

केंद्रीय रिजर्व पुलिस बल

मार्च, 2025

साइबर बाइट

एनपीसीआई ने कॉल मर्जिंग
घोटाले के खिलाफ
उपयोगकर्ताओं को चेतावनी
दी

कॉल मर्जर धोखाधड़ी के
खिलाफ कैसे प्रतिक्रिया करें



गूगल प्ले पर पाया गया “ स्पाईलेंड ”
एंड्रॉइड मेलवेयर वित्तीय साइबर
अपराध और जबरन वसूली को सक्षम
बनाता है

1. साइबर गीक समाचार

क) एनपीसीआई ने कॉल मर्जिंग घोटाले के खिलाफ उपयोगकर्ताओं को चेतावनी दी ।



भारतीय प्राधिकारियों ने लोगों से पैसे चुराने के लिए इस्तेमाल किए जा रहे एक नए घोटाले के बारे में चेतावनी जारी की है । लोगों को ठगने के इस नवीनतम तरीके में, धोखेबाज कॉल को मर्ज करके और उनके वन-टाइम पासवर्ड (ओटीपी) तक पहुँच करके उपयोगकर्ताओं को धोखा देते हैं । इससे धोखेबाज अनधिकृत लेन-देन करने और पैसे चुराने में सफल हो जाते हैं।

जालसाज पीड़ित को कॉल करके दावा करता है कि उसे उनका नंबर उसके दोस्त के माध्यम से मिला है । फिर जालसाज पीड़ित से अपने "दोस्त" को जोड़ने का अनुरोध करता है, जो किसी दूसरे नंबर से कॉल कर रहा है। एक बार कॉल मर्ज हो जाने पर, यह अनजान उपयोगकर्ता को अनजाने में उनके बैंक से एक वास्तविक ओटीपी सत्यापन कॉल से जोड़ देता है।

जालसाज यूजर को धोखा देकर अपना ओटीपी बताने के लिए बोलते हैं। ओटीपी प्राप्त होने के बाद, लेन-देन पूरा हो जाता है और व्यक्ति को वित्तीय नुकसान होता है।

ख) मोबाइल नंबर, आईपी, आईएमईआई और एसएमएस हेडर से छेड़छाड़ या स्फूफिंग एक दण्डनीय अपराध है: दूरसंचार विभाग ।



दूरसंचार विभाग
Department of
Telecommunications



दूरसंचार विभाग (DoT) ने मोबाइल नंबर, आईपी पते, आईएमईआई नंबर और एसएमएस हेडर से छेड़छाड़ या स्फूफिंग सहित दूरसंचा संसाधनों के दुरुपयोग के खिलाफ सख्त चेतावनी जारी की है। DoT ने इस बात पर जोर दिया कि इस प्रकार की गतिविधियाँ दूरसंचार अधिनियम, 2023 का उल्लंघन करती हैं, जिसमें अपराधियों के लिए कठोर दंड का प्रावधान होता है। जालसाज साइबर अपराध और वित्तीय धोखाधड़ी के लिए दूरसंचार संसाधनों का तेजी से दोहन कर रहे हैं। बदमाशों को अवैध रूप से प्राप्त सब्सक्राइबर आईडेंटिटी मॉड्यूल (सिम) कार्ड और एसएमएस हेडर का उपयोग करके धोखाधड़ी वाले संदेश भेजने के लिए पाया गया है। कुछ व्यक्ति अपने नाम से सिम कार्ड भी खरीदते हैं

और उन्हें दूसरों को दे देते हैं, इससे अक्सर अनजाने में साइबर अपराधियों की सहायता करते हैं।

इसके अलावा, ऐसे मामले भी सामने आए हैं, जहां नकली दस्तावेजों, धोखाधड़ी या गलत पहचान का उपयोग करके सिम कार्ड प्राप्त किए गए हैं। कुछ मामलों में, पॉइंट्स ऑफ सेल (PoS) - सिम कार्ड जारी करने के लिए जिम्मेदार संस्थाएं-इस तरह की अवैध खरीद को सुविधाजनक बनाने में मिलीभगत रही हैं, जिससे अपराध को प्रभावी रूप से बढ़ावा मिला है।

