सावध रहा, जागरूक व्हा !

BE(A)WARE

आर्थिक गुन्हेगारांच्या कार्यपद्धतींवर पुस्तिका

A BOOKLET ON MODUS OPERANDI OF FINANCIAL FRAUDSTERS

OFFICE OF THE RBI OMBUDSMAN (MUMBAI-II)
MAHARASHTRA AND GOA

भारतीय रिज़र्व बैंक

RESERVE BANK OF INDIA

अनुक्रमणिका

	विषय	पृष्ठ क्र.
	प्रस्तावना	१
	भाग - ए – फसवणुकीच्या कार्यपद्धती - बँक	२
१	फिशिंग लिंक्स (नकली लिंकद्वारे फसवणूक)	३
२	विशिंग कॉल्स (फोनद्वारे माहिती चोरून फसवणूक)	४
३	ऑनलाइन विक्री संकेतस्थळांवरील फसवणूक	५
४	अनोळखी तसेच सत्यापित (व्हेरीफाय) न केलेल्या मोबाइल ॲपद्वारे फसवणूक	६
५	एटीएम कार्ड स्किमिंग	७
६	स्क्रीन शेअरींग ॲप किंवा रिमोट ॲक्सेस द्वारे फसवणूक	८
७	सिम कार्ड स्वॅप / सिम क्लोनिंग	९
८	इंटरनेटवरील सर्च इंजिनमध्ये दिसणाऱ्या माहितीशी छेडछाड करून फसवणूक	१०
९	क्यूआर कोड स्कॅनिंगद्वारे फसवणूक	११
१०	समाज माध्यमांवर बनावट खाते उघडून फसवणूक	१२
११	ज्यूस जॅकिंग (चार्जिंग पोर्टच्या माध्यमातून माहितीची चोरी)	१३
१२	लॉटरीचे आमिष दाखवून फसवणूक	१४
१३	नोकरीचे आश्वासन देऊन केलेली ऑनलाइन फसवणूक	१५
	भाग - बी – फसवणुकीच्या कार्यपद्धती – बिगर बँकिंग वित्तीय संस्था	१६
१	फसवणूक करणाऱ्याकडून कर्ज वितरणासाठी केलेल्या बनावट जाहिराती	१७
२	एसएमएस/ ई-मेल/ फोन द्वारे फसवणूक	१८
३	ओटीपीचा वापर करून फसवणूक	१९
४	कर्ज वितरणासाठी बनावट वेबसाईट/ ॲप	२०
५	मनी सर्क्युलेशन / पॉन्झी / मल्टी लेवल मार्केटिंग स्कीमच्या माध्यमातून फसवणूक	२१
६	बनावट कागदपत्रांच्या आधारे दिलेले / घेतलेले कर्ज	२२
	भाग – सी - आर्थिक व्यवहार करताना घ्यावयाची सर्वसामान्य खबरदारी	२३
	शब्दसूची	३०

प्रस्तावना

गेल्या काही वर्षांत, डिजीटल माध्यमांचा वापर करून पैसे देवाण घेवाण करण्याचे प्रमाण वाढले आहे. यामुळे ग्राहकांच्या सोयीसुविधेत तर भर पडली आहेच, शिवाय आर्थिक समावेशनाचे राष्ट्रीय उद्दीष्ट गाठण्यातही मोठा हातभार लागला आहे. परंतु आर्थिक व्यवहारांत सुलभता येण्याबरोबरच यामार्फत होणाऱ्या फसवणुकीच्या घटनांमध्ये देखील वाढ होत आहे. सर्वसामान्य, भोळया-भाबड्या नागरिकांनी मोठ्या स्वकष्टाने कमावलेले पैसे लुबाडण्यासाठी आर्थिक गुन्हेगारांकडून नवनवीन मार्गांचा अवलंब केला जात आहे. या गुन्हेगारांकडून मुख्यत: सध्याच्या तंत्रज्ञानाभिमुख आर्थिक व्यवहारांच्या जगाशी नव्यानेच ओळख होत असलेल्या व्यक्तींना लक्ष्य केले जाते.

अशा या आर्थिक व्यवहारांसाठी नव्यानेच डिजिटल माध्यमे वापरणाऱ्या नवख्या ग्राहकांना केंद्रस्थानी ठेऊन या पुस्तिकेची रचना करण्यात आली असून यासंदर्भात जास्तीत जास्त व्यावहारिक पद्धतीने मार्गदर्शन करण्याचा प्रयत्न याद्वारे करण्यात आला आहे. विविध ठिकाणांहून एकत्रित केलेल्या घटनांचा संग्रह एवढेच या पुस्तिकेचे स्वरूप मर्यादित न ठेवता, बँकिंग लोकपालाकडे आलेल्या विविध तक्रारींचे बारकाईने तपशीलवार संकलन करून विचारपूर्वक या पुस्तिकेची रचना करण्यात आली आहे. आर्थिक गुन्हेगारांच्या विविध कार्यपध्दतींबद्दल जनजागृती करून सोबत आर्थिक व्यवहार करताना घ्यावयाच्या खबरदारी संदर्भातही मार्गदर्शन केले आहे. वैयक्तिक माहितीची सुरक्षितता, अनोळखी व्यक्तींकडून आलेले फोन / ई-मेल, आर्थिक व्यवहार करताना घ्यावयाची दक्षता, वेळोवेळी पासवर्ड बदलाचे महत्त्व या व अशा अनेक गोष्टींवर भर देत यासंदर्भात विस्तृत विवेचन करून याच अनुषंगाने पुस्तिकेला यथोचित असे “जागरूक व सावध रहा!” हे शीर्षक दिले आहे.

या कार्यालयाच्या जनजागृती उपक्रमाअंतर्गत ही पुस्तिका प्रकाशित करण्यात येत आहे.

फसवणुकीच्या कार्यपद्धती आणि त्यासंदर्भात घ्यावयाची खबरदारी – बँक

१. फिशिंग लिंक्स (नकली लिंकद्वारे फसवणूक)

कार्यपद्धती

- यात फसवणूककर्त्यांकडून नकली संकेतस्थळांची निर्मिती केली जाते जी अगदी हुबेहूब खऱ्याखुऱ्या बँक संकेतस्थळ (वेबसाइट) किंवा ई-कॉमर्स, सर्च इंजिन सारखी दिसून येतात.
- साधारणत: एसएमएस, ई-मेल व समाजमाध्यमांद्वारे अशा नकली संकेतस्थळांच्या लिंक्स फसवणूककर्त्यांकडून पसरवल्या जातात
- बहुतेक वेळा, अशा लिंक्सवर क्लिक करून संकेतस्थळाची संपूर्ण शहानिशा न करताच ग्राहक आपली वैयक्तिक गोपनीय माहिती त्यावर नोंदवतात.
- प्रथमदर्शनी अधिकृत भासणाऱ्या या नकली संकेतस्थळांच्या माध्यमातून प्रत्यक्षात मात्र फसवणूककर्ते ग्राहकांना आपल्या जाळ्यात ओढत असतात.
- ग्राहक जेव्हा आपली गोपनीय वैयक्तिक माहिती त्यावर नोंदवतात, ती माहिती या फसवणूककर्त्यांना सहज उपलब्ध होते आणि त्याचाच वापर करून मग ग्राहकांना लुबाडले जाते.

खबरदारी

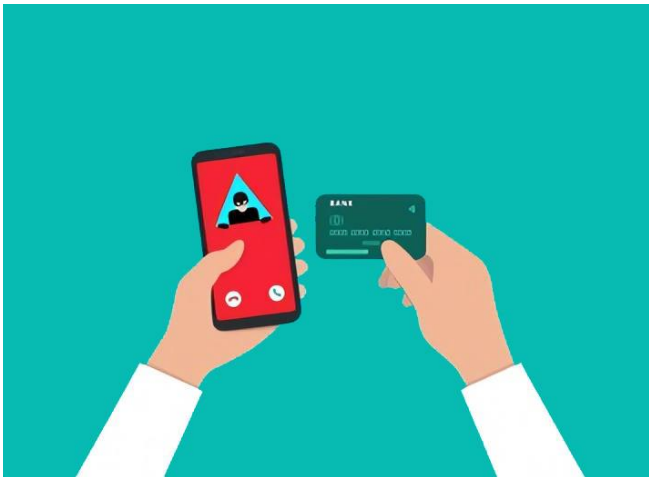
अनोळखी लिंक्स वर कधीच क्लिक करू नये. अशा लिंक्स असलेले ई-मेल्स आणि एसएमएस ताबडतोब डिलीट करावेत जेणेकरून भविष्यात देखील अजाणतेपणाने त्याचा वापर होणार नाही

कोणतेही संकेतस्थळ वापरताना त्याची योग्य ती शहानिशा करण्यात यावी. विशेषत: जेथे आर्थिक व्यवहारांसाठीची गोपनीय वैयक्तिक माहिती नोंदविणे आवश्यक आहे, अशा ठिकाणी विशेष खबरदारी घेणे आवश्यक आहे.

