# केंद्रीय रिजर्व पुलिस बल

# साइबर बाइट

साइबर बाइट
अप्रैल-2024
संस्करण

- रोमांस स्कैम" का उपयोग करके पैचवर्क वज्रस्पाई वेयर के साथ एंड्रॉइड डिवाइस को संक्रमित करने का प्रलोभन देता है।
- नई पायथन-आधारित स्नेक जानकारी चुराने वाला फेसबुक संदेशों के माध्यम से फैल रहा है।
- AndroxGh0st मैलवेयर क्लाउड क्रेडेंशियल्स चुराने के लिए लारवेल ऐप्स को लक्षित करता है।

- साइबर फ्रॉड अपडेट्स

ऑनलाइन वितीय धोखाधड़ी
की रिपोर्ट करने के लिए
**1930**
पर कॉल करें

https://cybercrime.gov.in
पर अपनी शिकायत दर्ज करें

# 1.साइबर गीक समाचार

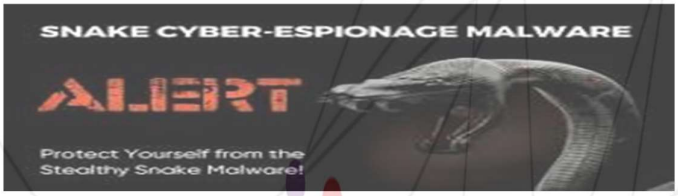
## ए) "रोमांस स्कैम" का उपयोग करके पैचवर्क वज्रास्पाई मैलवेयर के साथ एंड्रॉइड डिवाइस को संक्रमित करने का प्रलोभन देता है।

पैचवर्क नाम का साइबर अपराधी संभवतः पाकिस्तान और भारत में पीड़ितों को लुभाने और फंसाने के लिए "रोमांस स्कैम" का इस्तेमाल करते थे, और उनके एंड्रॉइड डिवाइस को वज्रस्पाई नामक रिमोट एक्सेस ट्रोजन से संक्रमित करते थे। वज्रस्पाई में जासूसी कार्यक्षमताओं की एक श्रृंखला है जिसे इसके कोड के साथ बंडल किए गए ऐप को दी गई अनुमतियों के आधार पर विस्तारित किया जा सकता है। यह संपर्क फ़ाइलें ,कॉल लॉग और एसएमएस संदेश चुराता है, लेकिन इसके कुछ एप्लीकेश व्हाट्सएप और सिगनल संदेश भी निकाल सकते हैं ,फोन कॉल रिकॉर्ड कर सकते हैं और कैमरे से तस्वीरें ले सकते हैं। मलिशियस ऐप गूगल प्ले और अन्य स्रोतों के माध्यम से मुख्य रूप से मैसेजिंग एप्लिकेशन के रूप में वितरित किए जाते हैं।

- प्रिवी टॉक( com.priv .talk )
- मीटमी(com.meeete.org)
- लैट्स चैट ( com.letsm .chat )
- क्विक चैट( com.qqc.chat )
- रफाकत ( com.rafaqat .news )
- चिट चैट( com.chit .chat )
- योहूटॉक( com.yoho .talk )
- टिकटॉक( com.tik.talk )
- हेलो चैट( com.hello .chat )
- निडस com.nidus.no) या(com.nionio.org
- ग्लोचैट( com.glow .glow )
- वेव चैट( com.wave .chat )

एंड्रॉइड उपयोगकर्ता एक एक्टॉर्सन स्कैम के रूप में एक नकली लोन ऐप (मनीफाइन या "कॉम.मनीफाइन.फाइन") का उपयोग कर रहे हैं, जो एक नग्न इमेज बनाने के लिए अपने नो योर कस्टमर (केवाईसी) प्रक्रिया के रूप में अपलोड की गई सेल्फी में हेरफेर करता है और पीड़ितों को राशि भुगतान करने या फिर उनकी छेड़छाड़ वाली तस्वीरों को उनके सभी कॉन्टेक्स में भेजने की धमकी देता है। ये अज्ञात, आर्थिक रूप से प्रेरित साइबर अपराधी न्यूनतम औपचारिकताओं के साथ त्वरित ऋण देने के लुभावने वादे करते हैं, उनके उपकरणों से समझौता करने के लिए मैलवेयर वितरित करते हैं, और धन उगाही के लिए धमकियों का इस्तेमाल करते हैं। यह उन लोगों की व्यापक प्रवृत्ति के बीच भी आया है जो धोकाधड़ी करने वाले ऋण ऐप्स का शिकार हो रहे हैं, जो संक्रमित उपकरणों से संवेदनशील जानकारी प्राप्त करने के लिए जाने जाते हैं, और पीड़ितों पर भुगतान करने के लिए दबाव डालने हेतु ब्लैकमेल और उत्पीड़न की रणनीति अपनाते हैं।

