नवंबर, 2024

केंद्रीय रिज़र्व पुलिस बल

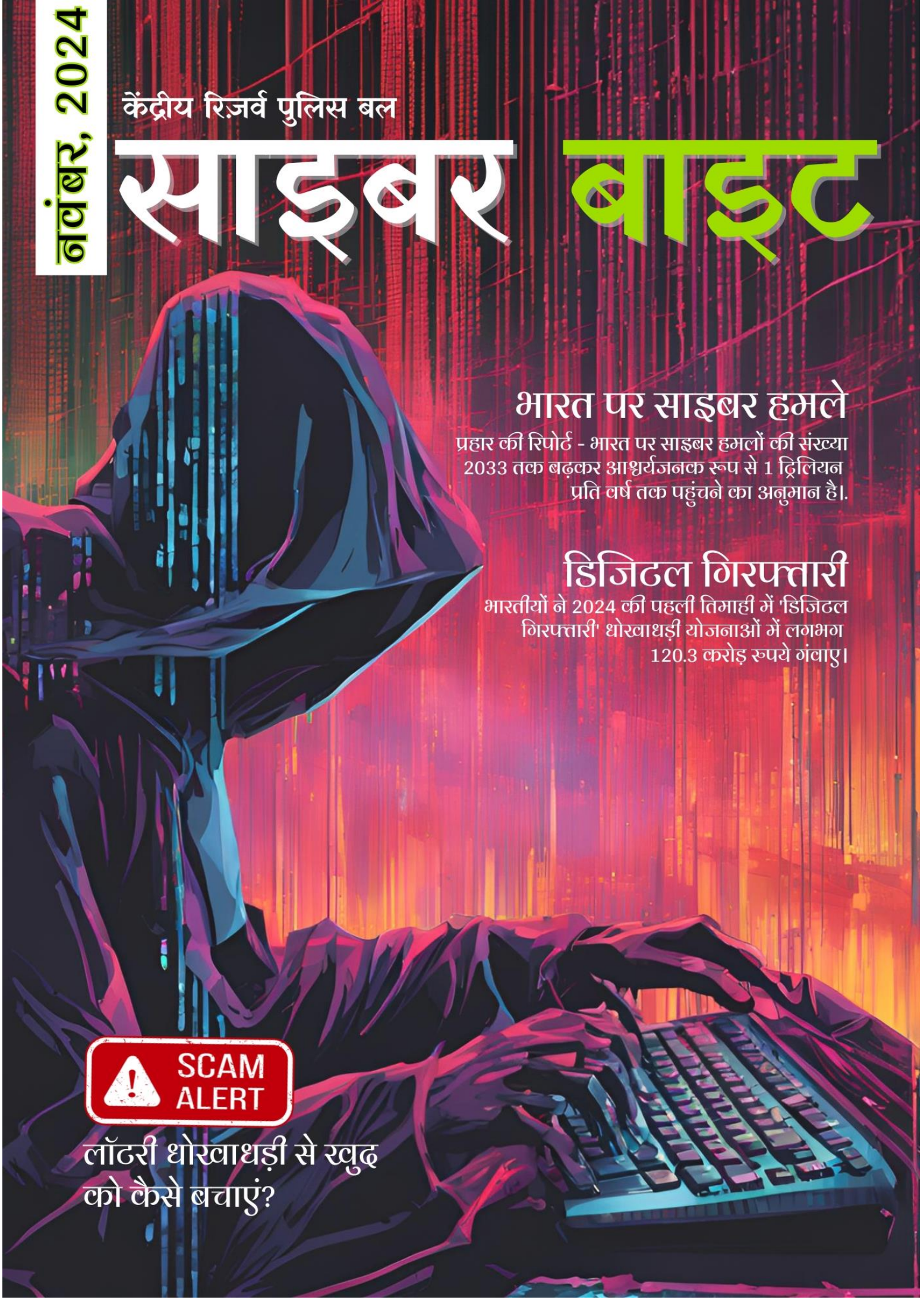
साइबर बाइट

भारत पर साइबर हमले

प्रहार की रिपोर्ट - भारत पर साइबर हमलों की संख्या 2033 तक बढ़कर आश्चर्यजनक रूप से 1 ट्रिलियन प्रति वर्ष तक पहुंचने का अनुमान है।.

