NBFC साइबर हमले: तीन महीने में दिल्ली-NCR की 12 कंपनियों का ₹65 करोड़ डूबा



मौलिक प्रतीकात्मक चित्र: pcsmantra.com

खबरों में क्यों

इंडियन एक्सप्रेस (16 नवंबर 2026) के अनुसार दिल्ली-NCR में **12 नॉन-बैंकिंग वित्तीय कंपनियों (NBFC)** ने पिछले तीन महीनों में **साइबर ठगी से ₹65 करोड़ से अधिक** गंवाए हैं। पुलिस के अनुसार हमलावरों ने कंपनियों के **पेआउट API** (भुगतान-संचालन प्रणाली) की कमज़ोरियों को निशाना बनाया - जिनके ज़रिए बड़े पैमाने पर ऋण-वितरण और भुगतान होते हैं। इसी बीच **तेलंगाना साइबर सुरक्षा ब्यूरो (TGCSB)** ने 12 नवंबर को AI-आधारित सहायता वाले साइबर हमलों के बढ़ते ख़तरे की चेतावनी दी, और हालिया अंतर्राष्ट्रीय छापों ने इस तरह के ऑपरेशनों के ट्रांसनेशनल नेटवर्क उजागर किए।

मुख्य तथ्य

- **घटना का दायरा:** तीन महीनों में दिल्ली-NCR की 12 NBFC से ₹65 करोड़+ की साइबर ठगी (IE रिपोर्ट, पुलिस सूत्रों के हवाले से)।
- **हमले का तरीका:** पेआउट API की भेद्यता; अंदरूनी/बाहरी एक्सेस-क्रेडेंशियल्स का दुरुपयोग; धन को कई खातों/वॉलेट में परतदार (layering) करना।
- **नया ख़तरा:** TGCSB के अनुसार जेनरेटिव AI से फ़िशिंग, डीपफ़ेक-कॉल और स्वचालित सोशल इंजीनियरिंग हमलों की गुणवत्ता बढ़ रही है।
- **प्रवर्तन:** अंतर्राष्ट्रीय समन्वित छापों (ToI, 13 नवंबर) में कॉल-सेंटर/ठगी नेटवर्क के ट्रांसबॉर्डर लिंक सामने आए।

नियामकीय ढाँचा

- **NBFC कोन नियंत्रित करता है:** भारतीय रिज़र्व बैंक (RBI) - पंजीकरण, सावधि मानदंड और आईटी गवर्नेंस; Top, Upper और Middle Layer की NBFC के लिए RBI के **Master Direction on IT Governance (2023)** साइबर-सुरक्षा ढाँचा, घटना-रिपोर्टिंग और बोर्ड-स्तरीय निगरानी अनिवार्य करते हैं।
- **कानूनी आधार:** सूचना प्रौद्योगिकी अधिनियम 2000 (धारा 43A - संवेदनशील डेटा की सुरक्षा; धारा 66 - कंप्यूटर-संबंधी अपराध), IPC/BNS के ठगी-प्रावधान।
- **डेटा संरक्षण:** DPDP अधिनियम की धारा 8 के डेटा-सुरक्षा और उल्लंघन-सूचना दायित्व 18-माह वाली चरणबद्ध प्रवर्तन अवधि में लागू होंगे; 16 नवंबर 2026 को ये दायित्व अभी प्रभावी नहीं हैं। CERT-In के तहत साइबर-घटनाओं की **6 घंटे में रिपोर्टिंग** अनिवार्य।

क्यों महत्वपूर्ण है

- **वित्तीय स्थिरता (GS-3):** NBFC छोटे ऋण और अंतिम-क़ड़ी वितरण की रीढ़ हैं; उन पर हमले वित्तीय समावेशन और ग्राहक-विश्वास दोनों को चोट पहुंचाते हैं।
- **साइबर सुरक्षा:** API-आधारित ढाँचे में पारंपरिक परिधि-सुरक्षा अपर्याप्त; ज़ीरो-ट्रस्ट आर्किटेक्चर, मज़बूत प्रमाणीकरण और रीयल-टाइम फ्रॉड-मॉनिटरिंग ज़रूरी।
- **AI का दोहरा चरित्र:** AI सुरक्षा-पहचान को भी मज़बूत करता है और हमलावरों के हथियार भी - नीति को दोनों पक्ष देखने होंगे।

प्रिलिम्स परीक्षा अभ्यास प्रश्न

प्रश्न 1: NBFC का पंजीकरण और नियमन मुख्यतः किसके अधीन होता है?

