

राजू आणि चाळीस चोर



आर्थिक घोटाळेबाजांच्या
मोडस ऑपेरेण्डीवर पुस्तिका

ग्राहक शिक्षण आणि संरक्षण विभाग (CEPD), आरबीआय







प्रस्तावना

भारतीय रिझर्व्ह बँकेच्या ग्राहक जागरूकता उपक्रमांचा एक भाग म्हणून, या कार्यालयाने जुलै 2021 मध्ये आर्थिक फसवणूक करणाऱ्यांच्या कार्यपद्धतीवर 'बी(अ)वेअर' ही पुस्तिका प्रकाशित केली होती. लोकांकडून तसेच विविध संस्थांकडून मिळालेल्या सकारात्मक प्रतिसादामुळे उत्साहित होऊन, ज्यांना ऑनलाइन आर्थिक व्यवहारांच्या बारीकसारीक गोष्टींची फारशी माहिती नाही आणि ज्यांनी डिजिटल आर्थिक विश्वात नुकताच प्रवेश झाला आहे, अशांसाठी आर्थिक शिक्षणाची कल्पना आम्ही पुढे नेत आहोत. यामध्ये शाळकरी मुले, किशोरवयीन, अर्ध-साक्षर आणि ज्येष्ठ नागरिक अशा सर्व स्तरातील लोकांचा समावेश आहे, मग ते शहरी, ग्रामीण किंवा निमशहरी भागात राहत असले तरीही.

'बी(अ)वेअर' मालिका सुरु ठेवत असतानाच, 'राजू आणि चाळीस चोर' ही सचित्र पुस्तिका वरील लक्ष्य समूहाला आर्थिक व्यवहारांसाठी सुरक्षित मुख्य प्रवाहात आणण्याच्या आमच्या प्रयत्नांचा एक भाग आहे. ही पुस्तिका आपल्या आजूबाजूला घडणाऱ्या घटनांचे सहज समजण्यासारखे चित्रण आहे आणि आपण स्वकष्टाने कमावलेले पैसे फसवणूक करणाऱ्यांपासून कसे सुरक्षित ठेवावेत आणि अश्या फसवणूक करणाऱ्यांपासून आपला बचाव कसा करावा हे शिकण्यास मदत करते.

'राजू आणि चाळीस चोर' या पुस्तिकेत अशा चाळीस कथांचा समावेश आहे ज्यामध्ये आमच्याकडे नोंदवलेल्या गेलेल्या फसवणुकीच्या घटनांची झलक दाखवून काय करावे व काय करू नये याबद्दलच्या सोप्या युक्त्या दिल्या आहेत. घोटाळेबाजांद्वारे वापरल्या जाणाऱ्या अशा पद्धतींची आपण माहिती करून घेवूया आणि आपल्या सभोवतालच्या लोकांना अशा आर्थिक फसवणुकीपासून सावध राहण्यासाठी शिक्षित करूया.

वाचकांना विनंती आहे की त्यांनी आपले अभिप्राय आणि सूचना, असतील तर, bomumbai2@rbi.org.in वर पाठवा.

सावध रहा आणि सजग रहा!



प्रस्तावना

क्रम सं	विषय	पृष्ठ संख्या
१	फिशिंग लिंक द्वारे फसवणूक	१
२	विशिंग कॉल्स	३
३	ऑनलाइन बाजारपेठेचा वापर करून केलेली फसवणूक	५
४	क्रेडिट कार्डचे वार्षिक शुल्क माफ करणे - खोटी ऑफर	७
५	एटीएम कार्ड स्कीमिंग फसवणूक	९
६	स्क्रीन शेअरिंग ऑप / रिमोट अॅक्सेस ऑप वापरून केलेली फसवणूक	११
७	सिम ची अदलाबदल / सिम प्रतिकृति बनवणे	१३
८	सर्च इंजिन द्वारे गोपनीय माहितीची गोपनीयता कमी होऊन फसवणूक करणे	१५
९	क्यूआर कोड स्कॅनिंग द्वारे घोटाळा	१७
१०	समाज माध्यमा द्वारे तोतयागिरी	१९
११	ज्यूस जॅकींग – चार्जिंग वायर द्वारे डेटा चोरणे	२१
१२	लॉटरी घोटाळा	२३
१३	ऑनलाइन नोकरी घोटाळा	२५
१४	खोटे खाते क्रमांक	२७
१५	ई-मेल द्वारे घोटाळा	२९
१६	संदेश ऑप बँकिंग घोटाळा	३१
१७	चोरलेल्या कागदपत्रे वापरून फसवे कर्ज घेणे	३३
१८	सट्टेबाजीचे घोटाळे	३५
१९	फसवे लसीकरणाचे कॉल	३७
२०	कोविड चाचणी - खोटी ऑनलाइन साइट	३९



क्रम सं	विषय	पृष्ठ संख्या
२१	वसूली प्रतिनिधीच्या रूपात (बहाण्याने) घोटाळेबाज	४१
२२	सामाजिक हित योजना घोटाळा	४३
२३	बहुस्तरीय विपणन (mlm) घोटाळे	४५
२४	घर बसल्या नोकरीचे घोटाळे	४७
२५	ऑनलाइन खरेदी घोटाळे	४९
२६	सार्वजनिक वायफाय वापरून घोटाळे	५१
२७	बनावट जाहिरात / ऑफर	५३
२८	बनावट कर्ज संधी/ ऑफर	५५
२९	क्रेडिट कार्ड सक्रियकरण घोटाळे	५७
३०	क्रेडिट कार्डाची मर्यादा वाढवण्याचे घोटाळे	५९
३१	तुमच्या आधार कार्डाचे संरक्षण करणे	६१
३२	कॅश बँक ऑफर वापरून ऑनलाइन घोटाळे	६३
३३	सवलत घोटाळे	६५
३४	देणगी घोटाळे	६७
३५	फिक्स्ड डिपॉजिटवर ओव्हरड्राफ्ट	६९
३६	स्वतंत्र इंटरनेट नोकरी वापरून घोटाळे	७१
३७	प्रचंड व्याज दर आणि छळ करणाऱ्या डावपेचांसह बेकायदेशीर कर्ज वितरण ऑप	७३
३८	व्यापारी/इंधन दुकानात कार्ड क्लोनिंग	७५
३९	ओळखीच्या व्यक्ती/ परिवार/ कुटुंबीयां सोबत माहिती सामाईक करून घोटाळे	७७
४०	पैसे पाठवण्याचे (पेमेंट स्पीफिंग) फसवे ऑप	७९

१. फिशिंग लिंक च्या माध्यमातून फसवणूक

एक दिवस राजूच्या फोनवर संदेश आला, "प्रिय ग्राहक, जर तुम्ही दोन दिवसात तुमची नवीन केवायसी माहिती दिली नाहीत, तर तुमचे खाते बंद केले जाईल. केवायसी माहिती देण्यासाठी पुढील लिंकचा वापर करा <http://updateKYC.ibank.com>".

राजू : ओरे! माझे सगळे पैसे अडकतील. मला माझे केवायसी तपशील दिले पाहिजेत.



राजूने लिंक उघडली, पण केवायसी तपशील पुरवण्याची लिंक नीट उघडली नाही. लगेच त्याला एक फोन आला.



घोटाळेबाज : नमस्कार साहेब. मी एक्स वाय जेड बँकेतून बोलत आहे. तुम्हाला केवायसी माहिती पुरवण्यात काही अडचण येत आहे का?

राजू : होय, लिंक नीट उघडत नाही.



घोटाळेबाज : वेबसाइट वर जास्त लोड आहे बहुतेक. मी स्वतःच तुमचे तपशील भरतो. कृपया तुमचे यूजर नाव, पासवर्ड आणि ओटीपी मला द्या.

Click!
click!

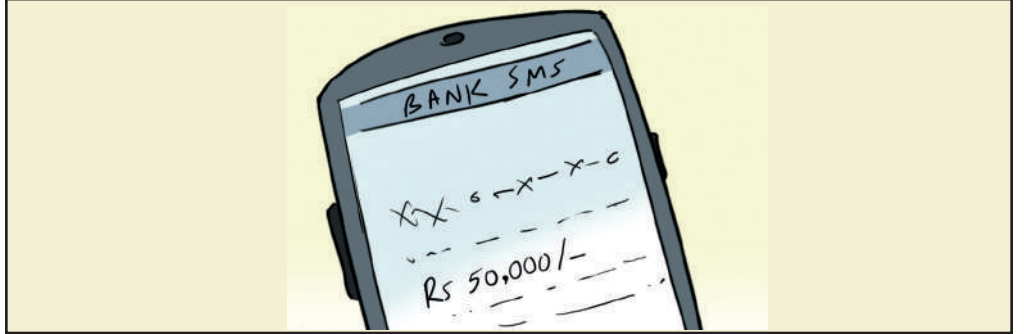


हे करा :

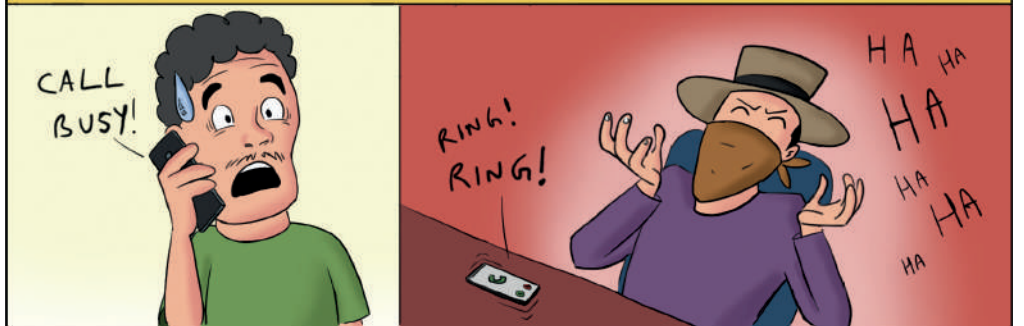
- ✓ तुम्हाला केवायसी तपशील देण्याबद्दल अनोळखी व्यक्ती कडून फोन, लिंक किंवा एसएमएस आला तर तुमचे खाते असलेल्या खातेत किंवा तुमच्या रिलेशनशिप / संबंध व्यवस्थापकाशी संपर्क साधून तुमच्या केवायसी स्थितीची फेर पडताळणी करून घ्या.
- ✓ पडलेली घटना जावळच्या सायबर गुन्हे पोलीस ठाण्यात आणि राष्ट्रीय सायबर गुन्हे रिवॉर्टिंग पोर्टल <https://cybercrime.gov.in> वर नोंदवा.



थोड्या वेळाने, राजूला एसएमएस आला की त्याच्या खात्यातून 50,000/- रुपयांची रक्कम वजा झाली आहे.



राजूने लगेच त्या व्यक्तीला फोन केला, पण त्याने फोन उचलला नाही. राजूला समजले की हा माणूस धोकेबाज होता आणि त्याने आपले वैयक्तिक तपशील त्याला द्यायला नको होते.



हे करू नका :

- ✗ फोन/ ई-मेल वर आलेल्या अनोळखी/अपरिचित लिंक साठी क्लिकविण्यास उपद्रव नका.
- ✗ अनोळखी लोकांना तुमचे गोपनीय तपशील देऊ नका.

२. विशिंग कॉल्स

एक दिवस राजूला एक फोन आला.

घोटाळेबाज : नमस्कार साहेब.
मी एक्स वाय जेड बँकेतून बोलत आहे.

राजू : बोला. काय काम आहे?

जालसाज : "घोटाळेबाज : तुमच्या निवा पॉलिसी संदर्भात
कोलपये आहे. तुमची पॉलिसी चालू सुलमी आहे आणि
तुम्हाला ₹.18,000/- चा कृप (प्रिमियम) भरण्या
आहे."

राजू : "नाही, एक्स वाय जेड बँकेत
माझा कोणताही निवा नाही."

घोटाळेबाज : "साहेब, ही पॉलिसी तुमच्यासाठी
प्रचारात्मक ऑफर म्हणून अत्यंत कमी शुल्क लावून
चालू केली आहे. तरीही तुम्हाला नको असेल तर मी ती
बंद करतो."

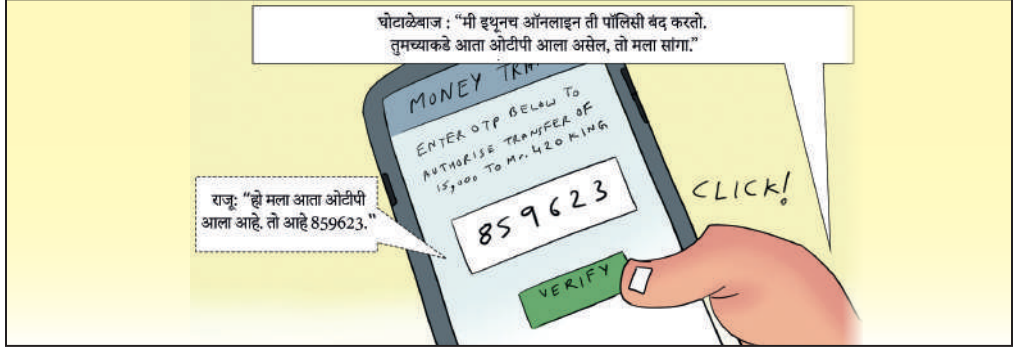
राजू : "मला कळत नाही माझ्या परवानगी निवाप
कुठेही हो पॉलिसी चालू केली केली आणि मी का
विश्वास ठेवू तुमच्यावर ?"

घोटाळेबाज : "साहेब, मी प्रत्यक्ष एक्स वाय जेड बँकेच्या ग्राहक संरक्षण विभागामातून बोलत
आहे. माझ्याकडे तुमची सर्व माहिती आहे, जसे, नाव, पत्ता, तुमच्या कार्डची माहिती, बचत
तारीख, तुमच्या कंपनीचे नाव आणि पद."

राजू : "ठीक आहे. मग मला सांगा ही
पॉलिसी बंद केली करता येईल?"

हे करा :

- ✓ कोणावरही विश्वास ठेवण्यापूर्वी नेहमी तुमच्या रिलेशनशिप / संकेत व्यवस्थापकाशी किंवा बँकेच्या साक्षेची बोलून सातटी करून घ्या.
- ✓ ओटीपी ही तुमच्या सुरक्षित संपदेची चावी आहे. ती घोटाळेबाजांपासून सुरक्षित / लांब ठेवा.
- ✓ घडलेली घटना जवळच्या सायबर क्राइम पोलीस ठाण्यात आणि राष्ट्रीय सायबर क्राइम रिपोर्टिंग पोर्टल <https://cybercrime.gov.in> वर लगेचच नोंदवा.



हे करू नका :

- × बँकेकडून बोलत आहे असे सांगणाऱ्या व गोपनीय माहिती / विवरण विचारणाऱ्या अनोळखी व्यक्तीवर विश्वास ठेवू नका. बँका कधीही असे तपशील फोनवर विचारत नाहीत.
- × डिजिटल विश्वास कोणाही अनोळखी व्यक्ती वर सहज विश्वास टाकू नका आणि अनोळखी क्रमांकावरून आलेल्या फोनला उत्तर देताना सावध रहा.

३. ऑनलाइन बाजारपेठेचा वापर करून केलेली फसवणूक

राजूला त्याचा सोफासेट काढून टाकायचा होता. म्हणून त्याने एका वेबसाइटवर जाहिरात दिली, जी वापरलेल्या वस्तूंची ऑनलाइन बाजारपेठ होती.



जाहिरात टाकल्याबरोबर लगेच एका पोकेटाजाकडून चौकशीसाठी फोन आला. त्याने सोफासेट साठी ₹.15,000/- देऊ केले. अशी ऑफर मिळाल्यामुळे राजू खूपच आनंदित झाला.



घोटाळेबाज : "कृपया तुमचा खाते क्रमांक द्या."

राजू : "माझा खाते क्रमांक आहे 123xxx67."

घोटाळेबाज : "पूर्ण पैसे पाठवण्याआधी खाते बरोबर आहे का, हे पाहण्यासाठी मी तुम्हाला ₹.10/- पाठवतो."

घोटाळेबाज राजूच्या खात्यात ₹.10/- पाठवतो आणि पूर्ण पैसे पाठवण्यासाठी पुष्टी मागवतो.

राजू : "होय, मला मिळाले."

