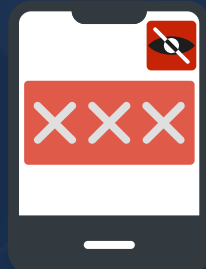


CYBER सास्कार

साइबर अपराध के खिलाफ एक कदम



Pornography content



HELPFUL TIPS

प्रीतेश मिश्रा
डॉ गौरव कुमार

Dark Side of Social Media



साइबर संस्कार : Dark Side of Social Media

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 : दिसम्बर 2023

मूल्य : ₹ 49

मुद्रक : कॉलकम, इंडिया

ISSN : 2583-9969

Dark Side of Social Media!

Contents

Page No.

• परिचय	03
• फ्रॉड के विभिन्न तरीके	04-12
- सोशल मीडिया अकाउंट हैक	04-08
- निवेश और क्रिप्टोकॉरेन्सी स्कैम	09-10
- सोशल मीडिया जॉब स्कैम	10-11
- सोशल मीडिया विज्ञापन ऑनलाइन शॉपिंग स्कैम	11-12
• सच्ची घटनाओं के माध्यम से फ्रॉड को समझना	12
• बचने के उपाय और सत्यता की जांच के तरीके	13-20
- सोशल मीडिया अकाउंट की प्राइवैसी को इनेबल करना	13
- अपने सोशल मीडिया अकाउंट में 2FA लागू करना	14-15
- वेबसाइट की सत्यता के जांच के तरीके	16-17
• साइबर सुरक्षा टिप्स	18-25
- अपलोडेड वायरल फोटो (प्राइवेट फोटो) को इंटरनेट से कैसे हटाएं ?	21
- सोशल मीडिया Account हैक होने की स्थिति में पहला कदम	22
- UPI फ्रॉड होने पर पहला कदम	24
- फ्रॉड होने पर शिकायत कहाँ करें ?	25
• मैगजीन के पिछले संस्करण	33

SPECIAL REPORT Senior citizen loses Rs 8.3 lakh while shopping for towels online, full story

Senior citizen loses Rs 8.3 lakh while shopping for towels online, full story

'Social Media'

पर ठगी का अंबार!

Cyber Fraud In MP: IAS-IPS अधिकारियों के फर्जी सोशल मीडिया अकाउंट बनाकर ठगी कर रहे ठग, कई पुलिसकर्मी फ्रॉड के शिकार

Cyber Fraud In MP: IAS और IPS अधिकारियों के सोशल मीडिया पर फर्जी अकाउंट के सहारे ठगी का मामला सामने आया है।

महिलाओं को सरकार Free में दे रही है शिलाई मशीन, फ्रॉड खबरों से रहें बचकर, सोशल मीडिया पर

FREE PRESS JOURNAL e-Paper

HOME MUMBAI NEWS INDIA BUSINESS ENTERTAINMENT SPORTS FEATURES VIRAL VIDEOS BRANDSUTRA ED

Home > Entertainment > Chhattisgarh: Singer Monika Raghuvanshi's Social Media Account Hacked, Obscene Content Posted

Chhattisgarh: Singer Monika Raghuvanshi's Social Media Account Hacked, Obscene Content Posted

The renowned singer, who has around three lakh followers on her Facebook account, began noticing explicit content on her official social media page on September 23.

NBT नवभारत टाइम्स फरीदाबाद पंजाब-हरियाणा राज्य भारत राम मंदिर मनोरंजन लाइफस्टाइल धर्म दुनिया विज्ञान टेक

Hindi News State Punjab And Haryana Faridabad Faridabad Cyber Fraud Hr Head Trapped Fake App Social Media Lost Rs

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

Reported By प्रमोद वैशित | नवभारत टाइम्स, कौम | Updated: 30 Dec 2023, 6:18 am

Home / India / News Online Shopping Scam: Curb Malpractices Like 'Dark Pattern', Government Asks E-Commerce Entities Like Amazon and Flipkart

The Indian EXPRESS JOURNALISM OF COURAGE Subscribe My Account Home Cities India Explained Opinion Business E 3 Things Podcast Play Crossword Latest News

News / Cities / Pune / Trying to contact bank on soc

Premium Trying to contact bank on social media, man falls prey to Rs 7.5L cyber fraud

By: Express News Service

bank automation news

Account takeover losses may exceed \$635B in 2023

Sift exploring gen AI to improve fraud tracking, data analysis

Vanik Trivedi November 21, 2023 in AI Reading Time 5 mins read

aahtak.in

सोशल मीडिया पर दिखा विज्ञापन, किया कॉल और धड़ाधड़ उड़े 27 लाख, साइबर फ्रॉड से ऐसे रहें सेफ

oneindia Join Channel

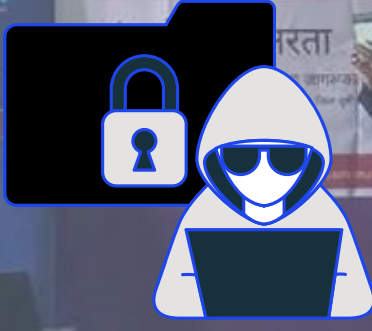
होम देश ताजा खबर विशेष लेख फीचर स्टोर्स

देश

मंत्री का बना दिया फेसबुक पर फेक अकाउंट और अश्लील फोटो से किया ऐसे बदनाम

मंत्री के फेक फेसबुक अकाउंट पर अश्लील फोटो डालकर वो अपनी पत्नी के लिए राजनीति में रास्ते बनाने चाहता था। इससे पहले वो पत्नी को सफल करने के चक्कर में कई और प्रयास कर चुका है।

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

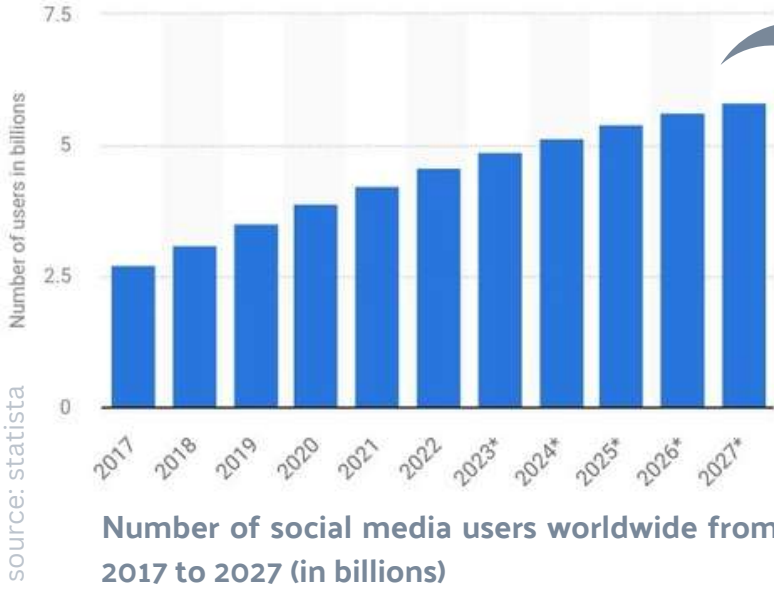


DARK SIDE OF SOCIAL MEDIA

नमस्कार दोस्तों,



मेरा नाम सैम है, आशा करते हैं आप सभी सपरिवार कुशल मंगल होंगे। आज एक बार फिर से साइबर सुरक्षा के इस कड़ी में सोशल मीडिया के माध्यम से हो रहे अपराध व उसने बचने के तरीकों के बारे में सच्ची घटना पर आधारित केस स्टडीज/कहानी के माध्यम से समझने का प्रयास करेंगे, और अपने परिवार एवं जुड़े सभी लोग जागरूक रहें ऐसा हम सब मिलकर प्रयास करेंगे।



Statista की एक रिपोर्ट के अनुसार, 2023 में सोशल मीडिया की वैश्विक पहुँच लगभग 60 प्रतिशत तक हो चुकी है और आगे उसी गति से वृद्धि भी कर रहा है। अनुमान के मुताबिक 2027 तक सोशल मीडिया उपयोगकर्ताओं की कुल संख्या **5.85 बिलियन (585 Cr)** से अधिक होने की उम्मीद है, जो दुनिया की आधी से अधिक आबादी होगी।

Social Media Fraud क्या है?

