An Initiative of CollCom

Empowering Youth through Community Service

ISSN: 2583-9969

Vol 12, Issue November 2023

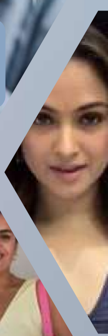
CYBER संस्कार

साइबर अपराध के खिलाफ एक कदम

A Women Loses Rs 1.4 Lakh To AI Voice Fraud

Voice cloning

Rashmika Deepfake



Kajol Deepfake

प्रीतेश मिश्रा

डॉ गौरव कुमार

AI Scams! 2023

साइबर संस्कार : AI Scams! 2023

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

© कॉलकम

प्रथम संस्करण : नवंबर 2023

मूल्य : ₹ 49

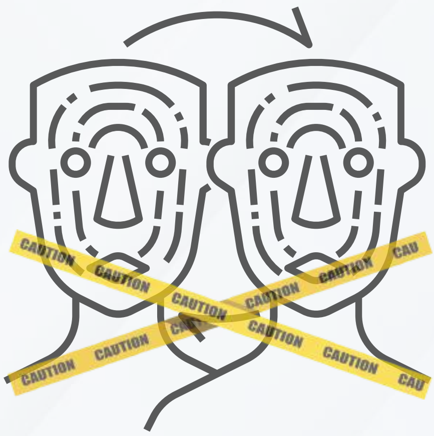
मुद्रक : कॉलकम, इंडिया

ISSN : 2583-9969

विषय-सूची

AI Scams! 2023

- परिचय
- फ्रॉड के विभिन्न तरीके
- सच्ची घटनाओं के माध्यम से फ्रॉड को समझना
- Deep Fake कैसे काम करता है ?
- बचने के उपाय और सत्यता की जांच के तरीके
  - सोशल मीडिया अकाउंट को प्राइवेट कैसे करे ?
  - अपने सोशल मीडिया अकाउंट में 2FA कैसे लागू करे ?
- फ्रॉड होने पर शिकायत कहाँ करे ?
  - अपने वायरल फोटो (प्राइवेट फोटो) कैसे हटाएं ?
- मैगजीन के पिछले संस्करण



INNOVATION • CONSUMER TECH

SPECIAL REPORT

A Voice Deepfake Was Used To Scam A CEO Out Of $243,000

Jesse Damiani Contributor

I run the Reality Studies newsletter and podcast

'AI Scam' से ठगी का अंबार!

Deepfake fraud attempts are up 3000% in 2023 — here's why

Fraudsters are capitalising on the rise of GenAI

Hindi News › Technology › Tech Diary › AI Scam Alert Scam Over Rs 5 Crore From A Man Using His

AI Fraud: आर्टिफिशियल इंटेलिजेंस की मदद से लगाया 5 करोड़ का चूना, स्कैम का अनोखा तरीका जानकर उड़ जाएंगे होश!

टेक डेस्क, अमर उजाला, नई दिल्ली Published by: विशाल मैथिल Updated Wed, 24 May 2023 06:06 PM IST

Stay ahead with India's leading business news app

Download mint App

mint Subscribe | e-paper

Kerala man loses ₹40,000 to AI-based deepfake scam

1 min read

18 Jul 2023, 08:25 PM IST

Join us

Livemint

A resident of Kozhikode in Kerala lost ₹40,000 after cybercriminals used deep fake AI technology and posed as a former colleague in a WhatsApp call and sought money for his sister-in-law's surgery

OPEN IN APP

News / Opinion / Columns / Rashmika Mandanna, deepfakes and us: I find myself constantly questioning the safety of uploading personal information and disclosing my travel location

Rashmika Mandanna, deepfakes and us: I find myself constantly questioning the safety of uploading personal information and disclosing my travel location

Do I truly know all my followers? What if my content is misused?

bt Business Today

HOME MAGAZINE BT TV MARKET TODAY TECH TODAY MONEY TODAY MUTUAL FUNDS INDUSTRY BTSHORTS

Immersives UPSTART ICC World Cup Corporate Petrol-Diesel Weather BT Bazaar

News / TECHNOLOGY / News / Phone Call Scam in India: Over 45% victims of AI fraud calls lost over Rs 50,000

Feedback

Phone Call Scam in India: Over 45% victims of AI fraud calls lost over Rs 50,000

The cost of falling for an AI voice scam can be significant, with 48 per cent of Indians who lost money saying it cost them over Rs 50,000.

News / Technology / News / He sounded exactly like my nephew: Woman loses Rs 1.4 lakh in AI voice scam

He sounded exactly like my nephew: Woman loses Rs 1.4 lakh in AI voice scam

A 59-year-old woman loses Rs 1.4 lakh in an AI voice scam where the fraudster mimick her nephew's voice. The incident is a stark reminder of the rising prevalence of advanc technology-enabled frauds.