साइबर अपराधियों को मोबाइल एप्लिकेशन और अन्य माध्यमों का उपयोग करके दूरसंचार पहचानकर्ताओं, जैसे कॉलिंग लाइन आइडेंटिटी (सीएलआई) - जिसे आमतौर पर फोन नंबर कहा जाता है - को संशोधित करते हुए भी पाया गया है।

2. साइबर धोखाधड़ी

क) नया साइबर धोखाधड़ी "पिग बूचरिंग" (Pig Butchering) बेरोजगार युवाओं, छात्रों, गृहिणियों को निशाना बनाता है :

SR CITIZENS, HOUSEWIVES TARGET

● 89,783 cyber crime complaints received from across Telangana in 2023

● FedEx courier frauds among top five MOs used by cyber crooks

● People lost between rs50k and ₹2cr on average in FedEx courier frauds



● 30% of all cyber crimes are courier frauds targeting retired employees & housewives, says police

सरकार ने पिग बूचरिंग नामक एक नई साइबर धोखाधड़ी योजना के बारे में चेतावनी जारी की है, जो बेरोजगार युवाओं, छात्रों और कमजोर व्यक्तियों को निशाना बनाती है। अधिकारियों ने बुधवार को बताया कि पीड़ित न केवल पैसे खो देते हैं, बल्कि उन्हें साइबर गुलामी के लिए भी मजबूर होना पड़ता है।

उन्होंने बताया कि पिछले महीने केंद्रीय गृह मंत्रालय द्वारा प्रकाशित नवीनतम वार्षिक रिपोर्ट में भी इस बात को उजागर किया गया है। उन्होंने बताया कि कुछ जालसाज व्यक्तियों और संस्थाओं को इन अपराधों को शुरू करने के लिए गूगल सेवा प्लेटफार्मों का उपयोग करते हुए देखा गया है।

सूत्रों के अनुसार, ऐसा माना जाता है कि इस तरह की धोखाधड़ी पहली बार वर्ष 2016 में चीन में शुरू हुई थी। इस तरह के धोखाधड़ी मॉड्यूल में, बदमाश भोले-भाले व्यक्तियों को निशाना बनाते हैं, जिनके साथ वे पहले समय के साथ विश्वास कायम करते हैं और फिर एकत्र किए गए धन को चुराने से पहले उन्हें क्रिप्टोकॉर्सेसी या किसी अन्य आकर्षक योजना में निवेश करने के लिए राजी करते हैं।

ख) गूगल प्ले पर पाया गया “ स्पाईलैंड ” एंड्रॉइड मैलवेयर वित्तीय साइबर अपराध और जबरन वसूली को सक्षम बनाता है:



CYFIRMA के शोधकर्ताओं ने स्पाईलेंड नामक एक एंड्रॉइड मैलवेयर की खोज की है, जिसे गूगल प्ले के माध्यम से वित्तीय सरलीकरण के नाम से वितरित किया गया था। यह मैलवेयर अनधिकृत ऋण ऐप के माध्यम से भारतीय उपयोगकर्ताओं को निशाना बनाता है, जिससे अनूचित ऋण, ब्लैकमेल और जबरन वसूली संभव हो पाती है।

यह ऐप एक वित्तीय उपकरण के रूप में प्रस्तुत होता है, यह उपयोगकर्ताओं को आसान ऋण वादों के साथ लुभाता है लेकिन संपर्कों, कॉल लॉग, एसएमएस, फ़ोटो और लोकेशन तक पहुँचने के लिए अत्यधिक अनुमतियाँ माँगता है। ऐप गूगल प्ले सुरक्षा को दरकिनार करते हुए, एपीके डाउनलोड के लिए उपयोगकर्ताओं को बाहरी लिंक पर पुनर्निर्देशित करता है। एक बार इंस्टॉल होने के बाद, यह फ़ोटो, वीडियो और संपर्कों तक पहुँचता है, संवेदनशील जानकारी चुराने के लिए क्लिपबोर्ड डेटा कैप्चर करता है।

