साइबर जागरुक नागरिक बनें

साइबर नेत्र

साइबर घटनाओं और निवारक उपायों पर कॉमिक बुकलेट

सीआईएसओ कार्यालय द्वारा

यूको बैंक UCO BANK

(भारत सरकार का उपक्रम) (A Govt. of India Undertaking)

सम्मान आपके विश्वास का Honours Your Trust

विज़न

सूचना की सुरक्षा हेतु बैंक के लिए
एक सुरक्षित साइबर स्पेस बनाना

Vision

To build a secure and resilient cyber space
for the Bank to protect information

मिशन

बैंक की बुनियादी संरचना, व्यक्ति, प्रक्रिया और प्रौद्योगिकी
के सम्मिलन से साइबर स्पेस में सूचना तथा बुनियादी संरचना
की सुरक्षा करना, साइबर के खतरों को रोकना एवं अनुक्रिया करना

Mission

To protect information and information infrastructure in cyber space, build capability to prevent and respond to cyber threat, reduce vulnerabilities and minimize damage from cyber incidents through a combination of the Bank infrastructure, people, process and technology

विषय-सूची

यूको बैंक
UCO BANK

क्रं. सं.	विषय	पृष्ठ संख्या
01.	प्रबंध निदेशक एवं मुख्य	01 - 05
	कार्यपालक	01
	कार्यपालक निदेशक	02
	कार्यपालक निदेशक	03
	मुख्य सतर्कता अधिकारी	04
	मुख्य सूचना सुरक्षा अधिकारी	05
02.	उभरते साइबर रुझानों पर नजर रखना	06
03.	भ्रामक डायलर: नकली ग्राहक सेवा खतरे पर कहानी	07
04.	धन मृगतृष्णा : नकली ऋण ऐप धोखाधड़ी पर कहानी	09
05.	कूरियर षड्यंत्र: पार्सल डिलीवरी के बहाने घोटाला	11
06.	भ्रामक डेव: निवेश विश्वासघात की कहानी	13
07.	डिजिटल धोखाधड़ी: यूपीआई और क्यूआर कोड के माध्यम से किराया घोटाले की कहानी	15
08.	फेडएक्स घोटाला: पार्सल में ड्रग्स के धोखे का पर्दाफाश	17
09.	कार्य समस्या: कार्य आधारित जॉब ऑफर ट्रैप पर कहानी	19
10.	गहरी दुविधा: आर्टिफिशियल इंटेलिजेंस आधारित घोटाले पर कहानी	21
11.	मालिक का विश्वासघात: कॉर्पोरेट धोखाधड़ी के गलियारों में सामने आने वाला साइबर घोटाला	23
12.	फर्जी जुर्माना: फर्जी संदेशों/कॉल के जरिए ई-चालान घोटाले पर कहानी	25
13.	साइबर धोखाधड़ी की घटनाओं और संदिग्ध धोखाधड़ी संसूचना की रिपोर्टिंग	27
14.	परिशिष्ट	28

प्रबंध निदेशक एवं मुख्य कार्यपालक अधिकारी की कलम से

सभी यूकोजन एवं मूल्यवान ग्राहकगण,

तकनीक के चमत्कारों के इस युग में, जहाँ प्रत्येक क्लिक हमें संभावनाओं की दुनिया में ले जाता है, वहीं डिजिटल दुनिया में हमें वादे और खतरे दोनों ही मिलते हैं। इस डिजिटल महासागर में 'साइबर नेत्र' प्रकाश-स्तंभ की तरह उभरा है। यह साइबर-सुरक्षित समाज के निर्माण की दिशा में हमारी प्रतिबद्धता का प्रमाण है।

इस कॉमिक पुस्तक के स्पंदित पृष्ठों से होकर हम एक ऐसी कथा-यात्रा पर निकलते हैं जो पारंपरिक ज्ञान की सीमाओं से परे है। जैसे-जैसे हम इन चित्रमय मुखर आख्यानों को पढ़ते जाते हैं हम न केवल कहानियां पढ़ते हैं वरन अपने डिजिटल परिवेश-तंत्र की जटिलताओं से लिपटे अमूल्य सबक भी सीखते चलते हैं।

आज, इस डिजिटल युग के अभिरक्षक के रूप में हमारा दायित्व महज़ भागीदारी तक सीमित नहीं है, हमें एक सतर्क अभिभावक बनना है। 'साइबर नेत्र' सिर्फ़ कथा-संकलन नहीं है; यह एक पहल है, कार्रवाई का आह्वान है। यह हममें से प्रत्येक को साइबर जागरूकता का अग्रदूत बनने का आवाहन करता है। वह अग्रदूत जो न केवल सूचना-सुसज्जित ही है बल्कि समझने और बचाव करने के ज्ञान से भी सम्पन्न है।

मैं आपको इन कथाओं में तल्लीन होने, अंतर्दृष्टि पाने और हमारे 'साइबर रक्षक' के परामर्श पर ध्यान देने का अनुरोध करता हूं। आइए, हम इस ज्ञान को एक ऐसा कवच बनाएं जिससे न केवल हमारी बल्कि हमारे डिजिटल समाज की भी सुरक्षा हो सके।

आइए, हम सब मिलकर एक ऐसी कहानी रचें जिसमें साइबर जागरूकता इस पुस्तक के पन्नों से निकलकर हमारे दैनिक जीवन के लोकाचार में ढ़ल जाए।

आइए, 'साइबर नेत्र' से साइबर जागरूकता की ज्योति जलाएं, सभी मिल कर संकल्प लें और हममें से प्रत्येक को सशक्त बनाएं ताकि डिजिटल दुनिया को और अधिक सुरक्षित हो सके।

सावधान रहें, सुरक्षित रहें।

हार्दिक शुभकामनाओं के साथ,

[अश्वनी कुमार]

प्रबंध निदेशक एवं मुख्य कार्यपालक अधिकारी

कार्यपालक निदेशक की कलम से

आदरणीय पाठकगण,

ऐसे युग में जहां हमारा दैनिक जीवन डिजिटल परिवेश के साथ सहज भाव से सुसंबद्ध है, साइबर जागरूकता के महत्व की अनदेखी नहीं की जा सकती। 'साइबर नेत्र' साइबर साक्षरता के माध्यम से सशक्त समाज के निर्माण के प्रति हमारी अटूट प्रतिबद्धता का प्रमाण है।

'साइबर नेत्र' की जो जीवंत चित्रपट इन पन्नों में बना है वह केवल एक आख्यान नहीं बल्कि वह डिजिटल क्षेत्र की जटिलताओं के भीतर देख पाने की एक गहन अंतर्दृष्टि भी देता है। इन ग्राफिक कथाओं को पढ़ते-पढ़ते हम बोध की एक यात्रा पर निकल पड़ते हैं, जहाँ हर कथा हमें किसी मार्गदर्शक की तरह उच्च साइबर चेतना की ओर ले जाती है।

इस पहल का उद्देश्य केवल कहानी सुनाने तक सीमित नहीं है; यह सक्रिय साइबर सतर्कता की संस्कृति विकसित करने की हमारी आकांक्षा का प्रतीक है। इस कॉमिक पुस्तक में कलाकार की कूची के हर स्ट्रोक तथा संवाद की हर पंक्ति का उद्देश्य है - बोध कराना, जानकारी देना और सशक्त बनाना।

प्रिय पाठको, मैं आपसे आग्रह करता हूँ कि आप इन कथाओं को न केवल पढ़ें, बल्कि उनमें निहित बोध को आत्मसात भी करें। आइए, हमारे 'साइबर रक्षक' के अनुभव मार्गदर्शक सिद्धांतों के रूप में प्रतिध्वनित हों तथा उससे हम सभी के भीतर जागरूकता की एक ज्योति जले, ताकि डिजिटल भूलभुलैया में हमारा मार्ग रोशन हो सके।

इन पन्नों को पलटते हुए, आइए हम सीखे गए सबक को इस पुस्तक में ही सीमित न रहने दें बल्कि इस सबक को कार्यरूप बदलने की चेष्टा करें। 'साइबर नेत्र' एक उत्प्रेरक बनकर निष्क्रिय ज्ञान को उस सक्रिय अभिभावकता में बदल दे जो हमारी सामूहिक साइबर जागरूकता को एक मजबूत डिजिटल परिदृश्य का रूप प्रदान करती है।

अटूट दृढ़ संकल्प और खुले दिल के साथ, आइए हम 'साइबर नेत्र' में दी गई अंतर्दृष्टि अपनाएं और एक संरक्षित तथा सुरक्षित डिजिटल भविष्य की ओर कदम बढ़ाएं।

हार्दिक शुभकामनाओं के साथ,

[राजेन्द्र कुमार साबू]

