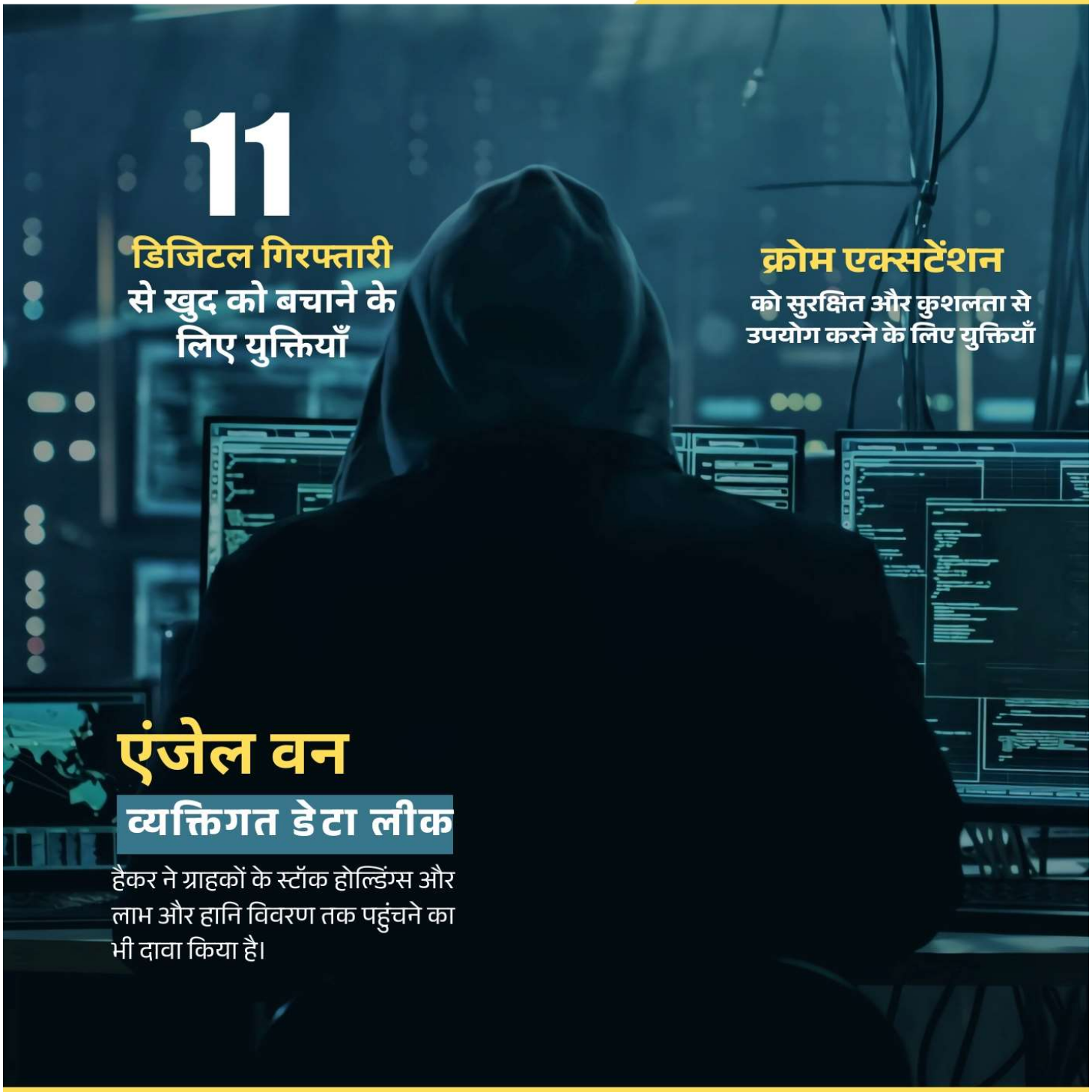
केंद्रीय रिज़र्व पुलिस बल

साइबर बार्ईट

जनवरी 2025



11
डिजिटल गिरफ्तारी से खुद को बचाने के लिए युक्तियाँ

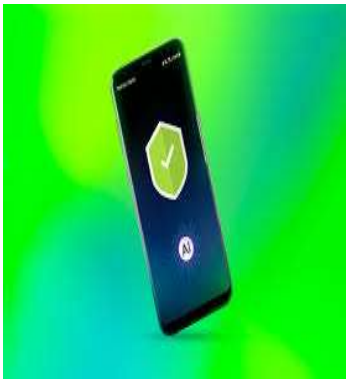
क्रोम एक्सटेंशन
को सुरक्षित और कुशलता से उपयोग करने के लिए युक्तियाँ