Hindi News › टेक्नोलॉजी

Deepfake AI Scam: वॉट्सऐप पर आपका न्यूड वीडियो भेजकर कोई कर रहा ब्लैकमेल? बिना डरे यहां करें शिकायत

Cyber Crime Complaint Online: साइबर क्रिमिनल्स AI की मदद से लोगों की Deepfake न्यूड फोटो और वीडियो बनाते हैं. फिर वॉट्सऐप के जरिए उन्हें ब्लैकमेल करते हैं. ऐसा होने पर आपको तुरंत साइबर क्राइम हेल्पलाइन पर शिकायत दर्ज करानी चाहिए. आइए देखते हैं कि ये सब कैसे होता है.

iTVoice IT IN DEPTH

NOVEMBER 25, 2023 · DEEPFAKE / NEWS · 1 MIN READ

FALSE VIDEO FEATURING RATAN TATA EXPL... ONLINE FRAUD FOLLOWING RASHMIKA MANDANNA, KAJOL, KATRINA DEEPFAKE INCIDENTS

Search

AI Voice Scam: आवाज से लूट रहे हैं लाखों रुपये, यहां जानिए कैसे बच सकते हैं इस फ्रॉड से...

Deep Fake: डीप फेक का इस्तेमाल करके बुजुर्ग से लूटे 74000 रुपये, AI वीडियो में नजर आए रिटायर्ड IPS अधिकारी!

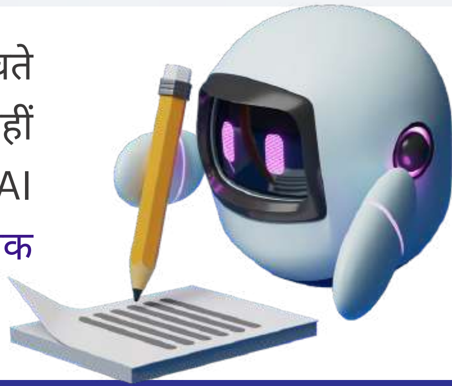
| Dec 01, 2023, 11:42 AM

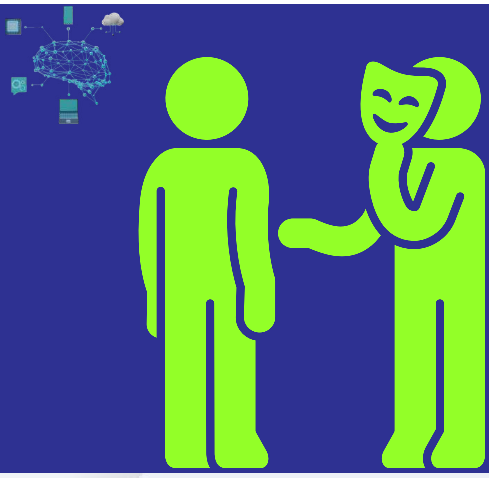
Ghaziabad: गाजियाबाद में डीप फेक का एक नया मामला सामने आया है. जहां AI के माध्यम से एक शख्स उत्तर प्रदेश के रिटायर्ड आईपीएस अधिकारी का चेहरा दिखाकर बुजुर्ग से 74 हजार रुपये लूट लिया. दरअसल एक AI के माध्यम से पहले बुजुर्ग को सेक्स स्कैंडल में फंसाने की धमकी देता है और उससे पैसे मांगना शुरू कर देता है. इसके बाद शख्स को पुलिस के द्वारा निकली कॉल करके जेल भेजने की धमकी देता है, इससे परेशान होकर बुजुर्ग पैसे देने लगता है, लेकिन लगातार पैसे की मांग ने बुजुर्ग को परेशान कर दिया और वह आत्महत्या करने की कोशिश करने लगा, ऐसे में जब इस बात की जानकारी बुजुर्ग की बेटी को हुआ तो उसने इसकी जानकारी असली पुलिस को दी और फिर मामले का हकीकत सामने आई.

SPECIAL REPORT

AI SCAM!

McAfee की एक रिपोर्ट के अनुसार, आधे से अधिक (69%) भारतीय सोचते हैं कि वे AI आवाज और वास्तविक आवाज के बीच अंतर नहीं जानते हैं या नहीं बता सकते हैं। रिपोर्ट के अनुसार, 83% भारतीय पीड़ितों ने कहा कि उन्हें AI Scam से पैसे का नुकसान हुआ है जिनमे 48% को 50,000 रुपये से अधिक का नुकसान हुआ है।





Deep Fake AI Scam क्या है ?

डीपफेक एक तरह की भ्रम पैदा करने वाली तकनीकी है जिसका इस्तेमाल ठग ऑडियो या वीडियो कॉल अथवा फोटो या वीडियो के रूप में करते है। जिसे सुनकर या देखकर आपको ये लगेगा कि आप किसी अपने से ही बात कर रहे हैं, या जिसे जानते है उन्ही का वीडियो है परंतु ऐसा होता नही है। डीपफेक तकनीक **किसी की भी आवाज को हुबहू उतारने में सक्षम है**, ऐसे में किसी के कॉल आने पर आपको लग सकता है कि ये तो मेरे अपने ने ही कॉल किया है और ऐसे समझकर जब आप उसकी मदद करते हैं, तो आपके साथ फ्रॉड हो चुका होता है।

साधारण भाषा में कहे तो deep fake तकनीकि से मात्र उस व्यक्ति की फोटो और कुछ सेकंड की आवाज से हुबहू उसके जैसे दिखने वाला व्यक्ति बना कर उससे कुछ भी कहवाया जा सकता है।