कार्यपालक निदेशक

कार्यपालक निदेशक की कलम से

मेरे प्रिय साथियो एवं ग्राहको,

जैसे-जैसे हम 'साइबर नेत्र' के पाठ पढ़ते जाते हैं, हम साइबर चेतना के गर्भ में अपनी रूपांतरकारी यात्रा में आगे बढ़ते जाते हैं। यह अनूठी कॉमिक पुस्तक न केवल कथाओं का एक खजाना है, बल्कि यह डिजिटल रूप से एक लोचदार समाज बनाने की हमारी प्रतिबद्धता का प्रमाण भी है।

इन सुस्पष्ट चित्र-कथाओं में अंतर्दृष्टि का खजाना छिपा है। इसमें साइबर बोध के धागों से बुना गया एक चित्रपट है। 'साइबर नेत्र' जटिल अवधारणाओं को आकर्षक और सुलभ प्रारूप में प्रस्तुत करके साइबर शिक्षा की पारंपरिक सीमाओं का अतिक्रमण करने का प्रयास करता है।

यह पहल केवल पन्ने पलटने के लिए नहीं की जा रही है; यह मानसिकता में बदलाव लाने का एक प्रयास है। यह पहल न केवल आकर्षक कथाओं में खो जाने के लिए है बल्कि प्रत्येक ग्राफिक चित्रण में अंतर्निहित साइबर जागरूकता के सार को आत्मसात करने के लिए है।

जैसे-जैसे डिजिटल परिदृश्य विकसित होता है, वैसे-वैसे हमारी समझ और तैयारी भी विकसित होनी चाहिए। मैं आपको 'साइबर नेत्र' के गलियारों से गुजरने के लिए प्रोत्साहित करता हूँ, निष्क्रिय पाठकों के रूप में नहीं बल्कि साइबर सतर्कता के सक्रिय राजदूतों के रूप में।

उम्मीद है कि यह कॉमिक पुस्तक जागरूकता की ज्योति जलाएगी, संवाद को प्रेरित करेगी और एक सुरक्षित डिजिटल पारिस्थितिकी तंत्र के लिए एक सामूहिक आंदोलन की प्रेरणा बनेगी। आइए, हम इस प्रयास को बदलाव के उत्प्रेरक के रूप में लें, एक ऐसे समाज को बढ़ावा दें जहां साइबर साक्षरता हमारी सामूहिक ताकत बन जाए।

आशा और दृढ़ संकल्प के साथ ज्ञान को कार्रवाई में बदलने के लिए और जागरूकता को एक सुरक्षित डिजिटल भविष्य का प्रतिरक्षक बनाने के लिए तैयार रहें। आइए, हम एक साथ इस यात्रा पर चलें।

हार्दिक शुभकामनाओं के साथ,

[विजय एन कांबले]

कार्यपालक निदेशक

मुख्य सतर्कता अधिकारी की डेस्क से

सभी सम्मानित सहकर्मियों और नागरिकों

ऐसे युग में जहाँ डिजिटल और भौतिक दुनिया एक दूसरे से आकार मिलती हैं, सतर्कता ही हमारी सबसे बड़ी प्रतिरक्षा हो जाती है। जबकि सतर्कता जागरूकता सप्ताह बहुत निकट है, साइबरस्पेस और हमारी रोज़मर्रा की ज़िम्मेदारियों में सक्रिय सतर्कता के महत्व को कम करके नहीं आंका जा सकता। ऐसे समय में हम ईमानदारी, पारदर्शिता और सुरक्षा के प्रति अपनी प्रतिबद्धता की पुन: पुष्टि करते हैं।

मुझे 'साइबर नेत्र' को न सिर्फ एक कॉमिक पुस्तक के रूप में बल्कि तेजी से विकसित हो रहे इस डिजिटल परिदृश्य में हम में से प्रत्येक को सतर्क बनाए रखने के एक गतिशील उपकरण के रूप में प्रस्तुत करते हुए गर्व हो रहा है। यह ग्राफिक कथा प्रभाविता के साथ याद दिलाती है कि किस प्रकार साइबर सतर्कता हमारे बुनियादी मूल्यों यथा ईमानदारी, जिम्मेदारी और सुरक्षा का ही एक विस्तार है।

'साइबर नेत्र' हमारे डिजिटल इंटरैक्शन के ही नहीं बल्कि हमारे संस्थान और समुदाय की सामूहिक सुरक्षा की देख-रेख में लगे हममें से प्रत्येक की महत्वपूर्ण भूमिका को दर्शाते करते हुए साइबर दुनिया के वास्तविक और विद्यमान खतरों को उजागर करनेवाली कथाओं को प्राणवान करता है। अपनी मोहक प्रस्तुति से यह इस विचार को दृढ़ करता है कि साइबर सतर्कता, जो विश्वास बरकरार रखने और सुरक्षित डिजिटल परिवेश सुनिश्चित करने के लिए महत्वपूर्ण है, हम सबका एक साझा दायित्व है।

प्रिय साथियों और नागरिकों, मेरी कामना है यह कॉमिक आपको जागरूक बनाने की दिशा में एक मार्गदर्शक बने तथा आपको याद दिलाए कि चाहे धोखाधड़ी पकड़ने की बात हो, कदाचार पहचानने की बात हो या साइबर खतरों से बचाव करने की बात हो, सतत सतर्कता अवश्य बनी रहनी चाहिए। यह केवल जोखिमों से बचने के लिए ही नहीं, बल्कि हमारे जीवन के हर क्षेत्र में जागरूकता, अखंडता और जवाबदेही की संस्कृति को विकसित करने के लिए भी जरूरी है।

हम सतर्कता जागरूकता सप्ताह मनाने जा रहे हैं। आइए, हम 'साइबर नेत्र' में दिए गए सबक सीखें तथा सतर्कता के मूल्यों को बनाए रखने की अपनी प्रतिज्ञा दुहराएं। यह सुनिश्चित करते हुए कि हम न केवल अपनी डिजिटल दुनिया के प्रति बल्कि अपनी नैतिक प्रतिबद्धताओं के प्रति भी सतर्क संरक्षक बने रहें। आइए, हम मिलकर जागरूकता को अपनी कार्रवाई में बदलें।

दृढ़ समर्पण के साथ

[वी आनंद]
मुख्य सतर्कता आधिकारी

मुख्य सूचना सुरक्षा अधिकारी की डेस्क से

मेरे सभी प्रिय सहकर्मियों एवं मूल्यवान ग्राहकों को,

हमारी परस्पर सम्बद्ध दुनिया की डिजिटल सुरलहरी में, नवाचार की धुनें उभरते साइबर खतरों की कर्कश ध्वनि के साथ टकराने लगी हैं। 'साइबर नेत्र' न केवल एक कॉमिक पुस्तक के रूप में बल्कि साइबर तैयारी को मजबूत करने के हमारे साझा मिशन की बुनियाद के रूप में प्रस्तुत किया जा रहा है।

'साइबर नेत्र' के पन्नों में हम न केवल आख्यानों को उजागर करते हैं, बल्कि साइबरस्पेस की जटिल भूलभुलैया से बच कर निकालने के तरीके भी बताते हैं। इस पुस्तक का उद्देश्य आपको शब्दजाल से अभिभूत करना नहीं है, बल्कि साइबर साक्षरता को अपनी डिजिटल चेतना में सबसे आगे रखते हुए व्यावहारिक ज्ञान के साथ सशक्त बनाना है।

अपने बैंक की साइबर सुरक्षा के संरक्षक के रूप में मैं आपसे 'साइबर नेत्र' को किसी पुस्तक से अधिक महत्व देने का आग्रह करता हूं। यह आपकी साइबर किलेबंदी को मजबूत करने के उपायों का एक संग्रह है। हमारी कामना है कि यह पुस्तक हमें निष्क्रिय पर्यवेक्षकों से बदलकर साइबर शुचिता के सक्रिय प्रतिरक्षक बना कर रख देने वाले परिवर्तन का उत्प्रेरक बने। आइये, हम सब मिलकर साइबर जागरूकता के आह्वान पर ध्यान दें। आप न केवल इन पृष्ठों को पढ़ें बल्कि अपने दैनिक डिजिटल लेन-देन में भी साइबर जागरूकता बनाए रखें।

'साइबर नेत्र' साइबर चेतना का प्रतीक बने, एक ऐसे आंदोलन को प्रेरित करे जहां हर क्लिक, हर लेन-देन में सूचित सतर्कता का नाद ध्वनित हो । हमारे साइबर रक्षक का मार्गदर्शन उभरते साइबर खतरों की उथल-पुथल के बीच हमें सहारा देने वाला एक स्तंभ बने।

आइए, अटूट निष्ठा के साथ एकजुट हों, ज्ञान-सम्पन्न हों और साइबर जागरूकता बढ़ाने, कमजोरियों को ताकत में और अनिश्चितताओं को तैयारियों में बदलने का संकल्प लें।

