भारतीय रिज़र्व बैंक

RESERVE BANK OF INDIA

షయ సూచిక

క్రమ సంఖ్య	విషయం	పుట సంఖ్య
	ముందుమాట	
	<u>పార్ట్ ఎ - కార్యనిర్వహణ విధానం మరియు మోసపూరిత లావాదేవీలకు వ్యతిరేకంగా తీసుకోవలసిన జాగ్రత్తలు - బ్యాంకులు</u>	
1	ఫిషింగ్ లింక్‌లు	
2	విషింగ్ కాల్స్	
3	ఆన్‌లైన్ సేల్స్ ప్లాట్‌ఫారమ్‌లను ఉపయోగించి చేసే మోసాలు	
4	తెలియని / ధృవీకరించబడని మొబైల్ యాప్‌లను ఉపయోగించడం వల్ల జరిగే మోసాలు	
5	ATM కార్డ్ స్కిమ్మింగ్	
6	స్క్రీన్ షేరింగ్ యాప్ / రిమోట్ యాక్సెస్ ఉపయోగించి చేసే మోసాలు	
7	సిమ్ స్వాప్ / సిమ్ క్లోనింగ్	
8	శోధన ఇంజిన్ల ద్వారా ఆధారాలను రాజీ చేయడం వల్ల జరిగే మోసాలు	
9	QR కోడ్ స్కాన్ ద్వారా జరిగే మోసాలు	
10	సోషల్ మీడియాలో ప్రతిరూపణ ద్వారా జరిగే మోసాలు	
11	జ్యూస్ జాకింగ్	
12	లాటరీ మోసాలు	
13	ఆన్‌లైన్ ఉద్యోగ మోసాలు	
14	మనీ మ్యూల్స్	

	పార్ట్ బి - కార్యనిర్వహణ విధానం మరియు మోసపూరిత లావాదేవీల నుండి తీసుకోవలసిన జాగ్రత్తలు - NBFCలు	
1	రుణాల మంజూరు కోసం నకిలీ ప్రకటనలు	
2	సంక్షిప్త సందేశ సేవ (SMS) / ఇమెయిల్ / తక్షణ సందేశం / కాల్ ద్వారా మోసాలు	
3	OTP ఆధారిత మోసాలు	
4	నకిలీ రుణ వెబ్‌సైట్‌లు / యాప్ మోసాలు	
5	మనీ సర్క్యులేషన్ / పోంజీ / మల్టీ-లెవల్ మార్కెటింగ్ (MLM) పథకం ద్వారా మోసాలు	
6	నకిలీ పత్రాలతో రుణాలు	
	పార్ట్ సి - ఆర్థిక లావాదేవీల కోసం తీసుకోవలసిన సాధారణ జాగ్రత్తలు	

ముందుమాట

ఇటీవలి సంవత్సరాలలో డిజిటల్ చెల్లింపు పద్ధతుల వినియోగంలో పెరుగుదల ఎక్కువగా ఉంది. కోవిడ్-19 ప్రేరిత లాక్‌డౌన్‌ల సమయంలో ఇది మరింత ఊపందుకుంది. వినియోగదారు సౌలభ్యాన్ని పెంపొందించడంతోపాటు, ఇది ఆర్థిక చేరిక యొక్క జాతీయ లక్ష్యాన్ని కూడా పెంచింది. అయితే, ఆర్థిక లావాదేవీలు చేయడంలో వేగం మరియు సౌలభ్యం మెరుగుపడినందున, చిల్లర (రిటైల్) ఆర్థిక లావాదేవీలలో నివేదించబడిన మోసాల సంఖ్య కూడా పెరిగింది. కష్టపడి సంపాదించిన డబ్బును సామాన్యులు మరియు మోసపూరిత వ్యక్తులను మోసం చేయడానికి, మోసగాళ్లు వినూత్న పద్ధతులను ఉపయోగిస్తున్నారు, ముఖ్యంగా సాంకేతిక-ఆర్థిక పర్యావరణ వ్యవస్థతో పూర్తిగా పరిచయం లేని డిజిటల్ ప్లాట్‌ఫారమ్‌ల వినియోగంలో కొత్తగా ప్రవేశించిన వారిపై.

ఈ చేతి పుస్తకం (బుక్‌లెట్) వివిధ మోసాల సంఘటనల నుండి మరియు ఆర్‌బిఐ అంబుడ్స్‌మెన్ కార్యాలయాలలో స్వీకరించబడిన ఫిర్యాదుల నుండి/ ఆధారంగా సంకలనం చేయబడింది, ప్రత్యేకించి డిజిటల్ మరియు ఎలక్ట్రానిక్ ఆర్థిక లావాదేవీలలో అనుభవం లేని వారికి లేదా అంత ఎక్కువగా అనుభవం లేని వారికి, విలువైన గరిష్ట ఆచరణాత్మక సమాచారాన్ని అందించడానికి. మోసం చేయడానికి మరియు తప్పుదారి పట్టించడానికి మోసగాళ్లు అవలంబించే కార్యనిర్వహణ పద్ధతి గురించి ప్రజలకు అవగాహన కల్పించడానికి ఉద్దేశించబడింది, అదే సమయంలో ఆర్థిక లావాదేవీలు నిర్వహించేటప్పుడు తీసుకోవలసిన జాగ్రత్తల గురించి కూడా వారికి తెలియజేయడానికి ఈ బుక్‌లెట్ ఉద్దేశించబడింది. ఇది ఒకరి వ్యక్తిగత సమాచారాన్ని, ప్రత్యేకించి ఆర్థిక సమాచారాన్ని ఎల్లప్పుడూ గోప్యంగా ఉంచడం, తెలియని కాల్‌లు / ఇమెయిల్‌లు / సందేశాల పట్ల జాగ్రత్త వహించడం, ఆర్థిక లావాదేవీలు నిర్వహించేటప్పుడు తగిన శ్రద్ధ వహించడం

