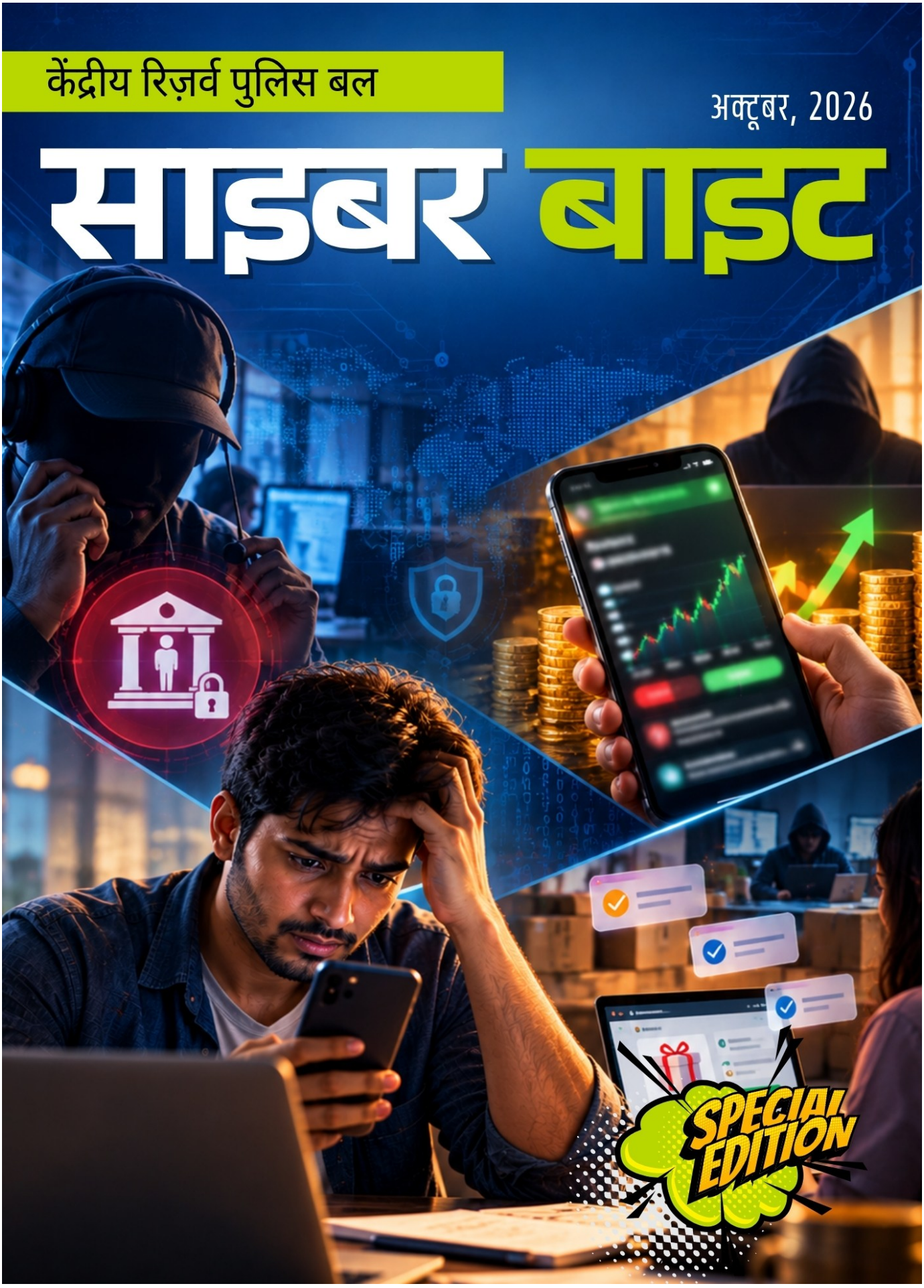
केंद्रीय रिज़र्व पुलिस बल

अक्टूबर, 2026

साइबर बाइट



संचार एवं सूचना प्रौद्योगिकी निदेशालय, सीआरपीएफ

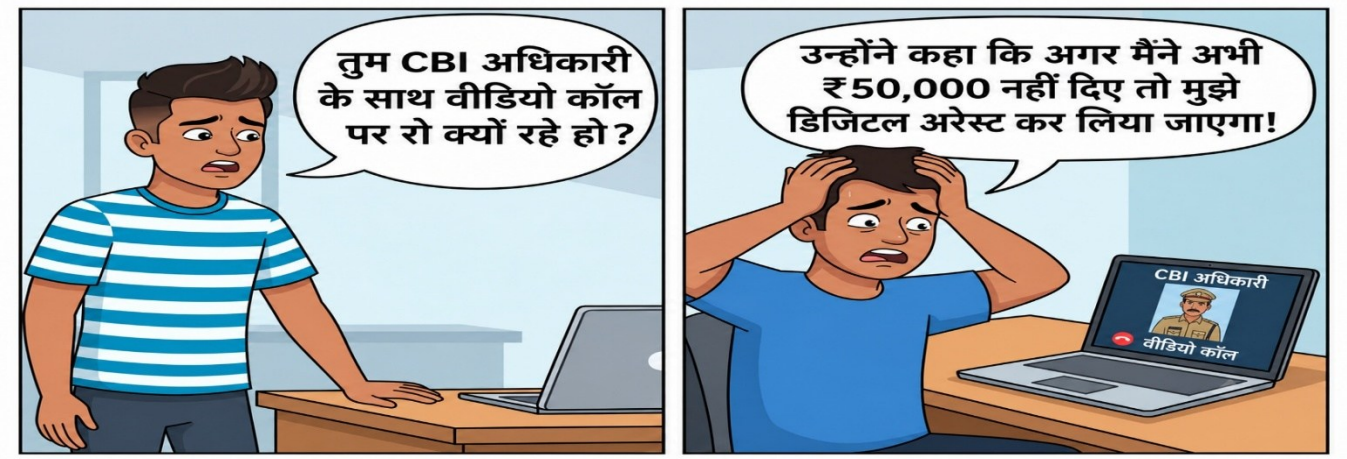
साइबर बाइट — अक्टूबर 2026

राष्ट्रीय साइबर सुरक्षा जागरूकता माह विशेषांक

"साइबर जाग्रत भारत" — अपनी भूमिका निभाएँ, साइबर स्मार्ट बनें

1. वर्ष 2026 के दौरान नवीनतम साइबर खतरे

1. डिजिटल अरेस्ट धोखाधड़ी



सीबीआई, पुलिस, कस्टम या प्रवर्तन निदेशालय के अधिकारी बनकर धोखेबाज एक फर्जी वीडियो कॉल करते हैं। वे दावा करते हैं कि पीड़ित व्यक्ति किसी जांच के दायरे में है या "डिजिटल अरेस्ट" में है, और फिर मनगढ़ंत कानूनी कार्रवाई से बचने के लिए उन पर तुरंत पैसे ट्रांसफर करने का मानसिक दबाव बनाते हैं। सीबीआई के 'ऑपरेशन चक्र-VI' के तहत इसी धोखाधड़ी के खिलाफ देश भर में दर्जनों ठिकानों पर छापेमारी की गई है।

सुरक्षित कैसे रहें:

• कोई भी भारतीय कानून प्रवर्तन एजेंसी कभी भी वीडियो कॉल पर किसी को गिरफ्तार नहीं करती है, और न ही मामला रफा-दफा करने के लिए पैसों की मांग करती है।

• कॉल को तुरंत काट दें और संबंधित विभाग की आधिकारिक हेल्पलाइन के जरिए स्वतंत्र रूप से मामले की सत्यता को जांचें।

मुख्य संदेश: "डिजिटल अरेस्ट' जैसा कोई कानून नहीं है — कॉल काटें, पैसे बिल्कुल न दें।"

2. निवेश और ट्रेडिंग ऐप धोखाधड़ी



