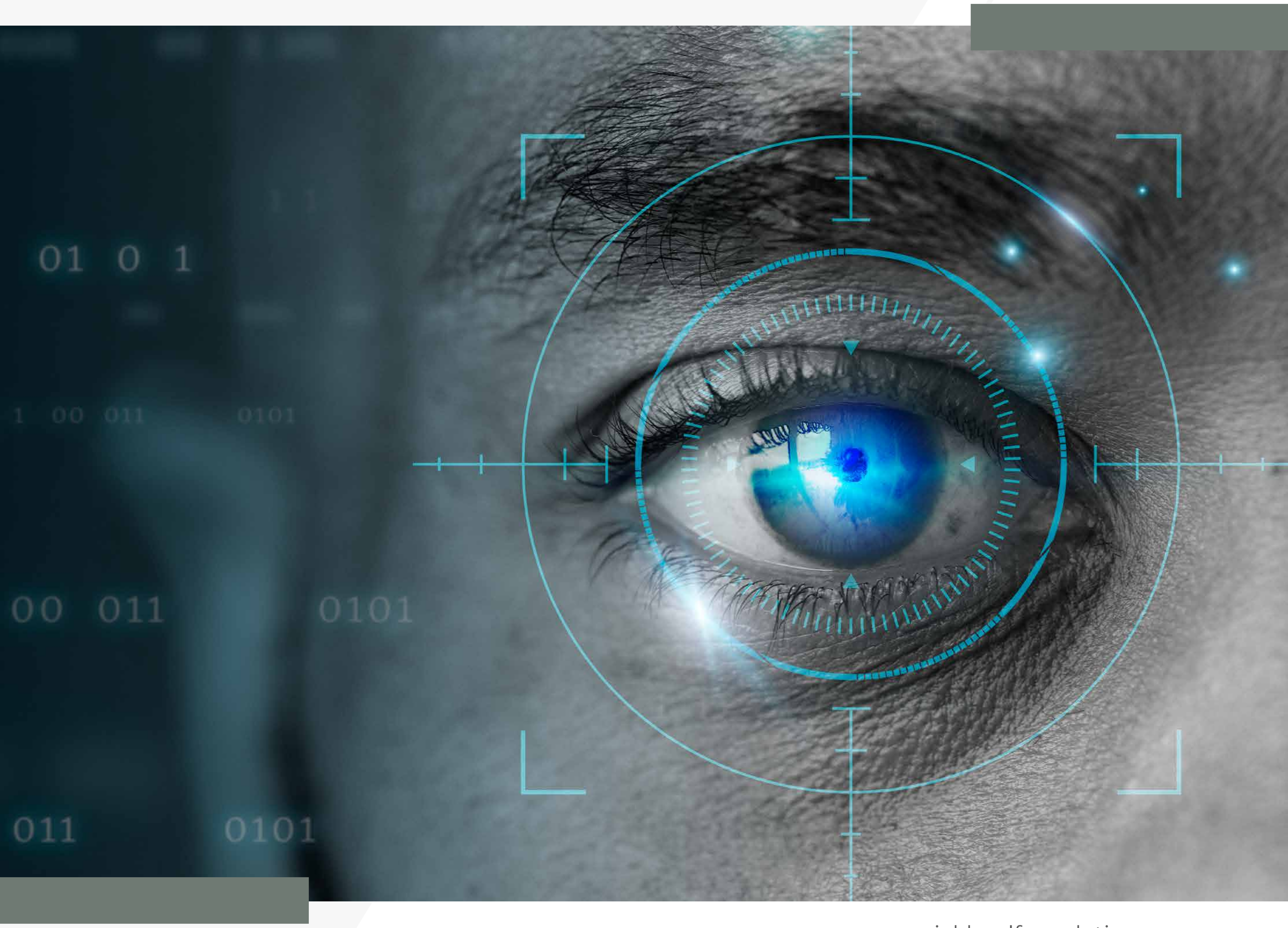
Quick Heal
Foundation

क्विक हिल फाउंडेशन
साइबर जागरूकता पर ईबुक



www.quickhealfoundation.org

क्या आपको ऑनलाइन धोखा दिया गया है?

साइबर अपराध

के शिकार लोगों के लिए एक गाइड

Quick Heal
Foundation

क्विक हिल फाउंडेशन
साइबर जागरूकता पर ईबुक

विषय–सूची

Quick Heal
Foundation

क्विक हील फाउंडेशन के बारे में

क्विक हील फाउंडेशन भारत की अग्रणी साइबर सुरक्षा उत्पादों और समाधान कंपनी, क्विक हील टेक्नोलॉजीज लिमिटेड की सीएसआर शाखा है। हमने अपनी यात्रा में एक नया पाठ्यक्रम तैयार करने के लिए सुरक्षा को सरल बनाने में २५ से अधिक वर्षों के अनुभव का लाभ उठाया है – 'सिक्योरिंग फ्यूचर्स' की दिशा में।

कॉर्पोरेट सामाजिक जिम्मेदारी में हमारी पहल संयुक्त राष्ट्र सतत विकास लक्ष्यों द्वारा उल्लिखित विकास के लिए चुनौतियों का सामना करती है। शिक्षा को बढ़ावा देने, और रोजगार वृद्धि, व्यावसायिक प्रशिक्षण और साइबर सुरक्षा जागरूकता के उद्देश्य से किए गए प्रयासों के माध्यम से, हम इन वैश्विक बाधाओं के लिए नवीन और प्रौद्योगिकी-आधारित समाधान प्रदान करना चाहते हैं। क्विक हील फाउंडेशन द्वारा कार्यान्वित, इनमें से प्रत्येक पहल सभी के लिए सफलता और सुरक्षा के वादे के साथ भविष्य सुनिश्चित करने में मदद करती है।

परिचय

आज के इंटरनेट युग में साइबर घोटाले कोई नई बात नहीं है!

हर दिन, चोर नई शिकार की तलाश में रहते हैं। और अगर आपको लगता है कि आप एक छात्र हैं या साइबर क्राइम का निशाना बनने लायक नहीं हैं? फिर से विचार करे!

हैकर्स इस बात की परवाह नहीं करते कि आपके बैंक खातों में कितना बैलेंस है। वे चोरी करने और उससे पैसे कमाने की कोशिश करते हैं। चाहे आपकी पहचान हो या आपका डेटा, उनके लिए सब कुछ मूल्यवान है। वे यह दिखाने की कोशिश करते हैं कि आप लक्ष्य नहीं हैं!

वे आपकी सभी जानकारी प्राप्त करने का प्रयास करते हैं और आपको एक लक्ष्य के रूप में भी तैयार कर सकते हैं, जो आपके द्वारा किए गए अपराधों के लिए आपको और अधिक दंडित कर सकता है। इसलिए, साइबर खतरों से सावधान रहें और साइबर शिकार न बनें्। सतर्क रहें!