మరియు సురక్షితమైన ఆధారాలు / పాస్‌వర్డ్‌లను ఎప్పటికప్పుడు మార్చడం వంటి అవసరాన్ని నొక్కి చెబుతుంది. అందుకే "తెలుసుకోండి / జాగ్రత్తగా వుండండి" (BE(A)WARE) అనే శీర్షిక పెట్టడం జరిగింది.

- తెలుసుకోండి మరియు జాగ్రత్తగా వుండండి!

వినియోగదారుల విద్య మరియు రక్షణ విభాగం, భారతీయ రిజర్వు బ్యాంకు ప్రజలకు అవగాహన కల్పించడంలో భాగంగా మరియు అంబుడ్స్‌మన్, ముంబై-II కార్యాలయం రూపొందించడం ద్వారా ఈ బుక్‌లెట్ రూపొందించబడింది.

కార్యనిర్వహణ విధానం మరియు మోసపూరిత లావాదేవీలకు వ్యతిరేకంగా తీసుకోవలసిన జాగ్రత్తలు – బ్యాంకులు

1. ఫిషింగ్ లింక్‌లు

కార్యనిర్వహణ విధానం

- మోసగాళ్లు థర్డ్-పార్టీ ఫిషింగ్ వెబ్‌సైట్‌ను సృష్టిస్తారు, ఇది ఇప్పటికే ఉన్న అసలైన వెబ్‌సైట్ గా కనిపిస్తుంది. ఉదాహరణకు - ఒక బ్యాంక్ వెబ్‌సైట్ లేదా ఒక ఇ-కామర్స్ వెబ్‌సైట్ లేదా ఒక సెర్చ్ ఇంజన్ మొదలైనవి.

- ఈ వెబ్‌సైట్‌లకు లింక్‌లను మోసగాళ్లు సంక్షిప్త సందేశ సేవ (SMS) / సోషల్ మీడియా / ఇమెయిల్ / తక్షణ మెసెంజర్ మొదలైన వాటి ద్వారా పంపిస్తారు.

- చాలా మంది వినియోగదారులు వివరణాత్మక యూనిఫాం రిసోర్స్ లొకేటర్ (URL)ని తనిఖీ చేయకుండా లింక్‌పై క్లిక్ చేసి, వ్యక్తిగత గుర్తింపు సంఖ్య (పిన్/PIN), వన్ టైమ్ పాస్‌వర్డ్ (OTP), పాస్‌వర్డ్ మొదలైన సురక్షిత ఆధారాలను నమోదు చేసినప్పుడు, వీటిని మోసగాళ్లు ఉపయోగించి, మోసాలకు పాల్పడుతున్నారు.

ముందు జాగ్రత్తలు

- **తెలియని / ధృవీకరించని లింక్‌లపై క్లిక్ చేయవద్దు మరియు భవిష్యత్తులో పొరపాటున వాటిని ఉపయోగించకుండా ఉండటానికి, తెలియనివారు పంపిన SMS / ఇమెయిల్‌లను వెంటనే తొలగించండి.**
- **బ్యాంక్ / ఇ-కామర్స్ / సెర్చ్ ఇంజిన్ వెబ్‌సైట్‌కి లింక్‌లను అందించే మెయిల్‌లను అన్‌సబ్‌స్క్రైబ్ చేయండి మరియు అటువంటి ఇమెయిల్‌లను తొలగించే ముందు పంపినవారి ఇ-మెయిల్ IDని బ్లాక్ చేయండి.**
- **ఎల్లప్పుడూ మీ బ్యాంక్ / సర్వీస్ ప్రొవైడర్ అధికారిక వెబ్‌సైట్‌కి**

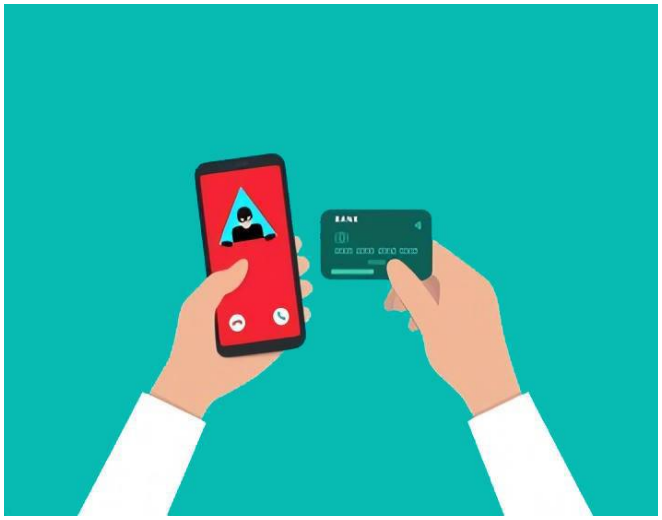
వెళ్లండి. ముఖ్యంగా ఆర్థిక ఆధారాలను నమోదు చేయాల్సిన వెబ్‌సైట్ వివరాలను జాగ్రత్తగా ధృవీకరించుకోండి. సురక్షిత ఆధారాలను నమోదు చేయడానికి ముందు వెబ్‌సైట్‌లో సురక్షిత గుర్తు (ప్యాడ్‌లాక్ చిహ్నంతో https) కోసం తనిఖీ చేయండి.