एंजेल वन
व्यक्तिगत डेटा लीक
हैकर ने ग्राहकों के स्टॉक होल्डिंग्स और लाभ और हानि विवरण तक पहुंचने का भी दावा किया है।

2024 में साइबर घोटालों में भारतीयों को लगभग 12,000 करोड़ रुपये का नुकसान हुआ

1.साइबर गीक्स न्यूज

A) साइबर सुरक्षा फर्म Zscaler के अनुसार, वैश्विक मोबाइल मैलवेयर हमलों की सूची में भारत शीर्ष पर है -



Zscaler के थ्रेटलैब्ज़ 2024 मोबाइल, IoT और OT की फ्रेट खतरा रिपोर्ट के खुलासे के अनुसार, दुनिया भर में कुल मोबाइल मैलवेयर हमलों में से 28% मोबाइल मैलवेयर हमले भारत में होते हैं, जो संयुक्त राज्य अमेरिका (27.3%) और कनाडा (15.9%) से अधिक है।

रिपोर्ट में जून 2023 से मई 2024 तक के डेटासेट का विश्लेषण किया गया जिसमें 20 बिलियन से अधिक मोबाइल से लेनदेन संबंधित खतरे और उससे संबंधित साइबर खतरे शामिल थे। Zscaler के एक ब्लॉग में कहा गया है कि उनकी शोध टीम ने वित्तीय रूप से प्रेरित मोबाइल हमलों में वृद्धि को ट्रैक किया, जिसमें स्पाइवेयर में 111% और बैंकिंग मैलवेयर में 29% की वृद्धि देखी गई ।

भारत में सबसे हालिया मामलों में से एक मामला **नकली शादी के कार्ड का था** । अपनी नवीनतम चाल में, स्कैमर्स व्हाट्सएप पर शादी के कार्ड के पीडीएफ दस्तावेज भेजते हैं, जिन्हें खोलने पर प्राप्तकर्ता के डिवाइस पर मैलवेयर डाउनलोड हो जाता है।

इस वर्ष की शुरुआत में, अगस्त के महीने में, रैनसमवेयर हमले के कारण लगभग 300 छोटे भारतीय बैंकों को ऑफ़लाइन होने के लिए मजबूर होना पड़ा। देश के लगभग 1,500 सहकारी और ग्रामीण क्षेत्रीय बैंकों में से पांचवा हिस्सा प्रभावित हुआ।

2022 में, **एम्स** दिल्ली पर 15 दिनों से ज़्यादा समय तक हमला होता रहा, जिसे तत्कालीन इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी राज्य मंत्री राजीव चंद्रशेखर ने "एक साज़िश और बाहरी ताकतों द्वारा नियोजित" कहा था।

Zscaler ने अपने ब्लॉग पोस्ट में कहा कि साइबर हमले भी ज़्यादा परिष्कृत हो गए हैं, उन्होंने कहा कि उद्यमों को एक शून्य-विश्वास रहित (जीरो ट्रस्ट) दृष्टिकोण अपनाना चाहिए जो साइबर खतरों को कम करता है और उनकी सुरक्षा स्थिति में सुधार करता है।

बी) 2024: भारत में साइबर हमले

बीएसएनएल डेटा ब्रीच

भारत संचार निगम लिमिटेड (बीएसएनएल) को इस साल जून में डेटा चोरी का सामना करना पड़ा, जिसमें