## बी) नया पायथन-आधारित " स्नेक जानकारी चुराने वाला'' फेसबुक संदेशों के माध्यम से फैल रहा है।




फेसबुक संदेशों का उपयोग साइबर अपराधी द्वारा पाइथॉन-आधारित सूचना चुराने वाले स्नेक को वितरित करने के लिए किया जा रहा है ,जिसे क्रेडेंशियल और अन्य संवेदनशील डेटा को प्राप्त करने के लिए डिज़ाइन किया गया है।

"असंदिग्ध उपयोगकर्ताओं से प्राप्त क्रेडेंशियल्स को डिस्कॉर्ड ,गिटहब और टेलीग्राम जैसे विभिन्न प्लेटफार्मों पर प्रेषित किया जाता है। "हमलों में संभावित उपयोगकर्ताओं को अहानिकर प्रतीत होने वाली RAR या ZIP संग्रह फ़ाइलें भेजना शामिल है ,जिन्हें खोलने पर ,संक्रमण अनुक्रम सक्रिय हो जाता है।

एकत्र की गई जानकारी ,जिसमें क्रेडेंशियल्स और कुकीज़ शामिल हैं , को टेलीग्राम बॉट एपीआई के माध्यम से एक ज़िप संग्रह के रूप में बाहर निकाला जाता है। चोरी करने वाले को फेसबुक के लिए विशिष्ट कुकी जानकारी को डंप करने के लिए भी डिज़ाइन किया गया है ,जो एक संकेत है कि साइबर अपराधी संभवतः अपने स्वयं के उद्देश्यों के लिए खातों को हाईजैक करना चाह रहा है।

फेसबुक कुकीज़ को लक्षित करते हुए एकाधिक चुराने वाले सामने आए हैं, जिनमें S1deload Stealer, MrTonyScam, NodeStealer और VietCredCare शामिल हैं। यह एक खोज का भी अनुसरण करता है कि साइबर अपराधी "लुआ मैलवेयर चलाने के लिए संभावित गेम-हैकर्स को धोखा देने हेतु एक क्लोन गेम चीट वेबसाइट, एसईओ पॉजनिंग और गिटहब में एक बग का उपयोग कर रहे हैं।"

## सी) AndroxGh0stमैलवेयर क्लाउड क्रेडेंशियल्स चुराने के लिए लारवेल ऐप्स को लक्षित करता है।

साइबर सुरक्षा शोधकर्ताओं ने AndroxGh0st नामक एक उपकरण पर प्रकाश डाला है जिसका उपयोग लारवेल अनुप्रयोगों को लक्षित करने और संवेदनशील डेटा चुराने के लिए किया जाता है। "यह .env फ़ाइलों से महत्वपूर्ण जानकारी को स्कैन करके और उसे निकालकर, AWS और Twilio से जुड़े लॉगिन विवरणों को प्रकट करके काम करता है।" AndroxGh0st कम से कम 2022 से अविवेचित पाया गया है, साइबर अपराधी इसका लाभ उठाकर लारवेल परिवेश संबंधी फ़ाइलों तक पहुँचते हैं और अमेज़ॅन वेब सर्विसेज (एडब्ल्यूएस), सेंडग्रिड और ट्विलियो' जैसे विभिन्न क्लाउड-आधारित अनुप्रयोगों के लिए क्रेडेंशियल चुराते हैं।

पायथन मैलवेयर से जुड़ी आक्रमण श्रृंखलाएं (अटैक चैन) प्रारंभिक पहुंच प्राप्त करने और विशेषाधिकार वृद्धि और दृढ़ता के लिए अपाचे HTTP सर्वर, लारवेल फ्रेमवर्क और PHP यूनिट में ज्ञात सुरक्षा

