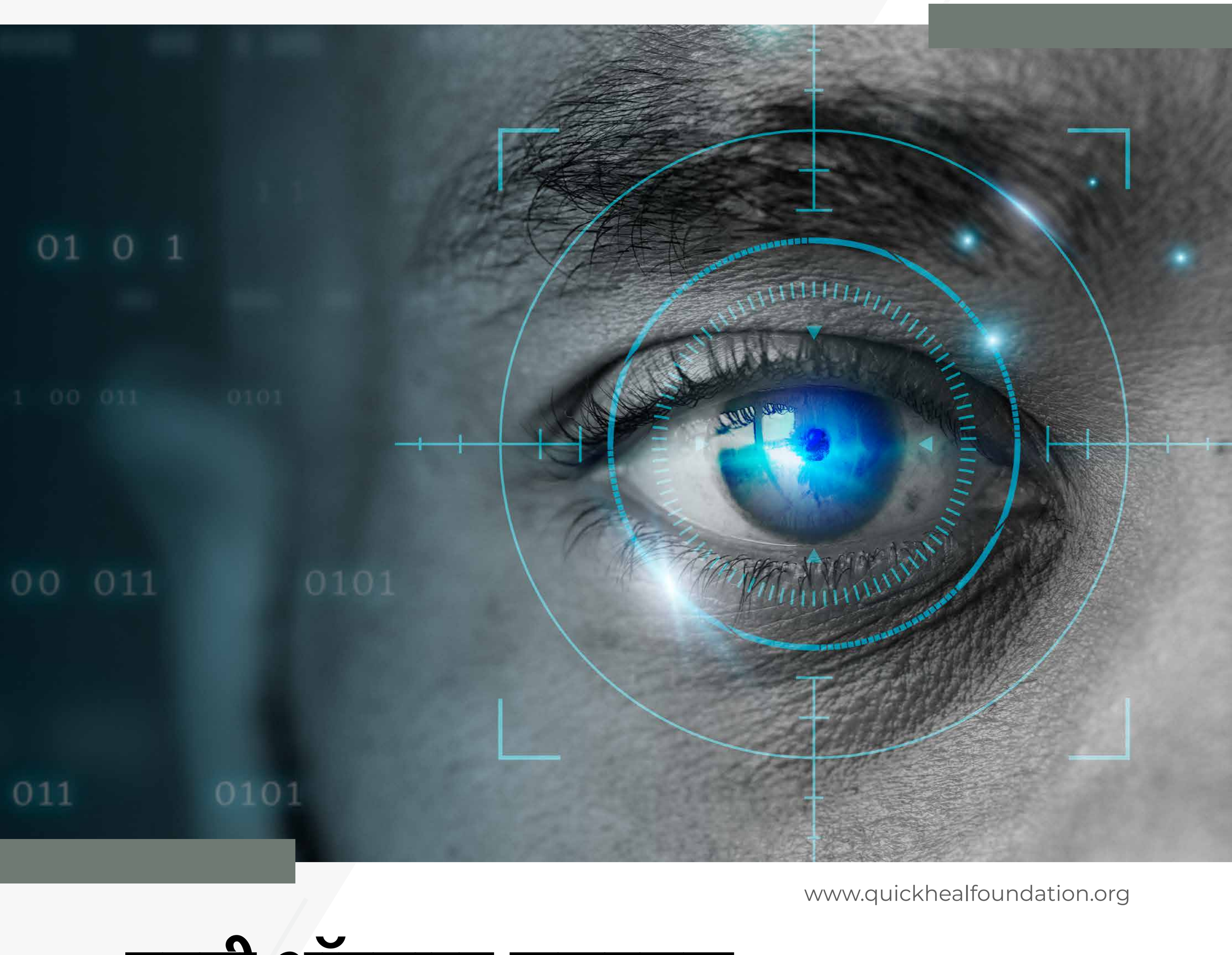
Quick Heal
Foundation

# क्विक हिल फाउंडेशन
# सायबर जागरूकता–ईबुक




## तुमची ऑनलाइन फसवणूक झाली आहे का?

**सायबर**

गुन्ह्यातील
पीडितांसाठी
मार्गदर्शिका

Quick Heal
Foundation

# क्विक हिल फाउंडेशन
# सायबर जागरूकता–ईबुक

## विषय–सूची

# क्विक हील फाउंडेशन बद्दल

क्विक हील फाउंडेशन ही भारतातील आघाडीची सायबर सुरक्षा उत्पादने आणि सोल्यूशन्स आधारित कंपनी क्विक हील टेक्नॉलॉजीज लिमिटेडची CSR शाखा आहे. सुरक्षितता सुलभ करण्यासाठी २५ वर्षांच्या अनुभवाचा फायदा घेऊन आम्ही 'भविष्य सुरक्षित करण्याच्या' दिशेने आमच्या प्रवासात एक नवीन संधी उपलब्ध करून दिली आहे.

कॉर्पोरेट सामाजिक उत्तरदायित्वातील आमचे उपक्रम संयुक्त राष्ट्रांच्या शाश्वत विकास उद्दिष्टांद्वारे वर्णन केलेल्या विकासासमोरील आव्हानांना सामोरे जातात. शिक्षणाचा प्रचार, आणि रोजगार वृद्धी, व्यावसायिक प्रशिक्षण आणि सायबरसुरक्षा जागरूकता या उद्देशाने केलेल्या प्रयत्नांद्वारे, आम्ही या जागतिक अडथळ्यांवर नाविन्यपूर्ण आणि तंत्रज्ञान आधारित उपाय प्रदान करण्याचा प्रयत्न करतो. क्विक हील फाऊंडेशनद्वारे राबविण्यात आलेले, यापैकी प्रत्येक उपक्रम सर्वांसाठी यश आणि सुरक्षिततेच्या वचनासह भविष्य सुनिश्चित करण्यात मदत करतो.


# परिचय

## सायबर घोटाळे काही नवीन संकल्पना नाही

कारण फसवणूक करणारी व्यक्ती रोज काहींना काहीतरी नवीन शोधत असते.जर तुम्हाला वाटत असेल की तुम्ही विद्यार्थी आहात आणि सायबर गुन्हेगार तुम्हाला टार्गेट करत नाहीत? तर पुन्हा विचार करा.

हॅकर्सना तुमच्या बँक खात्यात किती रक्कम आहे हे जाणून घेण्याची गरज नाही. तुमची ओळख, तुमचा डेटा, तुमच्या ईमेलमध्ये काय आहे, हे महत्वाचे वाटते. तुम्ही टार्गेट नाही असे ते तुम्हाला भासवतात.

जर तुमची ऑनलाइन फसवणूक झाली असेल किंवा तुम्ही सायबर गुन्ह्यांचे बळी ठरला असाल, तर तुम्हाला माहिती असणे आवश्यक आहे की अश्या धोक्यांना ओळखण्यासाठी, कमी करण्यासाठी आणि रोखण्यासाठी माहिती तंत्रज्ञान कायदा २००० लागू करण्यात आला आहे.

सामान्य आणि वारंवार नोंदवल्या जाणाऱ्या सायबर गुन्ह्यांमध्ये सायबरस्टॉकिंग, पोर्नोग्राफी, मॉर्फिंग, ऑनलाइन छळ, बदनामीकारक किंवा त्रासदायक संदेश, ट्रोलिंग किंवा गुंडगिरी, ब्लॅकमेलिंग, धमकी देणे, ईमेल फसवणूक, तोतयागिरी इत्यादींचा समावेश आहे.

या पुस्तिकेत तुम्हाला सायबर फसवणूक कशी होते आणि आभासी जगात सुरक्षित कसे राहायचे याबद्दल माहिती मिळेल.

Quick Heal
Foundation

# कर्जाद्वारे फसवणूक


या प्रकारची फसवणूक कमी-उत्पन्न गट/गरीब लोकांवर लक्ष्यित केली जाते. ज्यांना थोड्या कर्जाऊ रकमेची आवश्यकता असते आणि ज्यांना तारण ठेवण्यासाठी काहीही नसते किंवा कोणतेही हमीदार नसतात, अशांची कर्ज अँप द्वारे फसवणूक होऊ शकते.

