राजू आणि चाळीस चोर

आर्थिक घोटाळेबाजांच्या मोडस ऑपेरेंडीवर 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 सुरू 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 फसवणुकींपासून 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 करुन केलेली फसवणूक	५
४	क्रेडिट कार्डचे वार्षिक शुल्क माफ करणे - खोटी ऑफर	७
५	एटीएम कार्ड स्कीमिंग फसवणूक	९
६	स्क्रीन शेअरिंग ॲप / रिमोट ॲक्सेस ॲप वापरुन 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 ॲप बँकिंग घोटाळा	३१
१७	चोरलेल्या कागदपत्रे वापरुन फसवे कर्ज घेणे	३३
१८	सट्टेबाजीचे घोटाळे	३५
१९	फसवे लसीकरणाचे कॉल	३७
२०	कोविड चाचणी - खोटी ऑनलाइन साइट	३९

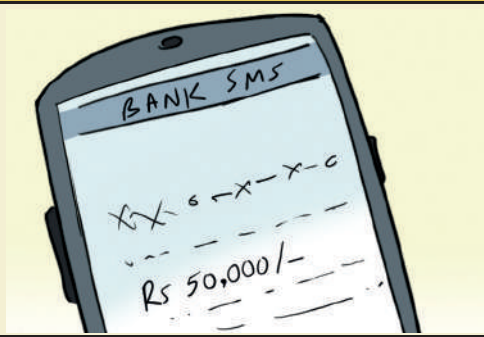
क्रम सं	विषय	पृष्ठ संख्या
२१	वसूली प्रतिनिधीच्या रूपात (बहाण्याने) घोटाळेबाज	४१
२२	सामाजिक हित योजना घोटाळा	४३
२३	बहुस्तरीय विपणन (mlm) घोटाळे	४५
२४	घर बसल्या नोकरीचे घोटाळे	४७
२५	ऑनलाइन खरेदी घोटाळे	४९
२६	सार्वजनिक वायफाय वापरुन घोटाळे	५१
२७	बनावट जाहिरात / ऑफर	५३
२८	बनावट कर्ज संधी/ ऑफर	५५
२९	क्रेडिट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

१. फिशिंग लिंक च्या माध्यमातून फसवणूक

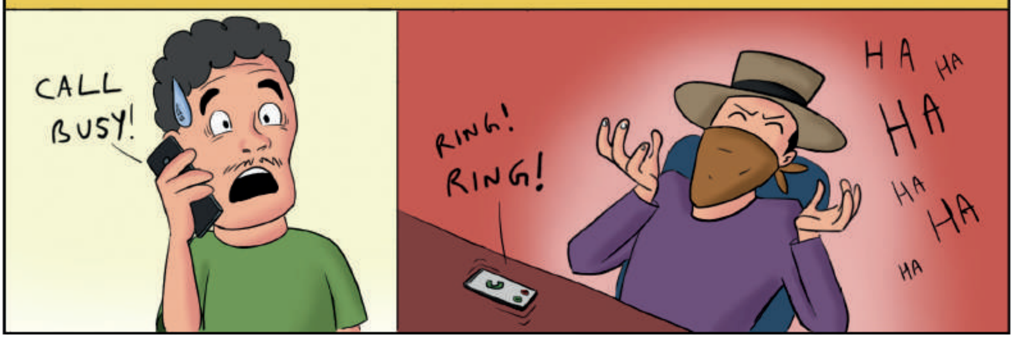
हे करा :

- ✔ तुम्हाला केवायसी तपशील देण्याबद्दल अनोळखी व्यक्ती कडून फोन, लिंक किंवा एसएमएस आला तर तुमचे खाते असलेल्या शाखेत किंवा तुमच्या रिलेशनशिप / संबंध व्यवस्थापकाशी संपर्क साधून तुमच्या केवायसी स्थितीची फेर पडताळणी करून घ्या.
- ✔ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस ठाण्यात आणि राष्ट्रीय सायबर गुन्हे रिपोर्टिंग 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 खात्री केल्याशिवाय उघडू नका.

✗ अनोळखी लोकांना तुमचे गोपनीय तपशील देऊ नका.

२. विशिंग कॉल्स

हे करा :

- ✔ कोणावरही विश्वास ठेवण्यापूर्वी नेहमी तुमच्या रिलेशनशिप / संबंध व्यवस्थापकाशी किंवा बँकेच्या शाखेशी बोलून खात्री 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 विश्वात कोणाही अनोळखी व्यक्ती वर सहज विश्वास टाकू नका आणि अनोळखी क्रमांकावरुन आलेल्या फोनला उत्तर देताना सावध रहा.

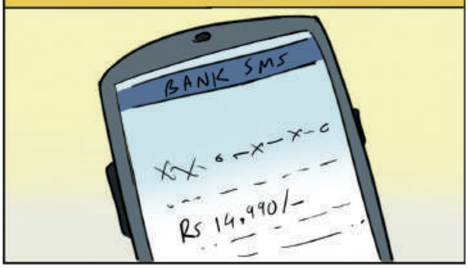
३. ऑनलाइन बाजारपेठेचा वापर करुन केलेली फसवणूक

हे करा :

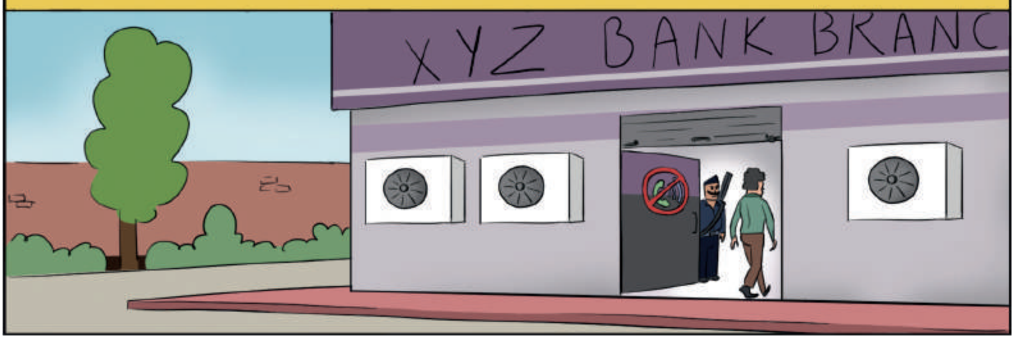
- ✔ नेहमी लक्षात ठेवा, UPI पिन हा फक्त पैसे देण्यासाठी (पेमेंट करण्यासाठी) आवश्यक आहे आणि पैसे मिळविण्यासाठी नाही.
- ✔ नेहमी पैसे देण्यास सुरुवात करण्यापूर्वी UPI ॲप्लिकेशन मधील मोबाइल क्रमांकाची खात्री करून घ्या.
- ✔ घडलेली घटना जवळच्या सायबर क्राइम पोलीस ठाण्यात आणि राष्ट्रीय सायबर क्राइम रिपोर्टिंग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

(नंतर घोटाळेबाज राजूला पैसे पाठवण्या ऐवजी रु.14,990/- मिळण्यासाठी UPI विनंती पाठवतो.)

