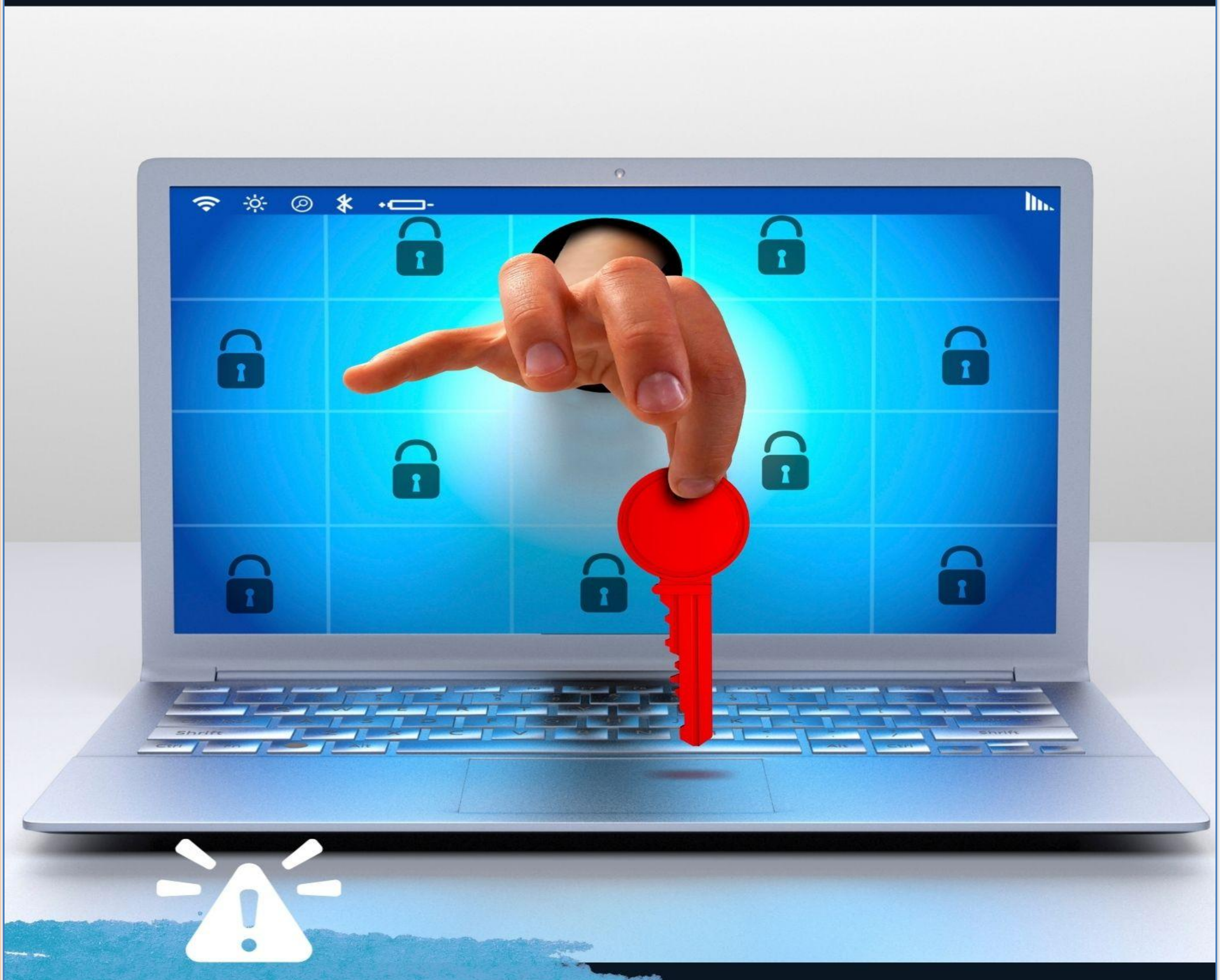
केंद्रीय रिज़र्व पुलिस बल

मई, 2026

साइबर बाइट



RTO/ई-चालान एंड्रॉयड मैलवेयर अभियान

AI-आधारित फ़िशिंग और डीपफ़ेक स्कैम

संचार एवं सूचना प्रौद्योगिकी निदेशालय, सीआरपीएफ

1. नवीनतम साइबर खतरे

(A) आरटीओ/ई चालान एंड्रॉयड मैलवेयर अभियान-:

