केंद्रीय रिज़र्व पुलिस बल

जनवरी, 2026

साइबर बोर्ड

गूगल ने रेड अलर्ट जारी किया है क्योंकि नया साइबर हमला 'अप्रत्यक्ष त्वरित इंजेक्शन' के साथ एआई का उपयोग करने वाले जीमेल उपयोगकर्ताओं को लक्षित करता है

FileFix हमला स्टेग्नोग्राफ़ीकाउपयोग करके StealC मैलवेयर को हटाता है

महानिरीक्षक, संचार एवं सूचना प्रौद्योगिकी निदेशालय, सीआरपीएफ

1. साइबर की दुनिया की

(A) नए साल की शुभकामनाओं वाले फर्जी लिंक से साइबर क्राइम का अलर्ट जारी हुआ।

साइबर अपराध विशेषज्ञ ने जनहित में सूचना जारी कर डिजिटल प्लेटफार्मों पर प्रसारित हो रहे नए साल की शुभकामनाओं वाले फर्जी लिंक और दुर्भावनापूर्ण एपीके फ़ाइलों से जुड़े साइबर धोखाधड़ी के मामलों में तेजी से वृद्धि के प्रति आगाह किया है। साइबर अपराधी एसएमएस, व्हाट्सएप, सोशल मीडिया और ईमेल के माध्यम से नए साल की शुभकामनाओं, उपहारों या वीडियो कार्ड की पेशकश करने वाले भ्रामक संदेश भेजकर त्योहारी सीजन का फायदा उठा रहे हैं। इन संदेशों में अक्सर **"NewYear.apk"** जैसे नामों वाली संदिग्ध लिंक या एपीके फ़ाइलें होती हैं, जिन्हें एक बार क्लिक या इंस्टॉल करने पर मोबाइल फोन और एप्लिकेशन, जिनमें मैसेजिंग ऐप भी शामिल हैं, जोखिम में पड सकते हैं। इससे व्यक्तिगत डेटा, बैंकिंग क्रेडेंशियल(बैंक खाते से जुड़ी गोपनीय जानकारी) की चोरी हो सकती है और वित्तीय व सोशल मीडिया खातों तक अनधिकृत पहुंच मिल सकती है।

इस सलाह में लोगों से निवेदन किया गया है कि वे सतर्क रहें और लाल झंडों पर ध्यान दें, जैसे कि तत्काल कार्रवाई की मांग करने वाले या दंड की धमकी देने वाले संदेशों, एपीके फ़ाइलों को डाउनलोड करने या अज्ञात स्रोतों से इंस्टॉलेशन को सक्षम करने के अनुरोध, और किसी भी लेनदेन या अनुरोध के बिना ओटीपी प्राप्त होना।

- अज्ञात या संदिग्ध लिंक पर क्लिक न करें।
- संदेशों या सोशल मीडिया के माध्यम से भेजी गई एपीके फ़ाइलों को कभी भी इंस्टॉल न करें।
- अपने फ़ोन पर "अज्ञात स्रोतों से इंस्टॉल करें" (Install from unknown sources) को अक्षम (Disable) करें।
- ओटीपी(OTP), पिन(PIN), या बैंकिंग विवरण साझा न करें।
- एसएमएस तक पहुंच या ओटीपी जैसी अनुमतियां मांगने वाले लिंक से सावधान रहें।

- मैसेजिंग ऐप्स पर दो-चरणीय सत्यापन (two-step verification) और मजबूत सुरक्षा सेटिंग्स को सक्षम करें।
- संदिग्ध संदेशों की साइबर अपराध प्राधिकारियों को रिपोर्ट करें 1930 (तत्काल रिपोर्टिंग) cybercrime.gov.in

(B) दूरसंचार विभाग (DoT) का वित्तीय धोखाधड़ी जोखिम संकेतक ₹660 करोड़ के नुकसान को रोकने में मदद करता है