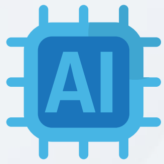
SPECIAL REPORT

DEEP FAKE AI FRAUD के विभिन्न तरीके

AI Voice cloning के माध्यम से

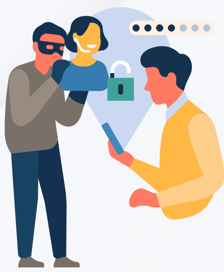
हर किसी की आवाज़ अद्वितीय होती है, जिसका अनिवार्य रूप से मतलब यह है कि यह बायोमेट्रिक फ़िंगरप्रिंट के बोलचाल के समकक्ष है। इसलिए, बोलना विश्वास स्थापित करने का एक स्वीकृत तरीका है। लेकिन 86% भारतीय वयस्कों द्वारा सप्ताह में कम से कम एक बार सोशल मीडिया के माध्यम से) अपना वॉयस डेटा ऑनलाइन या रिकॉर्ड किए गए नोट्स में साझा किया जाता है। जिसके जरिए ठग वॉयस क्लोनिंग बनाने में कामयाब है और इसी के साथ आज वॉयस क्लोनिंग साइबर अपराधियों के लिए एक शक्तिशाली उपकरण भी बन गया है। source: Times of India

इस तकनीकी से किसी व्यक्ति की आवाज को क्लोन करने के लिए केवल तीन सेकंड के ऑडियो की आवश्यकता होती है।



एक सर्वे रिपोर्ट के अनुसार AI Voice Cloning तकनीकी का प्रयोग "भारत सहित सात देशों के 7,054 लोगों के साथ किया गया था।"

इस बात से आप अंदाजा लगा सकते है की **ai voice cloning** कितना भयावह हो सकता है, आज हम जिस गति से आगे बढ़ रहे और नये तकनीक को अपना रहे उतनी ही गति से हम उसके दुष्प्रभाव और सावधानियों को नही अपनाते जिसका फायदा ठगी उठा रहे और लोगो को अपना शिकार बनाकर उनके जीवन भर की कमाई को एक झटके में साफ कर दे रहे है।



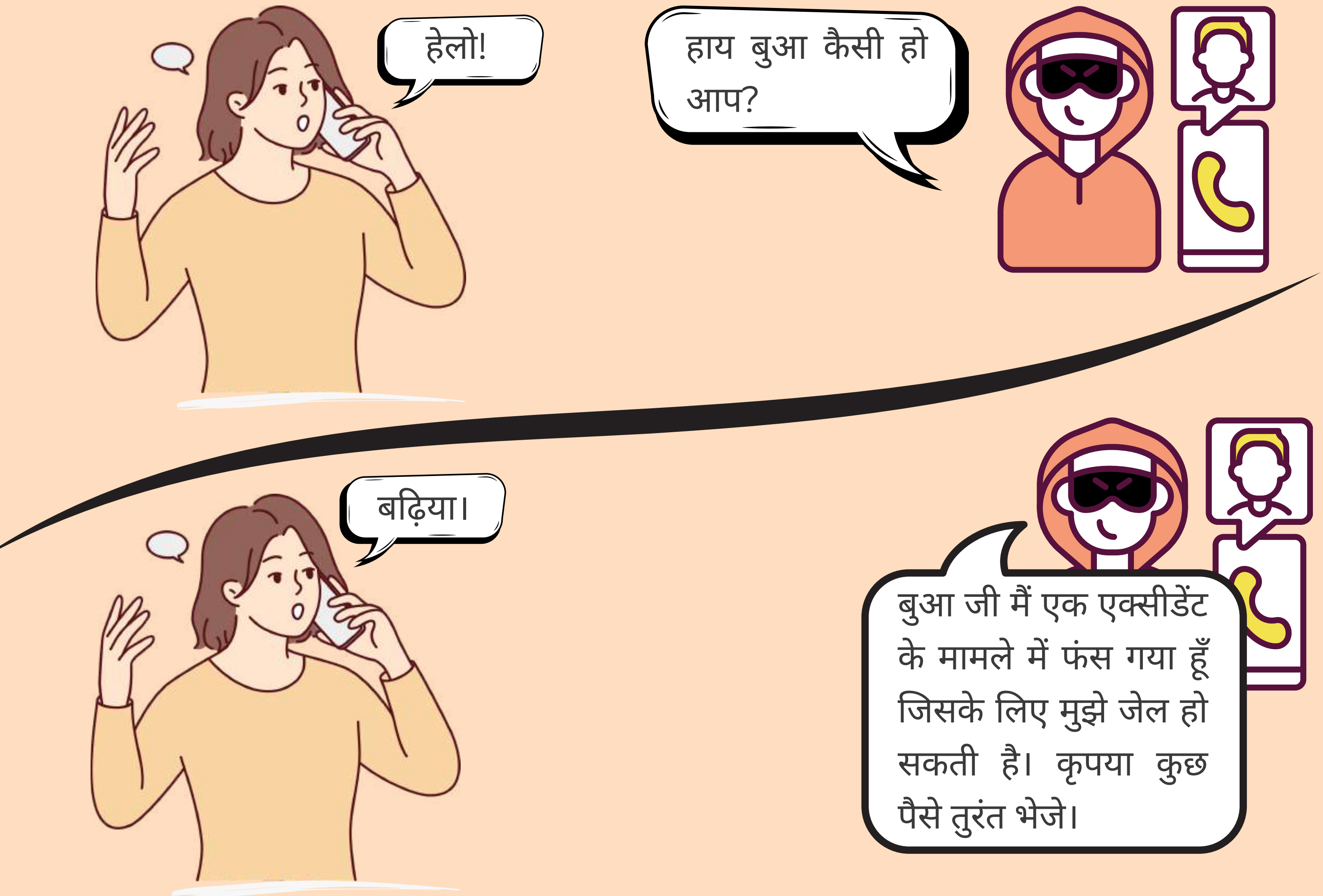
आइए अगले पृष्ठ पर इस फ्रॉड को और बेहतर तरीके से समझने के लिए एक वास्तविक घटना को देखते है।