साइबर अपराधी किबरफैंटम " ने दावा किया कि उसने 278 जीबी से अधिक संवेदनशील डेटा तक पहुंच बनाई है, जिसमें अंतर्राष्ट्रीय मोबाइल ग्राहक पहचान (आईएमएसआई) नंबर, सिम कार्ड विवरण, होम लोकेशन रजिस्टर डेटा और सुरक्षा कुंजी शामिल हैं। चोरी में सर्वर स्नैपशॉट शामिल थे जिनका उपयोग सिम क्लोनिंग और जबरन वसूली के लिए किया जा सकता था।

एन्जेल वन का व्यक्तिगत डेटा लीक

पिछले साल मुंबई स्थित स्टॉक ब्रोकिंग फर्म एंजेल वन में डेटा चोरी के कारण 7.9 मिलियन ग्राहकों की निजी जानकारी हैकर फोरम पर प्रकाशित हो गई थी। हैकर ने ग्राहकों की स्टॉक होल्डिंग्स और लाभ-हानी स्टेटमेंट तक पहुंच बनाने का भी दावा किया था।

वज़ीरएक्स साइबर अटैक

क्रिप्टोकरेंसी प्लेटफॉर्म वज़ीरएक्स में जुलाई में भारतीय एक्सचेंज पर सबसे बड़े साइबर हमलों में से एक हुआ, जिसमें हैकरों ने निवेशकों की 235 मिलियन डॉलर की होल्डिंग्स चुरा लीं, जो प्लेटफॉर्म के अनुमानित रिजर्व का लगभग आधा हिस्सा है, जिससे लगभग 15 मिलियन उपयोगकर्ता प्रभावित हुए।

लघु भारतीय बैंकों पर रैनसमवेयर हमला

एक और महत्वपूर्ण साइबर घोटाला रैनसमवेयर हमले से जुड़ा था, जिसके कारण लगभग 300 छोटे भारतीय बैंकों को ऑफ़लाइन होना पड़ा। देश के 1,500 सहकारी और ग्रामीण क्षेत्रीय बैंकों में से लगभग पांचवा हिस्सा प्रभावित हुआ, इन बैंकों को सेवा प्रदान करने वाली सी-एज टेक्नोलॉजीज इस हमले का लक्ष्य थी।

नकली शादी कार्ड घोटाला

इस साल एक नई धोखाधड़ी रणनीति में नकली शादी कार्ड शामिल थे। स्कैमर्स व्हाट्सएप के माध्यम से पीडीएफ शादी के निमंत्रण भेजते हैं, जिन्हें खोलने पर, प्राप्तकर्ता के डिवाइस पर मैलवेयर डाउनलोड हो जाता है।

आंकड़ों के अनुसार

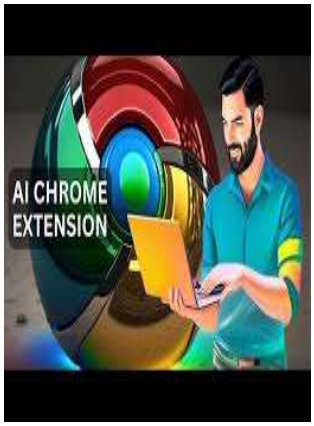
इस साल साइबर स्कैम में भारतीयों को लगभग 12,000 करोड़ रुपये का नुकसान हुआ है, जिसमें घोटाले 300% तक बढ़ गए हैं।
गैर-लाभकारी
प्रहार की एक रिपोर्ट में भविष्यवाणी की गई है कि भारत 2033 तक सालाना लगभग 1 ट्रिलियन साइबर हमलों का सामना कर सकता है, जो 2047 तक बढ़कर 17 ट्रिलियन हो जाएगा।

यह वृद्धि उद्योगों में, विशेष रूप से साइबर अपराधियों द्वारा लक्षित क्षेत्रों में, मजबूत

साइबर सुरक्षा की आवश्यकता को रेखांकित करती है।

2.साइबर धोखाधड़ी

(ए) दर्जनों क्रोम एक्सटेंशन हैक हो गए, जिससे लाखों उपयोगकर्ताओं का डेटा चोरी होने का खतरा है