(a) SEBI

(b) RBI

(c) IRDAI

(d) वित्त मंत्रालय सीधे

उत्तर और व्याख्या

उत्तर: (b) NBFC RBI अधिनियम 1934 की धारा 45-IA के तहत RBI में पंजीकृत होती हैं और RBI के सावधि/आईटी निर्देशों से बंधी हैं।

प्रश्न 2: CERT-In के दिशानिर्देशों के तहत साइबर-घटनाओं की रिपोर्टिंग की अनिवार्य समय-सीमा है:

(a) 24 घंटे

(b) 72 घंटे

(c) 6 घंटे

(d) 48 घंटे

उत्तर और व्याख्या

उत्तर: (c) CERT-In के 2022 दिशानिर्देश कुछ साइबर-घटनाओं की रिपोर्टिंग घटना की जानकारी के 6 घंटे के भीतर अनिवार्य करते हैं।

मेन्स परीक्षा अभ्यास प्रश्न

प्रश्न: "डिजिटल वित्त का विस्तार साइबर-जोखिम के समानांतर विस्तार के बिना टिकाऊ नहीं है।" NBFC क्षेत्र में बढ़ती साइबर ठगी के संदर्भ में इस कथन की विवेचना कीजिए और नियामकीय व तकनीकी उपाय सुझाइए। (250 शब्द)

रूपरेखा: भूमिका - NBFC ठगी के ताज़ा आंकड़े; जोखिम-आयाम - API भेद्यता, AI-हमले, डेटा-उल्लंघन; नियामकीय ढाँचा - RBI आईटी गवर्नेंस, CERT-In, DPDP; उपाय - ज़ीरो-ट्रस्ट, एमएफए, फ्रॉड-एनालिटिक्स, कर्मचारी-प्रशिक्षण, अंतर्राष्ट्रीय सहयोग; निष्कर्ष - विश्वास ही डिजिटल वित्त की मुद्रा।

FAQ

संक्षिप्त उत्तर: दिल्ली-NCR की 12 NBFC ने तीन महीनों में साइबर ठगी से ₹65 करोड़+ गंवाए; हमलावरों ने पेआउट API को निशाना बनाया। Top, Upper और Middle Layer की NBFC के लिए RBI के आईटी गवर्नेंस निर्देश तथा CERT-In की अलग 6-घंटे रिपोर्टिंग लागू हैं। DPDP अधिनियम की धारा 8 के डेटा-सुरक्षा और उल्लंघन-सूचना दायित्व 18-माह वाली चरणबद्ध प्रवर्तन अवधि में लागू होंगे; 16 नवंबर 2026 को ये दायित्व अभी प्रभावी नहीं हैं। TGCSB ने AI-हमलों की चेतावनी दी है।

प्रश्न: NBFC पर हमले कैसे हो रहे हैं?

पुलिस के अनुसार हमलावर कंपनियों के पेआउट API की कमज़ोरियों और क्रेडेंशियल्स का दुरुपयोग कर ऋण-वितरण/भुगतान धन को कई खातों में स्थानांतरित कर रहे हैं; TGCSB ने AI-आधारित फ़िशिंग और डीपफ़ेक की बढ़ती भूमिका बताई है।

प्रश्न: NBFC के लिए साइबर-सुरक्षा के कौन-से नियम लागू होते हैं?

Top, Upper और Middle Layer की NBFC के लिए RBI के Master Direction on IT Governance (2023) साइबर-ढाँचा और घटना-रिपोर्टिंग अनिवार्य करते हैं; CERT-In को 6 घंटे में घटना-रिपोर्ट; DPDP अधिनियम की धारा 8 के डेटा-सुरक्षा और उल्लंघन-सूचना दायित्व 18-माह वाली चरणबद्ध प्रवर्तन अवधि में लागू होंगे; 16 नवंबर 2026 को ये दायित्व अभी प्रभावी नहीं हैं। आईटी अधिनियम 2000 के दंड-प्रावधान।

प्रश्न: ग्राहक और कंपनियाँ क्या सावधानी रखें?

कंपनियाँ: API सुरक्षा-ऑडिट, मल्टी-फ़ैक्टर प्रमाणीकरण, रीयल-टाइम फ्रॉड मॉनिटरिंग, कर्मचारी-प्रशिक्षण। ग्राहक: OTP/पासवर्ड साझा न करें, अनजान लिंक से बचें, संदिग्ध लेन-देन की तुरंत शिकायत (1930 हेल्पलाइन/cybercrime.gov.in) करें।

स्रोत

- इंडियन एक्सप्रेस (16 नवंबर 2026): दिल्ली-NCR की 12 NBFC का तीन महीने में ₹65 करोड़+ डूबा
- टाइम्स ऑफ़ इंडिया (हैदराबाद): अंतरराष्ट्रीय छापे - पेआउट API बने चोरी के रास्ते
- द हिंदू: TGCSB की NBFC/फिनटेक को AI-आधारित हमलों की चेतावनी
- टिप्पणी: इस विषय पर कोई आधिकारिक आंकड़ा-विज्ञप्ति उपलब्ध नहीं मिली; आंकड़े समाचार-रिपोर्टों में उद्धृत पुलिस/TGCSB सूत्रों पर आधारित हैं