कहानी 1 (AI Voice Cloning)

ये कहानी है एक 59 साल की महिला की जिनके साथ **1.4 लाख रुपये की ठगी** हुई, ये पैसे उन्होंने अपने भतीजे को कॉल के दौरान हुई बातचीत पर उसकी मदद के लिए भेजा, परंतु बाद में पता चला वो उनका भतीजा था ही नही।

आइए समझते है ऐसी क्या गलतियाँ हुई जिससे वो अपने भतीजे की आवाज समझ नही पाई और पैसे किसी अंजान को दे दिए।

प्रभज्योत (बदला हुआ नाम) अपने घर पर बैठी होती, उस समय काफी रात हो चुकी होती है जब उनके **फोन पर कॉल आता है**.....



प्रभज्योत थोड़ी देर सोचती है परंतु आवाज उनके भतीजे की ही लग रही थी इसलिए बिना देरी किए वो तुरंत पैसे भेजती है।

इस तरह से 2 से 3 ट्रांजेक्शन में वो 1.4 लाख रुपए भेज देती है, और बाद में पता चलता है कि उनके साथ ठगी हो गई, क्योकि जिसे वो पैसे भेजी वो उनका भतीजा था ही नहीं।

वास्तव में ये सब AI और मशीन लर्निंग की मदद से ठगो ने उनके भतीजे की आवाज की क्लोन बनाकर कॉल किया जिससे प्रभज्योत् समझ नही पाई।

अतः ध्यान रहे किसी भी अनजान नंबर से कॉल आए, चाहे वो आपका रिश्तेदार ही क्यों न बात करे सत्यता की जांच किए बिना किसी को भी पैसे न भेजे।

SPECIAL REPORT

Deep Fake Vedio के माध्यम से

डीपफेक वीडियो एक तरह की भ्रम पैदा करने वाली रिकॉर्ड की हुई वीडियो या वीडियो कॉल है, जिसे देखकर आपको ये लगेगा कि आप किसी अपने से ही बात कर रहे हैं / उनकी ही वीडियो देख रहे है।

डीपफेक किसी की भी आवाज/चेहरे की नकल को हुबहू उतारने में सक्षम है, ऐसे में किसी रिकॉर्डेड वीडियो या वीडियो कॉल आने पर आपको लग सकता है कि ये तो मेरे अपने का ही वीडियो / वीडियो कॉल है और ऐसे समझकर जब आप मदद करते हैं, तो आपके साथ फ्रॉड हो चुका होता है।

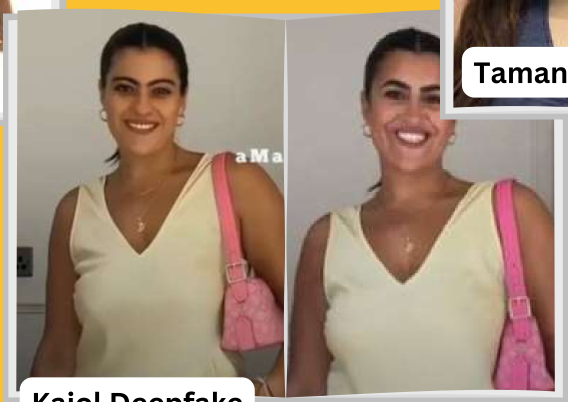
इसका उदाहरण हमने हाल ही में देखा...

Rashmika Deepfake

DEEP FAKE

Tamannaah Deepfake

रश्मिका कहती है– "ईमानदारी से कहूं तो ऐसा कुछ न केवल मेरे लिए, बल्कि हममें से हर एक के लिए बेहद डरावना है। अगर मेरे साथ ये तब हुआ होता, जब मैं स्कूल या कॉलेज में थी, तो मैं इससे निपटने का सोच भी नहीं सकती थी।"



Kajol Deepfake

अब आप अंदाजा लगा सकते है की ये कितना भयावह हो सकता है। आप पहली बार में डीप फेक वीडियो को वास्तविक ही मानेंगे क्योकि इसमें सभी हाव भाव बिलकुल वास्तविक व्यक्ति की कॉपी कर ली जाती है।

ये इतना खतरनाक है की किसी भी चरित्रवान व्यक्ति की व्यक्तित्व को सोशल मीडिया पर पल भर में खत्म कर सकता है।

Deep Fake कैसे काम करता है?