हमला करने की एक नई चाल ने ज्ञात क्रोम ब्राउज़र एक्सटेंशन को लक्ष्य बनाया है, जिसके परिणामस्वरूप कम से कम 35 एक्सटेंशन प्रभावित हुए हैं और 2.6 मिलियन से अधिक उपयोगकर्ताओं के डेटा के उजागर होने तथा क्रेडेंशियल चोरी होने का खतरा उत्पन्न हो गया है।

साइबरहेवन ने एक अलग तकनीकी लेख में कहा गया है कि, "हमलावर ने दुर्भावनापूर्ण एप्लिकेशन ('गोपनीयता नीति एक्सटेंशन') के माध्यम से आवश्यक अनुमतियां प्राप्त कीं और क्रोम वेब स्टोर पर दुर्भावनापूर्ण क्रोम एक्सटेंशन अपलोड कर दिया "पारंपरिक क्रोम वेब स्टोर सुरक्षा समीक्षा प्रक्रिया के बाद, दुर्भावनापूर्ण एक्सटेंशन को प्रकाशन के लिए मंजूरी दे दी गई।"

लेयरएक्स सिक्योरिटी के सीईओ ऑर HYPERLINK "https://layerxsecurity.com/" \t "_blank" एशेड कहते हैं, "ब्राउज़र एक्सटेंशन वेब सुरक्षा का सबसे कमजोर पक्ष है ।" हालांकि हम ब्राउज़र एक्सटेंशन को हानिरहित मानते हैं, लेकिन व्यवहार में, उन्हें अक्सर संवेदनशील उपयोगकर्ता जानकारी जैसे कि कुकीज़, एक्सेस टोकन, पहचान जानकारी और बहुत कुछ के लिए व्यापक अनुमति दी जाती है।

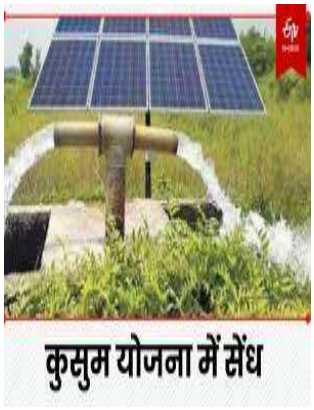
सिक्योर एनेक्स और एक्सटेंशन टोटल के अनुसार, आगे की जांच में और अधिक एक्सटेंशन [**गूगल शीट्स**] का पता चला है, जिनके निपटारा होने का संदेह है।

- **ए-आई असिस्टेंट – चैट जीपीट एंड जैमिनी फॉर क्रोम**
- **बार्ड एआई चैट एक्सटेंशन**
- **जीपीटी 4 समरी विथ ओपन एआई**
- **सर्च एआई कोपाइलट फॉर क्रोम**
- **टीनामाइंड एआई असिस्टेंट**
- **वेइन एआई**
- **वीपीएनसिटी**
- **इंटरनेक्स्ट वीपीएन**
- **विडहेल्पर वीडियो डाउनलोडर**
- **बुकमार्क फ़ेविकॉन चेंजर**
- **कैस्टोरस**
- **यू वॉयस**
- **रीडर मोड**
- **पैरट टॉक्स**

- **प्राइमस**
- **टैकर - ऑनलाइन कीलॉगर टूल**
- **एआई शॉप बडी**

ये अतिरिक्त कॅम्परोमाइज्ड एक्सटेंशन संकेत देते हैं कि साइबरहेवन एक बार का लक्ष्य नहीं था, बल्कि वैध ब्राउज़र एक्सटेंशन को लक्षित करने वाले व्यापक पैमाने पर हमले की चाल का हिस्सा था।

(बी) साइबर घोटालेबाज पीएम-कुसुम आवेदकों को निशाना बना रहे हैं



आज की दुनिया में ऐसा कोई क्षेत्र नहीं है जो साइबर अपराध से अछूता हो। इस सूची में नवीनतम नाम पीएम-कुसुम योजना का घटक बी है जिसके तहत किसानों को सौर पंप सेट प्रदान किए जाते हैं। हाल के दिनों में, कर्नाटक अक्षय ऊर्जा और विकास लिमिटेड (केआरईडीएल) से जुड़े होने का दिखावा करके किसानों को निशाना बनाया जिससे कई किसानों को पैसा गवाना पड़ा ।