## फसवणूक करणारी व्यक्ती/अॅप कशी ओळखायची?

- कमी रकमेचे कर्ज (२००० - २५०००) कोणत्याही गॅरेंटर,तारण किंवा कागदपत्रांशिवाय देऊ केले जाते.
- कर्ज न मागता किंवा तुम्ही जेव्हा मागता तेव्हा लगेच दिले जाते.
- काही वेळा तुमच्या खात्यात कर्जाऊ रक्कम जमा करण्यासाठी फक्त चौकशी पुरेशी असते.
- तुम्हाला ईमेल, फोन, टेक्स्ट मेसेज, व्हॉट्स ऍप मेसेजद्वारे सतत आकर्षक ऑफर दिल्या जातात.
- कोणीही तुम्हाला प्रत्यक्ष भेटत नाही किंवा कार्यालयाचा पत्ता सांगत नाही.

## फसवणूक रोखायची कशी?

- सोशल मीडियावर शेअर केलेल्या अॅप्स/लिंकवर कधीही विश्वास ठेवू नका.
- कागदपत्रे, गॅरेंटर किंवा काहीही तारण ठेवल्याशिवाय कोणीही कर्ज देत नाही.
- कार्यालयात प्रत्यक्ष भेट देण्याचा आग्रह धरा.
- व्यक्तीला भेटल्याशिवाय फसव्या ग्राहकांच्या बोलण्यावर विश्वास ठेवू नका.
- इंटरनेटवर कर्ज देणाऱ्या संस्थेचे तपशील, स्थानिक पत्ता, संपर्क तपशील आणि पदाधिकारी यांची नावे घेऊन त्यांना भेटून त्यांचे तपशील तपासा.

# अपराधाला बळी पडलेल्या व्यक्तींनी उचलावयाची पावले

एकदा पीडित व्यक्तीला स्वत:ची शिकार झाल्याचे समजले की, त्यांनी फसवणूक करणाऱ्यांना प्रतिसाद देणे थांबवावे – वाद घालू नये. फसवणूक करणारा तुमचा तपशील इतर गुन्हेगारांना देऊ शकतो जो तुमचा तपशील उदा. मॉर्फ केलेला फोटो पैसे उकळण्यासाठी वापरू शकतो.

**01**

तुम्हाला धमकीचे कॉल/मेसेज येत असल्यास घाबरू नका आणि पुढे पैसे देणे थांबवा

**02**

फसवणुकीबद्दल तुमच्या संपर्कांना कळवा आणि त्यांना तुमच्या वतीने पैसे न देण्यास सांगा.

**03**

तुमच्या संपर्क यादीला त्यांच्या मॉर्फ केलेल्या फोटोंसह धमक्याही मिळू शकतात,परंतु घाबरू नका, त्याऐवजी पोलिसांकडे तक्रार करा.

**04**

कॉल/चॅट, पेमेंट हिस्ट्री इत्यादी सारखे सर्व पुरावे संकलित करा.

**05**

ॲप, शेअर केलेल्या लिंक्स, फसवणूक करणाऱ्यांचा तपशील  यासारखे कोणतेही पुरावे मिटवू नका यामुळे पोलिसांना तपास करण्यात आणि कारवाई करण्यास मदत होते.

**06**

जवळच्या सायबर पोलिस स्टेशनमध्ये तक्रार करा किंवा स्थानिक पोलिस स्टेशनची मदत घ्या.

**07**

पोलिसांपासून काहीही लपवू नका.

**08**

तक्रार करण्यासाठी तुम्ही हेल्पलाइन १९३० (गृह मंत्रालय, भारत सरकारद्वारे) वर कॉल करू शकता किंवा राष्ट्रीय सायबर क्राइम रिपोर्टिंग पोर्टल https://cybercrime.gov.in/ वर तक्रार नोंदवू शकता.

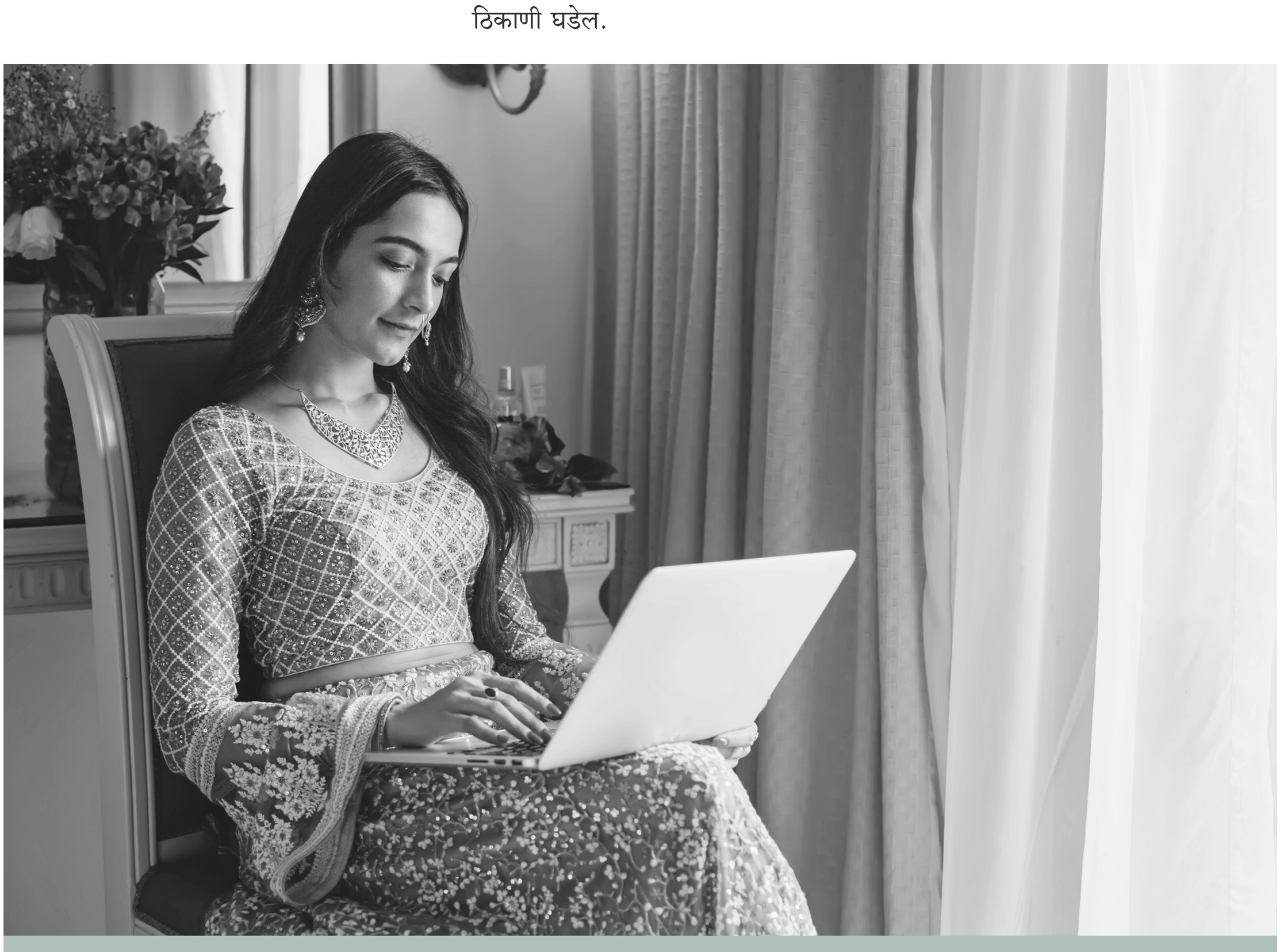
Quick Heal
Foundation

# विवाह फसवणूक

या फसवणूकी सोबत सीमाशुल्क फसवणुकदेखील होऊ शकते.
मुखत्वे विवाह साइटद्वारे जीवन साथी शोधत असलेल्या व्यक्तीसोबत घडते.