सोशल मीडिया विज्ञापनों या व्हाट्सएप ग्रुपों के माध्यम से प्रचारित किए जाने वाले ये फर्जी निवेश और ट्रेडिंग ऐप्स, निवेशकों का भरोसा जीतने के लिए अपने डैशबोर्ड पर बढ़ता हुआ मनगढ़ंत "मुनाफा" दिखाते हैं। लेकिन जैसे ही पीड़ित व्यक्ति बड़ी रकम निवेश कर देता है, उसके पैसे निकालने पर रोक लगा दी जाती है और अंततः यह ऐप ही गायब हो जाता है। भारत में साइबर वित्तीय धोखाधड़ी के कारण होने वाले कुल नुकसान में अकेले इस श्रेणी का बहुत बड़ा हिस्सा है।

सुरक्षित कैसे रहें:

- *केवल सेबी (SEBI) या आरबीआई (RBI) से पंजीकृत प्लेटफॉर्म के माध्यम से ही निवेश करें; और उनके रजिस्ट्रेशन नंबर की स्वतंत्र रूप से जांच अवश्य करें।*
- *गारंटीकृत या असामान्य रूप से बहुत अधिक मुनाफे का दावा करने वालों पर हमेशा संदेह करें।*

मुख्य संदेश: *"अगर आपकी रकम ही निकालना हमेशा 'बस एक और कदम दूर' बताया जाए, तो समझ लें कि वह प्लेटफॉर्म पूरी तरह से फर्जी है।"*

3. कार्य-आधारित नौकरी संबंधित धोखाधड़ी ("लाइक करो और कमाओ")

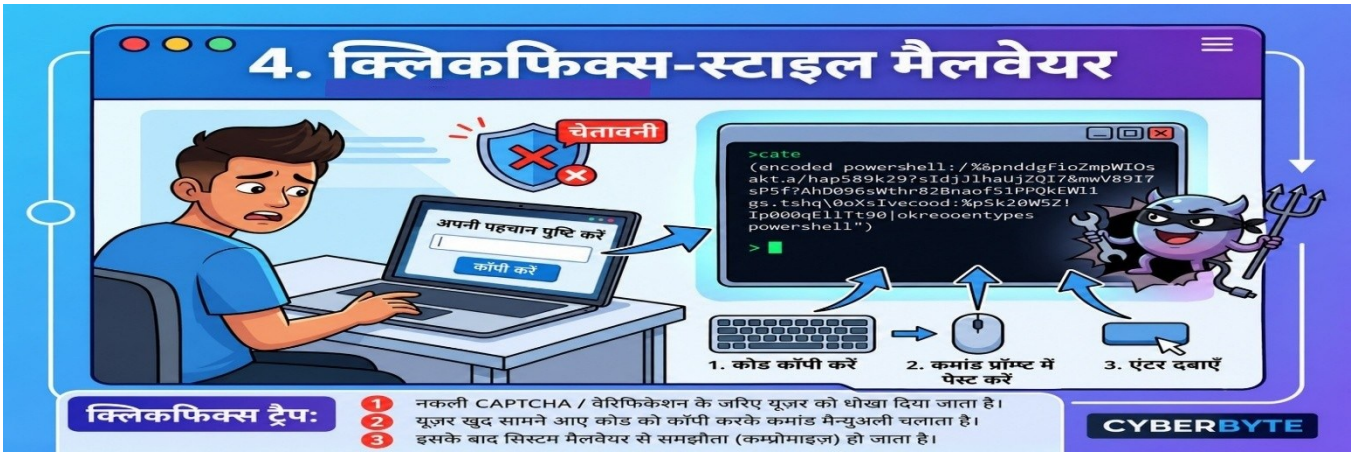


पीड़ितों को टेलीग्राम या व्हाट्सएप पर साधारण सशुल्क कार्यों (Paid Tasks) — जैसे वीडियो लाइक करने, उत्पादों की रेटिंग देने के लिए भर्ती किया जाता है और भरोसा जीतने के लिए शुरू में छोटा और वास्तविक भुगतान किया जाता है। इसके बाद उनसे अतिरिक्त मूल्य वाले कार्यों के लिए "प्रीमियम कार्य" के लिए या निकाली जाने वाली राशि को अनलॉक करने के लिए बड़ी से बड़ी रकम को जमा करने को कहा जाता है, जो उन्हें कभी वापस नहीं मिलती।