आपको सभी खतरों से सुरक्षित रखने के लिए, सूचना प्रौद्योगिकी अधिनियम २००० पारित किया गया था जिसे साइबर खतरों को पहचानने, कम करने और रोकने के लिए पेश किया गया था। इसलिए यदि आपको ऑनलाइन धोखा दिया गया है या आप साइबर अपराध का शिकार हो गए हैं, तो आपको आगे की आवश्यक कार्रवाई करने के लिए इस अधिनियम के बारे में पता होना चाहिए्।

सामान्यत: रिपोर्ट किए जाने वाले साइबर अपराधों की सुचि मे साइबर स्टॉकिंग, पोर्नोग्राफी, मॉर्फिंग, ऑनलाइन उत्पीड़न, मानहानि या कष्टप्रद संदेश, ट्रोलिंग या बदमाशी, ब्लैकमेलिंग, धमकी, ईमेल स्पूफिंग, प्रतिरूपण आदि शामिल हैं्।

यह पुस्तिका छात्रों के लिए साइबर दुनिया में साइबर धोखाधड़ी के बारे में और डिजिटल रूप से सुरक्षित रहने के तरीके को समझने के लिए एक संपूर्ण मार्गदर्शिका है।

Quick Heal
Foundation

ऋण आवेदन धोखाधड़ी

इस तरह की धोखाधड़ी कम आय वाले समूहों/गरीब लोगों पर लक्षित होती है, जिन्हें कम पैसे की आवश्यकता होती है और जिनके पास गवाह के लिए गिरवी या गारंटर के लिए कुछ भी नहीं होता है।

धोखेबाज व्यक्ति/ऐप की पहचान कैसे करें?

- बिना किसी गारंटर, गिरवी या दस्तावेज़ीकरण के छोटी राशि (२००० - २५०००) का ऋण दिया जाता है।
- बिना मांगे या मांगे जाने पर तुरंत ऋण प्रदान किया जाता है।
- कभी-कभी आपके खाते में पैसे जमा करने के लिए सिर्फ एक पूछताछ ही काफी होती है।
- आपको ईमेल, फोन, टेक्स्ट मैसेज, व्हाट्सएप मैसेज के जरिए लगातार आकर्षक ऑफर मिलते रहेंगे।
- कोई भी आपसे व्यक्तिगत रूप से नहीं मिलेगा या उनके कार्यालय का पता साझा नहीं करेगा।

उत्पीड़न को कैसे रोकें?

- सोशल मीडिया पर साझा किए गए ऐप्स/लिंक पर कभी भरोसा न करें।
- कोई भी संस्था या व्यक्ति कुछ गिरवी रखे बिना या दस्तावेज़, गारंटर के बिना ऋण प्रदान नहीं करता है।
- इसलीये व्यक्तिगत रूप से कार्यालय मे जाने पर जोर दें।
- व्यक्ति से मिले बिना मौजूदा ग्राहक के वीडियो बाइट्स पर विश्वास न करें्।
- इंटरनेट पर ऋण की पेशकश करने वाले संगठन की वेबसाइट, स्थानीय पता, संपर्क विवरण, और पदाधिकारियों के नाम, संपर्क विवरण आदि पर जाकर उनके विवरण की जांच करें्।

Quick Heal
Foundation

उत्पीड़न के मामले में उठाए जाने वाले कदम

एक बार जब पीड़ित को आत्म-पीड़ित होने का एहसास हो जाता है, तो धोखेबाज को जवाब देना बंद कर देना चाहिए। एक जालसाज आपके विवरण को अन्य सिंडिकेट को दे सकता है जो आप से पैसे निकालने के लिए किसी अन्य तारिके को अपना सकता है। जाल में फंसने के बाद इन चरणों का पालन करना सुनिश्चित करें।

01

अगर आपको धमकी भरे कॉल/संदेश मिलते हैं तो घबराएं नहीं और आगे भुगतान करना बंद कर दें।

02

इस धोखाधड़ी के बारे में अपने संपर्कों को सूचित करें और उन्हें अपनी ओर से भुगतान न करने के लिए कहें।

03

यहां तक कि आपकी संपर्क सूची को भी उनकी विकृत तस्वीरों के साथ धमकियां मिल सकती हैं, लेकिन घबराएं नहीं; इसके बजाय, पुलिस को रिपोर्ट करें।

04

कॉल/चैट इतिहास, भुगतान इतिहास आदि जैसे सभी साक्ष्य एकत्र/संकलित करें।

05

ऐप, साझा किए गए लिंक, या ऐसे धोखे-बाजों की संख्या जैसे किसी सबूत को न हटाएं जो पुलिस को आगे की जांच और कार्रवाई करने में मदद कर रहे हैं।

06

नजदीकी साइबर पुलिस स्टेशन को रिपोर्ट करें / स्थानीय पुलिस स्टेशन से मदद ले।

07

पुलिस से कुछ भी न छुपाएं।

08

रिपोर्टिंग के लिए, आप हेल्पलाइन १९३० (गृह मंत्रालय, भारत सरकार द्वारा) पर कॉल कर सकते हैं या राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in/ पर शिकायत दर्ज कर सकते हैं।

Quick Heal
Foundation

वैवाहिक धोखाधड़ी

यह धोखाधड़ी सीमा शुल्क धोखाधड़ी के साथ में भी हो सकती है और आमतौर पर विवाह साइटस के माध्यम से जीवन साथी की तलाश करने वाले व्यक्तियों के साथ हो सकती है।

धोखेबाज व्यक्ति की पहचान कैसे करें?

- हाल की/नई आकर्षक प्रोफ़ाइल (५-१५ दिन पुरानी) नौकरी/व्यवसाय से आय को उजागर करती है।
- फ़ोटोग्राफ़ शानदार जीवन शैली दिखाते हैं - एक बंगले के सामने सेल्फ़ी, स्विमिंग पूल, ५-सितारा होटल, और ब्रांडेड पोशाक, घड़ियाँ और अन्य सामान पहने हुए मॉल में खीची हुई तस्वीरे।
- कोई सोशल मीडिया विवरण साझा नहीं किया जाता है, या यदि साझा किया जाता है, तो प्रोफ़ाइल न्यूनतम मित्रों के साथ हाल ही की है।
- सभी संवाद ऑडियो या व्हाट्सएप कॉल पर होते हैं। यदि आप वीडियो कॉल पर जोर देते हैं, तो यह घर/कार्यालय के बाहर होता है - ज्यादातर सार्वजनिक स्थानों पर जहां बहुत शोर हैं ।
- वे विश्वास हासिल करते हैं और पीड़ित को विश्वास दिलाते हैं कि परिवार का कोई भी सदस्य उनके साथ नहीं रहता है; इसलिए, परिवार के सदस्यों के साथ संवाद संभव नहीं है।

Quick Heal
Foundation

उत्पीड़न को कैसे रोकें?