## ही फसवणूक करणारी व्यक्ती कशी ओळखावी?

- नवीन प्रोफाइल (५ – १५ दिवस जुने) जे नोकरी/व्यवसायातून मिळणारे उत्पन्न प्रामुख्याने दर्शवते.
- श्रीमंत जीवनशैली दर्शवणारी छायाचित्रे, जसे बंगल्यासमोर सेल्फी, स्विमिंग पूल, ५-स्टार हॉटेल्स, ब्रँडेड वस्तू जसे घड्याळ, फोन असलेले मॉल मधील फोटो इत्यादी
- कोणतेही सोशल मीडिया तपशील ते शेअर करत नाहीत आणि जर ते शेअर केले असतील तर, ती प्रोफाइल अगदी नवीन आणि मर्यादित मित्रांसह दिसेल .
- सर्व संवाद व्हॉट्स ऍप कॉलवर केवळ ऑडिओवर होतात. जर तुम्ही व्हिडिओ कॉलचा आग्रह धरला तर ते त्यांचे घर / ऑफिस सोडून बाहेरून करतील त्यातील बहुतांश वेळी सार्वजनिक ठिकाणी जिथे खूप गोंगाट असेल अश्या ठिकाणी घडेल.
- तुम्हाला त्यांनी पटवून दिले असेल की कुटुंबातील कोणतेही सदस्य त्याच्यासोबत राहत नाहीत आणि त्यामुळे कुटुंबातील सदस्यांशी संवाद शक्य नाही.



Quick Heal
Foundation

# फसवणूक रोखायची कशी?

कौटुंबिक सदस्यांसह वैयक्तिक भेटी किंवा व्हिडिओ कॉलशिवाय प्रस्तावावर कधीही विश्वास ठेवू नका.

इतर सोशल मीडिया खाती आणि मित्र सूची तपासण्याचा आग्रह धरा. मित्रांची फ्रेंड लिस्ट देखील तपासून पहा.

तुम्ही त्या व्यक्तीला भेटला नसाल तर वैद्यकीय आणीबाणीसाठी पैसे देऊ नका.

प्रत्यक्ष भेटल्याशिवाय कधीही भेटवस्तू स्वीकारू नका.

नेहमी लक्षात ठेवा कस्टम अधिकारी फॉर्म भरण्याच्या औपचारिकतेशिवाय कधीही ऑनलाइन सेटलमेंटसाठी विचारत नाहीत.

जर भेटवस्तू खरी असेल तर ती तुमच्या शहरात पोहोचेल – (ज्या पोस्ट ऑफिसमध्ये  तुमचा पत्ता नोंदला आहे).

तुम्हाला कस्टम दिल्ली, मुंबई किंवा अशा कोणत्याही ठिकाणाहून कधीही कॉल येत नाही.

पोस्ट ऑफिसमधून येणारा कॉल तुम्हाला पोस्ट ऑफिसला भेट देऊन, शुल्क भरण्यास आणि भेटवस्तू घेण्यास सांगेल.

# पीडितांनी खालील पावले उचलली पाहिजेत

एकदा पीडिताला स्वत: ची शिकार झाल्याची जाणीव झाली की, व्यक्ती चिंताग्रस्त होते आणि पैसे देण्यास नकार देऊन प्रतिकार करण्यास सुरुवात करते. मग फसवणूक करणारा व्यक्ती मॉर्फ केलेले फोटो आणि व्हिडिओ शेअर करणे, ते तुमच्या मित्रांना, नातेवाईकांना शेअर करणे, पैसे चुकवल्याबद्दल तक्रार दाखल करणे इत्यादी धमक्या देऊन ब्लॅकमेलिंग सुरू करते .

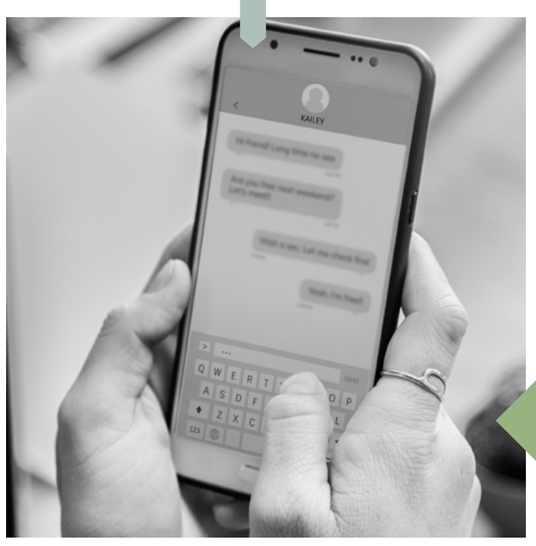
बळी पडल्यानंतर पुढील पावले उचलणे आवश्यक आहे.

**01**

फसवणूक करणाऱ्याला प्रतिसाद देणे थांबवा.

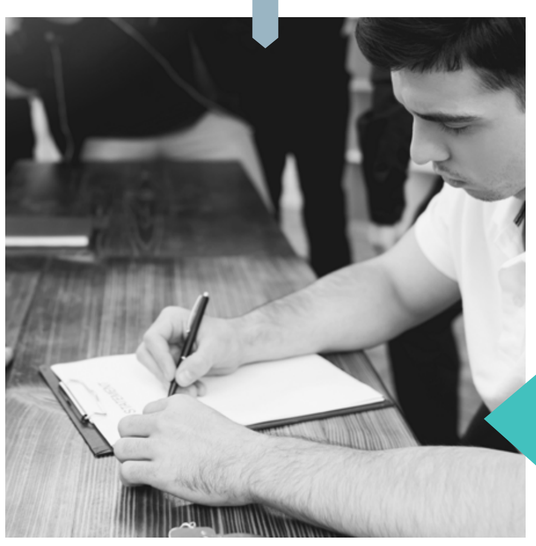
**02**

अजून पैस देऊ नका




**03**

कॉल/चॅट हिस्ट्री , पेमेंट हिस्ट्री इत्यादी सारखे सर्व पुरावे गोळा करा.



**04**

जवळच्या सायबर पोलिस स्टेशनमध्ये तक्रार करा किंवा स्थानिक पोलिस स्टेशनची मदत घ्या.

**05**

ऍप, शेअर केलेल्या लिंक्स, फसवणूक करणाऱ्याचा तपशील यासारखे कोणतेही पुरावे मिटवू नका.- यामुळे पोलिसांना तपास करण्यात आणि कारवाई करण्यास मदत होते.

**06**

पोलिसांपासून काहीही लपवू नका.

**07**

तक्रार करण्यासाठी तुम्ही हेल्पलाइन १९३० (गृह मंत्रालय, भारत सरकारद्वारे) वर कॉल करू शकता

**08**

राष्ट्रीय सायबर क्राइम रिपोर्टिंग पोर्टल https://cybercrime.gov.in/ वर तक्रार नोंदवू शकता.