हार्दिक शुभकामनाओं के साथ,

[मुहम्मद साबिर]
मुख्य सूचना सुरक्षा अधिकारी

उभरते साइबर रुझानों पर नज़र रखना

हमारे तेजी से विकसित हो रहे डिजिटल परिदृश्य में, उभरते साइबर रुझानों की वृद्धि ने आभासी क्षेत्र में हमारी बातचीत, लेन-देन और आवागमन के तरीके को नया रूप दे दिया है। प्रौद्योगिकीय प्रगति के साथ नवाचार और कनेक्टिविटी के लिए नए अवसर सामने आ रहे हैं, लेकिन इन अवसरों के साथ-साथ साइबर खतरे और कमजोरियां भी बढ़ रही हैं।

नमस्कार और '**साइबर नेत्र** ' में आपका स्वागत है, यह कहानी कहने और चित्रमय प्रतिनिधित्व की शक्ति के माध्यम से साइबर जागरूकता को बढ़ावा देने की हमारी पहल है। यह कॉमिक बुक हमारे पाठकों को शिक्षित और सशक्त बनाने के लिए एक आकर्षक और उदाहरणात्मक प्रारूप में प्रस्तुत साइबर रुझानों के लगातार विकसित हो रहे परिदृश्य पर प्रकाश डालती है।

इन पृष्ठों में, '**साइबर नेत्र** ' ऐसी कहानियाँ प्रस्तुत करता है जो उभरते साइबर परिदृश्यों को स्पष्ट रूप से चित्रित करती हैं। इन ग्राफिकल आख्यानों के माध्यम से, हमारा लक्ष्य प्रचलित साइबर खतरों पर प्रकाश डालना, साइबर सतर्कता के महत्व को प्रदर्शित करना और उभरते डिजिटल जोखिमों के विरुद्ध सुरक्षा के बारे में जानकारी प्रदान करना है।

साइबर जागरूकता के हमारे अवतार 'साइबर रक्षक' से मिलिए।

इन दो प्रतिष्ठित शुभंकरों को साइबर जागरूकता और सर्वोत्तम पद्धतियों के सार को मूर्त रूप देने के लिए तैयार किया गया है। जैसे-जैसे आप '**साइबर नेत्र** ' की कहानियों के माध्यम से आगे बढ़ेंगे, हमारे साइबर रक्षक मार्गदर्शन के प्रतीक के रूप में खड़े होंगे, तथा प्रत्येक कहानी के अंत में प्रमुख साइबर सुरक्षा पद्धतियों का वर्णन करेंगे।

इस ज्ञानवर्धक अन्वेषण में हमारे साथ शामिल हों, क्योंकि 'साइबर नेत्र ' हमारे साइबर रक्षक के साथ साइबर चेतना के दायरे को उजागर करता है, जो एक सुरक्षित डिजिटल दुनिया का मार्ग प्रशस्त करता है।

भ्रामक डायलर

नकली ग्राहक सेवा खतरे पर कहानी

ठीक है। यह कार्यालय में दोपहर के भोजन का समय है। चलो अब IRCTC से फैमिली वेकेशन के लिए टिकट बुक कर लेते हैं।

ओह! मेरा आईआरसीटीसी अकाउंट ब्लॉक हो गया!

चलिए इंटरनेट पर कुछ खोजते हैं।

आह!! यहाँ मुझे इंटरनेट पर कुछ हेल्पलाइन नंबर मिले। चलो फोन करते हैं, मुझे उम्मीद है कि इससे समस्या का समाधान हो जाएगा।

IRCTC Air Customer Care No. 1800 110 139

91 244 XXXX

नमस्ते ! मैं राज बोल रहा हूँ। मेरा आईआरसीटीसी अकाउंट ब्लॉक कर दिया गया है. कृपया मेरा खाता सक्रिय करें।

मुझे तत्काल टिकट बुक करना है।

ज़रूर सर, हम आपका खाता अनलॉक करने में आपकी मदद कर सकते हैं, लेकिन इसके लिए रु.10 का एक छोटा सा सुविधा शुल्क है।

कोई समस्या नहीं है। कृपया शीघ्रता से मेरा खाता सक्रिय करें!

91 244 XXXX
Dear customer, Please click the below link & pay the convenience fee for your IRCTC account.
Okay No Yes
CLICK

http://www.fakepayment.mysite/
Card Details
Enter your card information or use the camera
Name
Card Number
Expiration Date mm / yy
CVV Code
Pay Rs. 10

अरे नहीं!! यह पुनः भुगतान त्रुटि दिखा रहा है!

PAYMENT ERROR !
Close

कोई बात नहीं सर, सर्वर की समस्या के कारण ऐसा हो सकता है।

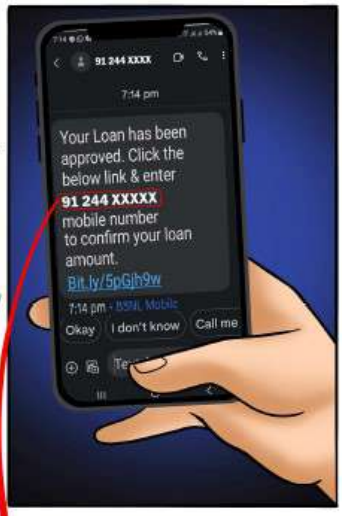
आपकी ओर से धनवापसी अनुरोध पर कार्रवाई करने के लिए मुझे कुछ मिनट दें।

सावधान! यदि आप कभी भी सर्च इंजन में दिखने वाले फर्जी कस्टमर केयर नंबरों पर भरोसा नहीं करते हैं तो जालसाज आपको कभी धोखा नहीं दे सकते हैं

- सर्च इंजन में ग्राहक सेवा या हेल्पलाइन नंबर से संबंधित जानकारी खोजने से बचें क्योंकि जालसाज उपयोगकर्ताओं को लुभाने के लिए भ्रामक जानकारी/विज्ञापन प्रदर्शित
- वैध ग्राहक सेवा या हेल्पलाइन नंबर से संबंधित जानकारी प्राप्त करने के लिए हमेशा संगठन की आधिकारिक वेबसाइट या ऐप देखें।
- किसी भी परिस्थिति में संवेदनशील, व्यक्तिगत या वित्तीय जानकारी, जैसे कार्ड विवरण, सीवीवी, पिन, ओटीपी, यूपीआई पिन, वित्तीय क्रेडेंशियल आदि किसी के साथ साझा न करें।
- अधिकांश ओटीपी संदेशों में ओटीपी जारी होने का कारण लिखा रहता है। कोई भी कार्रवाई करने से पहले प्रत्येक संदेश को ध्यान से पढ़ें।
- साइबर धोखाधड़ी की घटना की तुरंत साइबर अपराध हेल्पलाइन नंबर 1930 पर रिपोर्ट करें और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (https://wwwcybercrime.gov.in) पर शिकायत दर्ज करें।

धन मृगतृष्णा

फर्जी लोन ऐप धोखाधड़ी की कहानी



उन्होंने वही मोबाइल नंबर दर्ज किया जो एसएमएस से प्राप्त हुआ था।

ऐसे घोटाले से बचने के सर्वोत्तम पद्धति

- तत्काल ऋण प्राप्त करने के लिए ईमेल, एसएमएस, व्हाट्सएप, सोशल मीडिया आदि के माध्यम से प्राप्त संदिग्ध लिंक पर क्लिक न करें।
- कभी भी व्यक्तिगत, संवेदनशील या वित्तीय जानकारी किसी के साथ साझा न करें।
- ऐसे आसान ऋण प्रस्तावों से बचें जो सच होने के लिए प्रतीत हों।
- ऐसे ऋणदाताओं से दूर रहें जो ऋण स्वीकृत करने के नाम पर अग्रिम भुगतान मांगते हैं।
- किसी भी अनजान व्यक्ति के कहने पर कभी भी कोई अनजान ऐप डाउनलोड न करें। किसी ऐप को डाउनलोड करने से पहले हमेशा उसकी प्रामाणिकता की जांच करें, समीक्षाएँ और रेटिंग आदि पढ़ें।
- ऐप अनुमतियों की बार-बार समीक्षा करें और ऐप्स को अनावश्यक अनुमति न दें।
- हमेशा आरबीआई द्वारा अनुमोदित बैंकिंग और वित्तीय सेवा संस्थानों या कंपनियों से ऋण के लिए आवेदन करें।
- साइबर धोखाधड़ी की घटना की तुरंत साइबर अपराध हेल्पलाइन नंबर 1930 पर रिपोर्ट करें और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (https://www.cybercrime.gov.in) पर शिकायत दर्ज करें।

कूरियर साजिश

पार्सल डिलीवरी के बहाने घोटाला

उपयोगकर्ता ने कॉल पर हैकर के साथ अद्वितीय कोड (डेस्क आईडी) साझा किया।

यहाँ क्या हुआ ?