ठग **सबसे पहले आपके सोशल मीडिया की कुछ दिनों तक निगरानी करते है**, और वहाँ से आपकी अधिकतम जानकारियाँ (जैसे आपका घूमना फिरना, घर का पता, काम-काज, परिवार और रिश्तेदार जैसे महत्वपूर्ण जानकारी) प्राप्त कर लेते है।

नोट- अधिकतम जानकारी हमारे द्वारा अपलोड किये गए फोटो, स्टेटस और पोस्ट से पता चल जाती है।

इसके पश्चात **एकत्रित की गई जानकारियों से वो deepfake तकनीकि का प्रयोग करके आपके आवाज या चेहरे का क्लोन बनाते है**, और तत्पश्चात वो आपके रिश्तेदार को कॉल करके/रिकॉर्ड किया वीडियो भेजकर कुछ भी बहाना करते है और पैसे की मांग करते हैं।

यहाँ तक तो ठीक है परंतु **समस्या तब होती है जब आप बिना उस वीडियो/कॉल की जांच किए ठगी के बातों में फंस जाते है और पैसे भेज देते है।** ऐसा करते ही आप उनके शिकार बन जाते है।

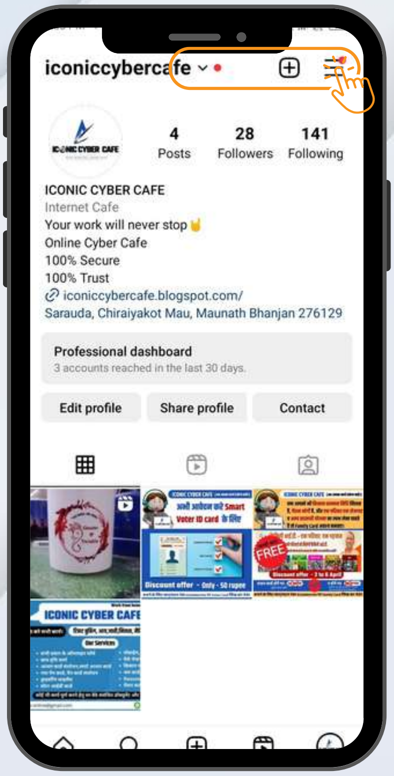
वर्तमान में Deepfake तकनीकि का उपयोग सबसे अधिक पोर्नोग्राफी कॉन्टेंट बनाने में किया जा रहा, जो बेहद ही शर्मनाक है, परंतु कुछ सावधानियां और उपाय करके हम इससे बच सकते है।

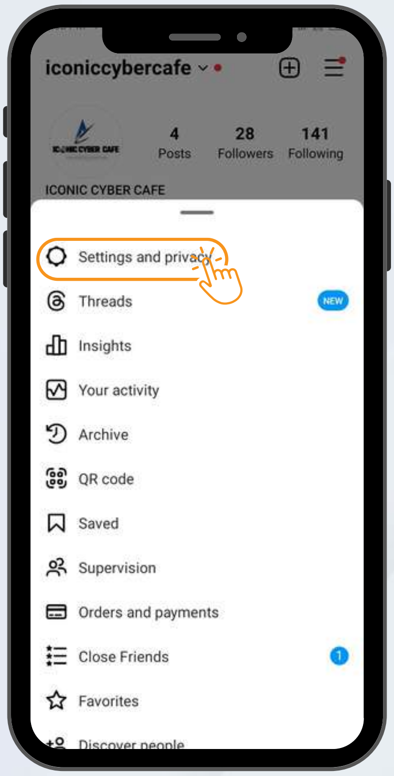
SPECIAL REPORT

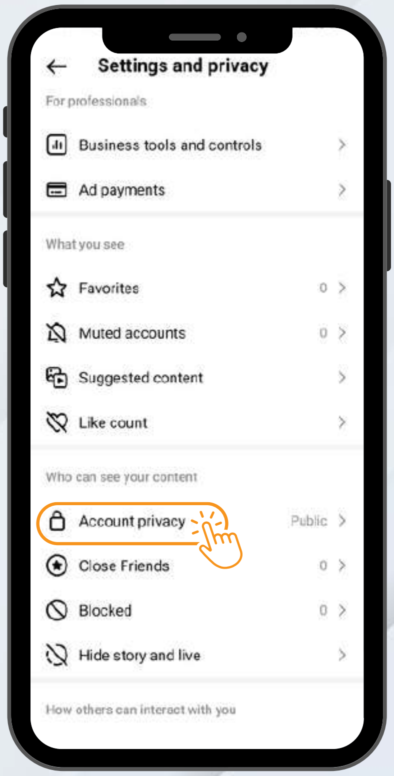
साइबर सुरक्षा टिप्स

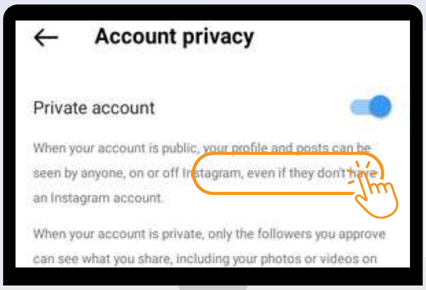
सभी सोशल मीडिया अकाउंट को प्राइवेट करे जिससे दूसरा कोई व्यक्ति आपके अनुमति के बिना आपके पोस्ट को देख न पाएं।

निचे दिखाए गए स्क्रीनशॉट्स से आप निम्न चरणों का पालन करके अपने अकाउंट को प्राइवेट कर सकते है-