सुरक्षित कैसे रहें :
● असली नौकरियों में पैसे कमाने के लिए आपको कभी भी पैसे नहीं देने पड़ते।

मुख्य संदेश:
अगर कोई नौकरी आपसे पैसे कमाने के लिए पहले पैसे मांगती है, तो वह नौकरी नहीं है।

4. क्लिकफ़िक्स-स्टाइल मैलवेयर



साइबर हमले का एक नया तरीका उपयोगकर्ताओं को झांसा देने के लिए "सत्यापित करें कि आप इंसान हैं" या "ब्राउज़र अपडेट" का एक फ़र्ज़ी पेज दिखाता है। यह पेज उपयोगकर्ताओं को एक कमांड को मैन्युअली कॉपी-पेस्ट करके रन (सक्रिय) करने का निर्देश देता है, जिससे बैकग्राउंड में चुपके से मैलवेयर इंस्टॉल हो जाता है। चूँकि इस प्रक्रिया को उपयोगकर्ता खुद अपने हाथों से करता है, इसलिए यह सिस्टम की कई ऑटोमैटिक सुरक्षा चेतावनियों को आसानी से पार (बायपास) कर जाता है।

सुरक्षित कैसे रहें
● किसी भी वेबसाइट पर दिए गए कमांड को कभी भी कॉपी-पेस्ट करके रन(Run) न करें, चाहे वह वेबसाइट कितनी भी प्रामाणिक या आधिकारिक क्यों न लग रही हो।

मुख्य संदेश:
"कोई भी वैध सत्यापन प्रक्रिया कभी भी आपसे किसी कमांड को रन(Run) करने के लिए नहीं कहेगी।"

5. फर्जी लोन ऐप द्वारा उत्पीड़न



धोखाधड़ी करने वाले इंस्टेंट-लोन ऐप पहले तो छोटी सी रकम आपके खाते में डालते हैं, और फिर इंस्टॉलेशन के समय ली गई कैमरा, कॉन्टैक्ट लिस्ट(संपर्क सूची) और गैलरी की परमिशन का गलत फायदा उठाकर आपको परेशान और ब्लैकमेल करना शुरू कर देते हैं, ताकि वे आपसे मनमानी ब्याज दरें वसूल सकें।

सुरक्षित रहने के तरीके

- हमेशा केवल आरबीआई (RBI) से पंजीक्रत बैंकों या एनबीएफसी (NBFCs) के जरिए ही लोन लें।
- किसी भी लोन ऐप को अपने कॉन्टैक्ट्स, गैलरी या कैमरा का एक्सेस(access) भी न दें।

मुख्य संदेश: "एक असली ऋणदाता (Lender) को आपके लोन को पास करने के लिए कभी भी आपकी कॉन्टैक्ट लिस्ट(संपर्क सूची) की जरूरत नहीं होती।"

6. फर्जी टेक-सपोर्ट कॉल सेंटर



धोखाधड़ी करने वाले कॉल सेंटर खुद को किसी इंटरनेशनल टेक-सपोर्ट या बैंक की फ्रॉड-अलर्ट टीम का कर्मचारी बताते हैं। ये लोगों को झांसे में लेकर उनके फोन या कंप्यूटर पर 'रिमोट-एक्सेस सॉफ्टवेयर' इंस्टॉल करवा लेते हैं या उनसे ओटीपी हासिल कर लेते हैं। दिल्ली पुलिस ने सितंबर 2026 में पश्चिमी दिल्ली में ऐसे ही तीन फर्जी कॉल सेंटरों पर छापा मारकर 23 लोगों को गिरफ्तार किया है।

सुरक्षित रहने के तरीके:

- कोई भी असली कंपनी कभी भी आपको अचानक फोन करके कोई रिमोट-एक्सेस सॉफ्टवेयर इंस्टॉल करने के लिए नहीं कहेगी।

मुख्य संदेश: "यदि कोई *कॉल करने वाला* किसी ऐसी खराबी को 'ठीक' करने के लिए आपकी डिवाइस का रिमोट एक्सेस(access) मांगता है जिसकी आपने शिकायत ही नहीं की थी, तो समझ जाएं कि वह एक धोखाधड़ी है।"

7. मेलिशियस (दुर्भावनापूर्ण) ब्राउज़र एक्सटेंशन



नकली "एडब्लॉकर" (adblocker) या "प्रॉडक्टिविटी" (productivity) ब्राउज़र एक्सटेंशन, जो अक्सर मुफ्त टूल के रूप में छिपे रहते हैं, ये एक्सटेंशन आपके द्वारा देखी जाने वाली हर वेबसाइट के डेटा को पढ़ने और उसमें बदलाव करने की व्यापक अनुमतियाँ मांगते हैं। इसकी आड़ में ये बैकग्राउंड में चुपचाप सेव(save) किए गए आपके पासवर्ड, सेशन कुकीज़ (session cookies) और क्रिप्टो-वॉलेट की संवेदनशील जानकारियों को चुरा लेते हैं।

सुरक्षित कैसे रहें?