केआरईडीएल अधिकारियों के अनुसार , पिछले साल से किसान शिकायत कर रहे हैं कि उन्हें ऐसे लोगों से कॉल और व्हाट्सएप संदेश मिल रहे हैं जो दावा करते हैं कि वे केआरईडीएल के अधिकारी हैं और उन्हें पैसे देने के लिए मजबूर कर रहे हैं। केआरईडीएल ने यह भी पाया है कि कई अन्य लोगों ने **फेसबुक** और **यूट्यूब** जैसी सोशल मीडिया साइटों का सहारा लिया है और पीएम कुसुम योजना के बारे में गलत सूचना फैला रहे हैं। कुछ मामलों में, उन्होंने किसानों से पैसे ट्रांसफर भी करवाए।

3. इस महीने की टिप

(A) डिजिटल गिरफ्तारी से खुद को कैसे बचाएं

डिजिटल गिरफ्तारी साइबर अपराधियों द्वारा इस्तेमाल की जाने वाली एक भ्रामक रणनीति है,जो अक्सर फोन पर या ऑनलाइन संचार के माध्यम से डिजिटल माध्यम से किसी व्यक्ति को गिरफ्तार करने का झूठा दावा करते हैं।

1. **अपने राउटर को मजबूत(Strong) पासवर्ड से सुरक्षित रखें ।**

अपने ब्रॉडबैंड राउटर के लिए डिफ़ॉल्ट एडमिनिस्ट्रेटर लॉगिन क्रेडेंशियल बदलें। ज़्यादातर राउटर डिफ़ॉल्ट यूज़रनेम और पासवर्ड (जैसे "एडमिन" या "पासवर्ड") के साथ आते हैं, जिसका आसानी से अनुमान लगाया जा सकता है । बड़े अक्षरों, छोटे अक्षरों, संख्याओं और प्रतीकों को मिलाकर एक मज़बूत, जटिल पासवर्ड का इस्तेमाल करें।

2. WPA3 या WPA2 एन्क्रिप्शन का उपयोग करें

बेहतर सुरक्षा के लिए अपने वाई-फ़ाई नेटवर्क पर नवीनतम WPA3 एन्क्रिप्शन मानक सक्षम करें। यदि WPA3 उपलब्ध नहीं है, तो WPA2 का उपयोग करें WEP एन्क्रिप्शन का उपयोग करने से बचें , क्योंकि यह पुराना हो चुका है और हैकर्स द्वारा आसानी से इसका उल्लंघन किया जा सकता है ।

3. अपने राउटर के फ़र्मवेयर को अपडेट रखें

निर्माता अक्सर कमज़ोरियों को दूर करने और राउटर की सुरक्षा में सुधार करने के लिए फ़र्मवेयर अपडेट जारी करते हैं । अपने राउटर की सेटिंग नियमित रूप से जांचें और कोई भी अपडेट लागू करें।

कुछ राउटर स्वचालित अपडेट की अनुमति देते हैं - यदि आपका राउटर इसका समर्थन करता है तो इसे सक्षम करें।

4. रिमोट प्रबंधन अक्षम करें

- रिमोट एक्सेस को बंद रखें । रिमोट मैनेजमेंट उपयोगकर्ताओं को इंटरनेट से राउटर सेटिंग्स तक पहुंचने की अनुमति देता है, जिसका हमलावरों द्वारा फायदा उठाया जा सकता है।

यदि दूरस्थ पहुंच की आवश्यकता है, तो सुरक्षित दूरस्थ प्रबंधन के लिए वर्चुअल प्राइवेट नेटवर्क (वीपीएन) का उपयोग करने पर विचार करें।

5. फ़ायरवॉल का उपयोग करें

अपने राउटर के अंतर्निहित फ़ायरवॉल को सक्षम करें । अधिकांश राउटर फ़ायरवॉल के साथ आते हैं जो आने वाले खतरों के विरूद् सुरक्षा की एक अतिरिक्त परत जोड़ता है।

अधिक सुरक्षा के लिए अपने डिवाइस पर अतिरिक्त सॉफ़्टवेयर फ़ायरवॉल का उपयोग करने पर विचार करें।