राजू लगेच पिन टाकतो आणि त्याच्या खात्यातून रु.14,990/- वजा होतात.



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



हे करू नका :

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

४. क्रेडिट कार्डचे वार्षिक शुल्क माफ करणे - खोटी ऑफर

हे करा :

- ✔ अनोळखी क्रमांकावरून बोलत असलेली व्यक्ती तुमच्या बँकेतून बोलत आहे असे सांगत असेल तरी अशा व्यक्तीशी बोलताना सावध रहा.
- ✔ फसवले गेलो आहोत, असे लक्षात आल्याबरोबर लगेच तुमच्या बँक शाखेत कळवा.
- ✔ अधिक आर्थिक हानीपासून बचाव होण्यासाठी तुमचे कार्ड ताबडतोब ब्लॉक करा .
- ✔ घडलेली घटना जवळच्या सायबर क्राइम पोलीस ठाण्यात आणि राष्ट्रीय सायबर क्राइम रिपोर्टिंग पोर्टल https://cybercrime.gov.in वर नोंदवा.

हे करू नका :

× तुमचा ओटीपी कोणालाही सांगू नका. घोटाळेबाज तुमच्या खात्याचे तपशील गोळा करु शकेल कदाचित, पण प्रत्यक्ष व्यवहार तेव्हाच पूर्ण होईल जेव्हा तुम्ही तुमच्या फोन वर आलेला गोपनीय ओटीपी द्याल.

५. एटीएम कार्ड स्कीमिंग फसवणूक

हे करा :

- ✔ एटीएम व्यवहार सुरु 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.

हे करू नका :

✕ एटीएमच्या परिसरात कोणालाही तुमच्या वतीने व्यवहार करण्यासाठी तुमचे एटीएम कार्ड देऊ नका.
अश्या 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 वापरुन केलेली फसवणूक

हे करा :

- ✔ ज्यांची ऑफर आली आहे त्यांची अधिकृतता / खरेपणा, संबंधित व्यवसायाच्या नोंदणीकृत वेबसाइट वर खात्री करून घ्या.
- ✔ तुमच्या मोबाइल फोन वर अँटी वायरस / स्पॅम ब्लॉकिंग सॉफ्टवेअर घालून 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 ॲप द्वारे पाठवलेल्या लिंक ने कोणतेही ॲप्लिकेशन डाउनलोड करू नका.

× अनोळखी व्यक्तीने पाठवलेले स्क्रीन शेअरिंग ॲप्लिकेशन डाउनलोड करू नका. अशा ॲप 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 पुरवठादारशी 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.)

(चोराने नवीन सिम कार्ड घेतले आणि बँकिंग ॲप्लिकेशन चे “forgot username“, “reset password“ इत्यादी विकल्प वापरुन यूजर नाव शोधून काढले आणि खात्यातील सर्व पैसे स्वत:च्या खात्यात वळवले.)

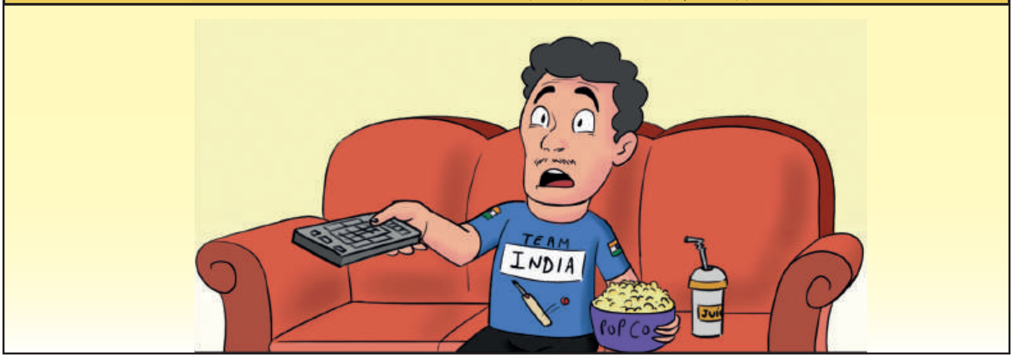
काही मिनिटातच, राजूला त्याच्या बँक खात्यातून पैसे वजा झाल्याचे ई-मेल आले. त्यांनी आपल्या बँक खात्यातील शिल्लक तपासली तेव्हा त्याच्या लक्षात आले की त्याच्या खात्यातून काही अनधिकृत डेबिट व्यवहार झाले आहेत, ज्यांचा त्याच्या नोंदणीकृत मोबाइल वर मेसेज आला नाही कारण ते सिम कार्ड पैसे अंतरित करणे, ऑनलाइन खरेदी करणे इत्यादी साठी निरुपयोगी ठरले होते.

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 ॲप उघडताच त्याचे सभासदत्व संपल्याचे त्याला लक्षात आले.



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

हे करा :

- ✔ नेहमी, फक्त सेवा पुरवठादाराच्या अधिकृत वेबसाइट वरुन संपर्कासाठी तपशील / ग्राहक सेवा क्रमांक इत्यादी घ्या.
- ✔ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (https://cybercrime.gov.in) वर नोंदवा.

हे करु नका :

× वेब सर्च इंजिन वरुन अचानक आलेल्या फोन क्रमांकावर, विशेषतः आर्थिक व्यवहार करत असताना, संपर्क करु नका.

९. क्यूआर कोड स्कॅनिंग द्वारे घोटाळा

राजूने त्याची जुनी गाडी विकण्यासाठी ऑनलाइन वेबसाइटवर नोंदणी केली.