२. विशिंग कॉल्स (फोनद्वारे माहिती चोरून फसवणूक)

कार्यपद्धती

- फसवणूककर्त्यांकडून ग्राहकांना बँकेतून फोन करत असल्याची बतावणी करत किंवा याचप्रकारे इंशुरन्स एजंट, कंपनी एक्जिक्यूटीव, सरकारी अधिकारी इत्यादी असल्याचे भासवत संपर्क केला जातो. ग्राहकाचे नाव, जन्मतारीख अशी जुजबी माहिती सांगून ग्राहकांचा विश्वास संपादन केला जातो आणि मग विविध क्लृप्त्या वापरून महत्त्वाची गोपनीय माहिती विचारली जाते.



- यात हे फोन करणारे फसवणूककर्ते विविध प्रकारे ग्राहकांवर दबाव आणून त्यांना घाईगडबडीत माहिती सांगण्यास उद्युक्त करतात. यासाठी तुमचे व्यवहार ब्लॉक होतील, पेनल्टी लागेल अशी विविध कारणे सांगून घाबरवले जाते किंवा काही वेळा सवलतींचे प्रलोभन दाखवले जाते. याप्रकारे ग्राहकांकडून गोपनीय माहिती मिळवून त्याद्वारे फसवणूक केली जाते.

खबरदारी

बँक कर्मचारी किंवा कोणतीही वित्तीय संस्था या कधीच ग्राहकांना यूजरनेम, पासवर्ड, कार्ड डीटेल्स, सीव्हीव्ही, ओटीपी अशी गोपनीय माहिती विचारत नाहीत, हे लक्षात ठेवावे.

३. ऑनलाइन विक्री संकेतस्थळांवरील फसवणूक

कार्यपद्धती

- ऑन लाईन खरेदी-विक्री संकेतस्थळांवर फसवणूककर्ते स्वतःला खरेदीदार असल्याचे भासवतात आणि तुम्ही विक्रीसाठी नोंदविलेली गोष्ट विकत घेण्यात स्वारस्य असल्याचे दाखवितात.
- नंतर तुम्हाला पैसे पाठविण्याऐवजी, ते “यूपीआय” द्वारे “रिक्वेस्ट मनी” च्या पर्यायाचा वापर करून उलट तुमच्याच खात्यातील पैसै त्यांच्याकडे ओढून घेण्याच्या प्रयत्नात असतात. यासाठी रिक्वेस्ट मनी हा पर्याय निवडून तुमच्या मोबाइल अ‍ॅपमधून ती मान्य (अप्रूव्ह) करण्याची गळ घातली जाते आणि परिणामत: पैसे मिळण्याऐवजी उलट ते तुमच्या खात्यातून वजा होतात.

खबरदारी

- लक्षात ठेवा - ऑनलाईन खरेदी विक्री व्यवहार करताना काळजी घेतली पाहिजे.
- सर्वात महत्वाचे म्हणजे आपल्याला दुस-या कोणाकडून पैसे स्वीकारण्यासाठी कधीच “पासवर्ड” किंवा “पिन” टाकण्याची आवश्यकता नसते हे लक्षात ठेवावे.
- आर्थिक व्यवहार पूर्ण करण्यासाठी जर कधी " यूपीआय" किंवा अन्य कोणत्याही अ‍ॅपमध्ये " पिन" प्रविष्ट करण्याची वेळ आली तर तुम्हाला पैसे मिळण्या ऐवजी तुमचेच पैसे वजा होतील.

४. अनोळखी तसेच सत्यापित (व्हेरीफाय) न केलेल्या मोबाइल ॲपद्वारे फसवणूक

कार्यपद्धती

- जेव्हा आपण एखादे अनोळखी किंवा व्हेरीफाय न केलेले मोबाईल ॲप डाऊनलोड करतो, तेव्हा फसवणूककर्ते सहज आपल्या मोबाईल / लॅपटॉप किंवा डेस्कटॉप पर्यंत पोहोचू शकतात व त्याचा ताबा मिळवू शकतात.
- साधारणपणे एसएमएस / इन्स्टंट मेसेंजर तसेच समाजमाध्यमांद्वारे या ॲप्लिकेशन्सच्या लिंक पसरवल्या जातात. वरवर पाहता या लिंक्स एखाद्या विश्वसनीय नावासारख्या भासवल्या जातात परंतु प्रत्यक्षात मात्र त्यावर क्लिक करताच त्याद्वारे अनोळखी ॲप्लिकेशन्स डाऊनलोड होऊ होतात.
- एकदा का हे फसवे ॲप्लिकेशन डाऊनलोड झाले की, फसवणूककर्ते आपल्या डिव्हाइसचा संपूर्ण ताबा मिळवितात.

खबरदारी

अनोळखी किंवा विश्वासार्ह नसलेल्या ठिकाणांहून ॲप्लिकेशन्स डाउनलोड करू नयेत.

५. एटीएम कार्ड स्किमिंग

कार्यपद्धती

- या प्रकारात आर्थिक गुन्हेगारांकडून ग्राहकांच्या एटीएम कार्डला लक्ष्य केले जाते. यासाठी एटीएम मशीनमध्येच स्किमिंग म्हणजेच कार्डमधील माहितीची चोरी करणारे उपकरण फसवणूककर्त्यांकडून लपविले जाते. याचा वापर करून नंतर डुप्लिकेट एटीएम कार्ड तयार केले जाते.
- तसेच डमी की-पॅड, सूक्ष्म पिन होल कॅमेरा अशा साधनांचा वापर करून ग्राहकांचा पिन क्रमांक देखील जाणून घेण्याचा प्रयत्न केला जातो. साधारणपणे कोणाला दिसून येणार नाही अशाप्रकारे ही उपकरणे लपविलेली असतात.
- पिन चोरीसाठी बऱ्याचदा हे फसवणूककर्ते तुमच्या बाजूला उभे राहून लपूनछपून तुम्ही पिन प्रविष्ट करीत असताना पाहत असतात.
- अशाप्रकारे डुप्लिकेट एटीएम कार्ड आणि पिनच्या सहाय्याने तुमच्या खात्यातील रक्कम नंतर काढून घेतली जाते.

खबरदारी

- मशीन मधे कार्ड टाकण्याच्या जागे जवळ किंवा की पॅडला एखादे एक्स्ट्रा डिव्हाइस तर बसवलेले नाही, याची मशीनमध्ये कार्ड टाकण्यापूर्वीच खातजमा करा.
- पिन क्रमांक टाकत असताना स्वतःच्याच दुसऱ्या हाताने की पॅड झाकावे, म्हणजे मागे उभ्या असलेल्या ग्राहकास ते दिसणार नाही.
- इतर कोणालाच तुमचे कार्ड देऊ नका. तसेच पिन क्रमांक प्रविष्ट करीत असताना कोणीही तुमच्या आजूबाजूस नाही याची खात्री केल्यानंतरच व्यवहार करा.

६. स्क्रीन शेअरींग ॲप किंवा रिमोट ॲक्सेस द्वारे फसवणूक

कार्यपद्धती

- निरनिराळ्या क्लृप्त्या वापरून फसवणूककर्त्यांकडून ग्राहकांना त्यांच्या मोबाईल किंवा संगणकावर स्क्रीन शेअरींग ॲप डाऊनलोड करण्यास भाग पाडले जाते.
- अशाप्रकारे ही ॲप्स डाऊनलोड केल्यानंतर प्रत्यक्षात दूर असूनही आपल्या संगणकाचा / मोबाईलचा पूर्ण ताबा फसवणूककर्त्यांकडे जातो आणि ते सहजपणे आपल्या खात्यातून परस्पर पैसे वळते करून घेतात.

खबरदारी

अनोळखी व्यक्तींबरोबर “स्क्रीन शेअर” ची सुविधा असलेले ॲप वापरणे टाळावे.

७. सिम कार्ड स्वॅप / सिम क्लोनिंग

कार्यपद्धती

- हल्ली बँक खात्याशी संबंधित सगळ्याच गोष्टी या आपल्या मोबाईल क्रमांकाशी जोडलेल्या असतात. त्यामुळे फसवणूककर्त्यांकडून सिम कार्डचा ताबा घेण्याचा, प्रसंगी डुप्लिकेट सिम मिळविण्याचा प्रयत्न केलो जातो. एकदा का डुप्लिकेट सिम चोरांच्या हातात पडले की त्यावर आलेल्या ओटीपींचा वापर करून तुमच्या खात्यातील पैसे काढले जातात किंवा परस्पर वळते केले जातात.

- या कार्यपद्धतीत बऱ्याचदा फसवणूककर्त्यांकडून ग्राहकांना संपर्क केला जातो आणि ते एखाद्या मोबाईल सिम कंपनीतून बोलत असल्याचा दिखावा केला जातो. 3G चे 4G मध्ये अपग्रेड किंवा काही सवलतींचे प्रलोभन देऊन ग्राहकांकडून त्यांची माहिती मागितली जाते.

खबरदारी

- सिम कार्डाशी संबंधित कोणतीच माहिती कोणालाच देऊ नका.
- सर्वसामान्य परिस्थितीत जर एखाद्या मोबाईलला बराच वेळ नेटवर्क येत नसेल, तर शंका घेण्यास वाव आहे हे लक्षात ठेवावे. अशा वेळी खातरमजा करण्याकरिता त्वरीत मोबाईल सिम कंपनीला संपर्क साधून डुप्लिकेट सिम जारी करण्यात येत नसल्याबद्दल खात्री करून घ्यायला हवी.