- **స్పెల్లింగ్ లోపాల కోసం ఇమెయిల్‌లలో వచ్చిన URLలు మరియు డొమైన్ పేర్లను తనిఖీ చేయండి. అనుమానం ఉంటే తెలియజేయండి.**

2. విషింగ్ కాల్స్

కార్యనిర్వహణ విధానం

- మోసగాళ్లు టెలిఫోన్ కాల్ / సోషల్ మీడియా ద్వారా బ్యాంకర్లు / కంపెనీ ఎగ్జిక్యూటివ్‌లు / ఇన్సూరెన్స్ ఏజెంట్లు / ప్రభుత్వ అధికారులు వారిమంటూ నమ్మబలికి వినియోగదారులకు కాల్ చేస్తారు లేదా సంప్రదిస్తారు. విశ్వాసం పొందడానికి, మోసగాళ్లు వినియోగదారు పేరు లేదా పుట్టిన తేదీ వంటి కొన్ని వినియోగదారు వివరాలను తెలియజేస్తారు.



- కొన్ని సందర్భాల్లో, అపరాధ రుసుము విధించకుండా ఆపడానికి, ఆకర్షణీయమైన తగ్గింపు మొదలైనవి తెలుపుతూ, పాస్‌వర్డ్‌లు / OTP / పిన్ / కార్డ్ వెరిఫికేషన్ సంఖ్య (CVV) మొదలైన రహస్య వివరాలను తెలుసుకోవడానికి/చెప్పమని మోసగాళ్లు ఒత్తిడి / మోసం చేస్తారు. ఈ

ఆధారాలు వినియోగదారులను మోసం చేయడానికి ఉపయోగించబడతాయి.

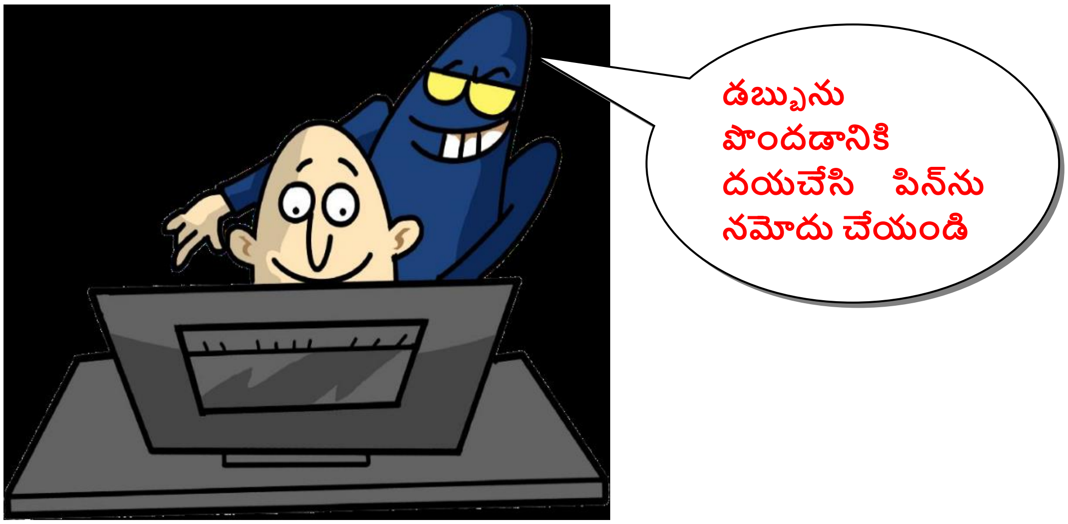
ముందు జాగ్రత్తలు

- **బ్యాంక్ అధికారులు / ఆర్థిక సంస్థలు / RBI / ఏదైనా నిజమైన సంస్థ, వినియోగదారు పేరు / పాస్‌వర్డ్ / కార్డ్ వివరాలు / CVV / OTP వంటి రహస్య సమాచారాన్ని పంచుకోమని ఎప్పుడూ అడగదు.**
- **ఈ రహస్య వివరాలను ఎవరితోనూ, మీ స్వంత కుటుంబ సభ్యులు మరియు స్నేహితులతో సహా, ఎప్పుడూ పంచుకోవద్దు.**

