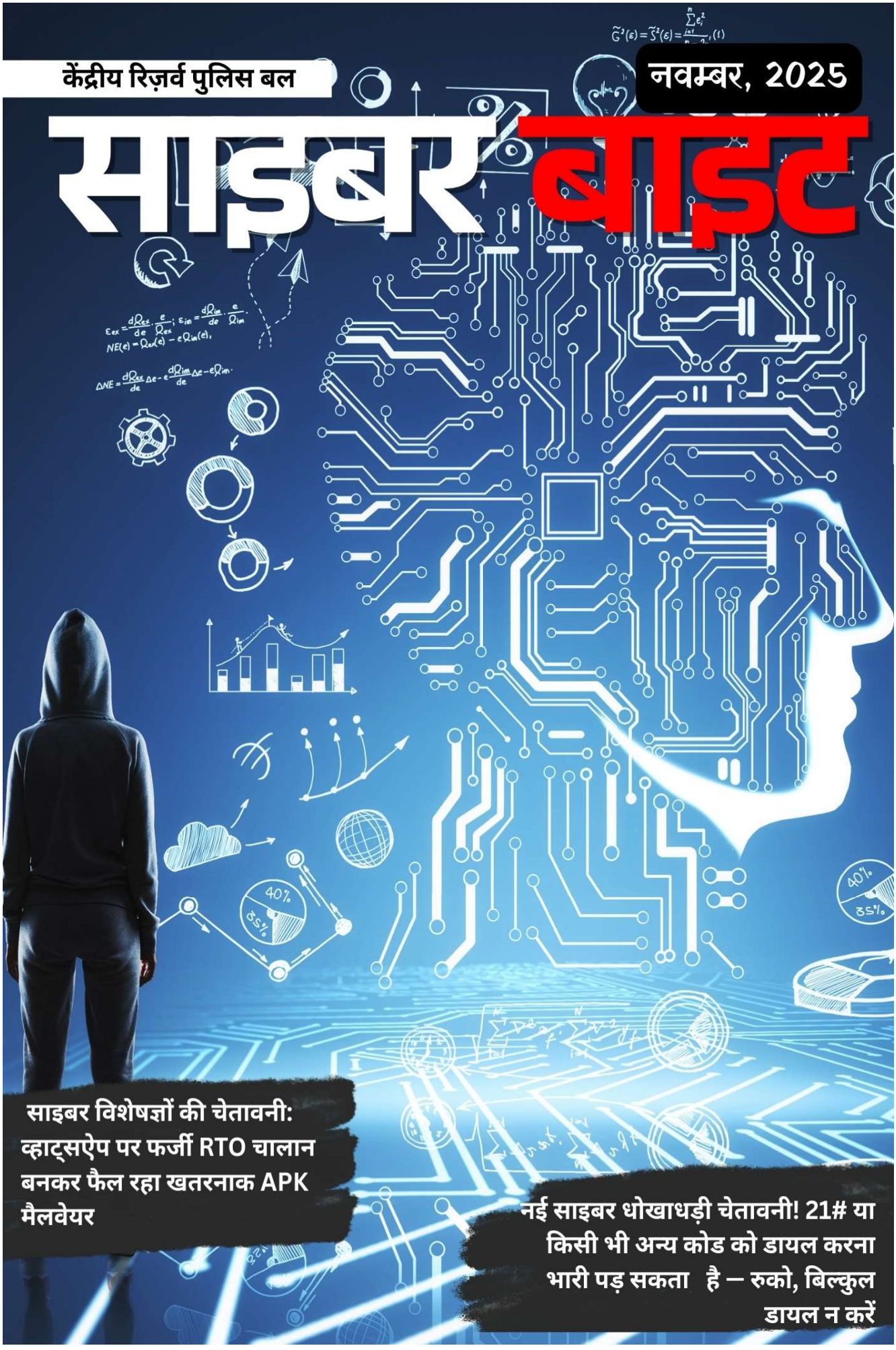
केंद्रीय रिज़र्व पुलिस बल

नवम्बर, 2025

साइबर बाइट



साइबर विशेषज्ञों की चेतावनी: व्हाट्सऐप पर फर्जी RTO चालान बनकर फैल रहा खतरनाक APK मैलवेयर

