केंद्रीय रिज़र्व पुलिस बल

अप्रैल, 2026

साइबर बाइट

ईरानी हैकर्स रैनसमवेयर प्रॉक्सी के जरिए अमेरिकी महत्वपूर्ण बुनियादी ढांचे को बना रहे निशाना

एसटीएफ(STF) ने साइबर धोखाधड़ी के खिलाफ बड़ी कार्रवाई शुरू की, नकली वेबसाइटों और सोशल मीडिया लिंक्स को ब्लॉक किया

संचार एवं सूचना प्रौद्योगिकी निदेशालय, सीआरपीएफ

1. साइबर की दुनिया की खबरें

(ए) उत्तर कोरिया ने नवीनतम सेंधमारी में Mac OS उपयोगकर्ताओं को बनाया निशाना:

माइक्रोसॉफ्ट के अनुसार, एप्पल(Apple) उपयोगकर्ताओं के क्रेडेंशियल्स और क्रिप्टोकरेंसी चुराने के इरादे से उत्तर कोरियाई अपराधी 'सोशल इंजीनियरिंग' और एक नकली ज़ूम(Zoom) सॉफ्टवेयर अपडेट के संयोजन का उपयोग कर रहे हैं। इसका मकसद लोगों को धोखा देकर उनके कंप्यूटर पर मैन्युअल रूप से मैलवेयर चलवाना है।

रेडमंड की थ्रेट इंटेलिजेंस टीम प्योंगयांग समर्थित इस गिरोह को 'सैफायर स्लीट' (Sapphire Sleet- (जिसे APT38 भी कहा जाता है) के रूप में ट्रैक करती है। लाजरस ग्रुप (Lazarus Group) की यह शाखा कम से कम 2020 से सक्रिय है, और मुख्य रूप से क्रिप्टोकरेंसी वॉलेट और क्रिप्टोकरेंसी ट्रेडिंग व ब्लॉकचेन प्लेटफॉर्म से संबंधित बौद्धिक संपदा (IP) चुराने के लिए वित्तीय सेक्टर को निशाना बनाती है।

इन हमलों की शुरुआत सोशल इंजीनियरिंग से होती है। यह गिरोह सोशल मीडिया और नेटवर्किंग प्लेटफॉर्म जैसे लिंक्डइन (LinkedIn) पर भर्ती करने वालों (recruiters) की नकली प्रोफाइल बनाता है और फिर वित्तीय पेशेवरों से नौकरी के झूठे अवसरों के लिए संपर्क करता है। इसके बाद एक तकनीकी साक्षात्कार(technical interview) तय किया जाता है—जो मैलवेयर पहुँचाने का माध्यम बनता है। और वे सोशल इंजीनियरिंग से होने वाले कई दूसरे हमलों का भी सहारा लेते हैं, जिनमें से एक में, नॉर्थ कोरिया से जुड़े हमलावरों ने Axios के एक मेंटेनर को सोशल इंजीनियरिंग के ज़रिए फँसाया, उसके अकाउंट से छेड़छाड़ की,और ओपन सोर्स जावास्क्रिप्ट (JavaScript)लाइब्रेरी के ऐसे नुकसान पहुँचाने वाले (malicious) संस्करण प्रकाशित किए जिनमें रिमोट-एक्सेस ट्रोजन मौजूद था।

संगठन अपने उपयोगकर्ताओं और स्वयं को इस तरह के सोशल-इंजीनियरिंग अभियानों का शिकार होने से बचाने के लिए एक काम कर सकते हैं—वे लोगों को लिंक्डइन और अन्य सोशल मीडिया साइटों से उत्पन्न होने वाले खतरों के बारे में शिक्षित करें, विशेष रूप से उन अवांछित संदेशों के बारे में, जिनमें उपयोगकर्ताओं को कोई सॉफ्टवेयर डाउनलोड करने या वर्चुअल मीटिंग टूल इंस्टॉल करने के लिए कहा जाता है।

व्यक्तिगत उपयोगकर्ताओं के लिए

"तत्काल सहायता" के अनुरोधों पर संदेह करें

• लिंक्डइन (LinkedIn),ईमेल या चैट पर मिले वे अनचाहे संदेश, जिनमें आपसे कहा जाए कि:

- किसी मीटिंग में शामिल हों
- कोई सॉफ़्टवेयर इंस्टॉल करें

☞ इन्हें डिफ़ॉल्ट रूप से संदिग्ध ही मानें।

कभी भी अज्ञात स्क्रिप्ट या फाइलें न चलाएं

• .scpt, .bat, .sh, .exe जैसी फाइलें = उच्च जोखिम वाली होती हैं

• विशेष रूप से तब, जब इन्हें किसी "सपोर्ट सेशन" के दौरान भेजा गया हो।

<u>संगठनों के लिए</u>

1. नियमित सुरक्षा जागरूकता प्रशिक्षण आयोजित करें

• इन पर ध्यान दें:

- सोशल इंजीनियरिंग
- नकली सपोर्ट स्कैम (घोटाले)

- वास्तविक स्थितियों का उपयोग करें (जैसे नकली मीटिंग के आमंत्रण)

2. "नो स्क्रिप्ट एक्ज़ीक्यूशन" (स्क्रिप्ट न चलाने की) नीतिको लागू करें

• इन्हें ब्लॉक या प्रतिबंधित करें:

- एप्पल स्क्रिप्ट (.scpt)
- पावरशेल (PowerShell) / शेल स्क्रिप्ट
  • विशेष रूप से जो अज्ञात स्रोतों से आए हों।

(B) चारधाम यात्रा से पहले: एसटीएफ (STF) ने साइबर धोखाधड़ी के खिलाफ बड़ी कार्रवाई शुरू की, नकली वेबसाइटों और सोशल मीडिया लिंक्स को ब्लॉक किया।

इसके अतिरिक्त, अधिकारियों ने साइबर धोखाधड़ी नेटवर्क में शामिल होने के संदेह में 52 मोबाइल नंबरों की पहचान की है। आगे के दुरुपयोग को रोकने के लिए दूरसंचार विभाग (DoT) को इन नंबरों को ब्लॉक करने का अनुरोध भेजा गया है। जांच में चारधाम यात्रा की व्यवस्थाओं के नाम पर हेलीकॉप्टर बुकिंग फर्जी सेवाएं देने वाली 10 वेबसाइटों का भी खुलासा हुआ है। इन वेबसाइटों को तत्काल बंद करवाने के लिए संबंधित
डोमेन रजिस्ट्रारों को रिपोर्ट कर दी गयी है।

साइबर अपराधी अक्सर भ्रामक विज्ञापनों और "आधिकारिक बुकिंग पोर्टल" जैसे शब्दों का उपयोग करते हैं ताकि लोगों को उनकी प्रामाणिकता पर भरोसा हो जाए। कई मामलों में, तीर्थयात्री असली और नकली प्लेटफार्मों के बीच अंतर नहीं कर पाते और अंततः भारी मात्रा में पैसा गंवा देते हैं।

प्राधिकारियों ने तीर्थयात्रियों से यात्रा संबंधी किसी भी सेवा के लिए केवल आधिकारिक सरकारी वेबसाइटों और अधिकृत बुकिंग चैनलों का उपयोग करने का आग्रह किया है। उन्होंने लोगों को अज्ञात लिंक पर क्लिक न करने या रियायती तीर्थयात्रा पैकेज देने वाले सोशल मीडिया विज्ञापनों पर भरोसा न करने की भी सलाह दी है।

साइबर सुरक्षा विशेषज्ञों ने गौर किया है कि धार्मिक आयोजनों के दौरान अक्सर ऑनलाइन धोखाधड़ी के मामलों में तेज़ी देखी जाती है, क्योंकि लोग अपनी आस्था और जल्दबाज़ी के चलते जल्दी निर्णय लेते हैं, जिससे वे घोटालों का आसानी से शिकार बन जाते हैं। उन्होंने इस बात पर ज़ोर दिया कि वित्तीय नुकसान को रोकने के लिए रियल-टाइम मॉनिटरिंग और त्वरित प्रतिक्रिया तंत्र अत्यंत महत्वपूर्ण हैं।

☑ क्या करें (DO's)

✔ केवल आधिकारिक प्लेटफॉर्म का उपयोग करें

• यात्रा, दर्शन या हेलीकॉप्टर सेवाओं की बुकिंग केवल प्रामाणिक सरकारी पोर्टलों के माध्यम से ही करें।

• विश्वसनीय स्रोतों (राज्य पर्यटन विभाग / आधिकारिक घोषणाओं) से प्राप्त लिंक की दोबारा जाँच (Cross-check) करें।

✔ भुगतान से पहले सत्यापन करें

• वेबसाइट की प्रामाणिकता की पुष्टि करें (जैसे HTTPS, सही स्पेलिंग, संपर्क के विवरण)।