आज के समय में सोशल मीडिया इंटरनेट पर आधारित **सबसे लोकप्रिय और मनोरंजन वाला प्लेटफॉर्म** है जिसका उद्देश्य लोगों को एक-दूसरे के साथ जुड़ने, जानकारी साझा करने, और नेटवर्किंग करने का है। मगर इसी बीच इन प्लेटफॉर्म पर स्कैमर्स या फ्रॉड संगठन विभिन्न तकनीकियों का इस्तेमाल करके नकली प्रोफाइल बनाते हैं और फिर इसका प्रयोग **विभिन्न तरीकों से व्यक्तियों से धन, व्यक्तिगत जानकारी, या अन्य भ्रांतिपूर्ण लाभ** हासिल करने का प्रयास करते हैं जिसे आम भाषा में **सोशल मीडिया धोखाधड़ी** (Social Media Fraud) कहा जाता है।

social Media platform जैसे- Facebook, Instagram, Twitter, WhatsApp, Telegram etc.

अक्सर हमे अखबारों और दोस्तों के माध्यम से सोशल मीडिया पर लोगो की फेक आईडी देखने और सुनने को मिलता है जिसमे ठग किसी सोशल मीडिया प्रोफाइल की नकल कर एक दूसरी डुप्लीकेट आईडी बनाते हैं और उस आईडी से जुड़े लोगो को उस फेक आईडी से जोड़कर किसी बहाने से पैसे की मांग करते हैं या फिर उस व्यक्ति की छवि खराब करने की कोशिश करते हैं।



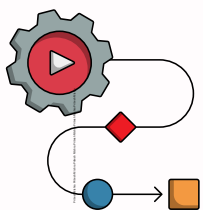
परंतु **वर्तमान स्थिति और भी भयावह है**, अब ठग सीधे सोशल मीडिया **अकाउंट को हैक** कर पल भर में उसके **छवि को खराब करने के धमकी के साथ एक मोटी रकम की मांग** करते हैं।

इस तरह की धोखाधड़ी को **सोशल मीडिया अकाउंट हैकिंग** (or **Social Media Account Takeover Fraud**) नाम दिया गया है, आइए आगे समझते हैं ये फ्रॉड कैसे घटित होता है और इससे कैसे बच सकते हैं।

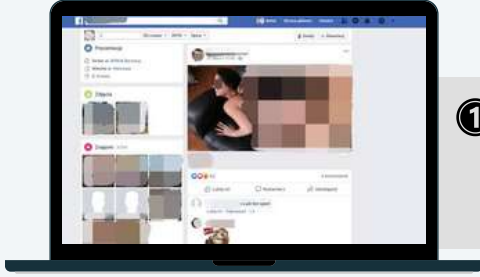
1 सोशल मीडिया अकाउंट हैकिंग धोखाधड़ी

सोशल मीडिया अकाउंट तभी हैक हो सकता है जब उस सोशल मीडिया अकाउंट का यूजर लॉगिन और पासवर्ड फ्रॉडस्टर या हैकर्स तक पहुँचता है। अकाउंट हैक करने के लिए हैकर्स अक्सर **फिशिंग तकनीक या संदिग्ध मैलवेयर एप्लीकेशन या रिमोट एक्सेस एप्लीकेशन जैसे टीम व्यूअर (Team Viewer), Any Desk जैसे एप्लीकेशन का इस्तेमाल करते हैं।**

ये कितना भयावह इसका अंदाजा आप इस न्यूज कटिंग और रिपोर्ट से लगा सकते हैं।



सोशल मीडिया अकाउंट को हैक करने के बाद फ्रॉडस्टर इसका इस्तेमाल अलग-अलग तरीके के फ्रॉड को अंजाम देने के लिए करते हैं-



① फ़िशिंग साइटों या नकली ऐप्स या अश्लील वीडियो के लिंक साझा करने के लिए।



② पीड़ितों के दोस्तों और परिवार के सदस्यों से व्यक्तिगत विवरण इकट्ठा करने के लिए।



③ अन्य ऑनलाइन खातों तक पहुँच प्राप्त करने के लिए (उदाहरण के लिए, "फेसबुक के साथ साइन इन करें" का उपयोग करके)।



④ नकली निवेश अवसरों के बारे में पोस्ट करना इत्यादि।



अकाउंट तक पहुँच/हैक करने का माध्यम

हैकर्स अक्सर फिशिंग तकनीक (डुप्लीकेट फेसबुक/इंस्टाग्राम लॉगिन पेज) का इस्तेमाल करते हैं। इसे समझने के लिए हम एक सच्ची घटना पर नजर डालते हैं। >>> >>>

केस स्टडी

सच्ची घटना पर
आधारित स्कैम

ये कहानी है राहुल (बदला हुआ नाम) की, जो BA तृतीय वर्ष का छात्र है, जिन्होंने ईमेल में प्राप्त हुए इंस्टाग्राम अलर्ट नोटिफिकेशन में दिए **sign in लिंक** पर क्लिक कर अपने अकाउंट का एक्सेस खो देता है।



आइए समझते हैं राहुल ने क्या गलती की ?

राहुल को मैसेज आता है की उनका इंस्टाग्राम अकाउंट किसी ने लॉगिन करने का प्रयास किया है, यदि वो नहीं है तो sign in लिंक पर क्लिक कर कन्फर्म करें।



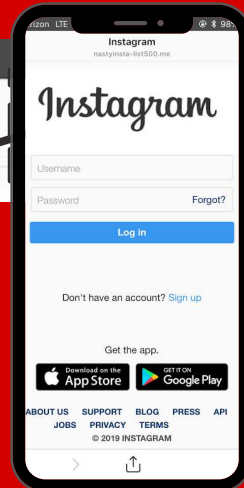
Instagram
FAKE
Hi [redacted]
Someone tried to log in to your Instagram account.
If this wasn't you, please use the following code to confirm your identity. Please [sign in](#)
382951

राहुल बिना कुछ सोचे समझे **sign in** पर क्लिक कर देता है।

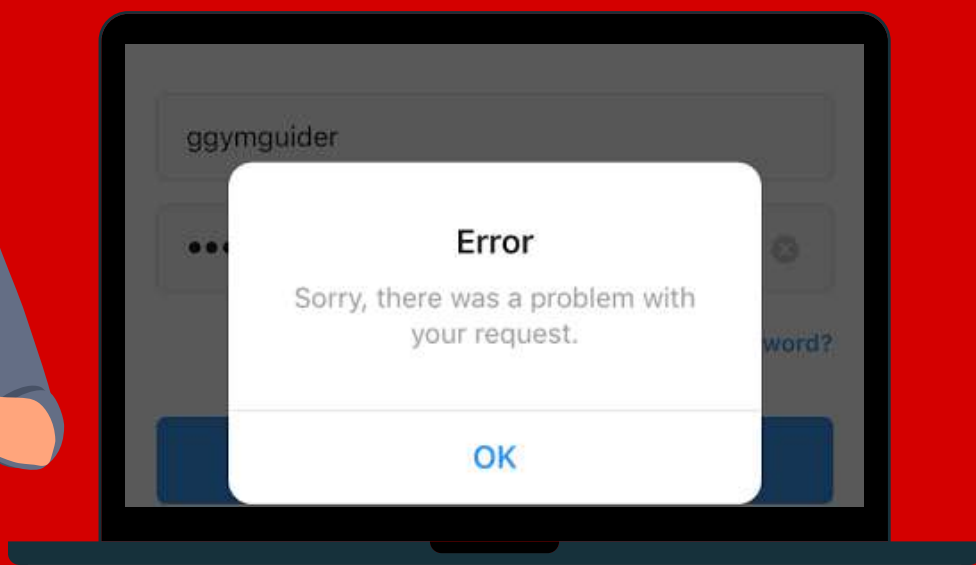
अब राहुल के सामने इंस्टाग्राम का लॉगिन पेज खुल जाता है।



Instagram
nastyinsta-list500.me

**Note-**

अगर इस इंस्टाग्राम पेज को ध्यान से देखे तो वेबसाइट के डोमेन से ही इसके **फेक होने का पता चल जाता है**, परंतु उस समय राहुल ने ये ध्यान नहीं दिया और यहाँ पर अपना इंस्टाग्राम लॉगिन और पासवर्ड इंटर कर दिया।