नई साइबर धोखाधड़ी चेतावनी! 21# या किसी भी अन्य कोड को डायल करना भारी पड़ सकता है — रुको, बिल्कुल डायल न करें

COMN. & IT DIRECTORATE, CRPF

1. साइबर गीक्स समाचार

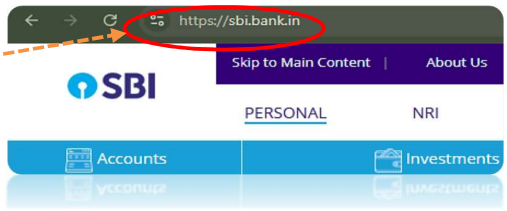
(ए) आरबीआई ने सुरक्षित ऑनलाइन बैंकिंग के लिए बैंकों को अक्टूबर, 2025 तक '.bank.in ' डोमेन अपनाने का आदेश दिया है :-

रिज़र्व बैंक ऑफ़ इंडिया (आरबीआई) ने देश के सभी बैंकों को **31 अक्टूबर, 2025** तक अपनी ऑफिशियल वेबसाइट और इंटरनेट बैंकिंग पोर्टल को नए **".bank.in" डोमेन पर माइग्रेट करने का निर्देश दिया है** । यह डिजिटल बैंकिंग में साइबर सिक्योरिटी को सुदृढ़ करने की दिशा में एक बड़ा कदम है। इस कदम का मकसद उपभोक्ताओं को फ़िशिंग अटैक, नकली वेबसाइट और ऑनलाइन फ्रॉड से बचाना है, ताकि यह सुनिश्चित किया जा सके कि सिर्फ़ सत्यापित और प्राधिकृतबैंक ही इस खास डोमेन के तहत काम करें।

पहले, बैंक **.com, .in या.co.in** , जैसे अधिक सामान्य डोमेन का उपयोग करते थे जिससे धोखेबाजों के लिए एक जैसी दिखने वाली साइटें बनाना आसान हो गया। विशेष .bank.in डोमेन प्रामाणिकता का एक स्पष्ट संकेत प्रदान करता है। नया '.bank.in' डोमेन, बैंकिंग प्रौद्योगिकी में विकास एवं अनुसंधान संस्थान (आईडीआरबीटी) द्वारा प्रबंधित और सतत निगरानी में रखा जाएगा। पंजाब नेशनल बैंक और भारतीय स्टेट बैंक सहित कई बैंक इस परिवर्तन की प्रक्रिया को शुरू कर चुके हैं। सुरक्षित और विश्वसनीय ऑनलाइन बैंकिंग सुनिश्चित करने के लिए ग्राहकों को सलाह दी जाती है कि लॉगइन करने- से पहले यह अवश्य जाँच लें कि उनके बैंक की वेबसाइट '.bank.in' पर समाप्त होती है।

उदाहरण के तौर पर, पहले आप https://www.onlinesbi.sbi.in/ पर जाते थे, लेकिन अब आपको https://onlinesbi.sbi.bank.in/ पर जाना होगा। यह नया डोमेन केवल प्रमाणित बैंकों को ही दिया जाता है, जिससे ग्राहकयह आसानी से सुनिश्चित कर सकें कि वे वास्तविक और सुरक्षित बैंक वेबसाइट पर ही लॉगइन कर- रहे हैं।

- लॉगिन विवरण दर्ज करने से पहले सुनिश्चित करें कि वेबसाइट का पता .bank.in पर समाप्त होता हो जैसे), https://sbi.bank.in)।
- सुनिश्चित करें कि वेबसाइट का पता https:// से शुरू होता हो और ब्राउज़र के एड्रेस बार में एक जैनरिक 'ट्यून'आइकन दिखाई दे।