इस घोटाले में जालसाज एसएमएस, व्हाट्सएप संदेश या ईमेल भेजकर दावा करते हैं कि आपका कोई ट्रैफ़िक जुर्माना लंबित है।

इन संदेशों में आपके बैंक या कार्ड विवरण को चोरी करने के लिए तैयार किए गए दुर्भावनापूर्ण भुगतान के लिंक शामिल होते हैं।

ऐसे धोखाधड़ी वाले संदेश इस तरह तैयार किए जाते हैं कि वे आधिकारिक सरकारी नोटिस जैसे दिखे और पीड़ितों को तुरंत क्लिक करने के लिए झांसे में ले सकें।

> ***रिपोर्ट किए गए कई मामलों में, लोगों ने इन लिंक पर क्लिक किया और उन्हें बड़े अनाधिकृत अंतर्राष्ट्रीय लेनदेन का सामना करना पड़ा। उदाहरण के लिए दिल्ली के एक निवासी ने हाल ही में एक नकली लिंक के माध्यम से "₹500 लंबित चालान" का भुगतान करने के प्रयास में ₹2.49 लाख से अधिक खो दिए।***

घोटाला कैसे काम करता है :

साइबर अपराधी अपने संदेशों को वैध और असली दिखाने के लिए कई हथकंडे अपनाते हैं:

1. **नकली एसएमएस/व्हाट्सपऐप अलर्ट**: ऐसे संदेशों में अक्सर यह दावा किया जाता है
    - "लंबित चालान पाया गया",
    - "लाइसेंस निरस्त होने से बचने के लिए तुरंत भुगतान करें",
    - "भुगतान न करने पर कोर्ट नोटिस जारी किया गया"।

   ये अलर्ट अक्सर सामान्य 10-अंकों वाले मोबाइल नंबरों से आते हैं, न कि सत्यापित प्रेषक आईडी से।

2. फर्जी भुगतान लिंक:

यूआरएल आधिकारिक सरकारी पोर्टलों की नकल करते हैं लेकिन पीड़ित का
डेटा चोरी करने के लिए बनाई गई फिशिंग साइटों पर भेज देते/रिडाइरेक्ट कर देते हैं। कई फर्जी डोमेन परिवहन (Parivahan) वेबसाइट से काफी

मिलते-जुलते हैं और छोटे किए गए यूआरएल का प्रयोग करते हैं। सुरक्षा शोधकर्ताओं ने आरटीओ ई-चालान साईटों का रूप धारण करने वाले 36 से अधिक फर्जी डोमेन का भी पता लगाया है।

3. ब्राउज़र-आधारित फिशिंग पेज:

मॉलवेयर वाले पुराने घोटालों से हटकर, साइबर अपराधी अब क्लोन किए गए हूबहू नकली सरकारी पोर्टलों का उपयोग करते हैं जो :

- नियम उल्लंघन के नकली विवरण को दिखाते हैं ।
- असली परिवहन पेजों के बिल्कुल समान दिखते हैं ।
- केवल कार्ड से भुगतान स्वीकार करते हैं (जो एक बड़ा चेतावनी संकेत है)।

अपना चालान सुरक्षित रूप से कैसे जांचें:

केवल आधिकारिक सरकारी पोर्टलों का उपयोग करें:

- परिवहन आधिकारिक पोर्टल: https://echallan.parivahan.gov.in
- राज्य ट्रैफ़िक पुलिस की आधिकारिक वेबसाइटें

सत्यापित करने के चरण :

