डीजी परिपत्र सं0-21/2025

राजीव कृष्णा, IPS
पुलिस महानिदेशक एवं
राज्य पुलिस प्रमुख, उत्तर प्रदेश

मुख्यालय पुलिस महानिदेशक, उ0प्र0
सिग्नेचर बिल्डिंग
शहीद पथ, गोमती नगर विस्तार,
लखनऊ – 226002
फोन नं.0522–2724003 / 2390240, फैक्स नं.0522–2724009
सीयूजी नं. 9454400101
ई–मेल : police.up@nic.in
वेबसाईट : https://uppolice.gov.in
दिनांक- जुलाई 14, 2025

विषय: Digital Arrest Cyber Scam की रोकथाम हेतु जन जागरूकता अभियान एवं पुलिस कार्यवाही के लिए निर्देश।

प्रिय महोदय / महोदया,

जैसा कि आप अवगत हैं कि आधुनिक युग में प्रौद्योगिकी के बढ़ते उपयोग के साथ-साथ साइबर अपराधों में भी वृद्धि हुई है। इनमें से एक नवीन तथा तेजी से बढ़ता अपराध है डिजिटल अरेस्ट, जो हाल के वर्षों में भारत में मुख्य रूप से चर्चा का विषय बन गया है। डिजिटल अरेस्ट एक ऐसी धोखाधड़ी है जिसमें साइबर अपराधी स्वयं को पुलिस, सी0बी0आई0, ईडी (प्रवर्तन निदेशालय), एन0सी0बी0 या अन्य सरकारी अधिकारियों के रूप में आनलाइन प्रस्तुत करके लोगों को डराता हैं और उनसे रूपयों की ठगी करता है। इस साइबर अपराध में स्कैमर्स लोगों को पैसे ट्रान्सफर करने या संवेदनशील व्यक्तिगत जानकारी साझा करने के लिए नकली गिरफ्तारी वारंट, मनगढ़ंत सबूत और मनोवैज्ञानिक दबाव (मनी लॉन्ड्रिंग, ड्रग्स तस्करी या अन्य गंभीर अपराध) बनाकर उसे "डिजिटल रूप से गिरफ्तार" किये जाने का भय दिखाता है।

2. डिजिटल अरेस्ट अपराध की कार्य पद्धतिः

- साइबर अपराधी पुलिस, सी0बी0आई0, एन0सी0बी0, एयरपोर्ट अधिकारी या साइबर क्राइम इकाइयों से होने का दावा करते हुए फोन कॉल, व्हाट्सएप मैसेज या ईमेल के माध्यम से संपर्क करते हैं।
- वे पीड़ित पर मनी लॉन्ड्रिंग, अवैध लेनदेन करने जैसे तस्करी (Drugs) अपराधों में सम्मिलित होने का आरोप लगाते हैं।
- साइबर अपराधी पीड़ितों को यह विश्वास दिलाने के लिए आधिकारिक दिखने वाले दस्तावेज़, स्क्रीनशॉट या यहाँ तक कि डीपफेक वीडियो भी भेजते हैं।
- फर्जी थाने/कोर्ट आदि के Fake Getup का प्रयोग करते हैं।
- तत्पश्चात वे जुर्माना या "जमानत राशि" का भुगतान न किए जाने पर तुरंत कानूनी कार्यवाही, जिसमें गिरफ़्तारी भी शामिल है, की धमकी देते हैं।
- डिजिटल अरेस्ट अपराध अधिकांशतः दक्षिण-पूर्व एशियाई देशों (म्यांमार, लाओस, कंबोडिया) से संचालित होते हैं।

3. डिजिटल अरेस्ट अपराध पंजीकृत प्रथम सूचना रिपोर्ट वर्षवार आंकड़े:

वर्ष	पंजीकृत प्र0सू0रि0
2023	18
2024	196

डिजिटल अरेस्ट अपराध की रोकथाम में निम्नलिखित **मंत्रालय और एजेंसियां सक्रिय** रूप से कार्य कर रही हैं:

i. **गृह मंत्रालय (Ministry of Home Affairs - MHA):**

- भारतीय साइबर अपराध समन्वय केंद्र (I4C) गृह मंत्रालय, डिजिटल अरेस्ट और साइबर अपराधों से निपटने के लिए समय-समय पर दिशानिर्देश एवं Advisory जारी करता है। यह विभिन्न एजेंसियों, राज्यों और केंद्र शासित प्रदेशों की पुलिस को तकनीकी सहायता और इनपुट प्रदान करता है तथा समन्वय स्थापित करता है। I4C द्वारा अपराध में प्रयुक्त फर्जी स्काइप आईडी और मोबाइल नंबरों/टेलीग्राम चैनलों को ब्लॉक कराया जा रहा है।
- राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (National Cyber Crime Reporting Portal- https://cybercrime.gov.in) नागरिकों को डिजिटल अरेस्ट और अन्य साइबर अपराधों की शिकायत दर्ज करने की सुविधा प्रदान करता है। यह त्वरित कार्यवाही के लिए I4C और अन्य एजेंसियों के साथ समन्वय करता है।
- साइबर दोस्त, I4C- गृह मंत्रालय, भारत सरकार द्वारा संचालित एक X-Handle है जो साइबर सुरक्षा जागरूकता पर केंद्रित है। इसका उद्देश्य लोगों को साइबर खतरों से बचाना और साइबर अपराधों के बारे में जागरूक करना है।

ii. **इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (MeitY):**

- कंप्यूटर इमरजेंसी रिस्पॉन्स टीम ऑफ इंडिया (CERT-In), इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (MeitY) के अंतर्गत कार्य करता है तथा साइबर सुरक्षा सुनिश्चित करने और साइबर ठगी के तरीकों की पहचान करने में महत्वपूर्ण भूमिका निभाता है। यह डिजिटल अरेस्ट जैसे अपराधों से निपटने के लिए तकनीकी समाधान प्रदान करता है।
- साइबर स्वच्छता केंद्र, MeitY के अंतर्गत यह केंद्र साइबर सुरक्षा को बढ़ावा देता है और डिजिटल अरेस्ट जैसे अपराधों से बचाव के लिए जागरूकता अभियान चलाता है।

iii. **दूरसंचार विभाग (DoT),** टेलीकॉम कंपनियों के साथ समन्वय कर डिजिटल अरेस्ट स्कैम में उपयोग किए जा रहे फर्जी सिम कार्ड और मोबाइल नंबरों को ब्लॉक कराता हैं।

iv. **भारतीय रिजर्व बैंक (Reserve Bank of India- RBI),** आरबीआई साइबर ठगी से संबंधित वित्तीय लेनदेन की निगरानी और फर्जी बैंक खातों को फ्रीज करने में सहायता करता है।

v. **केंद्रीय जांच ब्यूरो (Central Bureau of Investigation - CBI),** डिजिटल अरेस्ट जैसे संगठित साइबर अपराधों की जांच में शामिल होती है, विशेष रूप से जब ये अपराध अंतरराष्ट्रीय स्तर पर संचालित होते हैं।

LEAs एवं उपरोक्त के संयुक्त प्रयासों से Digital Arrest Scam की रोकथाम के लिए जागरूकता, तकनीकी सहायता, और कानूनी कार्यवाही सुनिश्चित की जा रही है।

5. **माननीय प्रधानमंत्री भारत सरकार** द्वारा भी देश में डिजिटल अरेस्ट स्कैम के बढ़ते मामलों को देखते हुए दिनांक 27 अक्टूबर, 2024 को "मन की बात" कार्यक्रम के सम्बोधन में जनता को इस अपराध से सावधान करते हुये डिजिटल सुरक्षा के तीन कदम **'रोको-सोचो-कार्यवाही करो'** बताये थे। वर्तमान में भी साइबर अपराधी लोगों के साथ डिजिटल अरेस्ट अपराधिक कार्यप्रणाली का प्रयोग कर साइबर अपराध कर रहे हैं इसके दृष्टिगत जनता को इस साइबर अपराध के प्रति जागरूक करने और इसकी रोकथाम के लिए **निम्न कार्यवाही अपेक्षित** है-

जागरूकता अभियान का संचालन:

- जागरूकता कार्यक्रम/कार्यशालाएं-

A. स्थानीय समुदायों, विशेष रूप से बुजुर्गों और कम तकनीकी जानकारी रखने वाले लोगों के बीच डिजिटल अरेस्ट स्कैम के बारे में जागरूकता फैलाने के लिए अभियान चलाएं।

B. सार्वजनिक स्थानों, सामुदायिक केंद्रों, और सोशल मीडिया प्लेटफॉर्म्स पर जागरूकता सामग्री (पोस्टर, वीडियो, और सोशल मीडिया पोस्ट) वितरित करें।

C. माह के प्रत्येक प्रथम बुधवार को साइबर जागरूकता दिवस के रूप में मनाये जाने के निर्देश आपको पूर्व में दिये गये हैं, इसका प्रभावी रूप से क्रियान्वन जागरूकता कार्यक्रम आयोजित कराकर कराया जाये।

D. स्थानीय पुलिस स्टेशनों में स्थापित साइबर हेल्प डेस्क के माध्यम से डिजिटल अरेस्ट साइबर अपराध एवं साइबर हेल्पलाइन नंबर (1930) से सम्बन्धित जागरूकता कार्यक्रम स्थानीय स्तर पर आयोजित करायें।