- जब आपके बैंक की नई आधिकारिक वेबसाइट सक्रिय हो जाए, तो उसे बुकमार्क कर लें और लिंक पर क्लिक करने के बजाय उसी का उपयोग करें।
- धोखेबाज़ अक्सर ऐसे नकली लिंक भेजते हैं जो बैंक संदेशों जैसे लगते हैं। इसलिए URL को स्वयं टाइप करें या आधिकारिक ऐप का ही उपयोग करें।

(बी) <u>दिल्ली के शीर्ष पुलिस अधिकारी ने साइबर अपराध मामलों में ई-एफआईआर दर्ज करने के लिए दिशानिर्देश जारी किए हैं:-</u>

दिल्ली पुलिस ने एक नई प्रणाली शुरू की है, जिसके तहत साइबर अपराध से जुड़े मामलों—विशेष रूप से वित्तीय धोखाधड़ी वाले मामलों—के लिए e-FIR अपने आप दर्ज हो जाएगी। पहले लोगों को शिकायत दर्ज कराने के लिए पुलिस स्टेशन जाना पड़ता था, जिससे अक्सर देरी हो जाती थी। अब, यदि कोई व्यक्ति साइबर धोखाधड़ी (जैसे ऑनलाइन घोटाला या फर्जी निवेश) की रिपोर्ट राष्ट्रीय हेल्पलाइन 1930 या **नेशनल साइबरक्राइम रिपोर्टिंग पोर्टल एनसीआरपी** के जरिए करता/करती है, तो इस प्रणाली द्वारा अपनेआप एक - इलेक्ट्रॉनिकFIR (e-FIR) दर्ज कर दी जाएगी और पीड़ित को तुरंत पुलिस स्टेशन जाने की आवश्यकता नहीं पड़ेगी।

इस नए सेटअप को **"e-Zero FIR सिस्टम" कहा जाता है, इसे दिल्ली में गृह मंत्रालय (MHA)** और **इंडियन साइबर क्राइम कोऑर्डिनेशन सेंटर (I4C)** ने पायलट प्रोजेक्ट के तौर पर लॉन्च किया है । शुरुआत में, इसमें सिर्फ़ बड़े फ्रॉड (₹10 लाख और उससे ज़्यादा) कवर होते थे, लेकिन अब यह **₹1 लाख या उससे ज़्यादा के मामलों पर भी लागू होता है** । एक बार e-FIR बन जाने के बाद, यह अपने आप सही पुलिस यूनिट को भेज दी जाती है, जिसमें शामिल पैसे की रकम के आधार पर छोटे मामले ज़िले के साइबर पुलिस स्टेशनों में जाते हैं, जबकि बड़े मामलों को **क्राइम ब्रांच** या **IFSO (इंटेलिजेंस फ़्यूज़न एंड स्ट्रैटेजिक ऑपरेशंस) जैसी स्पेशलाइज़्ड यूनिट संभालती हैं** ।

- ₹1-25 lakh → District Cybercrime PS
- ₹ 25-50 lakh → Crime Branch Cyber Cell
- Above ₹ 50 lakh → Special Cell's IFSO (Intelligence Fusion & Strategic Ops) unit

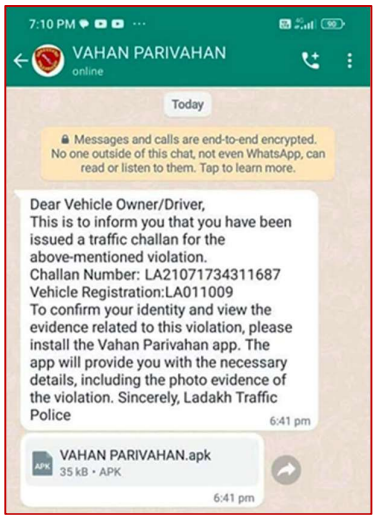
इस प्रणाली का मुख्य उद्देश्य समय बचाना और पीड़ितों की तेज़ी से मदद करना है। साइबर क्राइम में आमतौर पर तुरंत एक्शन लेने की ज़रूरत होती है, जैसे बैंक अकाउंट फ्रीज़ करना या डिजिटल ट्रांज़ैक्शन को ट्रेस करना। ऑटोमैटिक e-FIR रजिस्ट्रेशन से, पुलिस पेपरवर्क का इंतज़ार करने के बजाय तुरंत जांच शुरू कर सकती है। पीड़ितों को अभी भी शिकायत पर साइन करने और सपोर्टिंग डॉक्यूमेंट देने के लिए 72 घंटे के अंदर पुलिस स्टेशन जाना होगा ।