3. ఆన్‌లైన్ సేల్స్ ప్లాట్‌ఫారమ్‌లను ఉపయోగించి చేసే మోసాలు

కార్యనిర్వహణ విధానం

- ఆన్‌లైన్ విక్రయ ప్లాట్‌ఫారమ్‌లలో కొనుగోలుదారులుగా మోసగాళ్లు నటిస్తారు మరియు విక్రేత యొక్క ఉత్పత్తి/ల పట్ల ఆసక్తిని చూపుతారు. చాలా మంది మోసగాళ్లు తమ విశ్వాసాన్ని పొందడానికి రిమోట్ లొకేషన్స్‌లో రక్షణ (డిఫెన్స్) సిబ్బందిగా నటిస్తారు.
- విక్రేతకు డబ్బు చెల్లించే బదులు, వారు యూనిఫైడ్ పేమెంట్స్ ఇంటర్‌ఫేస్ (UPI) యాప్ ద్వారా "మనీ అభ్యర్థించండి" ఎంపికను ఉపయోగిస్తారు మరియు UPI PINని నమోదు చేయడం ద్వారా విక్రేత అభ్యర్థనను ఆమోదించాలని పట్టుబట్టారు. విక్రేత పిన్‌ను నమోదు చేసిన తర్వాత, మోసగాడి ఖాతాకు డబ్బు బదిలీ చేయబడుతుంది.



మ◌ు◌ందు జాగ్రత్తలు

- **మీరు ఆన్‌లైన్ సేల్స్ ప్లాట్‌ఫారమ్‌లను ఉపయోగించి ఉత్పత్తులను కొనుగోలు చేస్తున్నప్పుడు లేదా విక్రయిస్తున్నప్పుడు ఎల్లప్పుడూ జాగ్రత్తగా ఉండండి.**
- **డబ్బు అందుకోవడానికి ఎక్కడా పిన్ / పాస్‌వర్డ్‌ను నమోదు చేయాల్సిన అవసరం లేదని ఎల్లప్పుడూ గుర్తుంచుకోండి**
- **లావాదేవీని పూర్తి చేయడానికి UPI లేదా ఏదైనా ఇతర యాప్ లలో మీరు పిన్‌ను నమోదు చేయవలసి వస్తే, మీరు దాన్ని డబ్బును స్వీకరించడానికి బదులుగా పంపుతున్నారని అర్థం.**

4. తెలియని / ధృవీకరించని మొబైల్ యాప్‌ల వినియోగం వల్ల జరిగే మోసాలు

కార్యనిర్వహణ విధానం

- మోసగాళ్లు SMS / ఇమెయిల్ / సోషల్ మీడియా / ఇన్‌స్టంట్ మెసెంజర్ మొదలైన వాటి ద్వారా సర్క్యులేట్ చేస్తారు, నిర్దిష్ట యాప్ లింక్‌లు, ఇప్పటికే ఉన్న అధీకృత సంస్థల యాప్‌ల మాదిరిగానే కనిపించేలా మాస్క్‌లు వేస్తారు.
- మోసగాళ్లు వినియోగదారుల యొక్క మొబైల్ / ల్యాప్‌టాప్ / డెస్క్‌టాప్ మొదలైన వాటిలో తెలియని / ధృవీకరించని అనువర్తనాలను డౌన్‌లోడ్ చేయడానికి దారితీసే అటువంటి లింక్‌లపై క్లిక్ చేయడానికి వినియోగదారులను మాయ చేస్తారు.
- హానికరమైన అప్లికేషన్ డౌన్‌లోడ్ అయిన తర్వాత, మోసగాడు వినియోగదారు పరికరానికి పూర్తి యాక్సెస్‌ను పొందుతాడు. వీటిలో పరికరంలో నిల్వ చేయబడిన రహస్య వివరాలు మరియు అటువంటి యాప్‌లను ఇన్‌స్టాల్ చేయడానికి ముందు / తర్వాత స్వీకరించిన

సందేశాలు / OTPలు ఉంటాయి.

ముందు జాగ్రత్తలు

- **ఏదైనా ధృవీకరించబడని/తెలియని మూలాధారాల నుండి లేదా తెలియని వ్యక్తి అడిగినప్పుడు/మార్గనిర్దేశం చేయబడినప్పుడు అప్లికేషన్‌ను ఎప్పుడూ డౌన్‌లోడ్ చేయవద్దు.**
- **డౌన్‌లోడ్ చేయడానికి ముందు వివేకవంతమైన అభ్యాసంగా, డౌన్‌లోడ్ చేయబడుతున్న యాప్ యొక్క ప్రచురణకర్తలు / యజమానులు అలాగే దాని వినియోగదారు రేటింగ్‌లు మొదలైనవాటిని తనిఖీ చేయండి.**
- **అప్లికేషన్‌ను డౌన్‌లోడ్ చేస్తున్నప్పుడు, అనుమతి/లు మరియు అది కోరుకునే పరిచయాలు, ఫోటోగ్రాఫ్‌లు మొదలైన మీ డేటాకు యాక్సెస్‌ని తనిఖీ చేయండి. కావలసిన అప్లికేషన్‌ను ఉపయోగించడానికి ఖచ్చితంగా అవసరమైన అనుమతులను మాత్రమే ఇవ్వండి.**

5. ATM కార్డ్ స్కిమ్మింగ్

కార్యనిర్వహణ విధానం

- మోసగాళ్లు ATM మెషీన్లలో స్కిమ్మింగ్ పరికరాలను ఉంచుతారు మరియు వినియోగదారు కార్డ్ నుండి డేటాను దొంగిలిస్తారు.
- ATM పిన్‌ని క్యాప్చర్ చేయడానికి మోసగాళ్లు డమ్మీ కీప్యాడ్ లేదా చిన్న / పిన్‌హోల్ కెమెరాను కూడా ఉంచవచ్చు.
- కొన్నిసార్లు, మోసగాళ్లు ఇతర వినియోగదారులుగా నటిస్తూ, వినియోగదారు ATM మెషీన్‌లో పిన్‌ను నమోదు చేసినప్పుడు, సమీపంలోనే నిలబడి పిన్‌ను యాక్సెస్ చేస్తారు.
- ఈ డేటా డూప్లికేట్ కార్డ్‌ని సృష్టించడానికి మరియు వినియోగదారు ఖాతా నుండి డబ్బును ఉపసంహరించుకోవడానికి ఉపయోగించబడుతుంది.

