से अनभिज्ञ/जागरूक नही था । अतः फ्रॉड होने के स्थिति में आप सबसे पहले ज़रा भी न घबराए, परिवार वाले डाटेंगे या मित्र क्या कहेंगे ? ये कदापि न सोचे या कोई भी गलत फैसला न ले, समय रहते यदि आप शिकायत दर्ज करवा देते है तो आपके पैसे मिलने के अवसर बढ़ जाते है ।

अब तो RBI के दिशा निर्देश के अनुसार आप फ्रॉड होने के तुरंत बाद यदि अपने संबंधित बैंक में शिकायत दर्ज कराते है तो वो 90 दिन के भीतर ही आपकी समस्या सुलझाने का प्रयास करते है। परंतु आप को यहां तक पहुंचने की आवश्यकता ही क्या है, बस थोड़ी सी सावधानी के साथ आप अपने और अपने से संबंधित लोगों को साइबर अपराध से बचा सकते हैं ।

वर्तमान समय और भी भयावह है इस बढ़ती तकनीक में ठग आपके थोड़ी सी जानकारी से आपके पूरे जीवन को संकट में डाल सकते है, आने वाले समय में **कॉल स्पूफिंग के खतरे अधिक है** जिसमे आपको अपने संबंधी के मोबाइल में सेव नंबर से उन्ही के आवाज में कॉल आयेगा परंतु वो ठग होगा। इससे बचने के लिए हर एक चीज को सत्यापित करे बिना किसी के बात में न आए और अपनी व्यक्तिगत जानकारियों को ऑनलाइन कम से कम अपडेट करे।

समय-समय पर आपको साइबर से संबंधित जानकारी हम अपने ऑफिशियल वेबसाइट/ सोशल मीडिया/यूट्यूब वीडियो के माध्यम से साझा करते रहेगें ।

जागरूक रहें, सुरक्षित रहें !

WWW.COLLCOM.ORG

मैगज़ीन के पिछले संस्करण

May, 2024

March, 2024

FEB, 2024

JAN, 2024

Dec, 2023

NOV, 2023

Oct,2023

Sept,2023

Aug,2023

July,2023

June,2023

May,2023

April,2023

March,2023

FEB,2023

JAN,2023

DEC,2022

किसी भी मैगजीन को पढ़ने के लिए उस मैगजीन पर क्लिक करें।

पढ़ने के बाद अपना सुझाव अवश्य दें। https://g.page/r/CZmEUz-HXMe0EAI/review

collcom
Empowering Youth through Community Service

सावधान रहें, सुरक्षित रहें!

अपने मित्रों व रिश्तेदारों के साथ इस मैगज़ीन को शेयर जरूर करें ।

हमसे लगातार साइबर अपडेट्स पाने के लिए इस QR कोड को स्कैन करें और हमारे आधिकारिक चैनल/ग्रुप को सब्सक्राइब करें।

SUBSCRIBE

Cyber Sanskar
WhatsApp Channel

Telegram

Click to Check Out some interesting video on YouTube
https://www.youtube.com/@collcom

For volunteering, Type **Join** and Send it on **WhatsApp +91-9868189955**