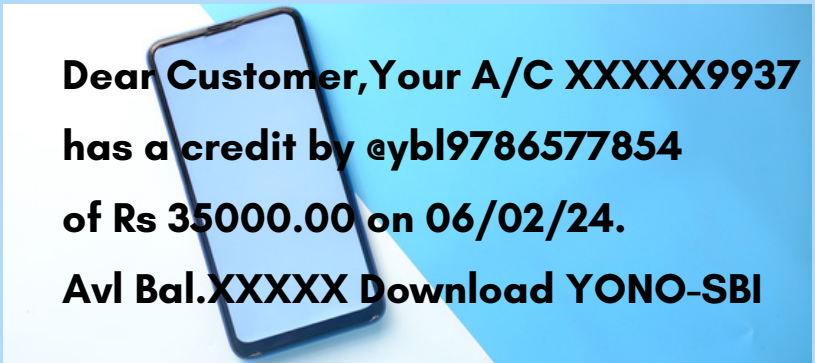
विषय- सूची

1.फर्जी क्रेडिट मैसेज फ्राड

साइबर ठगों द्वारा फ्राड का यह तरीका आजकल सबसे ज्यादा इस्तेमाल में लाया जा रहा है। इस जालसाजी में फ्राडस्टर की आपके मोबाइल पर काल आती है और वह आपसे कहता है कि मैं आपका रिश्तेदार बोल रहा हूं अथवा आपके पिता जी का मित्र बोल रहा हूं। आपके पिता जी से मैने 2000/- रुपए लिए थे। उनसे बात हो गई है। उन्होंने आपके नंबर पर भेजने को कहा है। आप इस नंबर पर फोन पे आदि चलाते हैं? आप अपना कोई बैंकिंग नंबर बता देते हैं। फिर वह 2000 की जगह बीस हजार रुपए क्रेडिट होने का फर्जी टेक्स्ट मैसेज बनाकर आपको भेजता है। फिर तुरंत ही उसका दुबारा फोन आता है और कहता है कि गलती से एक जीरो बढ़ गया है और आपके खाते में बीस हजार चले गए है। मुझे अभी तुरंत दवा लेनी है आप जल्दी से 18000/- वापस कर दीजिए। आप उस मैसेज को सही मान लेते है, कि आपके खाते में पैसा आ गए और आप तुरंत उतना रुपया वापस देते हैं, बिना अपना खाता चेक किए। कई बार वह सीधे ही आपके किसी मित्र, रिश्तेदार का नाम लेकर रुपये क्रेडिट होने का फर्जी टेक्स्ट मैसेज भेजकर कहता है कि मुझे किसी को रुपये भेजने थे और मेरे खाते से रूपये जा नहीं रहे मैंने आपको भेज दिया है, आप इस युपीआई पर उन्हें भेज दीजिए आपको आवाज भी कुछ जानी पहचानी सी लगती है जिसपर आप सहज ही विश्वास कर लेते हैं, बाद में आपको ठगी का एहसास होता है। कई बार ठग आपको विश्वास में लेने के लिए आपके मित्र या रिश्तेदार का नाम भी लेता है जिसकी जानकारी वह आपके सोशल मीडिया अकाउंट के माध्यम से पहले से कर लेते हैं या तुक्केबाजी में ऐसा नाम लेते हैं जो अक्सर कॉमन होते हैं। ऐसे में रुपये भेजने से पहले आपको अन्य माध्यमों से पहले वेरीफाई कर लेना चाहिए।



2. फेसबुक/ सोशल मीडिया पर अंजान से दोस्ती

फेसबुक/ सोशल मीडिया पर अंजान से दोस्ती पड़ सकती है भारी यह बात ध्यान में रख कर ही सोशल मीडिया पर किसी अंजान की फ्रेंड रिक्वेस्ट स्वीकार करें। फ्राडस्टर आपसे दोस्ती करता है। यहां पर महिलाएं भी शिकार हो रही हैं। महिला से पुरुष मित्र और पुरुष से महिला मित्र बनकर दोस्ती करते है। फ्राडस्टर खुद की विदेश में लग्जरी लाइफ फोटो, वीडियो भेजकर फर्जी दिखावा करता है।

लोगों की दो से तीन दिन में दोस्ती काफी गहरी हो जाती है यहां तक किसी किसी की तो बात शादी तक पहुंच जाती है। फिर शुरु होता असली खेल जल्द ही वह उधर से करोड़ो का गिफ्ट पैक जिसमें आईफोन, डायमंड रिंग, घड़ी, नेकलेस आदि कि पैकिंग दिखाकर आपको भेजता है। या फिर खुद ही कहता है कि मैं आपसे मिलने भारत आ रहा हूं/आ रही हूं। इधर आपसे बात होती रहती है। दो दिन बाद आप पर पुन: फोन आयेगा कि वह गिफ्ट का सामान कस्टम विभाग द्वारा एयरपोर्ट पर पकड़ लिया गया है ,

अथवा खुद को ही पकड़ा जाना बता देगा। फिर कहेगा कि कस्टम वाले उसे छुड़ाने के पैसे मांग रहे हैं। मेरे पास भारतीय मुद्रा नहीं है आप इनलोगों को रुपये भेज दो। मैं आपको मुद्रा बदल कर बाद में दे दूंगा। उसी दौरान दूसरी तरफ से उसी की गैंग के दूसरे लोग फर्जी कस्टम अधिकारी बनकर आपको फोन कर यही बात आपसे कहेंगे और आप उनकी बातों में उलझ जाते है। डर से या लालच में पड़कर यही सोचते है कि करोड़ो का गिफ्ट मिल रहा है लाख दो लाख चले ही जायेंगे तो क्या हुआ ।

और इस तरह कई बार में अलग-अलग बातें बनाकर आपसे लाख पचास हजार बड़ी आसानी से झटक लिए जाते हैं । यहां सावधानी यही रखनी है कि सोशल मीडिया पर पूर्णतया आश्वस्त होने के उपरान्त ही किसी के सम्पर्क करना चाहिए और जब बात पैसे की आये तो आपको सतर्क हो जाना चाहिए।

RAKESH KUMAR MISHRA
CYBER CRIME CELL LUCKNOW

3.फर्जी लोन App

फर्जी लोन Application के माध्यम से हो रही ठगी के बारे में सतर्क रहें। जागरूक रहें। किसी फर्जी लोन एप्लीकेशन से ऑनलाइन लोन के लिए अप्लाई न करें। आजकल लोग झटपट लोन लेने के चक्कर में फर्जी लोन एप्लीकेशन से दश-पांच हजार रुपए लोन के लिए अपलाई कर देते हैं।

उसी दौरान एप्लीकेशन डाउनलोड करते समय अथवा वेबसाइट पर फॉलो करते समय आप अपना contact और गैलरी एक्सेस की अनुमति भी दे देते हैं। लोन लेने के बाद फ्रॉडकर्ता आपको दिए गए रकम की कई गुना राशि वापसी मांगता है। यदि आप पैसा रिटर्न भी करते हैं तब भी उसकी डिमांड और बढ़ती जाती है इसके बाद आपके मोबाइल से एक्सेस किए गए फोटो विडियो एडिट कर अश्लील रूप में बना करके आपके कॉन्टैक्ट नंबरों को भेजने की धमकी देकर आपको ब्लैकमेल करते हैं। फिर बाद में आपकी परेशानी बढ़ जाती है। तमाम फर्जी लोन एप्लीकेशन को आरबीआई की तरफ से प्रतिबंधित कर दिया गया है। आप भी झटपट लोन लोने से पहले एप्लीकेशन/ वेबसाइट को सही तरह है जांच परख लें।