3. इस माह की टिप

क) कॉल मर्जर धोखाधड़ी के खिलाफ कैसे प्रतिक्रिया करें।



कॉल मर्जर धोखाधड़ी (जिसे कॉल स्पूफिंग धोखाधड़ी भी कहा जाता है) तब होता है जब धोखेबाज़ अपने फ़ोन नंबर छिपाने के लिए सॉफ़्टवेयर या तकनीकों का उपयोग करते हैं, जिससे ऐसा लगता है कि वे किसी वैध या विश्वसनीय स्रोत से कॉल कर रहे हैं, जैसे कि बैंक, सरकारी एजेंसी या यहाँ तक कि कोई स्थानीय नंबर। अगर आपको संदेह है कि आप कॉल मर्जर धोखाधड़ी का शिकार हुए हैं, तो खुद को बचाने और प्रतिक्रिया देने के लिए यहाँ कुछ उपाय/स्टेपस दिए गए हैं:

1. अज्ञात कॉल का उत्तर न दें।

अगर आपको किसी अपरिचित नंबर से कॉल आती है, खासकर अगर वह अंतरराष्ट्रीय या संदिग्ध रूप से स्थानीय नंबर है, तो जवाब न दें। स्कैमर्स अक्सर अपना नंबर आपको परिचित दिखाने के लिए कॉल स्पूफिंग का इस्तेमाल करते हैं।

2. अगर आपको किसी स्कैमर्स का संदेह हो तो तुरंत फ़ोन काट दें।

यदि आप कॉल का उत्तर देते हैं और दूसरी तरफ़ से कोई व्यक्ति संदिग्ध लगता है या आपसे व्यक्तिगत जानकारी मांगता है, तो तुरंत फ़ोन काट दें। कॉल करने वाले व्यक्ति से बातचीत न करें।

3. व्यक्तिगत जानकारी साझा न करें।

स्कैमर्स आपसे सोशल सिक्क्योरिटी नंबर, अकाउंट डिटेल या पासवर्ड जैसी संवेदनशील जानकारी आपसे मांग सकते हैं। फ़ोन पर कभी भी निजी जानकारी साझा न करें, खासकर तब जब आपने कॉल शुरू नहीं की हो।

4. कॉल की वैधता सत्यापित करें।

अगर कॉल करने वाला व्यक्ति किसी वैध संगठन (जैसे कि आपका बैंक या कोई सरकारी एजेंसी) से होने का दावा करता है, तो फ़ोन काट दें और अनुरोध की पुष्टि करने के लिए उस संस्था के आधिकारिक नंबर पर कॉल करें। हमेशा आधिकारिक वेबसाइट या दस्तावेज़ों से विश्वसनीय संपर्क विवरण का उपयोग करें।

5. कॉल ब्लॉकिंग और स्क्रीनिंग ऐप्स का उपयोग करें

कई स्मार्टफोन और ऐप में बिल्ट-इन कॉल स्क्रीनिंग या ब्लॉकिंग फीचर होते हैं। संदिग्ध कॉल को ब्लॉक करने या

पहचानने के लिए डूकॉलर, **Hiya** या नोमोरबो जैसे थर्ड-पार्टी ऐप का इस्तेमाल करने पर विचार करें।

6. घोटाले की रिपोर्ट करें।

अपने फ़ोन आपूर्तिकर्ता को धोखाधड़ी की रिपोर्ट करें। कई सेवा आपूर्तिकर्ता धोखाधड़ी वाली कॉल को रोकने में मदद करने के लिए सुविधाएँ प्रदान करते हैं।

