An Initiative of CollCom

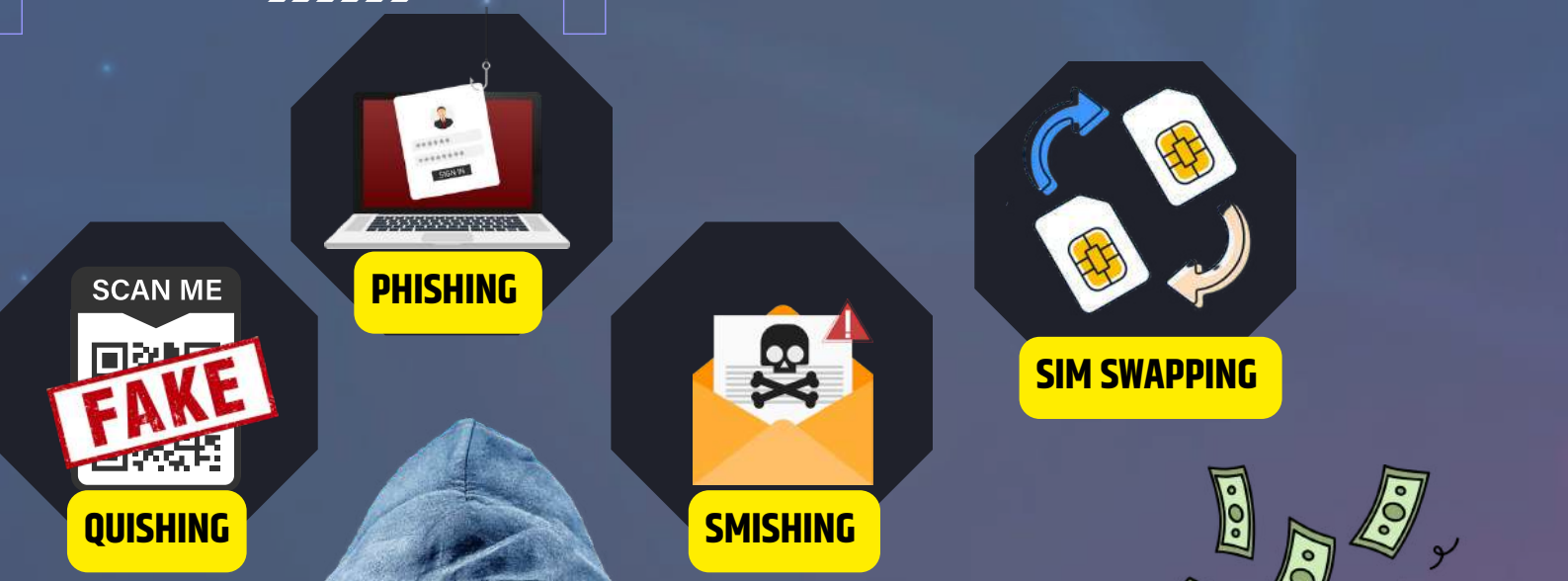
collcom
Empowering Youth through Community Service

ISSN: 2583-9969

Vol 14, Issue January 2024

# CYBER संस्कार

साइबर अपराध के खिलाफ एक कदम





प्रीतेश मिश्रा
डॉ गौरव कुमार

## UPI Fraud

# साइबर संस्कार : UPI FRAUD

**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 : जनवरी 2024

मूल्य : ₹ 49

मुद्रक : कॉलकम, इंडिया

ISSN : 2583-9969

# विषय-सूची

# UPI FRAUD

## Contents

Empowering Youth through Community Service

Page No.

SPECIAL REPORT

# 'UPI के जरिए' ठगी का अंबार!


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

INDIA TODAY — Magazine | Live TV | Search

Home / Technology / News / More than 95,000 UPI fraud cases reported in 2022, here is how you can stay safe

## More than 95,000 UPI fraud cases reported in 2022, here is how you can stay safe

The Indian government has revealed that there were 84,000 cases of UPI fraud reported in 2021-22, and in 2020-21, 77,000. The figures were revealed amid the rising cases of online cases and UPI-related fraud across the country.

THE TIMES OF INDIA

## Out on bail 3 months ago, computer engineer dupes 4 businessmen of Rs 2 lakh

Asseem Shaikh / TNN / Updated: Nov 29, 2023, 14:04 IST

THIS STORY IS FROM JULY 10, 2023

## Man duped of ₹2 lakh through UPI in online fraud

TNN / JUL 10, 2023, 08:34 IST

THE TIMES OF INDIA — OPEN APP

NEWS | VIDEOS | CITY | INDIA | BUSINESS

TRENDING | Ayodhya Ram Mandir Consecration

**News**

Kerala | India | World | Columns | Money | More+

## Kochi woman loses Rs 77,000 in online fraud, timely act of police helps to retrieve money

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

INDIA TODAY — Magazine | Live TV | Search

Home / Technology / News / Delhi-based journalist loses Rs 40,000 in UPI scam, says caller hypnotised him

## Delhi-based journalist loses Rs 40,000 in UPI scam, says caller hypnotised him

A freelance journalist based in Delhi, Ramesh Kumar Raja, was recently duped out of Rs 40,000 by a stranger over the phone.

## Businessman Dupes Hotel In UPI Fraud

CITY | TNN | Oct 30, 2023, 08:43 IST

DH — Home | Budget 2024 | India | Karnataka | Opinion | World | Business | Sports

Home › India ›

## Govt in talks to impose 4-hour delay for first UPI transfer over Rs 2,000 to curb digital payment fraud: Report

As per the RBI Annual Report 2022-23, banks experienced the highest number of fraudulent transactions in the digital payment category in the fiscal year 2022–2023.

What's Brewing

Magnitude 5.1 earthquake strikes US's Oklahoma

नवभारत टाइम्स

Faridabad Cyber Fraud: सोशल मीडिया पर फर्जी ऐप में फंसी HR हेड, गंवाए 41.36 लाख रुपये, जानें कैसे हुई ठगी

होम | टेक्नोलॉजी | टेक डायरी | टिप्स एंड ट्रिक्स | सोशल नेटवर्क

SIM SWAP: तीन मिस्ड कॉल और अकाउंट से निकल गए 50 लाख रुपये, विस्तार से समझें क्या है सिम स्वैपिंग?

kh by tampering payment gateway

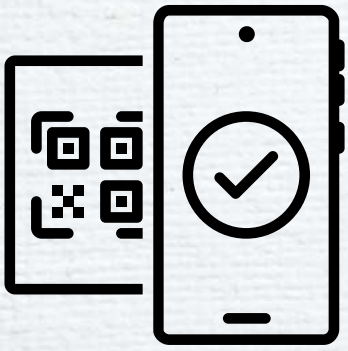
## Fraudsters dupe Gurugram company of Rs 35 lakh by tampering payment gateway

# UPI FRAUD

WARNING

## नमस्ते!

**आज हम साइबर सुरक्षा के इस कड़ी में यूपीआई (UPI) के माध्यम से हो रहे धोखाधड़ी व उससे बचने के तरीकों के बारे में जानेंगे।**



डिजिटल लेनदेन के बढ़ने के कारण भारत में यूपीआई धोखाधड़ी आम होती जा रही है। वित्त मंत्रालय के आंकड़ों के मुताबिक, वित्तीय वर्ष 2022-23 में यूपीआई धोखाधड़ी के 95,000 से अधिक मामले देखे गये हैं।

source: TOI

अतः हमे UPI Fraud से बचने के लिए उसके कुछ पहलुओं को समझना होगा जिससे हम इसके माध्यम से होने वाले सभी तरह के फ्रॉड से बच पाएं।