काही तासातच त्यांच्याशी एका व्यक्तीने (घोटाळेबाज) संपर्क केला.

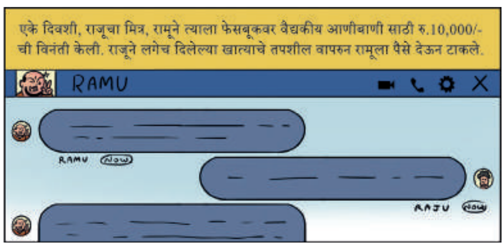
हे करा :

- ✓ 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.

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 करुन घ्या.
- ✔ पैसे पाठवण्या आधी नेहमी खात्याची माहिती तपासून पहा.
- ✔ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (https://cybercrime.gov.in) वर नोंदवा.

हे करु नका :

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

११. ज्यूस जॅकींग – चार्जिंग वायर द्वारे डेटा चोरणे

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.

हे करु नका :

× अनोळखी माणसांच्या चार्जिंग adapter / वायर वापरु नका.

१२. लॉटरी घोटाळा

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 वरुन नेहमी खात्री करून घ्या.
- ✔ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (https://cybercrime.gov.in) वर नोंदवा.

हे करू नका :

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

१३. ऑनलाइन नोकरी घोटाळा

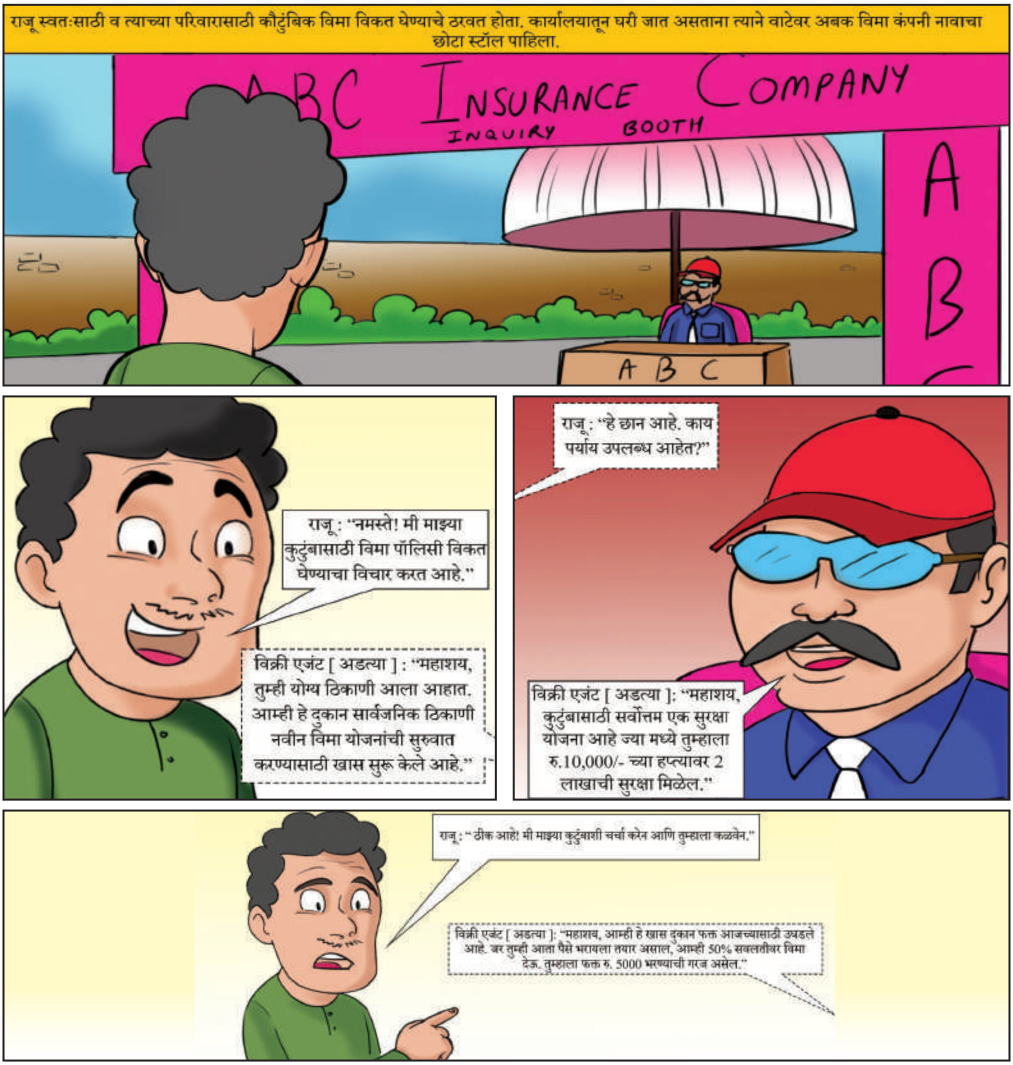
हे करा :

- ✔ कुठले ही पैसे भरण्या अगोदर, कंपनी किंवा भरती प्रतिनिधींच्या 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.

हे करु नका :

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

१४. बनावट खाते क्रमांक



हे करा :

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

हे करु नका :

✕ कंपनीच्या अस्सलपणाची खात्री झाल्या शिवाय कोणालाही कोणतीही रक्कम प्रदान करू नका.

१५. ई-मेल द्वारे घोटाळा

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 करु नका :

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

१६. संदेश ॲप बँकिंग घोटाळा

हे करा :