आजकल, पार्सल का इंतजार कर रहे व्यक्तियों को धोखेबाजों द्वारा सोशल इंजीनियरिंग रणनीति के माध्यम से धोखा दिया जाता है। जालसाज सर्च इंजन के परिणामों में हेरफेर करता है और फर्जी ग्राहक सेवा नंबर प्रदर्शित करता है। यदि कोई व्यक्ति उस नंबर पर संपर्क करता है, तो कूरियर सेवा कंपनी के एजेंट की आड़ में जालसाज चालाकी से व्यक्ति का विश्वास हासिल कर लेता है और फर्जी स्क्रीन शेयरिंग ऐप (रिमोट एक्सेस टूल) डाउनलोड करने के लिए मना लेता है और ऐप के भीतर प्रदर्शित अद्वितीय एड्रेस कोड को साझा करने के लिए राजी कर लेता है। भ्रामक तकनीकों का उपयोग करते हुए, जालसाज व्यक्ति को दूर से डिवाइस पर नियंत्रण पाने के लिए ऐप अनुमतियां और सुरक्षा चेतावनी सूचनाएं स्वीकार करने के लिए मजबूर करता है। गूगल फॉर्म लिंक व्यक्तिगत विवरण के साथ-साथ कार्ड विवरण, यूपीआई आईडी और पिन आदि जैसे वित्तीय क्रेडेंशियल्स को कैप्चर करने के लिए साझा किया जाता है। इस डेटा और पीड़ित के डिवाइस तक रिमोट एक्सेस के साथ, धोखेबाज अनधिकृत लेनदेन शुरू करता है और लेनदेन के दौरान प्राप्त ओटीपी को पढ़ता है, जिससे पीड़ित को वित्तीय नुकसान होता है।

ऐसे घोटाले से बचने के सर्वोत्तम पद्धति

- सर्च इंजन पर कस्टमर केयर या हेल्पलाइन नंबर खोजने से बचें क्योंकि जालसाज व्यक्तियों को लुभाने के लिए नकली/फर्जी वेबसाइट के तहत भ्रामक जानकारी/विज्ञापन प्रदर्शित कर सकते हैं।
- वैध ग्राहक सेवा या हेल्पलाइन नंबर से संबंधित जानकारी प्राप्त करने के लिए हमेशा संगठन की आधिकारिक वेबसाइट या ऐप देखें।
- या किसी अजनबी के कहने पर कभी भी वित्तीय लेनदेन न करें।
- कभी भी संवेदनशील, व्यक्तिगत या वित्तीय जानकारी, जैसे कार्ड विवरण, वित्तीय क्रेडेंशियल, ओटीपी, पिन, यूपीआई पिन किसी के साथ या किसी भी यादृच्छिक फॉर्म / वेबसाइट / सोशल मीडिया प्लेटफॉर्म आदि पर साझा न करें।
- ऐप की अनुमतियों, सूचनाओं, सुरक्षा चेतावनियों आदि की सावधानीपूर्वक समीक्षा करें। ऐप को अनावश्यक अनुमति न दें जो रिमोट एक्सेस की अनुमति देते हैं।
- साइबर धोखाधड़ी की घटना की तुरंत साइबर अपराध हेल्पलाइन नंबर 1930 पर रिपोर्ट करें और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (https://www.cybercrime.gov.in) पर शिकायत दर्ज करें।

भ्रामक डेव

निवेश विश्वासघात की कहानी

श्री मेहरा एक रियल एस्टेट बिल्डर हैं। एक दिन उन्हें एक अनजान नंबर से कॉल आया।

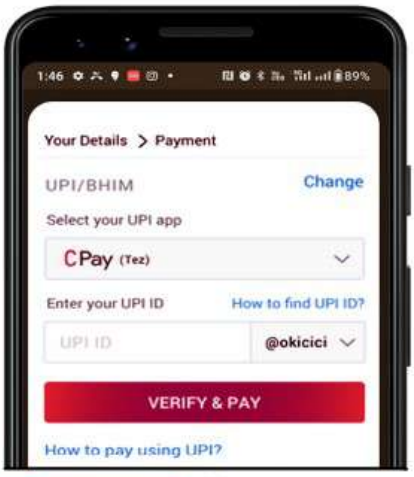
एसएमएस लिंक से ऐप डाउनलोड करना है।

सबसे पहले उन्होंने रु.50,000 का निवेश किया जो 7 दिनों के भीतर बढ़कर रु.100,000 हो गया।

उन्होंने पुनः रु.500,000 का निवेश किया जो केवल 4 दिनों में बढ़कर रु.10,00,000 हो गया।

उन्होंने पुनः रु.700,000 का निवेश किया जो केवल 4 दिनों में बढ़कर रु.20,00,000 हो गया।

मेहरा ने लिंक पर क्लिक किया और अपनी यूपीआई आईडी और पिन के माध्यम से कमीशन राशि का 10% भुगतान किया।



कुछ देर बाद...

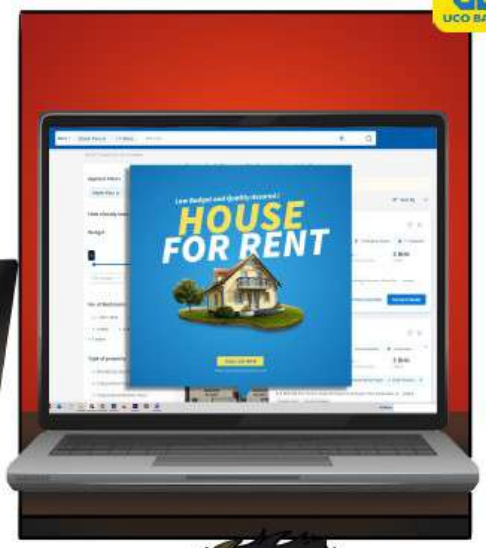
सुरक्षा पद्धति

- ऐसे निवेश अवसरों से सावधान रहें जो कम समय में असामान्य रूप से अधिक रिटर्न का वादा करते हैं।
- किसी को भी आप पर जल्दी से निवेश निर्णय लेने का दबाव न बनाने दें।
- किसी भी निवेश ऐप को डाउनलोड करने और उपयोग करने से पहले गहन शोध करें और समीक्षाएं, रेटिंग आदि पढ़ें।
- पंजीकृत और प्रतिष्ठित मध्यस्थों/निवेश कंपनियों के साथ व्यवहार करना सुनिश्चित करें।

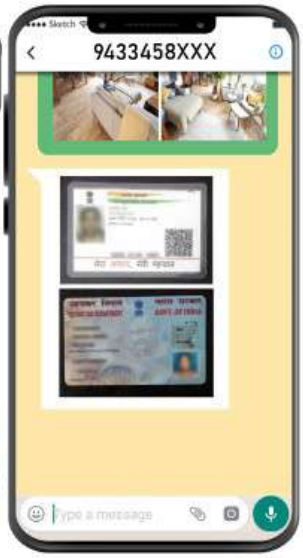
डिजिटल धोखा

यूपीआई और क्यूआर कोड के माध्यम से किराये के घोटाले की कहानी

रीना अपने घर के लिए किराएदार की तलाश कर रही थी। उसने एक रियल एस्टेट वेबसाइट पर अपने घर का विज्ञापन और अपना संपर्क विवरण डाला।



अगले ही दिन रीना को एक अज्ञात नंबर से व्हाट्सएप मैसेज मिला।



सुरक्षा पद्धति

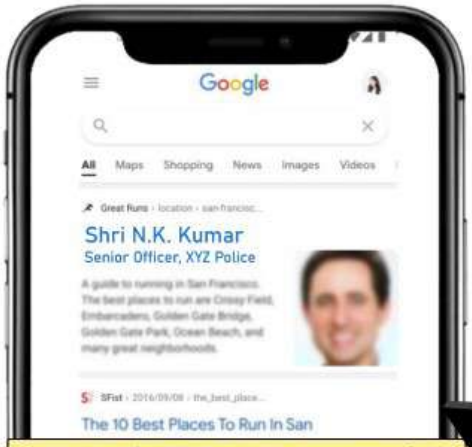
- पैसे प्राप्त करने के लिए कभी भी क्यूआर कोड स्कैन न करें और यूपीआई पिन दर्ज न करें।
- यदि किरायेदार या खरीदार आपसे पैसे प्राप्त करने के लिए क्यूआर कोड स्कैन करने या यूपीआई पिन दर्ज करने पर जोर देता है, तो वह व्यक्ति एक घोटालेबाज है।
- किसी भी अज्ञात यूपीआई आईडी से निधि अंतरण या भुगतान अनुरोध स्वीकार न करें। कोई भी लेनदेन करने से पहले हमेशा यूपीआई पता जांच लें।
- स्कैन करने से पहले, किसी भी छेड़छाड़ या बदलाव के संकेत के लिए क्यूआर कोड पर बारीकी से नज़र डालें।
- सार्वजनिक स्थानों पर यादृच्छिक क्यूआर कोड को स्कैन करने से बचें, यह बहुत अच्छा होने का वादा करता है जो सच नहीं हो सकता है।
- सरकार के चक्षु पोर्टल (https://sancharsaath.gov.in) पर संदिग्ध या धोखाधड़ी वाले कॉल, एसएमएस, व्हाट्सएप भेजने वाले नंबर की रिपोर्ट करें।
- साइबर अपराध और ऑनलाइन वित्तीय धोखाधड़ी की रिपोर्ट साइबर अपराध हेल्पलाइन नंबर 1930 और रिपोर्टिंग पोर्टल (https://www.cybercrime.gov.in) पर करें।