८. इंटरनेटवरील सर्च इंजिनमध्ये दिसणाऱ्या माहितीशी छेडछाड करून फसवणूक

कार्यपद्धती

- बहुतेकदा आपण आपल्याला हवी ती माहिति शोधण्यासाठी इंटरनेटवरील सर्च इंजिनची मदत घेतो. विशेषत: बँक, इन्शुरन्स किंवा आधार कार्ड संबंधित माहितीसाठी इंटरनेटवर संपर्क क्रमांक शोधले जातात.
- याचाच गैरफायदा घेण्यासाठी आर्थिक गुन्हेगारांकडून इंटरनेटरील या माहितीतच छेडछाड केली जाते व बँकेच्या किंवा तुम्ही शोधत असलेल्या कोणत्याही संस्थेच्या खऱ्या माहितीच्या जागी हे फसवणूककर्ते आपले स्वत:चेच मोबाईल क्रमांक टाकून ठेवतात.
- आणि एकदा का या क्रमांकांवर संपर्क साधला, की व्हेरीफिकेशनच्या नावाखाली तुम्हाला तुमचे कार्ड डिटेल्स वगैरे विचारले जातात. अर्थात आपणच आपल्या कामासाठी संपर्क केला असल्याने कोणतीही शंका न येता ही माहिती पुरवली जाते आणि आपसूक आपण या फसवणूककर्त्यांच्या जाळ्यात अडकतो व आपले पैसे गमावून बसतो.

खबरदारी

इंटरनेटवरून सर्च इंजिनच्या मार्फत बँक किंवा तत्सम संस्थेचे "कस्टमर केअर कॉन्टॅक्ट" क्रमांक शोधणे टाळावे. बहुतेकदा फसवणूककर्त्यांकडून यात छेडछाड केलेली असते.

असे संपर्क क्रमांक मिळविण्यासाठी नेहमीच बँक किंवा संस्थेच्या अधिकृत संकेतस्थळावर जाऊनच माहिती घ्यावी.

९. क्यूआर कोड स्कॅनिंगद्वारे फसवणूक

कार्यपद्धती

कोणत्याही निमित्ताने फसवणूककर्त्यांकडून ग्राहकांना संपर्क केला जातो व पेमेन्ट ॲप वापरून क्यू आर कोड स्कॅन करायला भाग पाडले जाते आणि याद्वारे तुमच्या खात्यातील पैसे परस्पर वळते केले जातात.

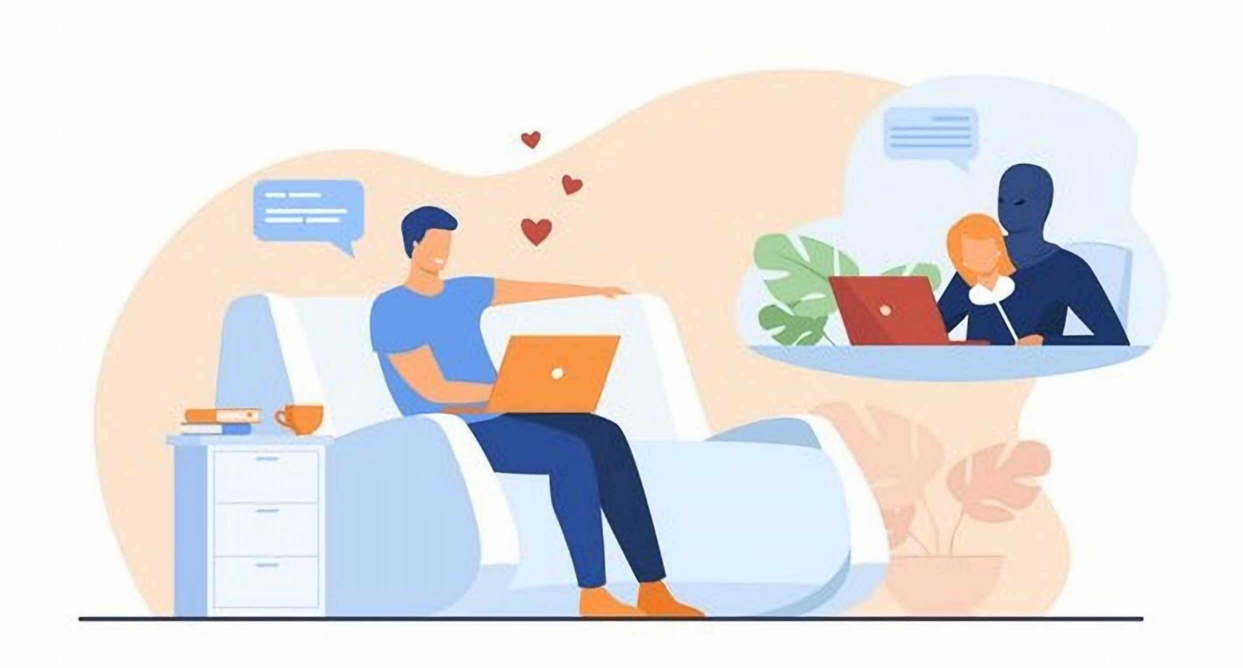
खबरदारी

पेमेन्ट ॲपद्वारे कोणतेही " क्यूआर " कोड स्कॅन करताना खबरदारी घ्यावी. हे क्यू आर कोड एकप्रकारे बँक खात्याशी जोडलेले असतात आणि ते स्कॅन केले असता तुमच्या खात्यातील पैसे त्या विशिष्ट खात्यात वळते होण्याची सोय असते.

१०. समाज माध्यमांवर बनावट खाते उघडून फसवणूक

कार्यपद्धती

- फेसबुक , इन्स्टाग्राम सारख्या लोकप्रिय समाजमाध्यमांवर फसवणूककर्त्यांकडून तुमच्या नावे बनावट खाती उघडली जातात. त्यानंतर तुमच्याच मित्रमंडळींना संपर्क साधून वैद्यकीय किंवा तत्सम कारणे सांगून तातडीच्या मदतीसाठी पैसे पाठविण्याची विनंती केली जाते.
- बऱ्याचदा मित्रमंडळींचा विश्वास संपादन करून त्यांच्याकडून मिळालेल्या खाजगी माहितीचा गैरवापर करून खंडणी मागण्याचे देखील प्रकार घडतात.



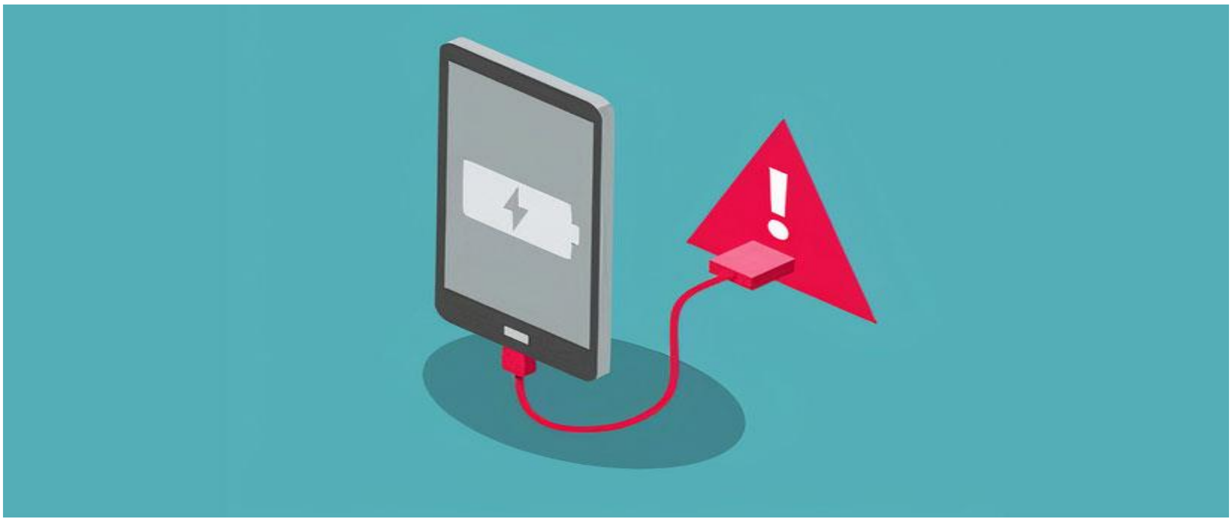
खबरदारी

- अनोळखी व्यक्तींना ऑनलाईन पैसे पाठवू नका.
- समाजमाध्यमांवर तुमची वैयक्तिक आणि खाजगी माहिती देऊ नका.
- समाज माध्यमांवर ओळखीतल्या व्यक्तीकडूनही पैशांची मागणी झाल्यास, फोनद्वारे किंवा प्रत्यक्ष भेटून खातरजमा करून घ्या.

११. ज्यूस जॅकिंग (चार्जिंग पोर्टच्या माध्यमातून माहितीची चोरी)

कार्यपद्धती

- आपण जेव्हा मोबाईल चार्जिंगला लावतो तेव्हा चार्जिंगबरोबरच मोबाईलमधला डेटा सुद्धा ट्रान्सफर होण्याची सोय असते.
- "ज्यूस जॅकींग" हा एक सायबर चोरीचा प्रकार आहे. जेव्हा तुम्ही एखाद्या अनोळखी चार्जिंग पोर्टला स्वतःचा मोबाईल चार्जिंग करायला लावता तिथे या गुन्हेगारांनी "मालवेअर" म्हणजे डेटा चोरण्याचे ॲप बसवलेले असते. त्याचा वापर करून गुन्हेगारांना तुमच्या मोबाईलचा ताबा मिळवून संवेदनशील डाटा, ई-मेल, मेसेजेस, सुरक्षित पासवर्ड इ. चोरणे शक्य होते.