RAKESH KUMAR MISHRA
CYBER CRIME CELL LUCKNOW

Fake, नकली

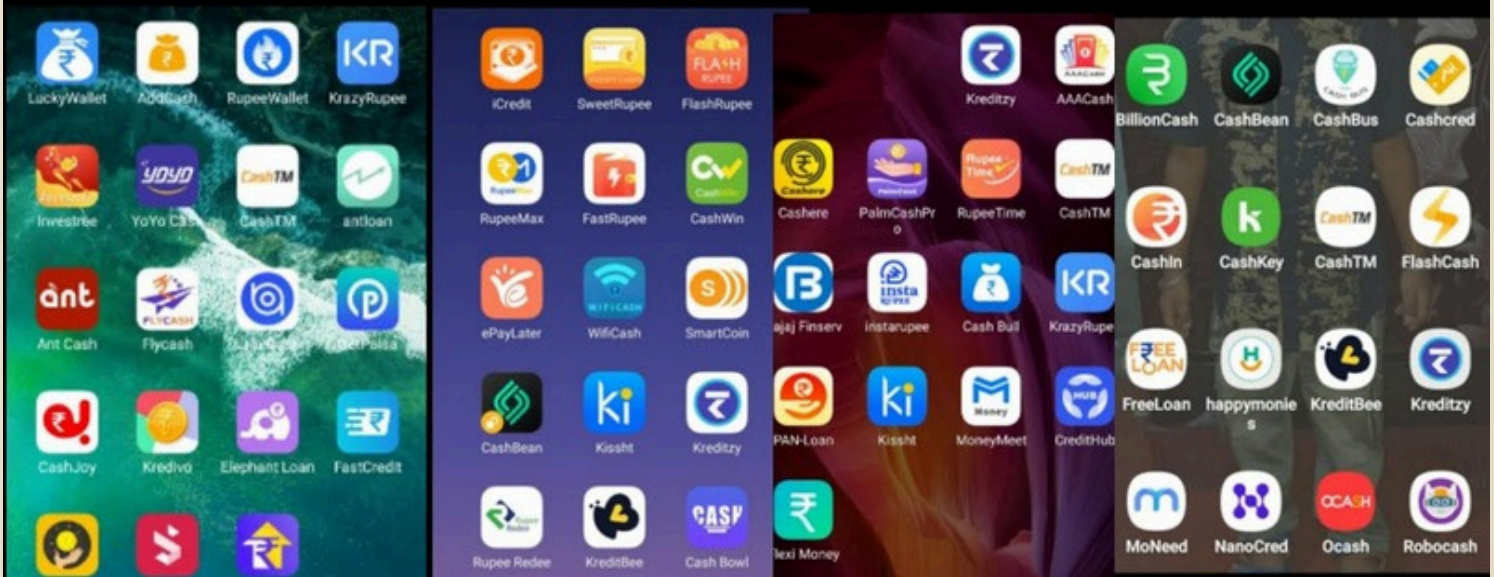
Loan App List

सावधान

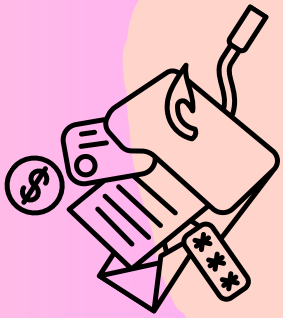
रहना इन से

ये सब LOAN APP FAKE है/

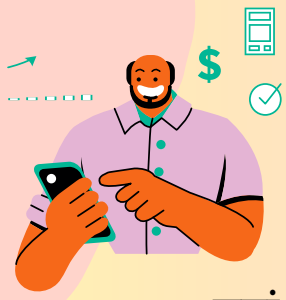
आपके खिलाफ कानूनी करवाई हो सकती है /



4. टेलीग्राम चैनल/ वर्क फ्रॉम होम फ्राड



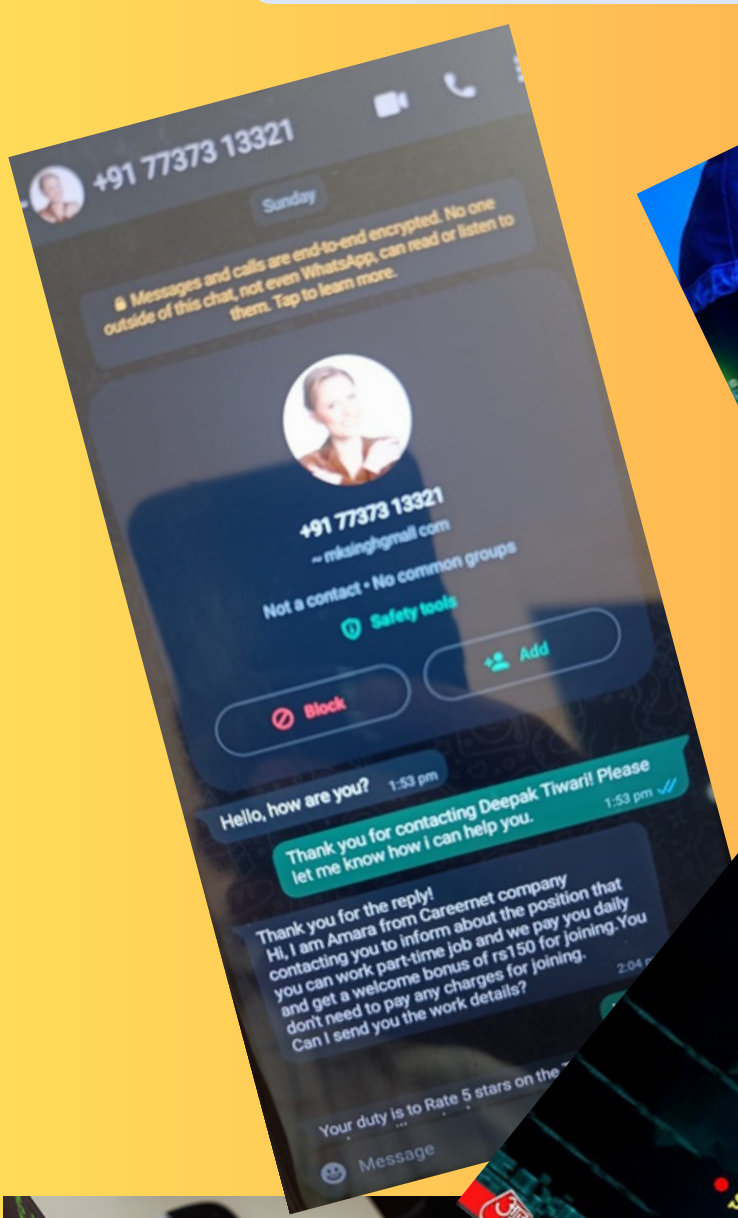
पिछले काफी दिनों से टेलीग्राम चैनल/ व्हाट्सएप के माध्यम से एक साइबर फ्राड बहुत प्रचलन में चल रहा है। प्रारंभ में आपके पास किसी सोशल साइट से वर्क फ्राम होम का मैसेज आता है, और आपको युट्यूब, फेसबुक चैनल लाइक करने या किसी होटल या रेस्टोरेंट अस्पतालों को रेटिंग करने को कहा जाता है। शाम तक आपको खाते कुछ रुपये आ जाते हैं और आपका भरोशा बढ जाता है। फिर धीरे धीरे आपको काम के साथ-2 दूसरी जगह टेलीग्राम पर शिफ्ट किया जाता है। टेलीग्राम चैनल के माध्यम से निवेश करके अत्यधिक रिटर्न प्राप्त करने का लोगों को प्रलोभन दिया जाता है। चैनल पर बहुत सारे फ्राडस्टर पहले से जुडे रहते हैं। वह अपने रिटर्न का फेक स्क्रीन शॉट शेयर करते रहते हैं, जिससे आपको यकीन हो सके कि बहुत सारे लोग जुडे हैं और उन्हें लाभ भी हो रहा है। शुरुआत छोटे अमाउंट से होती है। उसका आपको दुगुना रिटर्न भी प्रदान किया जाता है, परंतु बाद में अलग अलग टास्क देकर/ बहाने बनाकर कई बार में आपकी एक बड़ी राशि फंसा ली जाती है। आपको लगता है कि आप सही जगह निवेश कर रहे हैं।