आप स्थानीय प्राधिकारियों या उपभोक्ता संरक्षण एजेंसियों को भी घोटाले की सूचना दे सकते हैं, जैसे:

- www.cybercrime.gov.in (NCRP portal)
- Cybercrime helpline number 1930
- <https://www.cert-in.org.in>

7. कॉलर आईडी सेवाओं का उपयोग करें ।

अपने फोन की कॉलर आईडी सेवाएं सक्रिय करें, या ऐसे ऐप्स का उपयोग करें जो संभावित रूप से दुर्भावनापूर्ण कॉल की पहचान कर सकें, ताकि आप बेहतर ढंग से पता लगा सकें कि कौन कॉल कर रहा है।

8. नंबर ब्लॉक करें ।

अगर आपको कोई स्कैम कॉल आती है, तो ज़्यादातर स्मार्टफ़ोन आपको कॉल लॉग से सीधे नंबर ब्लॉक करने की सुविधा देते हैं। हालाँकि, चूँकि स्कैमर्स हर बार अलग-अलग नंबर इस्तेमाल कर सकते हैं, इसलिए एक नंबर को

ब्लॉक करने से आगे की धोखाधड़ी को रोका नहीं जा सकता है।

9. दूसरों को शिक्षित करें ।

कॉल मर्जर स्कैम के बारे में जानकारी अपने दोस्तों और परिवार के साथ साझा करें, खास तौर पर उन लोगों के साथ जो ज़्यादा असुरक्षित हो सकते हैं, जैसे कि बुजुर्ग रिश्तेदार। इन स्कैम के प्रभाव को कम करने के लिए जागरूकता बहुत ज़रूरी है।

ख) खो गए फोन के डेटा की सुरक्षा और अनाधिकृत पहुंच को रोकने के लिए फोन को दूर से कैसे लॉक किया जा सकता है ।



इस बात पर निर्भर करता है कि आप किसका उपयोग कर रहे हैं एंड्रॉइड या आईफोन :

एंड्रॉइड फोन के लिए :

1. गूगल के फाइंड माई डिवाइस का उपयोग करें:

- वेब ब्राउज़र पर फाइंड माई डिवाइस पर जाएं।
- अपने खोए हुए फ़ोन से जुड़े गूगल खाते का उपयोग करके साइन इन करें.
- सूची से अपना खोया हुआ फ़ोन चुनें.

आपके पास कई विकल्प होंगे:

ध्वनि बजाएँ : यदि आपका फ़ोन पास में है, तो आप उसे ढूँढने में सहायता के लिए उसे बजा सकते हैं।

सुरक्षित डिवाइस (लॉक): अपने फ़ोन को लॉक करने के लिए यह विकल्प चुनें। आप डिवाइस को लॉक करने और दूसरों को इसे एक्सेस करने से रोकने के लिए नया पासवर्ड, पिन या पैटर्न सेट कर सकते हैं। आप लॉक स्क्रीन पर अपनी संपर्क जानकारी (जैसे फ़ोन नंबर या ईमेल) के साथ एक संदेश भी प्रदर्शित कर सकते हैं, ताकि अगर कोई इसे प्राप्त कर ले तो वह आपसे संपर्क कर सके।

डिवाइस मिटाएँ: अंतिम उपाय के रूप में, यदि आपको यकीन है कि आप अपना फ़ोन वापस नहीं पा सकते हैं, तो आप उसका सारा डेटा रिमोट तरीके से मिटा सकते हैं। हालाँकि, ऐसा केवल तभी किया जाना चाहिए जब डिवाइस को लॉक करना कोई विकल्प न हो और आप अपने डेटा की सुरक्षा करना चाहते हों।

विकल्प: सैमसंग के फाइंड माई मोबाइल (सैमसंग फोन) का उपयोग करें :