बढ़ती डिजिटल वित्तीय धोखाधड़ी के खिलाफ भारत की लड़ाई में एक बड़ी सफलता मिली है। **दूरसंचार विभाग** (DoT) ने खुलासा किया कि उसके वित्तीय धोखाधड़ी जोखिम संकेतक (Financial Fraud Risk Indicator - FRI) ने लॉन्च होने के महज छह महीनों में ही लगभग ₹660 करोड़ के संभावित नुकसान को रोकने में मदद की है। यह पहल एक तेजी से बढ़ती डिजिटल अर्थव्यवस्था में नागरिकों की सुरक्षा के लिए दूरसंचार प्राधिकारियों, बैंकों और डिजिटल भुगतान प्लेटफार्मों के बीच बढ़ते समन्वय को दर्शाती है।

फिशिंग, फर्जी कॉल, पहचान की चोरी और यूपीआई(UPI) से संबंधित धोखाधड़ी सहित साइबर-सक्षम वित्तीय अपराधों पर अंकुश लगाने के लिए सरकार की व्यापक रणनीति के हिस्से के रूप में 22 मई, 2025 को एफआरआई(FRI) प्रणाली शुरू की गई थी। इसके शुरू होने के बाद से, इस टूल ने धोखेबाजों द्वारा पैसे की हेराफेरी से करने से पहले संदिग्ध लेनदेन का पता लगाने और उसे बाधित करने में महत्वपूर्ण भूमिका निभाई है।

"वित्तीय धोखाधड़ी जोखिम संकेतक कैसे काम करता है"

वित्तीय धोखाधड़ी जोखिम संकेतक (Financial Fraud Risk Indicator) एक आसूचना संचालित प्रणाली है जो संभावित वित्तीय धोखाधड़ी से जुड़े मोबाइल नंबरों की पहचान करती है। दूरसंचार सेवा प्रदाताओं, साइबर अपराध शिकायत डेटाबेस और वित्तीय संस्थानों से प्राप्त जानकारियों का उपयोग करके, यह प्रणाली धोखाधड़ी वाली गतिविधियों में इस्तेमाल होने वाले संदिग्ध मोबाइल नंबरों को मध्यम, उच्च या अत्यधिक जैसे जोखिम स्तर निर्धारित करती है।

फिर तुरंत प्रतिक्रिया देते हुए ये जोखिम संकेतक (indicators) बैंकों, यूपीआई प्लेटफॉर्मों और भुगतान प्रणाली ऑपरेटरों के साथ साझा किए जाते हैं। अलर्ट स्तर के आधार पर, वित्तीय संस्थान सुरक्षात्मक कार्रवाई कर सकते हैं जैसे कि लेन-देन में विलंब, भुगतान को ब्लॉक करना, अतिरिक्त सत्यापन मांगना या ग्राहकों को चेतावनी जारी करना। इस अग्रसक्रिय दृष्टिकोण ने धोखाधड़ी के सफल प्रयासों की संभावनाओं को काफी कम कर दिया है।

नागरिकों की भागीदारी

संचार साथी (Sanchar Saathi) जैसे प्लेटफार्मों के माध्यम से नागरिकों की भागीदारी प्रणाली में संदिग्ध गतिविधि की जमीनी स्तर की रिपोर्टों को फीड करने में मदद करती है, जिससे एफआरआई का खुफिया आधार मजबूत होता है।

एफआरआई (FRI) प्रणाली क्यों महत्वपूर्ण है

जैसे-जैसे भारत में डिजिटल भुगतान और मोबाइल बैंकिंग तेजी से बढ़ रहा है, साइबर-सक्षम वित्तीय धोखाधड़ी एक प्रमुख चिंता का विषय रहा है। **एफआरआई(**FRI) अन्य सुरक्षा उपायों का पूरक है, जो शुरुआती चेतावनियाँ और कार्रवाई योग्य जोखिम स्कोर प्रदान करता है जिनका उपयोग वित्तीय संस्थाएँ अग्रसक्रिय रूप से धोखाधड़ी को रोकने के लिए कर सकती हैं।