- सिर्फ़ ऑफिशियल चैनल इस्तेमाल करें, साइबरक्राइम हेल्पलाइन 1930 पर कॉल करें या ऑफिशियल पोर्टल cybercrime.gov.in पर जाएं । अपने केस की डिटेल्स कभी भी सोशल मीडिया या अनऑफिशियल वेबसाइट पर शेयर न करें।
- यदि आप कभी साइबर अपराध का शिकार हो जाएँ, तो सबसे महत्वपूर्ण बात है तुरंत कार्रवाई करना। जितनी जल्दी आप शिकायत करेंगे, पुलिस के लिए धोखेबाज़ के खाते को फ्रीज़ करने और आपका पैसा वापस दिलाने की संभावना उतनी ही अधिक होगी।
- स्कैमर के इस्तेमाल किए गए सभी सबूत, जैसे मैसेज के स्क्रीनशॉट, पेमेंट डिटेल्स और फ़ोन नंबर सेव करना न भूलें, क्योंकि इससे पुलिस को फ्रॉड का पता लगाने में मदद मिलेगी।
- जब आपकी ई-एफआईआर दर्ज हो जाए, तो अपनी शिकायत पर हस्ताक्षर करने और पुष्टि करने के लिए 72 घंटे के भीतर अपने नज़दीकी पुलिस स्टेशन जाएँ।

2. साइबर धोखाधड़ी

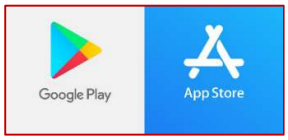
(ए) <u>साइबर विशेषज्ञों की चेतावनी: व्हाट्सऐप पर फर्जी RTO चालान बनकर फैल रहा खतरनाक APK मैलवेयर:-</u>

व्हाट्सऐप मैसेज के ज़रिए एक नया स्कैम फैल रहा है, जिसमें लोगों को नकली "RTO ई-चालान" ऐप डाउनलोड करने के लिए धोखा दिया जा रहा है। यह मैसेज अक्सर आपके किसी जानने वाले से आता है, जिससे यह सुरक्षित लगता है। इसमें " **RTO VAHAN PARIVAHAN.apk" नाम की एक फ़ाइल होती है** , जिसमें ट्रैफ़िक फाइन दिखाने का दावा किया जाता है। लेकिन एक बार ऐप इंस्टॉल हो जाने के बाद, यह चुपके से हैकर्स को आपके फ़ोन का एक्सेस दे देता है। कई लोग पहले ही अपने व्हाट्सऐप अकाउंट का एक्सेस खो चुके हैं, और कुछ के बैंक अकाउंट से पैसे भी गायब हो गए हैं।



साइबर विशेषज्ञों का कहना है कि यह साइबर हमले का एक नया तरीका है। अब अपराधी संदिग्ध लिंक या ईमेल भेजने के बजाय भरोसेमंद संपर्कों के माध्यम से मालवेयर फैलाने लगे हैं। यह नकली ऐप आपके संदेश पढ़ सकता है, व्यक्तिगत डेटा चुरा सकता है और यहाँ तक कि आपकी वित्तीय जानकारी पर भी नज़र रख सकता है। अधिकारियों ने चेतावनी दी है कि व्हाट्सऐप पर भेजे गए किसी भी ऐप को इंस्टॉल न करें—खासकर यदि वह .apk फाइल हो और आधिकारिक गूगल प्ले स्टोर से न आया हो।

- WhatsApp या SMS पर मिली किसी भी .apk फ़ाइल को कभी भी डाउनलोड या इंस्टॉल न करें। ऐप्स को सिर्फ़ **Google Play Store** या **Apple App Store** से ही इंस्टॉल करना चाहिए।