- अपने ब्राउज़र में यूआरएल खुद से टाइप करें (संदेशों में दिए गए लिंक पर कभी क्लिक न करें)।
- चालान की स्थिति की जांच करें "Check Challan Status" पर जाएं।
- अपने वाहन का वाहन नंबर + चेसिस/इंजन नंबर के अंतिम 5 अंक दर्ज करें।
- यदि सिस्टम कोई चालान नही है "No Challan Found" दिखाता है, तो वह संदेश फर्जी था।

(B) एआई संचालित फिशिंग और डीपफेक घोटाले: -

साइबर अपराधी क्रेडेंशियल्स (लॉगिन आईडी व पासवर्ड) और धनराशि चुराने के लिए बैंको, पुलिस व कंपनी के अधिकारियों का रूप धरकर एआई-जनरेटेड वॉयस कॉल, फर्जी एचआर ईमेल और बैंकों, डीपफेक वीडियो संदेशों का उपयोग कर रहे हैं। भारतीय कंपनियों में एआई द्वारा संचालित बिजनेस ईमेल समझौता (BEC) के प्रयासों में भारी वृद्धि देखी जा रही है।

दो मुख्य खतरे:

- **एआई फिशिंग:** धोखेबाज बिल्कुल सटीक और त्रुटिहीन ईमेल या टेक्स्ट लिखने के लिए एआई (जैसे चैटजीपीटी) का उपयोग करते हैं। वे आपके जीवन के बारे में वास्तविक विवरणों का उल्लेख करने के लिए आपके सोशल मीडिया का अध्ययन कर सकते हैं, जिससे उनका संदेश 100% असली दिखाई देता है।
- **डीपफेक:** यह किसी व्यक्ति के चेहरे या आवाज का "डिजिटल अपहरण" है। पैसे मांगने के लिए धोखेबाज आपके बॉस के चेहरे या आपके बच्चे की आवाज के कंप्यूटर-जनरेटेड संस्करण का उपयोग करके आपको कॉल कर सकता है।

सुरक्षित रहने के सरल नियम:

- **"गुप्त शब्द" (Safe Word) की रणनीति:** अपने परिवार या सहकर्मियों के साथ एक गुप्त शब्द (जैसे "Blue Pineapple") साझा करें। यदि कोई मुसीबत में होने या आपात स्थिति में कॉल करता है, तो उससे वह गुप्त शब्द पूछें। यदि वे इसे नहीं जानते हैं, तो समझ जाएं कि यह एक फर्जी कॉल है।
- **फोन काटें और वापस कॉल करें:** (Hang Up and Call Back): यदि आपको कोई संदिग्ध "आपातकालीन" कॉल आती है, तो तुरंत फोन काट दें। उस व्यक्ति को अपने फोन संपर्कों में पहले से सहेजे गए नंबर का उपयोग करके वापस कॉल करें—न कि उस नंबर पर जिसने अभी आपको कॉल किया था।
- **जल्दबाजी पर ध्यान दें (Watch for "The Rush"):** घोटालेबाज (स्कैमर) हमेशा चाहते हैं कि आप तेजी से कार्य करें ताकि आपके पास सोचने का समय न रहे। यदि कोई संदेश आपको घबराहट महसूस कराता है या पैसे भेजने के लिए जल्दबाजी करता है, तो यह निश्चित रूप से एक धोखाधड़ी है।

2. नवीनतम वित्तीय धोखाधड़ी संबंधी खतरा

A) Android God Mode मैलवेयर

"Android God Mode" एक खतरनाक नया मैलवेयर स्ट्रेन है जो Android उपयोगकर्ताओं के लिए गंभीर खतरा पैदा कर रहा है। यह धोखेबाजों को उपकरणों पर पूर्ण रिमोट कंट्रोल प्रदान करता है, जिससे वे बैंकिंग डेटा चोरी करने, OTPs को बीच में ही रोकने (intercept) और आपकी सभी गतिविधियों की जासूसी करने में सक्षम होते हैं। यह दुर्भावनापूर्ण APKs या फिशिंग लिंक के माध्यम से फैलता है। इसे सामान्य रूप से अनइंस्टॉल नहीं किया जा सकता, इसे हटाने के लिए Safe Mode removal की आवश्यकता होती है।