## UPI क्या है ?

**Unified Payments Interface**

- **यूपीआई (यूनिफाइड पेमेंट्स इंटरफेस)** एक लोकप्रिय ऑनलाइन पेमेंट सिस्टम है जो बैंकों के बीच पेमेंट्स को आसान बनाने के लिए बनाया गया है, जिसमे उपयोगकर्ता अपने मोबाइल डिवाइस का उपयोग करके **बैंक खातों** के बीच वित्तीय लेनदेन तुरंत कर सकते हैं।
- UPI ने खाताधारकों के लिए वित्तीय लेनदेन को बहुत आसान बना दिया है।
- यूपीआई के माध्यम से पैसे ट्रांसफर करने के लिए प्रत्येक उपयोगकर्ता के पास एक आईडी की आवश्यकता होती है, जिसे **यूपीआई आईडी** कहा जाता है।

SPECIAL REPORT

# यूपीआई के बारे में जानकारी

## UPI आईडी क्या है ?

**यूपीआई आईडी एक बैंक खाते के लिए एक विशिष्ट पहचान है जिसका उपयोग एक बैंक से दूसरे बैंक में धनराशि भेजने और प्राप्त करने के लिए किया जाता है।**

## UPI PIN (MPIN) क्या है ?

- **यूपीआई (UPI) पिन, UPI के माध्यम से धन हस्तांतरित करने के लिए आवश्यक 4 या 6 अंकों की व्यक्तिगत पहचान संख्या है।**
- **प्रत्येक खाताधारक के पास सुविधा के अनुसार अपना यूपीआई पिन सेट करने का विकल्प होता है।**

## UPI की विशेषताएं

- **UPI भुगतान बहुत तेज़ है और आमतौर पर भुगतान कुछ ही सेकंड में पूरा किया जा सकता है।**
- **लगभग हर बैंक मोबाइल एप्लिकेशन के माध्यम से यूपीआई लेनदेन की अनुमति देता है, भुगतान 24*7 किया जा सकता है और यह पूरी तरह से मुफ़्त है।**
- **भुगतान पूरी तरह सुरक्षित है। भुगतान पूरा करने के लिए उपयोगकर्ता को अपने मोबाइल नंबर का सिम कार्ड अपने फोन में मौजूद रखना होगा और हर बार गुप्त एमपिन (MPIN/UPI PIN) दर्ज करना होगा।**

## UPI Fraud क्या है ?

- **यूपीआई (UPI) फ्रॉड का मतलब व्यक्ति यूपीआई के माध्यम से धोखाधड़ी करके अनचाहे तरीके से पैसे निकालता है या अनजान व्यक्तियों से पैसे वसूलता है।**
- **यूपीआई ट्रांजैक्शन के दौरान धोखाधड़ी के तरीके का उपयोग करके व्यक्तिगत और वित्तीय नुकसान को यूपीआई फ्रॉड कहा जाता है।**
- **यूपीआई फ्रॉड से बचने के लिए आपको सतर्क रहने की आवश्यकता होती है और अपने पैसों की सुरक्षा के लिए सुरक्षित तरीकों का उपयोग करना चाहिए।**

# UPI Fraud के विभिन्न तरीके

यूपीआई (UPI) लेनदेन की संख्या में वृद्धि के साथ, ऑनलाइन वित्तीय हमलों, यूपीआई धोखाधड़ी शिकायतों , हैकिंग, साइबर-धोखाधड़ी और अन्य खतरों की संख्या में भी वृद्धि हुई है। आइए यूपीआइ फ्रॉड के विभिन्न तरीकों को समझते है जिससे यदि आपके साथ ऐसा कभी हो तो आप पहले ही सतर्क हो जाए।

## 1. QUISHING (QR CODE) SCAM !



**क्विशिंग घोटाले में घोटालेबाज नागरिकों के पैसे और पहचान चुराने के लिए क्यूआर कोड स्कैनिंग का उपयोग करते हैं।**

अक्सर धोखेबाज क्यूआर कोड बनाकर उसे सोशल मीडिया या ईमेल के माध्यम से शेयर करते हैं और आपको बताते हैं कि आपको उस क्यूआर कोड को स्कैन करने पर कुछ बेनिफिट मिलेगा, जब आप उस क्यूआर कोड को स्कैन करते हैं, तो आपके यूपीआई खाते से पैसे चोरी हो जाते हैं।


THE TIMES OF INDIA

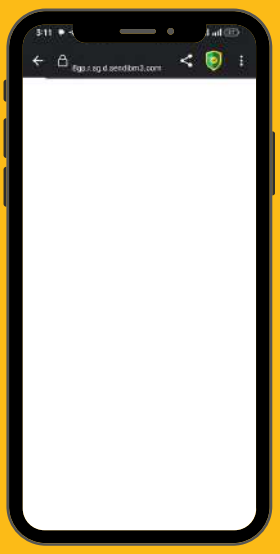
Quishing's here, look before you QR code

टाइम्स ऑफ इंडिया की रिपोर्ट के अनुसार, यूपीआई धोखाधड़ी से संबंधित शिकायतों की संख्या 2022 में 15,000 मामलों से बढ़कर 2023 में 30,000 से अधिक हो गई है। इस संख्या में से लगभग आधी शिकायतें QR कोड घोटाले से सम्बंधित हैं।

## क्विशिंग कैसे काम करता है ?


**स्कैमर आम तौर पर उपयोगकर्ता को अपने फ़ोन कैमरे का उपयोग करके एक क्यूआर कोड स्कैन करने के बाद उसमे दिए लिंक पर क्लिक करने के लिए कहता है।**

**2** **लिंक पर क्लिक करते एक (fake) वेबसाइट खुल जाता है।**



**3**

**यह वेबसाइट किसी वास्तविक ई-कॉमर्स या बैंक वेबसाइट की तरह दिखता है और आपसे आपकी व्यक्तिगत जानकारी या बैंक विवरण की मांग करता है।**


**4**

- इसके अलावा, कुछ जालासाज क्यूआर कोड सत्यापन के लिए उपयोगकर्ता से यूपीआई पिन मांगते हैं, जिसका उपयोग वो पीड़ित के बैंक खाते को खाली करने के लिए करता है।
- कुछ क्यूआर कोड में दुर्भावनापूर्ण (संदिग्ध) फ़ाइलें या मैलवेयर भी होते हैं, जो स्कैमर को आपके फ़ोन की सभी जानकारी तक पहुंच प्रदान करते हैं।

**5**

और अंत में सभी जानकारियों का प्रयोग कर वो आपसे ठगी करते है जिससे जीवन भर की कमाई एक क्षण में चली जाती है, बस बचती है तो निराशा!

**इस वीडियो को अवश्य देखें।**

https://youtu.be/n7LGy4ft8QI?si=NAPiWOwVqkx-y1ai

*Credit: NPCI*

## इस धोखाधड़ी से खुद को कैसे बचाएं ?

- अगर किसी वेबसाइट, ऐप या सोशल मीडिया द्वारा प्रदान किए गए **QR कोड के बारे में संदेह** हो, तो उसे **इग्नोर/रिपोर्ट** करें और ध्यान रहे, **संदिग्ध QR कोड को स्कैन कभी न करें**
- **सार्वजनिक (Public) Wi-Fi नेटवर्क पर QR कोड स्कैन करने से बचें**, क्योंकि ये कम सुरक्षित हो सकते हैं। ऑनलाइन लेन-देन के लिए विश्वसनीय और सुरक्षित नेटवर्क का उपयोग करें।
- याद रखे की **पैसे प्राप्त करने के लिए किसी भी पेमेंट QR कोड को स्कैन करने या UPI पिन दर्ज करने की आवश्यकता नहीं होती है**, केवल पेमेंट भेजने के लिए QR कोड स्कैन या UPI पिन का इस्तेमाल करना होता है।

# 2. PHISHING SCAM!

Phishing (फिशिंग) हैकर्स द्वारा इस्तेमाल किए जाने वाले **ऑनलाइन अटैक का सबसे आम तरीका है।** फिशिंग में हमलावर खुद को एक विश्वसनीय सोर्स की तरह पेश करता है और **एक मैलिशियस ईमेल भेजता है** जो पहली नज़र में वास्तविक सा लगता है।



और आप जब उस ईमेल में दिए **लिंक पर क्लिक करते** है तो आप एक वेबसाइट पर redirect होते है, जहां आपसे आपकी कुछ व्यक्तिगत जानकारी मांगी जाती है **जैसे की आपका नाम, DOB, CREDIT/DEBIT CARD number इत्यादि।**