डिजिटल गिरफ्तारी

भारतीयों ने 2024 की पहली तिमाही में 'डिजिटल गिरफ्तारी' धोखाधड़ी योजनाओं में लगभग 120.3 करोड़ रूपये गंवाए।



लॉटरी धोखाधड़ी से खुद को कैसे बचाएं?

1.साइबर गीक न्यूज

ए) अनुमान है कि वर्ष 2033 तक भारत पर साइबर हमले प्रति वर्ष 1 ट्रिलियन तक बढ़ जाएंगे।

वर्ष 2033 तक भारत पर साइबर हमले प्रतिवर्ष 1 ट्रिलियन तक बढ़ने का अनुमान है और वर्ष 2047 तक यह आंकड़ा 17 ट्रिलियन तक पहुंच जाने का अनुमान है जब देश 100 वर्ष का हो जाएगा, ऐसा प्रहार (पब्लिक रिस्पांस अगेंस्ट हेल्पलेसनेस एंड एक्शन फॉर रिड्रेसल) द्वारा किए गए एक अध्ययन में कहा गया है। प्रहार एक गैर-लाभकारी संगठन है जो ऐसे ज्वलंत मुद्दों को उठाता है, जिनसे निपटने में आम नागरिक अक्सर असहाय महसूस करते हैं।

रिपोर्ट में आगाह किया गया है कि यह चिंताजनक परिदृश्य, यह दर्शाता है कि देश के एक वैश्विक शक्ति के रूप में उदय को, इसकी सीमाओं के भीतर और बाहर, दोनों जगहों से इसके विकास को अस्थिर करने के उद्देश्य से विरोधियों द्वारा लगातार, पूर्ण-समन्वित प्रयासों से खतरा हो रहा है।वैश्विक स्तर पर, 2024 की पहली तिमाही में साइबर हमलों में 76% की वृद्धि हुई, जिसमें भारत सबसे अधिक प्रभावित देशों में से एक है। रिपोर्ट के अनुसार, यह उछाल उद्योगों में मजबूत साइबर सुरक्षा उपायों की बढ़ती आवश्यकता को दर्शाता है, विशेष रूप से उन क्षेत्रों में जो साइबर अपराधियों द्वारा तेजी से लक्षित किए जा रहे हैं।

2023 में, देश में 79 मिलियन से अधिक साइबर हमले हुए, जो ऐसी घटनाओं की संख्या के मामले में वैश्विक स्तर पर तीसरे स्थान पर है। यह पिछले वर्ष की तुलना में 15% की वृद्धि को दर्शाता है। यह वृद्धि 2024 में भी जारी रही। पहली तिमाही में, रिपोर्टों ने साइबर हमलों में तेज वृद्धि का संकेत दिया, जिसमें केवल तीन महीनों में 500 मिलियन से अधिक घटनाओं को रोकने की रिपोर्ट आई है।

प्रहार की रिपोर्ट में यह भी कहा गया है कि डिजिटल इंटरटेनमेंट और गेमिंग के प्रति नागरिकों की बढ़ती रुचि ने उन्हें अवैध विदेशी सट्टेबाजी और जुआ प्लेटफार्मों की ओर धकेल दिया है, जिससे वे साइबर धोखेबाजी के प्रति अरक्षित हो गए हैं, और वे हमलों के लिए साधन बन गए हैं।

बी) पैन विवरण के अनधिकृत उपयोग पर कार्रवाई

पैन विवरण के अनधिकृत उपयोग पर बड़ी कार्रवाई ! केंद्रीय गृह मंत्रालय के अधीन काम करने वाले भारतीय साइबर अपराध समन्वय केंद्र (I4C) ने वित्तीय प्रौद्योगिकी कंपनियों और अन्य उपभोक्ता प्रौद्योगिकी फर्मों द्वारा भारतीय नागरिकों के स्थायी खाता संख्या (पैन) के अनधिकृत उपयोग को रोकने का निर्देश दिया है।