फेडेक्स घोटाला

पार्सल में ड्रग्स के धोखे का पर्दाफाश

एक दिन मीनू को किसी अनजान नंबर से कॉल आया।

मीनू ने चैट ऐप खोला और फोटो के साथ एक वरिष्ठ पुलिस अधिकारी का नाम देखा।



उन्होंने सर्च इंजन से अधिकारी का नाम और फोटो भी जांचा और पाया कि यह सही है।

उसने व्यक्तिगत खाते की शेष राशि के साथ-साथ सभी खातों का विवरण भी दे दिया।

अब, आपको तुरंत नीचे दी गई यूपीआई आईडी पर विधिक शुल्क के लिए रु.49000/- और सीमा शुल्क अनापत्ति के लिए रु.49000/- का भुगतान

यूपीआई आईडी - NarcOticCell@1234.

मैं पुलिस से झंझट नहीं चाहता! आइए मामले को अंदर ही सुलझा लें

Your Details > Payment
UPI/BHIM Change
Select your UPI app
CPay (Tez)
Enter your UPI ID How to find UPI ID?
NarcOticCell@1234
VERIFY & PAY

UPI ID - NarcOticCell@1234

PAY
98000
PROCEED
BHIM UPI

महोदय, कृपया इस मामले को जल्द से जल्द निपटाने में मेरी मदद करें।

महोदया, मुझे लगता है कि आपने मामले की तत्कालिकता और गंभीरता को नहीं समझा है। यदि आप मेरी बात नहीं मानेंगी तो आपको जल्द ही गिरफ्तार कर लिया जाएगा।

इसलिए, तत्काल जांच शुल्क के रूप में रु.49000/- का भुगतान करें और दिए गए खाता संख्या: 1234XXXXXXXXX, आईएफएससी कोड- XXXX0XXXXXX में अभी रु.1.4 लाख अंतरित करें।

मीनू अधिक डर गई और उसने और अधिक पैसे अंतरित कर दिए।

Your Details > Payment
UPI/BHIM Change
Select your UPI app
CPay (Tez)
Enter yout Account no How to find UPI ID?
NarcOticCell@1234
VERIFY & PAY
How to pay using UPI?

PAY
49,000
PROCEED
BHIM UPI

बाबा, क्या आप मुझे तत्काल रु.1.4 लाख भेज सकते हैं? मैं बहुत खतरे में हूँ और मुझे जेल भी हो सकती है। कृपया मेरी मदद करें।

रुको, क्या!!! चिंता मत करो। मैं फोन करके स्थानीय पुलिस स्टेशन से बात करता हूँ।

नमस्ते सर! मेरी बेटी डांसर है। उन पर एक पार्सल में प्रतिबंधित नशीले पदार्थ पाए जाने के मामले में आरोप लगाया गया है। कृपया मदद करें।

आपकी बेटी को फर्जी पार्सल के नाम पर ठगा जा रहा है। आजकल, साइबर अपराधी इंटरनेशनल कूरियर सर्विस कंपनी के कार्यकारी होने का दावा करते हुए, पार्सल में प्रतिबंधित नारकोटिक ड्रग्स का पता लगाने के नाम पर लोगों को ठगते हैं।

अब तुरंत 1930 पर कॉल करें और राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://www.cybercrime.gov.in पर शिकायत दर्ज करें।

साइबर सुरक्षा सर्वोत्तम पद्धति

- अजनबियों से आने वाली अनचाही कॉल से सावधान रहें! याद रखें, कानून प्रवर्तन एजेंसियाँ आधिकारिक विश्वसनीय स्रोतों से पूर्व सूचना के बिना ऐसी कॉल नहीं करती हैं।
- अगर आपको कोई आपराधिक संलिप्तता का आरोप लगाने वाला कॉल आता है, तो बताए गए स्थानीय पुलिस स्टेशन से स्वतंत्र रूप से जानकारी की पुष्टि करने के लिए कदम उठाएँ। बातचीत में संपर्क नंबर, फ़ोटो और उद्धृत नामों की पुष्टि करने के लिए Truecaller और सर्च इंजन के नतीजों पर भरोसा न करें।
- किसी अज्ञात कॉल करने वालों को कभी भी व्यक्तिगत/संवेदनशील/वित्तीय जानकारी न बताएं।
- किसी अज्ञात कॉलर के कहने पर या अत्यावश्यकता/विश्वास/डर/धमकी/दबाव की रणनीति के आधार पर धन अंतरण न करें।
- स्कैमर्स डार्क पैटर्न / रिवर्स मनोवैज्ञानिक तकनीकों का उपयोग इस तरह से करते हैं कि वे जो कुछ भी कह रहे हैं उसे पिछली घटनाओं / व्यक्तिगत जीवन के अनुभवों से जोड़कर व्यक्ति उस पर विश्वास करना शुरू कर देता है।

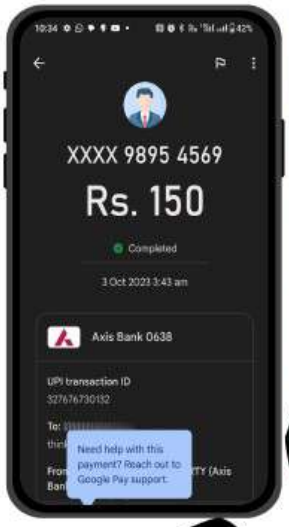
हमेशा सोचें! थोड़ा रुकें, और फिर समझदारी से कार्य करें

कार्य समस्या

कार्य आधारित नौकरी प्रस्ताव जाल पर कहानी

एक दिन रोनित को टेलीग्राम चैट पर एक अज्ञात नंबर से संदेश मिला।

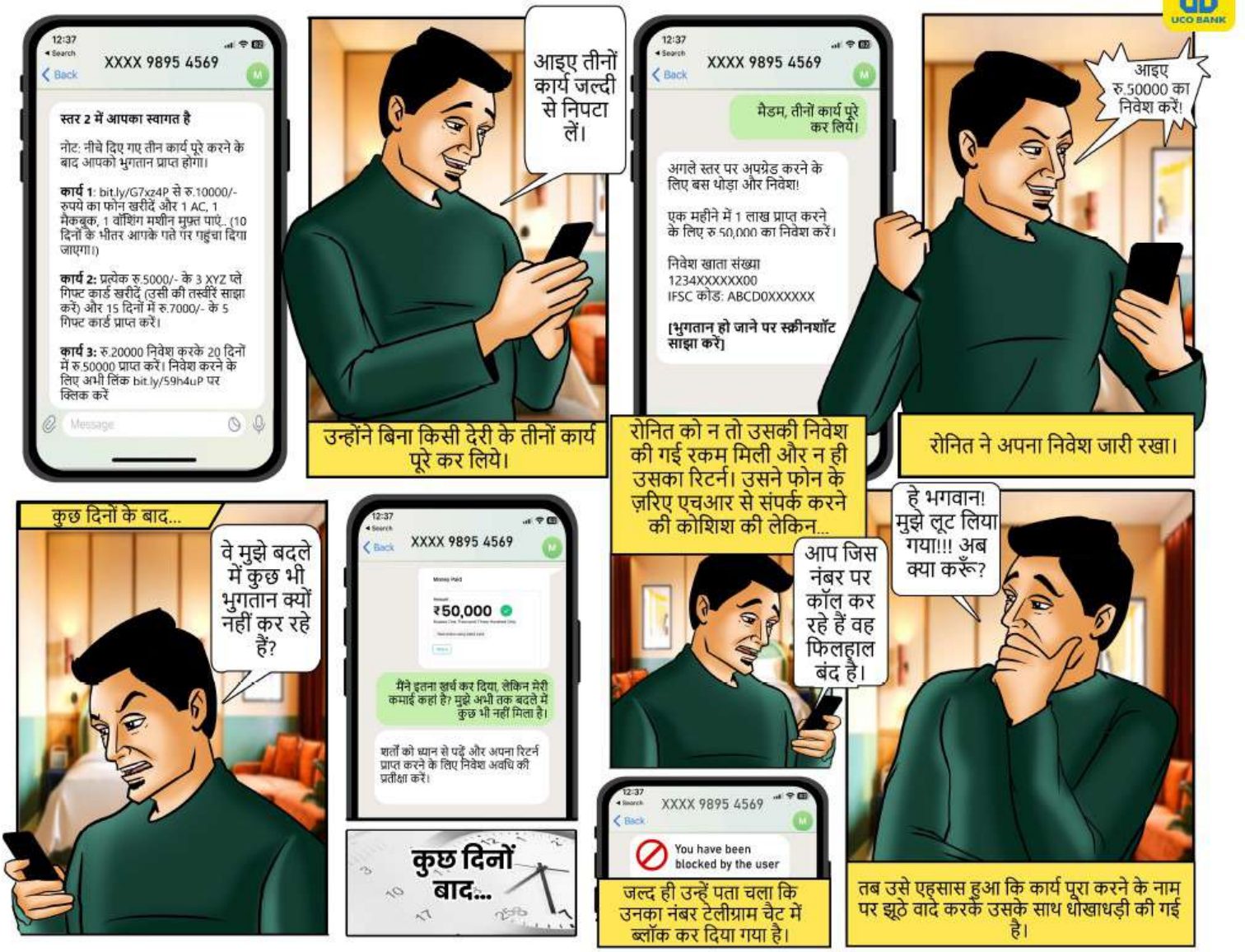
संदेश देखकर रोनित उत्साहित हो गया, क्योंकि यह कोई अतिरिक्त प्रयास किए बिना घर बैठे जल्दी और आसानी से पैसा कमाने का बहुत आसान विकल्प था।



