केंद्रीय रिज़र्व पुलिस बल

मार्च, 2026

साइबर बाइट

साइबर अपराध विशेषज्ञ ने एआई-आधारित बायोमेट्रिक घोटाले पर चेतावनी जारी की

सिम बॉक्स घोटाले का पर्दाफाश: गुरुग्राम में हुई गिरफ्तारी से चीन से जुड़े साइबर नेटवर्क का खुलासा

महानिरीक्षक, संचार एवं सूचना प्रौद्योगिकी निदेशालय, सीआरपीएफ

1. साइबर की दुनिया की खबरें

(ए) सिम बॉक्स घोटाले के अंदर: गुरुग्राम में हुई गिरफ्तारी ने चीन से जुड़े साइबर नेटवर्क का भंडाफोड़ किया।

गुरुग्राम पुलिस ने गृह मंत्रालय के तहत आने वाले **'भारतीय साइबर अपराध समन्वय केंद्र' (I4C)** के साथ एक संयुक्त अभियान में नागालैंड की एक 30 वर्षीय महिला को गिरफ्तार किया था। उस पर कथित तौर पर चीन से जुड़े एक साइबर धोखाधड़ी नेटवर्क की मदद करने का आरोप है। इस गिरफ्तारी ने शहर के एक किराए के अपार्टमेंट से चलाए जा रहे सीमा पार के घोटाले का खुलासा किया, जिससे भारत में अंतर्राष्ट्रीय साइबर अपराध की बढ़ती पहुंच को लेकर नई चिंताएं पैदा हो गई हैं।

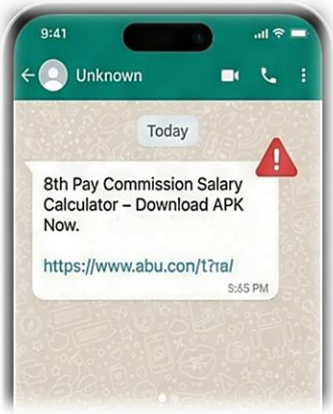
पुलिस अधिकारियों के अनुसार, महिला ने अपने पति के साथ मिलकर अपने किराए के फ्लैट में एक 'वर्चुअल सिम बॉक्स सिस्टम' लगाया था, जो अंतर्राष्ट्रीय वीओआईपी (VoIP) कॉल को भारतीय स्थानीय कॉल में बदल देता था। इस प्रक्रिया से ऐसा प्रतीत होता है मानो कॉल भारत के भीतर से ही आ रही हों, जिससे प्राधिकारियों के लिए इसके असली स्रोत का पता लगाना और भी मुश्किल हो जाता है। साइबर अपराधियों द्वारा देश भर में पीड़ितों को निशाना बनाते समय पकड़े जाने से बचने के लिए आमतौर पर ऐसे सिस्टम का प्रयोग किया जाता है।

जांचकर्ताओं ने खुलासा किया कि इस सेटअप में कई फोन और सिम कार्ड शामिल थे, जो **"VDMS Apk"** नामक ऐप का उपयोग करके स्वचालित कॉल करते थे—जो धोखाधड़ी के कार्यों में उपयोग किया जाने वाला एक सामान्य उपकरण है। आरोपी कथित तौर पर इन उपकरणों को चार्ज रखकर और इंटरनेट से जोड़कर उन्हें चालू रखने में मदद करती थी, जिससे विदेशी धोखेबाज भारतीय नागरिकों को बड़ी संख्या में कॉल कर सकें। कथित तौर पर इन कॉलों का उपयोग फर्जी निवेश योजनाओं, डिजिटल अरेस्ट की धमकी और अन्य ऑनलाइन वित्तीय धोखाधड़ी जैसी विभिन्न ठगी के लिए किया जाता था।

सिम-बॉक्स डिवाइस की कार्यप्रणाली (Working of SIM-Box Device):