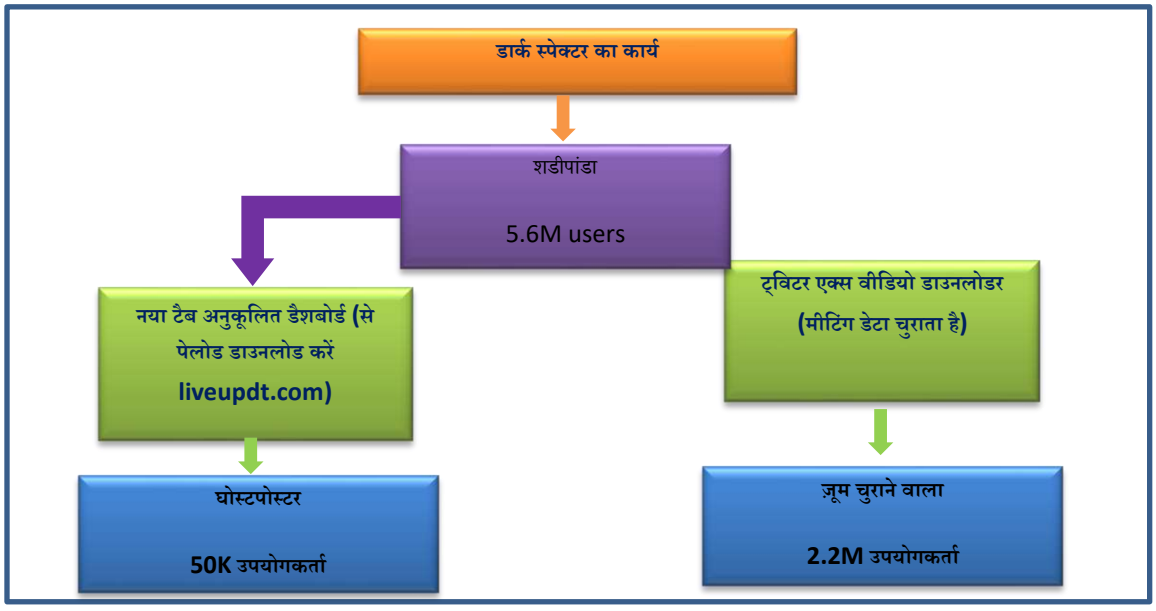
- **धनराशि खोने से पहले काम करता है.**
- **दूरसंचार, बैंकिंग और कानून प्रवर्तन का एकीकृत समन्वय**
- **राष्ट्रीय साइबर सुरक्षा के लिए एक विस्तारयोग्य प्रारूप (स्केलेबल मॉडल).**

2. साइबर धोखाधड़ी

(A) डार्कस्पेक्ट्रे (DarkSpectre) हैकर्स ने मैलवेयर से 88 लाख क्रोम, एज और फायरफॉक्स उपयोगकर्ताओं को संक्रमित किया :-

डार्कस्पेक्ट्रे एक परिष्कृत और लंबे समय से चल रहे मैलवेयर ऑपरेशन को संदर्भित करता है, जिसमें धमकी देने वालों ने गूगल क्रोम, माइक्रोसॉफ्ट एज और मोज़िला फायरफॉक्स के आधिकारिक एक्सटेंशन स्टोर के माध्यम से हानिकारक 'ब्राउज़र एक्सटेंशन' बांट कर अनुमानित 88 लाख उपयोगकर्ताओं को प्रभावित किया। ये एक्सटेंशन असली लगते थे और शुरू में अक्सर वास्तविक कार्यक्षमता प्रदान करते थे, जिससे उन्हें बड़ी संख्या में डाउनलोड और सकारात्मक समीक्षाएं प्राप्त करने में मदद मिलीं।