खामियों का फायदा उठाने के लिए जानी जाती हैं। AndroxghOst ने सबसे पहले अपाचे में एक त्रुटि के माध्यम से प्रवेश प्राप्त किया, जिसे CVE-2021-41773 के रूप में पहचाना गया, जिससे यह कमजोर प्रणालियों तक पहुंच प्राप्त कर सका। इसके बाद, यह अतिरिक्त कमजोरियों का फायदा उठाता है, विशेष रूप से CVE-2017-9841 और CVE-2018-15133, कोड को निष्पादित करने और लगातार नियंत्रण स्थापित करने के लिए, अनिवार्य रूप से लक्षित सिस्टम पर कब्जा कर लेता है। AndroxghOst को .env फ़ाइलों, डेटाबेस और क्लाउड क्रेडेंशियल्स सहित विभिन्न स्रोतों से संवेदनशील डेटा को बाहर निकालने के लिए डिज़ाइन किया गया है। यह साइबर अपराधी को छेड़छाड़ किए गए सिस्टम में अतिरिक्त पेलोड पहुंचाने की अनुमति देता है। इसमें कहा गया है कि इसके हनीपोट बुनियादी ढांचे को निशाना बनाने के अधिकांश हमले अमेरिका, ब्रिटेन, चीन, नीदरलैंड, जर्मनी, बुल्गारिया, कुवैत, रूस, एस्टोनिया और भारत से हुए।

चूँकि क्लाउड वातावरण तेजी से साइबर अपराधियों के लिए एक आकर्षक लक्ष्य बनता जा रहा है, **इसलिए सॉफ़्टवेयर को अद्यतन रखना और संदिग्ध गतिविधि की निगरानी करना महत्वपूर्ण है।** थ्रेट इंटेलिजेंस फर्म ने क्लाउडग्रैपलर नामक एक टूल भी जारी किया है, जो क्लाउड के फाउंडेशन टॉप पर बनाया गया है और जाने-माने साइबर अपराधियों से संबंधित मलेशियस घटनाओं को चिह्नित करने के लिए AWS और Azure को स्कैन करता है।

## सुझाव:

- अज्ञात लिंक से सावधान रहें।
- सॉफ्टवेयर अपडेट रखें।
- मजबूत पासवर्ड का प्रयोग करें।
- दो कारक प्रमाणीकरण सक्षम करें।
- स्वयं और दूसरों को शिक्षित करें।
- प्रतिष्ठित सुरक्षा सॉफ़्टवेयर का उपयोग करे।
- संदेशों और अनुलग्नकों को सत्यापित करें।
- संदिग्ध गतिविधि की रिपोर्ट करें।

# 2. साइबर फ्रॉड

### नवीनतम ''डिजिटल अरेस्ट स्कैम'' में नोएडा की महिला से 7 घंटे की स्काइप कॉल पर 3.7 लाख रुपए की ठगी की गई।

नोएडा स्थित एक 32 वर्षीय महिला आईटी इंजीनियर से साइबर अपराधियों ने कथित तौर पर 3.75 लाख रुपए की धोखाधड़ी की, जिन्होंने उसे लगभग सात घंटे तक स्काइप कॉल पर "बंधक" बनाए रखा, धीरे-धीरे योजनाबद्ध तरीके से उसके खाते से पैसे निकाल लिए। पुलिस ने कहा कि जालसाजों ने स्वयं को पुलिस कर्मी होने का दावा किया और उन पर मुंबई से ताइवान भेजे गए एक कथित पार्सल में ड्रग्स की आपूर्ति करने का आरोप लगाया। पीड़िता के पति ने शिकायत दर्ज कराई है जिसमें उन्होंने बताया कि उनकी पत्नी को एक कूरियर कंपनी के नंबर से कॉल आया था और फिर स्काइप कॉल के माध्यम से उनके साथ धोखाधड़ी की गई। एडिशनल डीसीपी, नोएडा ने कहा है कि मामला दर्ज करके आवश्यक कानूनी कार्रवाई की जा रही है। उन्होंने बताया कि एक कूरियर मुंबई से ताइवान जा रहा था, जिसे सीमा शुल्क अधिकारियों ने जब्त कर लिया और उसमें आपत्तिजनक वस्तुएं मिलीं। फिर कॉल एक पुलिस अधिकारी को स्थानांतरित कर दी गई जिसने मेरी पत्नी के खाते का विवरण और परिवार का विवरण मांगा। उन्होंने उसे डराया-धमकाया और उसे पैसे देने के लिए मजबूर किया।