6. अपना नेटवर्क नाम (SSID) बदलें

डिफ़ॉल्ट SSID (सर्विस सेट आइडेंटिफ़ायर) या नेटवर्क नाम बदलें। डिफ़ॉल्ट नाम अक्सर राउटर के ब्रांड को प्रकट करते हैं, जो हमलावरों को विशिष्ट

कमज़ोरियों को लक्षित करने में मदद कर सकता है।

SSID में व्यक्तिगत जानकारी (जैसे आपका नाम या पता) का उपयोग करने से बचें ।

7. उपयोग में न होने पर वाई-फाई अक्षम करें

- जब इस्तेमाल न हो रहा हो (जैसे, रात में या जब आप घर से बाहर हों) तो अपना वाई-फाई या ब्रॉडबैंड कनेक्शन बंद कर दें। इससे हमलावर द्वारा आपके नेटवर्क तक पहुँचने की कोशिश करने की संभावना कम हो जाती है।
- राउटर सेटिंग्स में विशिष्ट घंटों के दौरान वाई-फाई को स्वचालित रूप से अक्षम करने के लिए **शेड्यूल** सेट कर सकते हैं ।

8. मैक एड्रेस फ़िल्टरिंग सक्षम करें

- **MAC (मीडिया एक्सेस कंट्रोल) एड्रेस फ़िल्टरिंग** आपको यह सीमित करने की अनुमति देता है कि कौन से डिवाइस आपके ब्रॉडबैंड नेटवर्क से कनेक्ट हो सकते हैं। प्रत्येक डिवाइस का एक अद्वितीय मैक पता होता है, और आप निर्दिष्ट कर सकते हैं कि आपके नेटवर्क पर किन डिवाइस को अनुमति दी जाए।
- यधपि मैक पते को नकली बनाया जा सकता है, लेकिन इससे सुरक्षा की एक अतिरिक्त परत जुड़ जाती है।

9. एसएसआईडी प्रसारण अक्षम करें

- **SSID प्रसारण को अक्षम करें** । इससे आपका नेटवर्क पूरी तरह से छिपा हुआ नहीं रहेगा, लेकिन आकस्मिक हमलावरों के लिए आपके कनेक्शन को ढूँढना और उसे निशाना बनाना कठिन हो जाएगा।
- अपने नेटवर्क से नए डिवाइस कनेक्ट करते समय आपको अपना SSID मैन्युअल रूप से दर्ज करना होगा।

10. नेटवर्क से स्वचालित कनेक्शन अक्षम करें

- खुले या सार्वजनिक नेटवर्क से जुड़ने के लिए अपने डिवाइस पर **स्वचालित कनेक्शन सुविधा को** बंद करें । यह आपके डिवाइस को संभावित रूप से असुरक्षित या दुर्भावनापूर्ण नेटवर्क से गलती से कनेक्ट होने से रोकता है।
- कनेक्ट करने से पहले नेटवर्क को मैन्युअल रूप से चुनें और सत्यापित करें।

11. अपने राउटर को नियमित रूप से रीबूट करें

- अपने राउटर को रीबूट करने से **मेमोरी साफ़ करने**, प्रदर्शन में सुधार करने और

कुछ प्रकार के मैलवेयर संक्रमणों को कम करने में मदद मिल सकती है जो निरंतर अपटाइम/उपरिकाल पर निर्भर करते हैं।
- नियमित पुनः आरंभ कार्यक्रम से दीर्घकालिक कमजोरियों का फायदा उठाने से भी बचा जा सकता है।

ब्रॉडबैंड **सुरक्षा प्रथाओं का** पालन करके , आप अपने इंटरनेट कनेक्शन और उससे जुड़े उपकरणों को कई तरह के खतरों से बेहतर तरीके से सुरक्षित कर सकते हैं। अपने राउटर, मॉनिटरिंग डिवाइस को सुरक्षित रखना और एन्क्रिप्शन सक्षम करना आपके घर या व्यवसाय के ब्रॉडबैंड की सुरक्षा के लिए सबसे महत्वपूर्ण कदम हैं।