खबरदारी

सार्वजनिक तसेच अनोळखी ठिकाणच्या चार्जिंग पोर्ट किंवा केबल द्वारे चार्जिंग करणे टाळावे.

१२. लॉटरीचे आमिष दाखवून फसवणूक

कार्यपद्धती

- बहुतेकवेळा तुम्हाला ई-मेल किंवा फोन मार्फत एखादी मोठी लॉटरी जिंकली असल्याचे कळविले जाते. मात्र तुम्हीच ती व्यक्ती आहात याची पडताळणी करण्याचे निमित्त करून खोट्या संकेतस्थळावर तुमचे बँक खाते, क्रेडिट कार्डची माहिती वापरून व्हेरीफाय करायला सांगितले जाते. या गोपनीय माहितीचा दुरुपयोग करून पुढे फसवणूक होते.
- तसेच काही वेळा, लॉटरीची रक्कम प्राप्त करण्यासाठी किंवा जिंकलेली वस्तू मिळवण्यासाठी आधी टॅक्स भरावा लागेल किंवा शिपिंग चार्जेस, प्रोसेसिंग चार्जेस भरावे लागतील असे सांगून पैसे भरायला सांगितले जातात.
- लॉटरीच्या रक्कमेच्या तुलनेत ही आगाऊ भरावी लागणारी रक्कम फारच कमी असल्यामुळेच, ग्राहक या सापळ्यात अलगद अडकतात आणि पैसे पाठवून फसतात.

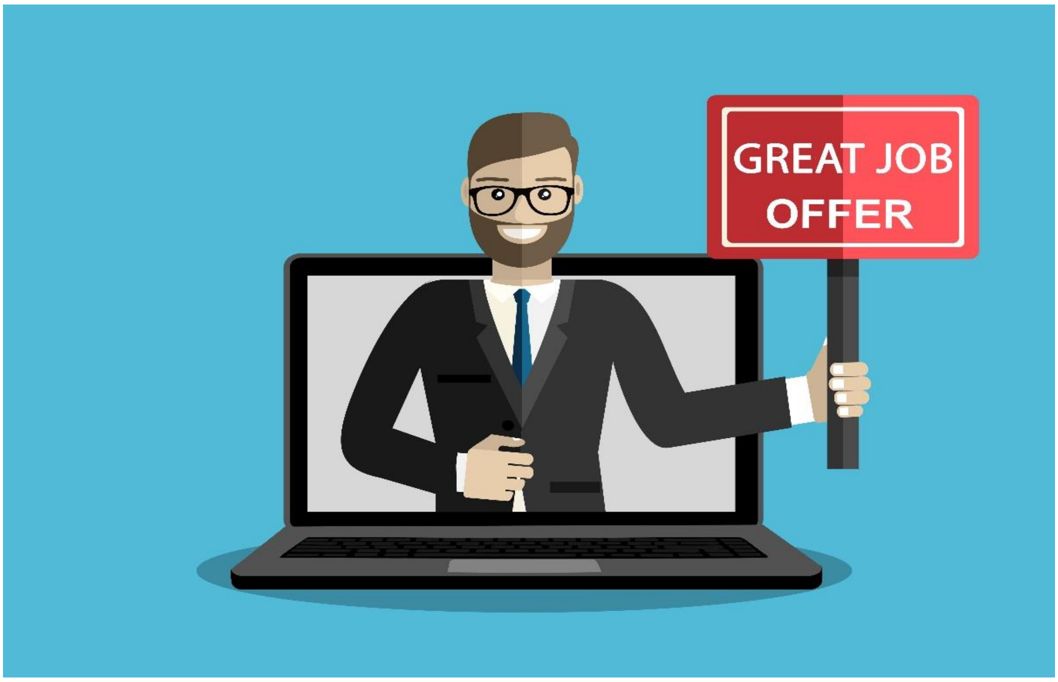
खबरदारी

फोन, ई-मेल्सच्या माध्यमातून लॉटरी संबंधित येण-या मोठ्या रक्कमेच्या भूलथापांना बळी पडू नये व त्यावर सांगितल्याप्रमाणे कोणत्याही रक्कमेचा भरणा करू नये. तसेच आपले बँक खाते, कार्ड डिटेल्स अशी गोपनीय माहिती सांगणे टाळावे.

१३. नोकरीचे आश्वासन देऊन केलेली ऑनलाइन फसवणूक

कार्यपद्धती

- अशा प्रकारात नोकरी संदर्भात माहिती देणाऱ्या खोट्या पोर्टलची निर्मिती करण्यात येते. इच्छुक उमेदवार त्यावर आपले नाव नोंदविताना स्वतःची सर्व गोपनीय माहिती , खाते क्रमांक, डेबिट/क्रेडिट कार्ड इत्यादीबद्दल तपशीलवार नोंद करतात आणि पुढे याच माहितीचा दुरूपयोग करून त्यांना लुबाडले जाते.
- बऱ्याचदा फसवणूककर्ते स्वतःच एखाद्या प्रसिद्ध कंपनीचा अधिकारी असल्याची बतावणी करून इच्छुकांची मुलाखत घेण्याचे नाटक करतात व निवड झाल्याबद्दल ट्रेनिंग प्रोग्रामकरिता पैसे भरणे आवश्यक आहे असे सांगून उमेदवारास लुबाडतात.



खबरदारी

नेहमीच लक्षात ठेवा की, कोणतीच खरीखुरी कंपनी नोकरी देताना पैसे मागत नाही.

अज्ञात जॉब पोर्टलवर पैशांचे व्यवहार करणे टाळावे.

फसवणुकीच्या कार्यपद्धती आणि त्यासंदर्भात घ्यावयाची खबरदारी – बिगर बँकिंग वित्तीय संस्था

१. फसवणूक करणा-यांकडून कर्ज वितरणासाठी केलेल्या बनावट जाहिराती

कार्यपद्धती

- फसवणूककर्त्यांकडून अत्यंत कमी व्याजदरात, सहजसोप्या परतफेड योजनेसह तसेच विनातारण वैयक्तिक कर्ज उपलब्ध असल्याच्या जाहिराती प्रसिद्ध केल्या जातात आणि कर्ज मिळविण्यासाठी संपर्क साधण्यास सांगितले जाते.

- सर्वसामान्य भोळ्याभाबड्या ग्राहकांचा विश्वास संपादन करण्यासाठी संपर्कासाठीचे ई-मेल पत्ते हे प्रस्थापित खऱ्याखुऱ्या एनबीएफसीच्या वरीष्ठ अधिका-यांचे असल्याचे भासवले जाते.
- मात्र जेव्हा ग्राहक कर्ज घेण्यासाठी अशा फसव्या लोकांशी संपर्क साधतात तेव्हा ग्राहकांकडून प्रोसेसिंग फी, जीएसटी, आगाऊ इएमआय, अनहोल्ड चार्जेस इत्यादीच्या नावाखाली सुरूवातीलाच पैसे भरण्यास सांगतले जाते. पैसे मिळताच कर्ज वितरित न करताच हे फसवणूककर्ते फरार होतात.
- आपण इंटरनेटवर सर्च इंजिनद्वारे कर्जासंबंधी माहिती शोधली असता लगेच दिसून येतील अशा बनावट संकेतस्थळांच्या लिंक्स देखील फसवणूकर्त्यांकडून तयार केल्या जातात

खबरदारी

- एनबीएफसी किंवा कोणतीही बँक कर्ज वितरित करण्यापूर्वी कधीच आगाऊ रक्कम मागत नाही.
- बँक किंवा एनबीएफसीतर्फे आकारली जाणारी प्रोसेसिंग फी, ही नेहमी कर्जाच्या रक्कमेतून कापून घेतली जाते.
- ऑनलाइन माध्यमातून कमी व्याजदरात कर्जाच्या ऑफर व्यवस्थित पडताळून घ्या. त्यासाठी थेट पैसे भरू नका किंवा तुमच्या गोपनीय माहितीची कुठेही नोंद करू नका.

२. एसएमएस/ई-मेल/ फोन द्वारे फसवणूक

कार्यपद्धती

- आर्थिक गुन्हेगारांकडून एसएमएस/ई-मेल तसेच समाजमाध्यमांवर कमी व्याजदरात कर्ज उपलब्ध असल्याची खोटी जाहिरात पसरवली जाते. लोकांचा विश्वास बसावा यासाठी यात दिलेल्या मोबाईल क्रमांकावर प्रस्थापित व प्रसिद्ध अशा एनबीएफसीचे लोगो प्रोफाइल फोटो म्हणून ठेवलेले असतात. तसेच फसवणूककर्त्यांकडून त्यांचे आधार किंवा पॅन कार्ड तसेच एनबीएफसीचे आय कार्ड देखील दाखवले जातात.
- कर्जाची निकड असणाऱ्या लोकांना मोठ्या प्रमाणावर असे एसएमएस/ई-मेल पाठविल्यानंतर काही ग्राहकांना फोनद्वारे संपर्क केला जातो आणि त्यांना कर्जाची खोटी मंजुरी पत्रे तसेच चेकचे खोटे फोटो पाठवून विविध चार्जेसच्या नावाखाली पैशांची मागणी केली जाते. एकदा का हे पैसे ग्राहकाने भरले, की ते घेऊन हे फसवणूककर्ते पसार होतात आणि कमी व्याजदरातील कर्जाच्या लोभापायी ग्राहक आपले पैसे गमावून बसतो.