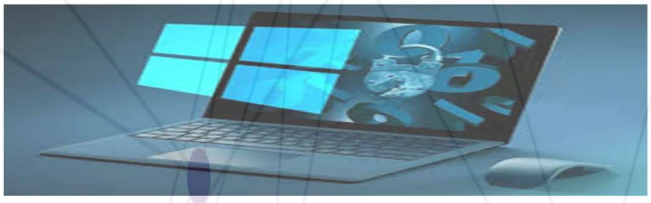
### फेसबुक फ्रेंड रिक्वेस्ट एक्सेप्ट करने के बाद गुजराती बिजनेसमैन से 95 लाख रुपए की ठगी की गई।

साइबर धोखाधड़ी अधिक व्यापक होती जा रही है, और बड़ी संख्या में लोग इनका शिकार बन रहे हैं। एक शख्स ने दावा किया कि फेसबुक पर एक महिला से दोस्ती के बाद उसने लाखों रुपए गंवा दिए। कथित तौर पर गुजराती व्यवसायी को एक धोखाधड़ी में कुल 95 लाख रुपए का नुकसान हुआ। टाइम्स ऑफ इंडिया (टीओआई) की रिपोर्ट के अनुसार, अलकापुरी निवासी एक पीड़ित ने धोखाधड़ी का शिकार होने के बाद साइबर क्राइम पुलिस स्टेशन में शिकायत की। उन्होंने पुलिस को बताया कि उन्हें पिछले साल अक्तूबर में फेसबुक पर एक महिला जालसाज से फ्रेंड रिक्वेस्ट मिली थी, जिसे उन्होंने स्वीकार कर लिया। बाद में उन्होंने अपनी बातचीत व्हाट्सएप के माध्यम से शुरू कर दी। आउटलेट के अनुसार, पीड़ित के दोस्त ने सुझाव दिया कि वह भारत से 1 लाख रुपए में अलग-अलग हर्बल सामान खरीदकर धोखेबाज फर्म को 2 लाख रुपए में बेच दे। एक बार जब पीड़ित सहमत हो गया, तो उसने उससे सामान प्राप्त करने के लिए किसी दोस्त से संपर्क करने का आग्रह किया। मित्र और पीड़ित को ईमेल द्वारा सूचित किया गया। उन्होंने 1 लाख रुपए का भुगतान किया और उनकी ऑनलाइन चैट के बाद एक सैंपल पैकेट प्राप्त किया। बक्सा तय समय पर आ गया, लेकिन पीड़ित ने उसे नहीं खोला।

**जैसा कि प्रकाशन में कहा गया है, उन्होंने इसके बजाय और अधिक ऑर्डर दिए।**

पीड़ित ने कथित तौर पर उसके बाद भी दोस्त को उसके निर्देशों के अनुसार कई खातों में पैसे देना जारी रखा। जब मित्र ने काल्पनिक बहानों के तहत अधिक पैसे का अनुरोध करना जारी रखा, तो उसे संदेह हुआ। टाईम्स ऑफ इंडिया के अनुसार, जब उसे वादे के मुताबिक रकम नहीं मिली तो पीड़ित ने अपने दोस्त से समझौता रद्द करने और उसे उसके पैसे वापस देने का आग्रह किया। लेकिन तब से न तो दोस्त और न ही महिला संपर्क में हैं।

# 3. इस माह के टिप



### विंडोज़ सुरक्षा संबंधी सुझाव:-

**अपने सिस्टम को अपडेट रखें:** सुनिश्चित करें कि आपका विंडोज ऑपरेटिंग सिस्टम, साथ ही सभी इंस्टॉल किए गए सॉफ़्टवेयर और ड्राइवर, नवीनतम सुरक्षा पैच और अपडेट के साथ अद्यतन हैं। ज्ञात भेद्यता से बचाने के लिए नियमित रूप से विंडोज अपडेट की जांच करें और इंस्टॉल करें।

**मजबूत पासवर्ड का उपयोग करें:** अपने उपयोगकर्ता खातों के लिए मजबूत, विशिष्ट पासवर्ड बनाएं, और अपने पासवर्ड को सुरक्षित रूप से संग्रहीत और प्रबंधित करने के लिए पासवर्ड मैनेजर का उपयोग करने पर विचार करें। सुरक्षा