- RTO या ट्रैफिक पुलिस कभी भी WhatsApp से चालान नहीं भेजते हैं। किसी भी लंबित चालान की पुष्टि केवल **echallan.parivahan.gov.in** या आधिकारिक **mParivahan ऐप** पर ही करें।

- अपने फ़ोन की सेटिंग्स में "अज्ञात ऐप्स इंस्टॉल करें" ऑप्शन को बंद कर दें, अपने फ़ोन के सॉफ़्टवेयर और ऐप्स को अपडेट रखें।
- अगर आपने इसे पहले ही इंस्टॉल कर लिया है, तो तुरंत अपने फ़ोन को इंटरनेट से डिस्कनेक्ट करें, संदिग्ध ऐप को अनइंस्टॉल करें और अपने ऑनलाइन बैंकिंग पासवर्ड और UPI PIN को बदलें।

(बी) <u>नई साइबर धोखाधड़ी चेतावनी! 21# या किसी भी अन्य कोड को डायल करना भारी पड़ सकता है —रुको, बिल्कुल डायल न करें:</u>

साइबर पुलिस ने लोगों को एक नए और बेहद खतरनाक ऑनलाइन धोखाधड़ी के तरीके से सावधान किया है। इस घोटाले में ठग लोगों को उनके मोबाइल फोन पर 21# जैसे खास कोड डायल करने के लिए बहला-फुसलाते हैं। अपराधी खुद को बैंक, मोबाइल सेवा प्रदाता या सरकारी एजेंसी का अधिकारी बताकर कॉल करते हैं। वे झूठे बहाने बनाते हैं — जैसे कि आपकी SIM की जांच करनी है, नेटवर्क तेज करना है, या किसी तकनीकी समस्या को तुरंत ठीक करना है — और फिर उस खास कोड को डायल करने के लिए कहते हैं। जैसे ही कोई व्यक्ति यह कोड डायल करता है, उसके सभी इनकमिंग कॉल और संदेश ठग के नंबर पर फॉरवर्ड होने लगते हैं। इससे धोखेबाज़ को पीड़ित के सभी OTP, बैंक अलर्ट और वेरिफिकेशन कोड मिलने लगते हैं। एक बार यह जानकारी मिलने के बाद, ठग आसानी से पीड़ित के बैंक खाते, व्हाट्सऐप और सोशल मीडिया अकाउंट में घुसपैठ कर सकते हैं। इतना ही नहीं, वे पीड़ित की पहचान का इस्तेमाल करके उसके परिवार और दोस्तों को भी निशाना बना सकते हैं।

***21*Mobile No.#**
(For Call Forwarding)

***#21#**
(To Check Call Forwarding on a Phone)

विशेषज्ञों ने कहा है कि यह धोखाधड़ी का बेहद खतरनाक तरीका है और ज़रा-सी भी गलती किसी व्यक्ति की पूरी डिजिटल जिंदगी को खतरे में डाल सकती है। उन्होंने सभी लोगों को सलाह दी है कि वे किसी भी अज्ञात कोड को कभी डायल न करें और न ही ऐसे कॉलर्स की बात मानें जो खुद को बैंक या सरकारी कार्यालय का अधिकारी बताते हों।

#21#
(To Deactivate Call Forwarding)

यदि किसी ने गलती से ऐसा कोई कोड डायल कर दिया है, तो तुरंत अपने मोबाइल ऑपरेटर से संपर्क करें और कॉल फ़ॉरवार्डिंग बंद कराएँ। इसके बाद अपने सभी

पासवर्ड बदलें और घटना की रिपोर्ट नज़दीकी साइबर क्राइम पुलिस स्टेशन में या आधिकारिक वेबसाइट cybercrime.gov.in पर दर्ज करें।

पुलिस का कहना है कि ठग अपने तरीक़े लगातार बदलते रहते हैं, इसलिए जागरूकता और सतर्कता ही ऐसे साइबर फ्रॉड से बचने का सबसे मजबूत तरीका है।