**विश्वसनीय बैंक के वेबसाइट की डुप्लीकेट कॉपी**

बिना सोचे जैसे ही आप अपनी सभी निजी जानकारी साँझा करते हैं **आपके अकांउट से पैसे पल भर में खाली हो जाता है।**

## ऐसे फिशिंग ईमेल जिसे खोलने के लिए आप बाधित हो जाते हैं -

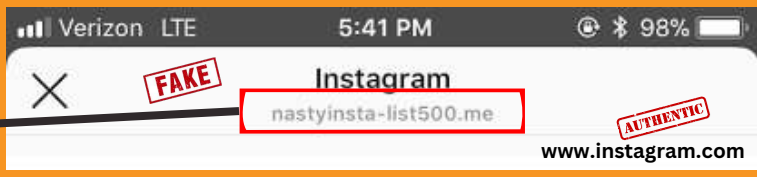
**नौकरी अवसर -** जब आप एक जॉब की तलाश में हो।

**बैंक केवाईसी/डेबिट कार्ड से संबंधित**- जब आप एक खाता धारक हो।

**शॉपिंग ऑफर** - जब आप एक आकर्षक ऑफर की तलाश में हो।

**लॉटरी/प्राइज विजेता-** जब एक विश्वसनीय कम्पनी की तरफ से हो ( ठीक उसकी कॉपी)।

सोशल मीडिया फॉलोअर बढ़ाने का दावा।


## ध्यान दे :

**कुछ फिशिंग लिंक में आपके सोशल मीडिया को लॉगिन करने का ऑप्शन होता है और जैसे ही आप उनके फेक लिंक से लॉगिन करते है आपका सोशल मीडिया अकाउंट भी हैक हो जाता है।**

**अगर इस इंस्टाग्राम पेज को ध्यान से देखे तो वेबसाइट के डोमेन से ही इसके फेक होने का पता चल जाता है, परंतु अगर आपने ये ध्यान नहीं दिया तो अपना इंस्टग्राम लॉगिन और पासवर्ड इंटर करते ही आपका अकाउंट हैक हो जाता है।**

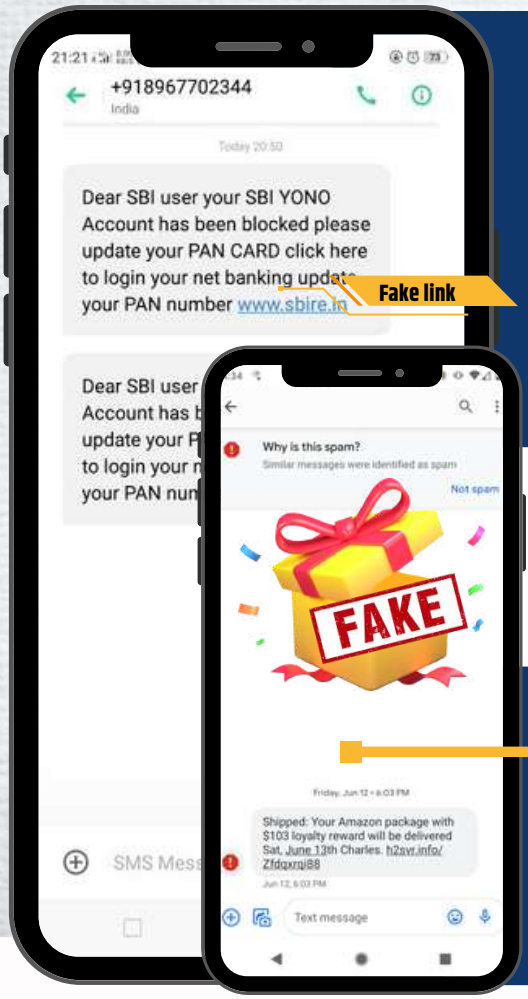
**इस फ्रॉड को और बेहतर समझने के लिए निचे दिए गए मैगजीन के पोस्टर पर क्लिक करें ।**


## Saftey tips!

- ईमेल के माध्यम से व्यक्तिगत जानकारी मांगने वाले संदेशों का जवाब न दें।
- क्लिक करने से पहले लिंक की जांच करें - सुनिश्चित करें कि लिंक https:// से शुरू हों न कि http:// से।
- अपने सभी ऑनलाइन खातों पर दो-कारक प्रमाणीकरण सक्षम करें।

# 3. SMISHING SCAM !

स्मीशिंग भी फिशिंग के ही समान है अंतर केवल इतना है की फिशिंग में इमेल के जरिए ठगी की जाती है और स्मिशिंग में टेक्स्ट मैसेज के सहारे अपराध को अंजाम दिया जाता है।


इस तरह के स्कैम में आपको आधिकारिक बैंक (Example- HDFC, UNION BANK, Axis Bank, State Bank etc. ) के नाम पर संदेश आता है -

" **प्रिय खाता धारक अपने खाते में Pan card को निचे दिए लिंक से आज ही अपडेट करें अन्यथा आपका बैंक अकाउंट आज ब्लॉक हो जायेगा** ।"

**जब आप बिना जांच के उस लिंक पर क्लिक कर पूछे गए सभी विवरण को भरते है, सभी परमिशन की अनुमति देते है तो कुछ ही पल में आपका अकांउट खाली हो जाता है।**

**इस तरह के स्कैम में आपको अन्य संदेश जैसे- amazon की तरफ से उपहार, पार्ट टाइम जॉब, शॉपिंग ऑफर इत्यादि भी आते है।**

**परन्तु ध्यान रहे संदेश में दिए लिंक पर कभी भी क्लिक न करें ।**

**आइए आगे इस तरह के फ्रॉड को एक सच्ची घटना के माध्यम से समझते जो बॉलीवुड की जानी मानी एक अभिनेत्री से साथ घटित हुई।**

## कहानी 1

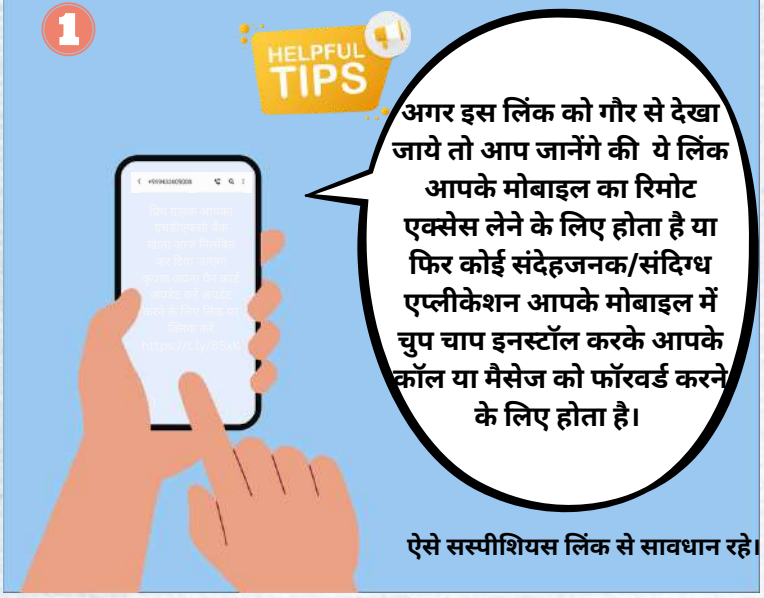
# सच्ची घटना पर आधारित

ये घटना है बॉलीवुड की जानी मानी अभिनेत्री नगमा जी की
जिनके मोबाइल पर एक दिन किसी बैंक से संदेश आता है, जिसमे लिखा होता है -

प्रिय ग्राहक आपका एचडीएफसी बैंक खाता आज निलंबित (suspend) कर दिया जाएगा कृपया अपना पैन कार्ड अपडेट करें, अपडेट करने के लिए लिंक पर क्लिक करें https://t.ly/8SxK
धन्यवाद।