लेकिन उनमें गुप्त रूप से छिपा हुआ या निष्क्रिय कोड होता था जिसे बाद में अपडेट या रिमोट कमांड के माध्यम से सक्रिय किया गया था। सक्रिय होने के बाद, इस मैलवेयर ने व्यापक निगरानी क्षमताओं को सक्षम किया, जिसमें ब्राउजिंग गतिविधि को ट्रैक करना, कुकीज़ और सत्र के डेटा(session data) को चुराना, विज्ञापन डालना, ट्रैफ़िक को रि-डायरेक्ट करना और कुछ मामलों में ऑनलाइन मीटिंग यूआरएल(URL), आईडी, प्रतिभागियों के विवरण और एम्बेडेड क्रेडेंशियल्स (अंतर्निहित लॉगिन विवरण/पासवर्ड) जैसी संवेदनशील जानकारी एकत्र करना शामिल था। हमलावरों ने कोड को छिपाने (code obfuscation), देरी से निष्पादन और वैध क्लाउड सेवाओं पर होस्ट किए गए कमांड-एंड-कंट्रोल इन्फ्रास्ट्रक्चर जैसी उन्नत तकनीकों का उपयोग किया, जिससे इस अभियान का वर्षों तक पता नहीं चल पाया। शोधकर्ताओं ने डार्कस्पेक्ट्रे के तहत कई समन्वित उप-अभियानों की पहचान की है, जो एक संगठित और अच्छी तरह से संसाधनों से संपन्न हमलावर होने की ओर इशारा करते हैं, जिसमें बुनियादी ढांचे और विकास पैटर्न के आधार पर इसके चीन से जुड़े होने के प्रमाण भी मिले हैं। यह घटना ब्राउज़र एक्सटेंशन इकोसिस्टम में एक बड़े सुरक्षा जोखिम को रेखांकित करती है और यह दर्शाती है कि कैसे अत्यधिक अनुमतियों और उपयोगकर्ता के विश्वास का बड़े पैमाने पर दोहन किया जा सकता है, और यह ब्राउज़र ऐड-ऑन को स्थापित या अपडेट करते समय एक्सटेंशन की सख्ती से जाँच, निरंतर निगरानी और उपयोगकर्ता को अधिक सावधान होने की ज़रूरत पर ज़ोर देता है।



कैसे जांच करें कि क्या आप प्रभावित हो सकते हैं :

इंस्टॉल किए गए एक्सटेंशन की समीक्षा करें

- **क्रोम/एज(**Edge): **सेटिंग**(Settings) → एक्सटेंशन(Extensions)
- **फायर फॉक्स**(Firefox) : एड ऑन एवं विषय-वस्तु (Add-ons and themes)

  → एक्सटेंशन(Extensions)
- ऐसी किसी भी चीज़ को हटा दें जिसे आप स्पष्ट रूप से नहीं पहचानते या अब उपयोग नहीं करते हैं।

अनुमतियों (Permissions) की सावधानीपूर्वक जांच करें

- उन एक्सटेंशन पर संदेह करें जो बिना किसी ठोस कारण के वेबसाइटों के पूर्ण एक्सेस(पहुंच) की मांग करते हैं।
- प्रोडक्टिविटी या यूटिलिटी टूल्स को शायद ही कभी ब्राउज़िंग डेटा तक पहुंच की आवश्यकता होती है।

चेतावनी संकेतों पर ध्यान दें

- ब्राउज़र का धीमा होना, अप्रत्याशित रीडायरेक्ट, नए विज्ञापन या बदले हुए खोज परिणाम।
- बिना किसी स्पष्ट फीचर(रूप) परिवर्तन के बार-बार अपडेट होने वाले एक्सटेंशन।
- ब्राउज़र निष्क्रिय(idle) होने पर भी बैकग्राउंड गतिविधि का होना।