# नोकरी फसवणूक

या फसवणुकीचे बळी नवीन किंवा अनुभवी दोघेही असू शकतात. नोकरीच्या फसवणुकीमध्ये, फसवणूक करणारा इच्छुकांना पटवून देतो की जर त्यांनी पैसे दिले तर नोकरी मिळू शकते. गुन्हेगार पैसे मागण्याआधी समोरच्या व्यक्तीच्या पैसे देण्याच्या क्षमतेचाअंदाज घेऊन रु.५००० किंवा त्याहून अधिक रकमेची मागणी करतो

## फसवणूक करणारा कसा ओळखायचा?

- एचआर हेड, सेल्स हेड इत्यादीसारख्या उच्च पदावरील व्यक्तीकडून कॉल येऊ शकतो.
- दूरध्वनीद्वारे मुलाखत घेतली जाते.
- अत्यंत सोपे प्रश्न विचारले जातात.
- तुमच्या ज्ञानासाठी, आतापर्यंत मिळालेल्या यशासाठी किंवा कोणत्याही वैयक्तिक कारणास्तव मुलाखतीदरम्यान तुमची प्रशंसा केली जाते
- तुम्हाला तुमच्या निवडीबद्दल त्याच मुलाखतीमध्ये माहिती दिली जाते
- तुम्हाला अनेक भत्ते/सुविधांसह तुमच्या अपेक्षेपेक्षा जास्त पगार देऊ केला जातो

Quick Heal
Foundation

# फसवणूक रोखायची कशी?

- सोशल मीडियावर शेअर केलेल्या ॲप्स/लिंक/वेबसाईटवर कधीही विश्वास ठेवू नका.
- तुम्हाला ऑफर लेटर मिळाले तरीही कंपनीला भेट द्या आणि ऑफर लेटरची खातरजमा करून घ्या.
- कुठलाही अधिकारी स्वतः फोन करून मुलाखत घेत नाही.
- तुम्हाला प्रशिक्षण कालावधीत कमी पगार किंवा छात्रवृत्ती  मिळू शकते किंवा एखादी  कंपनी या कालावधीत तुम्हाला कोणताही मोबदला देणार नाही असेही शक्य आहे पण कोणतीही कंपनी प्रशिक्षण शुल्क मागत नाही. त्यामुळे प्रशिक्षणासाठी शुल्क देण्यास कधीही सहमत होऊ नका.
- रिमोट मोडच्या कामाच्या बाबतीतदेखील कधीही पैसे देऊ नका.
- तुमचे बँक खाते तपशील शेअर करताना काळजी घ्या. कार्ड तपशील शेअर करू नका – आपल्या खात्यात पगार हस्तांतरित करण्यासाठी त्याची आवश्यकता नसते.

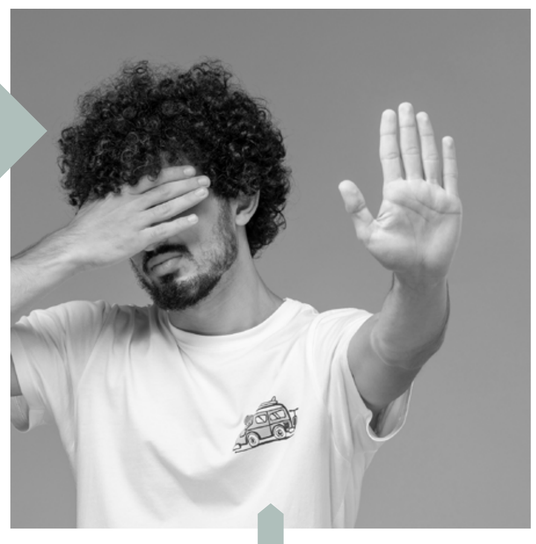
# पीडितांनी घ्यावयाची खबरदारी

एकदा पीडिताला आपली फसवणूक झाल्याचे लक्षात आल्यावर, ती व्यक्ती चिंताग्रस्त होते आणि पैसे देण्यास नकार देऊन बदला घेण्यास सुरुवात करते. मग फसवणूक करणारा मॉर्फ केलेल्या प्रतिमा आणि व्हिडिओ पैसे उकळण्यासाठी वापरू शकतो पीडिताला धमकावून, ते त्यांच्या मित्र आणि नातेवाईकांना पाठवून, पैसे चुकवल्याबद्दल तक्रार नोंदवून ब्लॅकमेल करण्यास सुरुवात करतो.

## आपण पीडित आहात हे लक्षात आल्यास, खालील पावले उचलणे आवश्यक आहे.

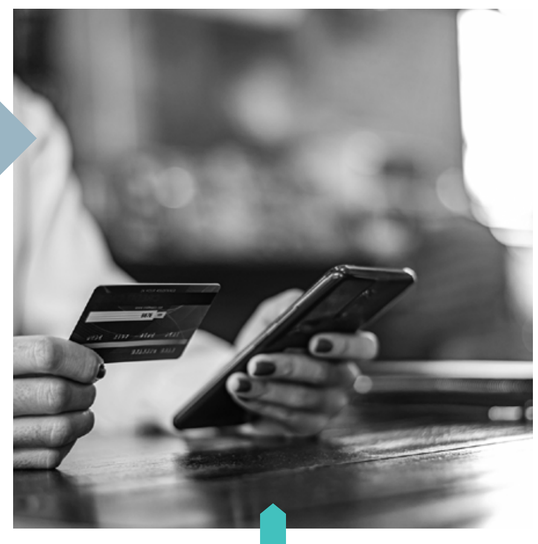
**01**

फसवणूक करणाऱ्याला प्रतिसाद देणे थांबवा



**02**

पुढे पैसे देऊ नका



**03**

कॉल/चॅट हिस्ट्री, पेमेंट हिस्ट्री इत्यादी सारखे सर्व पुरावे गोळा करा.


**04**

जवळच्या सायबर पोलिस स्टेशनमध्ये तक्रार करा किंवा स्थानिक पोलिस स्टेशनची मदत घ्या.

**05**

ॲप, शेअर केलेल्या लिंक्स, फसवणूक करणाऱ्याचा तपशील यासारखे कोणतेही पुरावे मिटवू नका .- यामुळे पोलिसांना तपास करण्यात आणि कारवाई करण्यास मदत होते.

**06**

पोलिसांपासून काहीही लपवू नका.

**07**

तक्रार करण्यासाठी तुम्ही हेल्पलाइन १९३० (गृह मंत्रालय, भारत सरकारद्वारे) वर कॉल करू शकता

**08**

राष्ट्रीय सायबर क्राइम रिपोर्टिंग पोर्टल https://cybercrime.gov.in/ वर तक्रार नोंदवू शकता.

# सेक्सटॉर्शन

गेल्या ५-६ वर्षापासून जेव्हा स्मार्टफोनने बाजारपेठेढ धुमाकूळ घातला आहे तेव्हापासून हा गुन्हा घडत आहे. आता  प्रत्येकाकडे स्मार्टफोन आहेत त्यामुळे व्हिडिओ कॉल करणे सोयीचे झाले आहे.या गुन्ह्यात, नग्न व्हिडिओ/फोटो शेअर केला जातो आणि त्याचा वापर गुन्हेगार समोरच्या व्यक्तीला ब्लॅकमेल करण्यासाठी करतो. असे फोटो किंवा व्हिडीओ व्हायरल करण्याची आणि मित्र व नातेवाईकांना शेअर करण्याची धमकी देतो.

## फसवणूक कशी रोखायची?

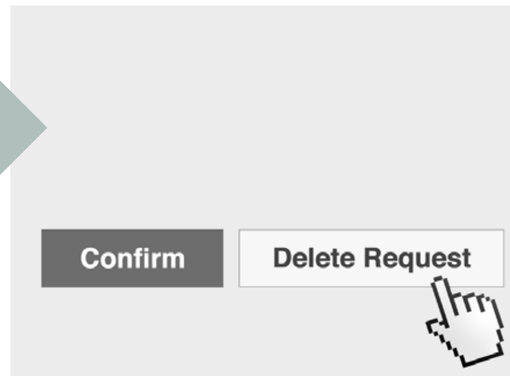
- हाय रिझोल्यूशनचे फोटो, व्हिडिओ सोशल मीडियावर कधीही शेअर करू नका.
- सोशल मीडियावर तुमच्या एकाकी/सिंगल स्टेटसची माहिती देऊ नका.
- टिंडर सारख्या ॲप्सवर तुमचे खरे नाव आणि इतर तपशील कधीही वापरू नका.
- अनोळखी नंबरवरून आलेल्या व्हिडिओ कॉलला प्रतिसाद देऊ नका.
- तुमचे वैयक्तिक फोटो/व्हिडीओ इतरांच्या फोनमध्ये काढू देऊ नका.
- जर तुम्ही अनोळखी नंबरवरून आलेला  व्हिडिओ कॉल उचलणे आवश्यक असेल तर प्रथम कॅमेरा कव्हर करूनच मग तो फोन उचला.