ముందు జాగ్రత్తలు

- **లావాదేవీ చేయడానికి ముందు, కార్డ్ ఇన్సర్షన్ స్లాట్ లేదా ATM మెషీన్ కీప్యాడ్ దగ్గర అదనపు పరికరం ఏదీ జోడించబడలేదని ఎల్లప్పుడూ తనిఖీ చేయండి.**
- **పిన్‌ను నమోదు చేస్తున్నప్పుడు మీ మరో చేత్తో కీప్యాడ్‌ను కవర్ చేయండి.**
- **మీ ATM కార్డ్‌పై పిన్‌ను ఎప్పుడూ వ్రాయవద్దు.**
- **మీకు దగ్గరగా నిలబడి ఉన్న ఇతర / తెలియని వ్యక్తుల సమక్షంలో పిన్‌ను నమోదు చేయవద్దు.**
- **నగదు ఉపసంహరణ కోసం మీ ATM కార్డును ఎవరికీ ఇవ్వకండి.**

- **ఏ అపరిచిత వ్యక్తి ఇచ్చిన సూచనలను అనుసరించవద్దు లేదా ATMల వద్ద అపరిచితులు / తెలియని వ్యక్తుల నుండి సహాయం / మార్గదర్శకత్వం తీసుకోవద్దు.**
- **ATM వద్ద నగదు పంపిణీ చేయకపోతే, ATM నుండి బయలుదేరే ముందు 'రద్దు చేయి' బటన్‌ను నొక్కి, హోమ్ స్క్రీన్ కనిపించే వరకు వేచి ఉండండి.**

6. స్క్రీన్ షేరింగ్ యాప్ / రిమోట్ యాక్సెస్ ఉపయోగించి చేసే మోసాలు

కార్యనిర్వహణ విధానం

- మోసగాళ్లు స్క్రీన్ షేరింగ్ యాప్‌ను డౌన్‌లోడ్ చేయడానికి వినియోగదారును మాయ చేస్తారు.
- అటువంటి యాప్‌ని ఉపయోగించి, మోసగాళ్లు వినియోగదారు యొక్క మొబైల్ / ల్యాప్‌టాప్‌ను చూడవచ్చు / నియంత్రించవచ్చు మరియు వినియోగదారు యొక్క ఆర్థిక ఆధారాలకు ప్రాప్యతను పొందవచ్చు.

- నిధుల అనధికార బదిలీని నిర్వహించడానికి లేదా కస్టమర్ యొక్క ఇంటర్నెట్ బ్యాంకింగ్ / చెల్లింపు యాప్‌లను ఉపయోగించి చెల్లింపులు చేయడానికి మోసగాళ్లు ఈ సమాచారాన్ని ఉపయోగిస్తారు.

ముందు జాగ్రత్తలు

- **మీ పరికరం ఏదైనా సాంకేతిక లోపాన్ని ఎదుర్కొంటే మరియు మీరు**

ఏదైనా స్క్రీన్ షేరింగ్ యాప్‌ని డౌన్‌లోడ్ చేయాల్సి ఉంటే, మీ పరికరం నుండి అన్ని చెల్లింపు సంబంధిత యాప్‌లను నిష్క్రియం చేయండి / లాగ్ అవుట్ చేయండి.

- **కంపెనీ అధికారిక వెబ్‌సైట్‌లో కనిపించే అధికారిక టోల్-ఫ్రీ నంబర్ ద్వారా మీకు సలహా ఇచ్చినప్పుడు మాత్రమే అటువంటి యాప్‌లను డౌన్‌లోడ్ చేసుకోండి. కంపెనీ అధికారి తన వ్యక్తిగత సంప్రదింపు నంబర్ ద్వారా మిమ్మల్ని సంప్రదిస్తే అటువంటి యాప్‌లను డౌన్‌లోడ్ చేయవద్దు.**
- **పని పూర్తయిన వెంటనే, మీ పరికరం నుండి స్క్రీన్ షేరింగ్ యాప్ తీసివేయబడిందని నిర్ధారించుకోండి.**

7. సిమ్ స్వాప్ / సిమ్ క్లోనింగ్

కార్యనిర్వహణ విధానం

- వినియోగదారు యొక్క బ్యాంక్ ఖాతాకు అనుసంధానించబడిన రిజిస్టర్డ్ మొబైల్ నంబర్ కోసం, మోసగాళ్లు వినియోగదారు సబ్‌స్క్రయిబర్ ఐడెంటిటీ మాడ్యూల్ (సిమ్) కార్డ్‌కి (ఎలక్ట్రానిక్-సిమ్‌తో సహా) యాక్సెస్ పొందుతారు లేదా నకిలీ సిమ్ కార్డ్‌ని పొందవచ్చు