नगमा जी को लगता है, वास्तव में ये बैंक से मैसेज है और वो मैसेज में दिए गए लिंक पर क्लिक कर देती है।

1




ऐसे सस्पीशियस लिंक से सावधान रहे।


लिंक पर क्लिक करते ही थोड़ी देर बाद उन्हे एक कॉल (स्कैमर) आता है।

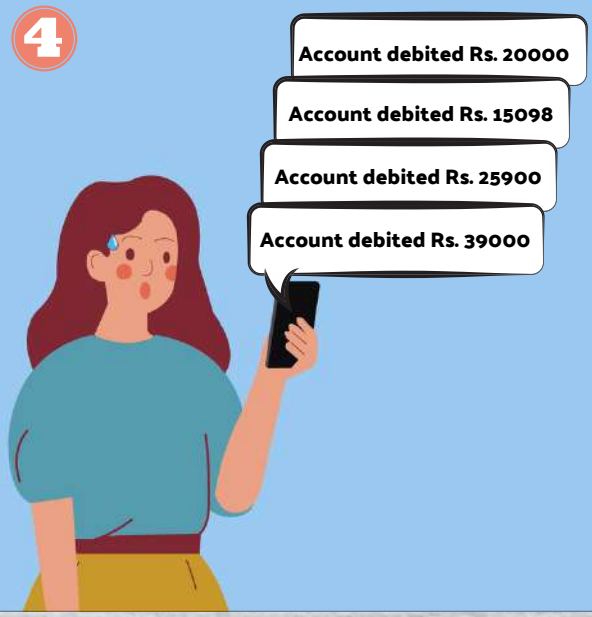
2


थोड़ी देर में स्कैमर बेनिफिशियरी अकाउंट बनाकर उनके अकाउंट से लगभग एक लाख रुपये दूसरे बैंक में ट्रांसफर कर देता है।

3


जब तक नगमा जी कुछ समझ पाती उनके अकाउंट से 99,998 रुपये कट चुके होते हैं।

4



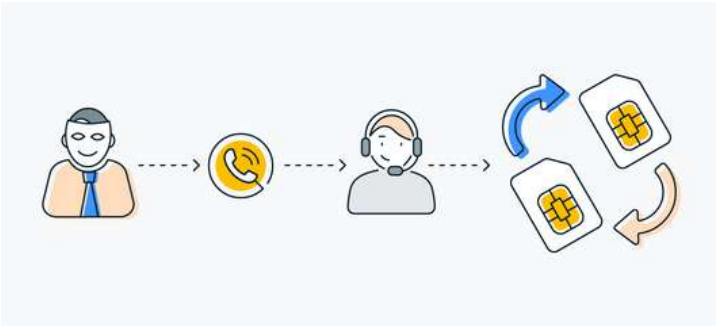

- इस तरह की जरा सी लापरवाही/जागरूकता के अभाव में नगमा जी के हजारों रुपए पल भर में साइबर धोखेबाजों ने उड़ा दिए, हम सभी को प्रतिपल सतर्क रहने की जरूरत है।
- सरकार और बैंको द्वारा जारी की गए के दिशा निर्देशों का ध्यान से पालन करे और हमारे द्वारा बताये गए साइबर सुरक्षा के उपायों को भी समझ कर भी साइबर अपराध होने से बचा जा सकता है।

# 4. SIM SWAPPING (SIM JACKING )

Image Credit: Avast

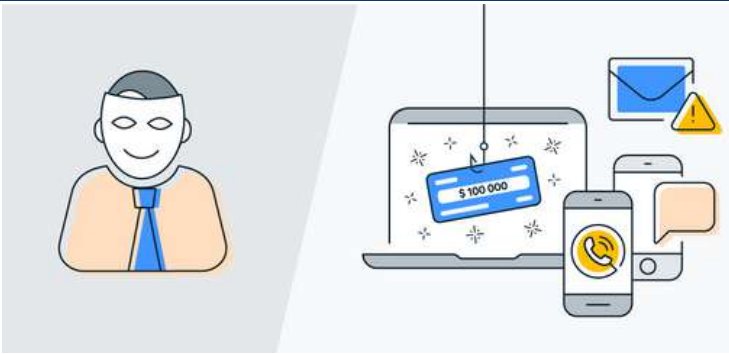
## इसे "सिम जैकिंग" या "सिम कार्ड हैकिंग" के रूप में भी जाना जाता है।

- सिम स्वैप का सीधा मतलब सिम कार्ड को बदल देना यानी उसी नंबर से दूसरा सिम निकलवा लेना है।
- सिम स्वैपिंग में आपके मोबाइल नंबर से एक नए सिम का रजिस्ट्रेशन किया जाता है। इसके बाद आपका सिम कार्ड बंद हो जाता है और आपके मोबाइल से नेटवर्क गायब हो जाता है।

सिम स्वैपिंग के लिए अलग-अलग तरह के मीडिया, सोशल मीडिया के जरिए पहले तो आप पर नजर रखी जाती है और कई बार आपको किसी अनजान नंबर से कॉल आता है जिसका उद्देश्य आपकी जानकारियों प्राप्त करना होता है।

और उन्ही जानकारियों के मदद से ठग आपके मोबाइल नंबर से नया सिम चालू करने में कामयाब हो जाते है जिसका फायदा उठाकर वह आपके नंबर पर ओटीपी मंगाता है और विभिन्न UPI ऐप के माध्यम से आपके खाते से पैसे उड़ा ले जाता है।




## इस धोखाधड़ी से खुद को कैसे बचाएं?

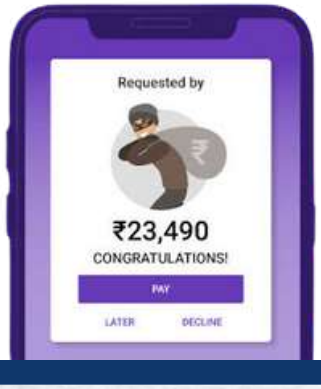
यदि आपका मोबाइल नंबर निष्क्रिय/सीमा से बाहर है, तो तुरंत अपने मोबाइल ऑपरेटर से पूछताछ करें।

अपने बैंकिंग लेनदेन के लिए नियमित एसएमएस के साथ- साथ ई-मेल अलर्ट के लिए भी पंजीकरण करें।

धोखाधड़ी की स्थिति में, अपना खाता ब्लॉक कराने और आगे की धोखाधड़ी से बचने के लिए तुरंत फोन बैंकिंग से संपर्क करें।

# 5. FAKE UPI ID REQUEST

Image Credit: Phone Pay




- इस तरह के फ्रॉड में जालसाज यूजर को पैसे देने का वादा करके यूपीआई आईडी के माध्यम से पेमेंट रिक्वेस्ट (REQUEST) भेजता है।
- ऐसे में यूजर इस तरह के रिक्वेस्ट को देखता है तो उसे लगता है कि ये पैसे लेने के लिए है, और जैसे ही यूजर रिक्वेस्ट स्वीकार कर UPI PIN दर्ज करता है, तो वह धोखाधड़ी का शिकार बन जाता है।

## इस तरह के फ्रॉड को अंजाम देने के लिए जालसाज कई हथकंडे अपनाते है -

### परिवार के किसी सदस्य से लिए पैसे वापस देने का झांसा देकर ।

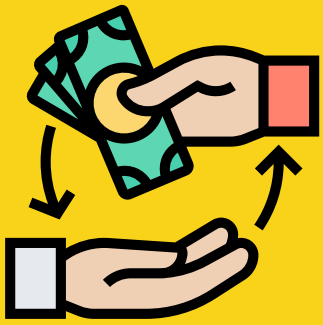
आपको अंजान नंबर से कॉल आता है और कहा जाता है आपके पिता जी/ भाई ने बोला है आपको पैसे भेज दे क्योंकि उनका UPI काम नही कर रहा।


### लॉटरी जितने के नाम पर।

कभी-कभी आपको लॉटरी जितने के नाम पर आपको पैसे देने का वादा करके रिक्वेस्ट मनी का लिंक भेजा जाता है।