की एक अतिरिक्त परत के लिए जहां भी संभव हो बहु-कारक प्रमाणीकरण (एमएफए) सक्षम करें।

**विंडोज डिफेंडर एंटीवायरस सक्षम करें:** विंडोज डिफेंडर एंटीवायरस विंडोज़ इंफो से बना है और वायरस, मैलवेयर एवं अन्य खतरों के विरूद्ध वास्तविक समय में सुरक्षा प्रदान करता है। सुनिश्चित करें कि यह आपके सिस्टम को सुरक्षित रखने में मदद के लिए सक्षम और नियमित रूप से अपडेट किया गया है।

**विंडोज फ़ायरवॉल सक्षम करें:** इनकमिंग और आउटगोइंग नेटवर्क ट्रैफ़िक की निगरानी और नियंत्रण के लिए विंडोज फ़ायरवॉल चालू करें या तीसरे पक्ष फ़ायरवॉल का उपयोग करें। अनधिकृत पहुंच को रोकने के लिए फ़ायरवॉल सेटिंग्स कॉन्फ़िगर करें और केवल आवश्यक कनेक्शन की अनुमति दें।

**ईमेल अटैचमेंट और लिंक से सावधान रहें:** ईमेल अटैचमेंट खोलते समय या लिंक पर क्लिक करते समय सावधानी बरतें, विशेषकर यदि वे अज्ञात या संदिग्ध स्रोतों से हों। संवेदनशील जानकारी का खुलासा करने के लिए आपको धोखा देने के लिए डिज़ाइन किए गए फ़िशिंग ईमेल और धोखाधड़ी से सावधान रहें।

**सुरक्षित ब्राउज़िंग प्रथाओं का उपयोग करें:** एक सुरक्षित वेब ब्राउज़र का उपयोग करें, जैसे कि **Microsoft Edge** या **Google Chrome**, और इसे नवीनतम सुरक्षा अपडेट के साथ अद्यतन रखें। अपरिचित वेबसाइटों पर जाते समय सतर्क रहें और अविश्वसनीय स्रोतों से सॉफ़्टवेयर डाउनलोड करने से बचें।

**अपना डेटा एन्क्रिप्ट करें:** अपनी हार्ड ड्राइव और संवेदनशील डेटा को एन्क्रिप्ट करने के लिए **BitLocker** जैसे अंतर्निहित एन्क्रिप्शन टूल का उपयोग करें। यदि आपका उपकरण खो जाता है या चोरी हो जाता है, तो आपके डेटा को एन्क्रिप्ट करने से इसे अनधिकृत पहुंच से बचाने में मदद मिलती है।

**अपने डेटा का नियमित रूप से बैकअप लें:** अपनी महत्वपूर्ण फ़ाइलों और डेटा का बाहरी हार्ड ड्राइव, क्लाउड स्टोरेज सेवा या नेटवर्क ड्राइव पर नियमित बैकअप लें। किसी सुरक्षा घटना या सिस्टम विफलता की स्थिति में, आप बहुमूल्य जानकारी खोए बिना बैकअप से अपना डेटा पुनर्स्थापित कर सकते हैं।

**एकाउन्ट टाइप का उचित उपयोग करें:** रोजमर्रा के कार्यों के लिए व्यवस्थापक (एडमिनिस्ट्रेटर) एकाउन्ट का उपयोग करने से बचें। इसके बजाय, नियमित उपयोग के लिए एक मानक उपयोगकर्ता एकाउन्ट का उपयोग करें, और आवश्यक होने पर ही व्यवस्थापक खाते पर स्विच करें। यह आपके सिस्टम में अनधिकृत परिवर्तनों को रोकने में मदद कर सकता है।

**जानकार बनें और शिक्षित रहें:** प्रतिष्ठित सुरक्षा ब्लॉग, समाचार स्रोतों और फोरम के माध्यम से नवीनतम सुरक्षा खतरों और सर्वोत्तम प्रथाओं के बारे में जानकारी रखें। स्वयं को और अपने घर या संगठन में अन्य लोगों को सामान्य सुरक्षा जोखिमों और उन्हें कम करने के बारे में शिक्षित करें।