(बी) क्रोम एक्सटेंशन को सुरक्षित और कुशलतापूर्वक उपयोग करने के लिए सुझाव

1. केवल विश्वसनीय स्रोतों से ही एक्सटेंशन इंस्टॉल करें

- हमेशा **आधिकारिक क्रोम वेब स्टोर** या विश्वसनीय डेवलपर्स से एक्सटेंशन इंस्टॉल करें। थर्ड-पार्टी /अन्य पक्ष वेबसाइट से एक्सटेंशन डाउनलोड करने से बचें, क्योंकि उनमें मैलवेयर या दुर्भावनापूर्ण कोड हो सकता है।
- बड़ी संख्या में उपयोगकर्ताओं से **सकारात्मक समीक्षा** वाले एक्सटेंशन की तलाश करें ।

2. अनुमतियों की सावधानीपूर्वक समीक्षा करें

- एक्सटेंशन इंस्टॉल करने से पहले, यह जाँच लें कि वह **किन अनुमतियों** का अनुरोध करता है। ऐसे एक्सटेंशन से सावधान रहें जो ज़रूरत से ज़्यादा एक्सेस मांगते हैं (जैसे, सभी वेबसाइट तक पहुँच, डेटा पढ़ना और संशोधित करना)।
- यदि कोई एक्सटेंशन आपके ब्राउज़िंग इतिहास या क्लिपबोर्ड तक पहुंच जैसी संवेदनशील अनुमतियों का अनुरोध करता है, तो सुनिश्चित करें कि यह एक्सटेंशन की कार्यक्षमता के लिए आवश्यक है।

3. एक्सटेंशन को न्यूनतम रखें

- केवल उन एक्सटेंशन को इंस्टॉल करें जिन्हें आप **सक्रिय रूप से उपयोग करते हैं** । बहुत अधिक एक्सटेंशन होने से आपका ब्राउज़र धीमा हो सकता है, इंटरफ़ेस अव्यवस्थित हो सकता है और सुरक्षा जोखिम बढ़ सकता है।
- **अप्रयुक्त एक्सटेंशन की** समीक्षा करें और उन्हें हटा दें .

4. अनुमतियों में परिवर्तन से सावधान रहें

- यदि कोई एक्सटेंशन अपडेट होता है और **नई अनुमतियों का अनुरोध करता है** , तो उनकी सावधानीपूर्वक समीक्षा करें। कुछ दुर्भावनापूर्ण डेवलपर्स अपडेट के बाद अनधिकृत पहुँच प्राप्त करने के लिए पहले

से सुरक्षित एक्सटेंशन को अपडेट कर सकते हैं।

- अपडेट के बाद अनुमतियों में बदलाव होने पर क्रोम आपको सूचित करेगा - सावधान रहें और तय करें कि एक्सटेंशन को रखना है या हटाना है।

5. उन एक्सटेंशन को अक्षम करें जिनकी आपको आवश्यकता नहीं है

- यदि आप किसी एक्सटेंशन को पूरी तरह से हटाना नहीं चाहते हैं, लेकिन इसका नियमित रूप से उपयोग नहीं करते हैं, तो **इसे अस्थायी रूप से अक्षम करें** । यह आपके ब्राउज़र को तेज़ रखने और संभावित सुरक्षा जोखिमों को कम करने में मदद करेगा।
- **chrome://extensions/** पर जाकर और विशिष्ट एक्सटेंशन के लिए स्विच को बंद करके किसी एक्सटेंशन को अक्षम कर सकते हैं।

6. एक्सटेंशन व्यवहार की निगरानी करें

- एक्सटेंशन इंस्टॉल या अपडेट करने के बाद असामान्य ब्राउज़र व्यवहार पर नज़र रखें, जैसे:
  - **धीमा प्रदर्शन**
  - **अप्रत्याशित पॉप-अप या विज्ञापन**
  - **आपके डिफ़ॉल्ट खोज इंजन या होमपेज में परिवर्तन** .
- यदि आपको कुछ भी संदिग्ध दिखाई दे तो **एक्सटेंशन को तुरंत अक्षम करें या हटा दें** ।