रोनित ने कार्य पूरा किया और पुनः रु.200 प्राप्त किए। उसकी रुचि और अधिक बढ़ती जा रही थी।

अगले दिन रोनित को एक और मैसेज मिला।

रोनित ने तुरंत फीस का भुगतान किया और कुछ नए कार्य प्राप्त किए।


12:37
Search
Back
XXXX 9895 4569
स्तर 2 में आपका स्वागत है
नोट: नीचे दिए गए तीन कार्य पूरे करने के बाद आपको भुगतान प्राप्त होगा।
कार्य 1: bit.ly/G7xz4P से रु.10000/- रुपये का फोन खरीदें और 1 AC, 1 मैकबुक, 1 वॉशिंग मशीन मुफ़्त पाएं.. (10 दिनों के भीतर आगके गते पर गहुंचा दिगा जाएगा।)
कार्य 2: प्रत्येक रु.5000/- के 3 XYZ प्ले गिफ्ट कार्ड खरीदें (उसी की तस्वीरें साझा करें) और 15 दिनों में रु.7000/- के 5 गिफ्ट कार्ड प्राप्त करें।
कार्य 3: रु.20000 निवेश करके 20 दिनों में रु.50000 प्राप्त करें। निवेश करने के लिए अभी लिंक bit.ly/59h4uP पर क्लिक करें
Message
आइए तीनों कार्य जल्दी से निपटा लें।
उन्होंने बिना किसी देरी के तीनों कार्य पूरे कर लिये।
मैडम, तीनों कार्य पूरे कर लिये।
अगले स्तर पर अपग्रेड करने के लिए बस थोड़ा और निवेश!
एक महीने में 1 लाख प्राप्त करने के लिए रु 50,000 का निवेश करें।
निवेश खाता संख्या
1234XXXXXX00
IFSC कोड: ABCD0XXXXXX
[भुगतान हो जाने पर स्क्रीनशॉट साझा करें]
आइए रु.50000 का निवेश करें!
रोनित ने अपना निवेश जारी रखा।
रोनित को न तो उसकी निवेश की गई रकम मिली और न ही उसका रिटर्न। उसने फोन के ज़रिए एचआर से संपर्क करने की कोशिश की लेकिन...
आप जिस नंबर पर कॉल कर रहे हैं वह फिलहाल बंद है।
हे भगवान! मुझे लूट लिया गया!!! अब क्या करूँ?
तब उसे एहसास हुआ कि कार्य पूरा करने के नाम पर झूठे वादे करके उसके साथ धोखाधड़ी की गई है।
You have been blocked by the user
जल्द ही उन्हें पता चला कि उनका नंबर टेलीग्राम चैट में ब्लॉक कर दिया गया है।
कुछ दिनों बाद...
वे मुझे बदले में कुछ भी भुगतान क्यों नहीं कर रहे हैं?
₹50,000
मैंने इतना खर्च कर दिया, लेकिन मेरी कमाई कहां है? मुझे अभी तक बदले में कुछ भी नहीं मिला है।
शर्तों को ध्यान से पढ़ें और अपना रिटर्न प्राप्त करने के लिए निवेश अवधि की प्रतीक्षा करें।
कुछ दिनों बाद...


ऐसे घोटाले से बचने के सर्वोत्तम पद्धति
सोशल मीडिया/इंस्टैंट मैसेजिंग प्लेटफॉर्म पर ऑनलाइन काम पूरा करने के बाद आसानी से पैसे देने की पेशकश करने वाले अनचाहे संदेशों के बारे में संदेह करें।
किसी भी अजनबी के कहने पर उपयोगकर्ता द्वारा प्रेरित कार्यों/क्रियाओं में कभी भी शामिल न हों।
अवास्तविक रिटर्न का वादा करने वाले आकर्षक निवेश प्रस्तावों के झांसे में न आएं।
अधिक भुगतान वाले कार्यों का वादा करने वाले किसी भी व्यक्ति को पैसे भेजने से बचें।
आधिकारिक वेबसाइट/ऐप्स से नौकरी के ऑफर, निवेश के अवसरों आदि की वैधता की पुष्टि करें।
कभी भी अनजान व्यक्तियों के साथ लॉगिन क्रेडेंशियल / व्यक्तिगत / संवेदनशील / वित्तीय जानकारी साझा न करें, खासकर मैसेजिंग ऐप पर।
अज्ञात फ़ाइलें/ऐप्स डाउनलोड न करें और संदिग्ध लिंक पर क्लिक करने से बचें।
साइबर रक्षक
यूको बैंक
UCO BANK
CYBER RAKSHAK

गहरी दुविधा

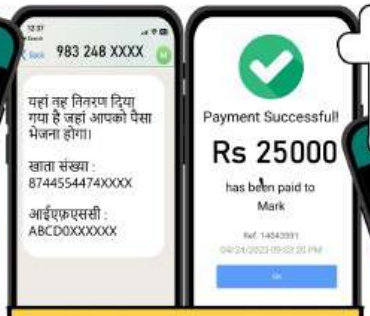
आर्टिफिशियल इंटेलिजेंस आधारित घोटाले पर कहानी

एक दिन, सारा नामक एक युवा पेशेवर, घर पर अपना फोन चेक कर रही थी।

वह देखती है कि उसकी सबसे अच्छी दोस्त निशा व्हाट्सएप पर कॉल कर रही है। इसमें निशा की फोटो है, लेकिन नंबर अज्ञात है।

सारा चिंतित है लेकिन उसे निशा की शक्ल-सूरत में कुछ अजीब बात नज़र आती है।

निशा ने फ़ोन काट दिया ।



बैंक खाते का विवरण मिलने पर, सारा ने तुरंत धन अंतरण शुरू कर दिया।

इस बार "निशा" अपने जवाब में असामान्य व्यवहार कर रही थी, वही लाइन दोहरा रही थी!!