Use full codes

***#06#** To check IMEI number

***#67#** To check all forwarding services

#002# To de activate all forwarding

HELPFUL TIPS

- कभी भी अनजान कोड जैसे *21*, *401* या किसी अजनबी का दिया हुआ कोई भी कोड डायल न करें।
- OTP, PIN या पासवर्ड किसी के साथ शेयर न करें , यहां तक कि ऐसे किसी व्यक्ति के साथ भी नहीं जो आपके बैंक या सरकारी एजेंसी से होने का दावा करता हो।
- अपने फ़ोन की कॉल-फ़ॉरवर्डिंग सेटिंग्स रेगुलर चेक करें और किसी भी अनजान नंबर को बंद कर दें।
- ई-मेल, सोशल मीडिया और बैंकिंग ऐप्स जैसे सभी ज़रूरी अकाउंट्स के लिए टू-फैक्टर ऑथेंटिकेशन (2FA) चालू करें ।
- अपने SIM कार्ड या फोन को किसी के साथ भी, चाहे थोड़े समय के लिए ही क्यों न हो, कभी साझा न करें।

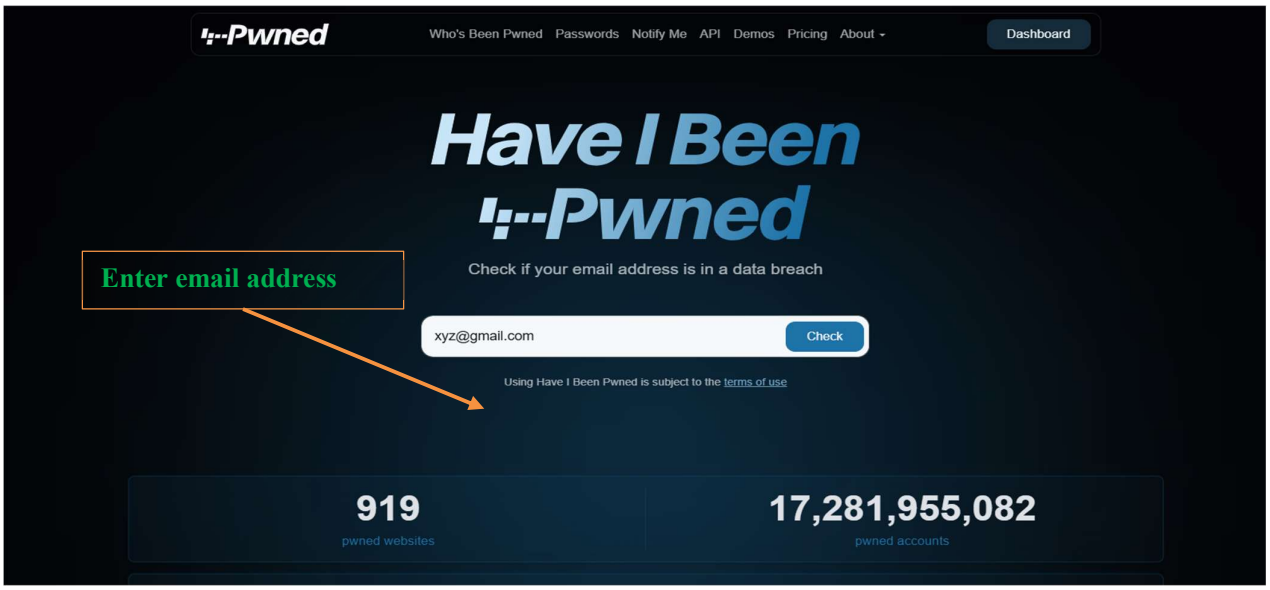
3. महीने के सुझाव (टिप्स)

(ए) Have I Been Pwned: ऑनलाइन डेटा लीक का पता करने का एक भरोसेमंद और मुफ्त टूल:-

Have I Been Pwned एक निःशुल्क और बेहद आसान वेबसाइट है, जिसकी मदद से आप यह जांच सकते हैं कि आपका ईमेल आईडी, पासवर्ड, फोन नंबर या अन्य निजी जानकारी किसी ऑनलाइन डेटा लीक में उजागर हुई है या नहीं। सीधे शब्दों में समझें—जब कोई वेबसाइट या ऑनलाइन सेवा हैक हो जाती है, तो हैकर्स अक्सर उपयोगकर्ताओं की लॉगिन जानकारी चोरी करके उसे इंटरनेट पर बेच देते हैं या सार्वजनिक