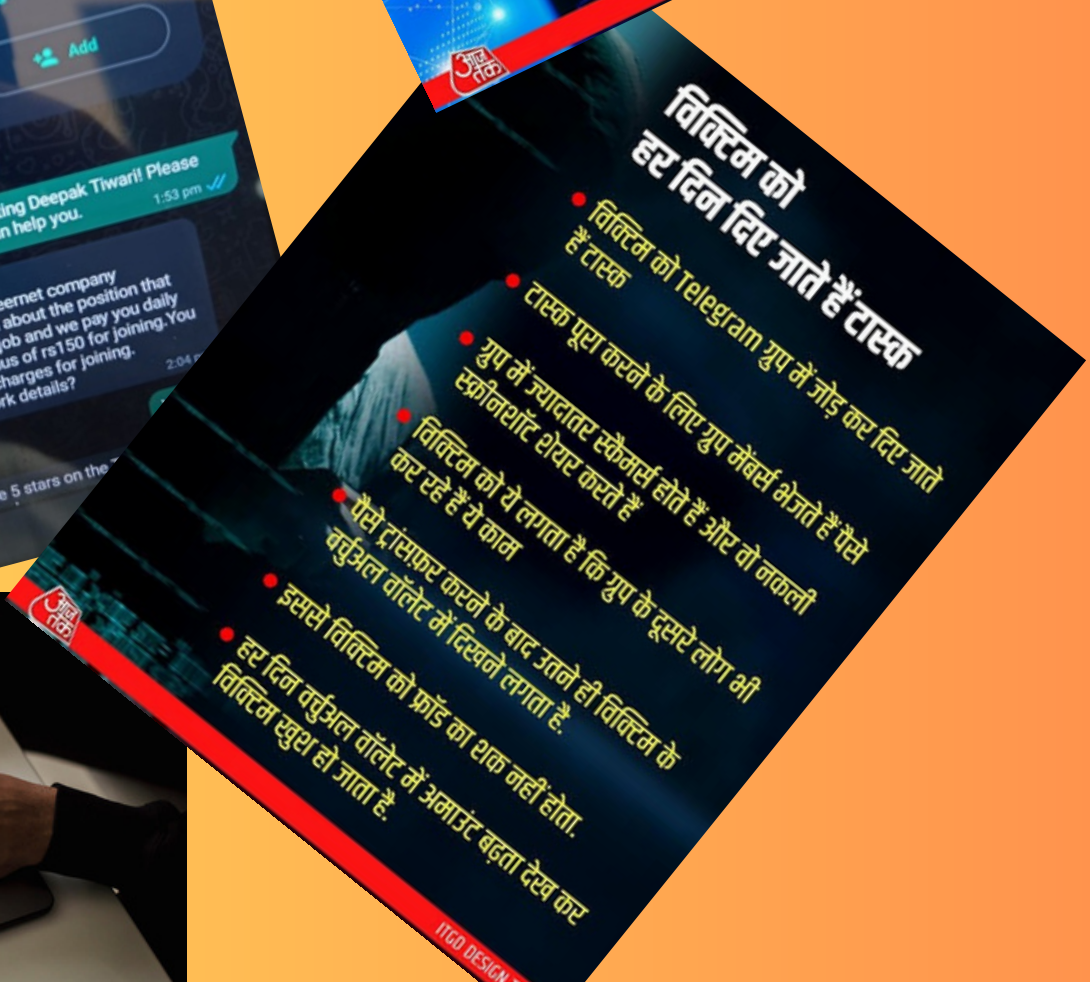


यहां कभी-2 आपकी किसी क्रिप्टो में निवेश करने के लिए एक फर्जी प्लेटफॉर्म पर आपकी आईडी बनायी जाती हैं। वह वेबसाइट फर्जी होती है। जिसे ठगी करने वाले 35- 40 हजार रूपए खर्च कर करके बनवा लेते हैं। वह कृप्टो करेंसी भी फर्जी होती है। जो केवल उस वेबसाइट/ वालेट पर आपको दिखाई देती है। आपका निवेशित पैसा जो उस वालेट पर शो करता वह भी फेक होता है। जिसे न ही आप उसका विड्राल कर सकते हैं और न ही किसी अन्य करेंसी में बदल सकते। इस तरह से आपका पैसा एक खाते से दूसरे खातें में होता हुआ या फिर किसी अन्य के द्वारा क्रिप्टों में बदलकर आउट ऑफ इंडिया चला जाता है।

साइबर अपराधियो द्वारा एक बार आपका पैसा फंसा लेने के बाद वह पैसा निकालने के लिए और अधिक रुपये निवेश करने के नये-2 नियम व टास्क बताने लगते हैं और लोग भी वह पैसा निकालने के लिए बार-2 पैसा भेजते जाते हैं और इस तरह कई लोग कर्ज की स्थिति तक पहुंच जाते हैं।

इस तरह के मामलों में लोग एक दिन से लेकर हफ्ते भर में कई लाख रुपये फंसा दे रहे हैं।





5.गुगल पर पड़े फर्जी हेल्प लाइन नंबर

अक्सर हम मोबाइल कंपनी से संबंधित, बैंक से संबंधित या किसी पार्सल डिलीवरी को लेकर तकनीकी सहायता प्राप्त करने के लिए अथवा अपनी शिकायत दर्ज कराने के लिए फटाफट गुगल से नंबर सर्च करके बात करने लग जाते हैं । ऐसा करने पर हम गलत नंबरों के संपर्क में आ जाते हैं और साइबर ठगी का शिकार हो जाते हैं।

(तत्सम्बन्धित कम्पनी की असली वेबसाइट से नम्बर प्राप्त करें व उसकी जांच पडताल कर लें।)

यहां आपको बताना चाहूंगा कि साइबर ठगों द्वारा वेबसाइट पर फर्जी प्लेटफार्म बनाकर कुछ पैसे खर्च करते हैं और अपना फोन नम्बर अलग- अलग कंपनियों की टेक्निकल असिस्टेंट अथवा हेल्प लाइन नंबर आदि के रूप के सर्च इंजन पर प्रमोट कराते हैं। जब भी हम किसी तकनीकी सहायता के लिए गुगल पर नंबर सर्च करते हैं तो साइबर ठगों के नंबर गुगल सर्च बार में सबसे ऊपर मिल जाते हैं। इन नम्बरों पर सम्पर्क करने पर हमारी बात इन ठगों से होती है और हम इस पर ध्यान नहीं देते। बात करते करते-2 वह जैसा बताता है हम वैसा ही करते जाते हैं। उसके कहने पर हम अपना डाटा बता देते है या किसी फर्जी लिंक पर क्लिक कर देते है अथवा कोई फर्जी एप्लीकेशन डाउनलोड कर लेते हैं। फिर कुछ समय बात जब हमारे खाते से पैसे कटने का मैसेज आता है, तब पता चलता है कि हम फ्राड के शिकार हो गए।

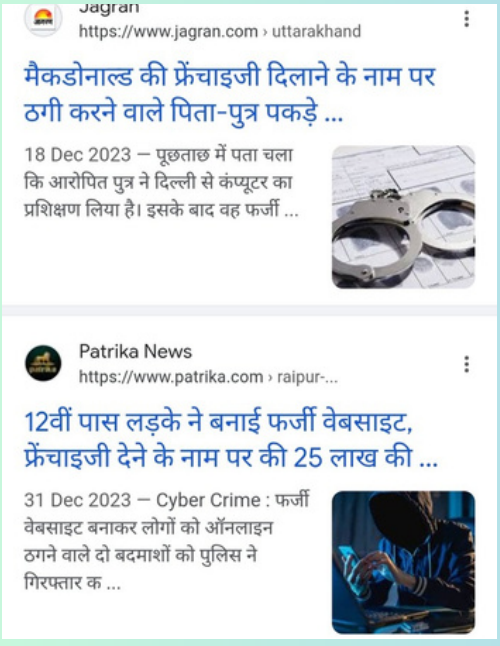
राकेश कुमार मिश्र उप निरीक्षक साइबर क्राइम सेल कमिश्नरेट, लखनऊ

6. गुगल आदि सर्च इंजन की फर्जी वेबसाइट

जिस तरह गुगल पर बहुत सारे फर्जी नंबर पड़े हुए है उसी तरह तमाम ब्रांडेड कंपनियों के नाम से फर्जी वेबसाइट भी साइबर अपराधियों द्वारा बनाकर सर्च इंजन गुगल आदि पर डाल दी गईं हैं।

फर्जी वेबसाइट बना देश भर से ठगे करोड़ों रुपये

धोखाधड़ी करने वाले गिरोह का भंडाफोड़, तीन गिरफ्तार, फ्रेंचाइजी व सरकारी योजनाओं के नाम पर लगाते थे चूना



Jagran
https://www.jagran.com › uttarakhand

मैकडोनाल्ड की फ्रेंचाइजी दिलाने के नाम पर ठगी करने वाले पिता-पुत्र पकड़े ...

18 Dec 2023 – पूछताछ में पता चला कि आरोपित पुत्र ने दिल्ली से कंप्यूटर का प्रशिक्षण लिया है। इसके बाद वह फर्जी ...

Patrika News
https://www.patrika.com › raipur-...

12वीं पास लड़के ने बनाई फर्जी वेबसाइट, फ्रेंचाइजी देने के नाम पर की 25 लाख की ...