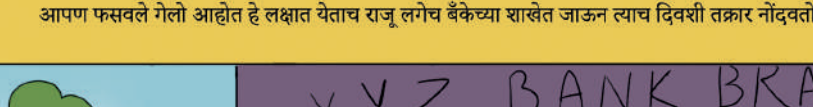
हे कट :

- ✓ नेहमी लक्षात ठेवा, UPI पिन हा फक्त पैसे देण्यासाठी (पेमेंट करण्यासाठी) आवश्यक आहे आणि पैसे मिळविण्यासाठी नाही.
- ✓ नेहमी पैसे देण्यास सुरुवात करण्यापूर्वी UPI ऑप्शनमधील मोबाइल क्रमांकाची खात्री करून घ्या.
- ✓ पडलेली घटना जवळच्या सायबर क्राइम पोलीस ठाण्यात आणि राष्ट्रीय सायबर क्राइम रिपोर्टिंग पोर्टल <https://cybercrime.gov.in> वर नोंदवा.



A cartoon illustration of a mobile phone screen. The screen displays a text message titled "BANK SMS". The message content is "X X X X X X X X" followed by "RS 14,990/-".

आपण फसवले गेलो आहोत हे लक्षात येताच राजू लगेच बाँकेच्या शाखेत जाऊन त्याच दिवशी तक्रार नोंदवतो.



- ✘ ओटीपी किंवा तुमच्या खात्यासंदर्भातील गोपनीय तपशील अनोळखी व्यक्तीला देऊ नका.
- ✘ दुसऱ्या माणसाकडून पैसे घेत असताना UPI पिन टाकू नका.

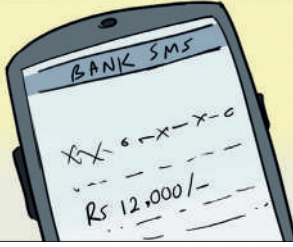


राजूने विचार केला, फोन करणाऱ्याला त्याच्या कार्डची सर्व माहिती आहे, त्या अर्थी तो खरा असला पाहिजे. त्याने लगेच चोराला ओटीपी सांगितला .

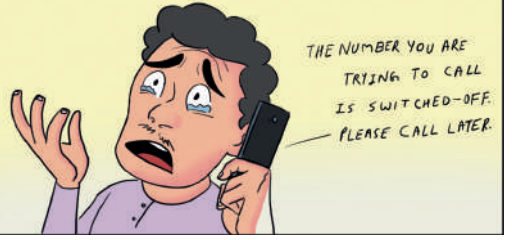
चोटाळेबाज : "राजू साहेब धन्यवाद. तुमची वार्षिक फी माफ झाली आहे. तुमचा दिवस आनंदात जावो."



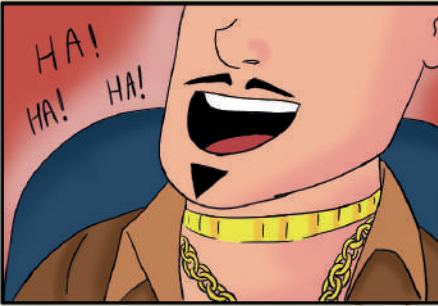
फोन कट झाला आणि लगेच राजूला त्याच्या क्रेडिट कार्ड खात्यातून रु.12,000/- वजा झाल्याचा एसएमएस आला.



राजूने चोराला ताबडतोब फोन लावला, पण फोन बंद होता.



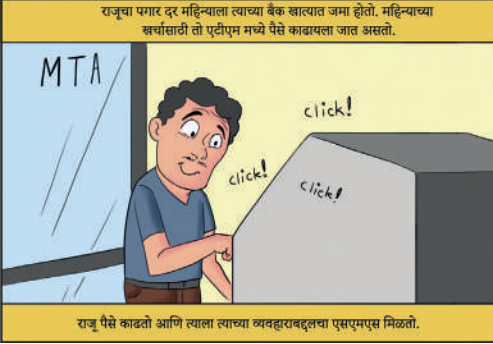
राजूला समजले की ही व्यक्ती चोटाळेबाज होती, आणि त्याने त्याला ओटीपी द्यायला नको होता.



हे करू नका :

- × तुमचा ओटीपी कोणालाही सांगू नका. चोटाळेबाज तुमच्या खात्याचे तपशील गोळा करू शकेल कदाचित, पण प्रत्यक्ष व्यवहार तेव्हाच पूर्ण होईल जेव्हा तुम्ही तुमच्या फोन वर आलेला गोपनीय ओटीपी घाल.

५. एटीएम कार्ड स्कीमिंग फसवणूक



हे करा :

- ✓ एटीएम व्यवहार सुरू करण्या पूर्वी, मशीनला स्कीमिंग उपकरण तर लावलेले नाही ना याची खात्री करून घ्या. हे उपकरण एटीएम कार्ड घालण्याच्या फटीखाली लपवलेले असते.
- ✓ क्लोनिंगच्या घटनेनंतर 3 दिवसांच्या आत बँकेला कळवा. तुमच्या व्यवहाराची यादी वारंवार पडताळून पाहत जा.
- ✓ घडलेली घटना जवळच्या सायबर क्राइम पोलीस ठाण्यात आणि राष्ट्रीय सायबर क्राइम रिपोर्टिंग पोर्टल <https://cybercrime.gov.in> वर नोंदवा.



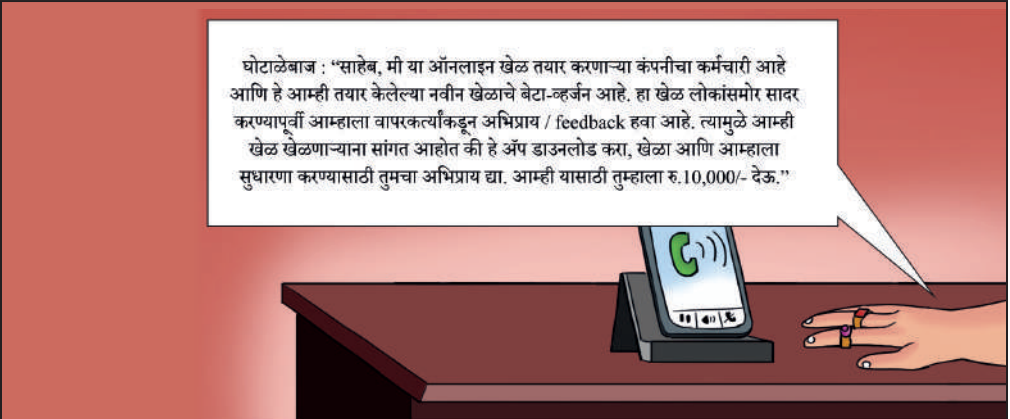
दोघे एटीएम मध्ये गेले.



हे करू नका :

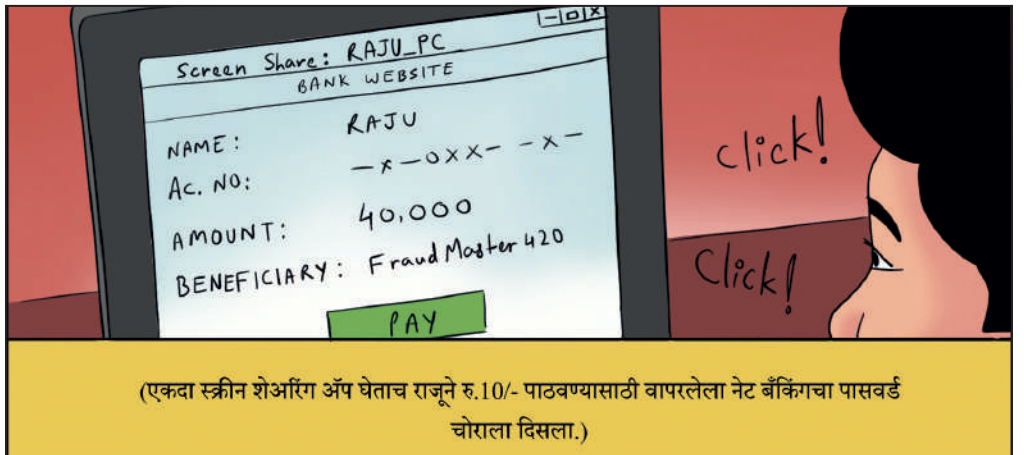
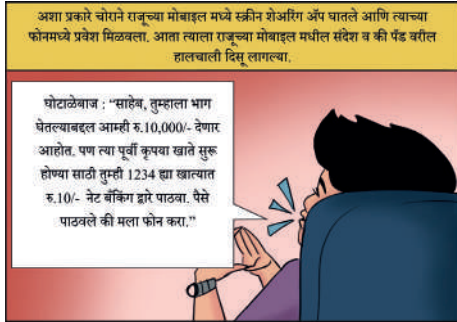
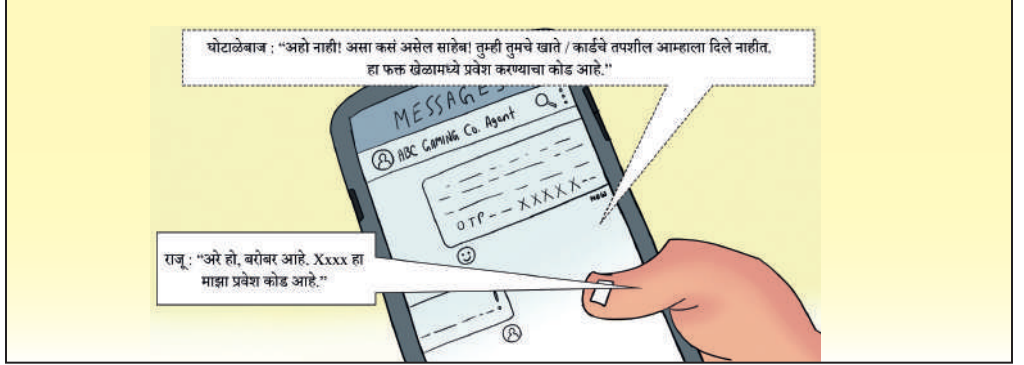
- ✗ एटीएमच्या परिसरात कोणालाही तुमच्या वतीने व्यवहार करण्यासाठी तुमचे एटीएम कार्ड देऊ नका.
अशा प्रकारचे सामाजिक अभियांत्रिकीकरण विशेषतः ज्यांना एटीएम वापरण्यास अडचण येते अशा वरिष्ठ नागरिक / अर्ध शिक्षित लोकांना लक्ष्य करण्यासाठी वापरले जाते.

६. स्क्रीन शेअरिंग ॲप / रिमोट ॲक्सेस ॲप वापरून केलेली फसवणूक



हे करा :

- ✓ ज्याची ऑफर आली आहे त्याची अधिकृतता / खरेपणा, संबंधित व्यवसायाच्या नोंदणीकृत वेबसाइट वर लाली करून घ्या.
- ✓ तुमच्या मोबाइल फोन वर ॲंटी वायरस / स्पॅम ब्लॉकिंग सॉफ्टवेअर चालू घ्या.
- ✓ ही घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हा नोंदणी पोर्टल वर (<https://cybercrime.gov.in>) वर नोंदवा.



हे करू नका :

- × एसएमएस, ई-मेल किंवा झटपट संदेश ऑप द्वारे पाठवलेल्या लिंक ने कोणतेही ऑनलाइन डाउनलोड करू नका.
- × अनोळखी व्यक्तीने पाठवलेले स्क्रीन शेअरिंग ऑनलाइन डाउनलोड करू नका. असा ऑप द्वारे आलेला स्क्रीन शेअरिंग कोड कोणाही अनोळखी व्यक्तीला देऊ नका.

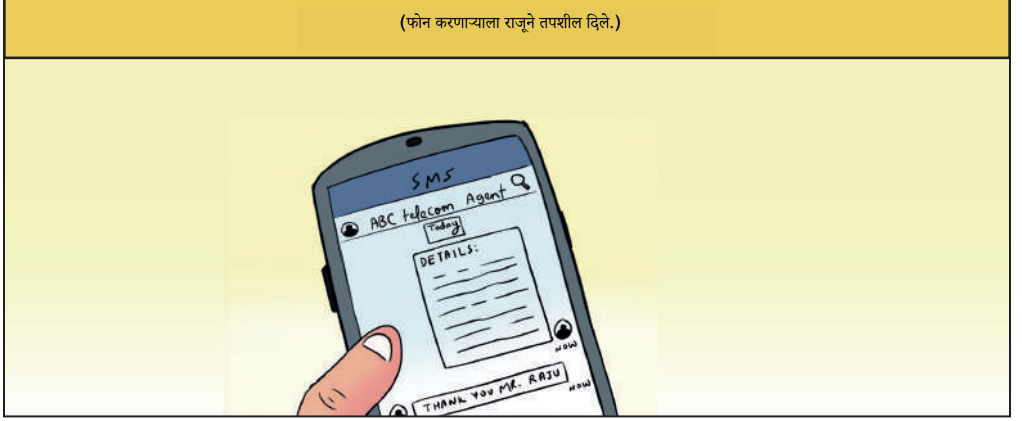
७. सिमची अदलाबदल / सिमची प्रतिकृति बनवणे



हे करा :

- ✓ अनोळखी लोकांवर विश्वास ठेवण्या ऐवजी जेव्हा शंका असेल तेव्हा तुमच्या टेलीकॉम सेवा पुरवठादाराशी बोलून तुमच्या सिम कार्डच्या स्थितीची खात्री करा.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.

(फोन करणाऱ्याला राजूने तपशील दिले.)



राजू : “काय झालं माझ्या मोबाइल ला?
नेटवर्क नाही आणि मी फोन, मेसेज इत्यादी
करू शकत नाही.”



(चोराने नवीन सिम कार्ड घेतले आणि बँकिंग ॲप्लिकेशन चे “forgot username”, “reset password” इत्यादी विकल्प वापरून गुजर नाव शोधून काढले आणि खात्यातील सर्व पैसे स्वतःच्या खात्यात वळवले.)

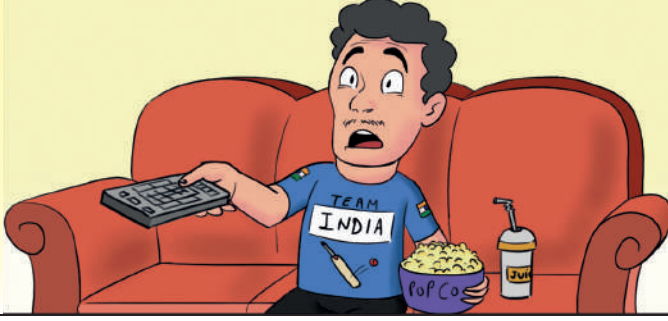


हे करू नका :

- × फोन करणाऱ्या अनोळखी लोकांना तुमचे गोपनीय तपशील जसे आधार कार्ड, सिम क्रमांक देऊ नका.

८. सर्च इंजिन द्वारे गोपनीय माहितीची गोपनीयता कमी होऊन फसवणूक करणे

राजूला क्रिकेट पाहण्याची आवड आहे. आणि पुढील क्रिकेट मॅच बाबत तो खूप उत्सुक होता. पण खेळाचे ऑन उघडताच त्याचे सभासदत्व संपल्याचे त्याला लक्षात आले.



राजूने विचार केला "त्यात काय मोठे! इंटरनेट वर सगळ्याचा तोडगा असतो."

SNAP!

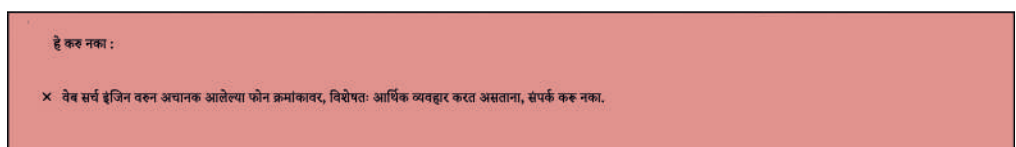


असा विचार करून तो इंटरनेट वर खेळाच्या ऑनचे पैसे भरण्यासाठी उरावर शोधू लागला. थोडा वेळ शोधल्यावर ह्यासाठी त्याला एक फोन नंबर मिळाला. राजूने लगेच नंबर फिरवला.



हे करा :

- ✓ नेहमी, फक्त सेवा पुरवठादाराच्या अधिकृत वेबसाइट वरून संपर्कासाठी तयारीत / याहक सेवा क्रमांक इत्यादी घ्या.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस थ्रीकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.



९. क्यूआर कोड स्कॅनिंग द्वारे घोटाळा

राजूने त्याची जुनी गाडी विकण्यासाठी ऑनलाइन वेबसाइटवर नोंदणी केली.



काही तासातच त्यांच्याशी एका व्यक्तीने (घोटाळेबाज) संपर्क केला.