● ब्राउज़र एक्सटेंशन हमेशा केवल प्रमाणित पब्लिशरों (verified publishers) से ही इंस्टॉल करें और इंस्टॉल करने से पहले उनके द्वारा मांगी जा रही अनुमतियों की जांच ज़रूर करें।

● समय-समय पर अपने ब्राउज़र एक्सटेंशन की समीक्षा (review) करते रहें और जिन एक्सटेंशन का अब आप इस्तेमाल नहीं करते, उन्हें तुरंत हटा दें।

मुख्य संदेश: "अगर कोई मुफ्त एक्सटेंशन आपसे 'सभी वेबसाइट डेटा' का एक्सेस(access) मांग रहा है, तो यह खतरे की घंटी (red flag) है, कोई सुविधा नहीं।"

8. त्योहारी सीज़न में ई-कॉमर्स और कूरियर धोखाधड़ी



त्योहारी सीजन में खरीदारी के दौरान प्रत्येक वर्ष अक्टूबर-नवंबर में कूरियर में देरी से जुड़े फर्जी एसएमएस और ईमेल अचानक बढ़ जाते हैं। इनमें 'कस्टम शुल्क' या 'दोबारा डिलीवरी' के नाम पर बहुत मामूली रकम मांगी जाती है। ये लिंक पीड़ितों को फर्जी पेमेंट पेजों पर ले जाते हैं, जहाँ उनके कार्ड की गोपनीय जानकारी चुरा ली जाती है।

सुरक्षित कैसे रहें

- पैकेजों को केवल कूरियर के आधिकारिक ऐप या वेबसाइट के माध्यम से ही ट्रैक करें, एसएमएस में आए लिंक के माध्यम से कभी नहीं।
- यदि किसी ऐसे ऑर्डर के लिए डिलीवरी शुल्क मांगा जा रहा है जिसे मंगवाना आपको याद न हो, तो तुरंत सतर्क हो जाएं।

मुख्य संदेश: "कोई भी असली कूरियर कंपनी आपके पार्सल को डिलीवर करने के लिए एसएमएस के जरिए कार्ड से भुगतान करने के लिए कभी नहीं कहती।

2. ज्ञान कोष

1. सीईआरटी-इन **(CERT-In)** क्या है?
   इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (MeitY) के तहत भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सीईआरटी-इन) साइबर सुरक्षा से जुड़ी घटनाओं से निपटने के लिए भारत की राष्ट्रीय नोडल एजेंसी है। यह **सुरक्षा परामर्श** जारी करती है, सूचना प्रौद्योगिकी अधिनियम के तहत **साइबर घटनाओं पर त्वरित कार्रवाई का समन्वय करती है,** और साइबर सतर्कता पर नागरिकों को जागरूक करने के लिए प्रति वर्ष अक्टूबर में **'राष्ट्रीय साइबर सुरक्षा जागरूकता माह' का आयोजन करती है।**



2. **सोशल इंजीनियरिंग: मानव फ़ायरवॉल (The Human Firewall)**
   ज़्यादातर साइबर हमले किसी चालाकी भरे तकनीकी हमले (exploit) से शुरू नहीं होते — वे एक फ़ोन कॉल, ईमेल या संदेश से शुरू होते हैं, जो किसी व्यक्ति को अपने ही सुरक्षा हितों के खिलाफ काम करने के लिए उकसाता है। नियमित प्रशिक्षण और सजग संदेह के जरिए एक 'मानव फ़ायरवॉल' तैयार करना, अक्सर किसी भी अकेले तकनीकी नियंत्रण की तुलना में कहीं अधिक प्रभावी होता है।



3. वीएपीटी (VAPT) क्या है?

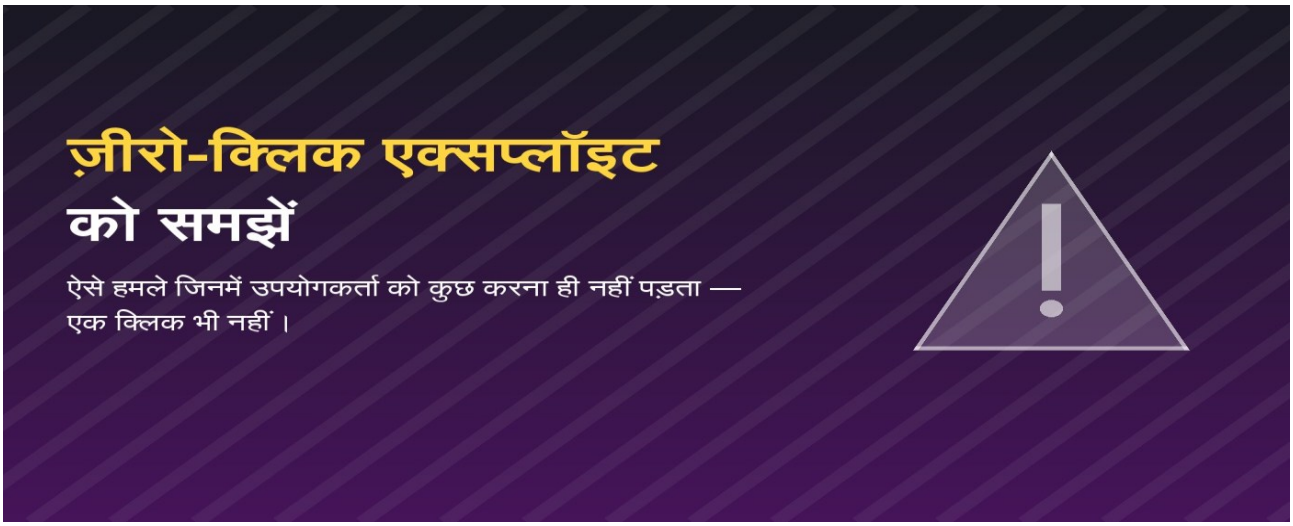
भेद्यता आकलन और भेदन परीक्षण(VAPT), ज्ञात सुरक्षा कमियों का पता लगाने के लिए ऑटोमेटेड स्कैनिंग और यह जांचने के लिए कि एक वास्तविक हमलावर प्रणाली(सिस्टम) में कितनी भीतर तक सेंध लगा सकता है, व्यवहारिक एथिकल हैकिंग दोनों का एक सशक्त संयोजन है। नियमित रूप से भेद्यता आकलन और भेदन परीक्षण(VAPT) चक्र