(B) आई4सी(I4C) ने आठवें वेतन आयोग ऐप घोटाले के खिलाफ कर्मचारियों को किया आगाह।

भारतीय साइबर अपराध समन्वय केंद्र (I4C) ने प्रस्तावित आठवें केंद्रीय वेतन आयोग से जुड़ी एक नई धोखाधड़ी के बारे में सरकारी कर्मचारियों के लिए चेतावनी जारी की है। केंद्रीय गृह मंत्रालय ने यह चेतावनी तब जारी की है, जब ऐसी रिपोर्टें सामने आई हैं कि जालसाज़ एक फ़र्ज़ी मोबाइल एप्लिकेशन के ज़रिए कर्मचारियों को निशाना बना रहे हैं।



अधिकारियों के अनुसार, धोखेबाज व्हाट्सएप के माध्यम से लिंक फैला रहे हैं, जिसमें दावा किया जा रहा है कि यह ऐप आगामी वेतन आयोग के तहत संशोधित वेतन के लिए 'सैलरी कैलकुलेटर' प्रदान करता है। इन संदेशों को आधिकारिक दिखाने के लिए डिजाइन किया गया है और इनमें जल्दबाजी का माहौल बनाया जाता है ताकि लोग ऐप को तुरंत डाउनलोड कर लें। हालांकि, प्राधिकारियों ने स्पष्ट किया है कि आठवें वेतन आयोग के संबंध में कोई भी आधिकारिक सैलरी कैलकुलेटर या मोबाइल ऐप लॉन्च **नहीं** किया गया है। इस फर्जी ऐप का उद्देश्य बैंक विवरण, आधार नंबरों, पैन की जानकारी, पासवर्ड और ओटीपी (OTP) सहित संवेदनशील व्यक्तिगत और वित्तीय जानकारी को चुराना है। कुछ मामलों में, यह डिवाइस में मैलवेयर(malware) भी इंस्टॉल कर सकता है, जिससे उपयोगकर्ताओं को वित्तीय हानि या पहचान की चोरी का और अधिक खतरा हो सकता है।

कर्मचारियों को सख्त हिदायत दी गई है कि वे किसी भी अज्ञात लिंक पर क्लिक न करें और अनधिकृत स्रोतों से एप्लिकेशन डाउनलोड न करें। उन्हें वेतन आयोग के बारे में किसी भी अपडेट की पुष्टि केवल आधिकारिक सरकारी वेबसाइटों (**8cpc.gov.in**) के माध्यम से करनी चाहिए और संदिग्ध संदेशों की रिपोर्ट राष्ट्रीय साइबर अपराध पोर्टल (**cybercrime.gov.in**) पर करनी चाहिए। प्राधिकारियों ने सभी से सतर्क रहने का आग्रह किया है, क्योंकि साइबर अपराधी अक्सर बड़ी सरकारी घोषणाओं में जनता की रुचि का फायदा उठाते हैं।

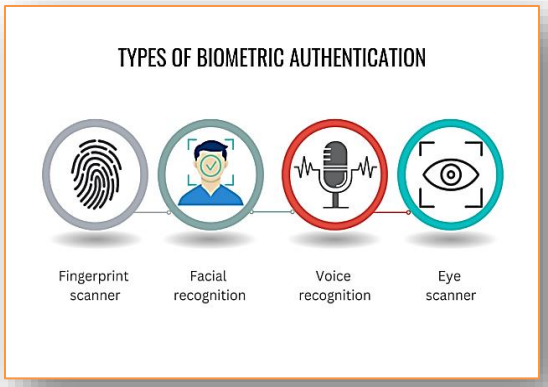
<u>यदि आपने ऐप पहले ही इंस्टॉल कर लिया है, तो ये कदम उठाएं :-</u>

- तुरंत एयरप्लेन मोड (**Airplane Mode**) ऑन करें
- ऐप को अनइंस्टॉल (**Uninstall**) करें
- सिक्योरिटी या एंटीवायरस **स्कैन** चलाएं
- बैंकिंग और ईमेल के **पासवर्ड** बदलें
- अपने बैंक को **सूचित** करें
- **1930** (भारत की साइबर अपराध हेल्पलाइन) पर कॉल करें या **cybercrime.gov.in** पर रिपोर्ट करें।