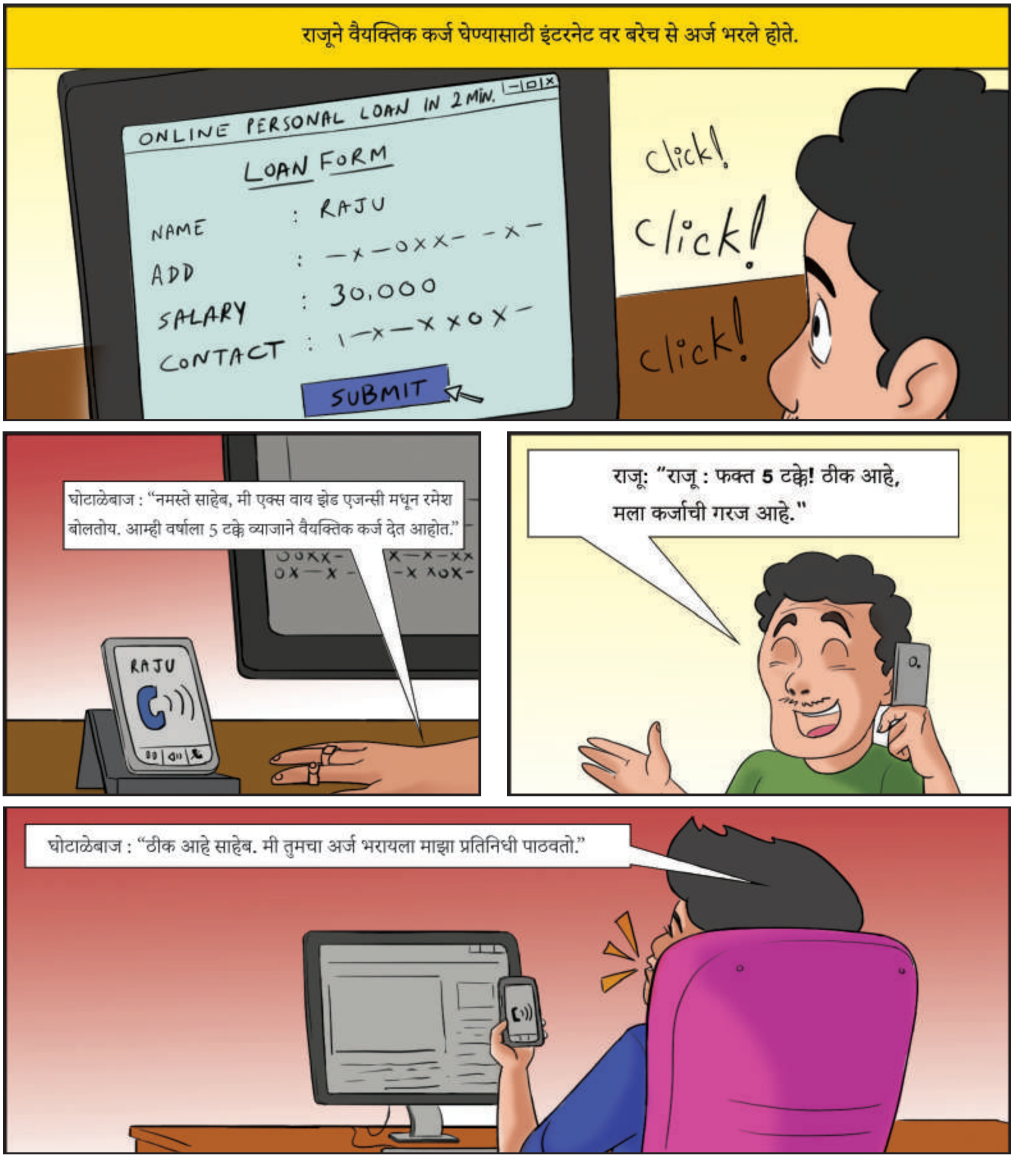
- ✔ अनोळखी क्रमांकावरून खात्याचे तपशील मिळवण्यासाठी फोन आल्यावर उत्तर देताना सावध रहा.
- ✔ घोटाळ्याची जाणीव होताच लगेच तुमच्या बँक शाखेत तक्रार करा. पुढे अधिक आर्थिक तोटा टाळण्यासाठी तुमचे खाते ब्लॉक करा.
- ✔ घडलेली घटना जवळच्या सायबर गुन्हे पोलीस चौकी आणि राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (https://cybercrime.gov.in)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

हे करु नका :

✗ सोप्या बँकिंग सेवा देऊ करणाऱ्या आणि संदेशवाहक ॲप द्वारे संदेश पाठवणाऱ्या अनोळखी फोन करणाऱ्यावर विश्वास ठेवू नका.

✗ आपल्या कार्डाचे तपशील आणि ओटीपी कोणालाही देऊ नका.

१७. चोरलेली कागदपत्रे वापरुन फसवे कर्ज घेणे



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.

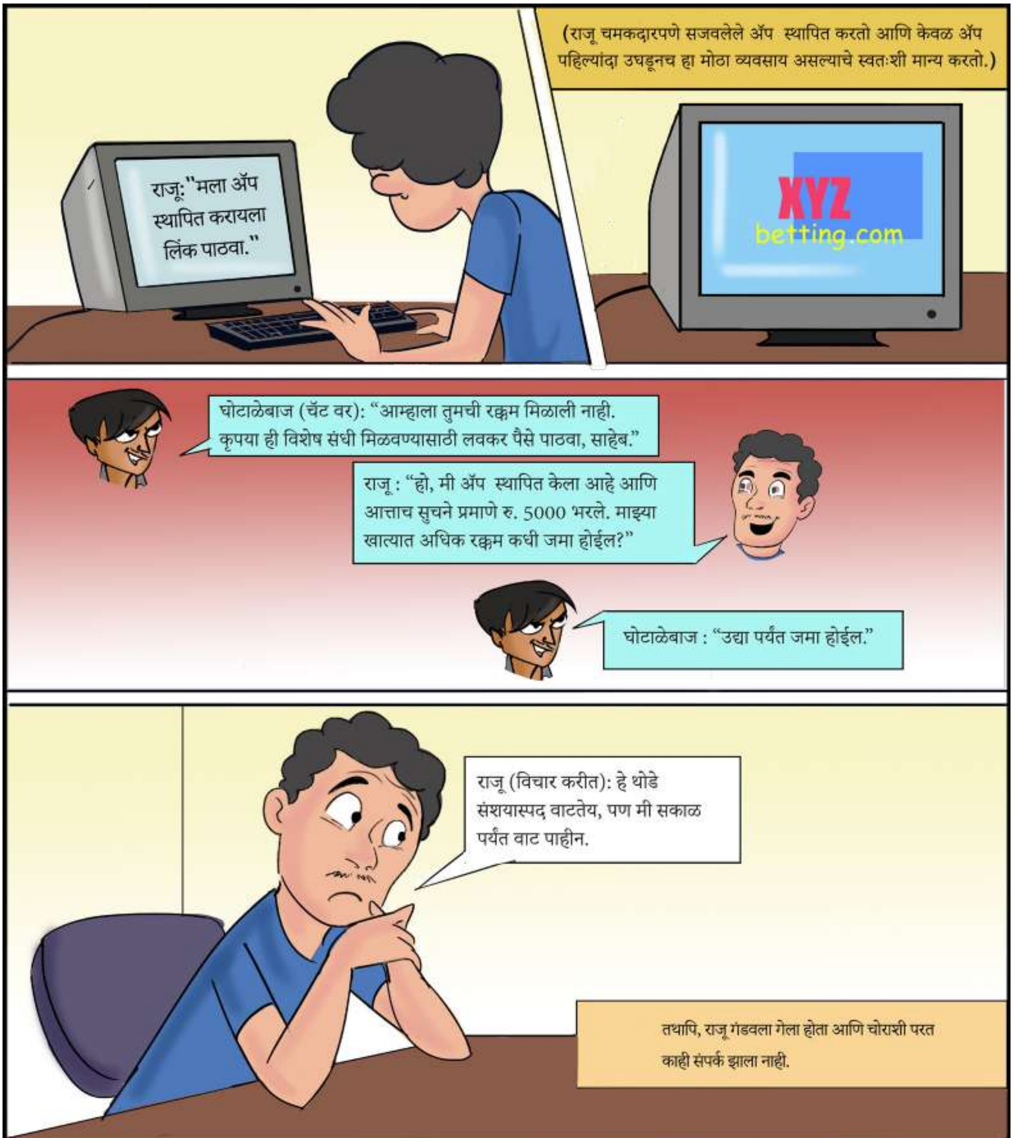
हे करु नका :

