

केंद्रीय रिजर्व पुलिस बल

जुलाई, 2026

साइबर बाइट

AI-आधारित
और डीपफेक
फ़िशिंग:

राष्ट्रीय सुरक्षा के लिए
बढ़ता खतरा

RISE OF THE DEEPFAKES



Data scientists are sounding the alarm about advances in artificial intelligence that enable video and images to be generated that are impossible to distinguish from the real thing. Fakes and forgeries have been around for centuries, but the proliferation of powerful new techniques from machine learning and AI have made them

more effective. Misleading video and images produced by the new technology are known as 'deepfakes', a combination of the words 'deep learning' and 'fake'. "Give it a few years and it will become impossible to tell what's real and what's fake," said a top

potential for fake news and financial fraud. "The government is investing in counter deepfakes and the same AI techniques that create deepfakes can be used to detect them. It's an arms race," she said. "There's no telling who will win."



फ़ेक प्रोफ़ाइल, शादी का वादा: सरकार ने मैट्रिमोनियल धोखाधड़ी के बढ़ते मामलों को लेकर चेतावनी दी है।

1. नवीनतम साइबर खतरा

1. AI और डीपफेक से होने वाली ऑनलाइन ठगी: देश की सुरक्षा के लिए बढ़ता खतरा

AI और डीपफेक phishing सोशल इंजीनियरिंग का एक उन्नत रूप है जिसमें साइबर अपराधी अत्यधिक विश्वसनीय ईमेल, संदेश, वॉयस कॉल या वीडियो बनाने के लिए कृत्रिम बुद्धिमत्ता (AI) का उपयोग करते हैं जो वरिष्ठ अधिकारियों, कमांडरों या अधिकारियों जैसे विश्वसनीय व्यक्ति बनकर सामने आते हैं। इसका उद्देश्य पीड़ितों को संवेदनशील जानकारी साझा करने, वित्तीय लेनदेन को मंजूरी देने, या सुरक्षित प्रणालियों तक अनधिकृत पहुंच प्रदान करने के लिए धोखा देना है।



Scam कैसे संचालित होता है?

हमलावर सार्वजनिक स्रोतों/सोशल मीडिया से जानकारी एकत्र करते हैं और व्यक्तिगत फ़िशिंग संदेश उत्पन्न करने या किसी व्यक्ति की आवाज़ और उपस्थिति को Clone करने के लिए AI का उपयोग करते हैं। ये नकली संचार अक्सर तात्कालिकता या अधिकार की भावना पैदा करते हैं, जिससे पीड़ितों को आधिकारिक चैनलों के माध्यम से अनुरोध को सत्यापित किए बिना कार्य करने के लिए प्रेरित किया जाता है।