घोटाळेबाज : "नमस्कार, मी साइटवर तुमच्या गाडीची जाहिरात पहिली. मला तुमची गाडी खूप आवडली आणि मला ती विकत घेण्यात स्वारस्य आहे."



घोटाळेबाज : "अहो, किमतीची काळजी करू नका. मी सैन्यातला माणूस आहे, आणि मी एक महिन्यात निवृत्त होणार आहे. माझ्या मुलाला गाडी घ्यायची आहे आणि त्याला हीच गाडी हवी आहे."

राजू : "तुम्हाला आवडली हे ऐकून मला आनंद झाला. माझी गाडी अत्यंत उत्तम स्थितीत आहे. मी नवीन गाडी विकत घेतो आहे, केवळ भरणून मी ही विकत आहे. मी किमतीच्या बाबतीत भाव करणार नाही."

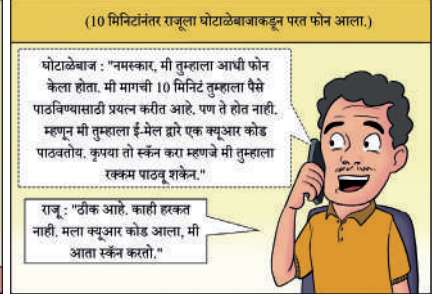
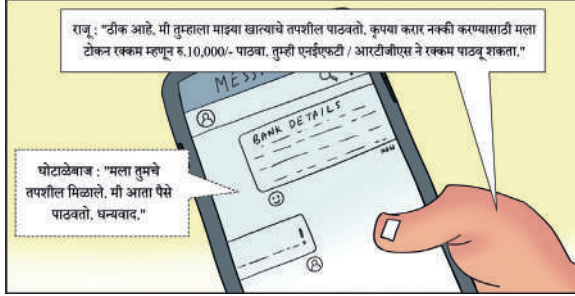
राजू : "अरे वा छान! मला वाटते खरेदी करण्या पूर्वी तुम्हाला गाडी बघायची असेल."

घोटाळेबाज : "नक्कीच, आम्हाला गाडी पहायची आहे, पण त्या पूर्वी मी तुम्हाला टोकन रक्कम पाठवतो कारण ही संधी मला सोडायची नाही."

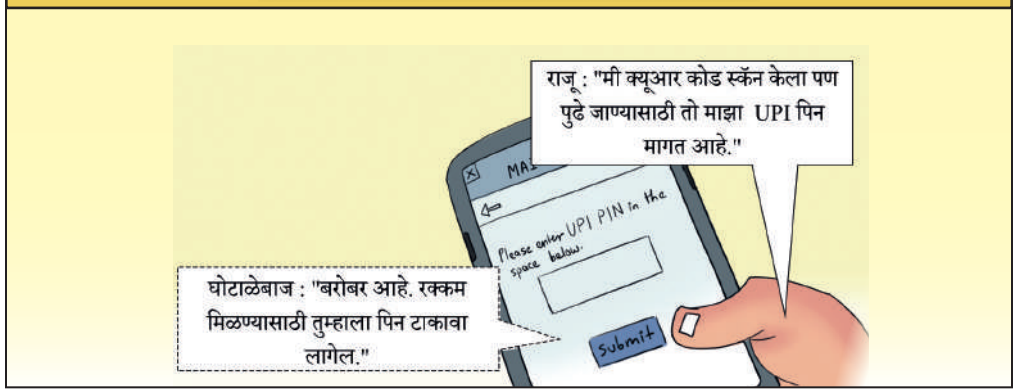


हे करा :

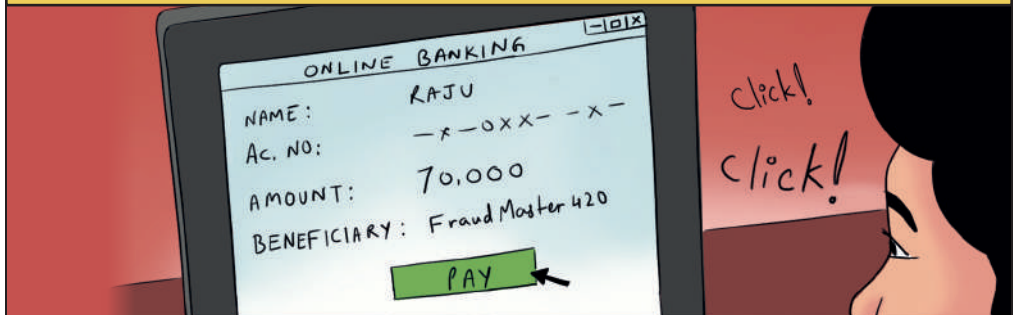
- ✓ क्यूआर कोड वापरण्यापूर्वी त्याचा उपयोग करणे शिकून घ्या.
- ✓ झालेला व्यवहार तुमच्या बँकेला त्वरीत कळवा.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.



(राजू क्यूआर स्कॅन करतो आणि त्याला UPI पिन साठी पॉप-अप विनंती दिसते.)



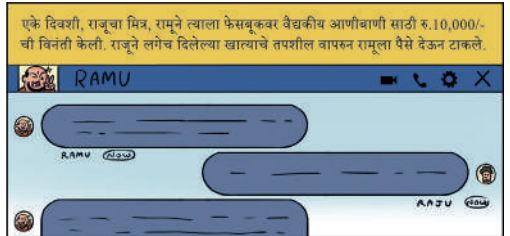
(राजूने त्याच्यावर विश्वास ठेवला आणि UPI पिन टाकला. ताबडतोब, त्याच्या खात्यातून ₹. 70,000 जमा! घाबऱ्याची समस्याग्रस्त तर समस्या मिळाली तो घाबरला ३
लागला पण तो पर्यंत त्याचा फोन बंद झाला होता.)



हे करू नका :

- × दुसऱ्या व्यक्ती कडून रक्कम येण्यासाठी तुमचा UPI पिन घालू नका. UPI पिन हा फक्त रक्कम पाठवण्यासाठी आवश्यक असतो. मिळण्यासाठी नाही.
- × कोणतीही रक्कम मिळण्यासाठी क्यूआर कोड स्कॅन करू नका. क्यूआर कोड फक्त पैसे पाठवण्यासाठी स्कॅन करावा लागतो, पैसे मिळविण्यासाठी नाही.

१०. समाज माध्यमा द्वारे तोतयागिरी



हे करा :

- ✓ पैसे देण्या अगोदर नेमक्या व्यक्तीला फोन करून / भेटून खात्री करून घ्या.
- ✓ पैसे पाठवण्या आधी नेहमी खात्याची माहिती तपासून घ्या.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.

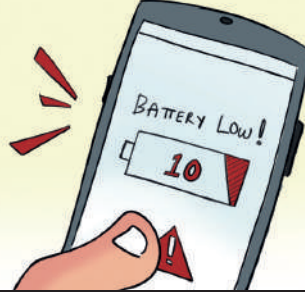


हे करू नका :

- × तुमची वैयक्तिक माहिती जसे फोन क्रमांक, ई-मेल आयडी आणि मित्र-मैत्रीणींची यादी समाज माध्यमावर जाहीर करू नका.
- × ज्याला कधी प्रत्यक्ष भेटलो नाही अस्या व्यक्ती कडून मैत्रीची विनंती / अनुसरणाची विनंती स्वीकारू नका.

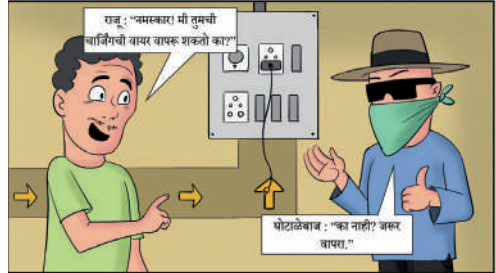
११. ज्यूस जॅकींग – चार्जिंग वायर द्वारे डेटा चोरणे

राजूला वैद्यकीय आणीबाणी मुळे पटकन निघावे लागले.
त्याच्या लक्षात आले की त्याच्या फोनची बॅटरी कमी आहे.



राजू : “अरेरे! माझी बॅटरी संपलीच की, आणि माझ्याकडे चार्जर ही नाही.”

(घोटाळेबाजाने वायरस असलेली चार्जिंगची वायर लावली आणि सार्वजनिक चार्जिंग पॉइंटवर सोडून गेला. चार्जिंग पॉइंटला लागलेली चार्जिंग वायर राजूला दिसली आणि त्याने घोटाळेबाजाला ती बापरण्याची परवानगी विचारली.)



हे करा :

- ✓ अनधिकृत प्रवेशापासून रक्षण होण्यासाठी तुमच्या फोनमध्ये अँटी-वायरस सॉफ्टवेअर घाला.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.

चार्जिंग होत असताना, चार्जिंगच्या वायरी मधून वायरस राजूच्या फोनमध्ये शिरला



गुह्याचा काही दिवसांमध्ये, चोराने राजूच्या फोन मधील महत्वाचे तपशील जसे युजनेम, पासवर्ड इत्यादी मिळवले.



एके दिवशी, राजूला त्याच्या बचत खात्यातून अनधिकृत वजा व्यवहार सूचित करणारे एसएमएस ई-मेल आले



आणि त्याला समजले की त्याच्या खात्यात कुठेतरी गडबड होत आहे.



हे करू नका :

- x अनोळखी माणसांच्या चार्जिंग adapter / वायर वापरू नका.

१२. लॉटरी घोटाळा

राजूला एक ऑडिओ संदेश आला, ज्यात म्हटले होते की त्याने अबक जॅकपॉट जिंकला



घोटाळेबाज : "नमस्कार, मी अबक मधून पॅकज बोलतोय. रु. 10 लाखांचा अबक जॅकपॉट जिंकल्याबद्दल तुमचे अभिनंदन. मी तुम्हाला जॅकपॉट बद्दलची सर्व माहिती पाठवली आहे. तुम्ही त्यात दिलेल्या क्रमांकावर संपर्क करून बक्षीस मागू शकता. जरा घाई करा."

उत्तेजित झालेल्या राजूने लगेच जॅकपॉट मेसेज मध्ये दिलेल्या क्रमांकावर फोन केला, ज्यामध्ये सुपरस्टार जॅक पॉट जिंकल्याबद्दल त्याचे अभिनंदन करीन असल्याचा बनावट विडियो होत

राजू : "नमस्कार, मी राजू बोलतोय. अबक जॅकपॉट वर दावा करण्यासाठी मला तुमच्याशी संपर्क करायला सांगितले आहे. मी माझ्या जॅक पॉट साठी असा दावा करू शकतो?"



घोटाळेबाज : "अभिनेत राजू! बक्षीस मिळण्यासाठी तुम्हाला रु. 1000/- वितरण शुल्क म्णून भरायचे आहेत. आमच्या खात्याचे तपशील मी तुमच्या मेसेज ऐप क्रमांकावर पाठवली आहे. कृपया लगेच शुल्क भरा आणि मला परत फोन करा."



(कसवेगीरीची जाणीव नसल्यामुळे राजूने लगेच पैसे भरले आणि त्याला फोन केला.)

राजू : "मी तुम्हाला पैसे पाठवले आणि त्याचे तपशील तुम्हाला पाठवले आहेत. माझे बक्षीस मला कधी मिळेल?"

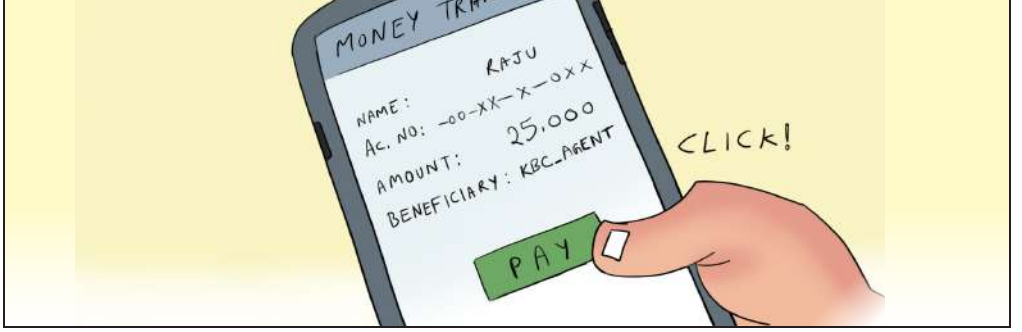


घोटाळेबाज : "खूप छान राजू! 10 लाख रुपयांचे जॅकपॉट मिळण्यासाठी अजून काही पायऱ्या बाकी आहेत. बक्षिसाच्या रकमेवर दावा करण्यासाठी तुम्हाला रु. 25,000/- कर शुल्क भरावे लागेल."

हे करा :

- ✓ कोणत्याही कंपनी किंवा व्यवस्थापक चमूकडून आले आहेत असे वाटणाऱ्या अनोळखी क्रमांकावरून आलेल्या संदेशांवर विश्वास ठेवण्यापूर्वी त्यांची खात्री करून घ्या.
- ✓ अशा लॉटरी ऑफर ची त्यांच्या आयोजकाच्या अधिकृत वेबसाइट वरून नेहमी खात्री करून घ्या.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.

दुसऱ्यांदा विचारही न करता राजू ने पैसे भरून टाकले.



.....शेवटी, त्याच्या लक्षात आले की तो फसवला गेला आहे.

हे करू नका :

x मोठी रक्कम मिळण्याच्या आशेने कोणतीही खात्री न करता पैसे पाठवू नका.

१३. ऑनलाइन नोकरी घोटाळा

राजूची नोकरी हल्लीच सुटली होती आणि तो खूप काळजीत होता. त्याने ऑनलाइन नोकरी पोर्टल वर नोकरी शोधणे सुरू केले होते. त्याने वेगवेगळ्या वेबसाइट वर त्याची वैयक्तिक तपशील (शिक्षण व अनुभव) टाकले होते.



एक दिवशी, त्याला एक फोन आला, जो एक्स वाय जेड कंपनीच्या कर्मचाऱ्याची तोतयागिरी करत होता.

घोटाळेबाज : "माझ बोलणं श्री. राजू यांच्याशी होत आहे का?"



SCRATCH!

SCRATCH!

राजू : "हो, मला कळू शकेल का माझ बोलणं कोणाशी होत आहे ते?"

घोटाळेबाज : "नमस्ते, राजू. मी एक्स वाय जेड कंपनीच्या मानव संसाधन कक्षा मधून रोहित बोलत आहे. तुमच्या अर्जाच्या आधारावर तुमची निवड आमच्या कंपनीतल्या व्यवस्थापकीय पदासाठी झाली आहे."



राजू : "अरे वा! मला निवडण्यासाठी धन्यवाद."

घोटाळेबाज : "तुमच्या पात्रतेमुळे ही नोकरी तुम्हाला मिळत आहे."

राजू : "अच्छा, बरे आहे. ह्या पुढची पायरी काय?"



हे करा :

- ✓ कुठले ही पैसे भरण्या अगोदर, कंपनी किंवा भरती प्रतिनिधीच्या खरेपणाची खात्री करून घ्या. सहसा, भरती प्रतिनिधी भरतीसाठी उमेदवाराकडे शुल्क मागत नाहीत.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in/>) वर नोंदवा.



खुशीने उत्तेजित होऊन, राजूने त्या व्यक्तीने सांगितलेल्या खात्यामध्ये रु. 5000 भरले



(बरेच दिवस थांबून ही, राजूला लॅपटॉप मिळाला नाही. त्याने पूर्वीच्या क्रमांकावर फोन करायचा प्रयत्न केला, पण फोन नेहमी बंद असे. त्याने कंपनीचे नाव ऑनलाइन शोधले पण काही सापडले नाही. राजूला अखेरीस जाणवले की त्याची त्याच्या मेहेनतीने कमवलेल्या पेश्यासाठी फसवणूक झाली आहे.

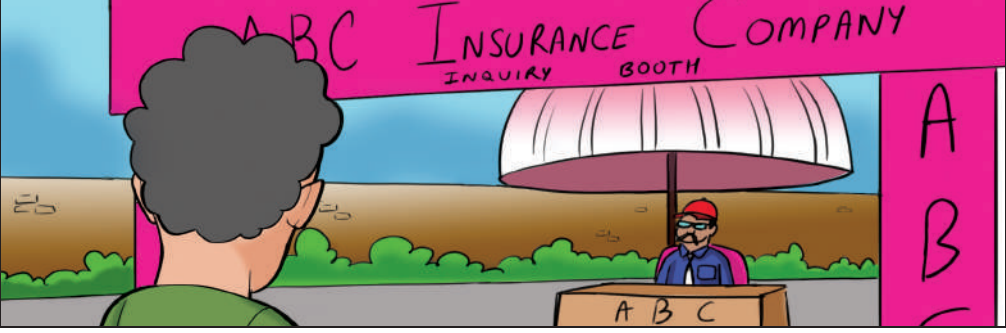


हे कर नका :

- ✗ कोणालाही नोकरी मिळण्याच्या सबबी वर पैसे देऊ नका. कोणतीही वैध कंपनी कधीही संभाव्य उमेदवाराकडून नोकरीच्या संधीसाठी रक्कम मागणार नाही.