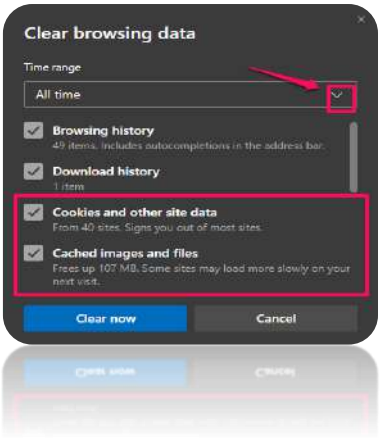
एक्सटेंशन अपडेट हिस्ट्री की जांच करें

- कुछ डार्कस्पेक्ट्रे(DarkSpectre) एक्सटेंशन शुरुआत में हानिरहित थे और बाद में अपडेट के माध्यम से मैलिशियस(दुर्भावनापूर्ण) हो गए।

सुरक्षा स्कैन चलाएं

- एक प्रतिष्ठित एंटीवायरस या एंडपॉइंट सुरक्षा टूल का उपयोग करें जिसमें ब्राउज़र एक्सटेंशन स्कैनिंग शामिल हो।

- **ब्राउज़र डेटा रीसेट करें (यदि संदिग्ध लगे)**



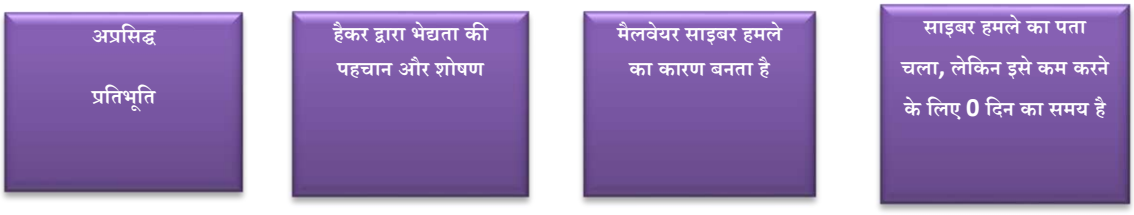
- कुकीज़ और साइट डेटा साफ़ करें।
- महत्वपूर्ण खातों से लॉग आउट करें और पासवर्ड बदलें, विशेष रूप से काम से संबंधित खातों के।

(B) व्हाट्सएप जीरो-डे अटैक (Zero-Day Attack): सिर्फ एक वॉइस कॉल से स्मार्टफोन हैक हो सकता है

साइबर सुरक्षा शोधकर्ताओं और सरकारी एजेंसियों ने हाल ही में रिपोर्ट की गई व्हाट्सएप जीरो-डे भेद्यता(vulnerability) पर गंभीर चिंता जताई है जो हमलावरों को केवल इनकमिंग वॉयस कॉल के माध्यम से स्मार्टफोन को जोखिम में डालने की अनुमति दे सकती है, भले ही पीड़ित उस कॉल का उत्तर न दे या किसी भी तरह से इंटरैक्ट(बातचीत) न करे। माना जाता है कि यह दोष व्हाट्सएप के वॉइस-कॉलिंग की प्रक्रिया में है, जो 'जीरो-क्लिक' हमले को सक्षम बनाता है। इसमें कॉल प्राप्त होते ही बैकग्राउंड में चुपचाप मैलिशियस(दुर्भावनापूर्ण) कोड सक्रिय हो सकता है। चूंकि यह एक जीरो-डे भेद्यता(vulnerability) है, इसलिए उपयोगकर्ताओं को बिना पता चले हमलावरों को निशाना बनाने का अवसर मिल गया होगा। विशेषज्ञों ने चेतावनी दी है कि इस खामी का सफलतापूर्वक लाभ उठाने पर रिमोट कोड निष्पादन, निजी चैट, फ़ोटो, संपर्कों (contacts) तक अनधिकृत पहुँच और यहां तक कि लंबे समय तक निगरानी रखने में सक्षम स्पाइवेयर इंस्टॉल किया जा सकता है। वित्तीय संस्थानों और साइबर सुरक्षा अधिकारियों ने, विशेष रूप से मध्य पूर्व (Middle East) में, बैंकिंग ग्राहकों, पत्रकारों, अधिकारियों और अन्य महत्वपूर्ण व्यक्तियों (high-value targets के लिए बढ़े हुए जोखिम पर जोर देते हुए "हाई अलर्ट" चेतावनी जारी की है। जब तक आधिकारिक पैच पूरी तरह से लागू नहीं हो जाता, उपयोगकर्ताओं को व्हाट्सएप और ऑपरेटिंग सिस्टम के उपलब्ध अपडेट तुरंत इंस्टॉल करने की सलाह दी जाती है।

शून्य-दिन भेद्यता क्या है?