सरकार डिजिटल निजी डेटा संरक्षण अधिनियम, 2023 (डीपीडीपी) को लागू करने की दिशा में आगे बढ़ते हुए, प्रौद्योगिकी कंपनियों द्वारा व्यक्तिगत डेटा के अनधिकृत संचालन के विरुद्ध कड़ी कार्रवाई कर रही है।

2.साइबर फ्रॉड

ए) डिजिटल गिरफ्तारी(अरेस्ट)

हाल ही में जारी सरकारी आंकड़ों के अनुसार, 2024 की पहली तिमाही के दौरान 'डिजिटल अरेस्ट' धोखाधड़ी योजनाओं में भारतीयों ने लगभग 120.3 करोड़ रुपये गंवाए हैं। प्रधानमंत्री नरेंद्र मोदी ने रविवार (27 अक्तूबर) को अपने मासिक रेडियो संबोधन 'मन की बात' के दौरान अन्य घोटालों के साथ-साथ इस धोखाधड़ी को भी उजागर किया।

डिजिटल गिरफ्तारी धोखाधड़ी को समझना

डिजिटल गिरफ्तारी धोखाधड़ी में स्कैमर जांच एजेंसियों या कानून प्रवर्तन निकायों, जैसे कि सीबीआई, नारकोटिक्स ब्यूरो, आरबीआई, ट्राई, कस्टम अथवा टैक्स प्राधिकारियों के अधिकारी बनकर स्वयं को पेश करते हैं। ये धोखेबाज ऑडियो या वीडियो कॉल के माध्यम से लक्ष्य तक पहुंचते हैं, उन्हें डरा-धमकाकर पैसे वसूलते हैं और उन्हें अक्सर उनके अपने घरों में ही बंधक बनाकर रखते हैं।

B) गुजरात के अहमदाबाद की साइबर अपराध शाखा ने एक अंतरराष्ट्रीय गिरोह का भंडाफोड़ किया

गुजरात के अहमदाबाद की साइबर अपराध शाखा ने ₹79,34,639 की धोखाधड़ी के मामले में शामिल एक अंतरराष्ट्रीय गिरोह का भंडाफोड़ किया है, जिसमें आरोपियों ने स्वयं को ट्राई, मुंबई साइबर क्राइम और सीबीआई का अधिकारी बताया था। गिरोह ने एक स्थानीय निवासी को यह झूठा दावा करके धोखा दिया कि उसके मोबाइल फोन का अवैध गतिविधियों में प्रयोग किया गया है।

गिरफ्तारी वारंट की धमकी और डराने-धमकाने की रणनीति का इस्तेमाल करते हुए अपराधियों ने लगातार व्हाट्सएप कॉल के माध्यम से शिकायतकर्ता पर नजर रखी। उन्होंने सत्यापन की आड़ में पीड़ित पर ₹79,34,639 बैंक खाते में ट्रांसफर करने का दबाव बनाया और प्रक्रिया पूरी होने के बाद पैसे वापस करने का वादा किया।

दिल्ली और बेंगलुरु में साइबर अपराध शाखा द्वारा संयुक्त अभियान चलाकर दो ताइवानी नागरिकों, म्यू ची सांग और चांग हाओ यून (जिन्हें मार्क के नाम से भी जाना जाता है) को गिरफ्तार किया गया, जो इस घोटाले में मुख्य अपराधी थे।

इस सेटअप से 120 से ज़्यादा मोबाइल डिवाइस जुड़े हुए थे, जिनका संचालन दिल्ली, बेंगलुरु और मुंबई में फैला हुआ था। गिरोह गुजरात, राजस्थान, दिल्ली और ओडिशा के स्थानीय लोगों द्वारा कमीशन के बदले में किराए पर दिए गए बैंक खातों का इस्तेमाल कर रहा था, जिनमें से आठ को छापेमारी के दौरान गिरफ़्तार किया गया।