### पैसे रिफंड करने के नाम पर।


कभी-कभी शॉपिंग या बिल या अन्य किसी कारण का हवाला देते हुए वो रिफंड देने की बात करते है, जैसे ही आप इच्छा जाहिर करते है आपको रिक्वेस्ट मनी का लिंक भेजा जाता है।



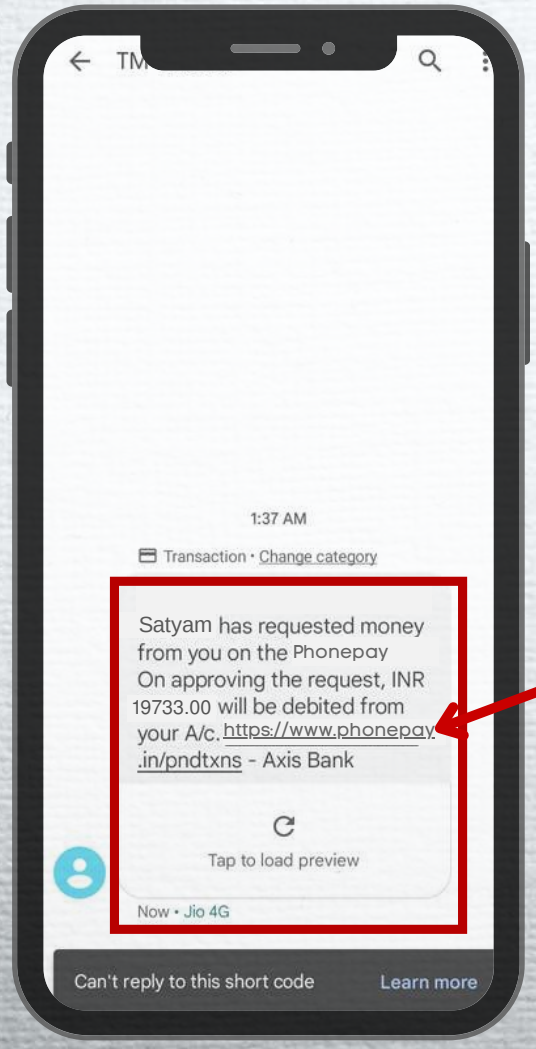
**और जैसे ही आप उस लिंक पर क्लिक करते हैं आपके अकाउंट में उतने पैसे आने के बजाय चले जाते है।**

वर्तमान में जालसाज QR CODE भेज कर भी पैसे देने का झांसा देते है।

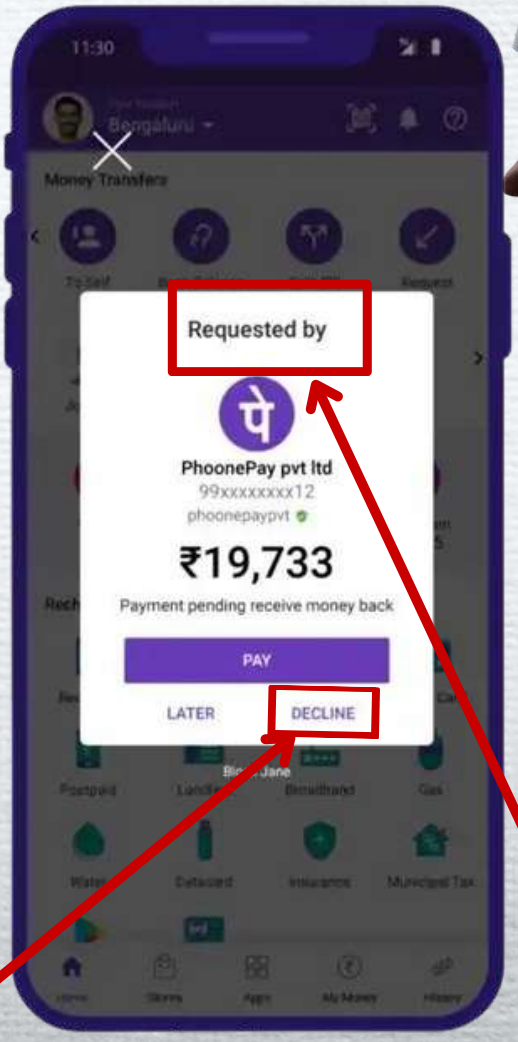

**अतः पैसे लेने के लिए किसी भी लिंक /QR CODE को स्कैन न करे।**

# साइबर सुरक्षा टिप्स

**पैसे प्राप्त करने के लिए यदि कोई लिंक भेजे तो उसपर भूलकर भी क्लिक ना करें, और ध्यान रहे कभी भी पैसे लेने के लिए आपको UPI PIN की आवश्यकता नही होती है।**


इस तरह के लिंक को भूलकर भी क्लिक ना करें



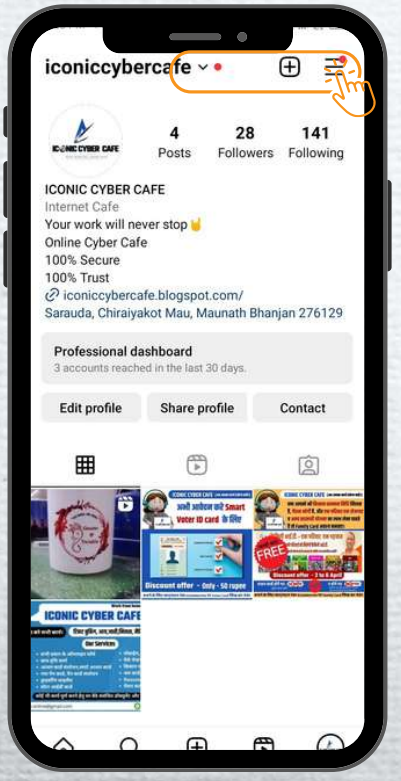

इस प्रकार के मैसेज दिखने पर तुरंत Decline button पर क्लिक करें।

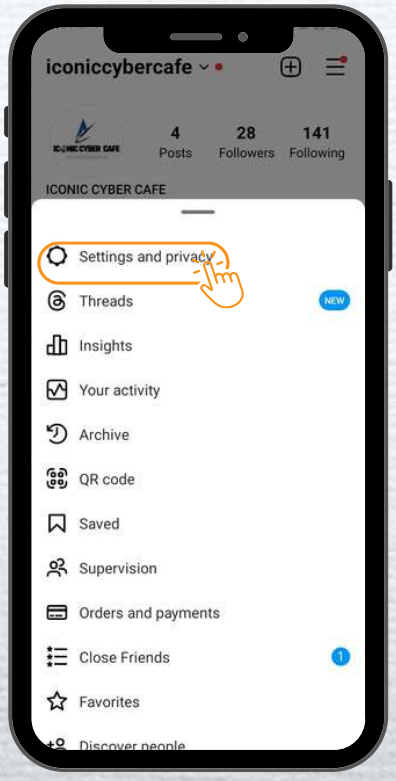
Requested By का अर्थ आपसे किसी व्यक्ति ने पैसे लेने की मांग की है जिसमे आपके अकाउंट से पैसे कटेंगे