अरे ये क्या, अब मैं अपने ही अकाउंट को एक्सेस (ओपन) नहीं कर पा रहा हूँ। राहुल ने हर संभावित पासवर्ड से लॉगिन करने का प्रयास किया परन्तु वह अपने अकाउंट में लॉगिन करने में असफल रहा, और अगले दिन उसके एक मित्र का फोन आता है।



हाय राहुल कैसा है?
अरे यार सुन वो जो कल मैंने तुम्हे 5000 रुपए भेजे थे, जरूरत है भेज दे ना।



हेलो भाई! कैसे 5000 ?
कब दे दिए भाई, मुझे तो मिला ही नहीं।



क्या मजाक है! अरे भाई कल इंस्टाग्राम पर कोई अचानक इमरजेंसी में जरूरत थी तो तुमने किसी अन्य व्यक्ति के खाते में पैसे भेजने को कहा।



ओह! कल से तो मैं अपना अकाउंट एक्सेस ही नहीं कर पा रहा हूँ।



मुझे अब समझ आया! शायद मेरा अकाउंट किसी ने hack कर लिया है, और वही पैसे की माँग कर रहा है।

अरे यार! मुझे एक बार पैसे भेजने के पूर्व तुम्हे कॉल कर लेना चाहिए था, अच्छा सुन! जल्दी से ये काम कर ले जिससे और लोग न फँसे.....



यदि आपके साथ भी इस तरह की घटना घटित हो तो नीचे बताए बिंदुओं का पालन करें।

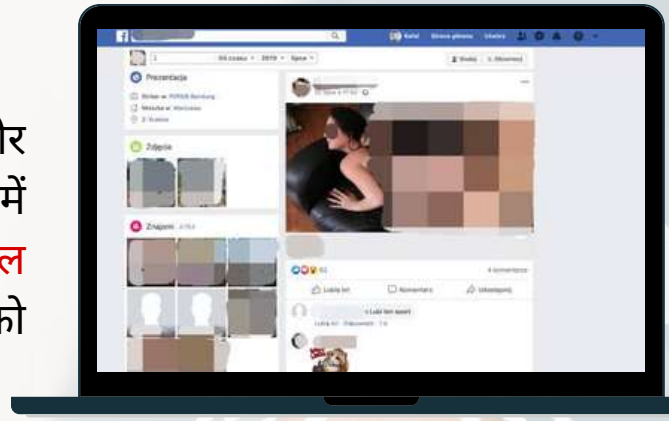


- ▶ जल्दी से अपने व्हाट्सएप और अन्य सोशल मीडिया पर स्टोरी अपडेट करो की मेरा अकाउंट हैक हो गया है, यदि मेरे अकाउंट से पैसे की माँग की जाए या अन्य ऑफर का लिंक भेजे तो स्वीकार न करें।
- ▶ अपने अकाउंट की हैक होने की रिपोर्ट करें - page number 22 का अनुसरण करें।
- ▶ www.cybercrime.gov.in पर शिकायत दर्ज करें।

क्या करें ?

- ▶ राहुल की तरह किसी भी अलर्ट और नोटिफिकेशन को बिना जांच पड़ताल किये अपना लॉगिन और पासवर्ड किसी भी पेज पर इंटर न करें।
- ▶ सोशल मीडिया पर टू-फैक्टर ऑथेंटिकेशन को इनेबल रखे।
- ▶ कभी-कभी कुछ आधिकारिक वेबसाइट की फेक वेबसाइट होती है, उसकी सत्यता की जांच हेतु Page No. - 16 का अनुसरण करें।
- ▶ संदेश के माध्यम से पैसे की माँग करने पर पैसे न दे चाहे वो आपके मित्र रिश्तेदार, अथवा परिवार का ही सदस्य क्यों न हो, कॉल के माध्यम से पहले कन्फर्म करे, तत्पश्चात संबंधित व्यक्ति के खाते में पैसे भेजे।

इस प्रकार स्कैमर्स अकाउंट को हैक कर पैसे की ठगी और कभी-कभी आपके छवि को खराब करने व समाज में अनैतिकता फैलाने के उद्देश्य से अकाउंट पर अश्लील वीडियो लिंक व फोटो अपलोड कर अन्य लोगों को प्रभावित करते हैं।



2 निवेश (INVESTMENT) और क्रिप्टोकॉरेन्सी स्कैम

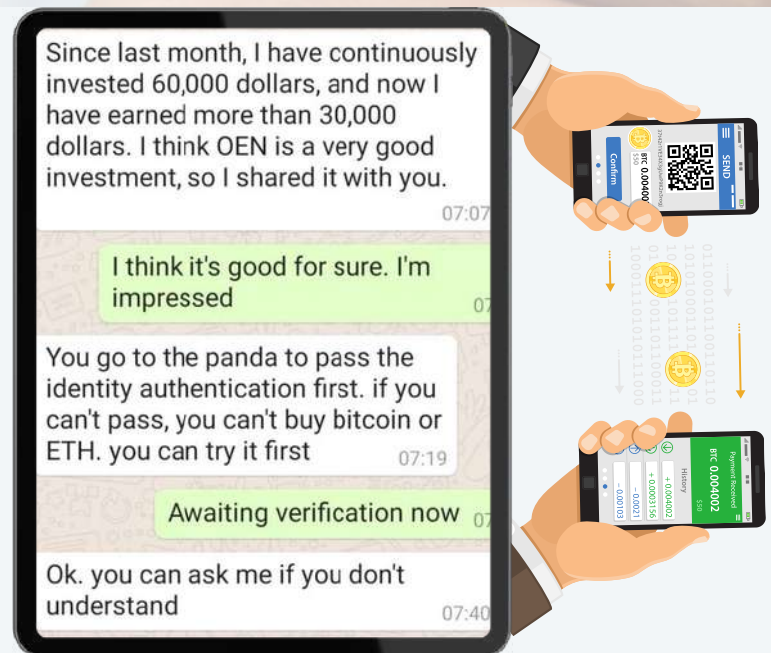


इंटरनेट-आधारित जानकारी के बढ़ते उपयोग के साथ, अधिक से अधिक लोग अपने निवेश निर्णय लेने में मदद के लिए इंटरनेट और सोशल मीडिया का उपयोग कर रहे हैं। वहीं स्कैमर्स ने भी लोगों तक पहुंचने के लिए इंटरनेट को अपना स्रोत बना लिया है। उनके पास इंटरनेट के माध्यम से आप तक पहुंचने के विभिन्न तरीके हैं और ऐसा ही एक तरीका सोशल मीडिया है।

यह अनुमान लगाया गया है कि पिछले वर्ष सभी सोशल मीडिया घोटाले के नुकसान का **37% निवेश घोटालों के कारण था** - जिनमें से अधिकांश क्रिप्टोकॉरेन्सी घोटाले थे।

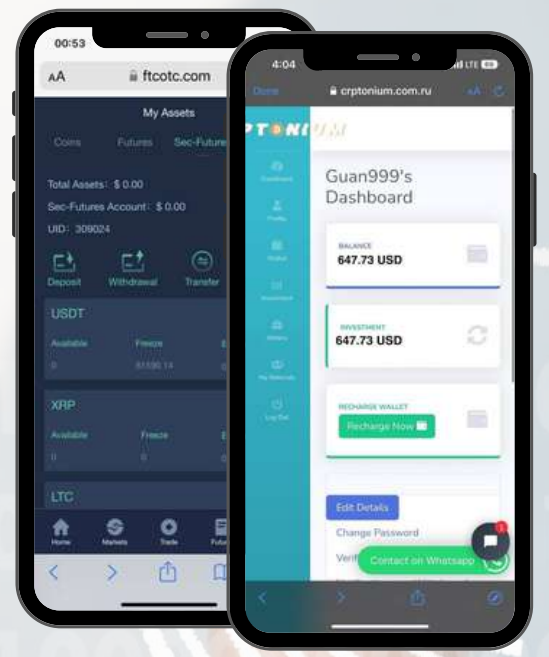
यह धोखाधड़ी तब शुरू होती है जब स्कैमर्स आमतौर पर सोशल मीडिया के माध्यम से आप तक पहुँच बनाता है। शुरुवात में स्कैमर्स सामान्य बातचीत के माध्यम से संबंध बनाने की कोशिश करता है और फिर बाद में एक "महान निवेश अवसर (Great Investment Opportunity)" के बारे में जानकारी साझा कर आपको बहुत तेजी से पैसा कमाने में बारे में अवसर बताता है और कई सफल उदाहरण देकर आपको निवेश करने के लिए उत्साहित करता है।