(cycles) आयोजित करने से संगठनों को साइबर अपराधियों से पहले अपने सिस्टम की कमियों को पहचानने और उन्हें ठीक करने में मदद मिलती है।



4. ज़ीरो-क्लिक एक्सप्लॉइट्स (Zero-Click Exploits) की विस्तृत व्याख्या

एक ज़ीरो-क्लिक एक्सप्लॉइट उपयोगकर्ता (victim) द्वारा किसी लिंक पर क्लिक किए बिना या कोई फ़ाइल खोले बिना ही उसके डिवाइस को पूरी तरह से हैक/संक्रमित (compromise) कर देता है; यह अक्सर केवल एक दुर्भावनापूर्ण (malicious) संदेश, इमेज या कॉल प्राप्त होने मात्र से ही सक्रिय हो जाता है। इस प्रकार के एक्सप्लॉइट्स अत्यंत दुर्लभ होते हैं और इन्हें विकसित करना अत्यधिक खर्चीला होता है, किंतु इनसे बचाव करना बेहद कठिन होता है। यही कारण है कि मैसेजिंग ऐप्स और ऑपरेटिंग सिस्टम(OS) सॉफ़्टवेयर को त्वरित रूप से अपडेट करना अनिवार्य हो जाता है।



3. सूचना प्रौद्योगिकी अवसंरचना की सुरक्षा कैसे करें

1. 3-2-1 का बैकअप नियम

अपने महत्वपूर्ण डेटा की कम से कम 3 कॉपियाँ रखें, जिन्हें दो अलग-अलग प्रकार के माध्यमों (media) पर स्टोर किया गया हो, और एक कॉपी ऑफलाइन या किसी अन्य स्थान (offsite) पर सुरक्षित हो। यह नियम सुनिश्चित करता है कि किसी सफल रैंसमवेयर हमले या हार्डवेयर के खराब होने की स्थिति में भी आपके डेटा की सभी कॉपियाँ एक साथ नष्ट नहीं होंगी।



2. एंडपॉइंट डिटेक्शन और रिस्पांस (EDR)

ईडीआर (EDR) टूल्स लैपटॉप, सर्वर और अन्य एंडपॉइंट्स की लगातार निगरानी करते हैं ताकि संदिग्ध गतिविधियों को पकड़ा जा सके। ये केवल जाने-माने मालवेयर सिग्नेचर (पहले से मौजूद खतरों) पर निर्भर नहीं रहते, बल्कि नेटवर्क में हमला आगे फैलने से पहले ही किसी भी प्रभावित (compromised) डिवाइस को अपने आप ही अलग कर सकते हैं।



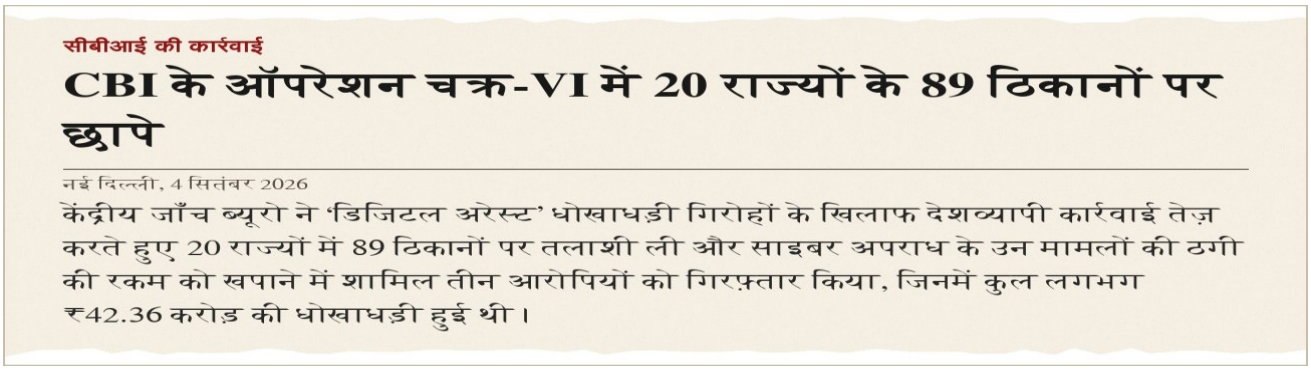
3. तृतीय-पक्ष और विक्रेता के लिए जोखिम प्रबंधन (Third-Party & Vendor Risk Management)

वर्ष 2026 में हुए बड़े डेटा उल्लंघनों (data breaches) का एक बड़ा हिस्सा किसी सीधे हमले की बजाय किसी भरोसेमंद विक्रेता (vendor) या जुड़े हुए ऐप (connected app) के माध्यम से शुरू हुआ था। तृतीय-पक्ष टूल (third-party tools) की डेटा तक पहुँच (access) की नियमित समीक्षा करनी चाहिए तथा वेंडर्स के लिए बुनियादी सुरक्षा मानकों (baseline security standards) को पूरा करना अनिवार्य बनाना, सुरक्षा की उस आम चूक (gap) को दूर करता है जिसे अक्सर नज़रअंदाज़ कर दिया जाता है।