31 Dec 2023 – Cyber Crime : फर्जी वेबसाइट बनाकर लोगों को ऑनलाइन ठगने वाले दो बदमाशों को पुलिस ने गिरफ्तार क ...

क्राइम ब्रांच की गिरफ्त में ठग।

लखनऊ सोमवार को हल्दीराम कंपनी की फ्रेंचाइजी दिलाने के नाम पर ठगी करने वाले पटना निवासी राकेश कुमार को गिरफ्तार कर लिया। ठग ने गूगल पर कंपनी के नाम से फर्जी वेबसाइट बना रखी थी। जो भी फोन करके फ्रेंचाइजी मांगता उसको बातों में फंसाकर सिक्योरिटी के नाम पर लाखों रुपए ले लेता।

हम जब भी किसी कंपनी जैसे सीमेंट, कपडे, फूड आइटम आदि की फ्रेंचाइजी लेने के लिए वेबसाइट के माध्यम से संपर्क करते हैं अथवा दूसरे शहर किसी होटल की बुकिंग करते हैं तो हमारा संपर्क फर्जी वेबसाइट से हो जाता है। उसी फर्जी वेबसाइट पर हम अपना पंजीकरण कर लेते हैं। वहीं इंटरव्यू भी हो जाता है।

बाद में उसी के बताए अनुसार हम पेमेंट भी कर देते हैं । वह सिक्योरिटी आदि के नाम पर तरह-2 के बहाने बनाकर और अधिक पैसे की मांग करता है। जिसका एहसास हमें कुछ समय बाद होता है। या फिर जब हम मौके पर जाते हैं। ऐसे में हमें किसी भी वेबसाइट की सही तरीके से पहचान करके ही आगे की कार्यवाही करनी चाहिए।

7. न्यूड वीडियो कॉल फ्राड

न्यूड वीडियो कॉल से ठगी का शिकार बहुत लोग हो रहे हैं और भारी भरकम राशि फ्राडस्टरों को स्थानांतरित कर देते है तथा बदनामी के डर से किसी से अपनी बात शेयर तक नहीं करते हैं।

इसमें ठगी करने वाले तरीका क्या अपनाते हैं आईये जानते हैं। साइबर ठग कंप्यूटर प्रोजेक्ट के माध्यम से फेसबुक अथवा व्हाट्सएप पर महिला के रूप में न्यूड काल करते हैं। काल वीडियो होती है या फिर कभी आडियो से शुरु होकर वीडियो काल में बदल दी जाती है ।

बात करते हुए आपको भी अपने वस्त्र उतारने को प्रेरित करते हैं। इसी में कुछ लोग फिसल जाते हैं और अपने कपड़े उतार देते हैं। कुछ लोग नहीं भी उतारते हैं। यहां दोनों ही मामलों में आपकी वीडियो बन जाती है। जिसने उतारे कपड़े उसकी असली फिल्म और जिसने वस्त्र नहीं उतारे उसकी एडिट करके वीडियो बना लेते हैं।

अब शुरू होता है दूसरा चरण ब्लैकमेल करने । चूंकि इसी दौरान आपको गैलरी के कॉन्टैक्ट भी उनके हाथ लग जाता है। बाद में वह आपसे पैसे की डिमांड करता है न देने पर वह आपके फेसबुक पर रिस्तेदारो को, कॉन्टैक्ट नंबरों को आपकी अश्लील तस्वीर/ वीडियो भेजने की धमकी देता है। कभी सोशल मीडिया, युट्यूब पर डालने की धमकी दी जाती है। दूसरी तरफ इन्ही की गैंग के कुछ लोग खुद को पुलिस अधिकारी कह कर फोन करके आपको डराते हैं कि महिला ने आप पर केश किया है। पैसे मांग रही है दे दो नहीं तो जेल चले जाओगे। डर कर लोग लाखों रुपये देते जाते हैं। काफी नुकसान होने के बात अपनी बात लोगों से शेयर करते हैं।

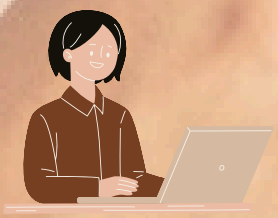
य़हां आपको ध्यान देना है कि यदि अचानक ऐसी काल रिसीब भी हो जाती है और कोई ब्लेकमेल करता है तो किसी भी कीमत पर पैसे नहीं देना है। एक स्टेटस के माध्यम से अपनी बात शेयर करनी है ताकि अन्य लोग भी सतर्क हो सकें।

8.फर्जी फोन कॉल फ्राड

साइबर अपराधी आपके फेसबुक अथवा अन्य सोशल मीडिया की गतिविधि पर नजर रखते हैं। उसके माध्यम से आपके मित्र रिश्तेदारों के बारे में थोड़ी बहुत जानकारी प्राप्त कर लेते हैं। अथवा आम जनमानस की साधारण मनोवृत्ति को लेकर ऐसे ही तुक्केबाजी मार कर आपको काल करते हैं

पुलिस अधिकारी बनकर आपके किसी सम्बन्धी को किसी अपराध में पुलिस द्वारा गिरप्तार किये जाना बताकर या स्वयं आपको किसी मामले सम्मिलित होना या आपके नाम से किसी अवैध पार्सल के पकड़े जाने बताकर डराते है।

अन्य कारण जिसमें आपकी केवाईसी अपडेट, या किसी पेंशन योजना, जीवित प्रमाण पत्र अपडेट लाटरी/ जैकपाट लगने को लेकर भी बातें बना सकते हैं। आपके किसी परिचित अथवा रिश्तेदार का नाम लेकर उसे अस्पताल में भर्ती होना बताकर सीधे पैसे मांग सकते है।



इसके अलावा बैंकिग कार्य, बीमा पालिसी, सिम कार्ड आदि बंद किए जाने/ एक्टिव किये जाने सम्बन्धित तरह-2 की बातें बनाकर पहले आपको डराते हैं और फिर सहायता करने के नाम पर आपसे डिटेल लेकर या कोई लिंक/ एप्लीकेशन डाउनलोड कराकर ठगी का शिकार बनाते हैं।

किसी अन्जान काल पर थोडी सतर्कता बरतें। किसी मदद को लेकर अपनी प्राइवेसी साझा न करें। न ही किसी अपराध को लेकर डरें जो आपने किया ही नहीं। अपनी बातें अपने सम्बन्धियों से साझा करें

9. आनलाइन खरीददारी

जब भी आप olx या किसी अन्य प्लेटफार्मों के माध्यम से किसी पुरानी स्कुटी, फर्नीचर, अच्छे नश्ल के कोई सुंदर जानवर या अन्य कोई वस्तु के विक्रय का प्रमोशन देखते हैं। उक्त वस्तुएं आपको काफी सस्ती लगती हैं। सामान पसन्द आने पर आप उसके नम्बरों पर सम्पर्क करते हैं। कुछ मामले में विक्रेता खुद को आर्मी में होना बताता है। जिसके सम्बन्ध में आपको अपनी फर्जी आईडी ड्रेस फोटो आदि भी दिखाता है।

साथ ही यह भी यह भी कह सकता है कि हाल ही में उसका ट्रांसफर हुआ है। चुकि आर्मी के नाम पर हम आसानी से विश्वास कर लेते हैं ।

इस तरह लोग बडी आसानी से विश्वास कर लेते हैं, और उस वस्तु की खरीददारी करने के लिए तत्पर हो जाते हैं। जालसाज आपसे थोड़ा- थोड़ा करके कई बार में काफी कीमत आपसे ट्रांसफर करा लेते हैं। कभी बताएंगे सामान आधे रास्ते में पहुंचा है, कभी कुछ कभी कुछ।

किसी फर्जी साइट सोशल मीडिया पर सस्ते सामानों के चक्कर में भरोस कर रुपये न दें । सही सामान जब आपको मिल जाये तभी विश्वास करें।

1930

www.cybercrime.gov.in

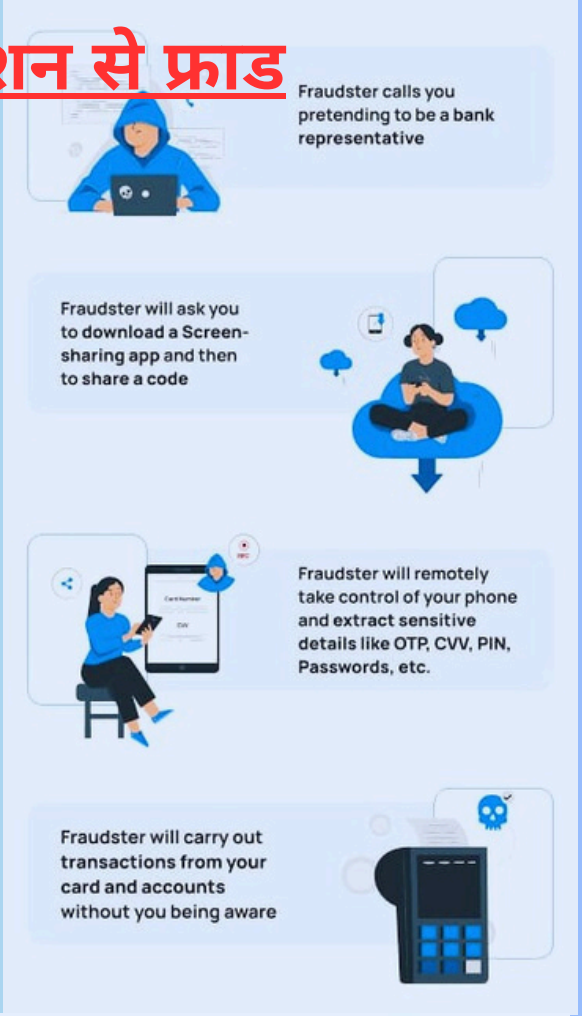
10.आनलाइन बिक्री

- कभी- कभी हम अपनी कोई सम्पत्ति फर्नीचर या अन्य कोई घरेलू सामान बेचने के लिए या मकान किराए पर देने के लिए किसी डिजिटल मर्केटिंग साइट जैसे OLX, Magic Bricks आदि पर डालते हैं। कुछ समय बाद उसके खरीददार की कॉल आती है। अक्सर इस मामले में भी साइबर ठग आर्मी के नाम का इस्तेमाल कर रहे हैं। आपके सामान को पसंद कर उसके लिए आपको कुछ अग्रिम भुगतान भेजने के लिए कहेंगे और दस- पांच रुपए आपके खाते में यूपीआई के माध्यम से डालेंगे। उसके बाद आप पर पैसे की एक औऱ रिक्वेस्ट आयेगी यह रिक्वेस्ट पैसे आने की नहीं बल्कि कटने की रहती है।