परिवार के सदस्यों के साथ व्यक्तिगत बैठकों/वीडियो कॉल के बिना किसी प्रस्ताव पर विश्वास न करें।

उनके सोशल मीडिया अकाउंट और फ्रेंड लिस्ट चेक करने पर जोर दें। साथ ही दोस्तों की फ्रेंड लिस्ट चेक करना न भूलें।

अगर आप उस व्यक्ति से नहीं मिले हैं, तो मेडिकल इमरजेंसी की स्थिति में भी कभी भी पैसे न भेजें।

व्यक्तिगत रूप से मिले बिना कभी भी कोई उपहार स्वीकार न करें।

याद रखें, सीमा शुल्क अधिकारी कभी भी फॉर्म भरने की औपचारिकता के बिना ऑनलाइन निपटान के लिए नहीं कहते हैं।

अगर उपहार असली है, तो यह आपके शहर (डाकघर जहां आपका पता है) तक पहुंच जाएगा।

आपको दिल्ली, मुंबई या ऐसी किसी भी जगह पर कस्टम से कॉल कभी नहीं आऐगी।

डाकघर से एक कॉल आपको डाकघर जाने, शुल्क का भुगतान करने और अपने उपहार प्राप्त करने के लिए कहेगी।

Quick Heal
Foundation

उत्पीड़न के मामले में उठाए जाने वाले कदम

एक बार जब पीड़ित को पता चलता है कि उन्हें धोखा दिया गया है, तो व्यक्ति चिंतित हो जाता है और भुगतान करने से इनकार करके प्रतिशोध करना शुरू कर देता है। फिर धोखेबाज विकृत छवियों और वीडियो से डराकर, उन्हें अपने दोस्तों और रिश्तेदारों के साथ साझा करके, भुगतान न करने की शिकायत दर्ज करके, आदि द्वारा ब्लैकमेल करना शुरू कर देता है।

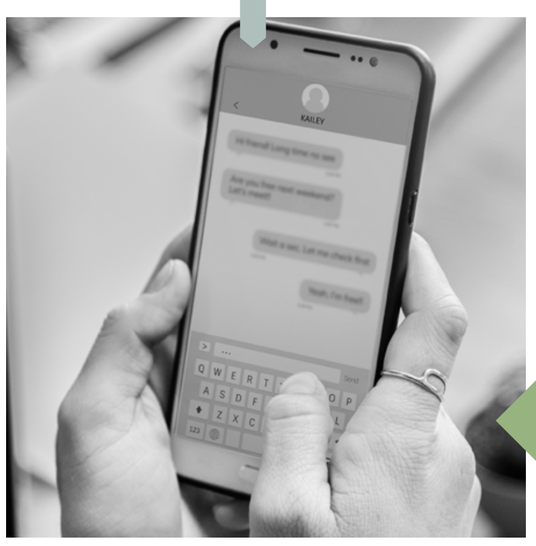
पीड़ित होने के बाद निम्नलिखित कदम उठाए जाने चाहिए:

01

धोखेबाज को जवाब देना बंद करें।

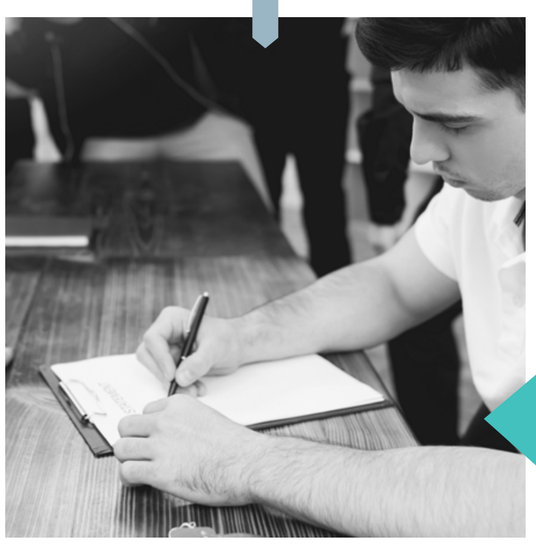
02

आगे भुगतान न करें।



03

कॉल/चैट इतिहास, भुगतान इतिहास आदि जैसे सभी साक्ष्य एकत्र/संकलित करें।



04

नजदीकी साइबर पुलिस स्टेशन को रिपोर्ट करें और स्थानीय पुलिस स्टेशन से मदद लें।

05

ऐप, शेयर किए गए लिंक, या धोखेबाजों की संख्या जैसे सबूत मिटाएं नहीं – इससे पुलिस को जांच करने और कार्रवाई करने में मदद मिलती है।

06

पुलिस से कुछ भी न छुपाएं।

07

कॉल हेल्पलाइन १९३०
(गृह मंत्रालय, भारत सरकार द्वारा)

08

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
https://cybercrime.gov.in/
पर शिकायत की रिपोर्ट करें।

Quick Heal
Foundation

नौकरी धोखाधड़ी

इन धोखाधड़ी के शिकार नए या अनुभवी दोनों हो सकते हैं। नौकरी धोखाधड़ी में, जालसाज उम्मीदवारों को आश्वस्त करता है कि अगर वे अपनी भुगतान क्षमता को देखते हुए ५ हजार रुपये से आगे की राशि का भुगतान कर सकते हैं तो उन्हें नौकरी मिल सकती है।

धोखेबाज की पहचान कैसे करें?

- एचआर हेड, सेल्स हेड आदि जैसे उच्च पदों पर किसी से कॉल आने पर।
- इंटरव्यू टेलीफोन पर होगा।
- सीधे प्रश्न् पूछे जाएंगे।
- इंटरव्यू के दौरान आपके ज्ञान, उपलब्धियों, या किसी व्यक्तिगत कारण से आपकी प्रशंसा की जाएगी।
- आपको उसी इंटरव्यू कॉल में आपके चयन के बारे में सूचित किया जाएगा।
- आपको ढेर सारे अनुलाभों/सुविधाओं के साथ आपकी अपेक्षा से अधिक वेतन की चर्चा की जाती है।

Quick Heal
Foundation

उत्पीड़न को कैसे रोकें?