• संशय होने पर आधिकारिक हेल्पलाइन नंबरों पर कॉल करें।

✔ डोमेन की सावधानी से जाँच करें

• स्पेलिंग में की गई छोटी-मोटी धोखाधड़ी पर नज़र रखें (जैसे, ".in.net", ".org.in")।

• नए बनाए गए डोमेन की बजाय जाने-माने डोमेन को प्राथमिकता दें।

✔ भुगतान के सुरक्षित तरीकों का उपयोग करें

• केवल भरोसेमंद गेटवे (नेट बैंकिंग, कार्ड) के जरिए भुगतान करें।

• लेन-देन की रसीदें या स्क्रीनशॉट अपने पास सुरक्षित रखें।

✕ क्या न करें (DON'Ts)(जिनसे आपको बचना चाहिए)

✕ "लुभावने और अविश्वसनीय" ऑफ़र पर भरोसा न करें

• बहुत सस्ती हेलीकॉप्टर की बुकिंग या वीआईपीदर्शन के दावे खतरे का संकेत (Red flags) हो सकते हैं।

✕ अज्ञात लिंक पर क्लिक न करें

• एसएमएस (SMS), व्हाट्सएप या सोशल मीडिया विज्ञापनों से प्राप्त लिंक पर क्लिक करने से बचें।

✕ सोशलमीडियापेजोंपरभरोसानकरें

• फर्जी पेज अक्सर असली सेवाओं के लोगो (logo) और फोटो की नकल करके बनाए जाते हैं।

✕ बिना सोचे-समझे अग्रिम (Advance) भुगतान न करें

• विशेष रूप से किसी अज्ञात यूपीआई(UPI)आईडी या व्यक्तिगत नंबरों पर पैसे भेजने से बचें।

2. साइबर धोखाधड़ी

(A) ईरानी हैकर्स रैनसमवेयर प्रॉक्सी के जरिए अमेरिकी महत्वपूर्ण बुनियादी ढांचे को बना रहे निशाना: केला (KELA)की चेतावनी

केला (KELA) के नए आंकड़ों से पता चलता है कि ईरान राष्ट्र द्वारा प्रायोजित खतरे पैदा करने वाले तत्व (threat actors) अब पारंपरिक जासूसी से काफी आगे निकल चुके हैं, और वे राष्ट्र-राज्य संचालन (nation-state operations) और आर्थिक रूप से प्रेरित साइबर अपराध के बीच के अंतर को कम कर रहे हैं। बड़े पैमाने पर अपना खुद का रैनसमवेयर कार्टेल चलाने के बजाय, ये समूह मौजूदा आपराधिक पारिस्थितिकी तंत्र (ecosystem) में शामिल हो गए हैं। ये 'इनिशियल एक्सेस ब्रोकर्स' के रूप में काम कर रहे हैं, रैनसमवेयर सहयोगियों के साथ मिलकर काम कर रहे हैं, और विनाशकारी हमलों को जबरन वसूली (extortion) अभियान के रूप में छिपाने के लिए 'स्यूडो-रैनसमवेयर' (छद्म-रैनसमवेयर) का इस्तेमाल करते हैं।

इसका एक प्रमुख उदाहरण 'Pay2Key' है, जो ईरान से जुड़ा एक रैनसमवेयर ऑपरेशन(अभियान) है। यह गुमनाम I2P नेटवर्क पर संचालित होने वाले एक पेशेवर RaaS (रैनसमवेयर-एज-ए-सर्विस) प्लेटफॉर्म के रूप में फिर से उभरा है। यह सक्रिय रूप से रूसी साइबर अपराध मंचों से सहयोगियों की भर्ती कर रहा है और अमेरिकी व इजरायली लक्ष्यों पर हमलों के लिए उनके मुनाफे का हिस्सा 70% से बढ़ाकर 80% करने की पेशकश कर रहा है। यह मॉडल पीड़ित संगठनों के लिए अनुपालन संबंधी एक बड़ा जोखिम पैदा करता है:एक सामान्य फिरौती की मांग के रूप में दिखने वाली रकम का भुगतान करने से, अनजाने में ओएफएसी (OFAC) द्वारा प्रतिबंधित ईरानी संस्थाओं तक पैसा पहुँच सकता है, जिससे कंपनियों को गंभीर कानूनी और वित्तीय दंडों का सामना करना पड़ सकता है।