१४. बनावट खाते क्रमांक

राजू स्वतःसाठी व त्याच्या परिवारासाठी कौटुंबिक विमा विकत घेण्याचे ठरवत होता. कार्यालयातून घरी जात असताना त्याने वाटेवर अवक विमा कंपनी नावाचा छोटा स्टॉल पाहिला.



हे करा :

- ✓ संस्थेच्या पालतेची सत्यता कोणत्याही ज्ञात डेटाबेसवर पडताळून पहा.
- ✓ नेहमी उत्पादने घेण्यासाठी नोंदणीकृत कार्यालयांशी संपर्क करा.
- ✓ पैसे फक्त खाते क्रमांकाच्या आधारवरच अंतरित करता येतात.
- ✓ घोटाळेबाज असलेल्या कंपनीचे नाव देऊ शकतो, पण खाते क्रमांक मात्र स्वतःचाच देईल. नेहमी पैसे भरण्या आधी कंपनी कडून खाते क्रमांकाची खाली करून घ्या.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.



हे करू नका :

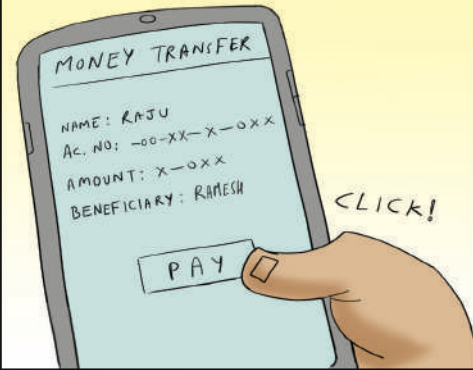
- ✗ कंपनीच्या असलपणाची खाली झाल्या शिवाय कोणालाही कोणतीही रक्कम प्रदान करू नका.

१५. ई-मेल द्वारे घोटाळा

चोराने राजूला ई-मेल पाठवले, त्याचा मित्र रमेश असल्याची बतावणी करून वैद्यकीय आणि बाणीसाठी आर्थिक मदतीची विनंती केली.



राजूने ई-मेल आयडी किंवा खात्याची तपशील न पडताळता लगेच पैसे पाठवले.



एक दिवसानंतर, राजूने रमेशांना त्याच्या तब्येतीची चौकशी करण्यासाठी फोन केला.



रमेश: "नमस्कार राजू, मी ठीक आहे. तू कसा आहेस? खूप दिवसांनी फोन केलास."



हे करा :

- ✓ आलेल्या ई-मेलवर आधारित कोणतेही पेमेंट करण्या अगोदर संबंधित व्यक्तीशी बोलून खात्री करून घ्या.
- ✓ ई-मेल आयडीची पडताळणी करा.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.



(हे कळल्यावर राजूला धक्काच बसला. त्याच्या हलगर्जीपणामुळे तो त्याच्या दयाळूपणाचाच बळी बनला. त्याने ई-मेल आयडीची खात्री करून घ्यायला हवी होती.)



हे करू नका :

✗ सहजगत्या ई-मेल किंवा सारख्या दिसणाऱ्या ई-मेल आयडी वरून आलेल्या विनंती वर विश्वास ठेवून पैसे पाठवू नका.

१६. संदेश ऑप बँकिंग घोटाळा

एके दिवशी राजूला एका अनोळखी क्रमांकावरून कॉल आला.

घोटाळेबाज : “नमस्कार साहेब. मी एक्स वाय स्नेह बँकेच्या ग्राहक सेवा केंद्रातून बोलत आहे. आम्ही एक नवीन ऑप, संदेश ऑप, जारी करत आहोत. ही एक बँकिंग सुविधा आहे जी 24x7 तुमच्या वखममम ऑप द्वारे तुम्हाला सहज बँकिंग सुविधा देते. तुम्हाला पहिल्या वापरावर एक गिफ्ट व्हाऊचर ही मिळेल. कृपया तुमचा भ्रमणध्वनि क्रमांक 99****99 संदेश ऑप मध्ये नोंदलेला आहे ना ह्याची पुष्टी करून घ्या.”

NAME: RAJU
OCCUPATION: XOXO
ADDRESS: X-X-X-X
XOXOX-X-X-X
X-XOXOX-X-X
CONTACT: 729256027
X-X-X-X

राजू : “अरे वा! आश्चर्य आहे. हो. ह्या माझा संदेश ऑपचा क्रमांक आहे.”

घोटाळेबाज : “ठीक आहे साहेब. आम्ही तुम्हाला आधीच संदेश ऑपवर एक स्वागत संदेश पाठवला आहे. कृपया पुष्टी करून घ्या.”

(राजू त्याचा संदेश ऑप उघडतो आणि एक स्वागत संदेश पाहतो ज्यात प्रोफाइल चित्रामध्ये एक्स वाय स्नेह बँकेची जाहिरात व स्टेटस मध्ये बँकेची घोषणा आहे.)

Message App
Welcome Mr. Raju!

घोटाळेबाज : “कृपया तुमच्या डेबिट कार्डचे तपशील पडताळणीसाठी टाका. तुम्हाला मला तपशील पुरवण्याची गरज नाही पण फक्त संदेश ऑपच्या अधिकृत क्रमांकावर टाका.”

राजू : “मी तो टाकला.”

हे करा :

- ✓ अनोळखी क्रमांकावरून खात्याचे तपशील मिळवण्यासाठी फोन आल्यावर उत्तर देताना सावध रहा.
- ✓ घोटाळ्याची जाणीव होताच लगेच तुमच्या बँक शाखेत तक्रार करा. पुढे अधिक आर्थिक तोटा टाळण्यासाठी तुमचे खाते ब्लॉक करा.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.

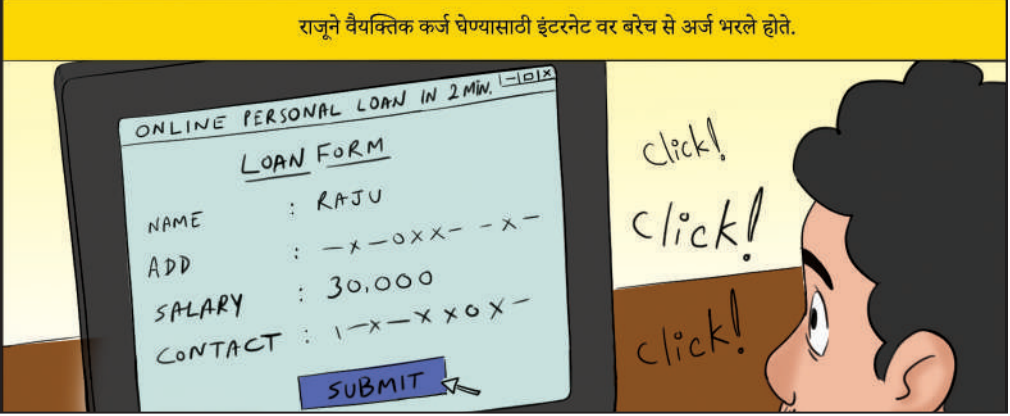


हे करू नका :

- ✗ सोप्या बँकिंग सेवा देऊ करणाऱ्या आणि संदेशवाहक ॲप द्वारे संदेश पाठवणाऱ्या अनोळखी फोन करणाऱ्यावर विश्वास ठेवू नका.
- ✗ आपल्या कार्डचे तपशील आणि ओटीपी कोणालाही देऊ नका.

१७. चोरलेली कागदपत्रे वापरून फसवे कर्ज घेणे

राजूने वैयक्तिक कर्ज घेण्यासाठी इंटरनेट वर बरेच से अर्ज भरले होते.



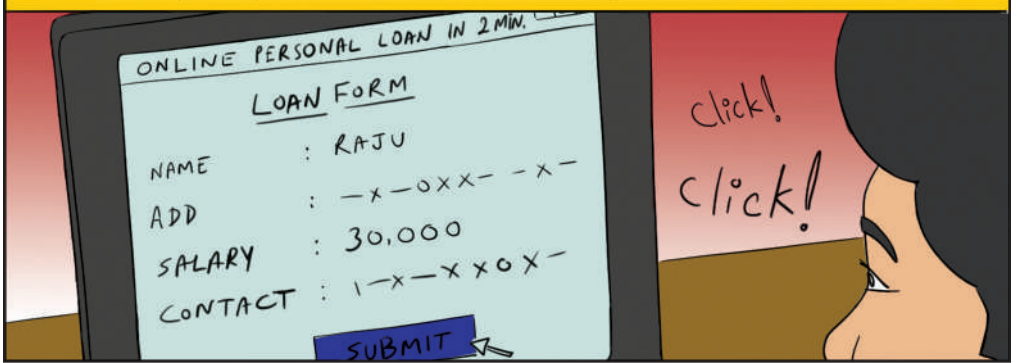
हे करा :

- ✓ कागदपत्रांच्या व्यवहाराच्या अंतिम उपयोगावर नेहमी नजर ठेवा.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in/>) वर नोंदवा.

राजू कर्जाच्या अर्जामध्ये आपले सर्व तपशील भरतो आणि प्रतिनिधीला एक रद्द केलेला चेक देतो.



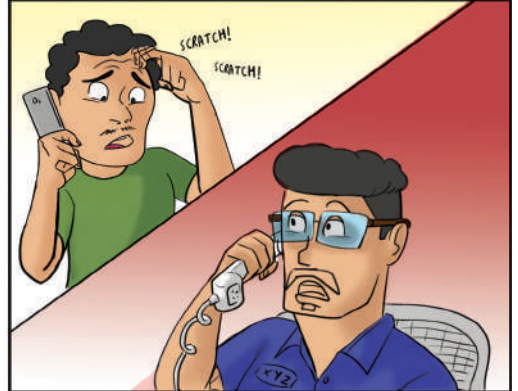
घोटाळेबाज राजूची कागदपत्रे वापरून कर्जासाठी अर्ज करतो पण कर्जाची रक्कम मिळण्यासाठी स्वतःचा खाते क्रमांक देतो.



एक महिन्या नंतर, राजूला कर्जाचा हप्ता रु.10,000/- भरण्याची सूचना देणारे पत्र मिळते.



हादरून, राजू त्याने कुठलेही कर्ज न घेतल्याचे कळवायला बँकेत फोन करतो. पण बँक त्याने भरलेला कर्जाचा अर्ज दाखवते.



हे करू नका :

- ✗ तुमची गोपनीय माहिती जसे आधार क्रमांक, पॅन क्रमांक, चेक बुक किंवा चेक; अनोळखी व्यक्तीला कधीही देऊ नका.

१८. सट्टेबाजीचे घोटाले

राजू जेकेएल क्रिकेटच्या नवीन येणाऱ्या हंगामासाठी उत्सुक होता.

राजू (विचारात): जेकेएल क्रिकेटचा नवा हंगाम आला आहे. सट्टा लावून सहज पैसे मिळवण्याच्या खूप गोष्टी ऐकल्या आहेत; मी ही प्रयत्न केला पाहिजे.



राजू इंटरनेटवर जेकेएल सट्ट्याचे गट शोधतो.



घोटाळेबाज (चॅट वर):
“स्वागत आहे, श्री. राजू.
तुम्ही पैजे बाबत चौकशी
केल्याचा आम्हाला आनंद
आहे. मी तुमची कशी
सहाय्यता करू शकतो?”





राजू: “मला ह्या जेकेएल
हंगामासाठी पैज
लावायची आहे.”

घोटाळेबाज (चॅट वर): “प्रथम, तुम्हाला xyzbetting.Com वर नोंदणी करावी लागेल, आणि स्वागताची भेट म्हणून तुमच्या निदान रु. 5000 च्या पहिल्या रीचार्जवर तुम्हाला रु. 5000 मिळतील.”



हे करा :

- ✓ फसवे ॲप / वेबसाइटने गंडवले गेल्यास, पुढचे व्यवहार टाळण्यासाठी त्वरित तुमच्या बँकेत कार्ड / खाते / UPI सेवा ब्लॉक करण्यासाठी फोन करा.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.

(राजू चमकदारपणे सजवलेले ऑप स्थापित करतो आणि केवळ ऑप पहिल्यांदा उघडूनच हा मोठा व्यवसाय असल्याचे स्वतःशी मान्य करतो.)

राजू: "मला ऑप स्थापित करायला लिंक पाठवा."

XYZ betting.com

घोटाळेबाज (चॅट बर): "आम्हाला तुमची रक्कम मिळाली नाही. कृपया ही विशेष संधी मिळवण्यासाठी लवकर पैसे पाठवा, साहेब."

राजू: "हो, मी ऑप स्थापित केला आहे आणि आत्ताच सुचने प्रमाणे रु. 5000 भरले. माझ्या खात्यात अधिक रक्कम कधी जमा होईल?"

घोटाळेबाज: "उद्या पर्यंत जमा होईल."

राजू (विचार करीत): हे थोडे संशयास्पद वाटतेय, पण मी सकाळ पर्यंत वाट पाहीन.

तथापि, राजू गंडवला गेला होता आणि चोराशी परत काही संपर्क झाला नाही.

हे करू नका :
✗ अनोळखी वेबसाइट वर पैसे अंतरित करू नका.

१९. फसवे लसीकरणाचे कॉल

एक दिवस, राजूला अनोळखी क्रमांका वरून फोन आला.

घोटाळेबाज : “मी स्थानिक आरोग्य केंद्रातून फोन करत आहे. आम्ही तुमच्या घरी लसीकरण सुविधा प्रदान करण्यासाठी फोन करत आहोत.”



राजू : “ओ! अच्छा. पण ते तर आम्ही फक्त कोविन ॲप द्वारेच करू शकतो, नाही का?”



घोटाळेबाज : “हो साहेब, पण घर बसल्या लसीकरणाची सुविधा ॲप वर उपलब्ध नाही.”



राजू : “काही अधिक शुल्क लागेल का?”

घोटाळेबाज : “नाही साहेब, हे विना शुल्क / मोफत आहे. मी तुमच्या पत्त्याची खाली करेन, आणि तुमची लसीकरणासाठी नोंदणी होईल. कृपया मला तुमच्या आधार आणि पॅन चा तपशील सांगा.”



हे करा :

- ✓ ओटीपी चे कारण समजण्यासाठी एसएमएस पूर्ण वाचा.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.

राजू : “माझा आधार क्रमांक 1234455 आहे, आणि माझा पॅन कार्ड क्रमांक adf1234 आहे.”

घोटाळेबाज : “धन्यवाद साहेब. कृपया थांबा. मी तुमच्या आधार आणि पॅन कार्डची नोंदणी करत आहे, तुम्हाला नोंदणी ओटीपी येईल. ते कृपया सांगा.”

(राजूला एक एसएमएस येतो- तुमचा सत्यापन कोड आहे 1234.)

राजू : “हो, ते 1234 आहे.”

घोटाळेबाज : “धन्यवाद साहेब. तुम्ही यशस्वी रित्या लसीसाठी नोंदणी केली आहे, आणि तुम्हाला लवकरच पुष्टीकरण येईल. कृपया आमचे आरोग्य अधिकारी तुमचे लसीकरण करायला आल्यास हा कोड द्या.”

कॉल बंद झाला. काही वेळा नंतर, राजूला एसएमएस आला-

‘प्रिय ग्राहक, तुमची रु. 50,000 ची वैयक्तिक कर्जा साठीची विनंती यशस्वी रित्या स्वीकारली गेली आहे.’

त्या चोराने राजूच्या वतीने रु. 50,000 चे कर्ज घेण्यासाठी राजूला त्याचा पॅन क्रमांक व ओटीपी देण्यास फसवून भाग पाडले. राजूच्या पॅन क्रमांकाच्या आधाराने कर्ज घेतल्यामुळे, राजू एक्स वाय जेड कंपनीला परतफेड करण्यास जबाबदार ठरतो.