शून्य-दिन की भेद्यता सॉफ्टवेयर या सिस्टम में एक छिपी हुई कमजोरी है जिसके बारे में इसे बनाने वाली कंपनी को अभी तक पता नहीं है। क्योंकि वे नहीं जानते कि यह मौजूद है, कोई फिक्स या अपडेट उपलब्ध नहीं है। हैकर्स इस कमजोरी का फायदा उठाकर सिस्टम पर हमला कर सकते हैं, इससे पहले कि कोई इसे रोक सके। इसे "शून्य-दिन" कहा जाता है क्योंकि डेवलपर के पास समस्या को ठीक करने के लिए शून्य दिन हैं।



उपयोगी सलाह :

- ऐप स्टोर या गूगल प्ले से अपडेट आते ही इंस्टॉल करें (सुरक्षा पैच आने की संभावना है)
- अपने फोन के ऑपरेटिंग सिस्टम(OS) को हमेशा अपडेटेड रखें।
- अज्ञात नंबरों से आने वाली कॉल को साइलेंस या ब्लॉक कर दें।
- व्हाट्सएप में दो चरणीय सत्यापन(Two-step verification) को सक्षम करें।
- अनजान नंबरों से आने वाली और अवांछित कॉलों से सावधान रहें।

महीने के सुझाव

(क) क्यूआर कोड(QR Codes) जोखिम भरे हो सकते हैं :-

क्यूआर कोड जोखिम भरे हो सकते हैं क्योंकि वे अपने गंतव्य (destination) को छिपाए रखते हैं, जिससे हमलावरों के लिए उपयोगकर्ताओं को बिना किसी स्पष्ट चेतावनी के फिशिंग वेबसाइटों, मैलवेयर डाउनलोड या फर्जी भुगतान पेजों पर निर्देशित करना आसान हो जाता है। धोखेबाज (स्कैमर्स) अक्सर पोस्टरों, पार्किंग मीटरों, मेनू पर या यहाँ तक कि असली कोड के ऊपर भी मैलेशियस(दुर्भावनापूर्ण) क्यूआर कोड लगा देते हैं, जिससे लोग धोखा खाकर अपनी व्यक्तिगत जानकारी या वित्तीय विवरण दर्ज कर देते हैं। चूंकि प्रयोगकर्ता स्कैन करने से पहले पूरा वेब पता(URL) नहीं देख सकते, इसलिए यह तय करना कठिन होता है कि लिंक भरोसेमंद है या नहीं।

- जोखिम को कम करने के लिए, लोगों को अज्ञात या संदिग्ध स्रोतों से क्यूआर कोड स्कैन करने से बचना चाहिए।
- किसी भी साइट पर आगे बढ़ने से पहले उसके यूआरएल (URL) की सावधानीपूर्वक समीक्षा करें, और जब तक आप आश्वस्त न हों कि स्रोत भरोसेमंद है, तब तक अपनी संवेदनशील जानकारी साझा न करें।

(ख) सोशल मीडिया फुटप्रिंट(जानकारी साझा करने की गतिविधि) **को सीमित करना :-**

अपनी व्यक्तिगत जानकारी की सुरक्षा और साइबर हमलों को रोकने के लिए अपने सोशल मीडिया फुटप्रिंट(जानकारी साझा करने की गतिविधि) **को सीमित करना** सबसे प्रभावी तरीकों में से एक है।