खबरदारी

- एसएमएस/ ई-मेल द्वारे पसरवलेल्या लिंक्सवर कधीच क्लिक करून नका. तसेच जाहिरात म्हणून आलेल्या एसएमएस व ई-मेलना प्रत्युत्तर पाठवू नका.
- अनोळखी व्यक्तींकडून आलेल्या आणि संशयास्पद अटॅचमेंट असलेल्या व फिशिंग लिंक्स असलेल्या मेल्स उघडू नका, त्यांना प्रतिसाद देऊ नका.
- फोन अथवा ई-मेल द्वारे संपर्क साधून स्वत:च कर्ज उपलब्ध करून देतो असे सांगणा-या लोकांवर कधीच विश्वास ठेऊ नका.
- ऑनलाइन माध्यमातून कमी व्याजदरात कर्जाच्या ऑफर व्यवस्थित पडताळून घ्या. त्यासाठी थेट पैसे भरू नका किंवा तुमच्या गोपनीय माहितीची कुठेही नोंद करू नका.

३. ओटीपीचा वापर करून फसवणूक

कार्यपद्धती

- ‘एनबीएफसी’तर्फे संपर्क करत असल्याचा बनाव करत फसवणूककर्त्यांकडून लोकांना नवीन तसेच वाढीव कर्जासाठी एसएमएस केले जातात आणि कर्ज मिळविण्यासाठी त्यांनी दिलेल्या मोबाईल क्रमांकावर संपर्क साधण्यास सांगितले जाते, जो खरेतर या फसवणूककर्त्यांचाच असतो.
- एखाद्याने या क्रमांकावर संपर्क केल्यास त्याला काही फॉर्म (जे ऑनलाइन सुद्धा असू शकतात) भरायला सांगितले जातात, ज्यामध्ये आर्थिक बाबींसंदर्भात माहिती विचारलेली असते. या माहितीबरोबर ओटीपी / पिन सारखी गोपनीय माहिती सुद्धा भरण्यास उद्युक्त केले जाते, ज्याद्वारे सहज ग्राहकाच्या खात्यातील पैसे काढले जातात.

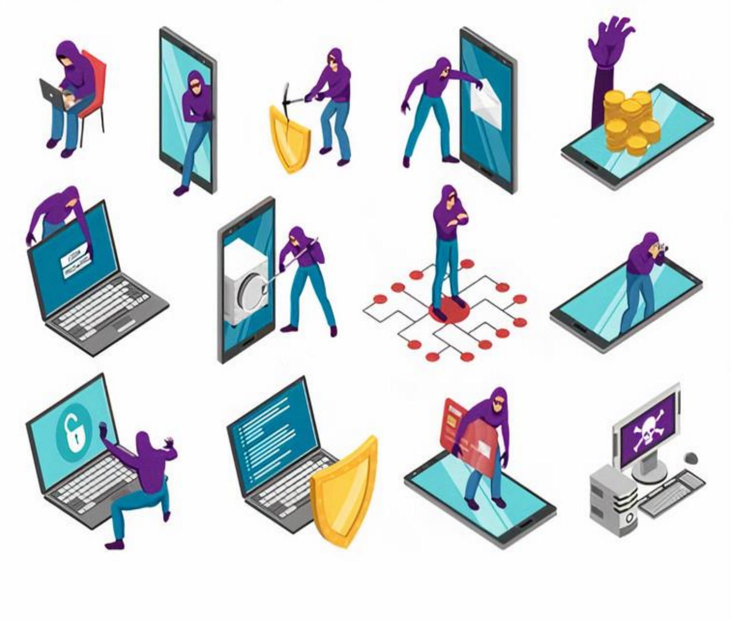
खबरदारी

- कधीच कोणालाच आपला ओटीपी/ पिन क्रमांक/ वैयक्तिक तपशील, कोणत्याही स्वरूपात शेअर करू नका.
- तुमच्या नकळत कोणी ओटीपी संदर्भातील व्यवहार करू पाहत नाही ना याची खबरदारी घ्या, त्यासाठी नियमित ई-मेल, एसएमएस तपासत जा.

४. कर्ज वितरणासाठी बनावट वेबसाईट/ ॲप

कार्यपद्धती

- तातडीने अल्प मुदतीची कर्जे उपलब्ध करून देणारी बरीचशी बोगस ॲप्स अस्तित्वात आहेत. या ॲप्सकडून ग्राहकांची फसवणूक केली जाते किंवा अनेकदा अव्वाच्या सव्वा व्याजआकारणी केली जाते.
- भोळ्याभाबड्या ग्राहकांना फसविण्यासाठी एखादी ऑफर मर्यादित कालावधीसाठीच उपलब्ध असल्याची भीती दाखवत त्यांना घाईगडबडीत निर्णय घेण्यास भाग पाडले जाते.



खबरदारी

संशयास्पद ॲप्स इत्यादी मार्फत कर्ज घेण्यापूर्वी खालील गोष्टी तपासून पहा.

- ग्राहकाच्या क्रेडिट स्कोरला महत्व द्यायचे सोडून इतर वैयक्तिक माहिती मिळविण्याकडे कर्ज पुरवठा करणा-याचा कल तर नाही ना ?
- सरकारी किंवा तत्सम अधिकृत संस्थेकडे कर्ज पुरवठादार नोंदणीकृत आहे का ?
- संपर्कासाठी प्रत्यक्ष पत्ता, फोन नंबर दिला आहे का याची खात्री करून घ्यावी अन्यथा पुढे जाऊन संपर्क करणे कठीण होऊ शकते.
- कर्जदाराच्या अर्जावर प्रक्रिया करण्यापूर्वी कोणतीही नामांकित एनबीएफसी / बँक पैशांची मागणी करीत नाही हे लक्षात असू द्यावे.
- मान्यताप्राप्त कर्जपुरवठादार कागदपत्रांची पडताळणी केल्याशिवाय कधीच कर्ज वितरित करीत नाही.
- एनबीएफसीतर्फे कर्ज पुरवठा करणारे ॲप मान्यताप्राप्त आहे का हे तपासून घ्यावे.

५. मनी सर्क्युलेशन / पॉन्झी / मल्टी लेवल मार्केटिंग स्कीमच्या माध्यमातून फसवणूक

कार्यपद्धती

- सोप्या पद्धतीने खूप पैसै कमाविण्याचे आमिष दाखवून एमएलएम / चेन मार्केटिंग किंवा पिरॅमिड स्ट्रक्चर सारख्या योजनांमध्ये सभासद नोंदणी करून घेतली जाते आणि पुढेही आणखी नवीन सदस्यांना जोडून घ्यायला सांगितले जाते.
- भोळयाभाबड्या लोकांचा विश्वास संपादन करण्यासाठी अशा योजना सुरूवातीला मोठ्या परताव्याचे आमिष दाखवून त्याप्रमाणे परतफेडही करतात आणि त्याद्वारे आणखी जाहिरातबाजी करत नवीन सदस्यांना आकर्षित करून घेतात.
- उत्पादनाच्या विक्रीवर कमिशन देण्याऐवजी अशाप्रकारे नवीन सदस्य जोडण्यासाठीच वर्तमान सदस्यांना प्रोत्साहित करून कमिशन दिले जाते
- अशा प्रकारामुळे काही काळानंतर सभासदही कमी होऊ लागतात आणि या योजना टिकाव धरू शकत नाहीत. त्यानंतर फसवणूककर्त्यांकडून ही योजना बंद केली जाते आणि गुंतवणूकदारांचे पैसे लुबाडून ते पळून जातात.

खबरदारी

- गुंतवणूकदारांसाठी परतावा हा जोखीमेच्या प्रमाणात असतो. जितका परतावा जास्त तितकीच जोखीम अधिक. त्यामुळे कधीही कोणी असामान्य, उदाहरणार्थ वर्षाला 40/50% परतावा देत असल्यास हे संभाव्य फसवणुकीचे पहिले लक्षण आहे हे लक्षात घ्यावे. अशा प्रसंगी खबरदारी घेणे आवश्यक आहे.
- प्रत्यक्षात मालाची विक्री न करताच किंवा कोणतीही सेवा न देता जर तुम्हाला कोणी कमिशन, बोनस देत असेल तर शंका घेण्यास वाव आहे असे समजावे.
- अशा उच्च परताव्याच्या योजनांच्या मोहजालात लोकांनी सापडू नये.
- मनी सर्क्युलेशन/ मल्टी लेव्हल मार्केटिंग/ पिरॅमिड स्ट्रक्चर अंतर्गत पैसे गोळा करणे हा “प्राइज चिट आणि मनी सर्क्युलेशन (बंदी) कायदा, १९७८” अंतर्गत दखलपात्र गुन्हा आहे. अशा पद्धतीने ऑफर देणा-यांविरुध्द राज्य पोलिसांकडे ताबडतोब तक्रार दाखल करावी.