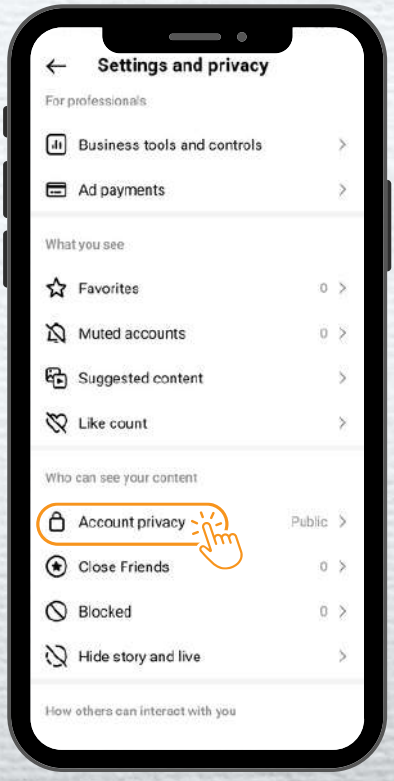
# प्राइवेसी इनेबल करना

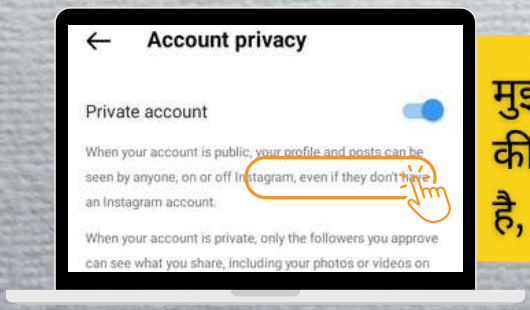
**अपने सभी सोशल मीडिया अकाउंट की प्राइवेसी को इनेबल करे जिससे दूसरा कोई व्यक्ति आपके अनुमति के बिना आपके पोस्ट को देख न पाए।**

## सोशल मीडिया अकाउंट की प्राइवेसी को इनेबल करने के लिए निम्न चरण का पालन करें-



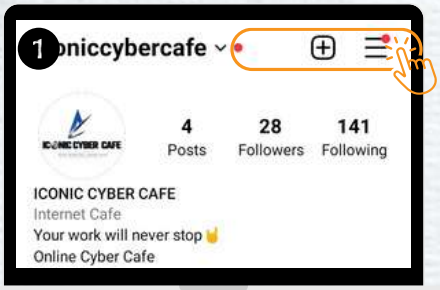



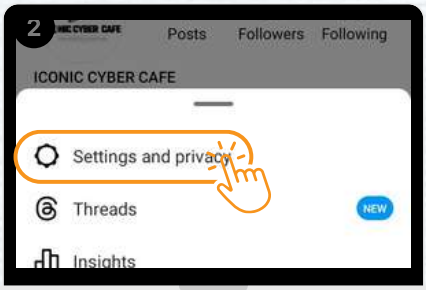

मुझे उम्मीद है अब तक बताये गए उदाहरण से आप समझ गए होंगे की आपके फोटो/वीडियो से किस हद तक छेड़खानी की जा सकती है, अत: अकाउंट की प्राइवेसी को अवश्य इनेबल (ON) करें।

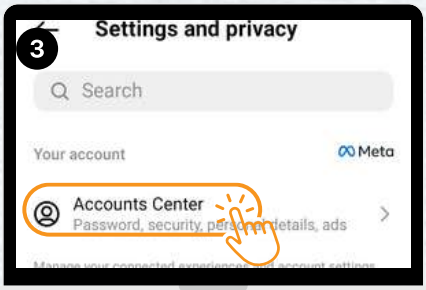
SPECIAL REPORT

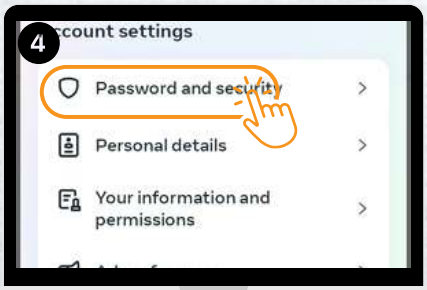
# 2FA को इनेबल करना

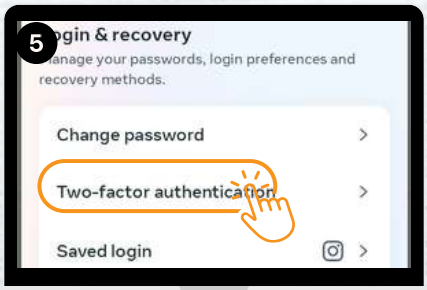
## अकाउंट हैकिंग से बचने के लिए सभी सोशल मीडिया अकाउंट पर Two-Factor Authentication (2FA) अवश्य लागू करें।

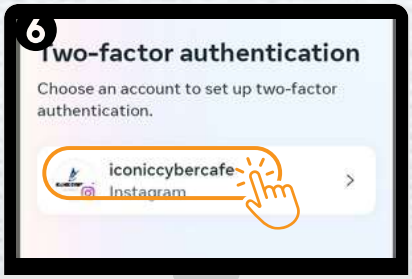


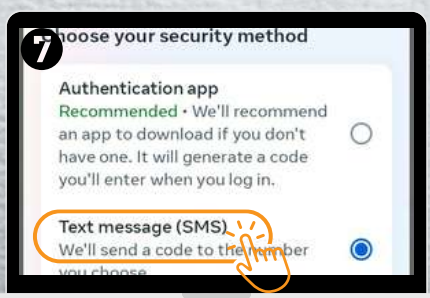



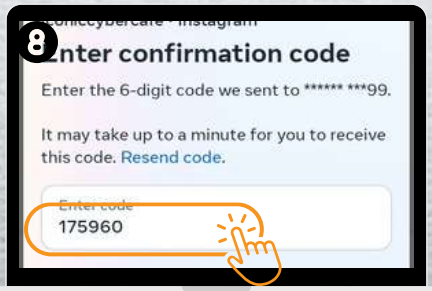



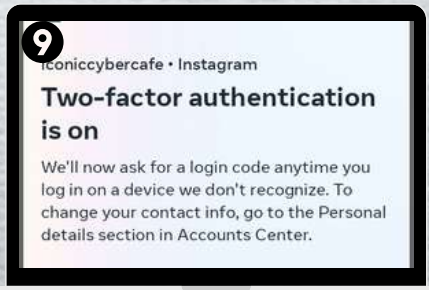




Instagram पर आप ऊपर संकेत किए गए निम्न चरणों का पालन कर 2FA ( 2 Factor Authentication) लगा सकते हैं। इसी तरह से बाकी सोशल मीडिया पर भी 2FA ON करें।

# साइबर सुरक्षा टिप्स

## किसी भी लिंक अथवा किसी व्यक्ति के कहने मात्र से कोई भी application download ना करें

Don't download these apps

ApowerMirror

AnyDesk

TeamViewer

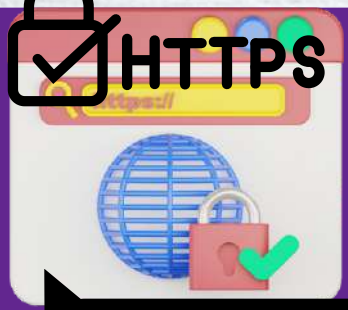
Baixar RemoDroid APK

इस तरह के एप्लीकेशन से आपके मोबाइल का पूरा ब्यौरा किसी अन्य के हाथ में चला जाता है, चाहे वो मोबाइल में रखी प्राइवेट फोटो हो या कोई व्यक्तिगत जानकारी।

किसी ऐप को डाउनलोड करने के लिए हमेशा ट्रस्टेड सोर्स- Google Play Store या Apple App Store या ऑथेंटिक वेबसाइट का ही इस्तेमाल करें।

# साइबर सुरक्षा टिप्स

## केवल विश्वसनीय वेबसाइटों से ऑनलाइन खरीदारी करें ।

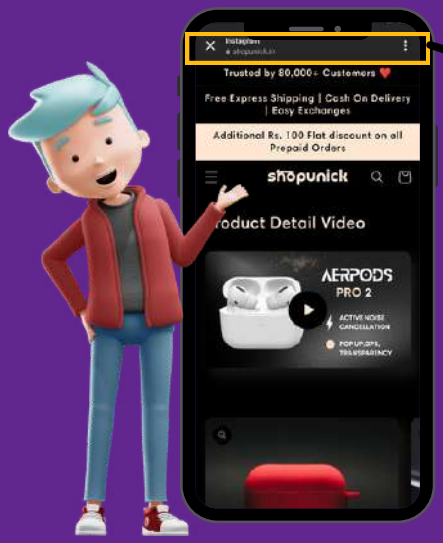




Secured Website

Unsecured Website


सुनिश्चित करें की अपना क्रेडिट/डेबिट कार्ड की जानकारी किसी भी शॉपिंग वेबसाइट या अपने कंप्यूटर/मोबाइल ब्राउज़र में खुद से सेव (save) न हो या न करें ।