मैलवेयर खुद को पुनः स्थापित कैसे करता है ?:

यह मैलवेयर उन्नत निरंतरता (persistence) विधियों पर निर्भर करता है। कई मामलों में, यह डिवाइस की एक्सेसिबिलिटी (Accessibility) अनुमतियों का अनुरोध करता है, जो इसे डिवाइस के मुख्य हिस्सों को नियंत्रित करने की अनुमति देती है। एक बार यह अनुमति मिलने के बाद, यह बैकग्राउंड में खुद को फिर से इंस्टॉल कर सकता है या छिपी हुई प्रक्रियाओं को ट्रिगर कर सकता है।

मैलवेयर को स्थायी रूप से हटाने के चरण

- बाहरी सर्वर के साथ आगे के संचार को रोकने के लिए तुरंत डिवाइस को इंटरनेट से डिस्कनेक्ट करें।
- फोन को Safe Mode में बूट करें, जो थर्ड-पार्टी ऐप्स को चलने से रोकता है।
- इंस्टॉल किए गए ऐप्स की समीक्षा करें और किसी भी अपरिचित या संदिग्ध ऐप को तुरंत हटा दें।
- एक्सेसिबिलिटी सेटिंग्स की जांच करें और उन ऐप्स से अनुमतियां वापस लें जिन्हें उनकी आवश्यकता नहीं है।
- अज्ञात ऐप्स के लिए डिवाइस एडमिनिस्ट्रेटर एक्सेस (Device Administrator Access) को अक्षम करें।
- संदिग्ध ऐप्स से जुड़े बैकअप डेटा को हटाएं और स्वचालित बहाली (Automatic Restore) को अस्थायी रूप से बंद करें।
- छिपे हुए कंपोनेंट की पहचान करने के लिए एक विश्वसनीय मोबाइल सुरक्षा स्कैन (Trusted Security Scan) चलाएं।

- यदि समस्या बनी रहती है, तो डिवाइस का Factory Reset करना आवश्यक हो सकता है। रीसेट करने से पहले सुनिश्चित करें कि महत्वपूर्ण डेटा का सुरक्षित बैकअप लिया गया है, जिसमें उन ऐप्स और सेटिंग्स को शामिल न करें जिनमें मैलवेयर हो सकता है।

B) अग्रिम भुगतान संबंधी धोखाधड़ी:

हालांकि यह एक पारंपरिक प्रकार का फ्रॉड है, लेकिन यह डिजिटल वातावरण के अनुसार पूरी तरह अनुकूलित हो चुका है। INTERPOL कई क्षेत्रों में इसकी निरंतरता पर प्रकाश डालता है, विशेष रूप से जब इसे अधिक परिष्कृत योजनाओं के साथ जोड़ा जाता है, जिसमें नौकरी के फर्जी प्रस्ताव (Fake Job Offers), लॉटरी/पुरस्कार या ऐसी सेवाएं शामिल हैं जिनके लिए अग्रिम भुगतान की आवश्यकता होती है।

बैंकिंग पर प्रभाव:

- धोखाधड़ी वाले सूक्ष्म लेनदेन (Fraudulent Microtransactions) की अधिक मात्रा।
- डिजिटल चैनलों और तत्काल भुगतान (Instant Payments) का दुरुपयोग।
- खुदरा धोखाधड़ी (Retail Fraud) में अत्यधिक वृद्धि।

अग्रिम भुगतान संबंधी धोखाधड़ी (फ्राड) का जवाब कैसे दें ?