Source : AURA

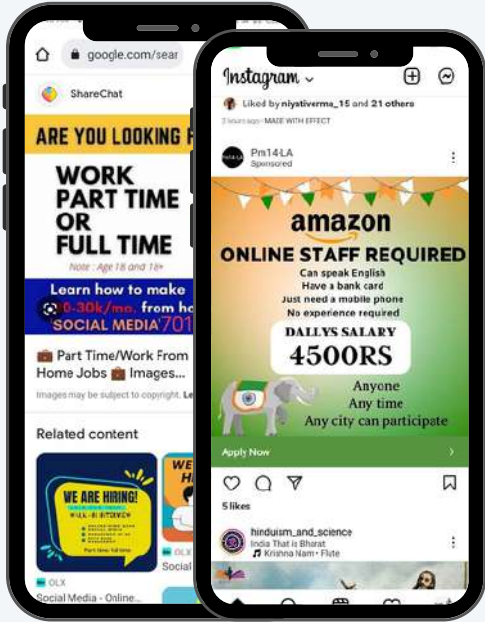


परन्तु वास्तव में स्कैमर्स एक **फर्जी एप्लीकेशन या वेबसाइट** के माध्यम से आपको पैसे इन्वेस्ट करने को कहता है, जो की देखने में **बिल्कुल ऑथेंटिक (Original)** सा दिखता है **लेकिन फेक होता है**, और आपके पैसे डबल होने के बजाय शून्य हो जाते हैं।

अतः भूलकर भी इस तरह के अंजान एप्लीकेशन अथवा वेबसाइट में पैसे इन्वेस्ट न करें।



3 सोशल मीडिया जॉब स्कैम



पिछले कुछ वर्षों में **जॉब स्कैम की संख्या में वृद्धि हुई है** क्योंकि अधिक भारतीय घर से या विशेष रूप से ऑनलाइन काम कर रहे हैं।

जालसाज़ अद्भुत दूरस्थ नौकरी के अवसरों को बढ़ावा देने के लिए **नकली सोशल मीडिया खाते बनाते हैं**। यह वादा करते हुए कि आप ढेर सारा पैसा कमा सकते हैं। नौकरी घोटाला करते समय घोटालेबाजों के **दो उद्देश्य होते हैं -**

पैसे के उद्देश्य से -

एक घोटालेबाज आपको नौकरी देगा, लेकिन केवल तभी जब आप पहले उनके बताये गए **“सामान/उपकरण खरीदेंगे”**। वास्तव में वो उपकरण के लिए कुछ **रजिस्ट्रेशन शुल्क** की मांग करते हैं, और किसी न किसी बहाने मांग बढ़ती जाती है और आप फँस जाते हैं।



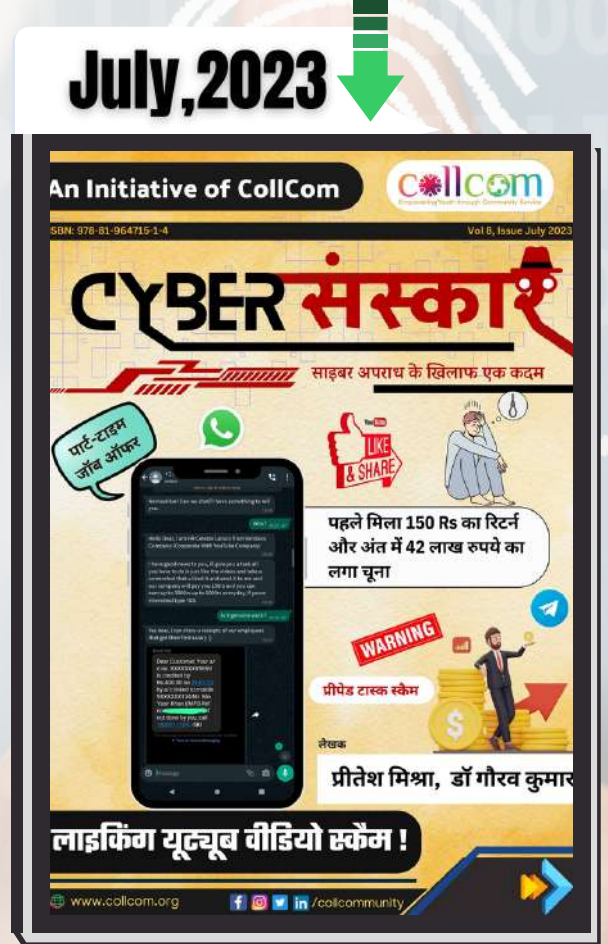
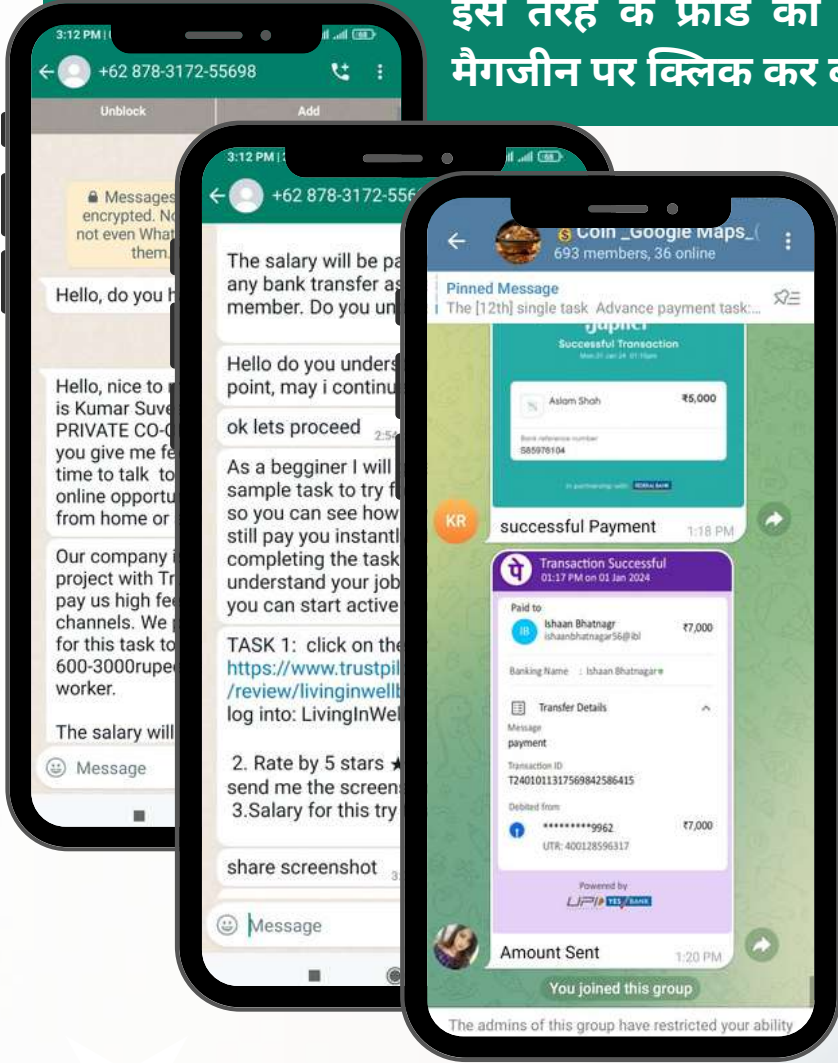
जानकारी के उद्देश्य से -

स्कैमर्स आपको इस उम्मीद में एक नौकरी आवेदन भेजेंगे कि आप उसमें अपनी निजी जानकारी, जैसे कि **आपका नंबर, घर का पता, आधार, बैंक डिटेल्स इत्यादि** भरेंगे, जिसका इस्तेमाल कर वो **ठगी को अंजाम देंगे**।