## वेबसाइट की सत्यता के जांच के अन्य तरीके।




**Step 1**

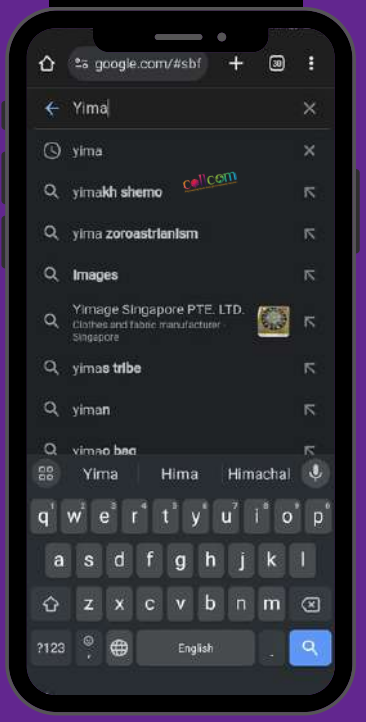
website* की लिंक three dot पर क्लिक कर शेयर बटन से कापी करें।

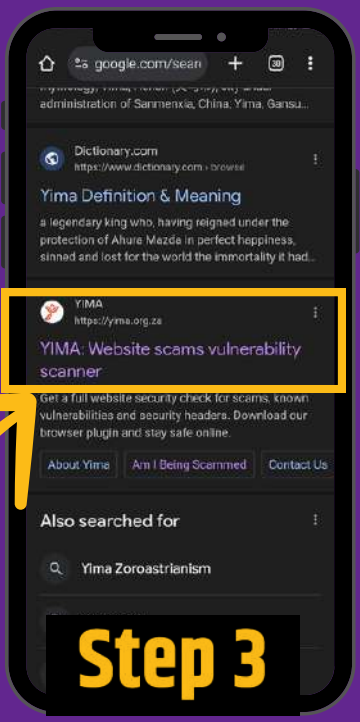
*जिस वेबसाइट की जांच करनी हो।

मान लीजिए आपको किसी भी सोशल मीडिया या गूगल पर किसी वेबसाइट द्वारा खास ऑफर की ad (sponsored) दिखाई दे रही हो, तो उस स्थिती में वेबसाइट की सत्यता की जांच के लिए निम्न चरणों का पालन करें -

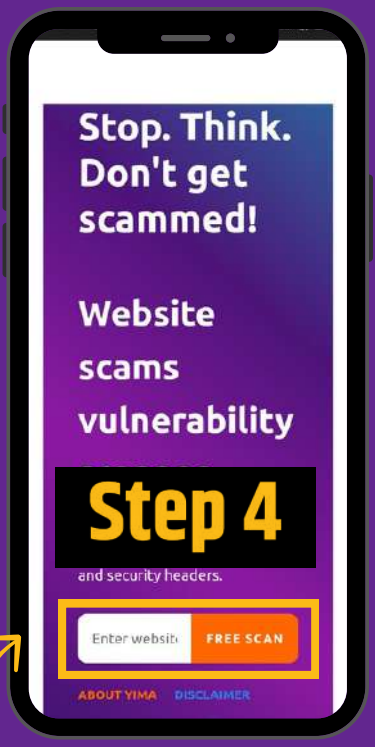
## Step 2

Google पर YIMA या www.yima.org.za सर्च करें।



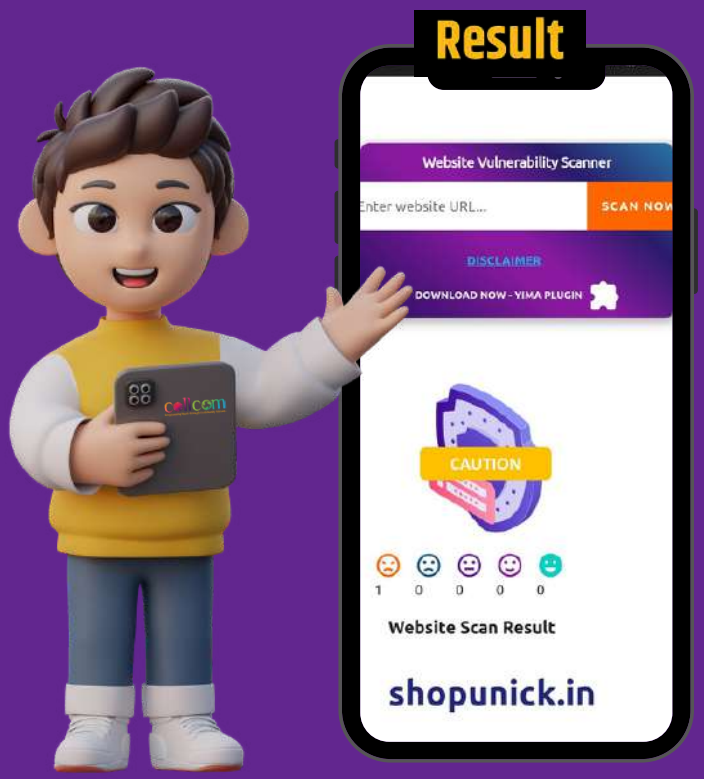




अब इस लिंक पर क्लिक करें।




यहाँ पर कॉपी किये गए लिंक को paste करें।

**परिणाम आपके सामने हैं ....**

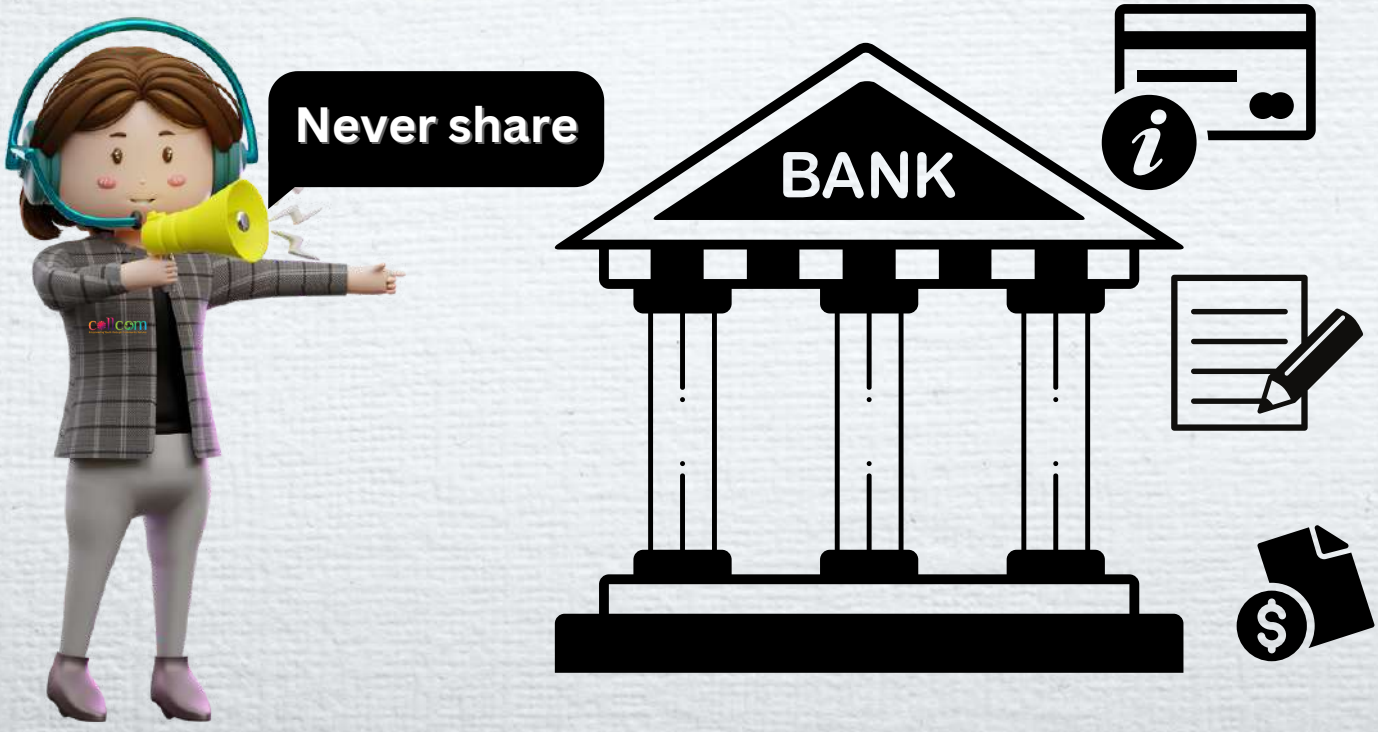



- इस वेबसाइट के माध्यम से आप किसी भी वेबसाइट की vulnerability (safe है या नही) का पता कर सकते हैं।
- अतः अगली बार किसी अज्ञात वेबसाइट पर अपनी जानकारी देने अथवा कुछ खरीदने से पहले उसकी जांच अवश्य करें।