हे करू नका :

- × तुमचे आधार, पॅन कार्डचे तपशील व ओटीपी परक्याना देऊ नका. पॅन कार्ड आधारित ओटीपी, बँक खात्यातून रोख रक्कम काढण्यासह वेगवेगळ्या आर्थिक सेवेसाठी वापरला जातो. त्यामुळे, तुमची गोपनीय माहिती जसे आधार आणि पॅन क्रमांक चोरांपासून सुरक्षित ठेवणे अतिशय महत्वाचे आहे.

२०. कोविड चाचणी - खोटी ऑनलाइन साइट

राजूला covid-19 ची चाचणी घरच्या घरी करायची होती. त्याने घरी चाचणी सुविधा प्रदान करणारे डायग्नोस्टिक्स केंद्र (रोगलक्षणसूचक केंद्र) इंटरनेटवर शोधले.

राजू : “नमस्कार, मला कोविड-19 चाचणी साठी नोंदणी करायची आहे.”

घोटाळेबाज : “अबक डायग्नोस्टिक्स केंद्रामध्ये आपले स्वागत आहे. कृपया नमूना संकलन करण्यासाठी तुमचा पत्ता द्या.”

राजू : “माझा पत्ता आहे 25, अबक गल्ली, मुंबई, महाराष्ट्र. चाचणीला किती पैसे लागतील?”

घोटाळेबाज : “त्याला ₹.1000 लागतील अधिक घरी संकलनाचे शुल्क ₹100. शिवाय, आगाऊ नोंदणी करीता तुम्हाला ₹.550 भरावे लागतील. मी तुम्हाला आगाऊ नोंदणी करता पैसे भरण्याची लिंक पाठवेन.”

राजूला चाचणी करायची घाई असल्यामुळे, त्याने आगाऊ रक्कम भरणे मान्य केले. त्याने सांगितलेली रक्कम त्याचे डेबिट कार्ड वापरून दिलेल्या लिंक वर भरली.

हे करा :

- ✓ नेहमी कुठल्याही प्रकारच्या चाचणीसाठी नोंदणी करताना, नोंदणीकृत पथॉलोजी प्रयोगशाळे द्वारेच करा.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.

त्यानंतर, त्या व्यक्तीने फोन ठेवला व फोन क्रमांक बंद केला.



राजू अस्वस्थ झाला आणि त्याने अबक डायग्नोस्टिक्सच्या
साइट वर सेवा क्रमांक शोधू लागला पण तो त्याला सापडला.



त्यानंतर राजूला आपण
गंडवले गेल्याची जाणीव
झाली.



हे करू नका :

- ✗ तुम्हाला शंका असताना आगाऊ रक्कम भरू नका. जर कोणी आगाऊ रक्कम मागत असेल, तर ही सावध राहण्याची बाब आहे आणि ते व्यवहार आवश्यक खबरदारी बाळगून करावे.

२१. वसूली प्रतिनिधीच्या रूपात (बहाण्याने) घोटाळेबाज



राजूने एक्स वाय जेड बँकेतून वाहन कर्ज घेऊन दुचाकी वाहन घेतले होते.

तथापि, राजूची नोकरी सुटली आणि कर्जाच्या हप्त्यांची परतफेड करण्यासाठी तो संघर्ष करत होता.

एक दिवस एक्स वाय जेड बँकेच्या वसूली प्रतिनिधीच्या रूपात एक घोटाळेबाज राजूच्या घरी भेटायला आला.

घोटाळेबाज : “मी एक्स वाय जेड बँकेचा वसूली प्रतिनिधी आहे. असे दिसते आहे की तुम्ही कर्जाच्या हप्त्यांची परतफेड चुकवली आहे. मी अधिकृतरीत्या तुमची गाडी जप्त करण्यास आलो आहे.”



घोटाळेबाज : “नाही नाही. ही बँकेची कार्यपद्धती आहे. तुम्ही जवळपास ₹ 20,000/- बँकेला देणे लागता. तुम्हाला आता निदान ₹. 5000/- भरावे लागतील नाहीतर मला तुमची गाडी न्यावी लागेल.”



राजू : “अहो नाही. कृपया माझी गाडी जप्त करू नका. माझी नोकरी गेल्याने मी मागचे काही हप्ते भरू शकलो नाही. मला नव्या नोकरीची संधी मिळाली आहे आणि मी वचन देतो की पुढच्या महिन्यापासून परतफेड करीन.”

हे करा :

- ✓ कुठलेही भुगतान / किंवा त्या साठी वचन देण्या आधी वसूली प्रतिनिधीची ओळख नेहमी तपासून घ्या. वसूली प्रतिनिधी कडे वसूली सूचनेची प्रत आणि बँके कडून अधिकृतता पत्र व बँकेने किंवा प्रतिनिधी कंपनी ने जारी केलेले ओळख पत्र असल्याची खात्री करून घ्या. तुम्ही बँकेच्या गुह्य शाखेत फोन करून फेर तपासणी ही करू शकता.

घोटाळेबाज पैसे घेतो. राजू : “ठीक आहे. मी आता रु. 5000/- भरतो आणि बाकीचे पुढच्या काही महिन्यात.”  घोटाळेबाज : “ठीक आहे साहेब. मी हे खास उपकार म्हणून करतो आहे. तुम्ही पावती व बाकी असलेली रक्कम थेट बँकेच्या शाखे मध्ये जमा करू शकता.”	काही दिवसा नंतर दुसरा वसूली प्रतिनिधी राजूच्या घरी भेटायला येतो:  वसूली प्रतिनिधी: “सुभ संघ्या साहेब. मी रवी, एक्स वाय जेड बँकेचा वसूली प्रतिनिधी. कृपया ही बँके तर्फे दिलेली वसूली सूचना पहा, ज्यात लिहिले आहे की तुम्ही तुमचे मागील तीन हफ्ते चुकवले आहेत आणि बँक गाडी जप्त करू शकते. तुम्ही एकतर पैसे थेट बँकेत भरू शकता किंवा पावतीच्या बदल्यात माझ्या हाती देऊ शकता.”
राजू गोंधळून “कसे काय? मी तुमच्या प्रतिनिधीकडे काही दिवसांपूर्वीच रु. 5000 दिले होते.” 	वसूली प्रतिनिधी: “हे शक्य नाही साहेब. मी एक्स वाय जेड बँकेसाठी ह्या क्षेत्राचा अधिकृत प्रतिनिधी आहे. कृपया माझे ओळखपत्र आणि देण्याची वसूली करण्यासाठी बँकेचे अधिकृत पत्र पहा. तुम्ही त्याचे ओळख पत्र पाहिले का? तुमच्या कडे पैसे दिल्याचा कुठला पुरावा आहे का?”  राजू : “अरे नाही!!! मी त्याच्यावर आंधळेपणाने विश्वास ठेवला!!!”
हे करू नका : ✗ कधीही योग्य पावती मिळाल्याशिवाय बँक / वसूली प्रतिनिधीला कुठलीही रोख रक्कम देऊ नका.	

२२. सामाजिक हित योजना घोटाळा

एक दिवस राजूला एका अनोळखी क्रमांका वरून फोन आला.

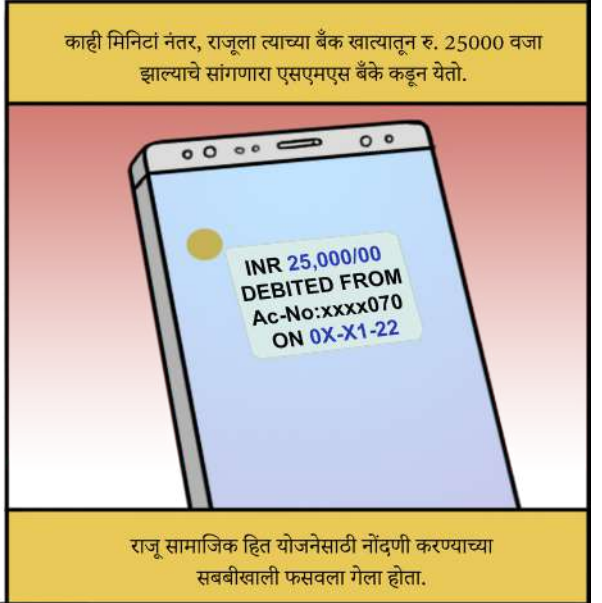
घोटाळेबाज : “मी कृषि विभागातून फोन करत आहे. तुमच्या खात्याचा तपशील किसान योजनेसाठी अद्ययावत केला गेलेला नाही, म्हणून तुमचे अनुदानाचे जवळपास रु. 12000/- आमच्याकडे न वापरताच पडून आहेत.”

राजू : “खाते अद्ययावत करण्यासाठी मी काय केले पाहिजे?”

घोटाळेबाज : “तुम्ही वेबसाइट वर जाऊन स्वतःच अपडेट करू शकता, किंवा तुम्ही मला तपशील दिलेल तर मी अपडेट करेन.”

हे करा :

- ✓ अनुदान मिळवण्यासाठी पैसे भरण्याआधी तुमच्या ग्राम पंचायत किंवा तहसीलदार कार्यालयात सरकारी योजनेच्या माहितीची खाली करून घ्या.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.



हे करू नका :

- ✗ असे फोन वरून अनुदान मिळण्याच्या कथेवर कधीच विश्वास ठेऊ नका.
- ✗ पाल लाभार्थी डेटा राज्य सरकार कडे आधीच उपलब्ध असतो.
- ✗ तुमच्या जिल्हा किंवा ग्राम पंचायतीतील तहसीलदार कार्यालयाच्या जन सेवा केंद्रात तुमची नोंदणी झाल्या नंतर सरकार तुम्हाला लाभ प्रदान करेल.
- ✗ कोणाला ही तुमचा ओटीपी देऊ नका.

२३. बहु स्तरीय विपणन (mlm) घोटाळे

राजूचा मित्र कृष्ण एका योजनेबद्दल, ज्यात चांगल्या कमाईची संधी आहे, समजावून घ्यायला राजूकडे आला.



कृष्ण : “नमस्ते राजू! मला एक कमीतकमी वेळ आणि गुंतवणूकीत पैसे कमवण्याची विलक्षण संधी आली आहे.”



राजू : “हो का? ऐकून भारी वाटते!!! मला त्या बद्दल अजून सांग. मला सगळे जाणून घ्यायचे आहे.”



कृष्ण : “तुला एक्स वाय जेड कंपनीचे उत्पादन रु. 20,000 ला विकत घ्यावे लागेल, आणि तुला रु.10,000 चा मोबाइल फोन फुकटात मिळेल. अजून तीन लोकांची नोंदणी केल्या नंतर, तू जसजसे अधिकाधिक लोक ह्या योजने अंतर्गत आणशील, तेव्हा तुला प्रति व्यक्ती रु. 3000/- कमिशन मिळेल.”



हे करा :

- ✓ तुम्हाला अश्या योजनेत खेचणाऱ्या लोकांपासून दूर रहा.
- ✓ बहु स्तरीय विपणन योजनेच्या खरेपणाची खाली करून घ्या. काही नेटवर्क विपणन योजना जसे पॉन्डि योजना, पिरॅमिड योजना इत्यादी;
- ✓ डायरेक्ट सेलिंग मार्गदर्शक तत्वे, 2016 आणि प्राइज चिट्स व मनी सरकुलेशन स्कीम्स (बंदी) अधिनियम, 1978 अंतर्गत भारतात बेकायदेशीर आहेत.
- ✓ ठामपणे नाही सांगा, अश्या योजनेचे प्रस्तावक तुमचे मित्र किंवा नातेवाईक असले तरीही.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.

राजू : “हा पैसे मिळवायचा आकर्षक मार्ग आहे. मी नेमलेले प्रतिनिधी माझ्या वतीने काम करीत असल्याने मला काम करायची गरजच नाही, आणि त्यांच्या विक्रीवर मला कमिशन मिळेल.”



कृष्ण : “होय राजू. म्हणूनच मी तुला भेटायला आलो. तू माझा प्रतिनिधी म्हणून माझ्या टीममध्ये येऊ शकतोस.”



राजूने लगेच अर्ज भरले आणि बहु स्तरीय विपणन कंपनीचा थेट विक्री प्रतिनिधी होण्यास संमती दिली.



तथापि विक्री झालीच नाही. कंपनीने ठरवलेले आणखीन 3 प्रतिनिधी भरती करण्याचे लक्ष्य तो पूर्ण करू शकला नाही, आणि त्याने कंपनी कडून विकत घेतलेले उत्पादन विकता न आल्याने त्याचे रु. 20,000 बुडले. त्याला कुठला फोनही मिळाला नाही.



हे करू नका :

✗ अनोळखी कंपनी मध्ये पैसे भरू नका आणि अनोळखी योजनेत नोंदणी करू नका.

२४. घर बसल्या नोकरीचे घोटाळे

घोटाळेबाज व्यक्ती इंटरनेट आणि सोशल मीडिया वर आकर्षक पगारासाठी घर बसल्या कामाच्या नोकऱ्या जाहीर करतो.
(घर बसल्या काम करून दर दिवशी रु.1000/- कमवा)



राजूला जाहिरात बघून खूप उत्सुकता वाटली आणि घर बसल्या कामासाठी नोंदणी करण्यासाठी त्याने लिंक वर क्लिक केले. राजूला अपरिचित व्यक्ती कडून फोन आला.



घोटाळेबाज : “सह्येब, आमच्या एजन्सी मध्ये नोंदणी करण्या करता धन्यवाद. आम्ही तुमचा सीव्ही पाहिला आणि घर बसल्या काम करायच्या नोकरीसाठी तुमची निवड केली आहे. तुम्हाला तुमच्या आधार व पॅन कार्डचे तपशील पुरवावे लागतील. आमच्या कंपनी धोरणा नुसार तुम्हाला काही अर्ज भरावे लागतील व काही कागदपत्रांवर तुमची सही सुद्धा लागेल.”



राजू : “धन्यवाद. मी सर्व अर्ज भरेन आणि माझ्या पत्त्याचा पुरावा व पॅन कार्डचे तपशील पाठवतो.”



हे करा :

- ✓ अनोळखी स्रोतां कडून गूगल फॉर्मस वर तपशील मागणाऱ्या लहान url पासून सावध रहा.
- ✓ ई-मेल, एसएमएस आणि पोर्टलस वर चुकीचे शब्दलेखन, व्याकरण यासाठी लक्ष ठेवा.
- ✓ व्यक्तीगत तपशील विचारणाऱ्या लिंक/फॉर्मस पासून सावध रहा.
- ✓ सधेी किंवा व्यवसायाच्या खरेपणाची खाली करण्यासाठी ई-मेलचे शीर्षक नेहमी तपासत जा.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.

घोटाळेबाज: "तुम्ही उद्यापासून काम सुरू करू शकता. तुम्हाला तुमचे काम www.workfromhome.com portal वर टाकावे लागेल. हे तुमचे यूजर आयडी व पासवर्ड आहे. तुम्हाला रु. 10,000/- ची सुरक्षा ठेव ही भरावी लागेल." 	 राजू सुरक्षा ठेव म्हणून चोराला रु. 10,000/- पाठवतो. नोकरी एक आठवडा भर सुरळीत चालली. राजूला नियमित पगार मिळाला. त्याला मानधन म्हणून रु. 7000/- मिळाले.
पुढच्या आठवड्यात, एजन्सीवाले चुका काढू लागले; त्यांनी चुका एकत्रित केल्या आणि राजूने सुरुवातीला सही केलेल्या कराराच्या नियम आणि अटीनुसार एजन्सी ला भरपाई म्हणून रु. 1 लाख चे बिल दिले.  भरपाई च्या स्वरूपात 1 लाख रुपये राजूला एकाच दिवशी वेगवेगळ्या क्रमाकांवरून एकापेक्षा जास्त छळणूकीचे व वसुलीचे फोन यायला सुरुवात झाली.	 त्याला 'वकील', 'पोलीस' इ. कडून कायदेशीर कारवाई करण्याचे धमकावणीवजा फोन आले आणि मग, ह्या सगळ्याला घाबरून, राजूने घोटाळेबाजाकडे एक लाख रुपये भरले.
हे करू नका : ✗ कधीही अनोळखी लोकांना ई-मेल द्वारे संवेदनशील, वैयक्तिक किंवा मालकी तपशील (आधार किंवा पॅन कार्ड) पाठवू नका. ✗ कधीही वकिलाचा सल्ला घेतल्या शिवाय कुठल्याही ऑनलाइन करारावर सही करू नका. ✗ कधीही नोकरी मिळवण्यासाठी पैसे देऊ नका; अस्सल कंपनी कधीही पैसे भरण्यास सांगत नाहीत.	