केला(KELA) साइबर इंटेलिजेंस सेंटर ने सोमवार को अपनी पोस्ट में बताया कि सबसे ज़्यादा चिंताजनक घटनाक्रमों में से एक, ईरान की सरकार से जुड़े तत्वों और व्यापक रैंसमवेयर पारिस्थितिकी तंत्र के बीच बढ़ता सहयोग है।

अगस्त 2024 में फेडरल ब्यूरो ऑफ इन्वेस्टिगेशन (FBI), साइबर सिक्योरिटी एंड इंफ्रास्ट्रक्चर सिक्योरिटी एजेंसी (CISA), और डिपार्टमेंट ऑफ डिफेंस साइबर क्राइम सेंटर की एक संयुक्त एडवाइजरी ने 'पायनियर किटन' (Pioneer Kitten) जैसे समूहों पर प्रकाश डाला, जिन्हें UNC757 या

फॉक्स किटन के रूप में भी जाना जाता है। अपना खुद का रैनसमवेयर इस्तेमाल करने के बजाय, ये तत्व शुरुआती पहुंच(initial access) प्राप्त करने के लिए वीपीएन (VPN) और फायरवॉल सहित इंटरनेट-फेसिंग एज डिवाइसेज की कमजोरियों का फायदा उठाने पर ध्यान केंद्रित करते हैं। एक बार अंदर पहुँचने के बाद, वे 'NoEscape', 'RansomHouse' और 'ALPHV/BlackCat' जैसे रैनसमवेयर सहयोगियों के साथ सीधे सहयोग करते हैं, और फिरौती की रकम में हिस्सेदारी के बदले में हैक किए गए नेटवर्क उन्हें सौंप देते हैं।

(B) एलपीजी (LPG) बुकिंग घोटाले का अलर्ट: आपूर्ति की चिंताओं के बीच साइबर अपराधी उठा रहे डर का फायदा, I4C ने जारी की चेतावनी

ईरान, इज़राइल और संयुक्त राज्य अमेरिका के बीच मध्य पूर्व में बढ़ते तनाव के बीच, एलपीजी आपूर्ति बाधित होने की चिंताएं अब भारत में उपभोक्ताओं को भी प्रभावित करने लगी हैं।जैसे-जैसे घबराहट के कारण मांग बढ़ रही है, साइबर अपराधी इस स्थिति का फायदा उठाकर फर्जी एलपीजी बुकिंग घोटाले(स्कैम) चला रहे हैं, जिनका निशाना अनजान यूज़र्स बन रहे हैं।

एलपीजी बुकिंग घोटाला क्या है ?

विशेषज्ञ एलपीजी बुकिंग घोटाले को एक तरह की साइबर धोखाधड़ी बताते हैं, जिसमें जालसाज़ गैस एजेंसियों या सर्विस प्रोवाइडर्स का रूप धर लेते हैं। पीड़ितों से नकली वेबसाइटों, कॉल्स या संदेशों के माध्यम से संपर्क किया जाता है और उनसे ओटीपी, बैंक विवरणया भुगतान क्रेडेंशियल्स जैसीसंवेदनशील जानकारी साझा करने के लिए कहा जाता है। एक बार ये विवरण साझा हो जाने के बाद, जालसाज़ पीड़ितों के बैंक खातों तक पहुँच प्राप्त कर लेते हैं और अक्सर कुछ ही मिनटों के भीतर धनराशि निकाल लेते हैं।

जालसाज पीड़ितों को कैसे फंसाते हैं ?

साइबर अपराधी जल्दबाजी और डर का फायदा उठाते हैं, खासकर ऐसे समय में जब आपूर्ति बाधित होने की खबरें आ रही हों। गैस एजेंसियों के अधिकारी या प्रतिनिधि बनकर,वे तुरंत या प्राथमिकता के आधार पर एलपीजीबुकिंग की पेशकश करते हैं।

पीड़ितों को जल्दबाजी में निर्णय लेने के लिए ललचाया जाता है और उन्हें फर्जी प्लेटफॉर्म पर भेज दिया जाता है या संदिग्ध लिंक के माध्यम से भुगतान करने के लिए कहा जाता है। कई मामलों में, उनसे ओटीपी के माध्यम से बुकिंग सत्यापित करने के लिए भी कहा जाता है, जिसका उपयोग धोखाधड़ी वाले लेनदेन को पूरा करने के लिए किया जाता है।

घबराहट और जल्दबाजी बनी धोखाधड़ी की वजह

एलपीजी की उपलब्धता को लेकर मौजूदा अनिश्चितताभरे माहौल ने लोगों को और भी ज्यादा असुरक्षित बना दिया है। देरी या कमी कीआशंका से चिंतित होकर, कई उपभोक्ता जल्दबाजी में सिलेंडर बुक कररहे हैं, और अक्सर वे स्रोत की प्रमाणिकता की जाँच नहीं करते।