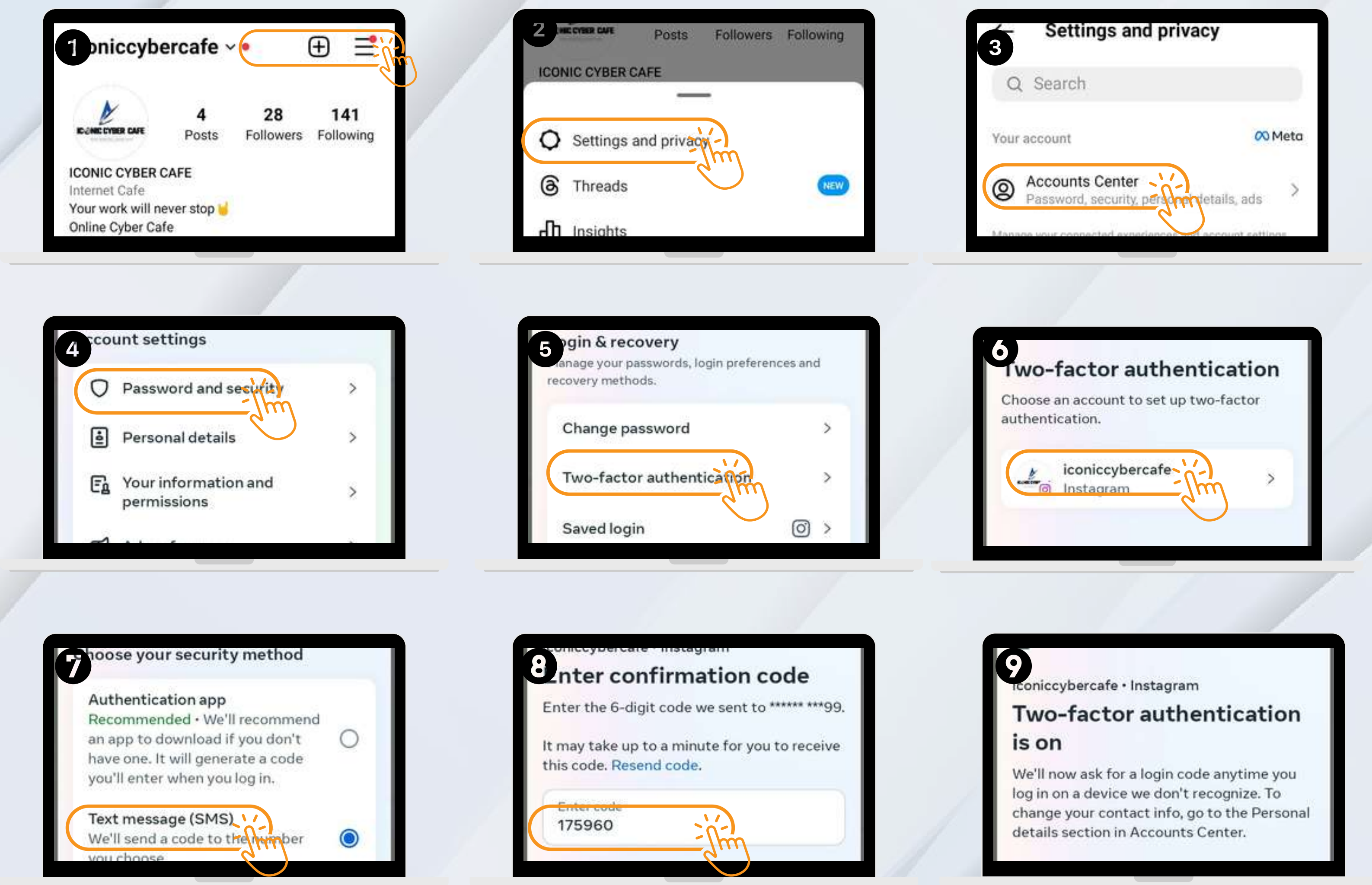


चूंकि अबतक आप समझ गए होंगे की आपके फोटो/वीडियो से किस हद तक छेड़खानी की जा सकती है, अतः अकाउंट को प्राइवेट अवश्य करें।

SPECIAL REPORT

साइबर सुरक्षा टिप्स

सभी सोशल मीडिया अकाउंट पर Two-Factor authentication (2FA) authentication (2FA) अवश्य लागू करें।



Instagram पर आप ऊपर संकेत किए गए निम्न चरणों का पालन कर 2FA लगा सकते है।

SPECIAL REPORT

साइबर सुरक्षा टिप्स

WhatsApp पर Two-factor authentication (2FA)