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

१८. सट्टेबाजीचे घोटाळे

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.



हे करु नका :

✕ अनोळखी वेबसाइट वर पैसे अंतरित करू नका.

१९. फसवे लसीकरणाचे कॉल

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.

हे करु 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

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.

हे करु 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

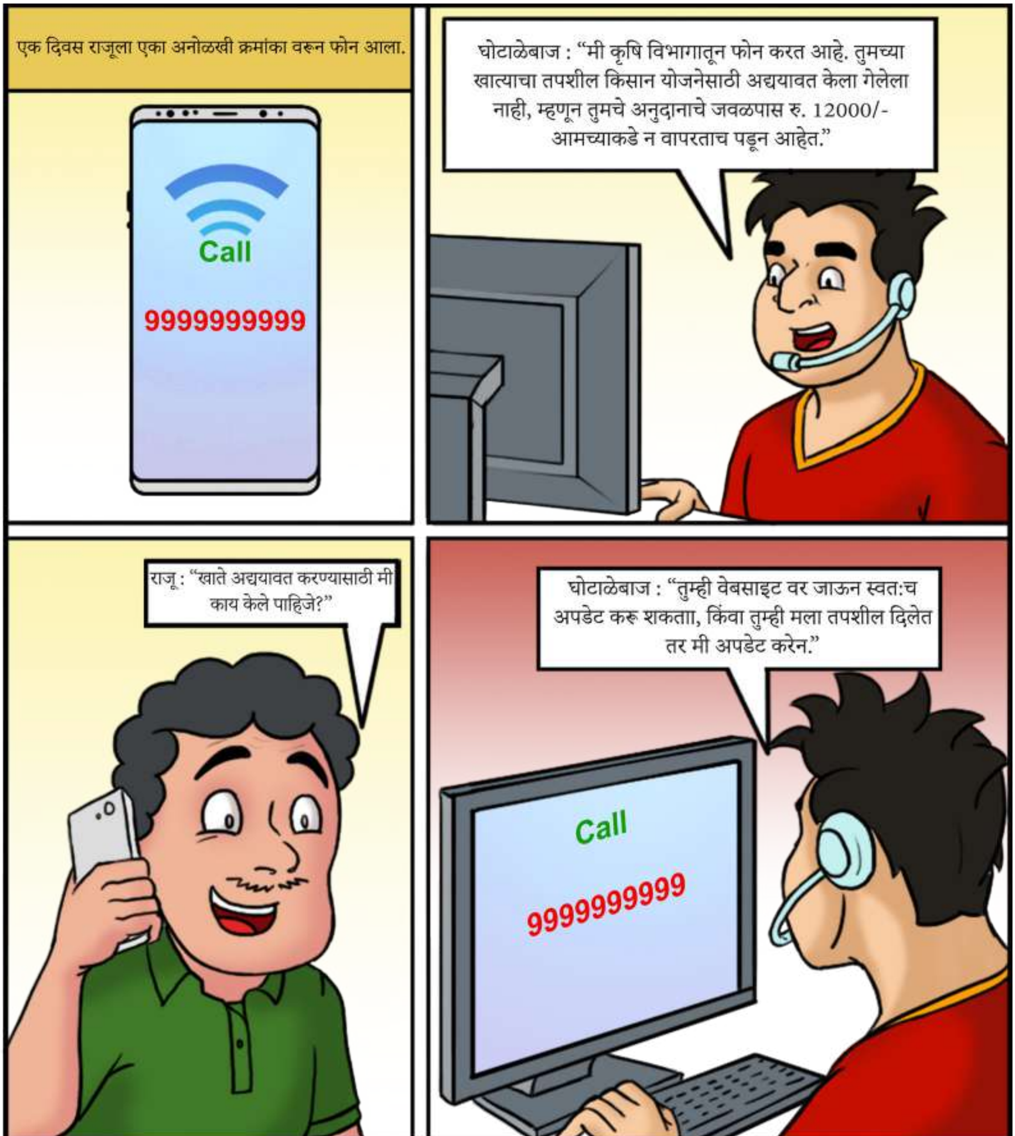
हे करा :

✔ कुठले ही 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 गृह शाखेत फोन करून फेर तपासणी ही करू शकता.

हे करु नका :

✕ कधीही योग्य पावती मिळाल्याशिवाय बँक / वसूली प्रतिनिधीला कुठलीही रोख रक्कम देऊ नका.