4. साइबर गपशप

1. CBI का ऑपरेशन चक्र-VI: 20 राज्यों में 89 ठिकानों पर छापे



सीबीआई की कार्रवाई

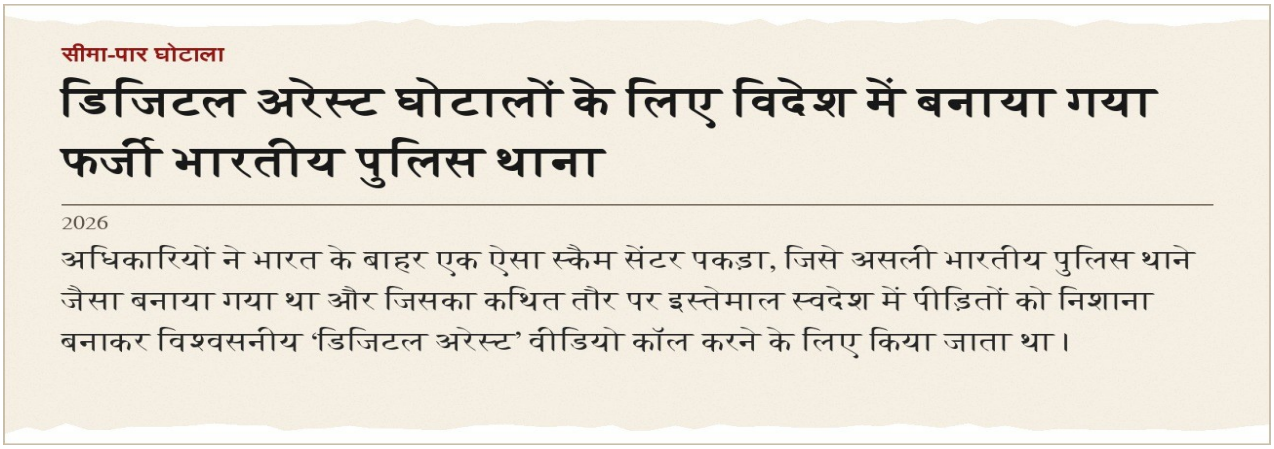
CBI के ऑपरेशन चक्र-VI में 20 राज्यों के 89 ठिकानों पर छापे

नई दिल्ली, 4 सितंबर 2026

केंद्रीय जाँच ब्यूरो ने 'डिजिटल अरेस्ट' धोखाधड़ी गिरोहों के खिलाफ देशव्यापी कार्रवाई तेज़ करते हुए 20 राज्यों में 89 ठिकानों पर तलाशी ली और साइबर अपराध के उन मामलों की ठगी की रकम को खपाने में शामिल तीन आरोपियों को गिरफ़्तार किया, जिनमें कुल लगभग ₹42.36 करोड़ की धोखाधड़ी हुई थी।

मुख्य निष्कर्ष : डिजिटल अरेस्ट धोखाधड़ी हैंडलर्स और म्यूल खातों (mule accounts) के एक संगठित, बहु-राज्यीय नेटवर्क के रूप में विकसित हो चुकी है — सीबीआई अब केवल कॉल करने वाले व्यक्तिगत अपराधियों को ही नहीं, बल्कि पैसों के पूरे लेन-देन (मनी ट्रेल) को ध्वस्त कर रही है।

2. डिजिटल अरेस्ट धोखाधड़ी को अंजाम देने के लिए विदेश में स्थापित किए गए फर्जी भारतीय पुलिस स्टेशन



सीमा-पार घोटाला

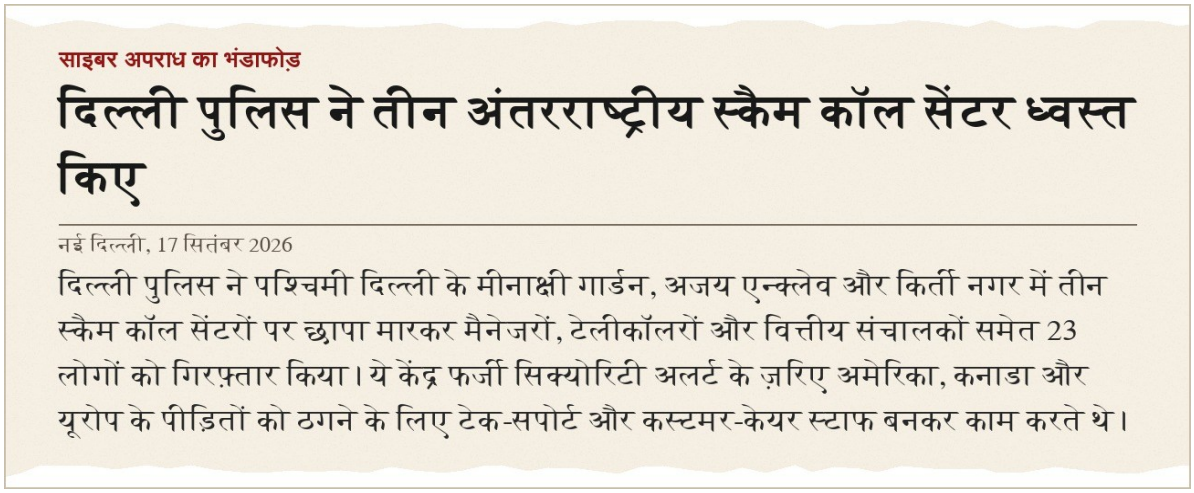
डिजिटल अरेस्ट घोटालों के लिए विदेश में बनाया गया फर्जी भारतीय पुलिस थाना

2026

अधिकारियों ने भारत के बाहर एक ऐसा स्कैम सेंटर पकड़ा, जिसे असली भारतीय पुलिस थाने जैसा बनाया गया था और जिसका कथित तौर पर इस्तेमाल स्वदेश में पीड़ितों को निशाना बनाकर विश्वसनीय 'डिजिटल अरेस्ट' वीडियो कॉल करने के लिए किया जाता था।