लागू करने के लिए विभिन्न चरणों का पालन करे:-

SPECIAL REPORT

साइबर सुरक्षा टिप्स

व्हाट्सएप पर आए अनजान इंटरनेशनल नंबर से कॉल को न उठाए।

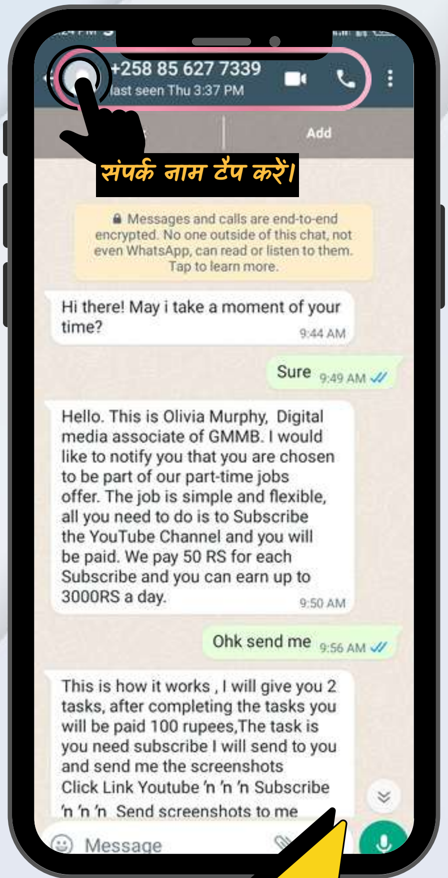
प्रतिपल सतर्क रहे, अनजान इंटरनेशनल नंबर से आए कॉल/ वीडियो कॉल कभी न उठाए अन्यथा आप ठगी के शिकार हो सकते हैं। बिल्कुल इनकी तरह।

https://zeenews.india.com/personal-finance/whatsapp-nude-video-call-scam-man-loses-rs-1-57-lakhs-but-gets-back-rs-1-39-lakh-check-how-2532720.html

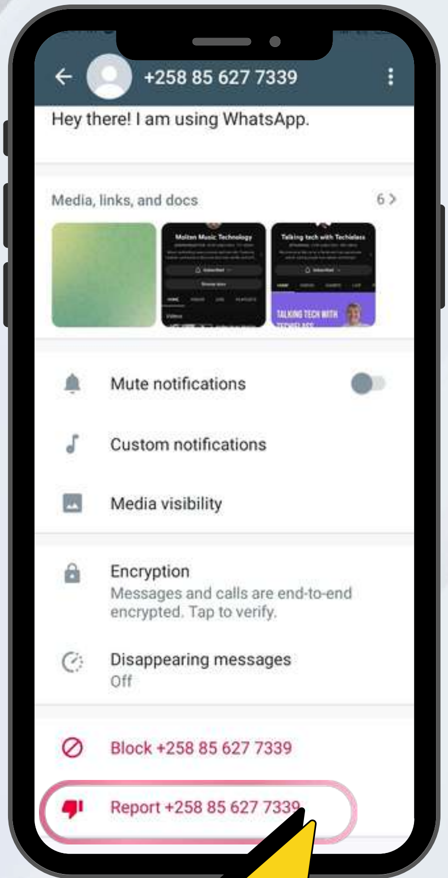
SPECIAL REPORT

साइबर सुरक्षा टिप्स

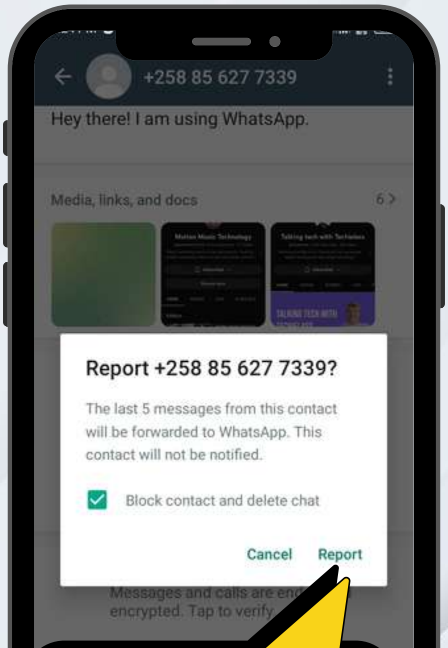
अनजान नंबर से आये इंटरनेशनल कॉल/ स्कैम कॉल और घोटाले की तुरंत रिपोर्ट करे