ऐसे मामलों में मापनीयता (Scalability) अत्यंत महत्वपूर्ण है। वित्तीय संस्थानों को ऐसे सिस्टम की आवश्यकता है जो वास्तविक समय (Real-time) में लेनदेन की बड़ी मात्रा का विश्लेषण करने में सक्षम हों, ताकि बिना किसी अनावश्यक बाधा के संदिग्ध पैटर्न की पहचान की जा सके।

डायनेमिक रिस्क मॉडल (Dynamic Risk Models) और मल्टीचैनल विश्लेषण का उपयोग संस्थानों को विभिन्न टचपॉइंट्स से संकेतों को सहसंबंधित करने, असामान्य व्यवहार का पता लगाने और उपयोगकर्ता के अनुभव को प्रभावित किए बिना सक्रिय रूप से कार्य करने की अनुमति देता है।

3. साइबर गपशप

बैंक खाता खोलकर चलाया जा रहा साइबर धोखाधड़ी रैकेट

Delhi Police Crime Branch ने कथित तौर पर जाली दस्तावेजों (Forged Documents) का उपयोग करके बैंक खाता खोलने और साइबर धोखाधड़ी रैकेट की सुविधा प्रदान करने के आरोप में एक 35 वर्षीय बैंक कर्मचारी को गिरफ्तार किया है। इस खाते का उपयोग बाद में कई पीड़ितों से पैसे निकालने (siphon) के लिए किया गया था।

पुलिस ने बताया कि आरोपी एक निजी बैंक में रिलेशनशिप मैनेजर (Relationship Manager) के रूप में कार्यरत था।

हैदराबाद पुलिस ने एक बड़े साइबर धोखाधड़ी नेटवर्क का भंडाफोड़ किया:

Operation Octopus 2.0 के तहत, हैदराबाद पुलिस ने नौ राज्यों में व्यापक कार्रवाई करते हुए 32 बैंक कर्मचारियों सहित 52 संदिग्धों को गिरफ्तार किया है। पुलिस के अनुसार, इस ऑपरेशन का मुख्य उद्देश्य उन बैंक अधिकारियों को पकड़ना था जो साइबर अपराधियों को अवैध धन स्थानांतरित करने के लिए फर्जी (Mule) खाते खोलने और उन्हें संचालित करने में मदद कर रहे थे। गिरफ्तार किए गए लोगों में बैंक ऑफ बड़ौदा, बंधन बैंक और इंडस बैंक जैसे प्रतिष्ठित बैंकों के प्रबंधक (Managers), क्लर्क और KYC कर्मचारी शामिल हैं। यह देशव्यापी कार्रवाई महाराष्ट्र, दिल्ली, कर्नाटक, तेलंगाना और अन्य राज्यों में एक सप्ताह तक चलाए गए अभियान के बाद पूरी हुई।

4. साइबर सुरक्षा के लिए अपनाई जाने वाली अच्छी आदतें (साईबर हाइजीन)

आप अपने पासवर्ड को कैसे बेहतर बना सकते हैं?

पासवर्ड आपके ऑनलाइन घर की चाबियों की तरह हैं। आप चाहेंगे कि वे अत्यधिक मजबूत हों। यहाँ कुछ महत्वपूर्ण सुझाव दिए गए हैं:

- लंबे पासवर्ड का उपयोग करें (Use Long Passwords): लंबे पासवर्ड का अनुमान लगाना बेहद कठिन होता है। एक वाक्य का उपयोग करने का प्रयास करें। उदाहरण के लिए, "I love eating pizza on Fridays!" एक अच्छा पासवर्ड है।
- कैरेक्टर मिक्स करें: विभिन्न प्रकार के वर्णों का उपयोग करें। इसमें नंबर, प्रतीक (Symbols) और बड़े व छोटे अक्षरों (Uppercase & Lowercase) को मिलाएं। जैसे कि "I<3EatingPizza0nFridays!" और भी बेहतर और सुरक्षित है।

- पासवर्ड का पुन: उपयोग न करें (Don’t Reuse Passwords): प्रत्येक खाते के लिए हमेशा एक अनूठा (Unique) पासवर्ड रखें। यदि कोई एक खाता हैक भी कर लेता है, तो आपके अन्य खाते पूरी तरह सुरक्षित रहेंगे।

आपको अपना सॉफ़्टवेयर अपडेट क्यों करना चाहिए?