यह जल्दबाजी जालसाजों के लिए एक उचित अवसर पैदा करती है, जो तकनीकी छलकी बजाय मनोवैज्ञानिक दबाव पर भरोसा करते हैं। कानून प्रवर्तन अधिकारियों सहित साइबर विशेषज्ञों ने नागरिकों से सतर्क रहने और किसी भी अज्ञात कॉलर या वेबसाइट के साथ व्यक्तिगत या बैंकिंग विवरण साझा न करने का आग्रह किया है।

वे इस बात पर जोर देते हैं कि असली एलपीजी प्रदाता कभी भी बुकिंग सेवाओं के लिए ओटीपी (OTP) या गोपनीय वित्तीय जानकारी नहीं मांगते हैं। इस तरह के किसी भी अनुरोध को खतरे का संकेत (red flag) माना जाना चाहिए।

प्राधिकारियों ने उपयोगकर्ताओं को सलाह दी है कि वे एलपीजी बुकिंग के लिए केवल आधिकारिक ऐप, वेबसाइट या पंजीकृत वितरकों पर ही भरोसा करें। किसी भी संदिग्ध गतिविधि के मामले में, नागरिकों को तुरंत राष्ट्रीय साइबर अपराध हेल्पलाइन या ऑनलाइन पोर्टल पर मामले की रिपोर्ट करनी चाहिए। इस तरह के घोटालों में वृद्धि एक बड़े पैटर्न को दर्शाती है, जहाँ साइबर अपराधी लक्षित धोखाधड़ी अभियान चलाने के लिए दुनिया के वास्तविक संकटों का फायदा उठाते हैं। ऐसे बढ़ते खतरों से बचने के लिए जागरूकता और सतर्कता ही सबसे प्रभावी बचाव है।

कानून प्रवर्तन अधिकारियों सहित साइबर विशेषज्ञों ने नागरिकों से सतर्क रहने और किसी भी अज्ञात कॉलर या वेबसाइट के साथ व्यक्तिगत या बैंकिंग विवरण साझा न करने का आग्रह किया है। वे इस बात पर जोर देते हैं कि असली एलपीजी प्रदाता कभी भी बुकिंग सेवाओं के लिए ओटीपी (OTP) या गोपनीय वित्तीय जानकारी नहीं मांगते हैं। इस तरह के किसी भी अनुरोध को खतरे का संकेत (red flag) माना जाना चाहिए।

प्राधिकारियों ने उपयोगकर्ताओं को सलाह दी है कि वे एलपीजी बुकिंग के लिए केवल आधिकारिक ऐप, वेबसाइट या पंजीकृत वितरकों पर ही भरोसा करें। किसी भी संदिग्ध गतिविधि के मामले में, नागरिकों को तुरंत राष्ट्रीय साइबर अपराध हेल्पलाइन या ऑनलाइन पोर्टल पर मामले की रिपोर्ट करनी चाहिए।

इस तरह के घोटालों में वृद्धि एक बड़े पैटर्न को दर्शाती है, जहाँ साइबर अपराधी लक्षित धोखाधड़ी अभियान चलाने के लिए दुनिया के वास्तविक संकटों का फायदा उठाते हैं। ऐसे बढ़ते खतरों से बचने के लिए जागरूकता और सतर्कता ही सबसे प्रभावी बचाव है।

3. इस महीने के लिए सुझाव

भारत में अप्रैल का महीना साइबर धोखाधड़ी के लिए उच्च जोखिम वाला महीना है—टैक्स फाइलिंग, नए वित्तीय वर्ष की गतिविधियाँ और **चारधाम यात्रा 2026** जैसे आयोजन ऐसी जल्दबाजी की स्थिति पैदा करते हैं जिसका फायदा धोखेबाज उठाते हैं। यहाँ अप्रैल के लिए एक व्यावहारिक' **साइबर सुरक्षा: क्या करें और क्या न करें'** मार्गदर्शिका दी गई है :

☑ क्या करें (अप्रैल साइबर सुरक्षा टिप्स)