- మోసగాళ్లు అనధికారిక లావాదేవీలను నిర్వహించడానికి అటువంటి డూప్లికేట్ సిమ్‌పై వచ్చిన OTPని ఉపయోగిస్తారు.
- మోసగాళ్లు సాధారణంగా టెలిఫోన్/మొబైల్ నెట్‌వర్క్ సిబ్బందిగా నటిస్తూ వినియోగదారు నుండి వ్యక్తిగత/గుర్తింపు వివరాలను సేకరిస్తారు మరియు 3G నుండి 4Gకి ఉచితంగా SIM కార్డ్‌ని

అప్‌గ్రేడ్ చేయడం లేదా SIM కార్డ్‌పై అదనపు ప్రయోజనాలను అందించడం వంటి ఆఫర్ల పేరుతో వినియోగదారు వివరాలను అభ్యర్థిస్తారు.

మ౦ు౦ందు జాగ్రత్తలు

- **మీ SIM కార్డ్‌కు సంబంధించిన గుర్తింపు ఆధారాలను ఎప్పుడూ ఎవరితోనూ పంచుకోవద్దు.**
- **మీ ఫోన్‌లో మొబైల్ నెట్‌వర్క్ యాక్సెస్ విషయంలో జాగ్రత్తగా ఉండండి. సాధారణంగా ఎక్కువ సమయం పాటు మీ ఫోన్‌లో మొబైల్ నెట్‌వర్క్ లేకపోతే, మీ మొబైల్ నంబర్‌కు డూప్లికేట్ సిమ్ ఏదీ ఇవ్వబడలేదని / జారీ చేయబడలేదని నిర్ధారించుకోవడానికి వెంటనే మొబైల్ ఆపరేటర్ని సంప్రదించండి.**

8. శోధన ఇంజిన్‌ల ఫలితాలపై ఆధారాలను రాజీ చేయడం ద్వారా మోసాలు

కార్యనిర్వహణ విధానం

- వినియోగదారులు వారి బ్యాంక్, బీమా కంపెనీ, ఆధార్ అప్‌డేషన్ సెంటర్ మొదలైన వాటి యొక్క సంప్రదింపు వివరాలు / కస్టమర్ కేర్ నంబర్‌లను పొందేందుకు శోధన ఇంజిన్‌లను ఉపయోగిస్తారు. శోధన ఇంజిన్‌లలోని ఈ సంప్రదింపు వివరాలు తరచుగా సంబంధిత సంస్థకు చెందినవి కావు కానీ మోసగాళ్లచే అలా కనిపించేలా చేయబడతాయి.
- శ్ోధన ఇంజన్‌లో బ్యాంక్/కంపెనీ కాంటాక్ట్ నంబర్‌లుగా ప్రదర్శించబడే మోసగాళ్లకు సంబంధించిన తెలియని/ధృవీకరించబడని సంప్రదింపు నంబర్‌లను వినియోగదారులు

సంప్రదించడం జరగవచ్చు.

- కస్టమర్‌లు ఈ సంప్రదింపు నంబర్‌లకు కాల్ చేసిన తర్వాత, ధృవీకరణ కోసం వారి కార్డ్ ఆధారాలు / వివరాలను పంచుకోమని మోసగాళ్లు వినియోగదారులను అడుగుతారు.
- మోసగాడు RE యొక్క నిజమైన ప్రతినిధిగా భావించి, వినియోగదారులు వారి సురక్షిత వివరాలను పంచుకుంటారు మరియు తద్వారా మోసాలకు బలైపోతారు.

ముందు జాగ్రత్తలు

- **ఎల్లప్పుడూ బ్యాంకులు / కంపెనీల అధికారిక వెబ్‌సైట్‌ల నుండి కస్టమర్ కేర్ సంప్రదింపు వివరాలను పొందండి.**
- **శోధన ఇంజిన్ ఫలితాల పేజీలో నేరుగా ప్రదర్శించబడే నంబర్‌లకు కాల్ చేయవద్దు, ఎందుకంటే ఇవి తరచుగా మోసగాళ్లచే మభ్యపెట్టబడతాయి.**
- **కస్టమర్ కేర్ నంబర్‌లు ఎప్పుడూ మొబైల్ నంబర్‌ల రూపంలో ఉండవని దయచేసి గమనించండి.**

9. QR కోడ్ స్కాన్ పద్ధతి ద్వారా మోసం

కార్యనిర్వహణ విధానం

- మోసగాళ్లు తరచూ వివిధ సాకులతో వినియోగదారులను సంప్రదిస్తారు మరియు వినియోగదారు ఫోన్‌లోని యాప్‌లను ఉపయోగించి క్విక్ రెస్పాన్స్ (QR) కోడ్‌లను స్కాన్ చేయడానికి వారిని మోసం చేస్తారు.
- అటువంటి QR కోడ్‌లను స్కాన్ చేయడం ద్వారా, వినియోగదారులు తమ ఖాతా నుండి డబ్బును విత్‌డ్రా

చేసుకునేందుకు మోసగాళ్లకు తెలియకుండానే అధికారం ఇచ్చే అవకాశం వుంది.