**सतर्क रहें, सुरक्षित रहें !**

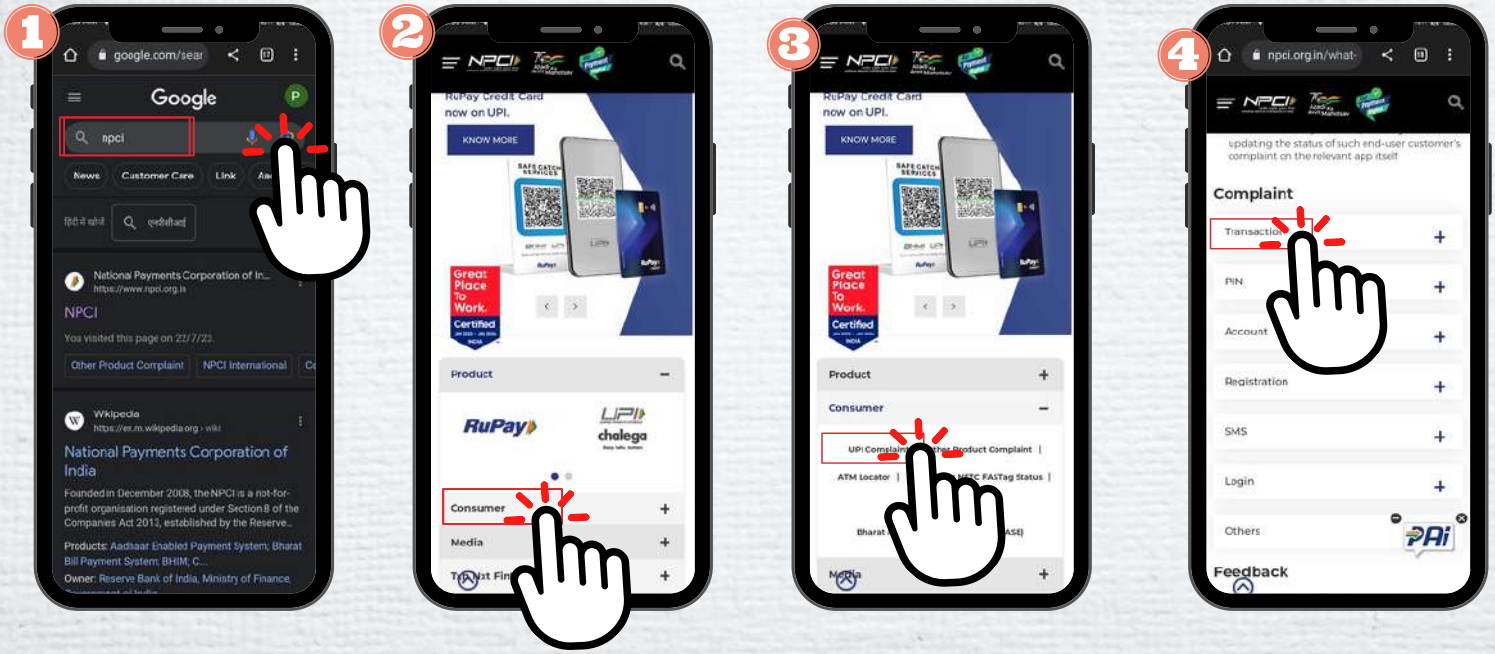
# साइबर सुरक्षा टिप्स

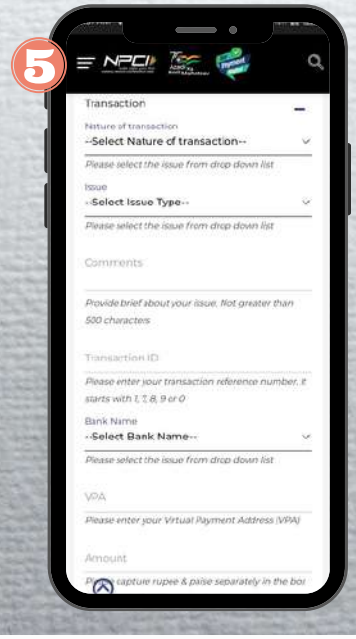
Bank details जैसे OTP, CVV, Customer ID, UPI PIN इत्यादि किसी भी व्यक्ति चाहे वो बैंक का कर्मचारी ही क्यों न हो, के साथ साझा न करें।

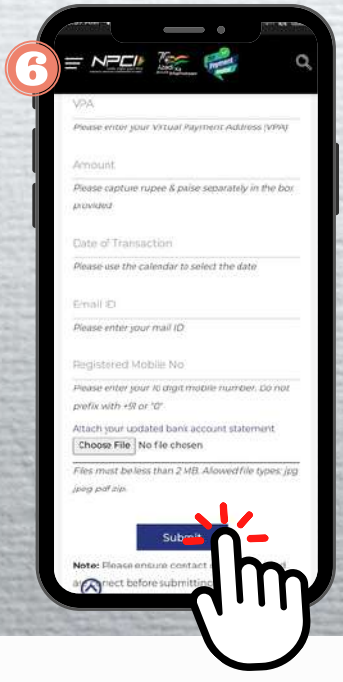




# फ्रॉड होने की स्थिति में क्या करें ?

**UPI के माध्यम से यदि फ्रॉड हो या गलती से किसी अन्य के UPI पर पैसे चले जाए तो उस स्थिति में आप विभिन्न चरणों का पालन कर अपने पैसे पुन: प्राप्त कर सकते हैं।**




**Step 1**- गूगल पर NPCI लिखकर सर्च करे, और 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 हैं 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

# 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 घर बैठे-बैठे अपनी शिकायत दर्ज करें । ऑनलाइन शिकायत दर्ज करने के लिए आपको साइबर पुलिस स्टेशन जाने की जरूरत नहीं होती है ।


शिकायत दर्ज करने के लिए यहां क्लिक करे और आगे के चरण का अनुसरण कर अपनी शिकायत दर्ज करे।

# नि:शुल्क ऑनलाइन साइबर प्रशिक्षण


- आजकल इसी प्रकार से अनेकों साइबर अपराध तेजी से प्रसारित हो रहे, जिसे देखते हुए हमने आपके लिए बिल्कुल फ्री में साइबर प्रशिक्षण महा-अभियान चलाया है जिसमे आप ऐसे साइबर अपराध से बचने के तरीको के बारे में सीख पाएंगे।

- साथ ही एक आकर्षक सर्टिफिकेट भी प्राप्त होगा।

यदि आपने अभी तक इस प्रशिक्षण में भाग नही लिया तो एक बार अवश्य ले।

- हिंदी में साइबर प्रशिक्षण- https://forms.gle/AJajaozGwTjLPExC7

- Cyber Training in English- https://forms.gle/8LyAQPWPucn8LHir8

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

WhatsApp

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**

# 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 52,000 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।

# 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 !**

# 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**
(Founder and Director, 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)

WWW.COLLCOM.ORG

# मैगज़ीन के पिछले संस्करण

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-HXMeOEAI/review