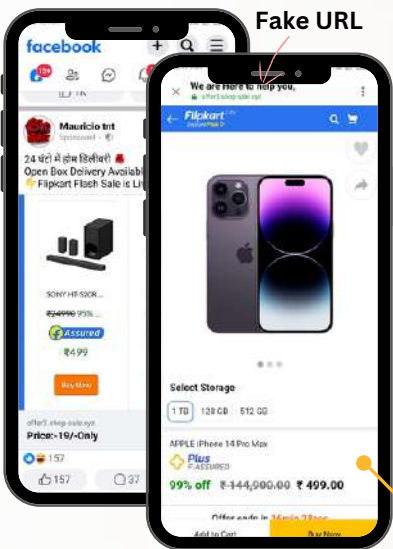
अक्सर स्कैमर्स का मुख्य उद्देश्य आपके पैसे चुराना होता है इसके लिए वो अनेक प्रकार के बहाने करते हैं।

वर्तमान में सबसे प्रचलित फ्रॉड पार्ट टाइम जॉब, वीडियो लाइक/ गूगल रेटिंग का है जिसमें ठग आपको वीडियो लाइक करने के पैसे देते हैं।*

इस तरह के फ्रॉड को बेहतर ढंग से समझने के लिए हमारे इस मैगजीन पर क्लिक कर बताये गए सुरक्षा टिप्स का अनुसरण करें।



4 सोशल मीडिया विज्ञापन ऑनलाइन शॉपिंग स्कैम



स्कैमर्स अक्सर सोशल मीडिया पर नकली उत्पादों या दुकानों को बढ़ावा देने के लिए सोशल मीडिया विज्ञापनों (Advertisement) का उपयोग करते हैं। The Better Business Bureau (बीबीबी) को भ्रामक फेसबुक और इंस्टाग्राम विज्ञापनों के बारे में हजारों शिकायतें मिली हैं।

आपको इंटरनेट पर हजारों ऐसी साइट्स मिलेंगी कुछ तो बिल्कुल वास्तविक वेबसाइट्स/ऐप्स की तरह होती है, जिसे पहचानना मुश्किल होता है।

Fake Flipkart website

ध्यान रखे, सोशल मीडिया पर दिखने वाले किसी भी विज्ञापन (Advertisement) पर क्लिक करने से पूर्व उसके प्रामाणिकता की जांच* उसके वास्तविक वेबसाइट पर जाकर जरूर करें।

Oct, 2023



*website की जांच के लिए पेज 16, 17 का अनुसरण करें।



इस तरह के फ्रॉड को और बेहतर समझने के लिए हमारे इस मैगजीन पर क्लिक कर बताये गए सुरक्षा टिप्स का अनुसरण करें।

5 रोमांस फ्रॉड

डेटिंग साइटों पर रोमांस फ्रॉड आम हैं, लेकिन कई स्कैमर्स टारगेट को ढूंढने के लिए सोशल मीडिया का भी सहारा लेते हैं।

सबसे पहले स्कैमर्स किसी भी सोशल मीडिया (ज्यादातर फेसबुक, इंस्टाग्राम) पर एक फेक प्रोफाइल बनाते हैं।

इसके बाद वो कुछ इस तरह के कमेंट अथवा मैसेज भेजने के साथ आपसे मित्रता करते हैं।

और शीघ्र ही प्यार का इजहार करते हैं, और आपसे किसी न किसी बहाने (बीमारी का बहाना, न्यूड वीडियो कॉल रिकॉर्ड करने और इसी प्रकार के नए हथकंडे अपनाकर) पैसे की मांग करते हैं।

पैसे भेजते ही आप ठगी के शिकार बन जाते हैं।

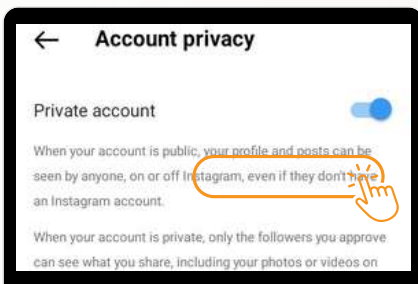
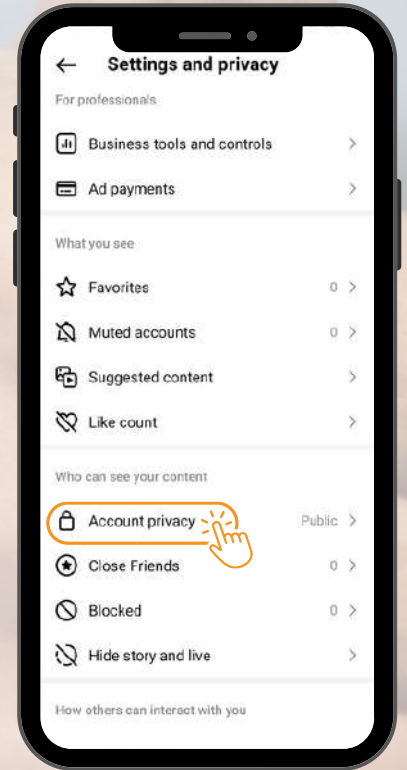
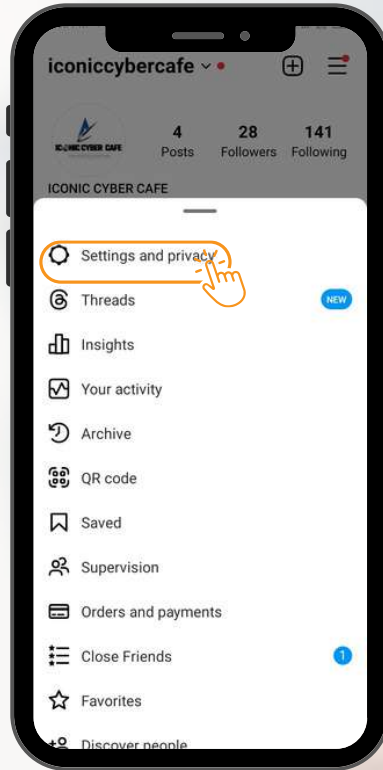
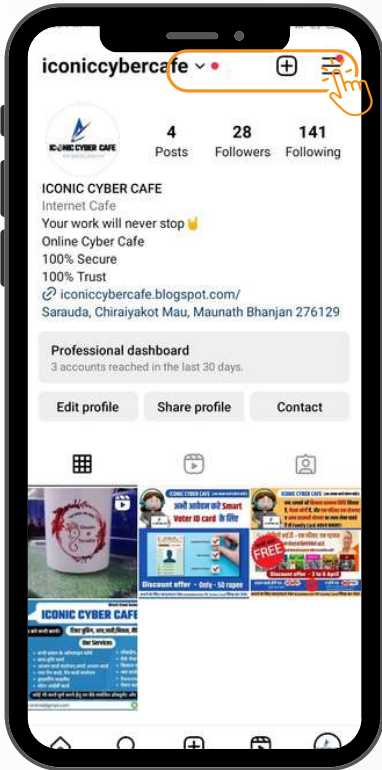
इस तरह के फ्रॉड से बचने हेतु आगे दिए गए सभी सुरक्षा टिप्स का अनुसरण करें। >>>>