कर देते हैं। यह टूल आपको बताता है कि आपकी जानकारी किसी ऐसे डेटा ब्रीच का हिस्सा बनी है या नहीं।

आपको बस https://haveibeenpwned.com पर जाना है और सर्च बॉक्स में अपना ईमेल एड्रेस या फोन नंबर टाइप करना है। साइट तुरंत आपको बताएगी कि आपकी जानकारी किसी ज्ञात डेटा ब्रीच में आई है या नहीं, और यह भी बताएगी कि किस वेबसाइट



से यह लीक हुई थी।

- Have I Been Pwned का उपयोग करते समय हमेशा आधिकारिक वेबसाइट haveibeenpwned.com पर ही जाएँ। ऑनलाइन नकली कॉपियाँ मौजूद हैं, इसलिए अपनी जानकारी दर्ज करने से पहले वेबसाइट के पते को दोबारा जाँच लें।
- वहां कभी भी अपना पासवर्ड शेयर न करें, इस साइट को सिर्फ़ आपकी ईमेल ID या फ़ोन नंबर की ज़रूरत होती है ताकि यह चेक किया जा सके कि आपकी जानकारी किसी डेटा ब्रीच में लीक तो नहीं हुई है।
- अगर वेबसाइट पर पता चलता है कि आपका डेटा लीक हो गया है (Pwned), तो जिन अकाउंट पर असर हुआ है, उन पर तुरंत अपना पासवर्ड बदल दें और पक्का करें कि हर अकाउंट का **पासवर्ड यूनिक और मज़बूत हो** ।

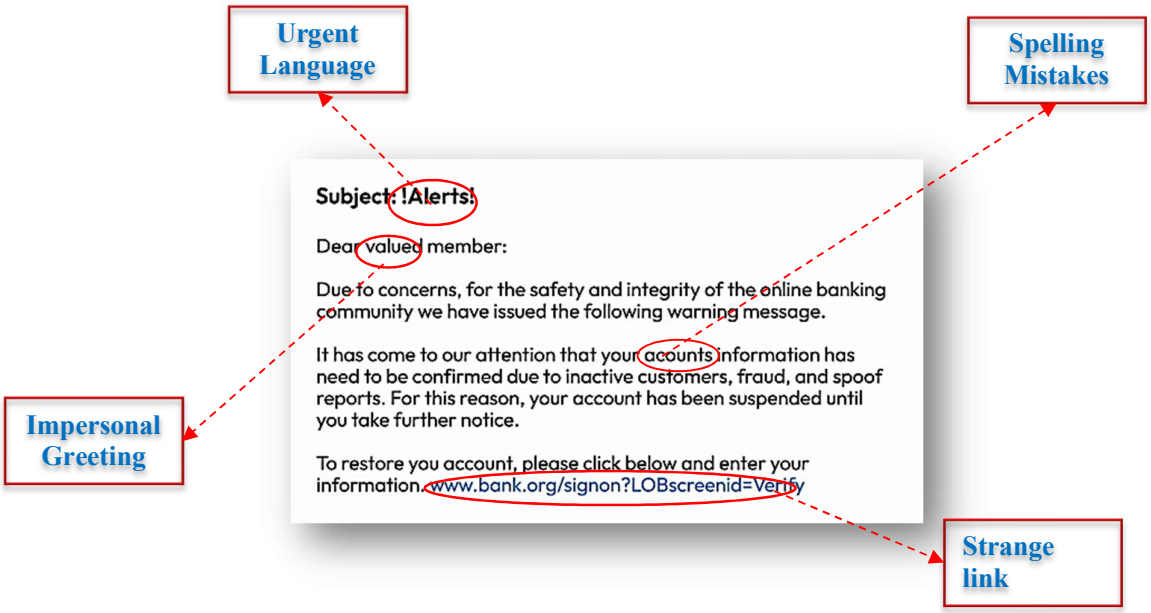
- टू-फैक्टर ऑथेंटिकेशन (2FA) चालू करें , ताकि अगर किसी को आपका पासवर्ड मिल भी जाए, तो वह आपके वेरिफिकेशन कोड के बिना लॉग इन न कर सके।