2. साइबर धोखाधड़ी

(ए) साइबर अपराध विशेषज्ञ ने एआई-आधारित बायोमेट्रिक धोखाधड़ी पर अलर्ट जारी किया :

साइबर अपराध विशेषज्ञ ने लोगों को एक नए प्रकार की **धोखाधड़ी** के बारे में चेतावनी दी है जो बायोमेट्रिक डेटा चुराने के लिए **आर्टिफिशियल इंटेलिजेंस (AI)** का उपयोग करता है। फिशिंग या वित्तीय धोखाधड़ी के माध्यम से मुख्य रूप से पैसा चुराने वाले पारंपरिक **धोखाधड़ी** के विपरीत, यह नया खतरा चेहरे के हाव-भाव और आवाज के नमूनों जैसी संवेदनशील बायोमेट्रिक जानकारी हासिल करने पर लक्षित है—ऐसा डेटा जिसे एक बार चोरी होने के बाद पासवर्ड या ओटीपी की तरह बदला नहीं जा सकता।



साइबर अपराध विशेषज्ञ के अनुसार, धोखेबाज, लोगों की जानकारी के बिना उनके चेहरे और आवाज जैसे बायोमेट्रिक विवरण एकत्र करने के लिए चालाकी भरे(स्मार्ट) और गुप्त तरीकों का उपयोग कर रहे हैं। उन्होंने कहा कि यह धोखाधड़ी शॉपिंग मॉल, मेट्रो स्टेशन और अन्य भीड़भाड़ वाले व्यस्त स्थानों पर देखी गयी है। इन जगहों पर, लोग आमतौर पर व्यस्त होते हैं और उन्हें इस बात का एहसास होने की संभावना कम होती है कि कोई गुप्त रूप से उनकी जानकारी रिकॉर्ड या इकट्ठा कर रहा है।

एआई-आधारित बायोमेट्रिक धोखाधड़ी कैसे काम करती है ? :

धोखेबाज़ अक्सर बुजुर्ग या अधेड़ उम्र के लोगों का रूप धरते हैं ताकि किसी को उन पर शक न हो। सार्वजनिक स्थानों पर सीधे-सादे दिखकर और सामान्य व्यवहार करके, वे बिना किसी का ध्यान आकृष्ट किए आराम से इधर-उधर घूम-फिर पाते हैं। वे किसी व्यक्ति की आवाज को गुप्त रूप से रिकॉर्ड करने के लिए साधारण और दोस्ताना बातचीत शुरू कर सकते हैं। वे किसी के चेहरे की स्पष्ट तस्वीरें या वीडियो लेने के लिए छिपे हुए कैमरों या मोबाइल फोन का भी प्रयोग कर सकते हैं। कभी-कभी, वे ऐसा दिखाते हैं जैसे कि वे कोई सर्वे कर रहे हों, किसी से रास्ता पूछ रहे हों, या बस हल्की-फुल्की बातचीत कर रहे हों, और इसी दौरान वे चुपके से आवाज़ और चेहरे के विवरण इकट्ठा कर लेते हैं।

बाद में, वे इस जानकारी की नकल(कॉपी) करने या उसे फिर से बनाने के लिए उन्नत एआई टूल का उपयोग करते हैं। आज **कृत्रिम बुद्धिमत्ता** (आर्टिफिशियल इंटेलिजेंस) किसी व्यक्ति के चेहरे, आवाज और हाव-भाव का बारीकी से अध्ययन कर सकती है। पर्याप्त डेटा के साथ, अपराधी नकली वीडियो (डीपफेक) या क्लोन की गई वॉयस रिकॉर्डिंग बना सकते हैं जो सुनने और देखने में बिल्कुल असली लगती हैं, जिससे उनके लिए किसी और का रूप धारण करना आसान हो जाता है।

यह क्यों खतरनाक है ?

