

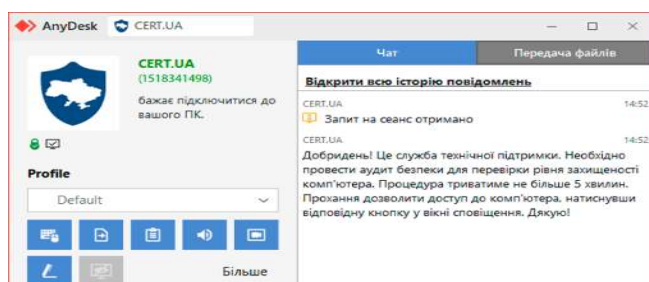
केंद्रीय रिज़र्व पुलिस बल

फरवरी, 2025

साइबर बाइट



1. साइबर गीक समाचार



क) (सीईआरटी-यूए) ने फ्रॉड सुरक्षा ऑडिट के लिए फर्जी एनीडेस्क अनुरोधों का उपयोग करने वाले साइबर स्कैम के बारे में चेतावनी दी है।

यूक्रेन की कंप्यूटर इमरजेंसी रिस्पांस टीम (सीईआरटी-यूए) अज्ञात थ्रेट एक्टर्स द्वारा एनीडेस्क कनेक्शन अनुरोध भेजकर साइबर सुरक्षा एजेंसी का प्रतिरूपण करने के चल रहे प्रयासों के बारे में चेतावनी दे रही है।

सीईआरटी-यूए ने कहा कि एनीडेस्क अनुरोध "सुरक्षा के स्तर" का आकलन करने के लिए ऑडिट आयोजित करने के लिए हैं, संगठनों को ऐसे सोशल इंजीनियरिंग प्रयासों पर नज़र रखने के लिए आगाह किया गया है जो उपयोगकर्ता के भरोसे का फ़ायदा उठाने की कोशिश करते हैं।

सीईआरटी-यूए ने कहा, "यह ध्यान रखना महत्वपूर्ण है कि सीईआरटी-यूए, कुछ परिस्थितियों में, एनीडेस्क जैसे रिमोट एक्सेस सॉफ़्टवेयर का उपयोग कर सकता है।" "हालांकि, आधिकारिक तौर पर स्वीकृत संचार चैनलों के माध्यम से साइबर रक्षा की वस्तुओं के मालिकों के साथ पूर्व समझौते के बाद ही ऐसी कार्रवाई की जाती है।"

■ हालांकि, इस हमले के सफल होने के लिए, यह आवश्यक है कि लक्षित कंप्यूटर पर एनीडेस्क रिमोट एक्सेस सॉफ़्टवेयर स्थापित और चालू हो।

इसके लिए हमलावर के पास लक्ष्य का एनीडेस्क आईडेंटिफायर होना भी आवश्यक है, जिसका

अर्थ है कि उन्हें पहले अन्य तरीकों से आईडेंटिफायर प्राप्त करना पड़ सकता है।

इन हमलों से उत्पन्न जोखिम को कम करने के लिए, यह आवश्यक है कि रिमोट एक्सेस प्रोग्राम को केवल उनके उपयोग की अवधि के लिए ही सक्षम किया जाए तथा रिमोट एक्सेस को आधिकारिक संचार चैनलों के माध्यम से समन्वित किया जाए।

ख) साइबर पुलिस ने जम्मू-कश्मीर में लोगों को घृणित सामग्री साझा करने के खिलाफ चेतावनी दी।

अपमानजनक टिप्पणियों के माध्यम से कथित रूप से सांप्रदायिक अशांति भड़काने के आरोप में पुलिस द्वारा छह लोगों को हिरासत में लेने के एक दिन बाद, साइबर पुलिस कश्मीर ने गुरुवार को लोगों को सोशल मीडिया पर घृणित