(बी) <u>फ़िशिंग ईमेल का पता लगाने के स्मार्ट तरीके</u>:-

फ़िशिंग ईमेल ऐसे धोखाधड़ी वाले संदेश होते हैं जो दिखने में आपके बैंक, सरकारी संस्थान या किसी प्रसिद्ध वेबसाइट की तरह लगते हैं। इनका उद्देश्य आपको भरोसे में लेकर आपकी संवेदनशील जानकारी—जैसे पासवर्ड, OTP या बैंक संबंधी विवरण—हड़पना होता है। इन्हें पहचानने में आसानी हो, इसके लिए नीचे दिए गए संकेतों पर ध्यान दें-

- भेजने वाले का ईमेल एड्रेस ध्यान से चेक करें। फ़िशिंग ईमेल अक्सर नकली एड्रेस से आते हैं जो असली एड्रेस जैसे ही दिखते हैं, जैसे **support@sbi.bank.in** की जगह **support@sbi-secure.com.** डोमेन में हमेशा स्पेलिंग की गलतियों या अतिरिक्त शब्दों को देखें।
- स्पेलिंग या व्याकरण की गलतियों पर ध्यान दें। असली कंपनियाँ हमेशा पेशेवर भाषा का उपयोग करती हैं। यदि किसी ईमेल में खराब व्याकरण, अटपटी भाषा या रैंडम कैपिटल लेटर दिखें, तो यह नकली हो सकता है।
- अर्जेंट या डराने वाले संदेशों से सावधान रहें। जैसे "आपका खाता बंद कर दिया जाएगा!" या "दंड से बचने के लिए अभी क्लिक करें!" जैसे वाक्य अक्सर आपको घबराने और जल्दबाजी में निर्णय लेने पर मजबूर करने के लिए होते हैं। असली संस्थान आमतौर पर ग्राहकों को ईमेल के माध्यम से धमकी नहीं देते।
- लिंक पर क्लिक करने से पहले हमेशा उन पर माउस घुमाएं; अगर वेबसाइट का एड्रेस अजीब या अनजान लगे, तो उसे न खोलें।
- अनजान ईमेल से अटैचमेंट कभी डाउनलोड न करें, उनमें वायरस हो सकते हैं।

- फ़िशिंग ईमेल अक्सर "प्रिय यूज़र" या "प्रिय ग्राहक" जैसे आम अभिवादन से शुरू होते हैं. असली कंपनियाँ आमतौर पर आपको आपके पूरे नाम से बुलाती हैं.



1.) **<u>पावर बीआई</u>**

4. सूचना प्रौद्योगिकी निदेशालय की नवीन गतिविधियाँ

- आयुष्मान कार्ड स्टेटस रिपोर्ट
- ई-बिल स्टेटस रिपोर्ट
- WARB (कल्याण और पुनर्वास बोर्ड) से रिटायर हुए कार्मिकों की सूची।

2.) **<u>पीपीएमएस (पेपरलेस प्रोसेस मैनेटमेंट सिस्टम)</u>**

- अपॉइंटमेंट करेक्शन ऑर्डर (नॉन-एक्टिव कार्मिकों के लिए)
- पोस्टिंग ऑर्डर (अपडेशन)
- रिकवरी ऑर्डर एनजीओ (अपडेशन) ।

राष्ट्रीय वंदेमातरम के 150 साल पूरे होने के उपलक्ष्य में सीआरपीएफ के जवानों ने नई दिल्ली में बल मुख्यालय सहित सभी इकाइयों, कार्यालयों और संस्थानों में वंदे मातरम गीत गाया।

सानिध्य पुस्तक का विमोचन

सीआरपीएफ स्कूल का वार्षिक समारोह

पीएनबी बैंक के साथ MoU