आजकल, कई ऐप्स और ऑनलाइन सेवाएँ आपकी पहचान की पुष्टि करने के लिए **'फेस रिकग्निशन (चेहरा पहचानने वाली तकनीक)** या **'वॉइस वेरिफिकेशन'** (आवाज की पुष्टि) का उपयोग करती हैं। लेकिन पासवर्ड की तरह, आप अपना चेहरा या आवाज़ आसानी से बदल नहीं सकते। अगर कोई आपकी बायोमेट्रिक जानकारी चुरा ले, तो उसका दुरुपयोग लंबे समय तक किया जा सकता है।

अपराधी चोरी की गई इस जानकारी का उपयोग आपकी ऑनलाइन पहचान बनाकर, आपके बैंक खातों या डिजिटल वॉलेट तक पहुँचने की कोशिश करने, आपके नाम पर फ़र्जी वीडियो या वॉयस (आवाज़) रिकॉर्डिंग बनाने, या पहचान की चोरी करने के लिए कर सकते हैं।

- **अजनबियों से अनावश्यक बात करने से बचें।**
- **यदि आपके पास कोई रिकॉर्डिंग कर रहा हो, तो सावधान रहें।**
- **सार्वजनिक रूप से जोर-जोर से व्यक्तिगत विवरण साझा न करें।**
- **किसी भी संदिग्ध गतिविधि की सूचना तुरंत साइबर अपराध प्राधिकारियों को दें।**

(बी) अंतर्राष्ट्रीय साइबर अपराध अभियान में वैश्विक 'फिशिंग-एज़-ए-सर्विस' प्लेटफॉर्म टायकून 2FA ("Tycoon 2FA)" को बाधित किया गया।

टायकून **2FA (Tycoon 2FA)** के नाम से मशहूर एक बड़े **'फिशिंग-एज़-ए-सर्विस'** प्लेटफॉर्म को यूरोपोल **(Europol)** के द्वारा समर्थित एक समन्वित अंतर्राष्ट्रीय अभियान में बंद कर दिया गया है। इस प्लेटफॉर्म का उपयोग साइबर अपराधियों के द्वारा बड़े पैमाने पर ऐसे फिशिंग हमले करने के लिए किया जाता था, जो **'मल्टी-फैक्टर अथेंटिकेशन' (MFA)** को बायपास कर सकते थे और ऑनलाइन खातों तक अनधिकृत पहुँच प्राप्त कर लेते थे। प्राधिकारियों का कहना है कि यह कार्रवाई उन संगठित साइबर अपराध नेटवर्कों का मुकाबला करने के व्यापक प्रयासों का हिस्सा है, जो दुनिया भर के अपराधियों को तैयार हैकिंग टूल प्रदान करते हैं। टायकून **2FA (Tycoon 2FA)** एक सब्सक्रिप्शन-आधारित सेवा के रूप में संचालित होता था, जिसने हमलावरों को उन्नत तकनीकी ज्ञान के बिना भी जटिल फिशिंग अभियान को चलाने की सुविधा दी। इस प्लेटफॉर्म के उपयोगकर्ता तैयार फिशिंग पेजों तक पहुँच सकते थे, जिन्हें असली लॉगिन पोर्टल की तरह दिखने के लिए डिज़ाइन किया गया था, साथ ही इसमें दुर्भावनापूर्ण (malicious)

वेबसाइटों को होस्ट करने के टूल और चोरी किए गए क्रेडेंशियल्स (यूजर आईडी और पासवर्ड) को ट्रैक करने के लिए डैशबोर्ड भी उपलब्ध थे। साइबर अपराध के लिए तकनीकी बाधाओं को कम करके, इस सेवा ने कई हमलावरों को बड़े पैमाने पर व्यक्तियों और संगठनों को निशाना बनाने वाले फिशिंग अभियान(ऑपरेशन) को चलाने में सक्षम बनाया।