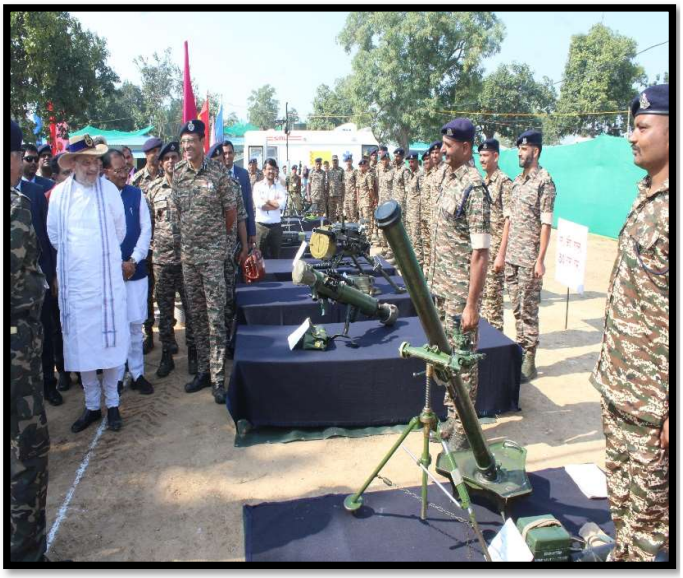
7. नकली एक्सटेंशन से सावधान रहें

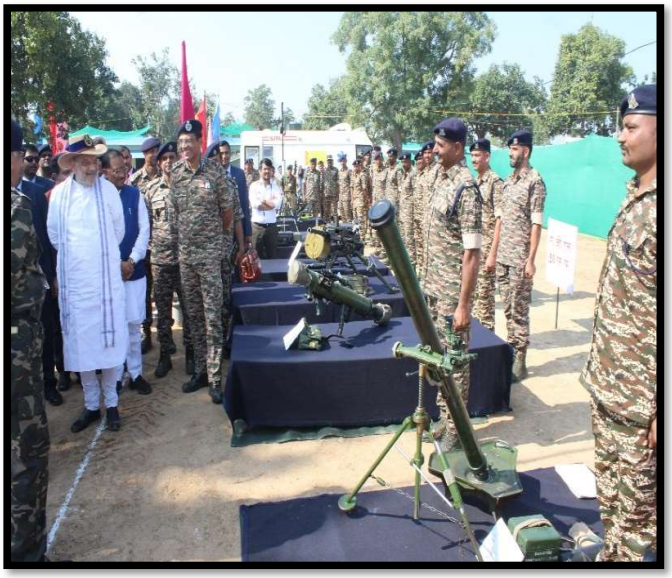
- कुछ एक्सटेंशन वैध एक्सटेंशन की नकल कर सकते हैं। इंस्टॉल करने से पहले, जाँच करें:
  - डेवलपर **का नाम** .
  - एक्सटेंशन **की रेटिंग** .
  - **इंस्टॉल की संख्या** और **समीक्षाएँ** यह सुनिश्चित करती हैं कि आपको वैध एक्सटेंशन मिल रहा है।

8. फ़िशिंग या एडवेयर से सावधान रहें

- कुछ दुर्भावनापूर्ण एक्सटेंशन विज्ञापन डाल सकते हैं, आपको अवांछित साइटों पर रीडायरेक्ट कर सकते हैं या फ़िशिंग प्रयासों में संलग्न हो सकते हैं। अप्रत्याशित पॉप-अप या लिंक का सामना करते समय सावधान रहें।
- लिंक से खुद को बचाने के लिए **विज्ञापन अवरोधक** या **एंटी-फ़िशिंग एक्सटेंशन का** उपयोग करें।

इन सुझावों का पालन करके, आप अपने क्रोम एक्सटेंशन को सुरक्षित रख सकते हैं, अपनी गोपनीयता की रक्षा कर सकते हैं और अपने समग्र ब्राउज़िंग अनुभव को बेहतर बना सकते हैं।






केन्द्रीय रिजर्व पुलिस बल
153 वाहिनी गुण्डम, बीजापुर (छ.ग.)