- जिस पर लोग ध्यान नहीं देते हैं । इस रिक्वेस्ट के बाद आपसे ट्रांजैक्शन पिन मांगेगा। अगर आप पूछते है कि मेरा पिन क्यों मांग रहा है। इस पर वह आपको भ्रमित करता है कि सुरक्षात्मक लेनदेन के लिए मेरे कंपनी या आर्मी में ऐसा नियम है कि दोनों तरफ से पिन डालने पड़ते हैं वगैरह-2 और जैसे ही आप पिन डालते हैं आपके खाते से पैसे कट जाते हैं ।
- यहां आपको ध्यान देना है कि पैसे प्राप्त करने के लिए न ही कभी पिन नहीं डालना पड़ता है न ही कोई QR कोड स्कैन करना पडता है।

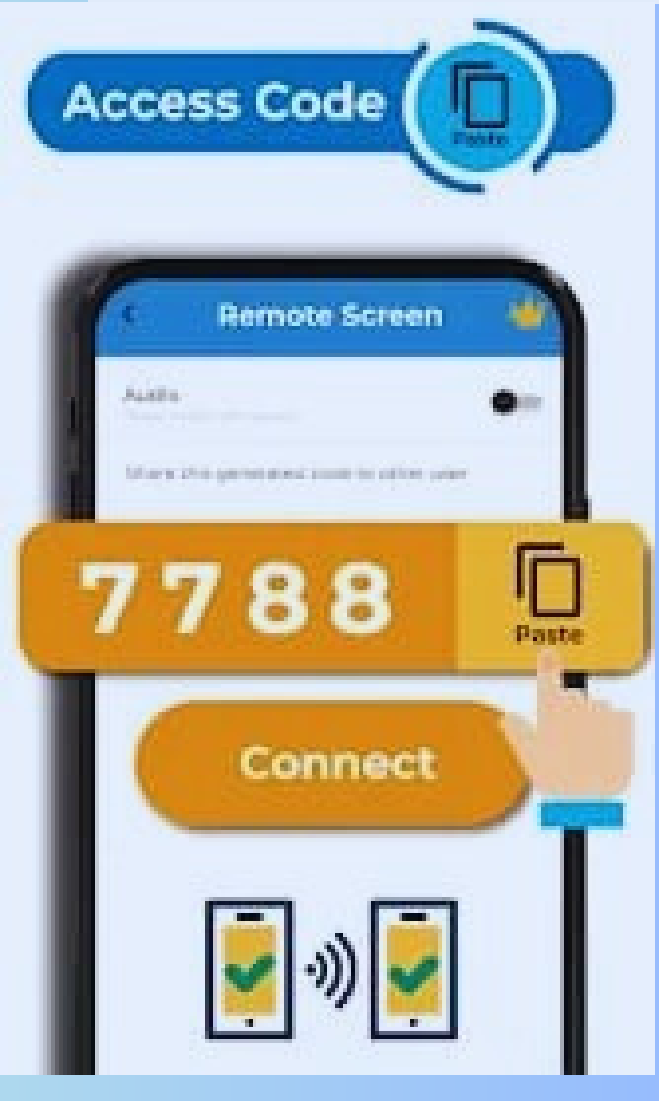
11. स्क्रीन शेयरिंग एप्लीकेशन से फ्राड

आपके मोबाइल/ टैब आदि की स्क्रीन शेयर करने बहुत सारे एप्लीकेशन प्लेस्टोर अथवा अन्य जगहों पर मौजूद हैं। जैसे any desk, rust desk, क्विक सपोर्ट आदि। जहां एक तरफ इसके फायदे हैं वही दूसरी तरफ साइबर अपराधी इसका इस्तेमाल ठगी में बहुत तेजी से कर रहे हैं। साइबर जालसाज आपको किसी न किसी बहाने जैसे- कोई तकनीकी सहायता प्रदान करने के लिए अथवा आनलाइन आपका कोई फॉर्म भरने के बहाने apk फाइल के माध्यम से यह स्क्रीन शेयर ऐप डाउनलोड करा कर उसका कोड पूछता है।



वह कोड बताने पर आपकी स्क्रीन उसके मोबाइल में दिखने लगती है। जिससे वह बडी आसानी से आपके मोबाइल पर आने वाली ओटीपी, आपके द्वारा भरे जाने वाले पिन, पासवर्ड आदि सब कुछ अपने मोबाइल पर देख सकता है। इस तरह से वह बड़ी आसानी से आपके नेट बैंकिंग अथवा upi के द्वारा आपका बैंक अकाउंट खाली कर देता है।

किसी अन्जान व्यक्ति के कहने पर ऐसे ऐप/ apk फाइल डाउनलोड करने से बचें।

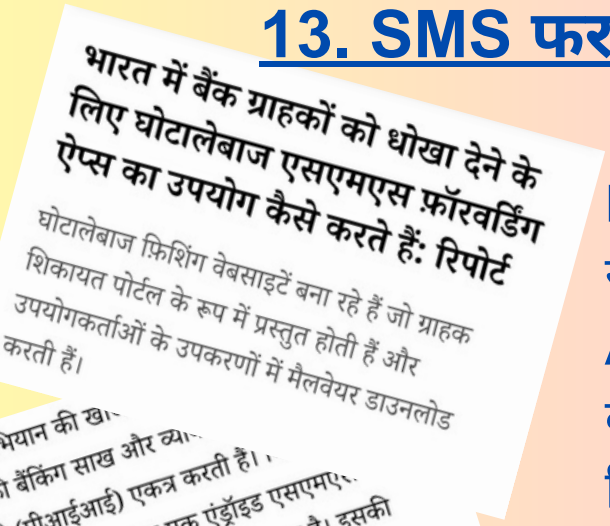


12. क्रेडिट कार्ड फ्राड

जब हम आपना क्रेडिट कार्ड जारी कराने के बाद एक्टिवेट कराते हैं। उसके बाद किसी अनजान नम्बर से काल आती है। कभी लिमिट बढ़ाने की बात कह कर या कोई अन्य बहाना बनाकर साइबर ठगों द्वारा आपके क्रेडिट कार्ड की डिटेल, ओटीपी आदि ले ली जाती है। अथवा किसी फर्जी ऐप के डाउनलोड करने से जिससे ओटीपी सहित हमारे कार्ड की प्राईवेसी लीक हो जा रही है। इस तरह से साइबर ठगों द्वारा हमारे क्रेडिट कार्ड के साथ फ्राड के कुछ समय बाद कभी कभी खरीदारी अथवा ट्रांजैक्शन का मैसेज नहीं आता है तो आपको इसकी जानकारी भी काफी दिन बाद मिल पाती है। क्रेडिट कार्ड फ्राड कुछ आपकी लापरवाही से होता कुछ लापरवाही कम्पनियो की होती है जहां से बल्क में डाटा लीक हो रहा है।