टाइकून 2एफए **(Tycoon 2FA)** की सबसे खतरनाक विशेषताओं में से एक **'एडवर्सरी-इन-द-मिडल' (Adversary-in-the-middle)** नामक तकनीक का उपयोग करके एमएफए (MFA) सुरक्षा को बायपास (दरकिनार) करने की क्षमता थी। इन हमलों में, पीड़ितों को एक फिशिंग लिंक पर क्लिक करने के लिए बरगलाया जाता है, जो उन्हें एक नकली लॉगिन पेज पर ले जाता है, जो काफी हद तक असली वेबसाइट जैसा दिखती है। जब पीड़ित अपना यूजरनेम, पासवर्ड और एमएफए (MFA) कोड दर्ज करता है, तो प्लेटफॉर्म वास्तविक समय(real-time) में उस जानकारी को बीच में ही रोक लेता है और प्रमाणित सत्र (authenticated session) को कैप्चर कर लेता है। इससे हमलावरों को दोबारा क्रेडेंशियल दर्ज किए बिना पीड़ित के खाते तक पहुँचने की अनुमति मिल जाती है।

सुरक्षा विशेषज्ञों का कहना है कि माइक्रोसॉफ्ट और गूगल जैसी कंपनियों की प्रमुख क्लाउड सेवाओं से जुड़े खाते आम लक्ष्यों में शामिल थे, क्योंकि इन खातों तक पहुँच प्राप्त करने से कॉर्पोरेट ई-मेल, संवेदनशील दस्तावेज़ और आंतरिक प्रणालियां (सिस्टम) उजागर हो सकती हैं। इस तरह की सेंधमारी से संगठनों के भीतर डेटा की चोरी, वित्तीय धोखाधड़ी और साइबर हमले हो सकते हैं।

- **हमेशा वेबसाइट के यूआरएल (URL) की सावधानीपूर्वक जाँच करें**
  - गलत वर्तनी वाले डोमेन पर ध्यान दें (जैसे, microsoft.com की बजाय **micros0ft.com**)
  - सुनिश्चित करें कि URL **https://** से शुरू होता हो
  - ई-मेल या एसएमएस में दिए गए लिंक से लॉगिन करने से बचें

- **मजबूत और यूनिक (विशिष्ट) पासवर्ड का उपयोग करें**
- **प्रेषक के ई-मेल पते की जाँच करें**
  - **फर्जी :** support@micr0soft-security.com
  - **असली:** support@microsoft.com
- **डिवाइस को अपडेट रखें**
  - ऑपरेटिंग सिस्टम
  - ब्राउज़र
  - सुरक्षा सॉफ्टवेयर

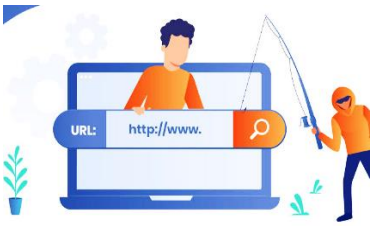
- **लॉगिन पेज किस तरह से काम कर रहा है इसकी जाँच करें (एक असली साइट, फ़िशिंग पेज से अलग तरह से काम करती है)**

✅ **असली साइट (Real site):**

- पासवर्ड मैनेजर अपने आप लॉगिन विवरण भर देता है
- डोमेन आधिकारिक वेबसाइट से मेल खाता है
- HTTPS सर्टिफिकेट उसी कंपनी का होता है

❌ **फिशिंग साइट :**

- पासवर्ड मैनेजर विवरण ऑटो-फिल नहीं करता
- पेज असली दिखता है लेकिन यूआरएल (URL) अजीब होता है
- लॉगिन पेज किसी रैंडम लिंक से खुलता है



3.इस महीने के सुझाव (Tips of the Month)

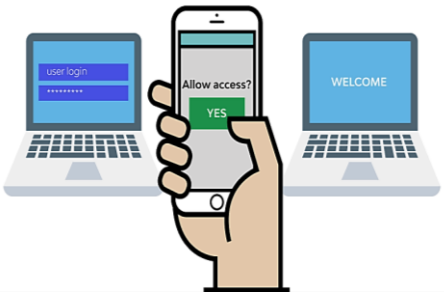
(क) सिस्टम और सॉफ्टवेयर अपडेट की जाँच करें :-