**BitLocker सक्षम करें:** यदि आप विंडोज 10 या एंटरप्राइज का उपयोग कर रहे हैं, तो अपने डिवाइस के खो जाने या चोरी हो जाने की स्थिति में अपने डेटा की सुरक्षा के लिए BitLocker के साथ अपने सिस्टम ड्राइव को एन्क्रिप्ट करने पर विचार करें। BitLocker पूर्ण-डिस्क एन्क्रिप्शन प्रदान करता है, यह सुनिश्चित करते हुए कि केवल अधिकृत उपयोगकर्ता ही आपके डेटा तक पहुंच सकते हैं।

**बायोमेट्रिक प्रमाणीकरण के लिए विंडोज "हैलो" का उपयोग करें:** यदि आपका डिवाइस इसका समर्थन करता है, तो केवल पासवर्ड पर निर्भर रहे बिना अपने सिस्टम में सुरक्षित रूप से लॉग इन करने के लिए चेहरे की पहचान या फिंगरप्रिंट स्कैनिंग जैसे बायोमेट्रिक प्रमाणीकरण के लिए विंडोज हैलो का उपयोग करने पर विचार करें।

**कंट्रोल्ड फ़ोल्डर एक्सेस सक्षम करें:** विंडोज सिक्योरिटी में कंट्रोल्ड फ़ोल्डर एक्सेस एक सुविधा है, जो आपकी महत्वपूर्ण फ़ाइलों और फ़ोल्डरों को मलिशियस एप्लिकेशन द्वारा अनधिकृत परिवर्तनों से बचाने में मदद करती है। अपने संवेदनशील डेटा में सुरक्षा की एक अतिरिक्त परत जोड़ने के लिए इस सुविधा को सक्षम करें।

**स्मार्टस्क्रीन:** विंडोज़ में स्मार्टस्क्रीन एक सुविधा है जो फ़िशिंग हमलों और मलिशियस सॉफ़्टवेयर डाउनलोड से बचाने में मदद करती है। यह ज्ञात खतरों की सूची के विरुद्ध वेबसाइटों और फ़ाइलों की जाँच करता है और संभावित रूप से हानिकारक सामग्री का सामना करने पर उपयोगकर्ताओं को चेतावनी देता है।

**डिवाइस गार्ड:** विंडोज 10 एंटरप्राइज और विंडोज सर्वर 2016 में डिवाइस गार्ड एक सुरक्षा सुविधा है जो केवल विश्वसनीय एप्लिकेशन को सिस्टम पर चलने की अनुमति देकर मैलवेयर से बचाने में मदद करता है। यह सुनिश्चित करने के लिए हार्डवेयर-आधारित सुरक्षा सुविधाओं का उपयोग करता है कि केवल हस्ताक्षरित और विश्वसनीय कोड निष्पादित किया जाता है।

**क्रेडेंशियल गार्ड:** क्रेडेंशियल गार्ड विंडोज 10 एंटरप्राइज और विंडोज सर्वर 2016 में एक सुरक्षा सुविधा है जो वर्चुअलाइज्ड वातावरण में उपयोगकर्ता क्रेडेंशियल को सुरक्षित रूप से संग्रहीत करके पास-द-हैश ( पीटीएच ) हमलों से बचाने में मदद करता है।

**विंडोज डिफेंडर एप्लिकेशन गार्ड:** विंडोज 10 एंटरप्राइज में यह सुविधा माइक्रोसॉफ्ट एज ब्राउज़र सेशन के लिए हार्डवेयर-आधारित पृथक्करण प्रदान करती है, बाकी सिस्टम को संभावित मैलवेयर और इंटरनेट से उत्पन्न होने वाले जीरो-डे के हमलों से बचाती है।

**सिक्युरिटी बेसलाइन:** माइक्रोसॉफ्ट सिक्युरिटी बेसलाइन प्रदान करता है जो संगठनों को उनकी सुरक्षा स्थिति में सुधार करने में मदद करने के लिए विंडोज सिस्टम हेतु अनुशंसित सुरक्षा सेटिंग्स का एक सेट है। उभरते खतरों और कमजोरियों को दूर करने के लिए इन बेसलाइनों को नियमित रूप से अपडेट किया जाता है।