మ◌ు◌ందు జాగ్రత్తలు

- **ఏదైనా చెల్లింపు యాప్‌ని ఉపయోగించి QR కోడ్/లను స్కాన్ చేస్తున్నప్పుడు జాగ్రత్తగా ఉండండి. QR కోడ్‌లలో నిర్దిష్ట ఖాతాకు డబ్బును బదిలీ చేయడానికి ఖాతా వివరాలను పొందుపరిచారు.**
- **డబ్బును స్వీకరించడానికి ఏ QR కోడ్‌ను ఎప్పుడూ స్కాన్ చేయవద్దు. డబ్బు రసీదుతో కూడిన లావాదేవీలకు బార్‌కోడ్‌లు / QR కోడ్‌లను స్కాన్ చేయడం లేదా మొబైల్ బ్యాంకింగ్ PIN (m-PIN), పాస్‌వర్డ్‌లు మొదలైనవాటిని నమోదు చేయడం అవసరం లేదు.**

10. సోషల్ మీడియాలో ప్రతిరూపణ

కార్యనిర్వహణ విధానం

- సోషల్ మీడియా ప్లాట్‌ఫారమ్‌లు- Facebook, Instagram, Twitter మొదలైన వాటినుండి వినియోగదారుల వివరాలను ఉపయోగించి మోసగాళ్లు నకిలీ ఖాతాలను సృష్టిస్తారు.
- తక్షణ వైద్య అవసరాలు, చెల్లింపులు మొదలైన వాటి డబ్బు కోసం వినియోగదారుల స్నేహితులకు మోసగాళ్లు అభ్యర్థనను పంపుతారు.

- నకిలీ వివరాలను ఉపయోగించి, వినియోగదారుల

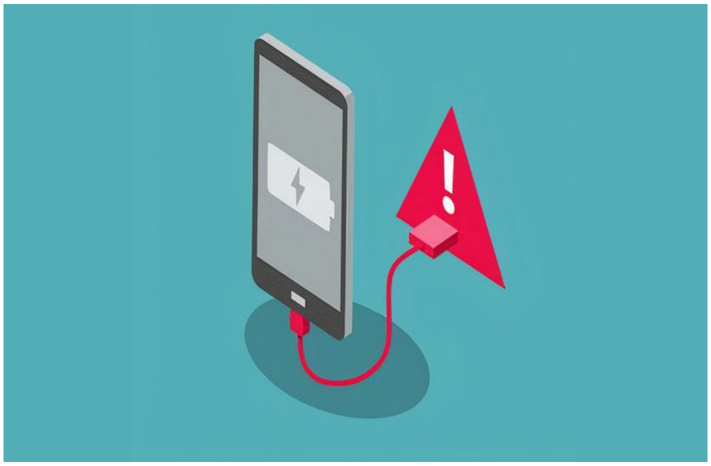
ను కూడా సంప్రదించి, కొంత కాల వ్యవధిలో మోసగాళ్లు వినియోగదారుల విశ్వాసాన్ని పొందుతారు. వినియోగదారులు వారి వ్యక్తిగత లేదా ప్రైవేట్ సమాచారాన్ని పంచుకున్నప్పుడు, మోసగాళ్ళు వినియోగదారుల నుండి డబ్బును బ్లాక్ మెయిల్ చేయడానికి లేదా దోపిడీ చేయడానికి అటువంటి సమాచారాన్ని ఉపయోగిస్తారు.

ముందు జాగ్రత్తలు

- **ప్రొఫైల్ వలె నటించలేదని నిర్ధారించుకోవడానికి ఫోన్ కాల్ / భౌతిక సమావేశం ద్వారా ధృవీకరించడం ద్వారా స్నేహితుడు / బంధువు నుండి ఫండ్ అభ్యర్థన యొక్క వాస్తవికతను ఎల్లప్పుడూ ధృవీకరించండి.**
- **ఆన్‌లైన్‌లో తెలియని వ్యక్తులకు చెల్లింపులు చేయవద్దు.**
- **సోషల్ మీడియా ప్లాట్‌ఫారమ్‌లలో వ్యక్తిగత మరియు రహస్య సమాచారాన్ని పంచుకోవద్దు.**

11. జ్యూస్ జాకింగ్

కార్యనిర్వహణ విధానం



- మొబైల్ యొక్క ఛార్జింగ్ పోర్ట్, ఫైల్‌లు / డేటాను బదిలీ చేయడానికి కూడా ఉపయోగించవచ్చు.
- మోసగాళ్లు అక్కడ కనెక్ట్ చేయబడిన కస్టమర్ ఫోన్‌లకు మాల్వేర్‌ను ఛార్జింగ్ పోర్ట్‌లను ఇన్‌స్టాల్ చేయడానికి ఉపయోగిస్తారు మరియు కస్టమర్ల మొబైల్ ఫోన్‌ల నుండి ఇమెయిల్‌లు, SMS, సేవ్ చేసిన పాస్‌వర్డ్‌లు మొదలైన డేటా సెన్సిటివ్ డేటాను కంట్రోల్ / యాక్సెస్ / దొంగిలిస్తారు (జ్యూస్ జాకింగ్).