- सोशल मीडिया पर साझा किए गए ऐप्स/लिंक्स/वेबसाइटों पर कभी भरोसा न करें।
- भले ही आपको ऑफर लेटर मिले, कंपनी पर जाएं और ऑफर लेटर के बारे में पुष्टि करें।
- कोई भी प्रमुख एक ही कॉल पर कॉल नहीं करेगा और साक्षात्कार आयोजित नहीं करेगा।
- प्रशिक्षण के लिए भुगतान करने के लिए कभी भी सहमत न हों। कोई भी कंपनी अलग से कोई प्रशिक्षण शुल्क नहीं मांगती है।
- प्रशिक्षण अवधि के दौरान आपको कम वेतन या कोई वेतन नहीं मिल सकता है।
- काम करने के रिमोट मोड के मामले में, कभी भी भुगतान न करें।
- अपना खाता विवरण साझा करते समय सावधान रहें। कार्ड विवरण साझा न करें – वेतन को आपके खाते में स्थानांतरित करने की आवश्यकता नहीं है।

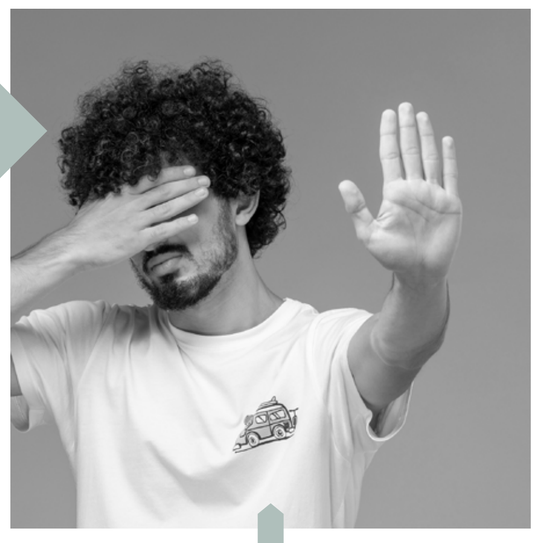
उत्पीड़न के मामले में उठाए जाने वाले कदम

एक बार जब पीड़ित को पता चलता है कि उन्हें धोखा दिया गया है, तो व्यक्ति चिंतित हो जाता है और भुगतान करने से इनकार करके प्रतिशोध करना शुरू कर देता है। फिर धोखेबाज विकृत छवियों और वीडियो के माध्यम से डराकर, उन्हें अपने दोस्तों और रिश्तेदारों के साथ साझा करने की धमकी देना, भुगतान न करने की शिकायत दर्ज करके ब्लैकमेल करना शुरू कर देता है।

यदि आपको पता चलता है कि आप जाल के शिकार हैं, तो इन कदमों को आगे बढ़ाना सुनिश्चित करें:

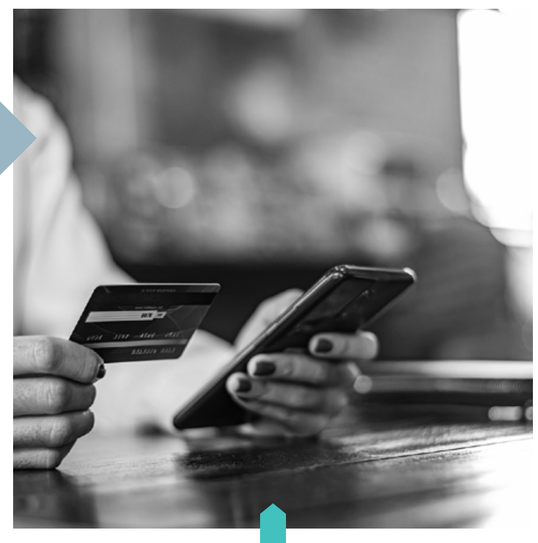
01

धोखेबाज को जवाब देना बंद करें।



02

आगे भुगतान न करें।



03

कॉल/चैट इतिहास, भुगतान इतिहास आदि जैसे सभी साक्ष्य एकत्र/संकलित करें।

04

नजदीकी साइबर पुलिस स्टेशन को रिपोर्ट करें और स्थानीय पुलिस स्टेशन से मदद लें।

05

ऐप, शेयर किए गए लिंक, या धोखेबाजों की संख्या जैसे सबूत मिटाएं नहीं – इससे पुलिस को जांच करने और कार्रवाई करने में मदद मिलती है।

06

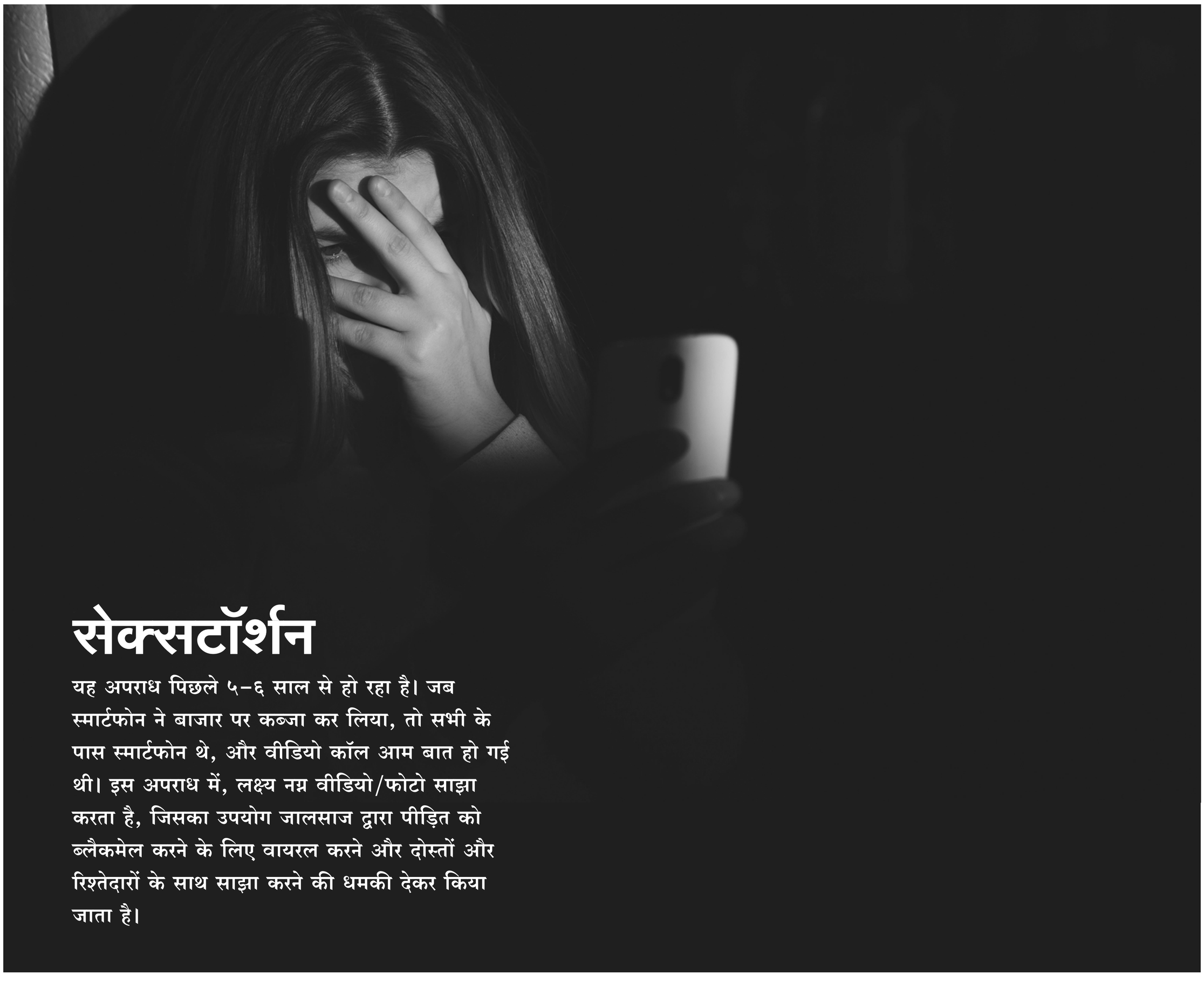
पुलिस से कुछ भी न छुपाएं।

07

कॉल हेल्पलाइन १९३०
(गृह मंत्रालय, भारत सरकार द्वारा)