अपने सॉफ़्टवेयर को अपडेट करना फ्लू के टीके (Flu Shot) लगाने की तरह है। यह आपको नए खतरों से सुरक्षित रखता है। इसलिए यह जरूरी है।

- सुरक्षा खामियों को ठीक करना (Fix Security Holes): अपडेट आमतौर पर सॉफ़्टवेयर की सुरक्षा कमियों या बग्स को ठीक करते हैं। ये वे सुराख होते हैं जिनका उपयोग साइबर अपराधी अंदर आने के लिए कर सकते हैं। अपडेट करने से ये बंद हो जाते हैं।
- नई सुविधाएँ प्राप्त करना (Get New Features): अपडेट्स आपको नई और बेहतर सुविधाएँ भी प्रदान करते हैं, जिससे आपके ऐप्स बेहतर ढंग से काम करते हैं।
- स्वचालित अपडेट सेट करें (Set Automatic Updates): जब भी संभव हो, ऑटो-अपडेट चालू रखें ताकि आपको इसे याद रखने की आवश्यकता न हो।

(2FA) कैसे काम करता है?

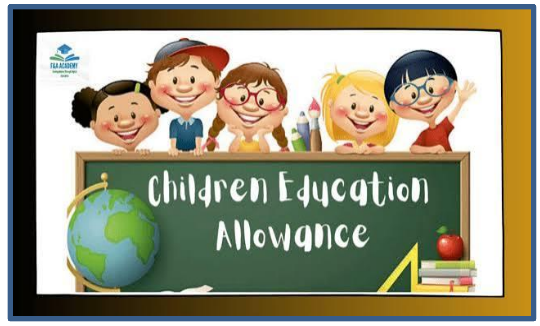
टू-फैक्टर ऑथेंटिकेशन आपके दरवाजे पर दो ताले लगाने जैसा है। यह अपराधियों के लिए सेंध लगाना बेहद कठिन बना देता है। यह कैसे काम करता है, देखें:-

- 2FA को यह साबित करने के लिए दो अलग-अलग चीजों की आवश्यकता होती है कि वह आप ही हैं। आमतौर पर, पहली चीज़ आपका पासवर्ड होती है। दूसरी चीज़ आपके फोन पर भेजा गया एक वन-टाइम कोड (OTP) या आपका बायोमेट्रिक्स (Biometrics) हो सकता है।
- 2FA क्यों ज़रूरी है? यदि कोई आपका पासवर्ड चुरा भी लेता है, तब भी वे आपके खाते में लॉगिन नहीं कर सकते क्योंकि उनके पास प्रमाणीकरण की वह दूसरी चीज़ नहीं होगी। यह अत्यधिक सुरक्षित है।

  2FA का कहाँ उपयोग करें: अपने सभी महत्वपूर्ण खातों जैसे ईमेल, नेट बैंकिंग और सोशल मीडिया प्रोफाइल पर 2FA को अनिवार्य रूप से सक्रिय करें।

5. IT DTE में नया विकास

SAMBHAV



- PPMS के माध्यम से SAMBAV ऐप द्वारा CEA का स्वचालन (Automation)।

PPMS

- Force order प्रकाशन प्रक्रिया का SELO ऐप से PPMS में माइग्रेशन ।
- Risk fund अंतिम मंजूरी प्रक्रिया का SELO से PPMS में माइग्रेशन।

श्री जी पी सिंह, भापुसे, महानिदेशक, केरिपुबल सेवानिवृत्ति के अवसर पर आयोजित
विदाई समारोह में सेवानिवृत्त होने वाले अधिकारियों को स्मृति-चिह्न भेंट करते हुए।

श्री जी पी सिंह, भापुसे, महानिदेशक, केरिपुबल पश्चिमी सिंहभूम के
चाईबासा में जवानों से संवाद करते हुए।

श्री जी पी सिंह, भापुसे, महानिदेशक, केरिपुबल, पश्चिम बंगाल में कानून एवं व्यवस्था बनाए
रखने के संबंध में हावड़ा में तैनात एडहॉक-315 के जवानों एवं पश्चिम बंगाल पुलिस को ब्रीफिंग करते हुए।