२५. ऑनलाइन खरेदी घोटाले

एक दिवस, राजूला एका अनोळखी क्रमांकावरून खूप स्वस्त किमतीच्या मोबाइल फोनची जाहिरात करणारा एसएमएस आला. कुतूहल वाटून, राजूने लिंक वर क्लिक केले आणि 50% सवलतीला स्मार्टफोन बघून चकित झाला.



राजू : “नमस्ते. मी तुमची वेबसाइट अबक पहिली, आणि मी एक नवीन स्मार्टफोन बघत आहे.”



घोटाळेबाज : “साहेब, आमच्या वेबसाइट मध्ये रुचि दाखवल्या बद्दल धन्यवाद. आमची कंपनी थेट निर्मात्या कडून फोन घेते, त्यामुळे तुम्हाला आमच्या वेबसाइटवर सर्वोत्तम किमती मिळतील.”

राजू : “ठीक आहे. मग मला व्ही 20 मोबाइल फोन घ्यायला आवडेल.”



घोटाळेबाज : साहेब, आपण ह्या वर्षाचा सर्वोत्तम फोन एस 20 एफई पहा, हा बाजारातला सर्वोत्तम स्मार्टफोन आहे. जर तुम्ही एक तासात पूर्ण पेमेंट करून ऑर्डर कराल, तर तुम्हाला मोबाइल फोनच्या वितरणा नंतर आणखी 50% रक्कम कॅशबॅक मिळेल.



हे करा :

- ✓ नेहमी सुरक्षित वेबसाइट वरून खरेदी करा. आम्ही असे सुचवू इच्छितो की ब्राऊजरच्या अॅड्रेस बार मध्ये, व्यवसाय सुरक्षित असल्याचे सूचित करणारे, वेबसाइट वर छोटेसे कुलूप चिन्ह किंवा 'https' दिसल्याची खात्री करून घ्या.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.

राजू : “बर. ह्या फोनची किंमत किती?” 	घोटाळेबाज : “साहेब, हीच वैशिष्टे असलेल्या फोनचा भाव सध्या बाजारात एक लाख पेक्षा जास्त आहे, पण तोच आम्ही फक्त रु. 50,000/- ला विकत आहोत. तुम्हाला रु. 25,000/- चे कॅशबॅक पण मिळेल.” 	
राजू : “ठीक आहे. मी ह्यावर विचार करेन आणि तुम्हाला कळवेन.” 	घोटाळेबाज : “साहेब, ही संधी फक्त पुढचे 50 मिनिटच चालू राहणार आहे, आणि फक्त काही फोनचाच साठा बाकी आहे. तुम्हाला संधीचा लाभ घेण्यासाठी लगेचच ऑर्डर आणि पेमेंट करावे लागेल.” 	
(राजूने विचार केला की त्याला रु. 50,000 किंमतीचा फोन परवडणार नाही, पण त्याने परत विचार केला की मोबाइल फोनच्या वितरणा नंतर त्याला 50% कॅशबॅक मिळेल, त्यामुळे ही त्याच्यासाठी उत्कृष्ट संधी आहे.)		
राजू : “ठीक आहे, मी लगेचच पेमेंट करेन.” 	घोटाळेबाज : “हा छान निर्णय आहे, साहेब. मी तुम्हाला पेमेंट करण्यासाठी लिंक पाठवतो आहे. कृपया लवकरात लवकर पैसे भरा.” 	राजूने पेमेंट केले आणि फोन मिळण्याची वाट पाहू लागला, पण त्याला कधीही कुठलाच मोबाइल मिळाला नाही. 
हे करू नका : ✗ कधीही अनोळखी वेबसाइट वरून खरेदी करू नका. ✗ कधीही फक्त गिफ्ट कार्ड, पैसे अंतरण इत्यादी माध्यमातून पेमेंट स्वीकारणाऱ्या ऑनलाइन विक्रेत्यांकडून काहीही विकत घेऊ नका. कारण अशा पेमेंटचा शोध लावणे आणि परत मिळवणे जवळजवळ अशक्य आहे. ✗ कधीही अनोळखी साइटला आगाऊ पेमेंट करू नका, कारण पैसे भरल्या नंतर उत्पादन मिळण्याची शक्यता धूसर असते.		

२६. सार्वजनिक वायफाय वापरुन घोटाले

तो रविवारचा दिवस होता. राजू आणि त्याचे कुटुंब खरेदीसाठी मॉल मध्ये गेले होते. राजूने काही कपडे व किराणा सामान खरेदी केले आणि पैसे भरायला काऊंटर वर गेला.

विक्री कर्मचारी: “तुमचे एकूण बिल रु. 12,000/- झाले, साहेब. तुम्ही कसे पेमेंट करणार, कार्ड की रोख?”

RECEPTION

राजू: “मी ऑनलाइन पैसे भरतो.”

राजूने पेमेंट ला सुरुवात केली पण नेटवर्कची समस्या येत होती.

राजू: “मला नेटवर्क मिळत नाहीय. तुम्ही मला ह्यासाठी मदत करू शकाल का?”



विक्री कर्मचारी: “साहेब, तुमचे नेटवर्क काम करत नसेल तर तुम्ही मोफत वायफाय ला जोडू शकता.”

हे करा :

- ✓ नेहमी सुरक्षित वायफाय नेटवर्क वापरले पाहिजे.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.

राजूने मोफत वायफाय जोडला आणि व्यवहार पूर्ण केले.

विक्री कर्मचारी: “इथे खरेदी केल्याबद्दल धन्यवाद, साहेब!”



दिवस चांगला गेल्याने राजू खुश होता. काही वेळा नंतर, त्याला बँके कडून सावध करणारे एसएमएस येऊ लागले. ‘तुमच्या खात्यातून रु. 14000/- आणि रु. 10000/- वजा झाले आहेत.’

राजू गोंधळात पडला.

त्याने शेवटचा व्यवहार मॉल मध्ये रु. 12,000/- चा केला होता, आणि हे व्यवहार वेगळे होते. त्याने त्याच्या मुलाला संदेशा बद्दल सांगितले.

मुलगा: “तुमचा शेवटचा व्यवहार काय होता, बाबा आणि तुम्ही कुठे केला तो?”



राजू: “मी शेवटचा व्यवहार मॉल मध्ये केला; मी बिल ऑनलाइन भरले. माझे नेटवर्क काम करत नव्हते म्हणून मी फोन मोफत वायफायला जोडला आणि पैसे भरले.”

मुलगा: “तुम्ही आर्थिक व्यवहारा साठी मोफत वायफाय वापरला का? ते सुरक्षित नाही, बाबा. हँकर लोक यूजर डेटा मिळवण्या साठी हा वायफाय वापरतात आणि ते बेकायदेशीर उद्देश्यांसाठी वापरतात.”



राजू: “खरंच? मला माहीतच नव्हते, बाळा.”



मुलगा: “जेव्हा तुम्ही वायफाय नेटवर्क आर्थिक व्यवहारा साठी वापरले, कोणत्यातरी हँकरला तुमच्या वैयक्तिक डेटा मिळाला आणि तुमच्या बँक खात्यातून अनधिकृत व्यवहार करण्यासाठी तो वापरला गेला.”



राजू: “अरे देवा!! मी मोठी चूक केली. आता आपण काय करू शकतो?”



मुलगा: “आपण लगेचच तुमच्या बँकेत जायला हवे आणि तुमचे खाते ब्लॉक करण्यास त्यांना सांगायला हवे.”



(राजू आर्थिक व्यवहारा साठी सार्वजनिक वायफाय वापरून हँकिंगचा बळी बनला होता.)

हे करू नका :

- ✗ सार्वजनिक वायफाय वापरू नका, खास करून आर्थिक व्यवहार करताना. सुरक्षा नसलेल्या सार्वजनिक वायफायला जोडलेले लॅपटॉप किंवा मोबाइल उपकरण हँकर करणे सोपे असते. हँकर तुमचे ई-मेल वाचू शकतात, पासवर्ड आणि अन्य अधिकारपत्रे चोरू शकतात.

२७. बनावट जाहिरात / ऑफर

पोस्टर:

"दिवाली बंपर ऑफर - केवळ एका घडयाळाच्या खरेदीवर रु. 2500 /- किमतीची तीन फास्ट्रूक घडयाळे अगदी मोफत!! त्वरा करा! मर्यादित काळासाठी संधी!! अधिक तपशीलासाठी कृपया क्र: 90xxxxxx99 वर फोन करा!

राजू : "वाह!! हे छान आहे! मी एक घडयाळ विकत घेईन आणि ३ मोफत मिळतील! असेही, ह्या दिवालीच्या सुट्टीत जेव्हा मी घरी जाईन, तेव्हा मला माझ्या भावंडांना द्यायला भेट घ्यायची होती! सवलत संपण्यापूर्वी फोन केलेला बरा."



राजू फोन लागल्यावर: "नमस्ते. मी तुमच्या ब्रँडेड घडयाळाची जाहिरात पाहिली. तुमचे दुकान कुठे आहे? मी खरेदीसाठी तुमच्या दुकाना मध्ये येऊ शकतो."



घोटाळेबाज : "साहेब! तुम्ही नशीबवान आहात. आम्ही ही ऑफर बंद करणारच होतो. तुम्हाला इथे येण्याची गरज नाही, साहेब. आम्ही वस्तू तुमच्या पत्त्यावर पाठवून देऊ."



हे करा :

- ✓ ब्रँडेड उत्पादना संबंधित असेल तर त्यांच्या अधिकृत वेबसाइट वर जाहिरातीची खाली करून घ्या.
- ✓ जाहिरात ब्रँडेड उत्पादनाची नसल्यास, दुकानात प्रत्यक्ष जाऊन किंवा वस्तू मिळाल्यानंतरच पैसे द्या.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.

राजू : “हे छान आहे! कृपया मला घड्याळ्यांचे फोटो पाठवा.”



घोटाळेबाज : “नक्की, साहेब. मी आधीच फोटो पाठवले आहेत. मी रक्कम अंतरित करण्यासाठी खात्याचे तपशील ही पाठवले आहेत. तुम्हाला ऑर्डर पक्की करण्यासाठी रु. 3000/- भरावे लागतील. एकदा हा व्यवहार पूर्ण झाला की आम्ही 3 दिवसांच्या आत तुम्हाला घड्याळं पाठवून देऊ. घाई करा, साहेब. सवलत संपण्यास शेवटची 30 मिनिटे आहेत. शुभ दिवाळी!!!”



राजू : “ठीक आहे. मी माझा पत्ता पाठवला. लगेचच पैसे पण पाठवतो.”



३ दिवसांनंतर:

राजू : “अरे देवा. अजूनही घड्याळं आली का नाहीत? त्यांचे फोन बंद आहेत. आता मी त्यांना कसे शोधू? मला वाटते माझे पैसे गेले.”



राजूने खरंच पैसे गमावले.

हे करू नका :

- ✗ जाहिरातीतल्या मोठ्या दाव्यांनी स्वतःची दिशाभूल करून घेवू नका. तुमच्या मेहनतीचे पैसे खर्च करण्याअगोदर चौकशी आणि खाली करून घ्या.
- ✗ वस्तू मिळाल्या शिवाय कुठलेही पेमेंट करू नका.

२८. बनावट कर्ज संधी/ ऑफर

राजू एक सर्वसाधारण शेतकरी आहे. एक दिवस, त्याला अनोळखी व्यक्तीचा फोन आला.

घोटाळेबाज : “नमस्कार, श्री राजू. आम्ही एक्स वाय जेड प्रायवेट लिमिटेड मधून बोलत आहोत. आम्ही तुमच्या विभागात शेतीसाठी एक नवीन योजना आणली आहे. आमच्या कंपनीने सवलतीच्या दरात कर्ज घेण्यासाठी तुम्हाला पात्र मानले आहे.”



राजू : “ओह! अच्छा. मला याची खूप मदत होईल. कसली ऑफर आहे?”



घोटाळेबाज : “आम्ही फक्त 3% व्याजाने ₹ 5 लाख पर्यंत खास कर्ज देतोय! ह्या कर्जाचा लाभ घेण्यासाठी, तुम्हाला पडताळणीसाठी तुमचे बँक खाते व आधारचे तपशील देणे आवश्यक आहे.”



राजू : “ठीक आहे. मी ह्या बद्दल विचार करेन आणि तुम्हाला कळवेन.”



हे करा :

- ✓ कर्ज घेण्या अगोदर, नेहमी कर्ज देणा-याची माहिती (जसे त्यांचा पूर्ण पत्ता / अधिकृत वेबसाइट, इत्यादी) तपासा.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.

घोटाळेबाज : “साहेब, ही संधी फक्त आजच्या दिवसासाठीच उपलब्ध आहे. ह्या संधीचा लाभ घेण्यासाठी तुम्हाला त्वरित रु. 5000/- प्रक्रिया शुल्क म्हणून पाठवावे लागतील. मी शुल्क अंतरित करण्यासाठी आमच्या खात्याचे तपशील पाठवले आहेत.”



घोटाळेबाज : “ठीक आहे साहेब!! आम्ही तुमच्या कर्जाच्या अर्जा बदल एका आठवड्यात कळवतो! धन्यवाद.”



राजू : “ओह! असे का? मग मी प्रक्रिया शुल्क आता पाठवेन. मी बाकीची माहिती सुद्धा तुमच्या क्रमांकावर लवकरच पाठवेन.”



राजू पैसे भरतो. तथापि, काही आठवड्यांनंतर सुद्धा, त्याला कंपनी कडून काहीच प्रतिसाद येत नाही, आणि ज्या क्रमांकावरून त्याला फोन आला होता तो आता बंद झाला आहे.



हे करू नका :

- ✗ तुमचे कर्ज मंजूर करण्यासाठी कधीही आधीच पैसे भरू नका. बँका आणि वित्तीय संस्था कधीही कर्ज मंजूरीसाठी आधीच शुल्क मागत नाहीत. शुल्क, असले तर, तुमच्या कर्ज रकमेतून वजा केले जाते आणि उरलेली रकम तुमच्या खात्यात अंतरित केली जाते.

२९. क्रेडिट कार्ड सक्रियीकरण घोटाले



घोटाळेबाज : “नमस्कार, श्री. राजू. मी एक्स वाय जेड बँकेतून बोलत आहे. तुमच्या नव्या क्रेडिट कार्डबद्दल अभिनंदन, साहेब.”

राजू : “हो, धन्यवाद; मला मिळाले ते.”

राजूला अलीकडेच एक्स वाय जेड बँकेचे क्रेडिट कार्ड वितरित झाले.

घोटाळेबाज : “बँकेच्या नीतीनुसार तुमचे क्रेडिट कार्ड फोनद्वारे चालू करण्यासाठी मी तुम्हाला फोन केला आहे. तुमच्या कार्डवरील माहितीची पुष्टी केलीत की तुम्हाला एक ॲक्टिवेशन कोड येईल. तो कोड घातला की तुमचे क्रेडिट कार्ड चालू होईल.”

घोटाळेबाजाकडे त्याच्या कार्डचे तपशील असल्यामुळे राजूने त्याच्यावर विश्वास ठेवला

राजू : “बरे. माझे कार्ड चालू करा.”

घोटाळेबाज : “तुमचे नाव आहे राजू देशपांडे. तुमचा पत्ता लोअर परेल, मुंबई, बरोबर?”

राजू : “हो बरोबर आहे.”

हे करा :

- ✓ पुढचे आर्थिक नुकसान टाळण्यासाठी तुमच्या बँकेला कार्ड/ बँक खाते/ UPI सेवा ब्लॉक करण्याकरिता फोन करा.
- ✓ घटनेची नोंद करण्यासाठी तुमच्या गृह शाखेला भेट द्या/ इमेल/ पत्र पाठवा.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.



घोटाळेबाज : “तुमचे कार्ड क्रमांक 45 ने सुरू होते. कृपया क्रमांकाची पुष्टी करा.”

राजू : “होय, क्रमांक आहे 4500 1000 1000 1000”

घोटाळेबाज : “पुष्टी करण्यासाठी धन्यवाद. कृपया कार्डची अंतिम तारीख व कार्डा मागचे कार्ड पडताळणी मूल्य (cvv) ह्यांची पुष्टी करा.”

राजू : “हो, कालबाह्य तारीख आहे 01/25 आणि 111 हा cvv क्रमांक आहे.”

राजू : “हो, तो आहे 123456.”

घोटाळेबाज : धन्यवाद साहेब. तुमचे कार्ड आला सक्रिय झाले आहे, आणि ह्याबद्दल तुम्हाला पुढच्या तासात एसएमएस येईल. तुमचा दिवस शुभ असो!