08

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
https://cybercrime.gov.in/
पर शिकायत की रिपोर्ट करें।



सेक्सटॉर्शन

यह अपराध पिछले ५-६ साल से हो रहा है। जब स्मार्टफोन ने बाजार पर कब्जा कर लिया, तो सभी के पास स्मार्टफोन थे, और वीडियो कॉल आम बात हो गई थी। इस अपराध में, लक्ष्य नग्न वीडियो/फोटो साझा करता है, जिसका उपयोग जालसाज द्वारा पीड़ित को ब्लैकमेल करने के लिए वायरल करने और दोस्तों और रिश्तेदारों के साथ साझा करने की धमकी देकर किया जाता है।

इस धोखाधड़ी को कैसे रोकें?

- कभी भी उच्च-रिज़ॉल्यूशन वाली फ़ोटो या वीडियो सोशल मीडिया पर साझा न करें।
- सोशल मीडिया पर कभी भी अपने अकेले स्टेटस का प्रचार न करें।
- कभी भी अपने असली नाम और अन्य विवरणों का उपयोग टिंडर जैसे ऐप्स पर न करें।
- अनजान नंबरों से कभी भी वीडियो कॉल का जवाब न दें।
- कभी भी अपने अंतरंग फ़ोटो/वीडियो को किसी के द्वारा कैप्चर न करने दें।
- यदि आपको किसी अज्ञात नंबर से वीडियो कॉल में भाग लेना है, तो कैमरे को कवर करना सुनिश्चित करें।

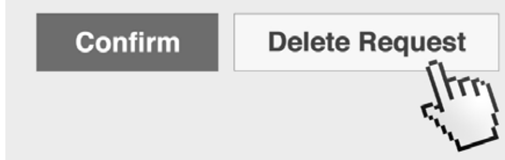
Quick Heal
Foundation

उत्पीड़न के मामले में उठाए जाने वाले कदम

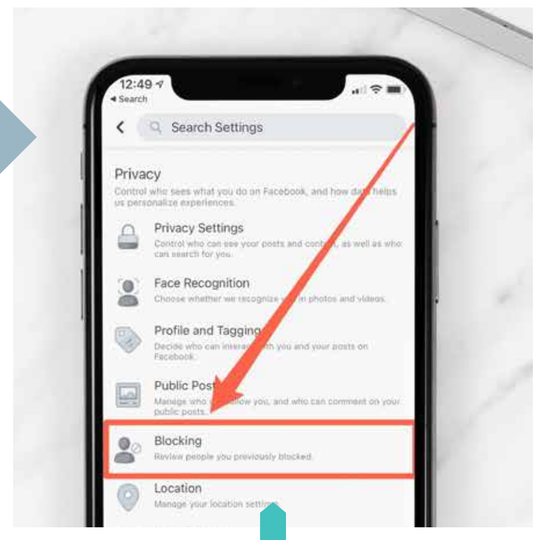
एक बार जब पीड़ित को पता चलता है कि उन्हें धोखा दिया गया है, तो व्यक्ति चिंतित हो जाता है और भुगतान करने से इनकार करके प्रतिशोध करना शुरू कर देता है। फिर धोखेबाज विकृत छवियों और वीडियो के माध्यम से डराकर, उन्हें अपने दोस्तों और रिश्तेदारों के साथ साझा करने की धमकी देना, भुगतान न करने की शिकायत दर्ज करके ब्लैकमेल करना शुरू कर देता है।

यदि आपको पता चलता है कि आप जाल के शिकार हैं, तो इन कदमों को आगे बढ़ाना सुनिश्चित करें:

01 –
धोखेबाज को जवाब देना बंद करें।



02 –
सोशल मीडिया पर रिपोर्ट और ब्लॉक विकल्प का उपयोग करें।



03 –
एफबी, इंस्टाग्राम, या इसी तरह के मीडिया के मामले में, अपने सभी सोशल मीडिया मित्रों को ऐसा करने के लिए कहें।

04 –
अपने सभी सोशल मीडिया कनेक्शनों को साइबर अपराध के बारे में सूचित करें और जब तक आप उन्हें नियमित कॉल पर व्यक्तिगत रूप से कॉल न करें, तब तक आपसे किसी कॉल/संदेश का जवाब न दें।

05
कॉल/चैट इतिहास, भुगतान इतिहास आदि जैसे सभी साक्ष्य एकत्र/संकलित करें।

06
ऐप, शेयर किए गए लिंक, या धोखेबाजों की संख्या जैसे सबूत मिटाएं नहीं – इससे पुलिस को जांच करने और कार्रवाई करने में मदद मिलती है।

07
नजदीकी साइबर पुलिस स्टेशन को रिपोर्ट करें/स्थानीय पुलिस स्टेशन से मदद लें।

08
पुलिस से कुछ भी न छुपाएं।

09
कॉल हेल्पलाइन १९३०
(गृह मंत्रालय, भारत सरकार द्वारा)

10
राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in/ पर शिकायत की रिपोर्ट करें।