✔ टैक्स संबंधी संचार का सत्यापन करें

• केवल भारत के आयकर विभाग के आधिकारिक पोर्टल का उपयोग करें।

• रिफंड या नोटिस का दावा करने वाले ईमेल/एसएमएस (SMS) की दोबारा जाँच करें।

✔ वित्तीय खातों को सुरक्षित रखें

• टू-फैक्टर ऑथेंटिकेशन (2FA) को सक्षम बनाएं।

• बैंक और यूपीआई (UPI) लेनदेन की नियमित जाँच करें।

✔ डिवाइस और ऐप्स को अपडेट करें

• फोन/लैपटॉप पर नवीनतम सुरक्षा पैच को इंस्टॉल करें।

• बैंकिंग और भुगतान ऐप्स को अपडेट रखें।

✔ आधिकारिक बुकिंग प्लेटफॉर्म का उपयोग करें

• यात्रा/तीर्थयात्रा (जैसे चारधाम) के लिए केवल सरकार द्वारा अधिकृत वेबसाइटों पर ही भरोसा करें।

✔ नौकरी या ऑफर संदेशों का सत्यापन करें

• अप्रैल में कई फर्जी "नए वित्तीय वर्ष की भर्ती" के घोटाले चलते हैं।

• कंपनी के विवरण (जैसे इंफोसिस, टीसीएस) को क्रॉस-चेक करें।

✔ महत्वपूर्ण डेटा का बैकअप लें

• महत्वपूर्ण दस्तावेजों की प्रतियां सुरक्षित रूप से (क्लाउड या एक्सटर्नल ड्राइव पर) स्टोर करें।

✕ क्या न करें (इन सामान्य गलतियों से बचें)

✕ रिफंड/ऑफर लिंक पर आँख बंद करके क्लिक न करें

• "आयकर रिफंड" या "वित्तीय बोनस" के लिंक अक्सर फ़िशिंग (phishing) होते हैं।

✕ ओटीपी (OTP) या बैंकिंग विवरण साझा न करें

• कोई भी वैध प्राधिकारी कभी ओटीपी नहीं मांगता।

✕ सोशल मीडिया विज्ञापनों पर भरोसा न करें

• अप्रैल में फर्जी यात्रा सौदे, नौकरी के प्रस्ताव और निवेश योजनाओं में वृद्धि होती है।

✕ अज्ञात ऐप्स/एपीके (APK) डाउनलोड न करें

• विशेष रूप से वे जो "तेज़ बुकिंग" या "आसान टैक्स फाइलिंग" का दावा करते हैं।

✕ पुराने पासवर्ड का पुनः उपयोग न करें

• बैंकिंग, ईमेल और सोशल मीडिया के लिए एक ही पासवर्ड रखने से बचें।

✕ छोटे संदिग्ध लेन-देन को नज़रअंदाज न करें

• ₹1 की कटौती भी धोखाधड़ी की टेस्टिंग का संकेत हो सकती है।

⚠ **अप्रैल** के खास **साइबर खतरे**

• टैक्स फ़िशिंग घोटाले (फर्जी रिफंड/पेनल्टी)
• तीर्थयात्रा बुकिंग धोखाधड़ी (चारधाम इत्यादि)
• नौकरी के घोटाले (नए वित्तीय वर्ष की भर्ती)
• यूपीआई से राशि प्राप्त करने के अनुरोध(Collect Request) के घोटाले
• फर्जी निवेश योजनाएं ("नए साल में उच्च रिटर्न")

🛡 **त्वरित सुरक्षा फॉर्मूला**

☞ **सोचें → सत्यापित करें → कार्रवाई करें**

यदि कुछ भी **जल्दबाजी वाला + वित्तीय + अप्रत्याशित** लगे → तो रुकें और जाँच करें।

4. सूचना प्रौद्योगिकी निदेशालय में नए विकास

1.) पीपीएमएस

- व्यक्तिगत उपलब्धि / कौशल प्रविष्टि आदेश
- वेतन निर्धारण आदेश
- डीसीपीएस कटौती आदेश

श्री जी.पी. सिंह (आईपीएस), महानिदेशक, के0रि.0पु0बल ने ग्रुप केन्द्र झरोदा कलां में दिब्यागं स्कूल (सक्षम) का अनावरण करने के दौरान ।

श्री जी.पी. सिंह (आईपीएस), महानिदेशक, के0रि.0पु0बल ने ग्रुप केन्द्र झरोदा कलां में दिब्यागं बच्चों एवम् उनके अभिभावकों के साथ बातचित करते हुए ।

श्री जी.पी. सिंह (आईपीएस), महानिदेशक, के0रि.0पु0बल ने वीरता पदक विजेता अलंकरण समारोह शौर्य दिवस–2026 के अवसर पर ।