साइबर अपराधी व्यक्तिगत फिशिंग हमले करने, पासवर्ड का अनुमान लगाने या पहचान की चोरी (identity theft) करने के लिए अक्सर सार्वजनिक रूप से उपलब्ध जानकारी जैसे कि जन्मदिन, पालतू जानवरों के नाम, छुट्टियों की योजना या काम के विवरणों जैसी छोटी-छोटी जानकारियां को इकट्ठा करते हैं।

- नियमित रूप से अपनी गोपनीयता सेटिंग की समीक्षा करें और अपनी पोस्ट, मित्र सूचियों और व्यक्तिगत विवरणों को केवल विश्वसनीय संपर्कों **के लिए ही दृश्यमान**(visible) रखें।
- आप जो भी शेयर करते हैं उसके प्रति सावधान रहें; जैसे अपने घर का पता, यात्रा की योजना, जन्मदिन या ऐसी कोई भी ऐसी जानकारी जिससे आपकी रोज़ाना की दिनचर्या का पता चले, उसे शेयर करने से बचें।
- विभिन्न प्लेटफॉर्मों पर अलग-अलग(unique) यूजरनेम का उपयोग करें ताकि हमलावरों के लिए आपको ट्रैक करना कठिन हो जाए।
- फ्रेंड रिक्वेस्ट स्वीकार करने में सावधानी बरतें और केवल उन्हीं लोगों को जोड़ें जिन्हें आप व्यक्तिगत रूप से जानते हैं।

(सी) दिन के अंत में लॉग आउट करें

दिन के अंत में लॉग आउट करना एक महत्वपूर्ण सुरक्षा अभ्यास है जो संवेदनशील जानकारी और प्रणालियों को अनधिकृत पहुंच से बचाने में मदद करता है। खातों को साइन-इन छोड़ना, विशेष रूप से साझा किए गए या कार्यस्थल के उपकरणों पर, किसी अन्य व्यक्ति द्वारा डेटा तक पहुँचने, संदेश भेजने या बिना अनुमति के परिवर्तन करने के जोखिम को बढ़ाता है। लॉग आउट करना यह सुनिश्चित करता है कि सत्र(sessions) ठीक से बंद हो गए हैं, आंतरिक खतरों के जोखिम को कम करता है, और समग्र साइबर सुरक्षा स्वच्छता का समर्थन करता है। जाने से पहले लॉग आउट करने को दैनिक आदत के रूप में बनाना व्यक्तिगत और संगठनात्मक दोनों जानकारियों को सुरक्षित रखने में मदद करता है।

- काम से निकलने या अपना डिवाइस बंद करने से पहले लॉग आउट करने के लिए रोज़ाना रिमाइंडर सेट करें।
- केवल ईमेल ही नहीं, बल्कि सभी एप्लिकेशन से लॉग आउट करें - जिसमें मैसेजिंग टूल, डेटाबेस और क्लाउड प्लेटफॉर्म शामिल हैं।
- कार्यस्थल या सार्वजनिक प्रणालियों पर पासवर्ड सहेजने(save) करने से बचें।
- काम के पूरा होने पर वीपीएन (VPN) और रिमोट एक्सेस टूल से साइन आउट करें।
- जहाँ उपलब्ध हो, वहां स्वचालित लॉगआउट (automatic logout) या सेशन टाइमआउट सक्षम करें।

सूचना प्रौद्योगिकी(IT) महानिदेशालय में नए विकास

1.) ई-बिल (E-bill)

दौरे के टीए/डीए का समायोजन

2.) पीपीएमएस (PPMS)

- नियुक्ति सुधार आदेश (पीआईएस फोटो अपडेट)
- पीटी/परेड आदेश

डॉ. श्रीनिवास एम, निदेशक, एम्स नई दिल्ली। जीवनशैली से जुड़ी बीमारियों को रोकने में स्वस्थ आहार पद्धतियों की महत्वपूर्ण भूमिका पर ज्ञानवर्धक भाषण दिया।

एसडीजी मैदान में एक दोस्ताना मैच के दौरान सीआरपीएफ के महानिदेशक

सीजीओ में राष्ट्रीय मतदाता दिवस की शपथ