# अपराधाला बळी पडल्यानंतर उचलावयाची पावले

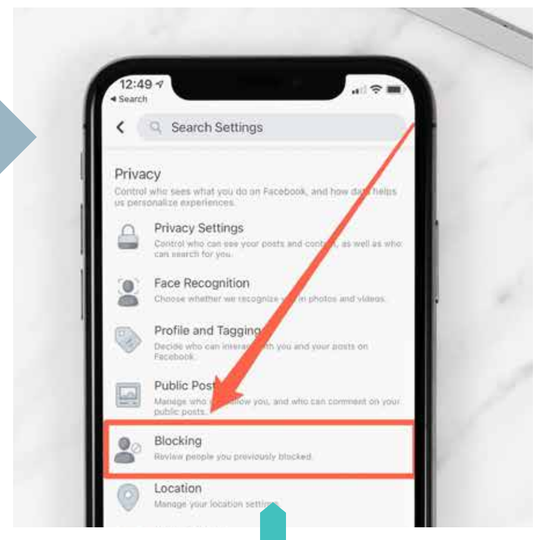
एकदा पीडिताला आपली फसवणूक झाल्याचे लक्षात आल्यावर, ती व्यक्ती चिंताग्रस्त होते आणि पैसे देण्यास नकार देऊन बदला घेण्यास सुरुवात करते. मग फसवणूक करणारा मॉर्फ केलेल्या प्रतिमा आणि व्हिडिओ पैसे उकळण्यासाठी वापरू शकतो  पीडिताला धमकावून, ते त्यांच्या मित्र आणि नातेवाईकांना पाठवून, पैसे चुकवल्याबद्दल तक्रार नोंदवून ब्लॅकमेल करण्यास सुरुवात करतो.

## आपण पीडित आहात हे लक्षात आल्यास, खालील पावले उचलणे आवश्यक आहे.

**01 –**
फसवणूक करणाऱ्याला प्रतिसाद देऊ नका.




**02 –**
सोशल मीडियावर रिपोर्ट आणि ब्लॉक हा पर्याय वापरा.





**03 –**
एफबी, इंस्टाग्राम किंवा तत्सम माध्यमांच्या बाबतीत, तुमच्या सर्व सोशल मीडिया मित्रांना असे करण्यास सांगा

**04 –**
तुमच्या  सोशल मीडियावरील सर्व मित्रांना  सायबर गुन्ह्याबद्दल माहिती द्या. जोपर्यंत तुम्ही स्वतः त्यांना फोन करून काही सांगत नाही किंवा कुठली मागणी करत नाही तोपर्यंत इतर कुठल्याही  कॉल/मेसेजला प्रतिसाद देऊ नका असे त्यांना सांगा

**05**
कॉल/चॅट हिस्ट्री, पेमेंट हिस्ट्री इत्यादी सारखे सर्व पुरावे गोळा करा.

**06**
ऍप, शेअर केलेल्या लिंक्स, फसवणूक करणाऱ्याचा तपशील यासारखे कोणतेही पुरावे मिटवू नका.- यामुळे पोलिसांना तपास करण्यात आणि कारवाई करण्यास मदत होते.

**07**
जवळच्या सायबर पोलिस स्टेशनमध्ये तक्रार करा किंवा स्थानिक पोलिस स्टेशनची मदत घ्या.

**08**
पोलिसांपासून काहीही लपवू नका.

**09**
तक्रार करण्यासाठी तुम्ही हेल्पलाइन १९३० (गृह मंत्रालय, भारत सरकारद्वारे) वर कॉल करू शकता

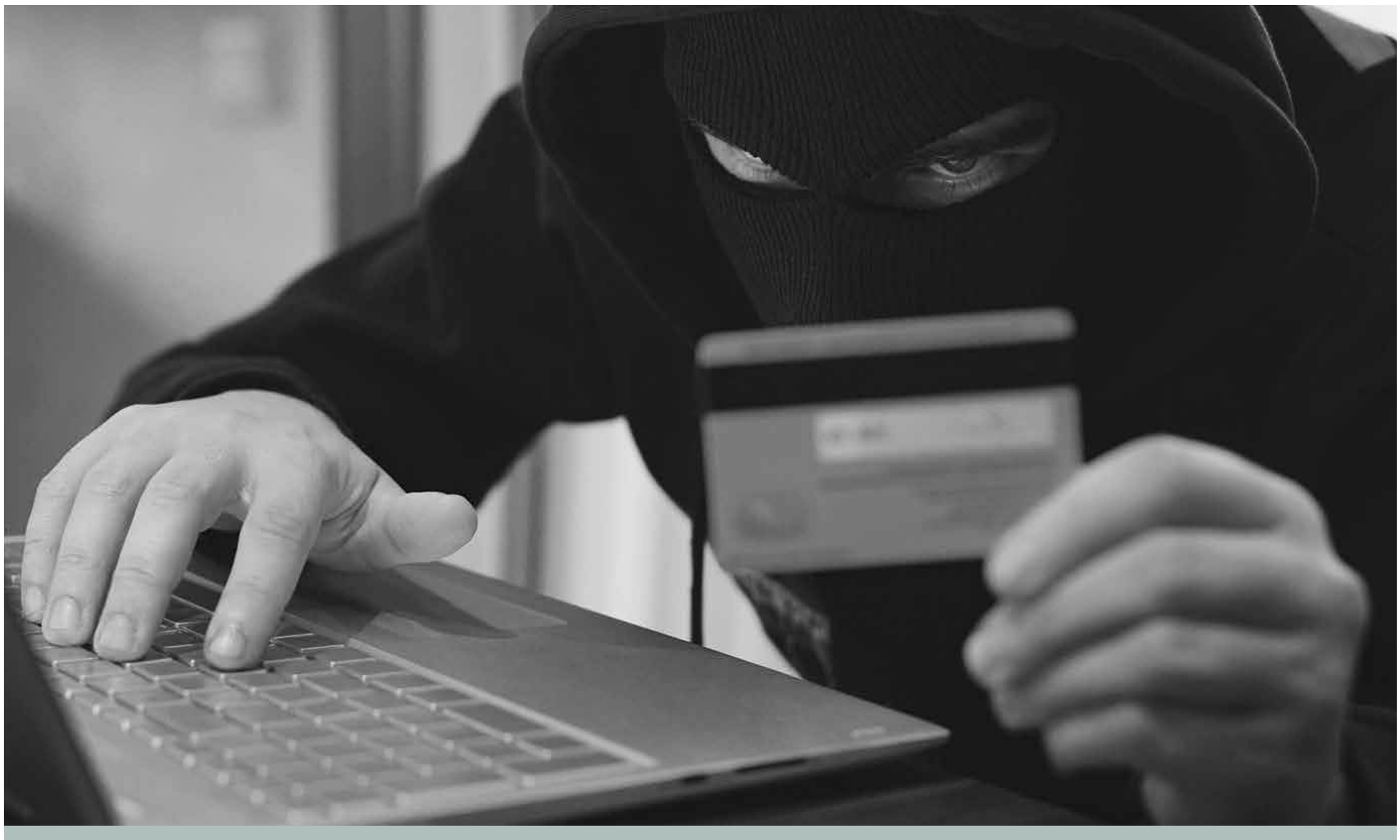
**10**
राष्ट्रीय सायबर क्राइम रिपोर्टिंग पोर्टल https://cybercrime.gov.in/ वर तक्रार नोंदवू शकता.

# आर्थिक फसवणूक

लोक कोणतेही तपशील शेअर न करता खात्यातून पैसे गमावतात. तुमचा बँक बॅलन्स शून्य आहे असा संदेश तुम्हाला मिळाल्यास, तुमच्या बँकेला भेट द्या आणि बँक अधिकाऱ्यांना त्याबद्दल कळवा. विवाद फॉर्म भरा आणि कॉलवर OTP किंवा इतर कोणतेही तपशील शेअर करू नका.