3. इस माह के टिप

ए) डिजिटल गिरफ्तारी से स्वयं को कैसे बचाएं

जानकारी को सत्यापित करें : कभी भी किसी के साथ फोन या ऑनलाइन व्यक्तिगत जानकारी या वित्तीय विवरण साझा न करें, जब तक कि आप उनकी पहचान और उनके अनुरोध की वैधता के बारे में पूरी तरह आश्वस्त न हों।

अपरिचित नंबरों से सावधान रहें :

अज्ञात नंबरों से आने वाली कॉल का उत्तर देने से बचें, विशेषकर उन नंबरों से जिनका एरिया कोड विदेशी हो।

जानकारी की दोबारा जांच करें:

यदि आपको कोई संदिग्ध कॉल या संदेश प्राप्त होता है, तो उस जानकारी को किसी विश्वसनीय स्रोत, जैसे कि किसी सरकारी वेबसाइट या किसी ज्ञात कानून प्रवर्तन एजेंसी से सत्यापित करने का प्रयास करें।

शांत रहें :

धोखाधड़ी करने वाले अपराधी अक्सर अपने शिकार को गुमराह करने के लिए डर और धमकी का सहारा लेते हैं। शांत रहें और आवेगपूर्ण निर्णय लेने से बचें।

धोखाधड़ी की रिपोर्ट करें :

अगर आपको लगता है कि आप डिजिटल गिरफ्तारी धोखाधड़ी का शिकार हुए हैं, तो स्थानीय पुलिस या साइबर अपराध प्राधिकारियों को इसकी रिपोर्ट करें। आप अपने इंटरनेट सेवा प्रदाता या मोबाइल कैरियर को भी इसकी रिपोर्ट कर सकते हैं।

बी) लॉटरी घोटाले से स्वयं को कैसे बचाएं:

इस प्रकार के घोटाले में, धोखेबाज एक बड़ी राशि के हस्तांतरण को सुगम बनाने में मदद का अनुरोध करता है, जो आम तौर पर एक ईमेल के रूप में होता है। बदले में, धोखेबाज एक कमीशन प्रदान करता है, जो आमतौर पर

कई मिलियन डॉलर में होता है। फिर धोखेबाज हस्तांतरण/प्रसंस्करण शुल्क या कर से जुड़ी कुछ लागतों का भुगतान करने के लिए कुछ पैसे भेजने का अनुरोध करते हैं। यदि धोखेबाज को पैसा भेजा जाता है, तो वे या तो तुरंत गायब हो जाएंगे या स्थानान्तरण में लगातार समस्या आने का दावा करके अधिक पैसे प्राप्त करने का प्रयास करेंगे।

लॉटरी घोटाले से सुरक्षा

- नकली लॉटरी जीतने के बारे में संदेशों या कॉल का कभी भी जवाब न दें और इसे अनदेखा करना जाल में फंसने से बचने के लिए एक स्मार्ट कदम है।

- लॉटरी चलाने वाले संगठन के बारे में पता करने के लिए समय निकालें और प्रस्ताव लेकर आने वाले किसी भी व्यक्ति से गहन पूछताछ करें।

- कभी भी संवेदनशील व्यक्तिगत जानकारी साझा न करें क्योंकि धोखेबाज अक्सर ऐसी जानकारी मांगते हैं। सावधान रहें, क्योंकि प्रतिष्ठित संगठन ऐसे डेटा नहीं मांगते हैं।

- किसी भी अप्रत्याशित लाभ को संदेह के साथ लेना आवश्यक है, क्योंकि वास्तविक लॉटरी जीत के लिए आमतौर पर भागीदारी की आवश्यकता होती है।

- कथित जीत का दावा करने के लिए किसी भी शुल्क का भुगतान करने से बचें; वैध लॉटरी में अग्रिम धन की मांग नहीं की जाती है।

- घोटालेबाजों द्वारा भुगतान की तत्काल मांग से सावधान रहें; वे प्रायः पीड़ितों पर शीघ्र कार्रवाई करने का दबाव डालते हैं, तथा उनकी तात्कालिकता की भावना का फायदा उठाने का प्रयास करते हैं।

****


NATIONAL
POLICE
MEMORIAL


स्वच्छता
ही सेवा 2024