सिस्टम और सॉफ्टवेयर अपडेट की नियमित रूप से जाँच करना, आपके डिवाइस को फ़िशिंग किट, मैलवेयर और अकाउंट-चोरी करने वाले टूल्स जैसे साइबर खतरों से बचाने का सबसे आसान और सबसे असरदार तरीका है। ओएस (OS), ब्राउज़र और ऐप्स को अपडेट रखें; उदाहरण के लिए: विंडोज 11, काली लिनक्स और गूगल क्रोम नियमित रूप से सुरक्षा पैच जारी करते हैं।

(ख) लॉगिन गतिविधि (Login Activity) पर नज़र रखें :-

लॉगिन गतिविधि की निगरानी करने से आपको यह जल्दी पता लगाने में मदद मिलती है कि क्या कोई और आपके खातों तक पहुँचने की कोशिश कर रहा है। कई प्रमुख सेवाएँ सुरक्षा डैशबोर्ड प्रदान करती हैं, जहाँ आप हाल के लॉगिन के डिवाइस, लोकेशन(स्थान) और समय को देख सकते हैं। यदि आपको कोई अज्ञात डिवाइस या लोकेशन(स्थान) दिखाई देता है, तो तुरंत साइन आउट करें और अपना पासवर्ड बदलें।

(ग) मल्टी-फैक्टर ऑथेंटिकेशन (MFA) सक्षम करें :-



मल्टी-फैक्टर ऑथेंटिकेशन (MFA) सक्षम करने से आपके खातों में सुरक्षा की एक अतिरिक्त परत जुड़ जाती है। भले ही कोई फिशिंग या मैलवेयर के माध्यम से आपका पासवर्ड चुरा ले, वे दूसरे वेरिफिकेशन स्टेप (सत्यापन चरण) के बिना लॉगिन नहीं कर पाएंगे। यह खातों को फिशिंग और पासवर्ड लीक जैसे हमलों से बचाता है।

(घ) मैलवेयर के लिए डिवाइस को स्कैन करें :-

मैलवेयर के लिए अपनी डिवाइस को नियमित रूप से स्कैन करने से उन हानिकारक सॉफ़्टवेयर का पता लगाने और उन्हें हटाने में मदद मिलती है जो पासवर्ड चुरा सकते हैं, आपकी गतिविधि की निगरानी कर सकते हैं या फिशिंग हमलों को बढ़ावा दे सकते हैं। ये खतरे माइक्रोसॉफ्ट विंडोज, एंड्रॉइड और मैक ओएस (mac OS) जैसे सिस्टम पर चलने वाले कंप्यूटर और स्मार्टफोन को निशाना बना सकते हैं।

4. सूचना प्रौद्योगिकी निदेशालय में नए विकास

1) पीपीएमएस (कागज रहित प्रक्रिया प्रबंधन प्रणाली)

- डी.सी.पी.एस. वसूली (अंशदायी पेंशन योजना की राशि की वसूली)

2.) पावर बी.आई.-

- सिग्नल वैयक्तिक (Personal) रिपोर्ट
- तैनात यूनिट के अनुसार सी.आर.पी.एफ. की नफरी की रिपोर्ट

श्री जी.पी. सिंह (आईपीएस), महानिदेशक, के0रि.0पु0बल ने रक्तदान शिविर में रक्तदान करते हुए ।

श्री जी.पी. सिंह (आईपीएस), महानिदेशक, के0रि.0पु0बल ने 26वीं अखिल भारतीय पुलिस शुटिंग प्रतियोगिता में उपस्थित के दौरान।

श्री जी.पी. सिंह (आईपीएस), महानिदेशक, के0रि.0पु0बल ने **IIM Pune** में **BDD** गाइड प्रकाशित करते हुए ।