चैट खोलें जिसको आप रिपोर्ट करना चाहते हैं।



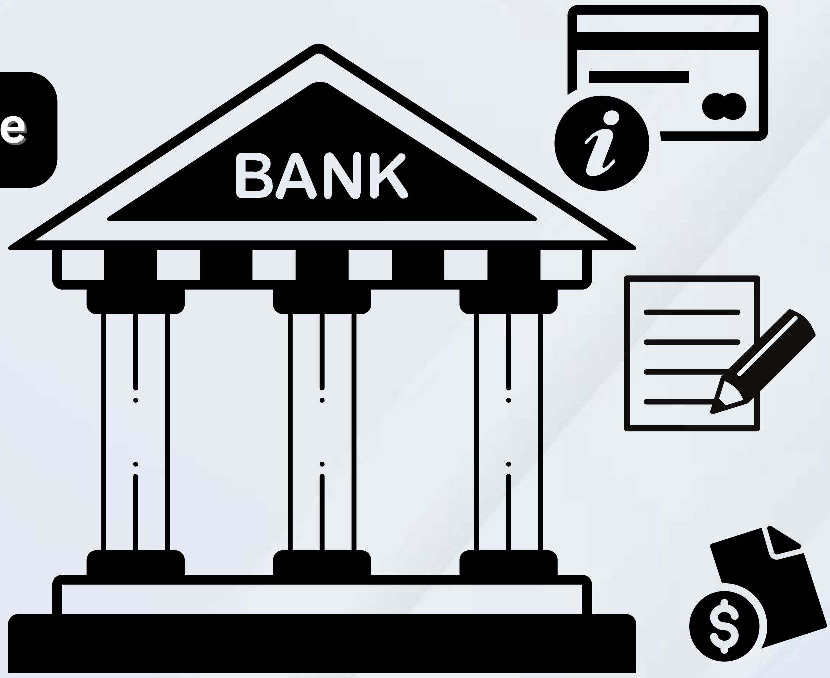
नंबर को रिपोर्ट करें ।



अंत में, फिर उस नंबर को ब्लॉक कर दें।

साइबर सुरक्षा टिप्स

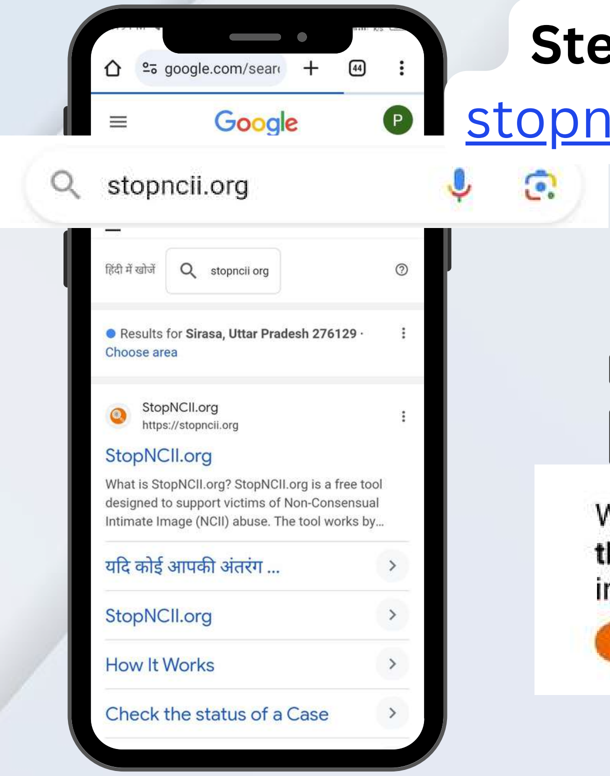
Bank details जैसे OTP, CVV, customer ID, UPI pin इत्यादि किसी भी व्यक्ति चाहे वो बैंक का कर्मचारी ही क्यों न हो, के साथ साझा न करें ।



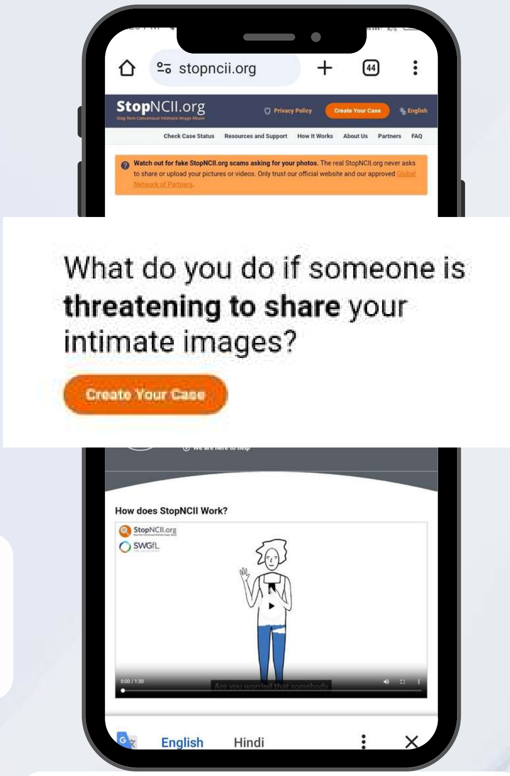
फ्रॉड होने की स्थिति में क्या करे ?

यदी आपकी कोई फोटो या वीडियो से छेड़छाड़ करके सोशल मीडिया पर अपलोड करे तो उसे तुरंत हटाने के लिए नीचे दिए चरणों का पालन करे।

Step 1- गुगल पर stopncil.org सर्च करे।



Step 2- परिणाम में आए इस लिंक पर क्लिक करे।



Step 3- creat your case पर क्लिक करे।

Step 4- सभी जानकारियों को ध्यान से भरे और रिपोर्ट दर्ज करे।

SPECIAL REPORT

फ्रॉड होने की स्थिति में क्या करे ?

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

SPECIAL REPORT

फ्रॉड होने की स्थिति में क्या करे ?

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 करे । 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।

SPECIAL REPORT

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 रहे!

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

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

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 । अत: 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

Oct,2023

Sept,2023

Aug,2023

July,2023

June,2023

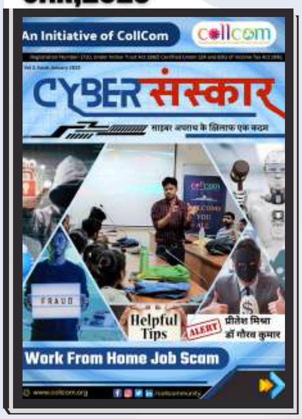
May,2023

April,2023

March,2023

FEB,2023

JAN,2023



DEC,2022

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

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