२२. सामाजिक हित योजना घोटाळा



हे करा :

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

हे करु नका :

- ✕ असे फोन वरुन अनुदान मिळण्याच्या कथेवर कधीच विश्वास ठेऊ नका.
- ✕ पात्र 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. बहू स्तरीय विपणन (mlm) घोटाळे

हे करा :

- ✔ तुम्हाला अश्या योजनेत खेचणाऱ्या लोकांपासून दुर रहा.
- ✔ बहु स्तरीय विपणन योजनेच्या खरेपणाची खात्री करून घ्या. काही नेटवर्क विपणन योजना जसे पॉन्झि योजना, पिरॅमिड योजना इत्यादी; डायरेक्ट सेलिंग मार्गदर्शक तत्वे, 2016 आणि प्राइज चिटस् 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.

हे करु नका :

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

२४. घर बसल्या नोकरीचे घोटाळे

हे करा :

- ✔ अनोळखी स्रोतां कडून गूगल फॉर्म्स वर तपशील मागणाऱ्या लहान url पासून सावध रहा.
- ✔ ई-मेल, एसएमएस आणि पोर्टलस वर चुकीचे शब्दलेखन, व्याकरण यासाठी लक्ष ठेवा.
- ✔ व्यक्तीगत तपशील विचारणाऱ्या लिंक/फॉर्म्स पासून सावध रहा.
- ✔ संधी किंवा व्यवसायाच्या खरेपणाची खात्री 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.

हे करु नका :

- ✕ कधीही अनोळखी लोकांना ई-मेल द्वारे संवेदनशील, वैयक्तिक किंवा मालकी तपशील (आधार किंवा पॅन कार्ड) पाठवू नका.
- ✕ कधीही वकिलाचा सल्ला घेतल्या शिवाय कुठल्या ही ऑनलाइन करारावर सही करु नका.
- ✕ कधीही नोकरी मिळवण्यासाठी पैसे देऊ नका; अस्सल कंपन्या कधीही पैसे भरण्यास सांगत नाहीत.

२५. ऑनलाइन खरेदी घोटाळे

हे करा :

- ✓ नेहमी सुरक्षित वेबसाइट वरून खरेदी करा. आम्ही असे सुचवू इच्छितो की ब्राऊजरच्या ॲड्रेस 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.

हे करु नका :

✕ कधीही अनोळखी वेबसाइट वरुन खरेदी करु नका.

✕ कधीही फक्त गिफ्ट कार्ड, पैसे अंतरण इत्यादी माध्यमातून पेमेंट स्वीकारणाऱ्या ऑनलाइन विक्रेत्यांकडून काहीही विकत घेऊ नका. कारण अशा पेमेन्टचा शोध लावणे आणि परत मिळवणे जवळजवळ अशक्य आहे.

✕ कधीही अनोळखी साइटला आगाऊ पेमेंट करु नका, कारण पैसे भरल्या नंतर उत्पादन मिळण्याची शक्यता धूसर असते.

२६. सार्वजनिक वायफाय वापरुन घोटाळे

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.

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.

हे करु नका :

✕ सार्वजनिक वायफाय वापरु नका, खास करुन आर्थिक व्यवहार करताना. सुरक्षा नसलेल्या सार्वजनिक वायफायला जोडलेले लॅपटॉप किंवा मोबाइल उपकरण हॅक करणे सोपे असते. हॅकर तुमचे ई-मेल वाचू शकतात, पासवर्ड आणि अन्य अधिकारपत्रे चोरु शकतात.

२७. बनावट जाहिरात / ऑफर

हे करा :

- ✓ ब्रँडेड उत्पादना संबंधित असेल तर त्यांच्या अधिकृत वेबसाइट वर जाहिरातींची खात्री 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.

राजूने खरंच पैसे गमावले.

हे करु नका :

- ✕ जाहिरातीतल्या मोठ्या दाव्यांनी स्वत:ची 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

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.

हे करु नका :

✕ तुमचे कर्ज मंजूर करण्यासाठी कधीही आधीच पैसे भरु नका. बँका आणि वित्तीय संस्था कधीही कर्ज मंजूरी साठी आधीच शुल्क मागत नाहीत. शुल्क, असले तर, तुमच्या कर्ज रकमेतून वजा केले जाते आणि उरलेली रक्कम तुमच्या खात्यात अंतरित केली जाते.

२९. क्रेडिट कार्ड सक्रियीकरण घोटाळे

हे करा :

- ✔ पुढचे आर्थिक नुकसान टाळण्यासाठी तुमच्या बँकेला कार्ड/ बँक खाते/ UPI सेवा ब्लॉक करण्याकरिता फोन करा.
- ✔ घटनेची नोंद करण्या साठी 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.

हे करु 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

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.