सामग्री साझा न करने की चेतावनी दी।

इसमें आगे कहा गया है कि कई उल्लंघनकर्ताओं को पहले ही साइबर पुलिस कश्मीर में बुलाया जा चुका है और सख्त कानूनी कार्रवाई की जा रही है। "हम उन सभी लोगों से आग्रह करते हैं जिन्होंने इस हानिकारक सामग्री को डाउनलोड या शेयर किया है, वे तुरंत ऐसा करना बंद कर दें।" नफ़रत फैलाने वाली सामग्री शेयर करना दंडनीय अपराध है। उल्लंघन करने वालों के खिलाफ कानूनी कार्रवाई की जाएगी।

"हम नजर बनाए हुए हैं"। साइबर पुलिस कश्मीर का संदेश भी प्रसारित किया गया था।

पुलिस ने कल छह लोगों को हिरासत में लिया था और उन पर अपमानजनक टिप्पणियों के माध्यम से अशांति भड़काने के आरोप में भारतीय नागरिक सुरक्षा संहिता (बीएनएसएस) की धारा 126 और 170 के तहत आरोप लगाए थे। बीएनएसएस की

दो धाराएं पुलिस को ऐसी स्थितियों में निवारक उपाय करने का अधिकार देती हैं जहां शांति भंग होने या सार्वजनिक शांति में व्यवधान उत्पन्न होने की विश्वसनीय सूचना हो।



2. साइबर फ्रॉड

क) यूपी पुलिस ने होटल में 7 घंटे तक डिजिटल गिरफ्तारी के तहत रखे गए डॉक्टर को बचाया।

बरेली में एक डॉक्टर खुद को साइबर जालसाजों के चंगुल में पाया, जिन्होंने उसे सात घंटे से ज्यादा समय तक धमकियों और छल-कपट के जाल में फंसाए रखा। यह घटना साइबर अपराध की बढ़ती जटिलता और त्वरित सोच और समय पर हस्तक्षेप के महत्व को उजागर करती है।

परेशानी तब शुरू हुई जब डॉक्टर को स्कैमर ने फोन किया और झूठा दावा किया कि उसका आधार कार्ड कई राज्यों में धोखाधड़ी की गतिविधियों में शामिल है। अधिकारियों के रूप में पेश आकर, धोखेबाजों ने उसे "डिजिटल गिरफ्तारी" की धमकी दी और चेतावनी दी कि अगर उसने फोन काट दिया, तो केंद्रीय जांच ब्यूरो (सीबीआई) के अधिकारी तुरंत उसके घर पर छापा मारेंगे। डर से कांपते हुए, डॉक्टर ने अपने परिवार को सचेत नहीं करने का फैसला किया। इसके बजाय, उसने एक नोट लिखा, जिसमें लिखा था, "मैं फंस गया हूँ," और चुपके से इसे अपने रिश्तेदारों को दे दिया।

मामले की गंभीरता को समझते हुए उनके परिवार ने तुरंत पुलिस से संपर्क किया। एसपी सिटी बरेली के मार्गदर्शन में पुलिस अधिकारियों ने तुरंत डॉक्टर के लोकेशन का पता लगाया और उसे एक

स्थानीय होटल में पाया। उन्हें पता चला कि उसे होटल के कमरे में अपने साथ संवेदनशील बैंकिंग दस्तावेज लाने के लिए मजबूर किया गया था।

स्कैमर्स ने लगातार फोन पर बातचीत करके उन्हें अपने नियंत्रण में रहने के लिए मजबूर किया था तथा उनसे महत्वपूर्ण वित्तीय जानकारी मांगी थी।

ख) एआई संचालित स्कैम: वॉयस क्लोनिंग और फर्जी कूरियर ने बेंगलुरु में साइबर अपराध को बढ़ावा दिया।

बेंगलुरु में 2021 से सितंबर 2024 के बीच साइबर अपराधों में 1,788 करोड़ रुपये का चोंका देने वाला नुकसान हुआ है, जो इस अवधि के दौरान ठगे गए कुल 2,270 करोड़ रुपये का 78.7% है। पुलिस के आंकड़ों से पता चलता है कि ये नुकसान छह प्रमुख धोखाधड़ी श्रेणियों में केंद्रित थे, जिसमें स्कैमर्स अपनी योजनाओं को बढ़ाने के लिए आर्टिफिशियल इंटेलिजेंस (एआई) का तेजी से लाभ उठा रहे थे।