राजूला त्याच्या बँकेतून एक एसएमएस आला, त्याच्या क्रेडिट कार्ड मधून रु. 1.2 लाख वजा झाल्याचा. इथे, राजू क्रेडिट कार्ड सक्रिय करण्याच्या सबबीखाली फसवला गेला होता.

हे करू नका :

- ✗ तुमच्या कार्डाचे तपशील आणि ओटीपी कोणालाही देऊ नका.
- ✗ अनोळखी कॉल करणाऱ्यावर तुमचे क्रेडिट कार्ड चालू करण्यासाठी विश्वास ठेवू नका. क्रेडिट कार्ड तुमच्या मोबाइल बँकिंग ॲप द्वारे सक्रिय करता येते.
- ✗ तुमच्या कार्डाची माहिती / ओटीपी कोणालाही देऊ नका, बँक कधीही ओटीपी विचारत नाही.

३०. क्रेडिट कार्डची मर्यादा वाढवण्याचे घोटाळे

एके दिवशी, राजूला बँकेतून कॉल आला.

घोटाळेबाज : “नमस्कार, श्री. राजू. मी एक्स वाय जेड बँकेतून बोलत आहे. अभिनेदन, साहेब. तुमचे क्रेडिट कार्ड मर्यादा वाढण्या साठी पात्र आहे.”



राजू : “ओह, धन्यवाद. नवीन मर्यादा काय असेल?”



घोटाळेबाज : “तुमची आताची मर्यादा रु. 1 लाख आहे ती रु. 5 लाखपर्यंत वाढवली जाईल.”



राजू : “अरे, हे छान आहे!”



हे करा :

- ✓ पुढील व्यवहार टाळण्यासाठी कार्ड/ खाते/ UPI सेवा ब्लॉक करण्याकरता त्वरित तुमच्या बँकेशी संपर्क साधा.
- ✓ घटनेची नोंद करण्या साठी तुमच्या गृह शाखेला भेट द्या/ई-मेल/पत्र पाठवा.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.

घोटाळेबाज : “साहेब, तुम्हाला मोफत मर्यादा वाढवण्याचे कोड येईल त्याची पुष्टी करणे गरजेचे आहे. आपण पुढे जाऊया का?”



राजू : “हो, चालेल.”



घोटाळेबाज : “तुमच्या कार्डचा क्रमांक आहे 4500 1000 1000 1000. तुम्हाला एसएमएस द्वारे एक सक्रियीकरण कोड आला असेल. तो कृपया सांगा.”



राजू : “हो, ते आहे 123456.”



घोटाळेबाज : पुष्टी करण्यासाठी धन्यवाद. आता तुमच्या कार्डची मर्यादा वाढली आहे, आणि पुढच्या दोन तासात ह्याबद्दल तुम्हाला एसएमएस येईल. तुमचा दिवस शुभ असो!



काही वेळानंतर, राजूला त्याच्या बँके कडून क्रेडिट कार्ड मधून रु. 70,000/- वजा झाल्याचा एसएमएस आला.

हे करू नका :

- ✗ क्रेडिट कार्ड सक्रिय करण्यासाठी / त्यांची मर्यादा वाढविण्यासाठी अनोळखी फोन करणाऱ्यांवर विश्वास ठेऊ नका.
- ✗ तुमच्या क्रेडिट कार्डची माहिती/ ओटीपी कोणालाही देऊ नका.

३१. तुमच्या आधार कार्डाचे संरक्षण करणे

एक दिवस, राजू बँक खात्याशी आधार कार्ड जोडण्यासाठी त्याच्या बँकेच्या शाखेत गेला.

राजू : “मला माझे आधार कार्ड माझ्या बँक खात्याशी जोडायचे आहे.”

राजू आवश्यक कागदपत्रे जमा करतो.

बँक कर्मचारी : “कृपया आधारचा अर्ज व तुमच्या आधार कार्डाची प्रत द्या आणि तुमचे मूळ आधार कार्ड मला दाखवा.”

बँक कर्मचारी : “तुमच्या नोंदणीकृत मोबाइल क्रमांकावर आलेला ओटीपी मला सांगा.”

राजू : “मला कोणताही ओटीपी आलेला नाही.”

बँक कर्मचारी : “ओटीपी तुमच्या नोंदणीकृत मोबाइल क्रमांकावर पाठवला होता.”

राजू : “पण मला ओटीपी आला नाही. कृपया तुम्ही माझ्या बँक खात्याशी जोडलेला मोबाइल क्रमांक तपासू शकता का?”

बँक कर्मचारी : “मला बघू द्या. तुमच्या खात्याला जोडलेला मोबाइल क्रमांक आहे 98***25621.”

हे करा :

- ✓ तुमच्या बँक खात्याशी संबंधित मोबाइल क्रमांकाची खात्री करा.
- ✓ संशयास्पद व्यवहार जाणून घेण्यासाठी तुमचे बँक स्टेटमेंट व पासबुक नियमितपणे तपासा.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.



राजू : “पण हा माझा मोबाइल क्रमांक नाही.”

बँक कर्मचारी : “तुम्ही मागच्या आठवड्यात बँकेत आला होता.”

राजू : “मागच्या वेळी जेव्हा मी माझा केवायसी अर्ज जमा करण्यास बँकेत आलो होतो, तेव्हा बँकेतल्या एका गृहस्थानी मला अर्ज भरण्यास मदत केली व माझ्यासाठी अर्ज जमाही केला होता.”

बँक कर्मचारी : “प्रस्तुत केलेल्या अर्जा मध्ये त्याचा मोबाइल क्रमांक असू शकतो आणि तुमचे बँक खाते त्या क्रमांकाशी जोडले आहे. तो सहजच तुमच्या बँक खात्याचा गैरवापर करू शकतो. जमा करण्यापूर्वी तो अर्ज तुम्ही तपासायला पाहिजे होता.”

राजू : “मला ह्याची काहीच कल्पना नव्हती. मी खूप मोठी चूक केली. आता मी काय करू शकतो?”

बँक कर्मचारी : “आता तुमचा नोंदणीकृत मोबाईल क्रमांक बदलण्यासाठी अर्ज भरा.”

हे करू नका :

✗ अनोळखी व्यक्तींना तुमची गोपनीय माहिती जसे आधार आणि बँक खात्याचे तपशील कळू देऊ नका.

३२. कॅश बँक ऑफर वापरून ऑनलाइन घोटाळे

राजू इंटरनेट वर खूप सक्रिय असे आणि नेहमी ऑनलाइन खरेदीला प्राधान्य देई कारण ई-कॉमर्स वेबसाइट त्यांच्या उत्पादनांवर आकर्षक सूट देत असतात.

घोटाळेबाज : “नमस्कार साहेब! मी अबक.कॉम मधून बोलत आहे. साहेब, आम्ही अतिशय आनंदाने तुम्हाला कळवीत आहोत की तुम्ही हल्ली अबक.कॉम वरून केलेल्या खरेदीवर आम्ही तुम्हाला 50% कॅश बँक देत आहोत.”



राजू : “खरच का? 50% कॅश बँक प्रचंड आहे. खूप खूप धन्यवाद...!”



घोटाळेबाज : “तुम्ही आमचे सन्माननीय ग्राहक आहात, साहेब.”



राजू : “ठीक आहे सांगा तर. कॅश बँक माझ्या खात्यात कधी जमा होईल?”



घोटाळेबाज : “जास्त वेळ नाही लागणार, साहेब. तुम्हाला हे ऑप उघडावे लागेल, आणि तिकडे कॅश बँक संबंधित एक पॉप-अप संदेश येईल.”



हे करा :

- ✓ पुढील आर्थिक तोटा टाळण्याकरता तुमच्या गृह शाखेला कळवा आणि तुमचे खाते ब्लॉक करा.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.

राजू : “आता मी ऑप उघडला. तो मला अबक.कॉम ला रु. 20000/- भरण्याचा संदेश दाखवत आहे.”

घोटाळेबाज : “बरोबर आहे, साहेब. कॅश बँक तुमच्या खात्यात जमा करण्यासाठी आम्हाला तुमची परवानगी घेणे आवश्यक आहे. तर कृपया "pay" वर क्लिक करा.”

राजू : “ठीक आहे आता ते माझा UPI पिन विचारात आहे.”

घोटाळेबाज : “कृपया तुमचा पिन टाका कारण तो फक्त पडताळणीसाठी आहे.”

राजू : “ठीक आहे.”

घोटाळेबाज : “धन्यवाद, साहेब. लवकरच तुमच्या खात्यात पैसे जमा होतील.”

(राजूने UPI पिन टाकता क्षणी, त्याच्या खात्यातून रु. 20,000/- ची रक्कम वजा झाली. राजूने घोटाळेबाजाला फोन करायचा प्रयत्न केला पण लागला नाही.)

हे करू नका :

- ✗ फोन करणाऱ्यावर आंधळेपणाने विश्वास ठेऊ नका; ऑफरची सत्यता पारखण्यासाठी कंपनीची अधिकृत वेबसाइट पाहून खाली केली पाहिजे.
- ✗ पैसे मिळवण्यासाठी UPI पिन लिहू किंवा सांगू नका कारण ते फक्त पैसे पाठवण्या करता लागते.

३३. सवलत घोटाळे

राजूला त्याच्या मुलीच्या वाढदिवस समारंभा साठी एक हॉल आरक्षित करायचा होता, म्हणून त्याने इंटरनेट वर उपलब्ध पर्याय शोधले आणि चौकशी साठी तपशील दिले.
काहीच क्षणां नंतर, राजूला एक कॉल आला.

घोटाळेबाज : "नमस्कार, मी एक्स वाय जेड हॉटेल मधून बोलतोय. तुम्ही आमच्या वेबसाइटवर आरक्षणा बदल चौकशी केली होती, मी तुमची काही सेवा करू शकतो का?"

राजू : "मला तुमच्या हॉटेल मधील बँकेट हॉल बदल विचारायचे होते. हॉल भाड्याने उपलब्ध आहे का?"

घोटाळेबाज : "हो, बँकेट हॉल साठी भाडे पर्याय उपलब्ध आहेत."

राजू : "काय किंमत आहे? मला माझ्या मुलीच्या वाढदिवसा साठी आरक्षित करायचे आहे."

घोटाळेबाज : "तासा प्रमाणे दर आहेत साहेब. ते एका तासाला रु. 2500/- आहे."

राजू : "हॉल XX-XX-XX तारखेला, रात्री 8 ते 10 उपलब्ध आहे का?"

घोटाळेबाज : "होय साहेब, उपलब्ध आहे. आरक्षण पूर्ण प्रक्रिया म्हणून, टोकन क्रमांक देण्यासाठी तुम्हाला रु. 1000/- मला पाठवावे लागतील."

राजू : "मी पैसे भरण्या साठी तुमच्या कार्यालयात येतो."

हे करा :

- ✓ कुठले ही करार किंवा ऑफर देणाऱ्या व्यक्ती/ संस्थेच्या सत्यतेची नेहमी खाली करून घ्या.
- ✓ ओटीपी एसएमएस मध्ये अन्य तपशील जसे अपेक्षित व्यवहाराची रकम/ व्यापाऱ्याचे नाव/ लाभार्थीचे नाव असते. वापरण्या अगोदर नेहमी दक्ष करणारे ओटीपी एसएमएस पूर्ण वाचा.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.



चोटाळेबाज : “तुम्ही ऑनलाइन क्रेडिट/डेबिट कार्डने पैसे भरल्यास 20% सवलत मिळेल.”

राजू : “ठीक आहे मी ऑनलाइन भरतो.”

चोटाळेबाज : “मला तुमच्या कार्ड वरील 16 अंकी कार्ड क्रमांक, सिव्हीव्ही आणि अंतिम तारीख सांगा.”

राजू : “16 अंकी क्रमांक आहे 5869*****456, CVV आहे 256 आणि अंतिम तारीख आहे 11/24.”

चोटाळेबाज : “तुम्हाला एक ओटीपी येईल; तो कृपया सांगा.”

राजू : “ओटीपी आहे 4256.”

चोटाळेबाज : “तुमचे आरक्षण पक्के झाले आहे, साहेब. तुम्हाला लवकरच एक एसएमएस येईल.”

राजू : “ठीक आहे. धन्यवाद!”

काही वेळा नंतर, राजूला त्याच्या फोन वर दक्ष करणारा एसएमएस आला. ‘तुमच्या खात्यातून 50,000/- रुपये घजा झाले आहेत.’ राजूने त्वरित त्या व्यक्तीला फोन लावला, पण त्याने उचलला नाही. राजूच्या लक्षात आले की ती व्यक्ती चोटाळेबाज होती आणि त्याने त्या व्यक्तीला कार्डचे कोणतेही तपशील चापला नको होते.

हे करू नका :

✗ कोणालाही तुमच्या क्रेडिट/डेबिट कार्डचे तपशील आणि ओटीपी सांगू नका.

३४. देणगी घोटाले

राजू एका सरकारी शाळेत शिक्षक आहे. त्याने एक बातमी पाहिली की अभिनेता मोनू सरकारी शाळेच्या विद्यार्थ्यांना स्मार्टफोन भेट देत आहे.

**NEWS
REPORT**

बातमी: 'अभिनेता मोनू सरकारी शाळेच्या विद्यार्थ्यांना 100 स्मार्टफोन भेट देताना दिसले.'

राजूने इंटरनेट वर अभिनेत्याच्या धर्मादाय संस्थेचा शोध लावला आणि मिळालेल्या क्रमांकावर फोन लावला.

**MONU
charity
Foundation**

राजू: "नमस्कार साहेब. ही अभिनेता मोनूची धर्मादाय संस्था आहे का??"

घोटाळेबाज: "होय साहेब. हा त्यांच्या कार्यालयाचा क्रमांक आहे. मी त्यांचा वैयक्तिक सचिव आहे. मी तुमची काय सेवा करू शकतो?"

हे करा :

- ✓ नेहमी संस्था खरी आहे की नाही हे बघण्यासाठी सरकारी वेबसाइट डेटाबेस वर धर्मादाय संस्था अस्तित्वात असल्याची खात्री करून घ्या..
- ✓ नेहमी जागरूक रहा कारण खोटी वेबसाइट अगदी अससल चॅरिटी साइट सारखी दिसू शकते, फक्त पैसे कुठे पाठवायचे ह्याचे तपशील बदललेले असू शकतात.
- ✓ घोटाळेबाज खूपदा अति दबावाची युक्ति वापरतात, जसे की किती निकड आहे यावर जोर देणे आणि अत्यंत भावनिक भाषा वापरणे.
- ✓ नेहमी त्वरित देणगी देण्याची गरज असल्याचा दावा करणाऱ्या पासूनही सावध रहा.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.

राजू : “साहेब. मी राजू, XXXX सरकारी शाळेतून बोलतोय. मी तुमच्या विद्यार्थ्यांना देणगी देण्याची बातमी पाहिली. साहेब, आमच्याकडे 100 गरीब विद्यार्थी आहेत ज्यांना लॅपटॉप/स्मार्टफोन परवडत नाही. तुम्ही आम्हाला काही मदत करू शकता का साहेब?”



घोटाळेबाज : “नक्की! गरीब मुलांच्या वतीने आमच्यापर्यंत पोचल्याबद्दल धन्यवाद. मी मदतीचे आश्वासन देतो.”



राजू : “ते छान होईल! साहेब.”



घोटाळेबाज : “ठीक आहे. कृपया तुमचा पत्ता द्या. आम्ही तुम्हाला 100 स्मार्टफोन पाठवू. तथापि, आमच्याकडून तुम्हाला फोन पाठवण्यासाठी तुम्हाला आजच्या आज रु. 50,000/- टोकन नोंदणी शुल्क म्हणून भरावे लागतील. फोन एका आठवड्यात पाठवले जातील आणि वितरित झाल्यावर आम्ही नोंदणी शुल्क परत करू.”



राजू : “ठीक आहे साहेब. मी तुम्हाला नोंदणी शुल्क लगेच पाठवेन. कृपया तुमच्या खात्याचे तपशील कळवा.”



राजू ने पैसे भरले, पण त्याला नंतर कळले की असे कुठलेही मोबाइल फोन सरकारी शाळेच्या विद्यार्थ्यांना देण्यात आले नव्हते. राजूला लक्षात आले की देणगी देण्याच्या नावाखाली घोटाळेबाजाने त्याला फसवले.