प्राइवेटि इनेबल करना

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



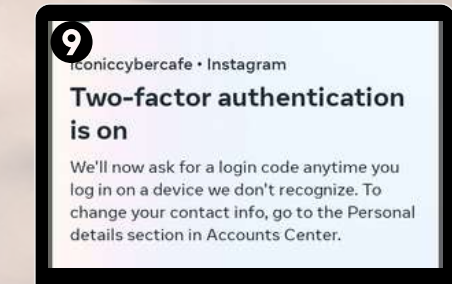
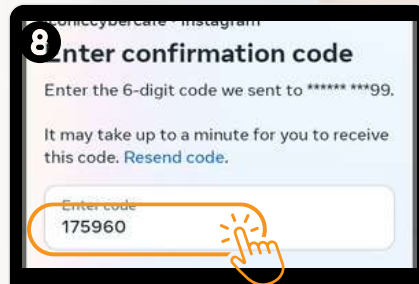
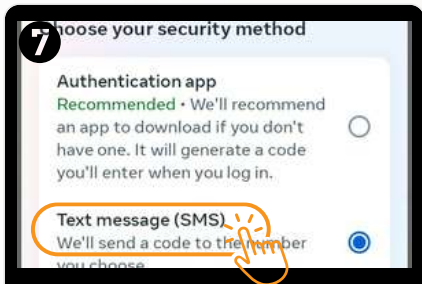
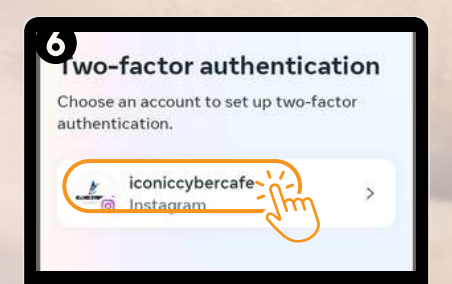
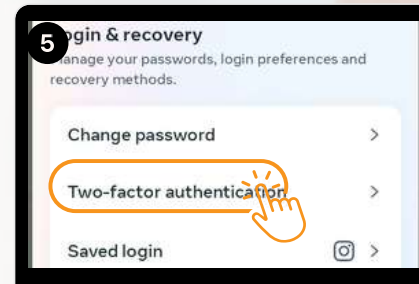
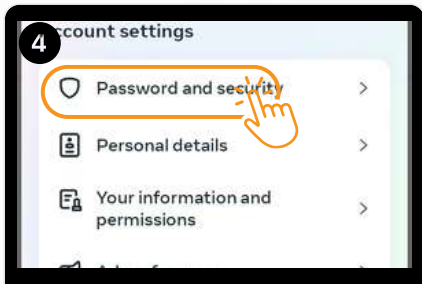
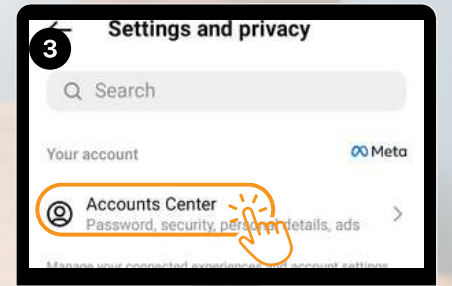
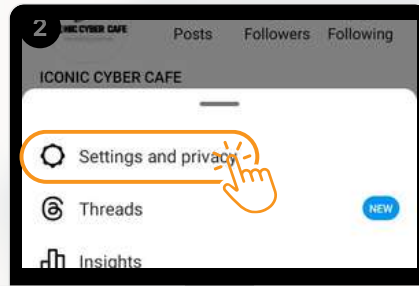
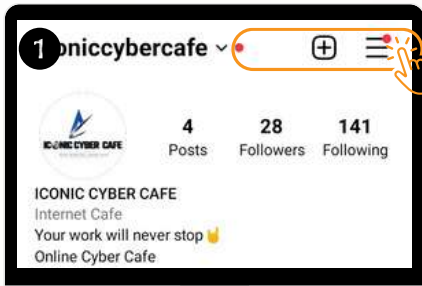
सोशल मीडिया अकाउंट की प्राइवेटि को इनेबल करने के लिए निम्न चरण का पालन करें-



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

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।

2FA को इनेबल करना

WhatsApp पर Two-Factor Authentication (2FA)



लागू करने के लिए विभिन्न चरणों का पालन करें:



1 Account

Privacy

Security **द्वि-चरणीय सत्यापन पर क्लिक करें।**

Two-step verification

Change number

Delete my account

2 Two-step verification

For added security, enable two-step verification, which will require a passcode when registering your phone number with WhatsApp again.

ENABLE

3 Two-step verification

Enter a 6-digit passcode which you'll be asked for when you register your phone number with WhatsApp:

1 2 ABC 3 DEF -

4 GHI 5 JKL 6 MNO

7 PQRS 8 TUV 9 WXYZ

अपनी पसंद का छह अंकों का पिन दर्ज करें और इसकी पुष्टि करें

4 Two-step verification

Confirm your passcode:

1 2 ABC 3 DEF -

4 GHI 5 JKL 6 MNO

7 PQRS 8 TUV 9 WXYZ

पिन को पुष्टि के लिए दुबारा दर्ज करें

5 Two-step verification

Add an email address to your account which will be used to reset your passcode if you forget it and safeguard your account.

q w e r t y u i o p

a s d f g h j k l

z x c v b n m

अपना ईमेल ID इंटर करके, next पर क्लिक करें

6 Two-step verification

Two-step verification is enabled. You'll need to enter your passcode when registering your phone number with WhatsApp again.

Disable

Change passcode

Change email address

ईमेल पते की पुष्टि करें और सहेजें या पूर्ण टैप करें।

वेबसाइट की सत्यता जाँच करना

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

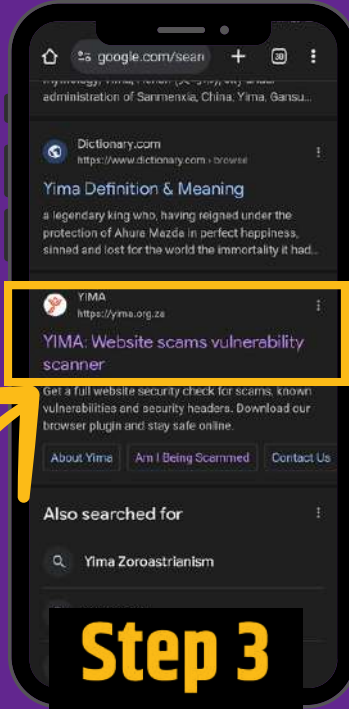
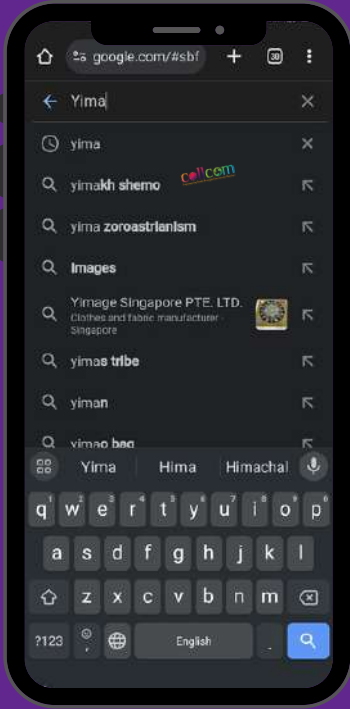
website* की लिंक three dot पर क्लिक कर शेयर बटन से कापी करें।