जांचकर्ता चोरी की गई धनराशि का केवल 20% ही बरामद करने में सफल रहे हैं, जिससे अधिकांश पीड़ितों को कोई राहत नहीं मिल पाई है। सबसे अधिक नुकसान निवेश धोखाधड़ी के कारण हुआ, जो 1,187.2 करोड़ रुपये था, इसके बाद नौकरी धोखाधड़ी (601.23 करोड़ रुपये), कूरियर स्कैम (165.57 करोड़ रुपये), डेबिट या क्रेडिट कार्ड स्कैम (116 करोड़ रुपये), फिशिंग (96.98 करोड़ रुपये) और ऋण ऐप धोखाधड़ी (32.25 करोड़ रुपये) का स्थान रहा।

एक वरिष्ठ पुलिस अधिकारी ने स्कैम की देरी से रिपोर्टिंग और बैंकों की ओर से सुस्त प्रतिक्रिया को रिकवरी प्रयासों में बाधा डालने वाले महत्वपूर्ण कारकों के रूप में पहचाना। अगस्त तक, बैंकों-राष्ट्रीयकृत बैंकों सहित- ने साइबर धोखाधड़ी से संबंधित खाता विवरण के लिए जांचकर्ताओं के अनुरोधों का जवाब देने में औसतन आठ दिन लगाए। अधिकारी ने बताया, "पीड़ित शायद ही कभी महत्वपूर्ण गोल्डन ऑवर के भीतर धोखाधड़ी की रिपोर्ट करते हैं, जो चोरी की गई धनराशि को फ्रीज करने के लिए महत्वपूर्ण है। बैंकों की देरी से प्रतिक्रिया के साथ, पैसे की रिकवरी लगभग असंभव हो जाती है।"

3. इस माह के टिप

क) नकली और असली में अंतर कैसे करें।



1. चेहरे और भावों का विश्लेषण करें।

- चेहरे की अप्राकृतिक हरकतें:- डीपफेक वीडियो में अक्सर चेहरे के प्राकृतिक भावों की नकल करने में कठिनाई होती है। अप्राकृतिक पलकें झपकाना (या तो बहुत अधिक या पर्याप्त नहीं) या चेहरे की मांसपेशियों की गतिविधियों की कमी पर ध्यान दें।
- लिप सिंकिंग:- कुछ नकली वीडियो में, होंठ ऑडियो के साथ पूरी तरह से सिंक नहीं हो सकते हैं, विशेष रूप से जटिल वाक्यों या तेज़ बोलने के दौरान।

2. दृश्य-श्रव्य विसंगतियों को देखें:-

- ऑडियो गुणवत्ता:- नकली वीडियो में ऑडियो ऐसा हो सकता है जो दृश्य वातावरण से मेल नहीं खाता, जैसे स्वर, वॉल्यूम या पृष्ठभूमि शोर में अचानक परिवर्तन।
- पृष्ठभूमि विसंगतियां:- पृष्ठभूमि पर ध्यान दें और देखें कि वह विषय के साथ किस प्रकार से अंतःक्रिया करती है। यदि छाया, प्रतिबिंब या पृष्ठभूमि की वस्तुएं अस्वाभाविक रूप से गति करती प्रतीत होती हैं, तो यह हेरफेर का संकेत हो सकता है।

3. वीडियो विरूपण की जाँच करें:-

- धुंधलापन या गड़बड़ियाँ:- डीपफेक या संपादित वीडियो में गड़बड़ियाँ, विकृतियाँ या धुंधले धब्बे हो सकते हैं, खासकर बालों या चश्मे जैसे किनारों के आसपास।
- त्वचा की बनावट से संबंधित समस्याएं:- नकली वीडियो अक्सर त्वचा के छिद्रों या सूक्ष्म प्रकाश भिन्नताओं जैसे सूक्ष्म विवरणों को दोहराने में विफल होते हैं, विशेष रूप से कम रोशनी की स्थिति में।