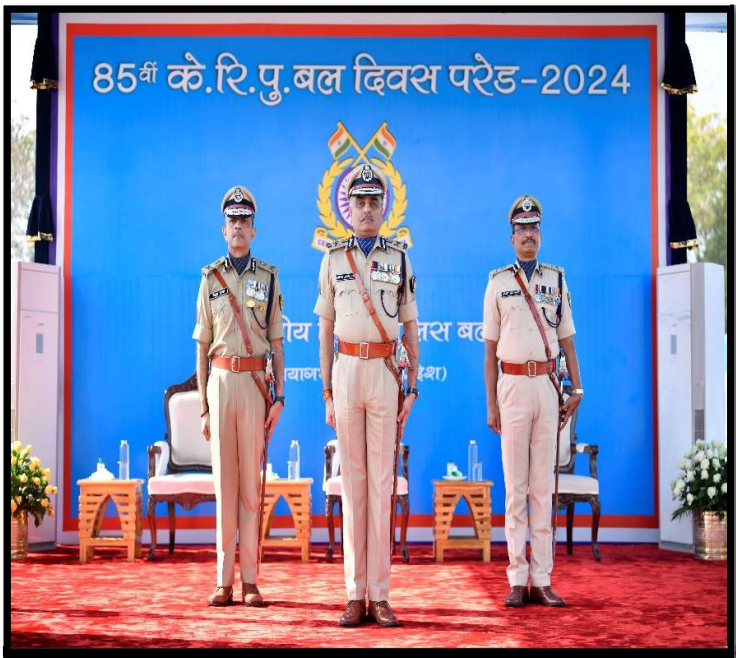
**माइक्रोसॉफ्ट सिक्युरिटी ब्लॉग:** माइक्रोसॉफ्ट नियमित रूप से अपने आधिकारिक सिक्युरिटी ब्लॉग पर विंडोज सुरक्षा से संबंधित अपडेट और अनाउंसमेंट्स प्रकाशित करता है। आप माइक्रोसॉफ्ट की नवीनतम सुरक्षा सुविधाओं, सर्वोत्तम प्रथाओं और खतरे की खुफिया जानकारी से अद्यतन रहने के लिए ब्लॉग पर जा सकते हैं।

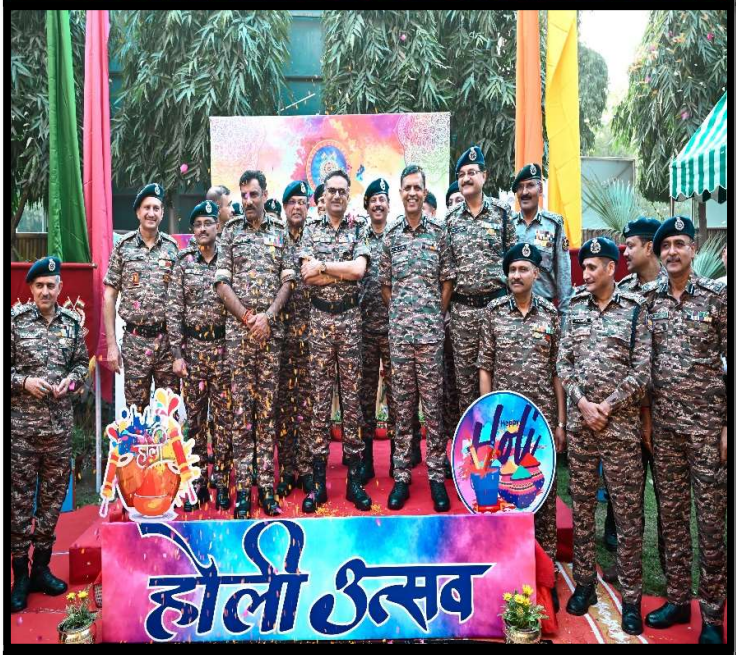
**विंडोज़ सिक्युरिटी केंद्र:** सुरक्षा से संबंधित किसी भी अलर्ट, अधिसूचना या अनुशंसाओं के लिए अपने सिस्टम पर विंडोज़ सिक्युरिटी केंद्र की जाँच करें। विंडोज़ सुरक्षा आपके सिस्टम की समग्र सुरक्षा स्थिति के बारे में जानकारी प्रदान करती है और सुरक्षा बढ़ाने के लिए अनुशंसाएँ प्रदान करती है।