## आर्थिक फसवणूक ओळखायची कशी?

- एटीएम कार्ड बंद केले जाईल, बिल न भरल्याने वीज कपात होणे किंवा केवायसी फॉर्म भरला नाही म्हणून बँक खाते निष्क्रिय करणे यासारख्या विविध कारणांसाठी तुम्हाला कॉल किंवा मेसेज येईल ज्यामध्ये निकडीची भावना निर्माण केली जाईल.
- तुम्हाला लिंकद्वारे पैसे भरण्यास सांगितले जाईल
- तुम्हाला जन्मतारीख, आईचे नाव, पत्ता इत्यादी तपशील शेअर करण्यास सांगितले जाईल.
- तुम्हाला OTP/PIN/code सारखे तपशील शेअर करण्यास सांगितले जाईल.
- तुम्हाला डेबिट/क्रेडिट कार्ड नंबर, CVV (ग्राहक पडताळणी मूल्य) इत्यादी शेअर करण्यास सांगितले जाईल.
- तुम्हाला ॲप डाउनलोड करण्यास, लिंकवर क्लिक करण्यास सांगून किंवा फोनवरील काही बटणे दाबून तुमच्या डिव्हाइसमध्ये प्रवेश करण्याचा प्रयत्न केला जाईल.



## आर्थिक गुन्हे कसे प्रतिबंधित करावे.

- फोन कॉल्स किंवा मेसेजवर कधीही विश्वास ठेवू नका. कारण बँक तुमचा तपशील कधीच विचारत नाही
- OTP (वन टाइम पासवर्ड) कधीही शेअर करू नका, कारण OTP वापर हा ग्राहकांच्या व्यवहाराची पुष्टी करण्यासाठी केला जातो.जर तुम्ही तुमचा OTP शेअर केला तर पोलीस किंवा बँक काहीही करू शकत नाहीत
- OTP प्रमाणेच CVV नंबर, आईचे पूर्वीचे नाव, जन्मतारीख हे बँकेमध्ये पासवर्ड किंवा गुप्त प्रश्नांची उत्तरे म्हणून वापरले जातात.
- ईमेलच्या बाबतीत, इंग्रजीचा वापर तपासा (फसवणूक करणाऱ्या बहुतेक इमेलमध्ये चुकीचे इंग्रजी किंवा शुद्धलेखनाच्या चुका असू शकतात.)

## फसवणूक झाल्यास काय कराल?

1. बँकेत विवाद फॉर्म भरा.
2. पोलीस स्टेशन/सायबर सेलला कळवा.
3. कॉल/चॅट हिस्ट्री, पेमेंट हिस्ट्री इत्यादी सारखे सर्व पुरावे गोळा करा.
4. ऍप, शेअर केलेल्या लिंक्स, फसवणूक करणाऱ्याचा तपशील यासारखे कोणतेही पुरावे मिटवू नका .– यामुळे पोलिसांना तपास करण्यात आणि कारवाई करण्यास मदत होते.
5. जवळच्या सायबर पोलिस स्टेशनमध्ये तक्रार करा किंवा स्थानिक पोलिस स्टेशनची मदत घ्या.
6. पोलिसांपासून काहीही लपवू नका.
7. तक्रार करण्यासाठी तुम्ही हेल्पलाइन १९३० (गृह मंत्रालय, भारत सरकारद्वारे) वर कॉल करू शकता
8. राष्ट्रीय सायबर क्राइम रिपोर्टिंग पोर्टल https://cybercrime.gov.in/ वर तक्रार नोंदवू शकता.

# सायबर बुलिंग


तंत्रज्ञानाचा वापर करून लोकांना त्रास देणे, धमकावणे,मानहानी करणे ह्या कृतीला सायबर बुलिंग म्हणतात. ऑनलाइन छेडखानी सामान्यतः अज्ञात व्यक्ती किंवा ओळखीच्या व्यक्तींद्वारे देखील केली जाते परंतु त्यांची ओळख लपवून ठेवली जाते. म्हणून हा गुन्हा जास्त हानीकारक आहे

ऑनलाइन छेडखानी, सोशल मीडिया फोरम किंवा ऑनलाइन गेमिंग,जिथे लोक सहभागी होऊ शकतात,बोलू शकतात किंवा शेअर करू शकतात अश्या ठिकाणी एसएमएस किंवा ॲप्सद्वारे देखील होऊ शकते.

## सायबर छेडखानीच्या बळींची लक्षणे

- मोबाईल, लॅपटॉप किंवा टॅब्लेटच्या वापरामध्ये लक्षणीय वाढ किंवा घट.
- त्यांची सोशल मीडिया खाती अचानक निष्क्रिय करणे किंवा नवीन उघडणे.
- इतर लोक जवळ असताना डिव्हाईस स्क्रिन लपवणे.
- दुःख, राग, नैराश्य यासारखे भावनिक प्रतिसाद दर्शवणे.
- ऑनलाइन घडामोडींवर चर्चा टाळण्याची प्रवृत्ती.

## लोकांचा लक्ष्यित वर्ग

- मुख्यतः मुले, लाजाळू विद्यार्थी, हुशार विद्यार्थी जे अंतर्मुख आहेत.

## सावज कसे हेरल्या जातात? आणि लोक सापळ्यात कसे अडकतात?

सोशल मीडियावर फ्रेंड रिक्वेस्ट पाठवून, व्हॉट्सॲपद्वारे संवाद साधून सावज हेरल्या जाते. काहीवेळा, सावज प्रत्यक्षात हेरून नंतर लोकांचा गट तयार करून सायबरछेडखानी सुरु होते.

बऱ्याच  वेळा सायबर गुन्ह्यांची आणि त्याच्या परिणामांची माहिती नसल्यामुळे अल्पवयीन मुलांकडून असे कृत्य केले जाते. हे कृत्य गमतीसाठी किंवा बदला घेण्यासाठी देखील केले जाते.

# बळी पडल्यांनंतर पुढील पावले उचलावीत.

1. फसवणूक करणाऱ्याला प्रतिसाद देणे थांबवा.
2. प्रत्येक गोष्ट तुमच्या कुटुंब/मित्र किंवा विश्वासू कोणाशीही शेअर करा.
3. कॉल/चॅट हिस्ट्री , पेमेंट हिस्ट्री इत्यादी सारखे सर्व पुरावे गोळा करा.
4. ऍप, शेअर केलेल्या लिंक्स, फसवणूक करणाऱ्याचा तपशील यासारखे कोणतेही पुरावे मिटवू नका .– यामुळे पोलिसांना तपास करण्यात आणि कारवाई करण्यास मदत होते.
5. जवळच्या सायबर पोलिस स्टेशनमध्ये तक्रार करा किंवा स्थानिक पोलिस स्टेशनची मदत घ्या.
6. पोलिसांपासून काहीही लपवू नका.
7. तक्रार करण्यासाठी तुम्ही हेल्पलाइन १९३० (गृह मंत्रालय, भारत सरकारद्वारे) वर कॉल करू शकता.
8. राष्ट्रीय सायबर क्राइम रिपोर्टिंग पोर्टल https://cybercrime.gov.in/ वर तक्रार नोंदवू शकता.


# ऑनलाइन टास्क फ्रॉड

ऑनलाइन टास्क फ्रॉडमध्ये सामान्यत: घरातून कामाच्या संधी किंवा त्यांच्या फावल्या वेळेत उत्पन्नाचा दुसरा स्रोत शोधत असलेल्यांना आमिष दाखवून, त्यांना सोप्या कार्याची ऑफर देऊन आणि त्या बदल्यात पैसे देण्याचे आश्वासन देऊन फसवणूक करणे समाविष्ट असते.