4. प्रकाश और छाया: -

- असंगत चमक:- व्यक्ति के चेहरे या शरीर पर अप्राकृतिक चमक की जांच करें। यदि चमक वातावरण से मेल नहीं खाती है या अचानक बदल जाती है, तो यह छेड़छाड़ का संकेत हो सकता है।
- छाया और प्रतिबिंब:- जाँच करें कि छाया और प्रतिबिंब प्रकाश स्रोत और व्यक्ति की गति से मेल खाते हैं या नहीं।

5. फ्रेम दर फ्रेम विश्लेषण:-

- गति अनियमितताएं: - अनियमितताओं को पकड़ने के लिए वीडियो को फ्रेम दर फ्रेम तोड़ें। नकली वीडियो में फ्रेम के बीच अवास्तविक संक्रमण, झटकेदार गति या विकृतियाँ हो सकती हैं जो वास्तविक समय प्लेबैक में कम दिखती हैं।

6. डीपफेक डिटेक्शन टूल का उपयोग करें

- छेड़छाड़ के संकेतों के लिए वीडियो का विश्लेषण करने के लिए ऑनलाइन उपकरण और सॉफ्टवेयर बनाए गए हैं। इनमें से कुछ उपकरण एआई का उपयोग करते हैं जो गहरे नकली कलाकृतियों का पता लगाते हैं जो मानव आंखों के लिए अदृश्य हो सकते हैं।

7. मेटाडेटा की जांच करें:-

- **फाईल मेटाडेटा:-** संपादन के किसी भी संकेत के लिए वीडियो फ़ाइल के मेटाडेटा का निरीक्षण करें। मेटाडेटा असामान्य संपीड़न विधियों या वीडियो को संपादित करने के लिए उपयोग किए गए सॉफ़्टवेयर जैसी विसंगतियों को प्रकट कर सकता है।

- **सोर्स सत्यापन:-** हमेशा वीडियो के स्रोत की पुष्टि करें। असत्यापित या संदिग्ध स्रोतों से आने वाले वीडियो के नकली होने की संभावना अधिक होती है

8. रिवर्स वीडियो सर्च का उपयोग करें:-

- रिवर्स इमेज सर्च के समान, आप रिवर्स वीडियो सर्च का उपयोग करके देख सकते हैं कि क्या वीडियो कहीं और पोस्ट किया गया है, विशेष रूप से किसी अलग संदर्भ में या अलग ऑडियो के साथ।

9. अपने अंतर्ज्ञान पर भरोसा करें:-

- अगर कोई बात सच होने के लिए बहुत अच्छी (या बुरी) लगती है या अजीब तरह से सनसनीखेज लगती है, तो इसकी आगे जांच करना उचित है। नकली वीडियो अक्सर दर्शकों को प्रभावित करने के लिए भावनात्मक प्रतिक्रियाओं का इस्तेमाल करते हैं।

इन तकनीकों को मिलाकर और असत्यापित स्रोतों के प्रति संदेहपूर्ण रहकर, आप नकली और वास्तविक वीडियो के बीच बेहतर अंतर कर सकते हैं।

ख) डेटा की सुरक्षा और अनधिकृत पहुंच को रोकने के लिए खोए हुए फोन को कैसे दूरस्थ रूप से लॉक किया जा सकता है।



यह इस बात पर निर्भर करता है कि आप android या iphone का उपयोग कर रहे हैं।

एन्ड्राइड फोन के लिए।

1. गूगल की फ्वाइंड माई डिवाइस का उपयोग करें:-

- वेब ब्राउज़र पर फ्वाइंड माई डिवाइस पर जाएँ।
- अपने खोए हुए फ़ोन से जुड़े गूगल खाते का उपयोग करके साइन इन करें।
- साइन इन करने के बाद, आपको अपने खाते से संबद्ध उपकरणों की एक सूची दिखाई देगी। सूची से अपना खोया हुआ फ़ोन चुनें।