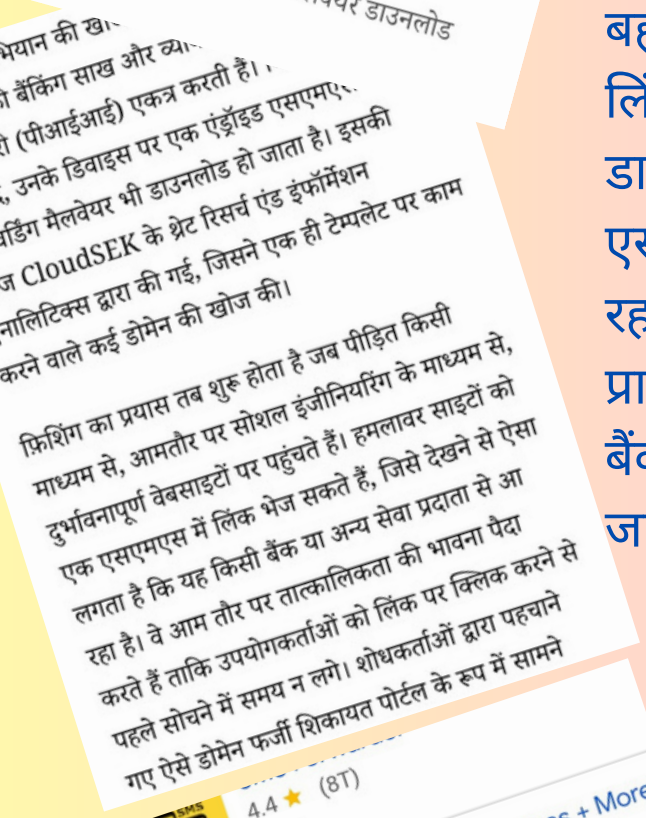
Rakesh Kumar Mishra

13. SMS फरवार्डर व अन्य APK फाइल से फ्राड



भारत में बैंक ग्राहकों को धोखा देने के लिए घोटालेबाज एसएमएस फ़ॉरवर्डिंग ऐप्स का उपयोग कैसे करते हैं: रिपोर्ट

घोटालेबाज फ़िशिंग वेबसाइटें बना रहे हैं जो ग्राहक शिकायत पोर्टल के रूप में प्रस्तुत होती हैं और उपयोगकर्ताओं के उपकरणों में मैलवेयर डाउनलोड करती हैं।



मियान की ख..
ो बैंकिंग साख और व्य..
ो (पीआईआई) एकत्र करती हैं। ,
, उनके डिवाइस पर एक एंड्रॉइड एसएमए..
वर्डिंग मैलवेयर भी डाउनलोड हो जाता है। इसकी
ज CloudSEK के थ्रेट रिसर्च एंड इंफॉर्मेशन
नालिटिक्स द्वारा की गई, जिसने एक ही टेम्पलेट पर काम
करने वाले कई डोमेन की खोज की।

फ़िशिंग का प्रयास तब शुरू होता है जब पीड़ित किसी माध्यम से, आमतौर पर सोशल इंजीनियरिंग के माध्यम से, दुर्भावनापूर्ण वेबसाइटों पर पहुंचते हैं। हमलावर साइटों को एक एसएमएस में लिंक भेज सकते हैं, जिसे देखने से ऐसा लगता है कि यह किसी बैंक या अन्य सेवा प्रदाता से आ रहा है। वे आम तौर पर तात्कालिकता की भावना पैदा करते हैं ताकि उपयोगकर्ताओं को लिंक पर क्लिक करने से पहले सोचने में समय न लगे। शोधकर्ताओं द्वारा पहचाने गए ऐसे डोमेन फर्जी शिकायत पोर्टल के रूप में सामने

4.4 ★ (8T)
Tools
SMS Forwarder: Messages + More
3.6 ★ (1T)
Tools
SMS Messaging & Forwarding
4.0 ★ (414)
Communication · Messaging & video · Me

साइबर अपराधियों द्वारा SMS FARWERDER जैसी फाइलों का इस्तेमाल साइबर ठगी के लिए किया जा रहा हैं। यह ज्यातर APK फाइल के रूप में होती हैं। किसी न किसी बहाने साइबर ठग आपको इस APK फाइल की लिंक भेज कर डाउनलोड करा देता है। इसके डाउनलोड होने के बाद आपके पास आने वाला हर एसएमएस आदि फॉरवर्ड होकर उनके पास जाता रहता है। आपकी कुछ डिटेल वह अन्य माध्यमों से प्राप्त कर लेते है। इस तरह उन लोगों द्वारा आपके बैंक खाता से कैश ट्रांसफर करना बहुत आसान हो जाता है।

कुछ अन्य APK फाइलें ऐसी बनायी जाती हैं। जो बैंक के फॉर्म या अन्य किसी सरकारी योजनाएं के लिए आवेदन करने वाले फॉर्म जैसी होती हैं। फ्राडस्टर आपको उस फाइल/ ऐप को डाउनलोड करा कर उसमे आपको अपनी डिटेल भरने को कहता है। आप आपकी डिटेल जैसे-2 इधर टाइप करते हैं वह दूसरी तरफ साइबर ठगों के सिस्टम में सारी डिटेल प्रिंट होती रहती है।

अत: फर्जी एप्लीकेशन फर्जी / एपीके फाइल डाउनलोड करने से परहेज करें। अपने सिस्टम में समय- समय पर चेक करते रहें

www.cybercrime.gov.in

14.कार्ड स्किमिंग डिवाइस/ कार्ड बदलना

देश भर में बढ़ते साइबर अपराधों के साथ, जालसाज एटीएम कार्ड/ क्रेडिट कार्ड यूजर को कार्ड स्किमिंग डिवाइस के ज़रिए लोगों निशाना बना रहे हैं। यह एक तरह की धोखाधड़ी है जहां अपराधी किसी व्यक्ति के एटीएम डेबिट (ATM DEBIT) या क्रेडिट कार्ड (CREDIT CARD) से जानकारी चुरा लेते हैं। वे अक्सर इसे एक स्किमिंग उपकरणों के द्वारा करते हैं, जो साइबर अपराधियों द्वारा सार्वजनिक स्थानों पर स्थित एटीएम (ATM), गैस पंप (GAS PUMP), या अन्य कार्ड-रीडिंग मशीनों पर स्थापित कर दिये जाते हैं।

जब भी कोई व्यक्ति किसी ऐसे मशीन में अपना कार्ड स्वाइप करता है या डालता है तो इन मशीनों के जरिए कार्ड की पूरी जानकारी सेव हो जाती है, और आपके कार्ड की क्लोनिंग हो जाती है। इन्ही मशीनों के आसपास हिडेन कैमरा भी लगा देते हैं। जिससे आपके द्वारा डाले गए पिन की जानकारी भी साइबर ठगों तक पहूंच जाती है।

इसके अलावा आप जब किसी एटीएम में पैसे निकालने जाते हैं तो हो सकता है वहां ऐसे अपराधिक तत्व पहले से वहां मौजूद हों। यदि आप उनसे सहायता मांगते हैं तो वह आपका पैसा निकालने के बाद उस कार्ड को बदलकर दूसरा कार्ड आपको दे सकते हैं। चुंकि आपकी पिन उन्हें पता चल गयी है और कार्ड भी मिल गया। तो अब आगे क्या होगा हम आप खुद सोच सकते हैं। ऐसें में आप वहां से हटनें से पहले अपना कार्ड ठीक तरह से चेक कर लें।

सावधानी- कार्ड स्वैप करने से पहले एटीएम मशीन स्लॉट के आसपास चेक कर लें। किसी अनजान दुकानदार जिसे आप पहले से न जानते हों अथवा जो अस्थायी दुकानदार हो, उनके यहां कार्ड स्वैप न करें।

1930

15. चार्जिंग केबल/ वाईफाई से डाटा चोरी

कहीं सफर के दौरान किसी अपरिचित व्यक्ति से हम अपना मोबाइल आदि चार्ज करने के लिए उसके चार्जिंग केबल का इस्तेमाल करते है। इसके साथ ही इंटरनेट का इस्तेमाल करने के लिए किसी अपरिचित के वाईफाई से भी कनेक्ट हो जाते है। हमारी यह लापरवाही भी ख़तरनाक हो सकती है। इसके माध्यम से हमारा डाटा चोरी हो सकता है।

हमें ऐसे अपरिचित जगहों पर इन सब चीज़ों को लेकर सावधान रहना चाहिए। किसी अपरिचित व्यक्ति/ दुकानदार से मोबाइल आदि रिपेयर कराना भी असुरक्षित है। यहां भी साइबर ठग आपका डाटा चोरी कर आपके साथ फ्राड कर सकते है। या कोई ऐसा डिवाइस उममें लगा सकते हैं जिससे आपकी प्राइवेसी उन्हें मिलती रहे।

16. फर्जी फेसबुक/ सोशल मीडिया अकाउंट बनाकर फ्राड

सोशल मीडिया का उपयोग करते समय इस बात का ध्यान रखना बहुत आवश्यक है कि आजकल सोशल मीडिया की प्रतिदिन हजारों फर्जी आईडी बनायी जा रही हैं। इसमें ज्यादातर आईडी प्रतिष्ठित लोगों के नाम से बन रही हैं। लोगों की प्रोफाइल पिक्चर डाटा आदि का इस्तेमाल करके फेक आईडी बनाकर पैसों की मांग की जाती है। फर्जी आईडी के साथ साथ लोगों की असावधानी से उनकी फैकबुक, इंस्टाग्राम,या व्हाट्सएप आईडी हैक भी हो जा रही हैं। हैक्ड अकाउंट पर अश्लील तस्वीरें पोस्ट कर लोगों को परेशान करने के साथ, आपके जानने वालों से पैसे की मांग की जाती हैं।