## फसवणूक करणारी व्यक्ती/ॲप कशी ओळखायची?

- **आगंतुक संदेश:** बहुतेक वेळा मुख्यतः व्हाट्सएप किंवा टेलिग्रामवर अनपेक्षित संदेशांसह सुरुवात होते.
- **खोटी आश्वासने:** लवचिक तासांसह घरातून कामाच्या संधी देणे, अनुभवाची किंवा विशिष्ट कौशल्याची आवश्यकता नसणे.
- **फिशिंग वेबसाइट्स:** संदेशामध्ये कंपनीच्या वेबसाइटची लिंक असू शकते, जी कोणत्याही नामांकित कंपनीची क्लोन केलेली किंवा फिशिंग वेबसाइट असू शकते.
- **पेमेंट पद्धती:** दैनंदिन किंवा साप्ताहिक आधारावर (कधीकधी क्रिप्टोकरन्सीमध्ये) पेमेंट ऑफर करण.
- **खोटे ट्रस्ट बिल्डिंग:** सुरुवातीच्या दिवसांमध्ये, तुमचा विश्वास संपादन करण्यासाठी तुम्हाला पेमेंट मिळू शकते.
- **पेमेंटसाठी विनंती:** अधिक पैसे कमवण्यासाठी, तुम्हाला प्रीमियम शुल्क भरण्यास सांगितले जाईल, सामान्यतः ते तुम्ही आजपर्यंत कमावलेल्या रकमेपेक्षा थोडे कमी असू शकते.
- **पेमेंट प्रक्रिया:** तुम्हाला विविध पद्धती वापरून पेमेंट करण्यास सांगितले जाईल. जसे की क्युआर कोड स्कॅन करणे, नेट बँकिंग इ. आणि प्रत्येक वेळी, तुम्हाला सांगितले जाईल की पेमेंट यशस्वी झाले नाही.

Quick Heal
Foundation

# फसवणूक कशी रोखायची?

- **अवांछित संदेश टाळा:** साध्या कार्यांसाठी किंवा घरातून कामाच्या संधींसाठी उच्च पगाराचे आश्वासन देणाऱ्या अवांछित संदेशांपासून सावध रहा
- **वेबसाइटची वैधता तपासा:** पुढे जाण्यापूर्वी वेबसाइट पत्ता आणि त्याची वैधता सत्यापित करा.
- **पेमेंट करण्यापूर्वी पुष्टीकरण:** पेमेंट करण्यास सांगितले असल्यास, कंपनीच्या वैधतेची पुष्टी केल्याशिवाय असे करणे टाळा

# बळी पडल्यांनंतर पुढील पावले उचलावीत.

एकदा पीडित व्यक्तीला स्वत:ची शिकार झाल्याचे समजले की, त्यांनी फ्फसवणूक करणाऱ्यांना प्रतिसाद देणे थांबवावे – वाद घालू नये. फसवणूक करणारा तुमचा तपशील इतर गुन्हेगारांना देऊ शकतो जो तुमचा तपशील उदा.मॉर्फ केलेला फोटो पैसे उकळण्यासाठी वापरू शकतो.

1. तुम्हाला धमकीचे कॉल/मेसेज येत असल्यास घाबरू नका आणि पुढे पैसे देणे थांबवा.
2. फसवणुकीबद्दल तुमच्या संपर्कांना कळवा आणि त्यांना तुमच्या वतीने पैसे न देण्यास सांगा.
3. तुमच्या संपर्क यादीला त्यांच्या मॉर्फ केलेल्या फ्फोटोंसह धमक्याही मिळू शकतात,परंतु घाबरू नका, त्याऐवजी पोलिसांकडे तक्रार करा.
4. कॉल / चॅट, पेमेंट हिस्ट्री इत्यादी सारखे सर्व पुरावे संकलित करा.
5. ऍप, शेअर केलेल्या लिंक्स, फसवणूक करणाऱ्याचा तपशील यासारखे कोणतेही पुरावे मिटवू नका.– यामुळे पोलिसांना तपास करण्यात आणि कारवाई करण्यास मदत होते.
6. जवळच्या सायबर पोलिस स्टेशनमध्ये तक्रार करा किंवा स्थानिक पोलिस स्टेशनची मदत घ्या.
7. पोलिसांपासून काहीही लपवू नका.
8. तक्रार करण्यासाठी तुम्ही हेल्पलाइन १९३० (गृह मंत्रालय, भारत सरकारद्वारे) वर कॉल करू शकता किंवा राष्ट्रीय सायबर क्राइम रिपोर्टिंग पोर्टल https://cybercrime.gov.in/ वर तक्रार नोंदवू शकता.

# सोशल मीडिया मार्केटप्लेस फसवणूक


सोशल मीडिया मार्केटप्लेस फसवणूक: मार्केटप्लेसच्या फसवणुकीमध्ये कंपनीद्वारे खोटे किंवा दिशाभूल करणारे दावे करणे समाविष्ट आहे, जसे की जाहिरातींमध्ये उत्पादन किंवा सेवा गुण अतिशयोक्ती करणे, नकली वस्तू अस्सल उत्पादने म्हणून विकणे किंवा नकारात्मक पैलू किंवा दुष्परिणाम लपवणे. खोट्या जाहिराती हा बाजारातील फसवणुकीचा एक सामान्य प्रकार आहे.

## फसवणूक करणारी व्यक्ती/ॲप कशी ओळखायची?

- आकर्षक ऑफर्ससह आकर्षक जाहिराती.
- असामान्य उत्पादने, जी सामान्यतः Amazon किंवा Flipkart सारख्या लोकप्रिय प्लॅट फॉर्मवर आढळत नाहीत.

# फसवणूक कशी रोखायची?

- किंमतीच्या तुलनेत उत्पादनाची गुणवत्ता आणि मूल्य यांचे मूल्यांकन करा.
- खरेदी करण्यापूर्वी विक्रेत्याची वैधता आणि उत्पादनाची सत्यता तपासा.
- ऑर्डर देण्यापूर्वी विक्रेत्याशी त्यांच्या अधिकृत वेबसाइटद्वारे संवाद साधण्याचा प्रयत्न करा.

Quick Heal
Foundation

# बळी पडल्यांनंतर पुढील पावले उचलावीत.

एकदा पीडित व्यक्तीला स्वत:ची शिकार झाल्याचे समजले की, त्यांनी फ्फसवणूक करणाऱ्यांना प्रतिसाद देणे थांबवावे – वाद घालू नये. फसवणूक करणारा तुमचा तपशील इतर गुन्हेगारांना देऊ शकतो जो तुमचा तपशील उदा.मॉर्फ केलेला फोटो पैसे उकळण्यासाठी वापरू शकतो.

1. तुम्हाला धमकीचे कॉल/मेसेज येत असल्यास घाबरू नका आणि पुढे पैसे देणे थांबवा.

2. फसवणुकीबद्दल तुमच्या संपर्कांना कळवा आणि त्यांना तुमच्या वतीने पैसे न देण्यास सांगा.

3. तुमच्या संपर्क यादीला त्यांच्या मॉर्फ केलेल्या फ्फोटोंसह धमक्याही मिळू शकतात,परंतु घाबरू नका, त्याऐवजी पोलिसांकडे तक्रार करा.

