साइबर ठगी के नये तरीके से सावधान रहने की जरूरत

लोगों को ठगने के लिए साइबर अपराधी हर रोज नये तरीके विकसित कर रहे हैं. ऐसा ही एक नया तरीका है डिजिटल अरेस्ट का. इस तकनीक के जरिये अपराधी लोगों के भय का दोहन कर उनसे लाखों-करोड़ों रुपये किसी अन्य खाते में ट्रांसफर करा रहे हैं. एक नजर डिजिटल अरेस्ट पर.

क्या है डिजिटल अरेस्ट

डिजिटल अरेस्ट में कहीं और बैठे साइबर अपराधी फोन या वीडियो कॉल के माध्यम से लोगों को डराते-धमकाते हैं. वे खुद को पुलिस या दूसरी सरकारी एजेंसी का अधिकारी बता पीड़ित को भयभीत करते हैं, उन्हें गिरफ्तारी का डर दिखाते हैं. यह सब कुछ पीड़ित को ठगने के लिए किया जाता है. कुछ मामलों में तो पीड़ित को डिजिटल रूप से गिरफ्तार भी किया जाता है और जब तक वे पैसे नहीं दे देते, तब तक उन्हें डरा-धमकाकर वीडियो कॉल पर बने रहने के लिए बाध्य किया जाता है. इन दिनों इस तरह के कई मामले सामने आये हैं. दूसरे शब्दों में कहा जाये, तो डिजिटल अरेस्ट साइबर अपराध का एक नया तरीका है, जिसका उद्देश्य पैसों की ठगी है. इस तरह के अपराध दूसरे देशों में मौजूद साइबर अपराध गिरोह द्वारा किये जा रहे हैं.

इन तरीकों से लोगों को फंसाते हैं अपराधी

साइबर अपराध के इस नये तरीके में अपराधियों का तरीका पूर्व के तरीकों से एकदम अलग और हटकर है. जहां कुछ समय तक तो पीड़ित ठगों के नियंत्रण में रहता है और कुछ भी कर पाने मे अपने आपको असहाय पाता है.

- पीड़ित को अपनी जाल में फंसाने के लिए साइबर ठग सबसे पहले एसएमएस, इमेल या व्हाट्सएप के जरिये मैसेज भेज उनसे संपर्क साधते हैं कि आपके नाम या फोन नंबर को आपराधिक गतिविधियों में संलिप्त पाया गया है.
- इसके बाद अपराधी पीड़ित को ऑडियो या वीडियो कॉल करते हैं और अपने आपको सीबीआई, कस्टम, ईडी, नारकोटिक्स, टैक्स आरबीआई, ट्राई के अधिकारी बताते हैं.
- इसके बाद वे पीड़ित को डराते हैं कि उनके नाम का कोई कूरियर या पार्सल आया है, या पीड़ित ने वह पार्सल किसी दूसरे को भेजा है, जिसमें मादक पदार्थ, नकली पासपोर्ट, नकली पहचान पत्र, अवैध वस्तु, या प्रतिबंधित सामान है. अपराधी पीड़ित को अपने काबू में करने के लिए यह भी कहते हैं कि आपके खाते से ट्रांजैक्शन हुआ है और यह वित्तीय धोखाधड़ी का मामला बनता है.
- पीड़ित को अपने जाल में फंसा लेने के बाद धोखेबाज उसे एक ही जगह पर रहने के लिए मजबूर कर देते हैं. इस तरह के मामले में पीड़ित अक्सर अपने ही घर में कैद हो जाता है और ठगों की हर बात मानने लगता है. अपनी सारी निजी जानकारियां उनसे साझा करता है. यहां तक कि उसके बैंक खाते में कितने पैसे हैं यह भी. उसके बाद ठग मामले को बंद करने या समझौता करने के लिए

पैसों की मांग करते हैं. ठगों का इतना खौफ होता है कि डिजिटली अरेस्ट व्यक्ति अपनी जमा-पूंजी धोखेबाजों द्वारा बताये खाते में हस्तातरित कर देता है. जब तक उसे कुछ समझ आता है, उसकी सारी कमाई लुट चुकी होती है.

- डिजिटल गिरफ्तारी में पीड़ित को यह भी बताया जा सकता है कि उसका कोई करीबी रिश्तेदार या दोस्त किसी अपराध में शामिल है और अब हिरासत में है. इस तरह की मनगढ़ंत कहानियों के जरिये साइबर ठग पीड़ित से लाखों या करोड़ों की ठगी कर सकते हैं.

हूबहू सरकारी कार्यालय जैसा सेटअप

- साइबर ठग जिस स्थान से वीडियो कॉल करते हैं वह स्थान बिल्कुल पुलिस स्टेशन या सरकारी एजेंसी के कार्यालय जैसा होता है. यह सब कुछ पीड़ित को चकमा देने के लिए किया जाता है.
- कॉल करने वाला व्यक्ति पुलिस या अन्य सरकारी अधिकारी की तरह यूनिफॉर्म में होता है, जो देखने में बिल्कुल असली लगता है.
- अपराधी जहां से कॉल करता है वहां बैकग्राउंड में पुलिस सायरन बज रहा होता है. इसके साथ ही वह अपनी फर्जी आइडी भी भेजता है, ताकि गिरफ्तारी वास्तविक लगे, पीड़ित को ठगों पर जरा सा भी शक न हो और वह भयभीत बना रहे.

ठगने के लिए इन हथकंडों का होता है इस्तेमाल

डिजिटल फ्रॉड का शिकार वही लोग होते हैं, जिनके पैन व आधार कार्ड समेत दूसरी गोपनीय जानकारियों को गलत तरीके से ठगों द्वारा एकत्र किया जाता है. इनके जरिये साइबर ठग पीड़ित से जुड़ी कई जानकारियों को जुटा लेते हैं. फिर उनके भय का दोहन कर फिरौती मांगते हैं. बैंक खाते में पैसे न होने पर ये लोन देने वाले एप्स के जरिये पीड़ित को लोन भी दिलवाते हैं.