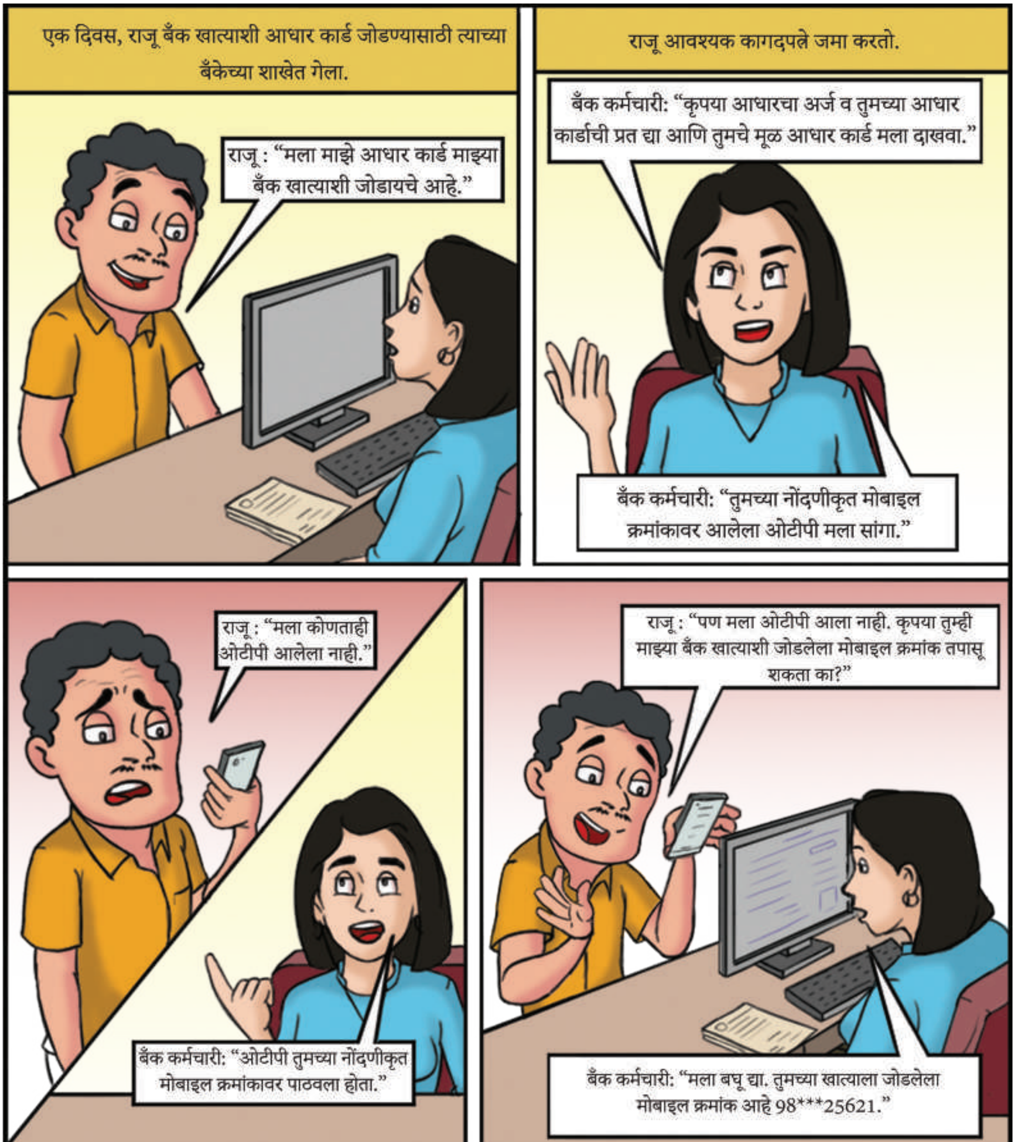
काही वेळानंतर, राजूला त्याच्या बँके कडून क्रेडिट कार्ड मधून रु. 70,000/- वजा झाल्याचा एसएमएस आला.

हे करु नका :

✕ क्रेडिट कार्ड सक्रिय करण्या साठी / त्यांची मर्यादा वाढविण्यासाठी अनोळखी फोन करणाऱ्यांवर विश्वास ठेऊ नका.

✕ तुमच्या क्रेडिट कार्डाची माहिती/ ओटीपी कोणालाही देऊ नका.

३१. तुमच्या आधार कार्डाचे संरक्षण करणे



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.

हे करु नका :

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

३२. कॅश बॅक ऑफर वापरुन ऑनलाइन घोटाळे

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

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.

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

हे करु नका :

✕ फोन करणाऱ्यावर आंधळेपणाने विश्वास ठेऊ नका; ऑफरची सत्यता पारखण्यासाठी कंपनीची अधिकृत वेबसाइट पाहून खात्री केली पाहिजे.

✕ पैसे मिळवण्यासाठी UPI पिन लिहू किंवा सांगू नका कारण ते फक्त पैसे पाठवण्या करता लागते.

३३. सवलत घोटाळे

हे करा :

- ✔ कुठले ही करार किंवा ऑफर देणाऱ्या व्यक्ती/ संस्थेच्या सत्यतेची नेहमी खात्री 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.

हे करु नका :

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

३४. देणगी घोटाळे

हे करा :

- ✔ नेहमी संस्था खरी आहे की नाही हे बघण्यासाठी सरकारी वेबसाइट डेटाबेस वर धर्मादाय संस्था अस्तित्वात असल्याची खात्री करून घ्या..
- ✔ नेहमी जागरुक रहा कारण खोटी वेबसाइट अगदी अस्सल 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 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 करु नका :

✕ फक्त गूगल शोधाच्या आधारावर कोणत्याही क्रमांकावर खात्री केल्याशिवाय फोन करू नका.

✕ कराराच्या खरेपणाची/अधिकृततेची खात्री केल्याशिवाय थेट पैसे पाठवू नका.

३५. फिक्स्ड डिपॉजिटवर ओव्हरड्राफ्ट

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.

हे करु 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.

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 लॅपटॉपवरुन 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 खात्री 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.

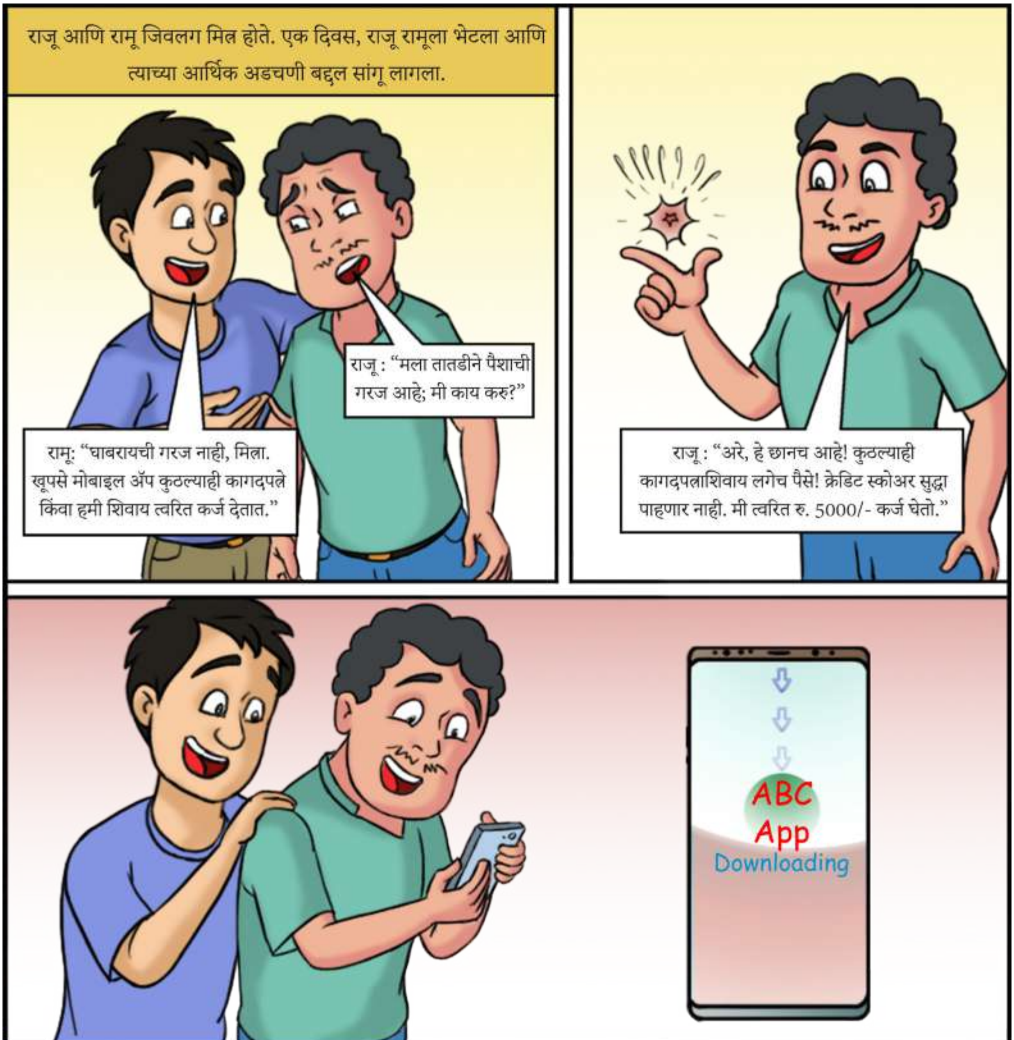
काही दिवसा नंतर, राजूला एसएमएस आला की रु. 50,000/- त्याच्या खात्यातून वजा झाले आहेत.
राजूला त्याचे खाते कसे धोक्यात आले किंवा पैसे कसे वजा झाले ह्याचा काहीच सुगावा लागला नाही.