Quick Heal
Foundation

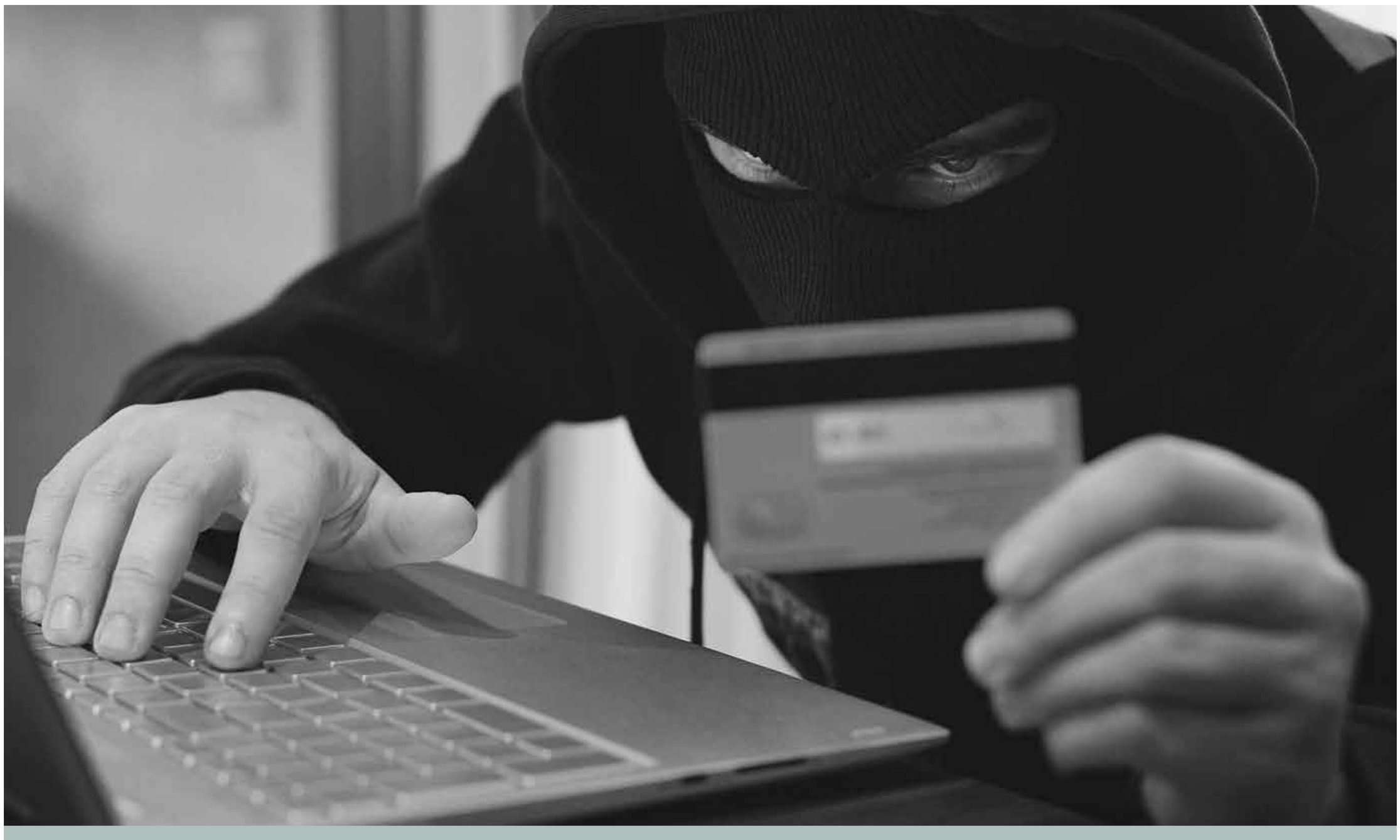
वित्तीय धोखाधड़ी

लोग बिना कोई विवरण साझा किए खातों से अपना पैसा खो देते हैं। यदि आपको यह संदेश मिलता है कि आपका बैंक बैलेंस शून्य है, तो अपने बैंक में जाएं और बैंक अधिकारियों को इसके बारे में सूचित करें्। विवाद फॉर्म भरें और कॉल पर ओटीपी या कोई अन्य विवरण साझा न करें्।

कैसे पहचानें?

- आपको एक कॉल (कभी-कभी संदेश) प्राप्त होगी जो विभिन्न कारणों जैसे एटीएम कार्ड ब्लॉकेज, बिजली कटौती, या बैंक खाता निष्क्रिय करने के लिए तात्कालिकता की भावना पैदा करेगी।
- आपको लिंक के माध्यम से भुगतान करने के लिए कहा जाएगा
- आपको जन्म तिथि, माता का नाम, पता आदि जैसे विवरण साझा करने के लिए कहा जाएगा।

  आपसे ओटीपी/पिन/कोड जैसे विवरण साझा करने के लिए कहा जाएगा।
- आपको अपना डेबिट/क्रेडिट कार्ड नंबर, सीवीवी (ग्राहक सत्यापन मूल्य), आदि साझा करने के लिए कहा जाएगा।
- आपको ऐप डाउनलोड करने के लिए कहा जाएगा / लिंक पर क्लिक करें / कुछ चाबियाँ दबाकर अपने डिवाइस तक पहुंच प्रदान करें।
- ईमेल के लिए, अंग्रेजी के उपयोग की जांच करें क्योंकि इसमें उचित व्याकरण नहीं हो सकता है या वर्तनी की कुछ गलतियां हो सकती हैं।



कैसे बचाना है

- फोन कॉल्स या संदेशों पर कभी भी विश्वास न करें। बैंक कभी भी आपकी व्यक्तिगत जानकारी नहीं मांगता
- कभी भी ओटीपी (वन टाइम पासवर्ड) को अनजान व्यक्ति से साझा न करें। औटीपी शेयर करने से पुलसि को करवाई करने में दक्कित होगी।
- ओटीपी की तरह ही सीवीवी नंबर, माता का मायके का नाम, जन्मतिथि का भी पासवर्ड या गुप्त प्रश्नों के उत्तर के रूप में उपयोग किया जाता है।

उत्पीड़न के मामले में क्या करना है?

1. बैंक में विवाद फ़ॉर्म भरें।
2. पुलिस स्टेशन/साइबर सेल को सूचित करें।
3. कॉल/चैट इतिहास, भुगतान इतिहास आदि जैसे सभी साक्ष्य एकत्र/संकलित करें्।
4. ऐप, शेयर किए गए लिंक, या धोखेबाजों की संख्या जैसे सबूत मिटाएं नहीं – इससे पुलिस को जांच करने और कार्रवाई करने में मदद मिलती है।
5. नजदीकी साइबर पुलिस स्टेशन को रिपोर्ट करें/स्थानीय पुलिस स्टेशन से मदद लें।
6. पुलिस से कुछ भी न छुपाएं।
7. कॉल हेल्पलाइन १९३० (गृह मंत्रालय, भारत सरकार द्वारा)।
8. राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cyber-crime.gov.in/ पर शिकायत की रिपोर्ट करें।

साइबर बुलिइंग

यह प्रौद्योगिकी के उपयोग से लोगों को परेशान करने, धमकाने और शर्मिंदा करने का कार्य है। गुमनाम व्यक्तियों के रूप में ऑनलाइन बदमाशी हानिकारक है, या एक ज्ञात व्यक्ति आमतौर पर ऐसा करता है लेकिन अपनी पहचान छुपाता है।

साइबर बुलिइंग एसएमएस, टेक्स्ट और ऐप्स के माध्यम से या सोशल मीडिया, फ़ोरम या गेमिंग में ऑनलाइन हो सकती है जहां लोग देख सकते हैं, इसमें भाग ले सकते हैं या साझा कर सकते हैं।

साइबर बुलिइंग पीड़ित के लक्षण

- मोबाइल, लैपटॉप या टैबलेट के उपयोग में उल्लेखनीय वृद्धि या कमी।
- उनके सोशल मीडिया खातों को अचानक निष्क्रिय करना या नए खाते खोलना।
- अन्य लोगों के पास होने पर डिवाइस स्क्रीन को छिपाना।
- भावनात्मक प्रतिक्रियाओं का प्रदर्शन जैसे उदासी, क्रोध, अवसाद, वापसी के लक्षण।
- ऑनलाइन गतिविधियों पर चर्चा से बचने की प्रवृत्ति।

लोगों का लक्षित तबका

- ज्यादातर बच्चे, शर्मीले छात्र, बुद्धिमान छात्र जो अंतर्मुखी होते हैं।

Quick Heal
Foundation

प्रार्थना की पहचान कैसे की जाती है? और लोग कैसे फंसते हैं?