हे करू नका :

- ✗ फक्त गूगल शोधाच्या आधारवर कोणत्याही क्रमांकावर खाती केल्याशिवाय फोन करू नका.
- ✗ कराराच्या खरेपणाची/अधिकृततेची खाती केल्याशिवाय थेट पैसे पाठवू नका.

३५. फिक्स्ड डिपॉजिटवर ओव्हरड्राफ्ट

राजू एक वरिष्ठ नागरिक आहे, जो हल्लीच त्याच्या नोकरीतून निवृत्त झाला आहे. त्याला सेवानिवृत्तीची खूप मोठी रकम मिळाली आहे, जी त्याला गुंतवायची होती. एक दिवस राजूला प्रतिष्ठित बँकेच्या कर्मचारी/प्रतिनिधी च्या रूपात बोलणारा एक फोन आला, जो मोठ्या व्याज दरासह नवीन योजनेची जाहिरात करत होता.



राजू : “नमस्कार! तुम्हाला खाली आहे का मला ९% व्याज दर मिळेल? कारण कुठलीही बँक ७.२% पेक्षा जास्त व्याज देत नाहीय.”

घोटाळेबाज : “हो साहेब, ही फक्त मर्यादित काळासाठी खास योजना आहे.”



राजू : “ठीक आहे मी बँकेत येतो आणि फिक्स्ड डिपॉजिट खाते उघडतो.”

घोटाळेबाज : “साहेब, तुम्ही ज्येष्ठ नागरिक असल्यामुळे आमची बँक तुमच्या घरी एक प्रतिनिधी पाठवेल.”



राजू : “नाही, मी माझे पैसे अनोळखी लोकांच्या हाती देऊ शकत नाही.”



हे करा :

- ✓ सही करण्या पूर्वी सगळी कागदपत्रे तपासा.
- ✓ बँकेच्या शाखेत जाणे किंवा ओळखीच्या व्यक्तीच्या सहाय्याने इंटरनेट वरून व्यवहार करण्याला प्राधान्य द्या.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.

घोटाळेबाज : “साहेब, पैसे हातात देण्याची काहीच गरज नाही. तुम्हाला फक्त रद्द केलेला चेक द्यायचा आहे. मी काळजी घेईन की तुमचे पैसे रोख काढले जाणार नाहीत आणि फक्त फिक्स्ड डिपॉजिट खात्यात ठेवले जातील.”

राजू : “ठीक आहे. त्याला चेक घेऊन जायला सांगा.”

घोटाळेबाज चेक जमा करायला राजूच्या घरी जातो आणि वेगळ्या अर्जावर सही घेतो, जे राजू सही करण्या पूर्वी तपासत नाही.



दुसऱ्या दिवशी, घोटाळेबाज राजूच्या प्रतिनिधी म्हणून शाखेत जातो आणि फिक्स्ड डिपॉजिट करण्यासाठी चेक भरतो. पण तो राजूला फिक्स्ड डिपॉजिट ची खोटी पावती देतो आणि खरी स्वतःकडेच ठेवतो.







घोटाळेबाज राजूचा प्रतिनिधी म्हणून बँकेत जातो आणि राजूने सही केलेला ओव्हरड्राफ्टचा अर्ज देतो, ज्यावर ओव्हरड्राफ्ट मिळवण्यासाठी घोटाळेबाजाचे बँक खाते क्रमांक असतो.

एका दिवसा नंतर, राजूला फिक्स्ड डिपॉजिटवर ओव्हरड्राफ्ट दिल्याचा एसएमएस येतो आणि शाखेत भेट दिल्यावर, आपल्याला मिळालेली एफडी ची पावती नकली असल्याचे कळून त्याला धक्का बसतो.

हे करू नका :

- ✗ महत्वाची कागदपत्रे/चेक अनोळखी लोकांच्या हाती सोपवू नका.

३६. स्वतंत्र इंटरनेट नोकरी (फ्री लांस इंटरनेट जॉब्स) वापरुन घोटाळे

एक दिवस, राजूला स्वतंत्र नोकरी साठी त्याची इच्छा विचारणारा एसएमएस आला. राजू बेरोजगार असल्याने त्याने त्वरित एसएमएस मध्ये लिहिलेल्या क्रमांकावर फोन लावला.

राजू : “नमस्ते, मला स्वतंत्र नोकरी संबंधित एसएमएस आला होता. नोकरीचा तपशील काय आहे?”



राजू : (हे खूप सोपे आहे, हे तर माझा मुलगा ही करू शकतो.) “ठीक आहे मी उत्सुक आहे.”



ॲप डाउनलोड केल्यानंतर राजूने कामाची सुरुवात केली. काम बरोबर दिसत होते. तथापि, त्याला माहीत नव्हते की घोटाळेबाज त्याच्या लॅपटॉप वरच्या त्याच्या सर्व हालचालींवर नजर ठेवून होता.



हळूहळू घोटाळेबाजाला त्याच्या ॲप द्वारे राजूच्या लॅपटॉपवरून सर्व सुरक्षित ओळखपत्रे मिळवणे शक्य झाले. त्याचा दुष्ट हेतु न जाणता, राजूने ॲप वापरणे चालू ठेवले. घोटाळेबाजाला राजूच्या ई-मेलमध्ये प्रवेश मिळाल्याने घोटाळेबाजाला राजूच्या ई-मेल वर पाठवलेला ओटीपी सुद्धा मिळू शकत होता.

हे करा :

- ✓ ऑफरच्या खरेपणाची खाली काम देणाऱ्या संबंधित व्यवसायाच्या अधिकृत वेबसाइट वर करा.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.

काही दिवसा नंतर, राजूला एसएमएस आला की रु. 50,000/- त्याच्या खात्यातून वजा झाले आहेत.
राजूला त्याचे खाते कसे धोक्यात आले किंवा पैसे कसे वजा झाले ह्याचा काहीच सुगावा लागला नाही.



तपास केल्या नंतर, हे समजले की त्याच्या लॅपटॉपमध्ये वाईट ॲप आहे, जे त्याच्या सर्व हालचाली पाहत होते आणि पासवर्ड नोंदवले जात होते.



हे करू नका :

- ✗ एसएमएस, ई-मेल किंवा झटपट संदेश ॲप च्या माध्यमातून, विशेषतः अनोळखी व्यक्ती कडून, पाठवलेल्या लिंकवरून, खरेपणाची खात्री केल्याशिवाय ॲप्लिकेशन डाउनलोड करू नका.

३७. प्रचंड व्याज दर आणि छळ करणाऱ्या डावपेचांसह बेकायदेशीर कर्ज वितरण ॲप

राजू आणि रामू जिवलग मित्र होते. एक दिवस, राजू रामूला भेटला आणि त्याच्या आर्थिक अडचणी बद्दल सांगू लागला.



राजू कर्ज देणारा अधिकृत असल्याची खात्री न करताच मोबाइल ॲप डाउन लोड करतो. काही वेळातच त्याच्या बँक खात्यात रु. 5000/- जमा होतात.

हे करा :

- ✓ ॲप डाउनलोड करताना आणि तुमच्या मोबाइल फोनच्या डेटा मध्ये प्रवेश करायची परवानगी देताना सावध रहा.
- ✓ नेहमी ज्या कंपनी/nbfc चे ॲप कर्ज मिळवण्या करिता वापरत आहात त्याच्या नोंदणीची स्थिति आणि अटी व शर्ती, त्या nbfc मधून कर्ज घेण्या आधी https://www.rbi.org.in/Scripts/BS_NBFCList.aspx वर तपासून घ्या.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.

7 दिवसांच्या आत, राजूला रु. 7500/- ची परतफेड करण्यासाठी फोन येऊ लागले. राजूने अजूनही जुने कर्ज फेडण्यासाठी पैशाची सोय केली नव्हती आणि रु. 5000/- च्या कर्जा साठी रु. 7500/- च्या वसुलीची मागणी ऐकून तो चकित झाला. राजू त्याचा दुसरा मित्र, लक्ष्मण, कडे गेला.



राजू : “मी अश्या कल्पनेत होतो की मी माझ्या कर्जाची अल्प व्याज शुल्का सहित परतफेड करेन, पण हा ऑप प्रचंड व्याज आणि अन्य बरेच शुल्क लावत आहे. आता मी काय करू?”



लक्ष्मण: “अरे! तू त्याची भारतीय रिझर्व्ह बँकेकडे किंवा अन्य कुठेही वैध नोंदणी असल्याची खाली केली होतीस का? अन्यथा, ते कुठल्याही नियमा अंतर्गत येणार नाहीत, आणि तू करारानुसारच भरपाई करण्यास बांधील आहेस. नेहमी वित्तीय कंपनीची (nbfc) भा. रि. बँकेकडे नोंदणी व परवाना मिळाला आहे की नाही हे भा. रि. बँकेच्या वेबसाइटवर तपासावे.”



हे करू नका :

- ✗ कोणतेही मोबाइल ऑप कुठलेही कागदपत्रे व क्रेडिट स्कोर न तपासता लगेच कर्ज देत असल्यास सावध रहा आणि नेहमी लागू होणारे व्याज दर तपासा.

३८. व्यापारी/इंधन दुकानात कार्ड क्लोनिंग

एके दिवशी राजू आपल्या मितासोबत उपहारगृहात जेवायला गेला. त्याने वेटरला बोलावले.

वेटर: “स्वागत आहे साहेब.
कृपया बसा.”

राजू: “धन्यवाद.”

वेटर: “मी तुमची काय सेवा
करू शकतो, साहेब?”

राजू: “मी तुमचे मेन्यू कार्ड
बघू शकतो का?”

व्यवस्थापक: “नक्की, साहेब. हे आहे आमचे
मेन्यू कार्ड.”

राजूने जेवण मागवले आणि मिता बरोबर आनंदात जेवला.

राजू: “कृपया बिल आणा.”

हे करा :

- ✓ डेबिट/क्रेडिट कार्ड द्वारे व्यवहार करताना नेहमी तुमचा पिन क्रमांक लपवा.
- ✓ नियमित कालांतराने पिन बदला.
- ✓ नेहमी व्यापाऱ्यांना/ विक्रेत्यांना तुमच्या समक्ष कार्ड स्वाईप करायला सांगा.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.



(वेटरने कार्ड घेतले, राजू पासून लांब गेला आणि राजूचे लक्ष नसताना स्कीमर मधून कार्ड स्वाईप केले.)



नंतर, कार्डचे स्किम केलेले तपशील एका घोटाळेबाजाला देण्यात आले ज्याने सर्व तपशीलांसह कार्ड क्लोन केले आणि त्या तपशीलांचा वापर करून राजूच्या खात्यातून पैसे काढले.

हे करू नका :

- ✗ कोणाला ही तुमचा डेबिट/क्रेडिट कार्डचा पिन देऊ नका.
- ✗ क्रेडिट आणि डेबिट कार्ड तुमच्या नजरेपासून दूर होऊ देऊ नका.

३९. ओळखीच्या व्यक्ती/ परिवार/ कुटुंबीयां सोबत माहिती सामाईक करून

राजू अतिशय मैत्रीपूर्ण आणि मदत करणारा माणूस आहे पण तो आर्थिक ओळखपत्रे व बँकेची माहिती सुरक्षित ठेवण्यात हलगर्जीपणा करत असे.
एक दिवस राजूला त्याचा मित्र, केशव, चा फोन आला.

केशव: "नमस्कार, राजू. तुला बोलायला वेळ आहे का?"

राजू: "हो, केशव; बोल ना."

राजू: "ठीक आहे मी तुला माझ्या कार्डची माहिती पाठवतो."

राजूने त्याच्या मित्राला आपल्या क्रेडिट कार्डचा फोटो पाठवला.

केशव: "एक उत्कृष्ट संधी आहे एक्स वाय जेड ई कॉमर्स वेबसाइट वर. त्या साठी अबक बँक द्वारे दिलेले क्रेडिट कार्ड आवश्यक आहे आणि तू हे कार्ड वापरतोस. तू मला तुझ्या कार्डची माहिती फोनवर देऊ शकतो का? मी तुला नंतर पैसे देतो."

"I received your card details.
Thank you so much."

राजूचे मित्र नेहमी त्याचे क्रेडिट कार्ड ई-कॉमर्स वेबसाइटवरील सवलतींचा लाभ घेण्यासाठी वापरत असत, आणि तो खूपदा त्याच्या कार्डची माहिती त्याच्या मित्रांना फोन वरून देत असे.

हे करा :

- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.
- ✓ नियमित कालांतराने पिन बदला.

एका महिन्या नंतर, राजूला त्याच्या मोबाइल क्रमांकावर एक एसएमएस आला आणि कार्ड कुठे वापरले आहे त्याला कळना.



राजूने त्वरित त्याच्या सर्व मित्रांना फोन केले, पण सगळ्यांनी सांगितले की त्यांनी हे व्यवहार केलेलेच नाहीत.



राजूने बँके कडे तक्रार नोंदवली. बँकेने त्याला पुढे कळवले की विवादित व्यवहार, ऑनलाइन व्यवसाय साईट वर झाला आहे.



केशव: “राजू, काही दिवसांपूर्वी माझा मोबाइल फोन हरवला आणि माझ्या फोन मध्ये तुझ्या कार्डची माहिती आहे. मला भीती वाटते की त्यामुळे हे व्यवहार झाले असतील.”



राजू: “अरे! केशव, ह्या घटनेबद्दल तू मला सांगायला हवे होतेस. मी कार्ड ब्लॉक केले असतं. मी फोन वरून माझ्या कार्डची माहिती द्यायला नको होती.”

हे करू नका :

- ✗ तुमच्या कार्डची माहिती सोशल मिडिया किंवा संदेश ॲप वरून, जरी प्राप्तकर्ता तुमचा मित्र / नातेवाईक / कुटुंबीय असले तरी, पाठवू नका.

४०. पैसे पाठवण्याचे (पेमेंट स्पूफिंग) फसवे ऑप

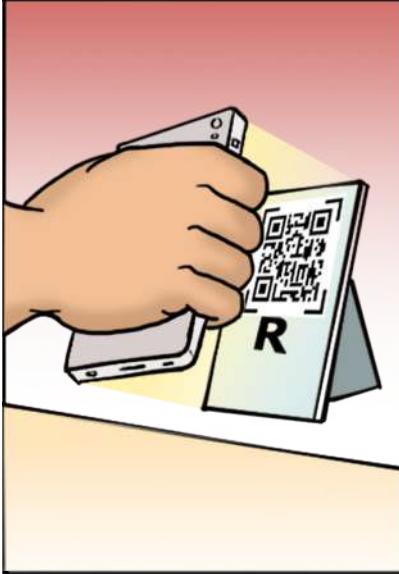
राजू एक किरकोळ दुकानाचा मालक आहे. तो त्याच्या दुकानात बसलेला असताना एक ग्राहक आला आणि त्याने काही खरेदी केली.

ग्राहक (घोटाळेबाज): “मी तुमच्या दुकानाचा क्यु आर कोड वापरून एक्स वाय जेड ऑप द्वारे पैसे भरू शकतो का?”

राजू: “हो, इथे आहे कोड. कृपया स्कॅन करा आणि पैसे भरा.”

हे करा :

- ✓ कधीही UPI द्वारे व्यवहार केल्या नंतर नेहमी तुमचे बँक खाते तपासून व्यवहाराची खात्री करा.
- ✓ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (<https://cybercrime.gov.in>) वर नोंदवा.



ग्राहकाने फसव्या एक्स वाय जेड ॲप ने कोड स्कॅन केला. त्याने बनावट भरपाई सूचना/ स्क्रीनशॉट तयार केला आणि राजूला दाखवला.



त्या दिवसाच्या अखेरीस, राजूने त्याच्या दुकानाच्या खात्याचा हिशोब जुळवण्यासाठी फेर पडताळणी करून पाहिली तेव्हा त्याच्या लक्षात आले की एक रकम अजून त्याच्या खात्यात जमा झालेली नाही. आता त्याला जाणवले की त्याला नकली स्क्रीनशॉट दाखवून फसवले गेले आहे.



फसवल्यावर, राजू बँकेकडे तक्रार ही करू शकत नव्हता किंवा फसवणुकीचा रिपोर्ट ही करू शकत नव्हता, कारण प्रत्यक्षात पैसे अंतरित कधी झालेच नव्हते आणि राजूकडे ग्राहकाची काहीच माहिती नव्हती.

हे करू नका :

✗ प्रत्यक्ष रकमेची पावती मिळाल्या शिवाय आर्थिक व्यवहार पूर्ण करू नका.







भारतीय रिज़र्व बैंक

<https://cms.rbi.org.in/>