मुख्य निष्कर्ष: धोखेबाज आजकल वीडियो कॉल के दौरान असली दिखने के लिए उच्च स्तरीय सामग्री का उपयोग करते हैं, जैसे कि असली दिखने वाले बैकग्राउंड सेट और नकली वर्दियाँ। चूंकि दिखने वाली वास्तविकता को आसानी से गढ़ा जा सकता है, इसलिए उपयोगकर्ताओं को आधिकारिक माध्यमों से कॉल करने वाले की पहचान का स्वतंत्र रूप से सत्यापन करना चाहिए।

3. दिल्ली पुलिस ने तीन अंतरराष्ट्रीय फर्जी (स्कैम) कॉल सेंटरों का भंडाफोड़ किया



साइबर अपराध का भंडाफोड़

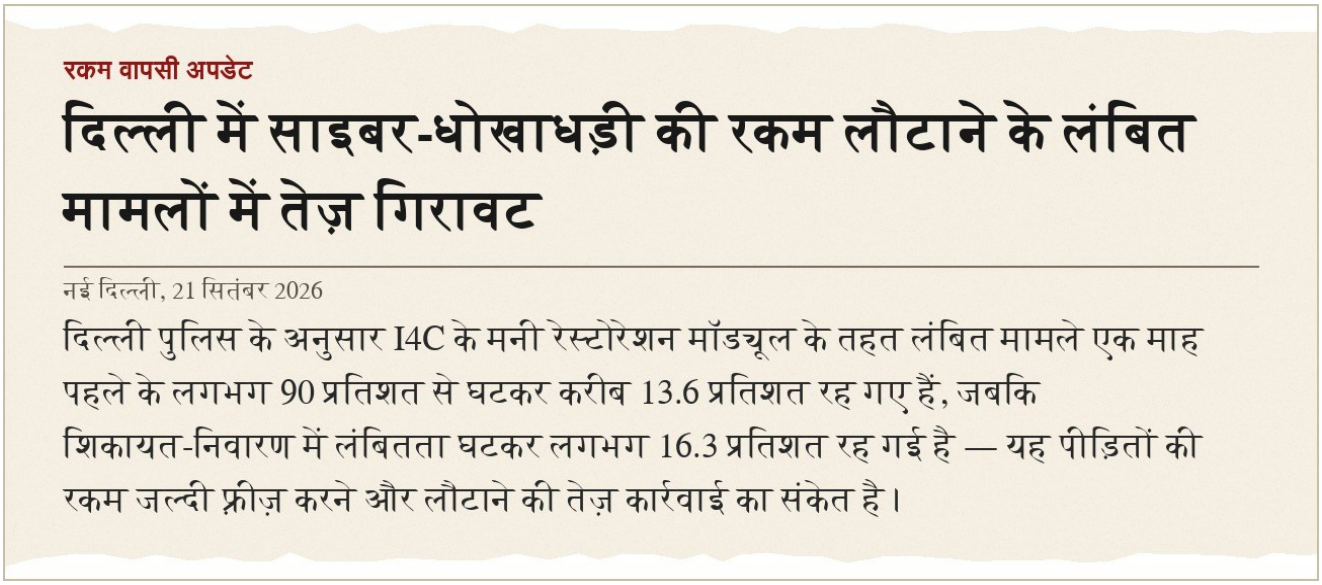
दिल्ली पुलिस ने तीन अंतरराष्ट्रीय स्कैम कॉल सेंटर ध्वस्त किए

नई दिल्ली, 17 सितंबर 2026

दिल्ली पुलिस ने पश्चिमी दिल्ली के मीनाक्षी गार्डन, अजय एन्क्लेव और किर्ती नगर में तीन स्कैम कॉल सेंटरों पर छापा मारकर मैनेजरों, टेलीकॉलरों और वित्तीय संचालकों समेत 23 लोगों को गिरफ़्तार किया। ये केंद्र फर्जी सिक्योरिटी अलर्ट के ज़रिए अमेरिका, कनाडा और यूरोप के पीड़ितों को ठगने के लिए टेक-सपोर्ट और कस्टमर-केयर स्टाफ बनकर काम करते थे।

मुख्य निष्कर्ष: भारत में सक्रिय कॉल सेंटर फर्जी टेक-सपोर्ट स्क्रिप्ट के जरिए विदेशी नागरिकों को अपनी धोखाधड़ी का शिकार बना रहे हैं—यह इस तथ्य को रेखांकित करता है कि यहाँ मौजूद साइबर अपराध का बुनियादी ढांचा वैश्विक स्तर पर प्रभावी और हानिकारक है।