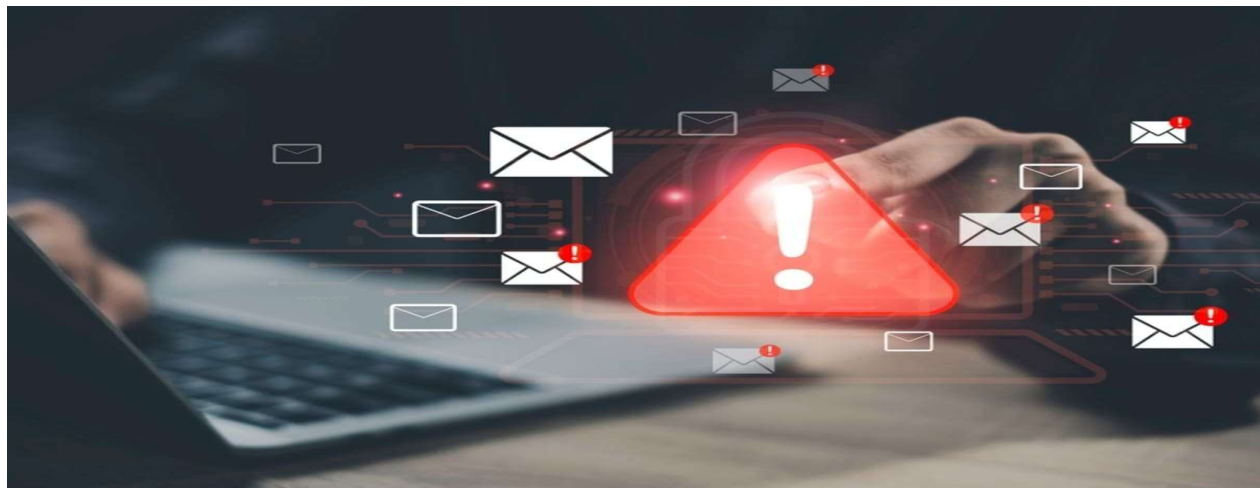
कैसे बचें?: -

- कार्रवाई से पहले संवेदनशील अनुरोधों की दोबारा जांच करें।
- ऑथेंटिकेशन के लिए कभी भी केवल आवाज या वीडियो पर निर्भर न रहें।
- सभी आधिकारिक खातों पर मल्टी-फैक्टर ऑथेंटिकेशन (MFA) लागू करें।
- वित्तीय या परिचालन निर्णयों के लिए स्थापित अनुमोदन और सत्यापन प्रक्रियाओं का पालन करें।
- किसी भी संदिग्ध संचार की सूचना तुरंत साइबर सुरक्षा या आईटी टीम को दें।

मुख्य संदेश: AI-generated धोखे के युग में, बिना जाँच किए किसी बात पर भरोसा न करें

2. भरोसेमंद माध्यमों के हैक होने का खतरा:

Compromised Trusted Channels ऐसे संचार या सॉफ्टवेयर सेवाएँ होती हैं जिन पर लोग और संस्थाएँ सामान्य रूप से भरोसा करती हैं, लेकिन साइबर अपराधियों द्वारा उनका गलत इस्तेमाल या नियंत्रण कर लिया जाता है और सीधे हमला करने के बजाय, साइबर हमलावर भरोसेमंद माध्यमों जैसे आधिकारिक ईमेल खाते, मैसेजिंग ऐप, सॉफ्टवेयर अपडेट प्रणाली, क्लाउड सेवाएँ या रिमोट एक्सेस सिस्टम का उपयोग करके वायरस (मैलवेयर) फैलाते हैं, पासवर्ड और अन्य जानकारी चुराते हैं या लोगों को धोखा देते हैं। क्योंकि ये माध्यम असली और भरोसेमंद दिखाई देते हैं, इसलिए लोग अक्सर बिना जाँच किए अटैचमेंट खोल देते हैं, गलत लिंक पर क्लिक कर देते हैं या फर्जी अनुरोधों को स्वीकार कर लेते हैं।



यह कैसे संचालित होता है?

जब कोई trusted channel हैक हो जाता है, तो साइबर हमलावर सामान्य सुरक्षा उपायों को पार करके संवेदनशील सिस्टम और जानकारी तक बिना अनुमति पहुँच सकते हैं। जैसे की — हैक किए गए आधिकारिक ईमेल खातों से भेजे गए फर्जी ईमेल, compromise किए गए सॉफ्टवेयर विक्रेताओं के माध्यम से भेजे गए खतरनाक अपडेट (सप्लाय चेन हमला), सहयोगी प्लेटफॉर्म पर भेजे गए नकली संदेश, तथा चोरी किए गए पासवर्ड का उपयोग करके VPN या रिमोट डेस्कटॉप कनेक्शन का दुरुपयोग करते हैं। ऐसे हमलों से डेटा चोरी, रैनसमवेयर संक्रमण, आर्थिक नुकसान, कामकाज में बाधा और संस्था की प्रतिष्ठा को नुकसान हो सकता है।

कैसे सुरक्षित रहें?

संगठन एक स्तरित साइबर सुरक्षा दृष्टिकोण को अपनाकर हैक किए गए विश्वसनीय चैनलों के जोखिम को कम कर सकते हैं। इसमें मल्टी-फैक्टर ऑथेंटिकेशन (MFA) को लागू करना, डिजिटल हस्ताक्षर के माध्यम से Software Update को सत्यापित करना, Zero Trust सुरक्षा मॉडल को लागू करना, उपयोगकर्ता और नेटवर्क गतिविधियों की निरंतर निगरानी करना और नियमित सुरक्षा जागरूकता प्रशिक्षण का संचालन करना शामिल है। समय पर Patch Management, ईमेल सुरक्षा समाधान, एंडपॉइंट डिटेक्शन और प्रतिक्रिया (EDR), और घटना प्रतिक्रिया योजना भी महत्वपूर्ण क्षति होने से पहले खतरों का पता लगाने और उन्हें रोकने में मदद करती है।