*जिस वेबसाइट की जांच करनी हो।

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

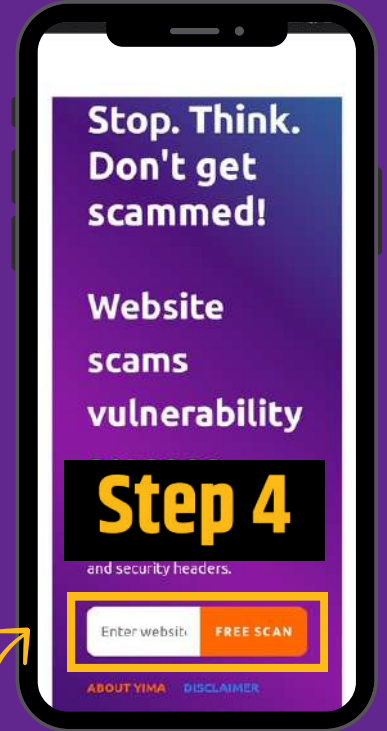
Step 2

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



Step 3

अब इस लिंक पर क्लिक करें।

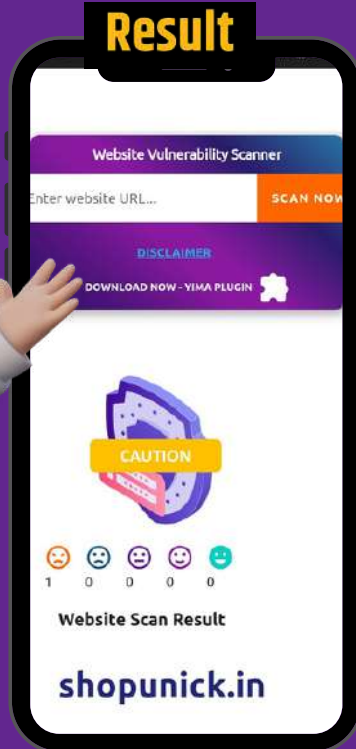


यहाँ पर कॉपी किये गए लिंक को paste करें।

परिणाम आपके सामने है



Result



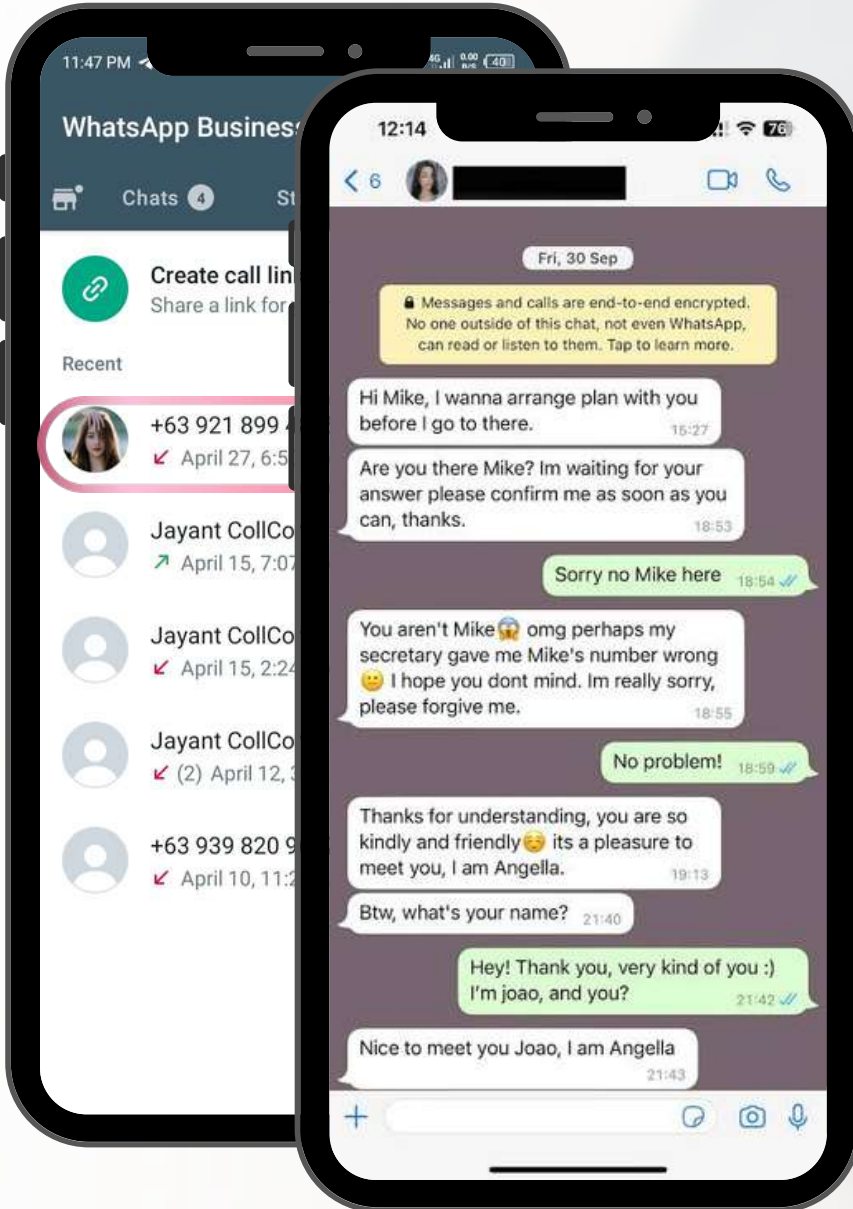
➤ इस वेबसाइट के माध्यम से आप किसी भी वेबसाइट की vulnerability (safe हैं या नहीं) का पता कर सकते हैं।

➤ 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

व्हाट्सएप पर अनजान नंबर से आए कॉल/मैसेज का जवाब न दें।

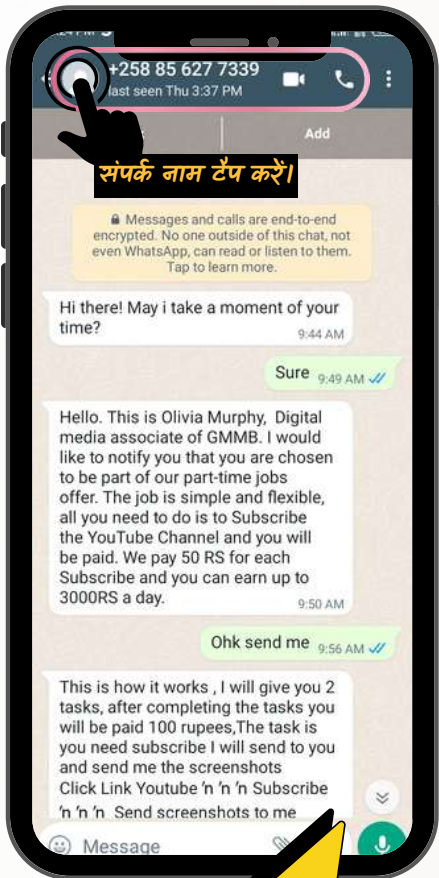


प्रतिपल सतर्क रहें, अनजान इंटरनेशनल नंबर से आए कॉल/वीडियो कॉल अथवा मैसेज का कभी जवाब न दे अन्यथा आप ठगी के शिकार हो सकते हैं। बिल्कुल इनकी तरह।

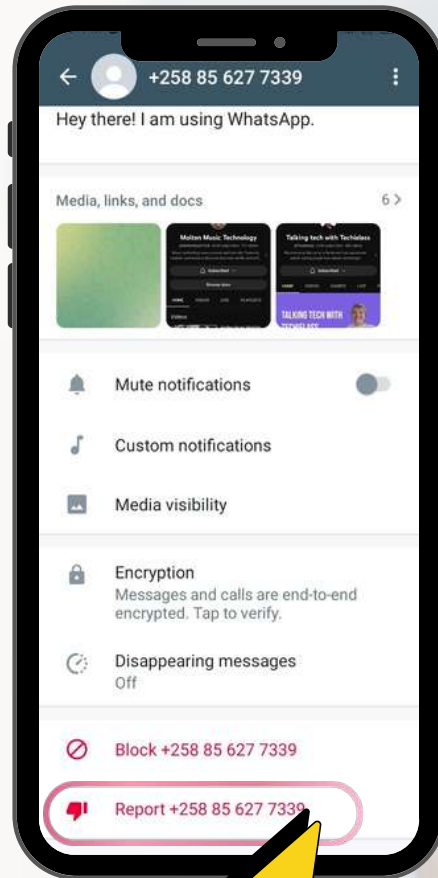
<https://zeenews.india.com/personal-finance/whatsapp-nude-video-call-scam-man-loses-rs-1-57-lakhs-but-gets-back-rs-1-39-lakh-check-how-2532720.html>

साइबर सुरक्षा टिप्स

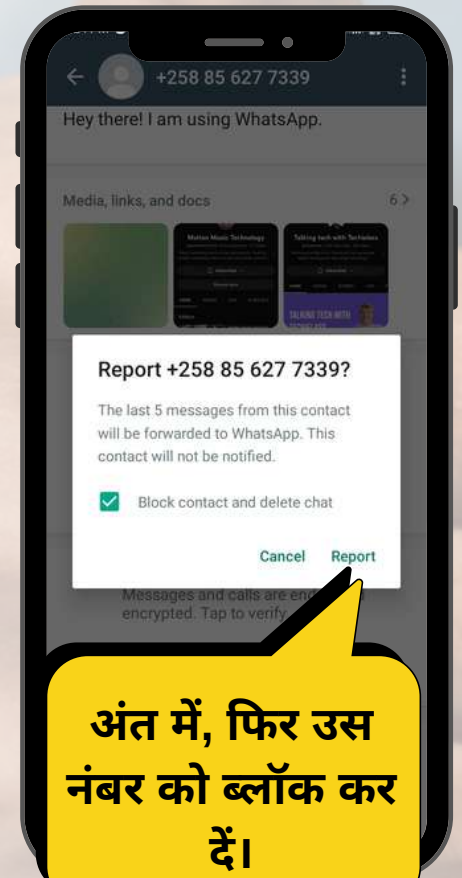
अनजान नंबर से आये इंटरनेशनल कॉल/
स्कैम कॉल और घोटाले की तुरंत रिपोर्ट करें