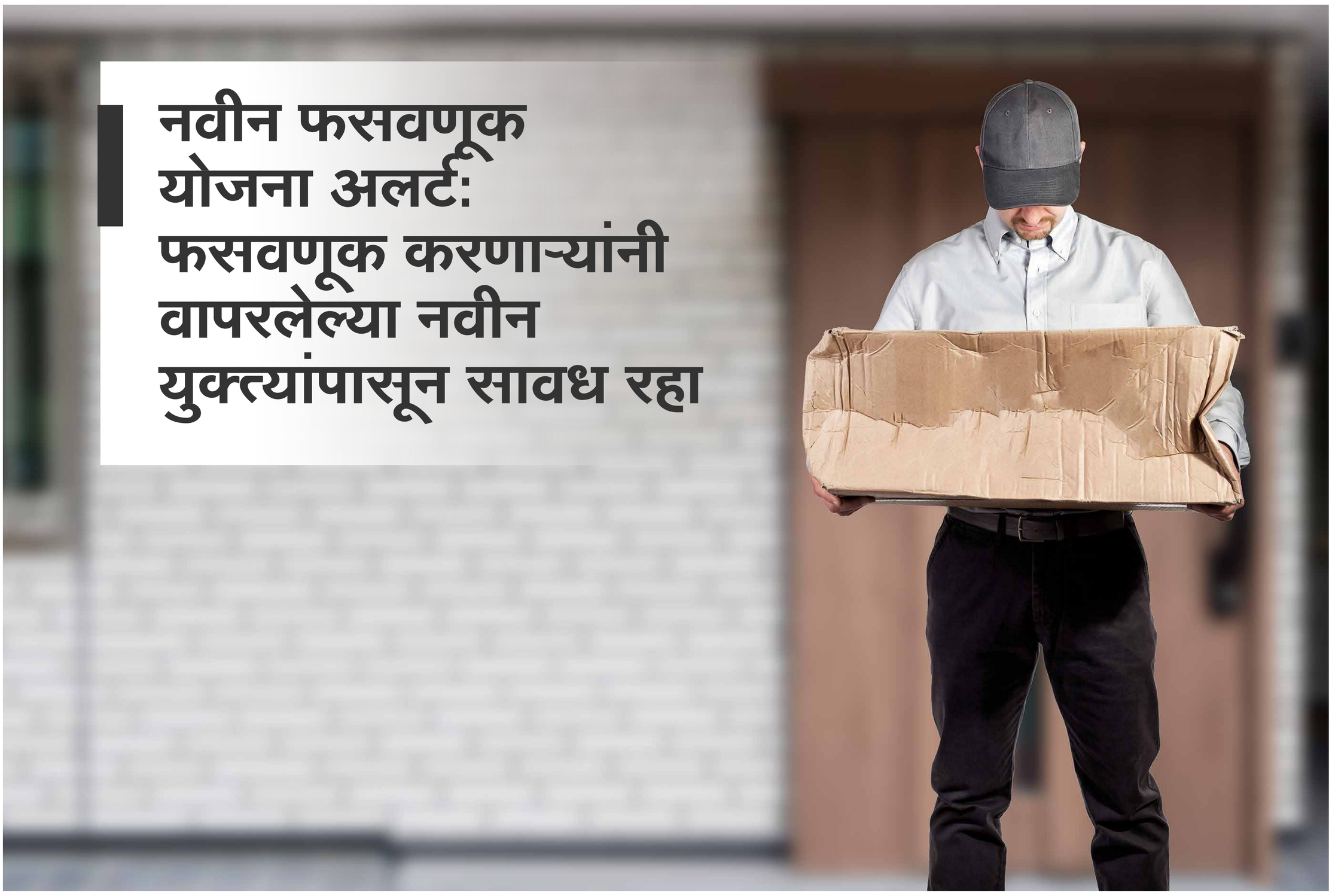
4. कॉल / चॅट, पेमेंट हिस्ट्री इत्यादी सारखे सर्व पुरावे संकलित करा.

5. ऍप, शेअर केलेल्या लिंक्स, फसवणूक करणाऱ्याचा तपशील यासारखे कोणतेही पुरावे मिटवू नका.– यामुळे पोलिसांना तपास करण्यात आणि कारवाई करण्यास मदत होते.

6. जवळच्या सायबर पोलिस स्टेशनमध्ये तक्रार करा किंवा स्थानिक पोलिस स्टेशनची मदत घ्या.

7. पोलिसांपासून काहीही लपवू नका.

8. तक्रार करण्यासाठी तुम्ही हेल्पलाइन १९३० (गृह मंत्रालय, भारत सरकारद्वारे) वर कॉल करू शकता किंवा राष्ट्रीय सायबर क्राइम रिपोर्टिंग पोर्टल https://cybercrime.gov.in/ वर तक्रार नोंदवू शकता.



# नवीन फसवणूक योजना अलर्ट: फसवणूक करणाऱ्यांनी वापरलेल्या नवीन युक्त्यांपासून सावध रहा

अलीकडे, फसवणुकीची एक नवीन पद्धत उघडकीस आली आहे, ज्यामध्ये त्यांच्या नावावर औषध असलेले कुरिअर आले आहे किंवा त्यांनी पाठवले आहे असा खोटा दावा करून लोकांचे शोषण केले आहे. दुसऱ्या घोटाळ्यात व्यक्तींना सूचित करणे समाविष्ट आहे की त्यांच्या मुलाला किंवा मुलीला रेव्ह पार्टीत सहभागी होण्यासाठी, परिस्थितीचे निराकरण करण्यासाठी पैशाची मागणी करण्यासाठी ताब्यात घेण्यात आले आहे.

## फसवणूक करणारी व्यक्ती/ॲप कशी ओळखायची?

- बेकायदेशीर पदार्थ असलेले कुरिअर मिळाल्याचे असामान्य दावे.
- रेव्ह पार्टीत सहभागी होण्यासाठी कुटुंबातील सदस्याला ताब्यात घेतल्याचा दावा.
- परिस्थितीचे निराकरण करण्यासाठी त्वरित पैसे देण्याची मागणी.

## फसवणूक कशी रोखायची?

- कायदेशीर अडचणीचा दावा करणाऱ्या अवांछित संदेश किंवा कॉलवर कधीही विश्वास ठेवू नका.
- कोणतीही कारवाई करण्यापूर्वी अधिकृत चॅनेलद्वारे दावे सत्यापित करा.
- दाव्यांची सत्यता पडताळल्याशिवाय कोणतीही देयके देण्यास नकार द्या.
- परिस्थिती संशयास्पद वाटत असल्यास, अधिकृत पत्त्यावर प्रत्यक्ष भेटण्याचा आग्रह धरा.

Quick Heal
Foundation

# बळी पडल्यांनंतर पुढील पावले उचलावीत.

एकदा पीडित व्यक्तीला स्वत:ची शिकार झाल्याचे समजले की, त्यांनी फ्फसवणूक करणाऱ्यांना प्रतिसाद देणे थांबवावे – वाद घालू नये.
फसवणूक करणारा तुमचा तपशील इतर गुन्हेगारांना देऊ शकतो जो तुमचा तपशील उदा.मॉर्फ केलेला फोटो पैसे उकळण्यासाठी वापरू शकतो.

1. तुम्हाला धमकीचे कॉल/मेसेज येत असल्यास घाबरू नका आणि पुढे पैसे देणे थांबवा.
2. फसवणुकीबद्दल तुमच्या संपर्कांना कळवा आणि त्यांना तुमच्या वतीने पैसे न देण्यास सांगा.
3. तुमच्या संपर्क यादीला त्यांच्या मॉर्फ केलेल्या फ्फोटोंसह धमक्याही मिळू शकतात,परंतु घाबरू नका, त्याऐवजी पोलिसांकडे तक्रार करा.
4. कॉल / चॅट, पेमेंट हिस्ट्री इत्यादी सारखे सर्व पुरावे संकलित करा.
5. ऍप, शेअर केलेल्या लिंक्स, फसवणूक करणाऱ्याचा तपशील यासारखे कोणतेही पुरावे मिटवू नका.– यामुळे पोलिसांना तपास करण्यात आणि कारवाई करण्यास मदत होते.
6. जवळच्या सायबर पोलिस स्टेशनमध्ये तक्रार करा किंवा स्थानिक पोलिस स्टेशनची मदत घ्या.
7. पोलिसांपासून काहीही लपवू नका.
8. तक्रार करण्यासाठी तुम्ही हेल्पलाइन १९३० (गृह मंत्रालय, भारत सरकारद्वारे) वर कॉल करू शकता किंवा राष्ट्रीय सायबर क्राइम रिपोर्टिंग पोर्टल https://cybercrime.gov.in/ वर तक्रार नोंदवू शकता.

# सतर्क राहा! तुमचे भविष्य सुरक्षित करा

- मोफत वाय-फाय वापरू नका
- परवानाकृत आणि अपडेटेड अँटीव्हायरस वापरा
- फोनवर पासवर्ड सेव्ह करू नका
- मजबूत पासवर्ड वापरा आणि तो वारंवार बदला
- विश्वसनीय ॲपवरून ॲप्स डाउनलोड करा
- टोरेंट साइट वापरू नका
- परवानाकृत आणि अपडेटेड ऑपरेटिंग सिस्टम वापरा

Quick Heal
Foundation


# क्विक हील फाउंडेशन

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