इससे बचने के लिए आपको अपने अकाउंट का टू स्टेप वेरीफिकेशन कर लेना चाहिए। किसी अंजान की फ्रेंड रिक्वेस्ट बिना वेरिफाई किए स्वीकार न करें। किसी के द्वारा पैसों की मांग किए जाने पर अन्य माध्यमों से सच्चाई को जांच परख कर लें। अपनी हर गतिविधि के बारे में अथवा अपने परिजनों की pic आदि सोशल मीडिया पर बहुत ज्यादा अपलोड न करें। साइबर अपराधी इसका भी फायदा उठाकर आपको झासे में ले सकते हैं।

17. जीवनसाथी/ डेटिंग ऐप से धोखाधड़ी

जीवन साथी खोज में अथवा किसी डेटिंग ऐप पर किसी से सम्पर्क में आने से पहले सतर्कता जरूर बरतें। आजकल साइबर ठग फेक आईडी बनकर लोगों के सम्पर्क में आते और उनसे बात करते हैं। धीरे धीरे घनिष्टता बढ़ने पर उनकी डिटेल लेकर ब्लैकमेल कर रहे है अथवा पैसे की भी मांग कर रहे हैं।

यहां आपको अपनी प्राइवेसी, डाटा शेयर करने से बचना है जब तक कि आप उनके बारे में ठीक तरह से जांच परख न कर लें।

18. शहरों/ गांवों में घूम कर धोखाधड़ी

आजकल गांवो/ गलियों में धूमकर ठगी करने वालों की कमी नहीं है। साइबर अपराधी शहरों/ गांवों में घूमकर लोगों को किसी सरकारी योजना में पंजीकरण करने अथवा किसी अन्य योजना जैसे टॉवर, सोलर प्लान्ट लगाने को लेकर अथवा आवास, कृषि, लघु उधोग जैसी किसी योजना का लाभ देने के लिए उसकी धनराशि निकलवाने के बहाने आपकी बैंकिंग डाटा की चोरी कर सकते हैं। ओटीपी लेकर पैसों की ठगी कर सकते हैं।

ऐसा भी हो सकता है कि आपसे आधार कार्ड, पैन कार्ड, हस्ताक्षर आदि लेकर आपके नाम से बैंक खाता खोलकर उसमें फ्राड का पैसा मंगाना शुरू कर दें।

यहां भी आपको ऐसे अंजान लोगों से अपनी प्राइवेसी शेयर करने से बचना है। उन्हें अपना आधार कार्ड, पैन कार्ड अथवा बैंकिंग डिटेल कभी प्रदान न करें।

CONTACT-

19.फेक नोटिस/दस्तावेज से सावधानी

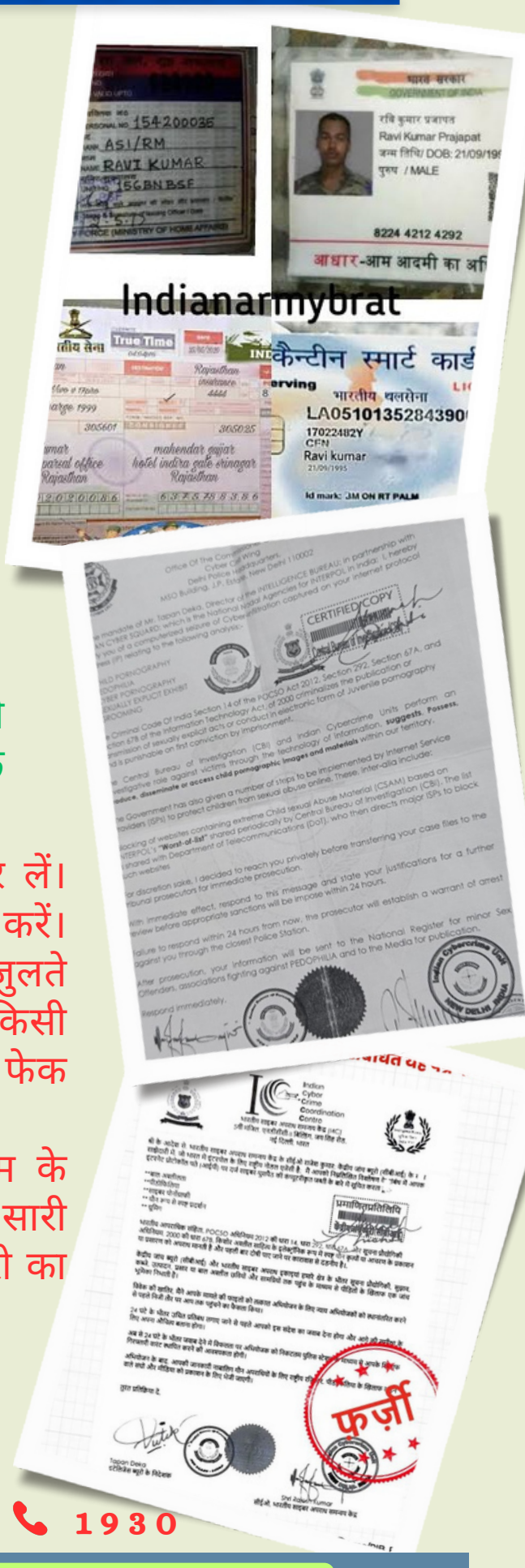
इस समय साइबर अपराधियों द्वारा धोखाधड़ी में विभिन्न प्रकार की फर्जी दस्तावेजों का इस्तेमाल किया जा रहा है। जैसे- कोई आरोप लगाकर पुलिस की किसी जांच एजेंसी के नाम से फर्जी नोटिस/ लेटर आपके ह्वाट्सएप/ ईमेल पर भेजकर आपको डराकर पैसे लेने के लिए ।

इसके अलावा ऑनलाइन खरीद बिक्री करने के लिए अथवा आनलाइन अन्य किसी गतिविधि के दौरान साइबर अपराधियों द्वारा किसी सैन्य कर्मी के नाम की आईडी का उपयोग बहुतायत किया जा रहा है।

ऐसे फर्जी दस्तावेजों पर विश्वास करने से पहले कुछ टिप्स अपना कर आप इनके फेक होने की जांच कर सकते हैं।

पहले उस दस्तावेज को गैलरी में सेव कर लें। फिर क्रोम पर जाकर गूगल लेंस पर स्कैन करें। आपको उसी उसी प्रकार अथवा उससे मिलते जुलते बहुत सारे दस्तावेज सोशल मीडिया अथवा किसी वेबसाइट पर मिल जायेंगी। इससे आप उसके फेक होने की पहचान कर सकते हैं।

इसके अलावा PIB FACT CHECKनाम के फेसबुक/ ट्वीटर प्लेटफॉर्म पर जाकर बहुत सारी फर्जी पत्र/ न्यूज के बारे समय-2 पर सूचना जारी का जाती हैं।



REGISTER YOUR COMPLAIN

WWW.CYBERCRIME.GOV.IN

1930

20.साइबर अपराध का नया ट्रेंड डिजिटल अरेस्ट

साइबर धोखाधड़ी यह ट्रेंड वर्तमान में काफी प्रचलित हैं । इसकी शुरुआत साइबर अपराधी ऑडियो कॉल अथवा वीडियो कॉल से करते हैं और कॉल के माध्यम से लोगों पर कोई न कोई आरोप लगाकर इतना डर भर देते है कि वह व्यक्ति डर के कारण अपने ही घर में कैद होकर रह जाता है ।

। वह अपनी बात किसी से कह नहीं पाता । साइबर अपराधी टारगेट व्यक्ति को तबतक संपर्क में बने रहने तथा विडियो कॉल पर ज्यादा समय बिताने और किसी को यह बात न बताने का प्रेशर दिया जाता है जबतक वह रुपए ट्रांसफर नहीं कर देता । वीडियो कॉल के माध्यम से उनलोगों द्वारा ऐसा बैक ग्राउंड क्रिएट किया जाता है कि वह कॉल आपको किसी पुलिस अधिकारी, किसी सरकारी जांच एजेंसी सीबीआई, ईडी, इनकम टैक्स विभाग आदि की लगती है । इससे डर कर लोग लाखों रुपए ट्रांसफर कर देते है।