चैट खोलें जिसको
आप रिपोर्ट करना
चाहते हैं।



नंबर को
रिपोर्ट करें।



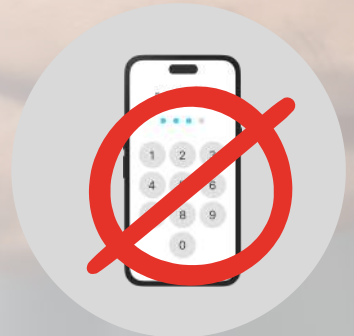
अंत में, फिर उस
नंबर को ब्लॉक कर
दें।

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।**



Never share

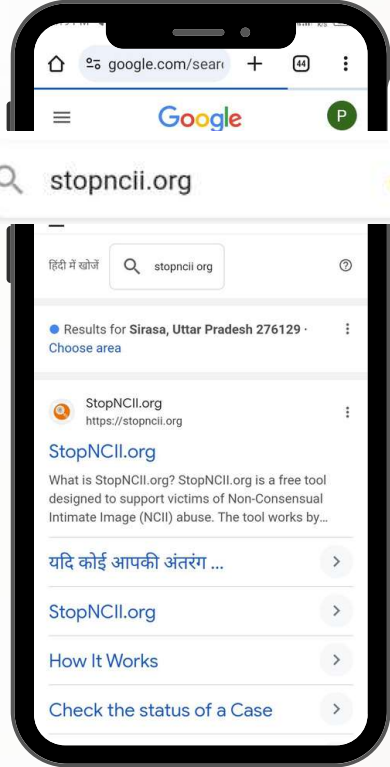


वायरल फोटो और वीडियो हटाने के लिए क्या करें ?

यदि आपकी कोई पर्सनल फोटो या वीडियो को छेड़छाड़ करके किसी ने सोशल मीडिया या इंटरनेट पर अपलोड कर दिया है तो उसे हटाने के लिए नीचे दिए चरणों का पालन करें -



Step 1- गुगल पर stopncii.org सर्च करें।

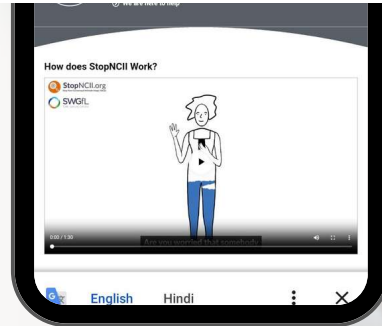


Step 2- परिणाम में आए इस लिंक पर क्लिक करें।



What do you do if someone is threatening to share your intimate images?

Create Your Case



Step 3- create your case पर क्लिक करें।

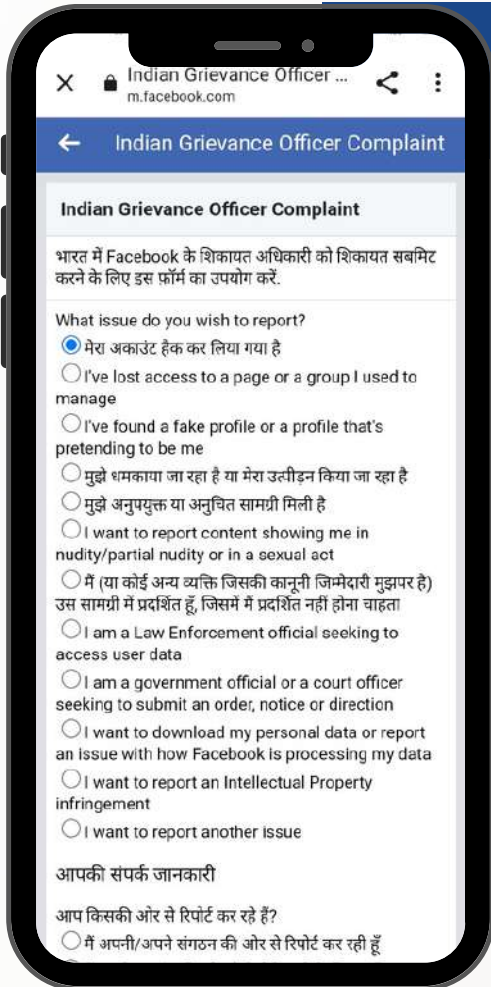


Step 4- सभी जानकारियों को ध्यान से भरे और रिपोर्ट दर्ज करें।

ACCOUNT हैक होने की स्थिति में क्या करें ?

जैसे ही आपके अकाउंट के हैक होने का पता चले तो संबंधित सोशल मीडिया अकाउंट के Grievance officers को रिपोर्ट करें।

यहाँ आप **सोशल मीडिया अकाउंट से जुड़े किसी भी समस्या** के लिए रिपोर्ट कर सकते हैं, चाहे वो आपका **अकाउंट हैक हुआ हो** या किसी ने **फेक आईडी बनाई हो** या आपको कोई **अन्य आईडी से परेशान कर रहा हो** सभी के लिए संबंधित सोशल मीडिया के **लिंक पर क्लिक कर रिपोर्ट** कर सकते हैं।



और **अधिकतम 15 दिन के भीतर** आपकी समस्या का निवारण कर दिया जाता है।



<https://www.whatsapp.com/contact/forms/1534459096974129>



<https://www.facebook.com/help/contact/278770247037228>



<https://www.facebook.com/help/contact/779201836048501>

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](#)



UPI पेमेंट 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 पुनः प्राप्त कर सकते हैं।



- 1** A hand icon points to the search bar containing 'npci'.
- 2** A hand icon points to the 'Consumer' link in the bottom navigation bar.
- 3** A hand icon points to the 'UPI Complaint' link under the 'Consumer' section.
- 4** A hand icon points to the 'Transaction' dropdown menu in the 'Complaint' form.
- 5** A hand icon points to the 'Transaction' form fields.
- 6** A hand icon points to the 'Submit' button at the bottom of the form.

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

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

Step 3- अब UPI पर क्लिक करें।

Step 4- नीचे स्क्रॉल करें 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 ?

यदि आप इस तरह के फ्रॉड के शिकार हो जाते हैं तो तुरंत ही आप सभी chat, भेजे गए डॉक्यूमेंट, और भेजे गए पैसे 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।

भारत सरकार गृह मंत्रालय
GOVERNMENT OF INDIA MINISTRY OF HOME AFFAIRS

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
National Cyber Crime Reporting Portal

75 आज़ादी का अमृत महोत्सव

Indian Cyber Crime Coordination Centre

REPORT WOMEN/CHILDREN RELATED CRIME + **REPORT CYBER CRIME** TRACK YOUR COMPLAINT CYBER VOLUNTEERS +

RESOURCES + CONTACT US HELPLINE

HELPLINE No 1930

HELPLINE NUMBER 1930

If you are a victim of Financial Cyber Fraud Dial Helpline Number 1930



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

निःशुल्क ऑनलाइन साइबर प्रशिक्षण



Cyber Crime Awareness Training Mega Campaign

साइबर अपराध जागरूकता प्रशिक्षण महा-अभियान (प्रोजेक्ट साइबर संस्कार)

#CyberSanskar #CollCom #CyberSafeWorld

Section 1 of 7

Cyber Crime Awareness Training Mega Campaign



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 जिसमें 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 नहीं लिया तो एक बार अवश्य ले।

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

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



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 कर 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



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।



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 नहीं था। अतः **फ्रॉड होने के स्थिति में आप सबसे पहले ज़रा भी न घबराए, परिवार वाले डारेंगे या मित्र क्या कहेंगे ?** ये कदापि न सोचे या कोई भी गलत फैसला न ले, समय रहते **यदि आप शिकायत दर्ज करवा देते हैं तो आपके पैसे मिलने के अवसर बढ़ जाते हैं।**

अब तो **RBI के दिशा निर्देश के अनुसार** आप फ्रॉड होने के तुरंत बाद यदि अपने संबंधित बैंक में शिकायत दर्ज कराते हैं तो वो **90 दिन के भीतर ही आपकी समस्या सुलझाने का प्रयास करते हैं।** 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 हैं, आने वाले समय में **कॉल स्पूफिंग के खतरे अधिक है** जिसमें 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 रहेंगे।

जागरूक रहें, सुरक्षित रहें !



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 Niranjn
(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)



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

पढ़ने के बाद अपना सुझाव अवश्य दें।

<https://g.page/r/CZmEUz-HXMe0EAI/review>