- मुख्य जागरूकता बिंदु-

a) जनता को शिक्षित करें कि डिजिटल अरेस्ट का कोई कानूनी प्रावधान नहीं है।

b) लोगों को सूचित करें कि कोई भी सरकारी एजेंसी वीडियो कॉल, व्हाट्सएप, या स्काइप के माध्यम से पूछताछ या गिरफ्तारी नहीं करती।

c) जनता को सूचित करें कि पुलिस या सरकारी एजेंसी कभी भी वीडियो कॉल पर व्यक्तिगत जानकारी, बैंक विवरण, या पैसे की मांग नहीं करती।

d) लोगों को सलाह दें कि वे अनजान नंबरों से आने वाली कॉल्स पर तुरंत विश्वास न करें और ऐसी कॉल्स को तत्काल काट दें।

e) संदिग्ध कॉल्स या घटित साइबर अपराध की घटना की शिकायत अविलम्ब (Golden Hour) राष्ट्रीय साइबर अपराध पोर्टल (https://cybercrime.gov.in) या हेल्पलाइन नंबर 1930 पर करने के लिए प्रोत्साहित करें।

f) कथित एजेंसी के आधिकारिक चैनलों (फ़ोन नंबर या वेबसाइट) से संपर्क कर जानकारी करें।

g) आम साइबर घोटालों और उन्हें पहचानने के तरीके के बारे में जानकारी रखें।

h) अनचाहे कॉल से सावधान रहें, खासकर उन कॉल से जिनमें धमकियाँ या पैसे की माँग शामिल हो। साइबर जागरूकता महत्वपूर्ण है, क्योंकि वे भय, धमकी और गलत सूचना पर निर्भर करते हैं।

I. पुलिस कार्यवाही और जांच:

A. डिजिटल अरेस्ट स्कैम से संबंधित शिकायतों को प्राथमिकता के आधार पर दर्ज करें और अविलम्ब जांच प्रारम्भ करें।

B. साइबर ठगों द्वारा उपयोग किए जाने वाले फर्जी सिम कार्ड, व्हाट्सएप अकाउंट्स, और स्काइप आईडी की पहचान करें और उन्हें ब्लॉक करने के लिए टेलीकॉम सेवा प्रदाताओं के साथ समन्वय करें।

C. अंतरराष्ट्रीय साइबर अपराध सिंडिकेट्स, विशेष रूप से दक्षिण-पूर्व एशियाई देशों (म्यांमार, कंबोडिया, लाओस) से संचालित होने वाले नेटवर्क के विरुद्ध कार्यवाही के लिए भारतीय साइबर अपराध समन्वय केंद्र (I4C) एवं अन्य केंद्रीय एजेंसियों के साथ सहयोग करें।

D. बैंकों और वित्तीय संस्थानों के साथ मिलकर संदिग्ध खातों को फ्रीज करने और ठगे गए धन की रिकवरी के लिए त्वरित कार्यवाही करें।

E. स्थानीय समुदाय, गैर-सरकारी संगठनों, और मीडिया के साथ मिलकर जागरूकता अभियान को और प्रभावी बनाएं।

6. उपरोक्त निर्देशों का कड़ाई से पालन करते हुए, आप न केवल डिजिटल अरेस्ट स्कैम के खिलाफ प्रभावी कार्यवाही कर सकते हैं, बल्कि जनता को जागरूक कर इस अपराध को कम करने में भी महत्वपूर्ण योगदान दे सकते हैं। अतः आपसे अपेक्षा है कि दिए गए निर्देशों का कड़ाई से अनुपालन करें तथा साइबर क्राइम मुख्यालय द्वारा आख्या मांगे जाने पर प्रेषित करें।

भवदीय,

14/7

(श्रजीव कृष्णा)

1. समस्त पुलिस आयुक्त, उत्तर प्रदेश।
2. समस्त वरिष्ठ पुलिस अधीक्षक/पुलिस अधीक्षक, प्रभारी जनपद, उत्तर प्रदेश।

<u>प्रतिलिपि:</u> निम्नलिखित को सूचनार्थ एवं आवश्यक कार्यवाही हेतु :-

1. समस्त अपर पुलिस महानिदेशक, उ०प्र०, लखनऊ।
2. समस्त जोनल अपर पुलिस महानिदेशक, उ०प्र०।
3. पुलिस महानिरीक्षक (कानून एवं व्यवस्था), उ०प्र०, लखनऊ।
4. समस्त परिक्षेत्रीय पुलिस महानिरीक्षक / पुलिस उपमहानिरीक्षक, उ०प्र०।