सोशल मीडिया पर फ्रेंड रिक्वेस्ट भेजकर और वॉट्सऐप के जरिए कम्युनिकेट कर टारगेट की पहचान की जाती है। कभी-कभी, लक्ष्य को ऑफ़लाइन पहचाना जाता है, और लोगों का एक समूह बनाकर साइबरबुलिंग शुरू की जाती है।

साइबर अपराध और उसके परिणामों के बारे में जानकारी के बिना किशोरों द्वारा अक्सर बदमाशी की जाती है। यह हरकत मजे के लिए या बदला लेने के लिए की जाती है।

पीड़ित होने के बाद निम्नलिखित कदम उठाए जाने चाहिए:

1. धोखेबाज को प्रत्युत्तर देना बंद करें।
2. अपने परिवार/दोस्त या भरोसेमंद किसी के साथ सब कुछ साझा करें।
3. कॉल/चैट इतिहास, भुगतान इतिहास आदि जैसे सभी साक्ष्य एकत्र/संकलित करें।
4. ऐप, शेयर किए गए लिंक, या धोखेबाजों की संख्या जैसे सबूत मिटाएं नहीं – इससे पुलिस को जांच करने और कार्रवाई करने में मदद मिलती है।
5. नजदीकी साइबर पुलिस स्टेशन को रिपोर्ट करें/स्थानीय पुलिस स्टेशन से मदद लें।
6. पुलिस से कुछ भी न छुपाएं।
7. रिपोर्टिंग निम्न तरीकों से की जा सकती है – हेल्पलाइन १९३० पर कॉल करें (गृह मंत्रालय, भारत सरकार द्वारा)
8. राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in/ पर शिकायत की रिपोर्ट करें।

ऑनलाइन टास्क फ्रॉड

ऑनलाइन टास्क फ्रॉड में आम तौर पर पीड़ितों को फंसाना शामिल होता है, जो अपने खाली समय में घर से काम करने के अवसर या किसी अन्य स्रोत से आय की तलाश में रहते हैं, उन्हें सरल कार्य करके बदले में पैसे देने का वादा करते हैं।

धोखेबाज व्यक्ति/ऐप की पहचान कैसे करें?

- **अनचाहे संदेश:** आमतौर पर इसकी शुरुआत व्हाट्सएप या टेलीग्राम पर अनचाहे संदेशों से होती है।
- **झूठे वादे:** लचीले घंटों के साथ घर से काम करना, जिसके लिए किसी अनुभव या विशिष्ट कौशल सेट की आवश्यकता नहीं होती है।
- **फ़िशिंग वेबसाइट:** किसी कंपनी की वेबसाइट का लिंक संदेश में शामिल हो सकता है, जो किसी प्रतिष्ठित कंपनी की क्लोन या फ़िशिंग वेबसाइट है।
- **भुगतान की विधि:** दैनिक या साप्ताहिक आधार पर (कभी-कभी क्रिप्टोकरेंसी में) भुगतान की पेशकश करता है
- **झूठा विश्वास निर्माण:** शुरुआती दिनों में आपको अपना विश्वास हासिल करने के लिए भुगतान प्राप्त हो सकता है
- **भुगतान के लिए अनुरोध:** अधिक पैसा कमाने के लिए, आपसे प्रीमियम शुल्क का भुगतान करने के लिए कहा जाएगा, जो आमतौर पर आपकी अब तक की कमाई से थोड़ा कम होगा
- **भुगतान प्रक्रिया:** आपसे विभिन्न तरीकों से भुगतान करने के लिए कहा जाएगा जैसे क्यूआर कोड को स्कैन करना, नेट बैंकिंग आदि, और हर बार, आपको बताया जाएगा कि भुगतान सफल नहीं हुआ।

उत्पीड़न को कैसे रोकें?

- **अनचाहे संदेशों से बचें:** साधारण कार्यों के लिए उच्च भुगतान या घर से काम करने के अवसरों का वादा करने वाले अनचाहे संदेशों से सावधान रहें।
- **वेबसाइट की वैधता की जाँच करें:** आगे बढ़ने से पहले वेबसाइट का पता और उसकी वैधता सत्यापित करें।
- **भुगतान से पहले पुष्टि:** यदि भुगतान करने के लिए कहा जाए तो कंपनी की वैधता की पुष्टि किए बिना ऐसा करने से बचें।

उत्पीड़न के मामले में उठाए जाने वाले कदम

एक बार जब पीड़ित को आत्म-पीड़ित होने का एहसास हो जाता है, तो धोखेबाज को जवाब देना बंद कर देना चाहिए। एक जालसाज आपके विवरण को अन्य सिंडिकेट को दे सकता है जो आप से पैसे निकालने के लिए किसी अन्य तरिके को अपना सकता है

जाल में फंसने के बाद इन चरणों का पालन करना सुनिश्चित करें।

1. अगर आपको धमकी भरे कॉल/संदेश मिलते हैं तो घबराएं नहीं और आगे भुगतान करना बंद कर दें
2. इस धोखाधड़ी के बारे में अपने संपर्कों को सूचित करें और उन्हें अपनी ओर से भुगतान न करने के लिए कहें
3. यहां तक कि आपकी संपर्क सूची को भी उनकी विकृत तस्वीरों के साथ धमकियां मिल सकती हैं, लेकिन घबराएं नहीं; इसके बजाय,पुलिस को रिपोर्ट करें
4. कॉल/चैट इतिहास, भुगतान इतिहास आदि जैसे सभी साक्ष्य एकत्र/संकलित करें।
5. ऐप, शेयर किए गए लिंक, या धोखेबाजों की संख्या जैसे सबूत मिटाएं नहीं – इससे पुलिस को जांच करने और कार्रवाई करने में मदद मिलती है।
6. नजदीकी साइबर पुलिस स्टेशन को रिपोर्ट करें/स्थानीय पुलिस स्टेशन से मदद लें।
7. पुलिस से कुछ भी न छुपाएं।
8. रिपोर्टिंग के लिए, आप हेल्पलाइन १९३० (गृह मंत्रालय, भारत सरकार द्वारा) पर कॉल कर सकते हैं या राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in/ पर शिकायत की रिपोर्ट करें।

सोशल मीडिया मार्केटप्लेस धोखाधड़ी

सोशल मीडिया मार्केटप्लेस धोखाधड़ी में किसी कंपनी के माध्यम से झूठे या भ्रामक दावे करना शामिल है, जैसे विज्ञापन में उत्पाद या सेवा की गुणवत्ता को बढ़ा-चढ़ाकर बताना, नकली उत्पादों को वास्तविक उत्पादों के रूप में बेचना, या नकारात्मक पहलुओं या दुष्प्रभावों को छिपाना। गलत विज्ञापन बाज़ार में धोखाधड़ी का एक सामान्य रूप है।

धोखेबाज व्यक्ति/ऐप की पहचान कैसे करें?