६. बनावट कागदपत्रांच्या आधारे दिलेले / घेतलेले कर्ज

- या प्रकारात बनावट कागदपत्रांच्या आधारे वित्तीय संस्थांकडून सेवा मिळविण्याचा प्रयत्न केला जातो.
- योग्य ती पडताळणी न करता आपली केवायसी कागदपत्रे चुकीच्या हाती सोपवल्यामुळे असे प्रकार घडतात.
- तसेच एखाद्याची ओळखपत्रे, बँक खातेसंदर्भात माहिती अशा वैयक्तिक माहितीची चोरी करून बनावट ओळख निर्माण करून देखील वित्तीय संस्थांकडून कर्ज घेण्याचे प्रकार घडतात.

खबरदारी

- ग्राहकाने कोणत्याही संस्थेकडून कर्ज घेण्यासाठी केवायसी व NACH सारखी इतर कागदपत्रे जमा करताना योग्य ती खबरदारी घेणे गरजेचे आहे.
- अशी कागदपत्रे संस्थेच्या अधिकृत व्यक्ती किंवा संस्थेच्या अधिकृत ई-मेल आयडीवरच पाठवावीत.
- तसेच कर्ज मंजूर न झाल्यास किंवा कर्ज परतफेड पूर्ण झाल्यावर, ग्राहकाने एखाद्या संस्थेला दिलेली कागदपत्रे रद्द करण्याची विनंती करावी.

आर्थिक व्यवहार करताना घ्यावयाची सर्वसामान्य खबरदारी

सर्वसाधारण मुद्दे :

- इंटरनेट ब्राउझिंग दरम्यान संशयास्पदरीत्या उघडणाऱ्या पॉप अप्स बाबत दक्ष रहा.
- ऑनलाईन पेमेंट करण्यापूर्वी नेहमी पेमेंट गेटवे सुरक्षित असल्याची खात्री करून घ्या (https:// - यूआरएल मध्ये पॅड लॉक सिम्बॉल असणे गरजेचे)
- तुमचा डेबिट कार्ड, क्रेडिट कार्ड क्रमांक, पिन, सीव्हीव्ही गुप्त ठेवा.
- संकेतस्थळांवर / उपकरणांवर / सार्वजनिक लॅपटॉप/ डेस्कटॉपवर कार्ड डिटेल्स जतन करणे टाळा.
- टू-फॅक्टर ऑथेन्टिकेशनची सुविधा उपलब्ध असल्यास त्याचा वापर करा.
- संशयास्पद अटॅचमेन्ट असलेले किंवा फिशिंग लिंक्स असलेले अनोळखी व्यक्तींकडून आलेले मेल्स उघडू नका.
- चेकबूक किंवा केवायसीच्या प्रती अनोळखी व्यक्तींना देऊ नका.

संगणक / उपकरणांच्या सुरक्षेसाठी :

- ठराविक कालावधी नंतर पासवर्ड बदलत रहा.
- संगणकात " अॅन्टीव्हायरस " अॅप बसवा व उपलब्धतेनुसार अपडेट करत रहा.
- अनोळखी यूएसबी ड्राइव्ह / उपकरणे वापरण्यापूर्वी स्कॅन करून घ्या.
- आपण वापरत असलेले उपकरण अनलॉक स्थितीत सोडून जाऊ नका.
- ठराविक वेळेनंतर संगणक आपोआपच लॉक होइल अशी रचना करून ठेवा.
- अज्ञात अॅप किंवा सॉफ्टवेअर इन्स्टॉल करू नका.
- अज्ञात उपकरणांवर (संगणकावर) पासवर्ड किंवा इतर गोपनीय माहिती जतन करून ठेवू नका.

इंटरनेट वापरताना घ्यावयाची काळजी :

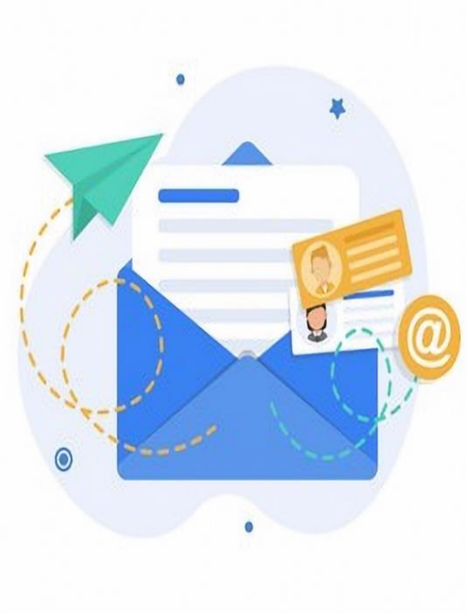
- असुरक्षित संकेतस्थळाला (वेबसाईट) भेट देणे टाळा.
- अज्ञात ब्राउजर वापरणे टाळा.
- सार्वजनिक उपकरणांवर पासवर्ड इत्यादी जतन करणे टाळा.
- अज्ञात संकेतस्थळांवर तुमची वैयक्तिक गोपनीय माहिती टाकणे टाळा.
- समाजमाध्यमांवर अनोळखी व्यक्तींसोबत स्वतःची खाजगी माहिती शेअर करू नका.
- ई-मेल किंवा एसएमएस द्वारे एखादी लिंक उघडल्यास ती सुरक्षित असल्याची खात्री करून घ्या.

इंटरनेट बँकिंगच्या सुरक्षित वापरासाठी :

- सार्वजनिक उपकरणांचा वापर करताना व्हर्च्युअल कीबोर्ड वापरा.
- काम झाल्यानंतर लगेच लॉगआऊट करा.
- ठराविक कालावधीनंतर पासवर्ड बदलत रहा.
- ई-मेल आणि इंटरनेट बँकिंगसाठी एकच पासवर्ड वापरू नका.
- आर्थिक व्यवहार करताना सायबर कॅफे इत्यादी सार्वजनिक ठिकाणांवरील संगणक वापरणे टाळा.

ई-मेल खात्याच्या सुरक्षिततेसाठी :

- अज्ञात ठिकाणांहून आलेल्या ई-मेल्सवर क्लिक करू नका.
- सार्वजनिक व मोफत अशा नेटवर्कवर ई-मेलचा वापर टाळा.
- बँक पासवर्ड इ. सारखी गोपनीय माहिती ई-मेल मध्ये जतन करू नका.



"पासवर्ड" सुरक्षेकरिता घ्यावयाची काळजी :

- अक्षरे, अंक आणि कीबोर्डवरील वैशिष्ट्यपूर्ण चिन्हे एकत्रित करून तुमचा पासवर्ड तयार करा.
- टू-फॅक्टर ऑथेन्टिकेशनची सुविधा उपलब्ध असल्यास त्याचा वापर करा.
- अधूनमधून पासवर्ड बदलत रहा.

ठेवी स्वीकारणारी " एनबीएफसी" अधिकृत आहे की नाही, हे कसे जाणून घ्याल?

- ठेवी स्वीकारण्याची परवानगी असलेल्या एनबीएफसींची यादी आरबीआयच्या https://www.rbi.org.in या संकेस्थळावर उपलब्ध आहे. या यादीत संबंधित एनबीएफसीचा समावेश आहे का हे तपासून घ्यावे. तसेच ठेवी स्वीकारण्यावर बंदी घातलेल्या कंपन्यांच्या यादीत नाव नसल्याची खात्री करून घ्यावी.
- 'एनबीएफसी'ने आपल्या संकेतस्थळावर, रिझर्व्ह बँकेने जारी केलेले नोंदणी प्रमाणपत्र ठळकपणे दिसेल अशाप्रकारे प्रसिद्ध करणे आवश्यक आहे. विशेषत: ठेवी स्वीकारण्यासाठी आरबीआयची मान्यता असल्याचे त्यात नमूद केले असावे. ठेवीदारांनी या प्रमाणपत्राची सत्यता तपासून पाहत सदर एनबीएफसी ही ठेवी स्वीकारण्यासाठी अधिकृत असल्याची खात्री करून घ्यावी.
- एनबीएफसी १२ महिन्यांपेक्षा कमी तसेच ६० महिन्यांपेक्षा अधिक कालावधीसाठी ठेवी स्वीकारू शकत नाहीत. तसेच ठेवीदारांना १२.५% पेक्षा जास्त दराने व्याज देऊ शकत नाहीत.
- व्याजदरात होणारे बदल आरबीआयतर्फे खालील दुव्यावर प्रसिद्ध केले जातात.

  https://rbi.org.in Sitemap------> NBFC list --------> FAQs

ठेवीदारांनी घ्यावयाची खबरदारी :

- ठेवीदारांनी प्रत्येक ठेवीसाठी योग्य ती पावती देण्याचा आग्रह कंपनीकडे धरावा.
- पावतीवर, त्या कंपनीच्या अधिकृत अधिका-यांची सही आवश्यक असून त्यात ठेवीदाराचे नाव, रक्कम (अंकात आणि अक्षरात लिहिलेली), व्याजदर, 'ठेवी'ची तारीख आणि 'ठेव परिपक्वता' तारीख या सर्वांचा समावेश असणे आवश्यक आहे.
- ब्रोकर अथवा एजंटमार्फत ठेव जमा करत असल्यास सदर ब्रोकर / एजंटना "एनबीएफसी"तर्फे अधिकृत मान्यता आहे का याची खात्री करून घ्यावी.
- एनबीएफसी मधील ठेवींना 'ठेव विमा कवच' उपलब्ध नाही, हे ठेवीदारांनी लक्षात घ्यावे.