अब सारा को अधिक संदेह होने लगा और उसने व्हाट्सएप कॉल काट दिया।

उसने तुरंत निशा के पिता को फ़ोन किया, पूरी बात बताई और मदद मांगी।

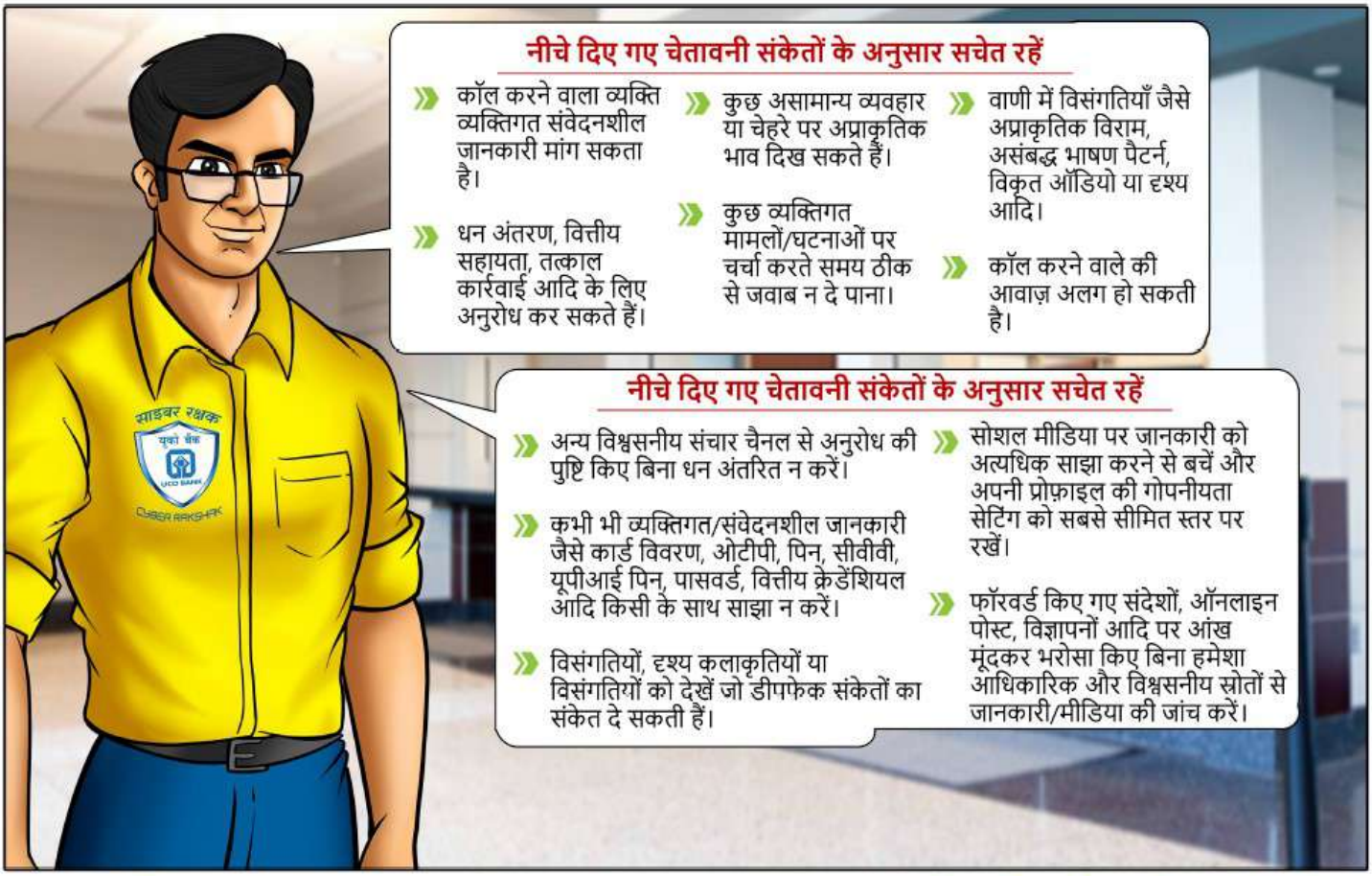
घटना की रिपोर्ट करने के बाद, दोनों को जल्द ही पता चला कि यह एक डीपफेक घोटाला था, जहां साइबर अपराधी आर्टिफिशियल इंटेलिजेंस (एआई) की मदद से नकली ऑडियो, वीडियो या टेक्स्ट सामग्री बनाते हैं जो वास्तविक व्यक्ति की आवाज, उपस्थिति या संचार शैली की नकल करते हैं, जिससे वास्तविक और नकली के बीच अंतर करना चुनौतीपूर्ण हो जाता है।

आइये समझते हैं कि यह घोटाला कैसे संचालित होता है?

- घोटालेबाज लक्षित व्यक्तियों के बारे में जानकारी एकत्र करते हैं, जैसे : आवाज रिकॉर्डिंग, चित्र, वीडियो आदि ताकि एक वास्तविक डिजिटल प्रतिकृति तैयार की जा सके।
- एकत्रित आंकड़ों को फिर एआई एल्गोरिदम द्वारा संसाधित किया जाता है ताकि एआई मॉडल को प्रशिक्षित किया जा सके और लक्ष्य की आवाज, चेहरे के भाव, हाव-भाव और संचार पैटर्न की नकल की जा सके।
- प्रशिक्षित एआई मॉडल का उपयोग करके, जालसाज डीपफेक सामग्री (जैसे वीडियो, ऑडियो आदि) तैयार करता है जिसमें लक्षित व्यक्ति के चेहरे या आवाज के साथ छेड़छाड़ की जाती है या उसे सिंथेटिक तत्वों से बदल दिया जाता है।
- इसके बाद डीपफेक सामग्री को विभिन्न चैनलों जैसे वॉयस कॉल, टेक्स्ट मैसेज, वीडियो कॉल, सोशल मीडिया आदि के माध्यम से लक्षित व्यक्ति के परिचितों को धोखा देने के लिए वितरित किया जाता है।
- मानवीय विश्वास और भावनाओं का शोषण करके, घोटालेबाज अन्य व्यक्तियों को विशिष्ट कार्य जैसे धन हस्तांतरित करना, भुगतान करना, संवेदनशील जानकारी साझा करना आदि करने के लिए बरगलाता है।
- इसके परिणामस्वरूप वित्तीय हानि से लेकर प्रतिष्ठा को नुकसान, डेटा उल्लंघन तथा व्यक्तिगत या व्यावसायिक जानकारी की हानि तक हो सकती है।

नीचे दिए गए चेतावनी संकेतों के अनुसार सचेत रहें

- कॉल करने वाला व्यक्ति व्यक्तिगत संवेदनशील जानकारी मांग सकता है।
- धन अंतरण, वित्तीय सहायता, तत्काल कार्रवाई आदि के लिए अनुरोध कर सकते हैं।
- कुछ असामान्य व्यवहार या चेहरे पर अप्राकृतिक भाव दिख सकते हैं।
- कुछ व्यक्तिगत मामलों/घटनाओं पर चर्चा करते समय ठीक से जवाब न दे पाना।
- वाणी में विसंगतियाँ जैसे अप्राकृतिक विराम, असंबद्ध भाषण पैटर्न, विकृत ऑडियो या दृश्य आदि।
- कॉल करने वाले की आवाज़ अलग हो सकती है।



नीचे दिए गए चेतावनी संकेतों के अनुसार सचेत रहें

- अन्य विश्वसनीय संचार चैनल से अनुरोध की पुष्टि किए बिना धन अंतरित न करें।
- कभी भी व्यक्तिगत/संवेदनशील जानकारी जैसे कार्ड विवरण, ओटीपी, पिन, सीवीवी, यूपीआई पिन, पासवर्ड, वित्तीय क्रेडेंशियल आदि किसी के साथ साझा न करें।
- विसंगतियों, दृश्य कलाकृतियों या विसंगतियों को देखें जो डीपफेक संकेतों का संकेत दे सकती हैं।
- सोशल मीडिया पर जानकारी को अत्यधिक साझा करने से बचें और अपनी प्रोफ़ाइल की गोपनीयता सेटिंग को सबसे सीमित स्तर पर रखें।
- फॉरवर्ड किए गए संदेशों, ऑनलाइन पोस्ट, विज्ञापनों आदि पर आंख मूंदकर भरोसा किए बिना हमेशा आधिकारिक और विश्वसनीय स्रोतों से जानकारी/मीडिया की जांच करें।