- आकर्षक ऑफर वाले आकर्षक विज्ञापन
- असामान्य उत्पाद जो आमतौर पर Amazon या Flipkart जैसे लोकप्रिय प्लेटफार्मों पर नहीं मिलते हैं।

उत्पीड़न को कैसे रोकें?

- उत्पाद की कीमत की तुलना में उसकी गुणवत्ता और मूल्य का आकलन करें
- खरीदारी करने से पहले विक्रेता की वैधता और उत्पाद की प्रामाणिकता को सत्यापित करें
- ऑर्डर देने से पहले विक्रेता से उनकी आधिकारिक वेबसाइट के माध्यम से संवाद करने का प्रयास करें

Quick Heal
Foundation

उत्पीड़न के मामले में उठाए जाने वाले कदम

1. अगर आपको धमकी भरे कॉल/संदेश मिलते हैं तो घबराएं नहीं और आगे भुगतान करना बंद कर दें
2. इस धोखाधड़ी के बारे में अपने संपर्कों को सूचित करें और उन्हें अपनी ओर से भुगतान न करने के लिए कहें
3. यहां तक कि आपकी संपर्क सूची को भी उनकी विकृत तस्वीरों के साथ धमकियां मिल सकती हैं, लेकिन घबराएं नहीं; इसके बजाय,पुलिस को रिपोर्ट करें
4. कॉल/चैट इतिहास, भुगतान इतिहास आदि जैसे सभी साक्ष्य एकत्र/संकलित करें।
5. ऐप, शेयर किए गए लिंक, या धोखेबाजों की संख्या जैसे सबूत मिटाएं नहीं – इससे पुलिस को जांच करने और कार्रवाई करने में मदद मिलती है।
6. नजदीकी साइबर पुलिस स्टेशन को रिपोर्ट करें/स्थानीय पुलिस स्टेशन से मदद लें।
7. पुलिस से कुछ भी न छुपाएं।
8. रिपोर्टिंग के लिए, आप हेल्पलाइन १९३० (गृह मंत्रालय, भारत सरकार द्वारा) पर कॉल कर सकते हैं या राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in/ पर शिकायत की रिपोर्ट करें।

नई धोखाधड़ी योजना चेतावनी: जालसाजों द्वारा इस्तेमाल की जाने वाली नई रणनीति से सावधान रहें

हाल ही में, धोखाधड़ी का एक नया तरीका सामने आया है, जिसमें झूठा दावा करके व्यक्तियों का शोषण किया जाता है कि दवाओं से भरा एक कूरियर उनके नाम पर प्राप्त हुआ है या उनके द्वारा भेजा गया है। एक अन्य घोटाले में व्यक्तियों को यह सूचित करना कि उनके बेटे या बेटी को एक रेव पार्टी में भाग लेने के लिए हिरासत में लिया गया है, स्थिति को सुलझाने के लिए पैसे की मांग करना शामिल है।

धोखेबाज व्यक्ति/ऐप की पहचान कैसे करें?

- अवैध पदार्थों से युक्त कूरियर प्राप्त करने के असामान्य दावे
- रेव पार्टी में भाग लेने के लिए परिवार के एक सदस्य को हिरासत में लेने का दावा
- समाधान के लिए तत्काल भुगतान की मांग

उत्पीड़न को कैसे रोकें?

- कानूनी परेशानी का दावा करने वाले अनचाहे संदेशों या कॉल पर कभी भरोसा न करें
- कोई भी कार्रवाई करने से पहले आधिकारिक चैनलों के माध्यम से दावों की पुष्टि करें
- दावों की प्रामाणिकता की पुष्टि किए बिना कोई भी भुगतान करने से इंकार करें
- यदि स्थिति संदिग्ध लगती है, तो आधिकारिक पते पर व्यक्तिगत रूप से मिलने पर जोर दें

उत्पीड़न के मामले में उठाए जाने वाले कदम

1. अगर आपको धमकी भरे कॉल/संदेश मिलते हैं तो घबराएं नहीं और आगे भुगतान करना बंद कर दें
2. इस धोखाधड़ी के बारे में अपने संपर्कों को सूचित करें और उन्हें अपनी ओर से भुगतान न करने के लिए कहें
3. यहां तक कि आपकी संपर्क सूची को भी उनकी विकृत तस्वीरों के साथ धमकियां मिल सकती हैं, लेकिन घबराएं नहीं; इसके बजाय,पुलिस को रिपोर्ट करें
4. कॉल/चैट इतिहास, भुगतान इतिहास आदि जैसे सभी साक्ष्य एकत्र/संकलित करें़।
5. ऐप, शेयर किए गए लिंक, या धोखेबाजों की संख्या जैसे सबूत मिटाएं नहीं – इससे पुलिस को जांच करने और कार्रवाई करने में मदद मिलती है।
6. नजदीकी साइबर पुलिस स्टेशन को रिपोर्ट करें/स्थानीय पुलिस स्टेशन से मदद लें।
7. पुलिस से कुछ भी न छुपाएं।
8. रिपोर्टिंग के लिए, आप हेल्पलाइन १९३० (गृह मंत्रालय, भारत सरकार द्वारा) पर कॉल कर सकते हैं या राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल https://cybercrime.gov.in/ पर शिकायत की रिपोर्ट करें।

सतर्क रहें! अपने भविष्य की रक्षा करें।

- मुफ़्त वाई-फ़ाई का इस्तेमाल न करें।
- लाइसेंस प्राप्त और अद्यतन एंटीवायरस का उपयोग करें।
- फोन पर पासवर्ड स्टोर न करें।
- मजबूत पासवर्ड का प्रयोग करें और इसे बार-बार बदलें।
- विश्वसनीय ऐप से ऐप्स डाउनलोड करें।
- टोरेंट साइटों का उपयोग न करें।
- लाइसेंस प्राप्त और अद्यतन ऑपरेटिंग सिस्टम का उपयोग करें।

Quick Heal
Foundation

क्विक हील फाउंडेशन

Regd. Address: S. No. 207/1A, "Marvel Edge", C Building,
7th Floor, Office No 7010 Viman Nagar, Pune - 411014
Contact: +91-20-41467229
E-Mail: contact@quickhealfoundation.org
Website: www.quickhealfoundation.org