2. आपके पास कई विकल्प हैं ।

प्ले साउंड:-यदि आपका फोन नजदीक है, तो आप उसे ढूँढने में मदद के लिए उसे रिंग कर सकते हैं।

सुरक्षित डिवाइस (लॉक) :- अपने फोन को लॉक करने के लिए इस विकल्प को चुनें। आप डिवाइस को लॉक करने और दूसरों को उस तक पहुंचने से रोकने के लिए एक 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, यदि कोई इसे पा लेता है।

इरेज डिवाइस:- अंतिम उपाय के रूप में, यदि आप सुनिश्चित हैं कि आप अपना फ़ोन पुनर्प्राप्त नहीं कर सकते हैं, तो आप इसके सभी डेटा को दूरस्थ रूप से मिटा सकते हैं। हालाँकि यह केवल तभी किया जाना

चाहिए जब डिवाइस को लॉक करना एक विकल्प नहीं है और आप अपने डेटा की सुरक्षा करना चाहते हैं।

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

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

अपने सैमसंग अकाउंट के साथ लॉगिन करें।

अपनी खो गई डिवाइस को सेलेक्ट करें और अपने फोन को रिमोटली सुरक्षित करने के लिए 'लॉक' विकल्प का चयन करें।

आईफोन के लिए:-

1. एप्पल के फाइंड माय आईफोन का उपयोग:-वेब ब्राउज़र पर icloud.com खोलें या किसी अन्य ऐप्पल डिवाइस पर फाइंड माई ऐप का उपयोग करें।

अपनी ऐप्पल आईडी से लॉगिन करें।

उपकरणों की सूची से अपना खोया हुआ आईफोन चुनें। खोये हुए के रूप में चिह्नित करें। यह आपके फोन को आपके मौजूदा पासवर्ड से लॉक कर देगा और एक कस्टम संदेश प्रदर्शित करेगा (यदि कोई इसे पा लेता है तो आप अपनी संपर्क जानकारी दर्ज कर सकते हैं)। जब आप "खोये हुए के रूप में चिह्नित करें" सक्षम करते हैं तो ऐप्पल पे भी अक्षम हो जाएगा।

प्ले साउंड- यदि फोन पास में है तो आप उससे ध्वनि बजा सकते हैं।

इरेज आईफोन:- अगर आपको लगता है कि आप फोन को रिकवर नहीं कर पाएंगे और अपने निजी डेटा को सुरक्षित रखना चाहते हैं, तो आप "इरेज आईफोन" विकल्प चुन सकते हैं, जो आपके डिवाइस पर मौजूद सभी डेटा को रिमोट तरीके से मिटा देगा। ध्यान दें कि

एक बार इसे मिटाने के बाद, आप फोन को ट्रैक नहीं कर पाएंगे।

2.लॉक एक्टिवेशन:- यदि आपने "फाइंड माई" सक्षम किया है, तो सक्रियण लॉक किसी को भी आपके आईफोन का उपयोग करने से रोक देगा, भले ही वे इसे मिटा दें। डिवाइस को पुनः सक्रिय करने के लिए आपके ऐप्पल आईडी और पासवर्ड की आवश्यकता होगी।

सामान्य टिप:-

- **अपने कैरियर को रिपोर्ट करें:-** आप अपने मोबाइल कैरियर को खोए हुए फोन 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:-** अगर आपको लगता है कि आपका फोन हमेशा के लिए खो गया है या उसमें संवेदनशील डेटा है, तो अपने महत्वपूर्ण खातों के पासवर्ड बदलें, जैसे कि आपकी गूगल, ऐप्पल आईडी, ईमेल और बैंकिंग ऐप।
- **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 उपायों का पालन करके, आप अपने खोए हुए फोन को लॉक कर सकते हैं और अपनी व्यक्तिगत जानकारी को दूरस्थ रूप से सुरक्षित कर सकते हैं।