ऑनलाईन तक्रार कशी कराल?

"आरबीआय"ला तक्रार करण्यासाठी –

- https://cms.rbi.org.in या दुव्यावर भेट द्यावी.

" सेबी" ला तक्रार करण्यासाठी –

- https://scores.gov.in या दुव्यावर भेट द्यावी.

"IRDA" म्हणजेच "भारतीय विमा नियामक आणि विकास प्राधिकरण"ला तक्रार करण्यासाठी –

- https://igms.irda.gov.in/ या दुव्यावर भेट द्यावी.

"NHB" म्हणजेच राष्ट्रीय गृह निर्माण बँकेला तक्रार करण्यासाठी -

- https://grids.nhbonline.org.in/ या दुव्यावर भेट द्यावी.

सायबर पोलीस स्टेशनला तक्रार करण्यासाठी -

- https://cybercrime.gov.in/ या दुव्यावर भेट द्यावी.

शब्दसूची*

- **ॲडव्हान्स फी/ प्रोसेसिंग फी/ टोकन फी** : कर्ज वितरण प्रक्रियेसंबंधित रक्कमा.
- **टू - फॅक्टर ऑथेन्टिकेशन** : द्विघटक प्रमाणीकरण (2FA म्हणूनही ओळखले जाते.) याच्या संयोजनामुळे वापरकर्त्याची सुस्पष्ट ओळख निर्माण होते. याद्वारे एखादा व्यवहार प्रमाणित करण्यासाठी दोन गोष्टींची गरज असते. त्यातील एक गोष्ट ग्राहकाजवळ उपलब्ध असते (उदा. कार्ड क्र, एक्सपायरी डेट, सीव्हीव्ही) आणि दुसरा घटक जो ग्राहकाला माहित असतो. (उदा. पिन क्रमांक किंवा ओटीपी)
- **3डी सेक्यूअर**: ऑनलाईन डेबिट कार्ड, क्रेडिट कार्डचे व्यवहार आणखी सुरक्षित व्हावे यासाठी "एक्सएमएल" आधारित नियमावलीची. व्हेरीफाइड बाय विजा, मास्टरकार्ड सेक्यूअर कोड, अमेरिकन एक्स्प्रेस सेफकी असेही संबोधले जाते.
- **ॲक्वायरींग बँक**: क्रेडिट किंवा डेबिट कार्डवर प्रक्रिया करणारी बँक. ॲक्वायरींग बँकद्वारे साधारणपणे विजा, मास्टर कार्ड, माएस्ट्रो, रुपे कार्डांवर प्रक्रिया केली जाते.
- **ऑथोरायझेशन (प्रमाणीकरण)**: कार्ड जारी करणाऱ्या बँकेकडून ग्राहकाच्या खात्यात शिल्लक उपलब्ध असल्याचे प्रमाणीकरण केले जाते.
- **बँक आयडेंटीफीकेशन नंबर (बिन) बँक ओळख क्रमांक**: व्हिसा आणि मास्टर कार्ड, त्यांच्या सभासद असणाऱ्या बँका, आर्थिक संस्था आणि अशा प्रक्रिया करणाऱ्या संस्थांना हा ओळख क्रमांक देतात.
- BIN Validation : "बिन" प्रमाणीकरण करण्याची पद्धत तपासणे म्हणजे व्हॅलिडेशन.
- **ब्लॅकलिस्टिंग**: आर्थिक फसवणूक रोखण्यासाठी, कपटी खरेदीदार आणि संशयास्पद विक्रेत्यांची माहिती गोळा करण्यात येते.

- **कार्ड कॅप्चर पेज**:
  - कार्ड डिटेल्स ज्यावर नोंदविले जातात असे सेक्यूअर पेज. PCI DSS प्रमाणित संस्थांना याची परवानगी असते. उदा.
  - अक्वायरींग बॅन्क (उदा. एसबीआय, एचडीएफसी)
  - ॲग्रीगेटर बँक (उदा. PayU)
  - व्यापारी (उदा. फ्लिपकार्ट, ॲमेझॉन)
- Card Number
  - बँकेकडून किंवा किंवा क्रेडिट कार्ड असोसिएशन ग्राहकांना कार्ड क्रमांक दिला जातो. पेमेंट करताना याची गरज असते.
  - कार्डाच्या दर्शनी भागावर हा क्रमांक असतो. (ओळख क्र., श्रेणी, चलन असे विविध संदर्भ घेऊन हा क्रमांक तयार झालेला असतो.
  - व्हिसा कार्ड, मास्टरकार्ड, माएस्ट्रो, रूपे - 16 अंक असतात.
  - ॲमेक्स - 15 अंक असतात.
- Card Present **(कार्ड प्रेझेंट)** : व्यवहार होत असताना कार्ड धारक किंवा कार्ड प्रत्यक्ष हजर असणे. (उदा. किराणामाल दुकानात कार्ड स्वाइप करणे). कार्ड नॉट प्रेझेंट पेक्षा कार्ड प्रेझेंट मधे टीडीआर/ एमडीआर दर कमी असतात. कारण या प्रकारात तुलनेने जोखीम कमी असते.
- Card Vaulting **(कार्ड वॉल्टिंग)**: कार्ड संबंधित माहिती पुढील वापरासाठी जतन करून ठेवण्याची प्रक्रिया. "पीसीआय डीएसएस" प्रमाणित संस्थांद्वारे (बँक, ॲग्रीगेटर किंवा व्यापारी) कार्ड संबंधित तपशील संग्रहित केले जाऊ शकतात.
- Closed-loop prepaid cards / wallet **(क्लोज्ड लूप प्रिपेड काड्‌र्स/ वॉलेट)**: या प्रकारचे कार्ड हे एका विशिष्ट व्यापारी किंवा विक्रेत्याकडेच वापरता येते. यातून पैसे काढून घेता येत नाहीत.

- **Co- branded card (को-ब्रांडेड कार्डस्)**: वित्तीय संस्थांकडून कॉर्पोरेट ब्रँण्डिंगसह विशिष्ट स्कीम अंतर्गत ही कार्डस् जारी केली जातात.
- **Collection account: (कलेक्शन खाते)** : पेमेंट गेटवेमार्फत येणारे पैसे हे व्यापारांच्या कलेक्शन खात्यात जमा होतात. हे खाते चालू खाते, नोडल खाते अथवा एस्क्रो प्रकारचे असू शकते.
- Credit Cards: क्रेडिट कार्डचा वापर करून वित्तीय संस्थांकडून कर्ज स्वरूपात पैसे घेऊन वस्तू तसेच सेवा विकत घेता येतात.
- **Chargback (चार्जबॅक)** : क्रेडिट कार्डधारकाने त्याला कार्ड जारी करणाऱ्या बँकेकडे एखाद्या व्यवहारासंदर्भात केलेली तक्रार

  चार्जबॅक दाखल करण्याची विविध कारणे असू शकतात.

  - सेवा किंवा वस्तू (माल) वितरित न करणे
  - कॅन्सलेशन नंतर रिफंड न मिळणे
  - संशयास्पद फसवणुकीचे व्यवहार.
  - कार्ड हॅकिंग.

  अशा परिस्थितीत कार्ड जारी करणारी बँक (इश्युइंग बँक) अक्कायरींग बँकेला चार्जबॅक पाठवते. अक्कायरींग बँक यासंदर्भात विक्रेत्याला थेट किंवा ॲग्रीगेटरमार्फत संपर्क करते आणि वस्तू किंवा सेवा दिल्याची अथवा परतावा दिल्याच्या पुराव्याची विचारणा करते. या सर्व प्रक्रियेसाठी कालमर्यादा निश्चित केली गेली आहे. त्याचे पालन न केल्यास विक्रेत्याला रक्कम परत करावी लागते.
- **Credit limit (क्रेडिट मर्यादा)** : आर्थिक संस्थेकडून देण्यात येणाऱ्या कर्जाच्या कमाल रक्कमेला क्रेडिट लिमिट संबोधले जाते. असे कर्ज क्रेडिट कार्ड स्वरूपात किंवा लाइन ऑफ क्रेडिट रुपात देखील मिळू शकते. ग्राहकाच्या कर्ज आवेदनातील माहितीवरून ही मर्यादा ठरविली जाते. ग्राहकाचा क्रेडिट स्कोर तसेच भविष्यात कर्ज मिळविण्याची शक्यता यावर क्रेडिट लिमिटचा प्रभाव असू शकतो.