मुख्य संदेश: Link, Attachment या गोपनीय डेटा साझा करने से पहले हमेशा प्रेषक को सत्यापित करें और अनुरोधों की पुष्टि करें। साइबर हमलों को रोकने और संगठनात्मक सुरक्षा की रक्षा करने में मदद के लिए किसी भी संदिग्ध गतिविधि की तुरंत रिपोर्ट करें।

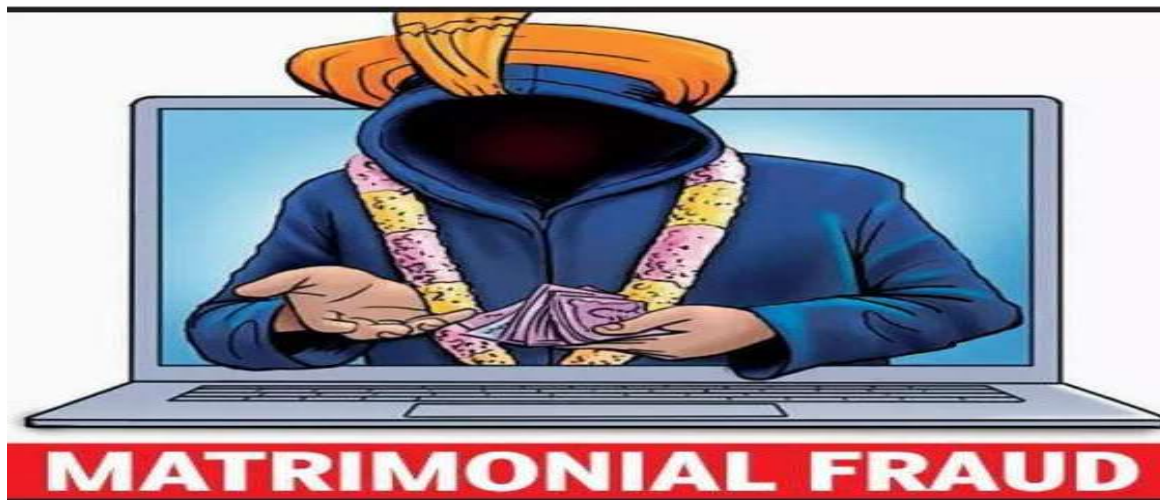
2. KNOWLEDGE बैंक

- सरकार ने 18 राज्यों और केंद्रशासित प्रदेशों में साइबर अपराध मामलों के लिए **e-zero FIR** प्रणाली शुरू की:



सरकार ने 18 राज्यों और केंद्र शासित प्रदेशों में साइबर अपराध मामलों में **e-zero FIR** दर्ज करने की प्रणाली शुरू की है। **e-zero FIR** प्लेटफॉर्म राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (NCRP) या 1930 साइबर हेल्पलाइन के माध्यम से रिपोर्ट की गई शिकायतों को योग्य साइबर वित्तीय धोखाधड़ी मामलों के लिए स्वचालित रूप से **e-zero FIR** में परिवर्तित करने में सक्षम बनाता है, जिससे पुलिस कार्रवाई और जांच तेज हो जाती है।

- फर्जी प्रोफाइल, शादी के वादे: सरकार ने बढ़ती वैवाहिक धोखाधड़ी के प्रति आगाह किया:



गृह मंत्रालय के भारतीय साइबर अपराध समन्वय केंद्र (I4C) ने लोगों को ऑनलाइन वैवाहिक धोखाधड़ी में तेज वृद्धि के प्रति आगाह करते हुए कहा है कि साइबर अपराधी खुद को अमीर पेशेवर या NRI बताकर वैवाहिक वेबसाइटों और ऐप्स का शोषण कर रहे हैं, शादी के वादे के साथ पीड़ितों का विश्वास हासिल कर रहे हैं और फिर उनसे बड़ी रकम ठग रहे हैं। एक सलाह में, एजेंसी ने कहा कि डिजिटल वैवाहिक प्लेटफार्मों की बढ़ती लोकप्रियता ने धोखेबाजों के लिए नए अवसर पैदा किए हैं।

3. आईटी बुनियादी ढांचे की सुरक्षा कैसे करें

1. मल्टी-फैक्टर ऑथेंटिकेशन (MFA) अपनाएँ:

मल्टी-फैक्टर ऑथेंटिकेशन (MFA) आपके खाते को अधिक सुरक्षित बनाता है। इसमें log-in करने के लिए केवल पासवर्ड ही नहीं, बल्कि OTP, a bio-metric (फिंगरप्रिंट, चेहरे की पहचान) या सुरक्षा कुंजी जैसी एक अतिरिक्त फैक्टर की भी आवश्यकता होती है। अगर किसी को आपका पासवर्ड पता भी चल जाए, तब भी वह बिना इस अतिरिक्त फैक्टर के आपके खाते में प्रवेश नहीं कर सकता। इससे आपका खाता सुरक्षित रहता है और साइबर अपराधियों के लिए उसमें घुसना बहुत मुश्किल हो जाता है।



सरकारी कार्यालयों में सभी Administrative Account, Remote Access, VPN, क्लाउड सेवाओं और अन्य महत्वपूर्ण प्रणालियों के लिए **मल्टी-फैक्टर ऑथेंटिकेशन (MFA)** का उपयोग अनिवार्य होना चाहिए। जहाँ संभव हो, FIDO2 (Fast Identity Online 2) सुरक्षा कुंजी (Security Key) या पासकी (Passkey) जैसी अधिक सुरक्षित लॉगिन व्यवस्था अपनानी चाहिए। साथ ही, लॉगिन गतिविधियों की नियमित जाँच और उपयोगकर्ताओं की पहुँच (Access) की समय-समय पर समीक्षा करने से सुरक्षा और मजबूत होती है।

आवश्यक कार्यवाही:

- सभी Administrative, privilege, VPN, रिमोट एक्सेस और क्लाउड Account के लिए Multi Factor Authentication (MFA) लागू करें।
- उच्च जोखिम वाले उपयोगकर्ताओं के लिए फ़िशिंग-प्रतिरोधी ऑथेंटिकेशन विधियों, जैसे Hardware सुरक्षा कुंजी या Passkey, को प्राथमिकता दें।
- Legacy Authentication Protocol अक्षम करें जो MFA का समर्थन नहीं करते हैं।
- समय-समय पर उपयोगकर्ता खातों की समीक्षा करें और अनावश्यक Privilege हटा दें।
- संदिग्ध लॉगिन प्रयासों और अनधिकृत पहुंच का पता लगाने के लिए प्रमाणीकरण Log की लगातार निगरानी करें।
- सुरक्षित लॉगिन की अच्छी आदतें और क्रेडेंशियल चोरी के जोखिमों पर नियमित उपयोगकर्ता जागरूकता कार्यक्रम आयोजित करें।

मूल संदेश:

सिर्फ पासवर्ड अब सरकारी प्रणालियों की सुरक्षा के लिए पर्याप्त नहीं हैं। मल्टी-फैक्टर ऑथेंटिकेशन (MFA) को लागू करने से अनधिकृत पहुंच का जोखिम काफी कम हो जाता है, संवेदनशील जानकारी की सुरक्षा होती है और सरकारी आईटी बुनियादी ढांचे की समग्र साइबर क्षमता मजबूत होती है।

4. साइबर गपशप

1. बैंक ऑफ बड़ौदा पर बड़े पैमाने पर डेटा लीक का आरोप; ग्राहकों का 1,000 जीबी डेटा की जानकारी कथित तौर पर उजागर:

एक हैकिंग समूह के दावों के बाद बैंक ऑफ बड़ौदा सुर्खियों में आ गया है कि उसने Dark Web पर लगभग 1000 GB संवेदनशील ग्राहक और आंतरिक बैंकिंग डेटा लीक कर दिया है। कथित घटना ने साइबर सुरक्षा शोधकर्ताओं और खतरे की खुफिया प्लेटफार्मों का महत्वपूर्ण ध्यान आकर्षित किया है। हालांकि, बैंक ऑफ बड़ौदा ने आधिकारिक तौर पर पुष्टि नहीं की है कि कोई डेटा लीक हुआ है, और किसी भी सरकारी एजेंसी ने अब तक दावों की authentication की पुष्टि नहीं की है।

2. वाराणसी में पांच साइबर अपराधी पकड़े गए: पुलिस ने 43 एटीएम कार्ड और 12 पासबुक जब्त किए:

वाराणसी कमिश्नरेट की साइबर क्राइम पुलिस ने साइबर धोखाधड़ी में शामिल एक अंतरराज्यीय गिरोह का भंडाफोड़ किया है। गिरोह ने लोगों को ठगने के लिए बैंक खातों और APK फाइलों का इस्तेमाल किया। गिरोह के पांच सदस्यों को गिरफ्तार किया गया है। पुलिस ने 15 Android मोबाइल, तीन आईफोन, 43 एटीएम कार्ड, 12 पासबुक, 10 चेकबुक, 11 क्यूआर कोड, 12 सिम कार्ड, एक लैपटॉप, एक डायरी, दो चार पहिया वाहन (महिंद्रा थार और हुंडई आई-20) और आरोपियों के कब्जे से ₹12,060 नकद बरामद किए हैं।

3. साइबर क्राइम इकाई ने पीएम, केंद्रीय मंत्रियों की तस्वीरों का इस्तेमाल कर फर्जी निवेश घोटालों की चेतावनी दी:

भारतीय साइबर अपराध समन्वय केंद्र (I4C) ने लोगों को Facebook और Instagram पर प्रसारित होने वाले फर्जी निवेश विज्ञापनों के प्रति सतर्क रहने की चेतावनी देते हुए कहा है कि साइबर अपराधी उच्च रिटर्न के झूठे वादों के साथ पीड़ितों को लुभाने के लिए Social Media का तेजी से उपयोग कर रहे हैं। I4C के अनुसार, धोखेबाजों ने प्रधान मंत्री, केंद्रीय मंत्रियों, प्रमुख उद्योगपतियों, निवेश विशेषज्ञों, फिल्मी हस्तियों और अन्य प्रसिद्ध हस्तियों के नाम, तस्वीरों और Video का दुरुपयोग करते हैं।

5. साइबर स्वच्छता

- Strong, Unique पासवर्ड का उपयोग करें और सभी आधिकारिक accounts के लिए मल्टी-फैक्टर प्रमाणीकरण (MFA) सक्षम करें।
- ऑपरेटिंग सिस्टम, एप्लिकेशन और एंटीवायरस सॉफ्टवेयर को latest security patches के साथ अपडेट रखें।
- फ़िशिंग ईमेल, संदिग्ध Link और अज्ञात attachments से सावधान रहें।
- नियमित रूप से महत्वपूर्ण सरकारी डेटा का बैकअप लें और सत्यापित करें कि बैकअप बहाल किया जा सकता है।
- उपयोगकर्ताओं को केवल वह पहुंच प्रदान करके least privilege के सिद्धांत का पालन करें जिसकी उन्हें आवश्यकता है।
- केवल अधिकृत यूएसबी डिवाइस का उपयोग करें और उपयोग से पहले removable मीडिया को स्कैन करें।
- ध्यान न दिए जाने पर कंप्यूटर को लॉक करें और Encryption और सुरक्षित storage के माध्यम से संवेदनशील जानकारी को सुरक्षित रखें।
- किसी भी संदिग्ध गतिविधि, सुरक्षा घटना या डेटा breach की सूचना तुरंत आईटी विंग को दें।

6. IT WING में नया विकास

1. Training मॉड्यूल के अंतर्गत पीटी/परेड/गेम Data Entry Screen विकसित की गई।
2. Sambhav मोबाइल ऐप में Leave Plan करने की सुविधा functionality जोड़ी गई।



सीआरपीएफ के महानिदेशक **श्री जी.पी. सिंह (आईपीएस)** ने ग्रुप केंद्र रांची में **209** कोबरा बटा के जवानों और अधिकारियों के साथ बातचीत की और 'बड़ा खाना' में शामिल हुए।



सीआरपीएफ फैमिली वेलफेयर एसोसिएशन (**CWA**) ने ग्रुप केंद्र पिंजौर में सक्षम स्कूल की स्थापना और उसे सुसज्जित करने के लिए ₹25 लाख प्रदान करने के लिए अपनी CSR पहल के तहत HDFC Life के साथ एक समझौता ज्ञापन पर हस्ताक्षर किए।



सीआरपीएफ के महानिदेशक **श्री जी.पी. सिंह (आईपीएस)** VRS पर जवान को स्मृति चिन्ह प्रदान करते हुए।

संचार एवं सूचना प्रौद्योगिकी निदेशालय, के0रि0पु0बल