साइबर अपराधी आरोप क्या लगाते हैं

पार्सल घोटाला: साइबर अपराधियों द्वारा यह आरोप लगाया जाता है कि एक अवैध पार्सल आपके नाम से पकड़ा गया है जिसमें ड्रग्स/ अवैध सामग्री विदेश भेजी जा रही है।

परिवार के सदस्यों की संलिप्तता: घोटालेबाज दावा करते हैं कि परिवार का कोई सदस्य अपराध में शामिल है जैसे रेप केस, मनी लांड्रिंग आदि और उसे तत्काल वित्तीय सहायता की आवश्यकता है।

आधार या फ़ोन नंबर का दुरुपयोग: पीड़ित पर अपने आधार या फ़ोन नंबर का अवैध गतिविधियों के लिए उपयोग करने का आरोप लगाया जाता है ।

पोर्न वीडियो देखने अथवा अपलोड करने का आरोप: पीड़ित पर ठगों द्वारा पोर्न वीडियो देखने और अपलोड करने का आरोप लगाया जाता है ।

कैसे बचें-

इस तरह किसी कॉल के आने पर डरें नहीं अपनी बात लोगों से शेयर करें । साथ ही अपने नजदीकी पुलिस स्टेशन अथवा साइबर सेल से संपर्क करें, और हां एक राज को बात और सरकारी लोगों में भी डर का आलम यह है कि वह ऑनलाइन लाइन पैसा तो ले ही नहीं सकता । तो इतना लॉजिक तो लगा ही सकते हैं कि कौनो फिरकी ले रहा है।

नोट - किसी भी जांच प्रक्रिया में किसी भी जांच एजेंसी द्वारा जांच के दौरान डिजिटल अरेस्ट जैसा कोई भी कानूनी प्रावधान नहीं है।

REGISTER YOUR COMPLAIN

WWW,CYBERCRIME.GOV.IN

1930

CYBER CRIME CELL
POLICE COMMISSIONERAT LUCKNOW

RAKESH KUMAR MISHRA CYBER CRIME CELL LKO

निष्कर्ष

जैसा कि अब तक तमाम केशों के अध्ययन से हमें यही ज्ञात होता है कि साइबर ठगों द्वारा ज्यादातर मामलों में लोगों को किसी न किसी बातो में गुमराह किया जाता हैं। जिसके झासे में आकर अक्सर लोगों द्वारा खुद ही रुपये ट्रांसफर कर दिये जा रहे हैं। चुंकि मानव जीवन की दैनिक गतिविधि व प्रवृत्ति लगभग समान होती है। इसके साथ-2 हम बहुत सारी बातों को सोशल मीडिया पर डालते रहते हैं। लोगों द्वारा डाली गयी पोस्ट को देखकर उनकी सोच, मनोदशा, दैनिक जीवन उनकी आवश्यकता आदि का अनुमान भी लगाया जा सकता हैं। सामान्यतया इसी के अनुसार अपराधियों द्वारा नये- नये तरीको का प्रयोग किया जाता है। डिजिटल वर्ल्ड में साइबर अपराधियों द्वारा हर जगह मछली फंसाने जैसी कटिया बिछाई जा रखी है जिससे हमें हर जगह सतर्क व सावधान रहना है।

Stop dreaming and start doing

साइबर ठग अक्सर हमारी लालच, डर, इमोशन वर्तमान जरुरत और हमारी भागदौड़ भरी जिन्दगी जहां हम दो मिनट रुककर सोचते नहीं, आत्म चिंतन नहीं करते, उसी का फायदा उठाते हैं।

RAKESH KUMAR MISHRA CYBER CRIME CELL
HAZRATGANJ LUCKNOW

डर

साइबर अपराधी हमारे अंदर किसी न किसी चीज का डर भरते है। जैसे- किसी अपराध में संलिप्तता को लेकर पुलिस, सीबीआई का डर। जैसे आपके नाम से कोई अवैध पार्सल पकड़ा गया। आपके किसी सम्बन्धी को किसी अपराध में पकड़ा गया है।

आपके किसी बैंकिंग सुविधा बन्द करने, क्रेडिट कार्ड, सिम कार्ड आदि ब्लॉक किए जाने का डर बनाकर। किसी न किसी प्रक्रिया के बहाने आपसे पैसे प्राप्त कर लेते हैं।

उस डर का सामना करने में हमें समझदारी दिखानी है।

लालच

अक्सर हम लालच में पड़कर बहुत जल्दी अपने पैसे को डबल करने के चक्कर में पड़ जाते हैं। साइबर अपराधी फर्जी प्लेटफॉर्म पर फर्जी क्रिप्टो में निवेश करा देते हैं। पैसा तो उनके ठगी करने वाले के खाते में चला जाता है। और आपकी राशि उस वेबसाइट पर केवल शो करती है। उसका आप उपयोग नहीं कर सकते। कंपनी कभी घाटे का बहाना करती है, कभी सर्वर की समस्या बताती है। लालच पैसों का भी हो सकता है या फिर लालच विपरीत जेंडर के आकर्षण का भी ।

इमोशन

दूसरों की समस्यायों के प्रति संवेदनशील होना उसकी मदद के लिए तत्पर रहना अच्छी बात है। परन्तु यहां हमें इस बात का ध्यान रखना चाहिए कि हम फ़ोन कॉल अथवा सोशल मीडिया पर विश्वास करके जिस व्यक्ति की मदद करने जा रहे हैं वह वही व्यक्ति है जिसे हम ऑनलाइन देख रहे हैं।

24/7

FREE CONSULTATION

आवश्यकता

हमारे दैनिक जीवन में अक्सर कोई न कोई डिजिटल या फिजिकल (स्वाश्थ्य) समस्या आती रहती है। जिसके क्रम में हम जब हम अपनी स्वास्थ्य सम्बन्धित समस्या अथवा----

किसी तकनीकी समस्या जैसे- बैंकिग, जॉब, शिक्षा अथवा कहीं यात्रा को लेकर आदि। इन समस्याओं का निदान/ सहायता के लिए लिए हम ऑनलाइन सर्च करते हैं। यहीं हमारा सम्पर्क साइबर ठगों से हो जाता है।

अनभिज्ञयता

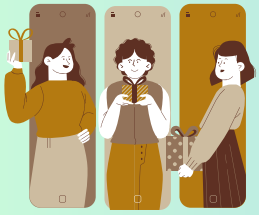
कम्प्यूटर युग में हम कभी पूर्ण विशेषज्ञ नहीं हो सकते हैं। प्रतिदिन नई नई चीजें सामने आती रहती हैं। साइबर अपराध के इस दौर में हमारी सतर्कता व presence of mind बहुत जरुरी है। मानव जीवन में गलतियां नैसर्गिक हैं, परन्तु कुछ लापरवाही हमलोगों से ऐसी हो जाती हैं, जिसके लिए हमें बाद में अफसोस होता है।

समय निकाल कर कुछ न कुछ अपने सामान्य जीवन की दैनिक गतिविधियों के साथ आसपास हो रही घटनाओं के सम्बन्ध में खुद को अपडेट रखना चाहिए। साइबर अपराध से सम्बन्धित घटनाओं व सावधानियों के बारे में बहुत सारी जानकारियां वेब पर मौजूद हैं।

1930

क्या करें क्या न करें

1.किसी अनजान काल पर विश्वास कर आपकी व्यक्तिगत बैंकिंग जानकारी शेयर नहीं करना है। परिचित जैसी आवाज लगने पर भी अन्य स्रोतों से उसे वेरिफाई कर लें।

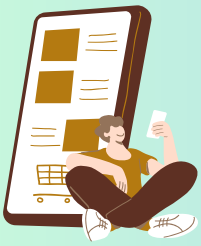


2.व्हाट्सएप, फेसबुक, या किसी अन्य ऐप/ वेबसाइट पर किसी फर्जी लिंक पर क्लिक न करें।

3.फ़ोन पर कोई पुलिस अधिकारी बन कर किसी कानूनी कार्यवाही का डर दिखाकर पैसों कि मांग करता है तो उसपर विश्वास न करें।

4.सोशल मीडिया पर किसी अनजान से दोस्ती न करें।

5.अनावश्यक एप्लीकेशन डाउनलोड करने बचें। फ्री की अनावश्यक किसी वेबसाइट पर सर्चिंग न करें, क्योंकि एप्लीकेशन डाउनलोड करने के उपरांत हम गैलरी, कॉन्टैक्ट, विडियो आदि का एक्सेस देते हैं। इससे हमारी प्राइवेसी का भंग होती है।



6.अपने बैंक खाते में अपने रजिस्टर्ड नम्बर का SMS अलर्ट एक्टिव रखे। फ़ोन नम्बर यदि बदल दिया है या खो गया है और उसी नम्बर का दूसरा सिम नहीं जारी करवाए हैं तो बैंक में नया नम्बर अपडेट कराएं।