- **CVV (Card Verification Value)**: ऑनलाईन व्यवहार करण्यासाठी सीव्हीव्ही क्रमांक अत्यंत महत्वाचा असतो. त्यामुळे तो गोपनीय ठेवावा व कोणाशीच शेअर करू नये.
- **Debit Card (डेबिट कार्ड)** : बँक खात्यात असणाऱ्या रक्कमेमार्फत खरेदीसाठी वापरले येणारे कार्ड.
- **Declined Payments (डिक्लाइंड पेमेंट्स)** : डिक्लाइंड पेमेंट्स म्हणजे कार्ड जारी करणाऱ्या बँकेकडून नाकारण्यात आलेले व्यवहार. अशा व्यवहारांवर पुढे काही कार्यवाही न होता ग्राहकास पुन्हा नव्याने व्यवहार करावा लागतो.
- **डिजीटल सिग्नेचर** : एखाद्या व्यक्तीची अथवा संस्थेची ओळख किंवा विश्वासार्हता तपासण्यासाठी डिजीटल स्वाक्षरीच्या रूपात असलेल्या इलेक्ट्रॉनिक फाइलचा वापर केला जातो. सर्टिफिकेट ऑथिरिटीकडून ही डिजीटल प्रमाणपत्रे जारी केली जातात व त्याचा वापर "सुरक्षित सॉकेट लेअर" (SSL) सह केला जातो.
- **E- Commerce Platform (ई-कॉमर्स प्लॅटफॉर्म)** – यात सॉफ्टवेअर मार्फत ई कॉमर्स व्ययसाय करण्यासाठी आवश्यक अशा वेबसाईट, श्रेणी व्यवस्थापन, किंमत व्यवस्थापन, मागणी आणि पेमेंटचे व्यवस्थापन या सुविधा पुरविल्या जातात. उदा. शॉपीफाय, मजेन्टो इ.
- **EMI – Equated Monthly Instalments (इएमआय)** -- बँकेकडून कार्ड धारकास किंवा ग्राहकास देय रक्कम छोट्या सुलभ हफ्त्यांमध्ये दर महिन्याला परतफेड करण्यासाठी केलेली सोय. यासाठी बँकेकडून प्रोसेसिंग फी किंवा व्याज आकारणी केली जाऊ शकते.
- **EVM : EuroPay, Master Card, & Visa (इव्हीएम)**: कार्डसंबंधित होणारी फसवणूक कमी करण्याच्या उद्देशाने हे मायक्रोचिप आधारित तंत्रज्ञान विकसित करण्यात आले आहे.
- **Encryption (एनक्रिप्शन)** : एनक्रिप्शन केलेली माहिती सर्वसाधारपणे कोणालाही वाचता येत नाही. फक्त संबंधित "की" माहित असलेल्या व्यक्तीलाच यातील माहिती उपलब्ध होऊ शकते.
- **Expiry Date (एक्सपायरी डेट)**: कार्डाची वैधता ज्या तारखेला संपते ती तारीख. या तारखेनंतर त्या कार्डचा वापर करता येत नाही.

- **Flat Fee (फ्लॅट फी):** एखाद्या व्यवहाराच्या रक्कमेच्या टक्केवारीनुसार फी न आकारता ठरलेली समान रक्कम फी म्हणून आकारली जाते.
- **Gift card (गिफ्ट कार्ड) :** विशिष्ट ठिकाणीच खरेदी करण्यासाठी आगाऊ पैसे भरलेले कार्ड.
- **Gateway: गेटवे** हा एक असा व्यवसाय आहे की जो डिजीटल आर्थिक सेवा पुरविणाऱ्या संस्थांना त्यांच्या विविध कार्याचे व्यवस्थापन करून देतो. आर्थिक देवघेव, ग्राहकांच्या माहितीचे संकलन आणि जोखमीचे व्यवस्थापन या सर्व बाबींचा समावेश या कार्यामध्ये होतो.
- **Interchange Fees (इंचरचेंज फी) :** कोणताही व्यवहार पूर्ण करताना येणाऱ्या खर्चासाठी इशुअर कडून अक्वायरला देण्यात येणारा मोबदला. व्हिसा, मास्टर कार्ड आणि इतर प्रदाते हे शुल्क निर्धारित करतात.
- **IMPS (आयएमपीएस) :** NPCI तर्फे तात्काळ पैसे पाठविण्यासाठी ही सेवा चालविली जाते. यात मोबाईल क्रमांकाच्या आधारे एक लाखापर्यंतची रक्कम त्वरीत पाठविता येते.
- **Know Your Customer (KYC):** व्यक्ती तसेच एखाद्या व्यवसायाशी संबंधित ओळख पटवून देणारी कागदपत्रे.
- **Multi Level Marketing (MLM):** एमएलएम चा अर्थ बहुस्तरीय विपणन. याचा अर्थ एखाद्या संस्थेतर्फे, माल अथवा सेवा विक्री करणाऱ्यास कमिशन दिले जाते तसेच त्याने नेमलेल्या सहभागीदारांनी केलेल्या विक्रीवर पण त्याला कमिशन मिळते.
- **Near Field Communication NFC:** एसएफसी प्रकारात संपर्क तंत्रज्ञानाने परिपूर्ण असलेल्या मोबाइलद्वारे सक्षम टर्मिनलवर पेमेंट तपशील पुरवला जातो.
- **NEFT : एनइएफटी** चा अर्थ राष्ट्रीय इलेक्ट्रॉनिक निधी हस्तांतरण. आरबीआयतर्फे चालवल्या जाणाऱ्या या प्रकारात विशिष्ट बॅचमध्ये समोरच्याला पैसे पाठविण्याची सोय उपलब्ध करून देण्यात आली आहे.

- **One Time Password (OTP) वन टाईम पासवर्ड**: ऑनलाइन व्यवहार करताना अतिरिक्त सुरक्षिततेसाठी ओटीपी हा प्रकार वापरला जातो. यामुळे कोणताही व्यवहार पूर्ण करण्यासाठी दोन वेळा गोपनीय माहितीची खात्री केली जाते. ओटीपी हा विशिष्ट व्यवहाराकरिता असतो व मर्यादित कालावधीत त्याचा वापर करावा लागतो.
- **Phishing :** नामांकित कंपन्यांच्या नावे खोटे ई-मेल पाठवून त्याद्वारे लोकांकडून पासवर्ड, क्रेडिट कार्ड यासारखी त्यांची वैयक्तिक गोपनीय माहिती काढून घेण्यासाठीचा प्रयत्न.
- **Point of Sale Device Terminal, Acceptance Device, POS, mPOS**: इलेक्ट्रॉनिक व्यवहार स्वीकारण्याची साधने.
- **PCI- DSS पीसीआय- डीएसएस** चा अर्थ अंतिम उपभोक्त्याची माहिती सुरक्षित ठेवण्यासाठी, व्यावसायिक संस्थांनी अवलंब केलेली प्रणाली.
- **P2P, Remote Cross- border Transfer of Value, Remittance:** एका देशातील एका व्यक्ती कडून दुसऱ्या देशातील व्यक्तीला पैसे देणे आणि प्राप्त करणे.
- **Quick Response code: QR Code :** क्यूआर कोड हा बारकोडचा एक प्रकार आहे ज्याद्वारे माहिती संग्रहित केली जाते आणि जी डिजीटल फोनद्वारे वाचता येऊ शकते.
- **Reconciliation:** आर्थिक व्यवहारांच्या हिशोबाची पडताळणी करण्याची व्यवस्था
- **Recurring Payments:** रिकरींग पेमेंट म्हणजे विशिष्ट कालावधीनंतर करावयाचे पेमेंट. हा कालावधी एक आठवडा, एक महिना, त्रैमासिक, सहामाही किंवा वार्षिक असू शकतो. उदा. वीज बील, विमा हप्ता इ.
- **Switch: (National Financial Switch) :** एका प्रोव्हायडर कडून दुसऱ्या प्रोव्हायडर कडे " स्वीच " तर्फे आर्थिक व्यवहार हस्तांतरित केले जातात.

- **TAT (Turn Around Time) टर्न अराऊंड टाईम** : एखादी विशिष्ट सेवा विशिष्ट मुदतीत पुरविण्याची दिलेली खात्री.(T + 2 days) चा अर्थ दोन दिवसांत कार्य पूर्ण व्हावे हा आहे.
- **Unified Payment Interface (UPI) :** डिजीटल व्यवहारांचा वापर वाढविण्यासाठी एनपीसीआयने यूपीआयची निर्मिती केली आहे. ग्राहकाने बँकेकडे यूपीआयसाठी नोंदणी केल्यानंतर एक विशिष्ट व्हर्च्युअल आयडी ग्राहकाला प्राप्त होतो जो ग्राहकाच्या मोबाईलला जोडलेला असतो. याद्वारे ग्राहक सहज एका क्लिकवर तात्काळ कोणलाही पैसे पाठवू शकतात. टू – फॅक्टर ऑथेन्टिकेशनच्या तत्त्वावर हे व्यवहार पार पडतात.
- **UTR (यूटीआर):** IMPS, NEFT, RTGS यांसारख्या माध्यमातून पैसे पाठविताना विशिष्ट व्यवहार ओळखण्याकरिता ज्या बँकेतून पैसे पाठविले जातात त्या बँकेतर्फे प्रत्येक व्यवहारासाठी ठरलेल्या स्वरूपात यूटीआर म्हणजेच युनिक ट्रान्जॅक्शन रेफरन्स क्रमांक दिला जातो.
- **वॉलेट:** वॉलेटमध्ये आपण पैसे ठेवू शकतो तसेच खरेदीसाठी वापरू शकतो. वॉलेट हे प्रत्यक्ष प्रीपेड कार्डच्या स्वरूपात तसेच पेटीएम, फोनपे यांसारख्या व्हर्च्युअल मोबाईल वॉलेट प्रकारात सुद्धा उपलब्ध होऊ शकते.

****

OFFICE OF RBI OMBUDSMAN (MUMBAI-II)
MAHARASHTRA AND GOA

Design by M Muralidhar, Anupam Sharma