यदि आप सैमसंग फोन का उपयोग कर रहे हैं, तो आप फाइंड माई मोबाइल का भी उपयोग कर सकते हैं ।

अपने सैमसंग खाते से लॉग इन करें। अपना खोया हुआ डिवाइस चुनें और अपने फोन को दूर से सुरक्षित करने के लिए "लॉक" विकल्प चुनें।

आईफोन के लिए :

1. एप्पल के फाइंड माई आईफोन का उपयोग करें:

वेब ब्राउज़र पर iCloud.com खोलें या किसी अन्य Apple डिवाइस पर **Find My ऐप** का उपयोग करें।

अपने एप्पल आईडी से साइन इन करें।

डिवाइसों की सूची से अपना खोया हुआ iPhone चुनें। **मार्क ऐज़ लॉस्ट** चुनें। यह आपके फ़ोन को आपके मौजूदा पासकोड से लॉक कर देगा और एक कस्टम संदेश प्रदर्शित करेगा (यदि कोई इसे पा लेता है तो आपसे संपर्क करने के लिए आप अपनी संपर्क जानकारी दर्ज कर सकते हैं)। जब आप "मार्क ऐज़ लॉस्ट" को सक्रिय करेंगे तो Apple Pay भी अक्षम हो जाएगा।

ध्वनि बजाना : यदि आपका फोन आपके नजदीक है तो आप उससे ध्वनि बजा सकते हैं।

iPhone मिटाएँ : अगर आपको लगता है कि आप फ़ोन को वापस नहीं प्राप्त कर सकेंगे और अपने व्यक्तिगत डेटा की सुरक्षा करना चाहते हैं, तो आप "**Erase iPhone**" विकल्प चुन सकते हैं, जो आपके डिवाइस पर मौजूद सभी डेटा को दूर से मिटा देगा। ध्यान दें कि एक बार इसे मिटाने के बाद, आप फ़ोन को ट्रैक नहीं कर पाएँगे।

2. **एक्टिवेशन लॉक** : यदि आपने "फाइंड माई" सक्रिय किया है, तो एक्टिवेशन लॉक किसी को भी आपके iPhone का उपयोग करने से रोक देगा, भले ही वे इसे मिटा दें। डिवाइस को फिर से सक्रिय करने के लिए आपके Apple

आईडी और पासवर्ड की आवश्यकता होगी।

सामान्य सुझाव :

- **अपने मोबाइल कैरियर को रिपोर्ट करें** : आप अपने मोबाइल कैरियर को खोए हुए फ़ोन के बारे में सूचित कर सकते हैं। वे आपके मोबाइल नंबर के अनधिकृत उपयोग को रोकने के लिए आपके सिम कार्ड को निष्क्रिय कर सकते हैं और डिवाइस को ट्रैक करने में भी मदद कर सकते हैं।
- **पासवर्ड बदलें** : यदि आपको लगता है कि आपका फोन स्थायी रूप से खो गया है या उसमें संवेदनशील डेटा है, तो अपने महत्वपूर्ण खातों, जैसे कि आपके Google, Apple आईडी, ईमेल और बैंकिंग ऐप के पासवर्ड बदलें।
- **पुलिस में रिपोर्ट दर्ज कराएं** : चोरी होने की स्थिति में, फोन चोरी होने की रिपोर्ट पुलिस में दर्ज कराएं, खासकर यदि उसमें मूल्यवान या संवेदनशील जानकारी हो।

इन चरणों का पालन करके आप अपने खोए हुए फोन को लॉक कर सकते हैं और अपनी व्यक्तिगत जानकारी को दूर से सुरक्षित कर सकते हैं।



होली मिलन समारोह-२०२५



पुलवामा शहीदों को श्रद्धांजलि



३८वा राष्ट्रीय खेल-२०२५



महिला दिवस-२०२५



गोल्फ पदक विजेता



15 वीं AIPDM कमांडो टीम महानिदेशक के.रि.पु. बल के साथ