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

हे करु नका :

✕ एसएमएस, ई-मेल किंवा झटपट संदेश ॲप च्या माध्यमातून,विशेषत: अनोळखी व्यक्ती कडून,पाठवलेल्या लिंकवरुन, खरेपणाची खात्री केल्याशिवाय ॲप्लिकेशन डाउनलोड करू नका.

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



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.

हे करु नका :

✕ कोणतेही मोबाइल ॲप 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

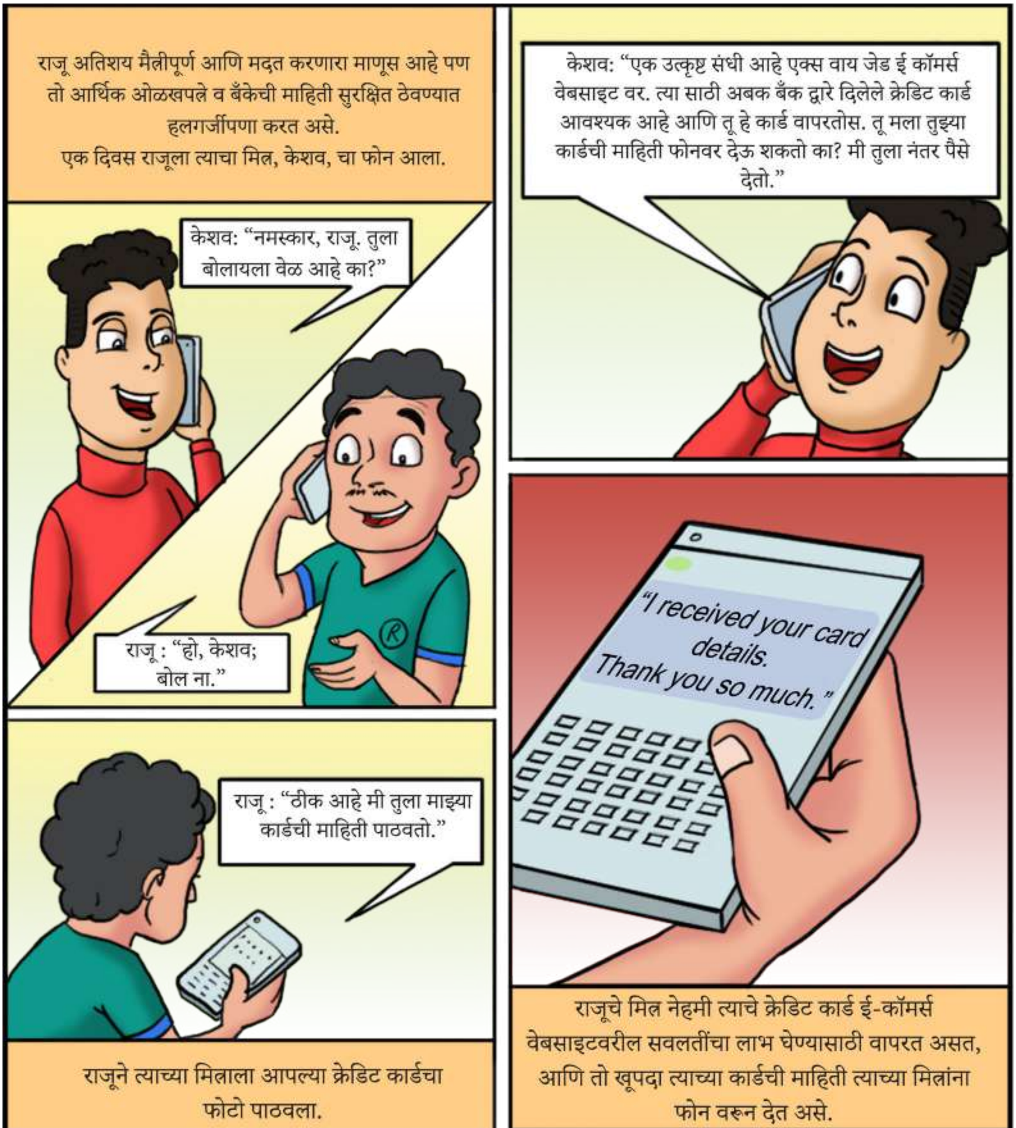
हे करा :

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

हे करु 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



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.

हे करु नका :

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

४०. पैसे पाठवण्याचे (पेमेंट स्पूफिंग) फसवे ॲप

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.

हे करु नका :

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

भारतीय रिज़र्व बैंक

RESERVE BANK OF INDIA

भारतीय रिज़र्व बैंक

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