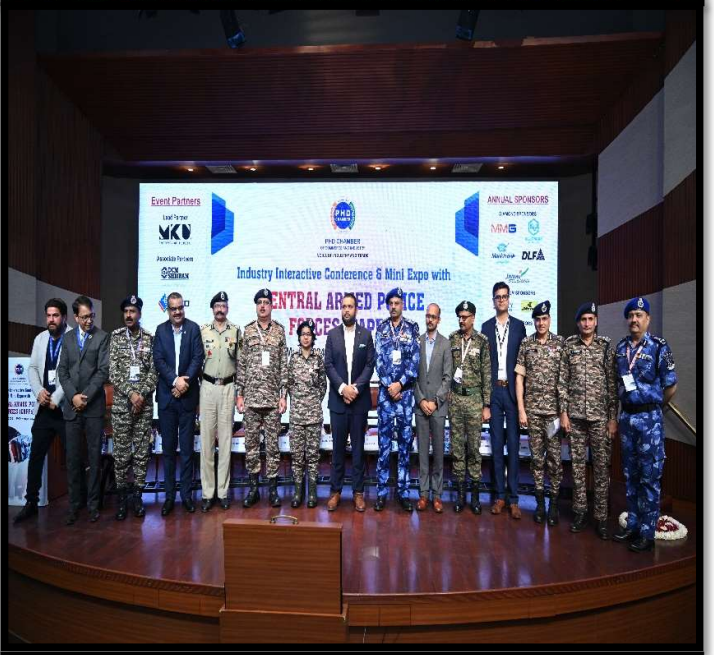
**माइक्रोसॉफ्ट सुरक्षा प्रतिक्रिया केंद्र (एमएसआरसी):** एमएसआरसी सुरक्षा शोधकर्ताओं, पेशेवरों और ग्राहकों के लिए माइक्रोसॉफ्ट का प्राथमिक सुरक्षा सूचना पोर्टल है। यह विंडोज सुरक्षा सहित माइक्रोसॉफ्ट उत्पादों से संबंधित सुरक्षा कमजोरियों, पैच और एडवायजरी के बारे में जानकारी प्रदान करता है।

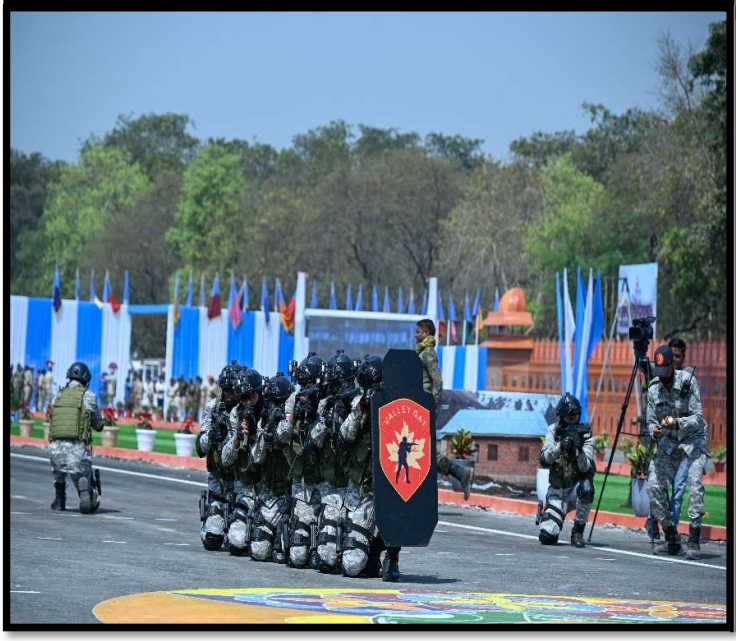
**सुरक्षा सम्मेलन और कार्यक्रम:** सुरक्षा सम्मेलनों, वेबिनार और आयोजनों पर नजर रखें जहां माइक्रोसॉफ्ट के प्रतिनिधि या सुरक्षा विशेषज्ञ नवीनतम सुरक्षा रुझानों, खतरों और विंडोज सुरक्षा से संबंधित सर्वोत्तम प्रथाओं पर चर्चा कर सकते हैं।

**सुरक्षा समुदाय और फ़ोरम:** सुरक्षा समुदायों, फ़ोरम और चर्चा समूहों से जुड़ें, जहाँ पेशेवर और उत्साही लोग विंडोज सुरक्षा और संबंधित विषयों के बारे में अंतर्दृष्टि, युक्तियाँ और समाचार साझा करते हैं।




संचार एवं सूचना प्रौधगिकी निदेशालय , सीआरपीएफ