4. दिल्ली में साइबर-धोखाधड़ी के पैसे वापसी के लंबित मामलों में भारी गिरावट



रकम वापसी अपडेट

दिल्ली में साइबर-धोखाधड़ी की रकम लौटाने के लंबित मामलों में तेज़ गिरावट

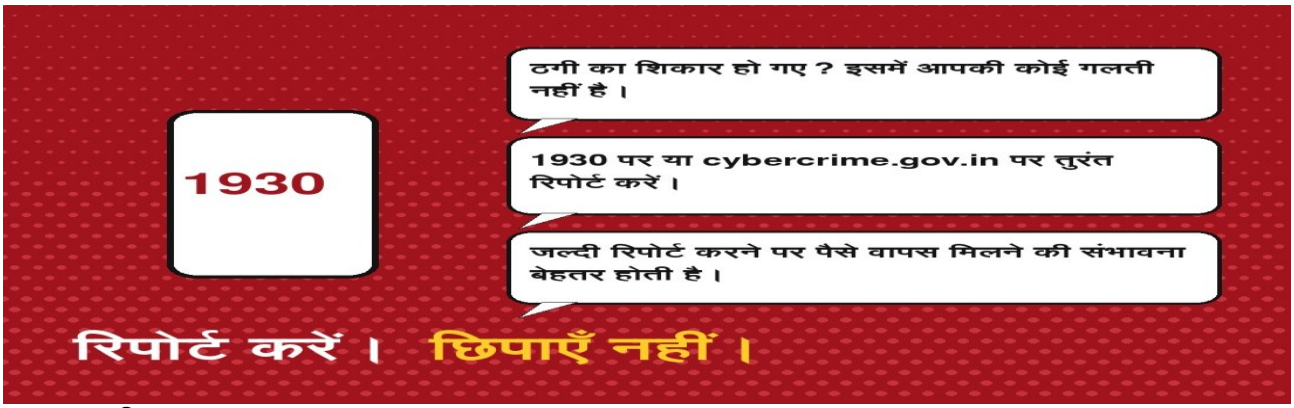
नई दिल्ली, 21 सितंबर 2026

दिल्ली पुलिस के अनुसार I4C के मनी रेस्टोरेशन मॉड्यूल के तहत लंबित मामले एक माह पहले के लगभग 90 प्रतिशत से घटकर करीब 13.6 प्रतिशत रह गए हैं, जबकि शिकायत-निवारण में लंबितता घटकर लगभग 16.3 प्रतिशत रह गई है — यह पीड़ितों की रकम जल्दी फ़्रीज़ करने और लौटाने की तेज़ कार्रवाई का संकेत है।

मुख्य बात: जितनी जल्दी रिपोर्ट करेंगे, उतना ही फायदा होगा — I4C के 'मनी रेस्टोरेशन मॉड्यूल' के तहत अब काम इतनी तेजी से हो रहा है कि यदि आप तुरंत शिकायत दर्ज कराते हैं, तो फ्रीज की गई रकम वापस मिलने की उम्मीद काफी बढ़ जाती है।

5. साइबर सतर्कता

- साइबर धोखाधड़ी का शिकार होने पर तुरंत 'गोल्डन ऑवर' (शुरुआती महत्वपूर्ण समय) के भीतर 1930 हेल्पलाइन या cybercrime.gov.in पर रिपोर्ट करें—आपकी त्वरित कार्रवाई ही यह तय करती है कि ठगी गई रकम को फ्रीज (ब्लॉक) किया जा सकेगा या नहीं।
- कोई भी पुलिस अधिकारी, सीबीआई (CBI) एजेंट या सरकारी अधिकारी वीडियो कॉल के माध्यम से कभी भी आपकी "गिरफ्तारी" नहीं कर सकता।
- किसी ऑनलाइन टास्क, पार्ट-टाइम जॉब या इन्वेस्टमेंट ऐप से अपनी ही कमाई को 'अनलॉक' करने के लिए कभी भी भुगतान न करें—वास्तविक मुनाफे या रिटर्न के लिए किसी भी अग्रिम शुल्क की आवश्यकता नहीं होती।
- किसी भी वेबसाइट द्वारा दिए गए कमांड या कोड को कभी भी कॉपी-पेस्ट करके रन न करें, चाहे वह वेबसाइट कितनी भी प्रामाणिक या आधिकारिक क्यों न दिखती हो।
- लोन हमेशा केवल आरबीआई (RBI) से पंजीकृत ऋणदाताओं के माध्यम से ही लें, और किसी भी लोन ऐप को अपने कॉन्टैक्ट्स (संपर्क सूची) या गैलरी का एक्सेस (access) कभी न दें।
- अपने ब्राउज़र एक्सटेंशन और ऐप परमिशन की नियमित रूप से जांच करें; ऐसी किसी भी चीज़ को तुरंत हटा दें जिसे आप पहचानते नहीं हैं या जिसका अब उपयोग नहीं करते है ।
- त्योहारी सीजन के शॉपिंग ऑफर्स, कूरियर में देरी के मैसेज और डिलीवरी लिंक्स पर क्लिक करने से पहले उनकी सत्यता की अच्छी तरह जांच कर लें।
- जहाँ भी विकल्प उपलब्ध हो, तो एसएमएस ओटीपी (SMS OTP) के मुकाबले ऑथेंटिकेटर ऐप या हार्डवेयर की (Key) के उपयोग को प्राथमिकता दें।
- अपने ऑपरेटिंग सिस्टम, ऐप्स और एंटीवायरस को नवीनतम सुरक्षा अपडेट (सिक्योरिटी पैचेज) के साथ हमेशा अपडेट रखें।
- अपनी हर डिवाइस पर एक पिन (PIN), पासवर्ड या बायोमीट्रिक लॉक लगाएं और जब भी डिवाइस का इस्तेमाल न हो रहा हो, तो उसे लॉक करना न भूलें।



रिपोर्ट करें। इसे छिपाएं नहीं।



उधमपुर(जम्मू-कश्मीर) में 187 बटालियन के अपने दौरे के दौरान श्री ज्ञानेन्द्र प्रताप सिंह, भा.पु.से, महानिदेशक केरिपुबल ने पुरस्कार विजेताओं को सम्मानित किया और वर्ष 2026 की अमरनाथ यात्रा ड्यूटी के दौरान जवानों कीअटूट निष्ठा के लिए उनकी सराहना की।



महानिरीक्षक के पद पर पदोन्नत होने पर श्री शाहनवाज खान, उप महानिरीक्षक को श्री ज्ञानेन्द्र प्रताप सिंह, भा.पु.से., महानिदेशक, केरिपुबल द्वारा उनके परिवारजनों और वरिष्ठ अधिकारियों की उपस्थिति में रैंक लगाने के अवसर की झलकियां ।



श्री रविदीप सिंह साही, अपर महानिदेशक, दक्षिणी अंचल, केरिपुबल की सेवानिवृत्ति के अवसर पर उनके सम्मान में ग्रुप केंद्र, हैदराबाद में आयोजित भव्य विदाई परेड की झलकियां।