मालिक का विश्वासघात

कॉर्पोरेट धोखे के गलियारों में सामने आने वाला साइबर घोटाला

मंदीप सिंह, कार्यपालक अभियंता अपने काम में तल्लीन हैं।

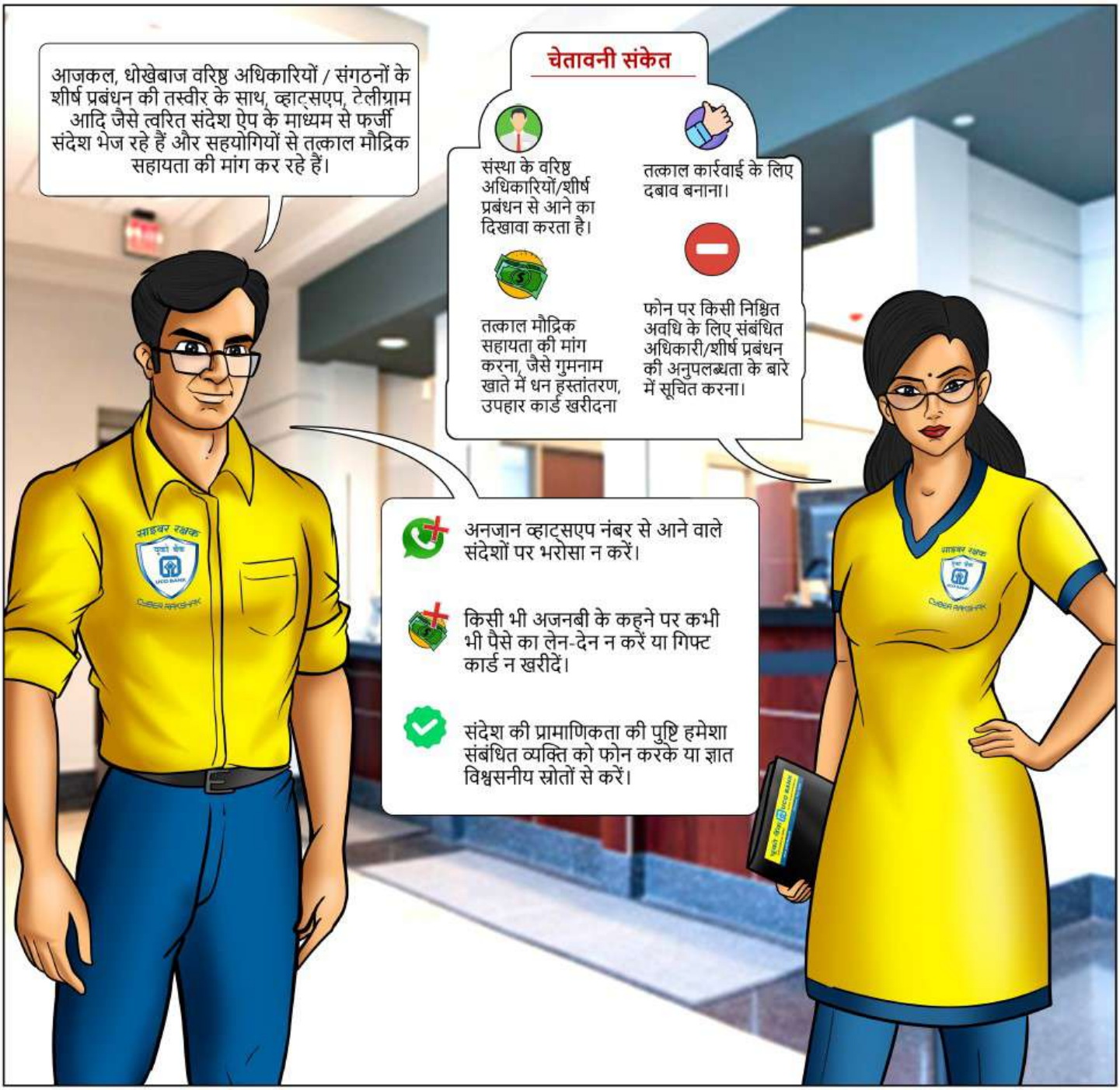
उसने बॉस के कहे अनुसार प्लेटफॉर्म से गिफ्ट कार्ड खरीदे।

मनदीप ने दिए गए खाता नंबर में रु.1.5 लाख अंतरण कर दिए और अपने बॉस को जवाब दिया।

कुछ ही मिनटों के बाद, मनदीप को फिर से एक अज्ञात नंबर से उसके बॉस की प्रोफाइल तस्वीर के साथ एक व्हाट्सएप संदेश प्राप्त हुआ।


महोदया, कृपया मेरी मदद करें।
क्या! यह कैसे संभव है? बॉस अपने चैंबर में हैं। हमें तुरंत अपने बॉस से इस मामले पर बात करनी चाहिए।
मनदीप ने बॉस सचिवालय को फोन किया और पूरी स्थिति की जानकारी दी।


यह मैसेज फर्जी है। कोई मेरी तस्वीर का इस्तेमाल करके आपको ठग रहा है। आपने मुझे सीधे फोन क्यों नहीं किया ?
अब, मैं समझ सकता हूँ कि छद्मवेश के जरिए मेरे साथ धोखाधड़ी की जा रही थी।
जल्द ही बॉस के चैंबर में एक आवश्यक बैठक आयोजित की गई।


आजकल, धोखेबाज वरिष्ठ अधिकारियों / संगठनों के शीर्ष प्रबंधन की तस्वीर के साथ, व्हाट्सएप, टेलीग्राम आदि जैसे त्वरित संदेश ऐप के माध्यम से फर्जी संदेश भेज रहे हैं और सहयोगियों से तत्काल मौद्रिक सहायता की मांग कर रहे हैं।
चेतावनी संकेत
संस्था के वरिष्ठ अधिकारियों/शीर्ष प्रबंधन से आने का दिखावा करता है।
तत्काल कार्रवाई के लिए दबाव बनाना।
तत्काल मौद्रिक सहायता की मांग करना, जैसे गुमनाम खाते में धन हस्तांतरण, उपहार कार्ड खरीदना
फोन पर किसी निश्चित अवधि के लिए संबंधित अधिकारी/शीर्ष प्रबंधन की अनुपलब्धता के बारे में सूचित करना।
अनजान व्हाट्सएप नंबर से आने वाले संदेशों पर भरोसा न करें।
किसी भी अजनबी के कहने पर कभी भी पैसे का लेन-देन न करें या गिफ्ट कार्ड न खरीदें।
संदेश की प्रामाणिकता की पुष्टि हमेशा संबंधित व्यक्ति को फोन करके या ज्ञात विश्वसनीय स्रोतों से करें।

फर्जी जुर्माना

फर्जी संदेशों/कॉल के माध्यम से ई-चालान घोटाले पर कहानी

एक दिन राजू को उसके मोबाइल पर एक एसएमएस आया।

राजू को ट्रैफिक उल्लंघन का संदेश देखकर आश्चर्य हुआ। पिछले हफ्ते से उसकी बाइक खराब हो गई है और चल नहीं रही है।

कुछ मिनट बाद उसे एक अज्ञात नंबर से कॉल आया।

राजू को कुछ समझ में नहीं आ रहा था। असमंजस में पड़कर उसने अपने दोस्त 'साइबर-रक्षक' को फोन करके सारी बात बताई।

फिर राजू ने भी अपनी गाड़ी के नंबर से चेक किया लेकिन उसे अपनी गाड़ी के खिलाफ कोई चालान जारी नहीं मिला।

राजू को तुरंत ही पता चल गया कि यह एक फर्जी चालान नंबर था जिसका इस्तेमाल धोखेबाज ने उसे धोखा देने के लिए किया था।

यूको बैंक
UCO BANK

अरे नहीं!!
मुझे लूट लिया गया है!!!

यदि आप

साइबर अपराध

के शिकार हैं,

तो सही समय पर सही जगह
पर हथौड़ा मारें!

1930

पर कॉल करें और

http//:cybercrime.gov.in

पर अपनी शिकायत दर्ज करें

धोखाधड़ी

वाले कॉल और मैसेज से
परेशान हैं?

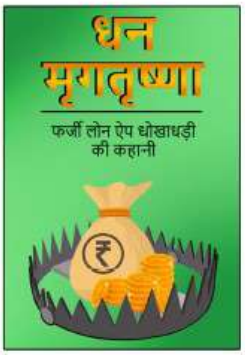
चक्षु पोर्टल
पर जाएं

https://sancharsaathi.gov.in

पर संदिग्ध धोखाधड़ी कॉल,
एसएमएस या व्हाट्सएप
संदेशों की रिपोर्ट करें

परिशिष्ट


भ्रामक डायलर
नकली ग्राहक सेवा खतरे पर कहानी


धन मृगतृष्णा
फर्जी लोन ऐप धोखाधड़ी की कहानी


कूरियर साजिश
पार्सल डिलीवरी के बहाने घोटाला


भ्रामक डेव
निवेश विश्वासघात की कहानी


डिजिटल धोखा
यूपीआई और क्यूआर कोड के माध्यम से किराये के घोटाले की कहानी


फेडेक्स घोटाला
पार्सल में ड्रग्स के धोखे का पर्दाफाश


कार्य समस्या
कार्य आधारित नौकरी प्रस्ताव जाल पर कहानी


गहरी दुविधा
आर्टिफिशियल इंटेलिजेंस आधारित घोटाले पर कहानी


मालिक का विश्वासघात
कॉर्पोरेट धोखे के गलियारों में सामने आने वाला साइबर घोटाला


फर्जी जुर्माना
फर्जी संदेशों/कॉल के माध्यम से ई-चालान घोटाले पर कहानी


साइबर नेत्र
जागरूकता की शक्ति
साइबर चेतना का
पूर्वानुमान करें!
डिजिटल सतर्कता
को सशक्त बनायें!
अपनी आभासी
सीमा को सुरक्षित करें
हमारी आधिकारिक वेबसाइट पर जाएँ: WWW.UCOBANK.COM
यूको बैंक
(भारत सरकार का उपक्रम)
UCO BANK
(A Govt. of India Undertaking)
सम्मान आपके विश्वास का
Honours Your Trust