ముందు జాగ్రత్త

- **పబ్లిక్ / తెలియని ఛార్జింగ్ పోర్ట్‌లు / కేబుల్‌లను ఉపయోగించడం మానుకోండి.**

12. లాటరీ మోసం

కార్యనిర్వహణ విధానం

- భారీ లాటరీని వినియోగదారు గెలుచుకున్నట్లు మోసగాళ్లు ఇమెయిల్‌లు పంపుతారు లేదా ఫోన్ కాల్‌లు చేస్తారు. ఇంకా, డబ్బును స్వీకరించడానికి మోసగాళ్లు స్వాధీనం చేసుకున్న వెబ్‌సైట్‌లో, తమ బ్యాంక్ ఖాతా / క్రెడిట్ కార్డ్ వివరాలను నమోదు చేయడం ద్వారా వారి గుర్తింపును నిర్ధారించమని అడుగుతారు. వినియోగదారులను

- లాటరీ / వస్తువుల కోసం పన్నులు/ఫారెక్స్ ఛార్జీలు/ముందుగానే చెల్లించమని లేదా షిప్పింగ్ ఛార్జీలు, ప్రాసెసింగ్ / హ్యాండ్లింగ్ రుసుము మొదలైనవాటిని చెల్లించమని వినియోగదారులను మోసగాళ్లు అడుగుతారు.
- కొన్ని సందర్భాల్లో మోసగాళ్లు, RBI లేదా ఒక విదేశీ బ్యాంక్/కంపెనీ/అంతర్జాతీయ ఆర్థిక సంస్థకు ప్రతినిధిగా కూడా పోజులివ్వవచ్చు మరియు ఆ సంస్థ నుండి విదేశీ కరెన్సీలో పెద్ద మొత్తాన్ని స్వీకరించడానికి సాపేక్షంగా చిన్న మొత్తాన్ని బదిలీ చేయమని వినియోగదారులను అడగవచ్చు.

- అభ్యర్థించిన డబ్బు సాధారణంగా వాగ్దానం చేసిన లాటరీ/బహుమతిలో చాలా తక్కువ శాతం కాబట్టి, మోసగాడి ఉచ్చులో పడి వినియోగదారు చెల్లింపు చేయవచ్చు.

ముందు జాగ్రత్తలు

- **అటువంటి నమ్మశక్యం కాని లాటరీ లేదా ఆఫర్‌ల పట్ల జాగ్రత్త వహించండి - ఎవరూ ఉచితంగా డబ్బు ఇవ్వరు, ప్రత్యేకించి ఇంత పెద్ద మొత్తంలో డబ్బు.**
- **ఏదైనా లాటరీ కాల్‌లు / ఇమెయిల్‌లకు ప్రతిస్పందనగా చెల్లింపులు చేయవద్దు లేదా సురక్షిత ఆధారాలను పంచుకోవద్దు.**
- **ఆర్‌బిఐ ఎప్పుడూ ప్రజా సభ్యుల ఖాతాలను తెరవదు లేదా వారి నుండి డిపాజిట్లు తీసుకోదు. ఇలాంటి సందేశాలు మోసపూరితమైనవి.**
- **ప్రజల సభ్యుల వ్యక్తిగత/బ్యాంకు వివరాలను RBI ఎప్పుడూ అడగదు. నకిలీ RBI లోగోలు మరియు సందేశాల పట్ల జాగ్రత్త వహించండి.**
- **బ్యాంకులు, సంస్థలు మొదలైన వాటి నుండి ప్రైజ్ మనీని స్వీకరించడానికి ప్రైజ్ మనీ, ప్రభుత్వ సహాయం మరియు నో యువర్ కస్టమర్ (KYC) అప్‌డేషన్‌ను అందించే/వాగ్దానం చేసే సందేశాలకు ఎప్పుడూ ప్రతిస్పందించవద్దు.**

13. ఆన్‌లైన్ ఉద్యోగ మోసం

కార్యనిర్వహణ విధానం

- మోసగాళ్లు నకిలీ ఉద్యోగ శోధన వెబ్‌సైట్‌లను సృష్టిస్తారు మరియు ఉద్యోగార్థులు తమ బ్యాంక్ ఖాతా / క్రెడిట్ కార్డ్ / డెబిట్ కార్డ్ యొక్క సురక్షిత ఆధారాలను రిజిస్ట్రేషన్ సమయంలో ఈ వెబ్‌సైట్లలో షేర్ చేసినప్పుడు, వారి ఖాతాలు రాజీపడతాయి.

- మోసగాళ్లు కూడా ప్రముఖ కంపెనీ(ల) అధికారులుగా నటిస్తారు మరియు నకిలీ ఇంటర్వ్యూలు నిర్వహించి ఉపాధిని అందిస్తామంటారు. రిజిస్ట్రేషన్, తప్పనిసరి శిక్షణ కార్యక్రమం, ల్యాప్‌టాప్ మొదలైనవాటి కోసం ఉద్యోగార్థులు నిధులను బదిలీ చేయడానికి ప్రేరేపించబడతారు.

ముందు జాగ్రత్తలు

- **విదేశీ సంస్థలతో సహా ఏదైనా ఉద్యోగ ఆఫర్ కోసం, ముందుగా ఉద్యోగం చేస్తున్న కంపెనీ/దాని ప్రతినిధి యొక్క గుర్తింపు మరియు సంప్రదింపు వివరాలను నిర్ధారించుకోండి.**
- **ఉద్యోగాన్ని అందించే నిజమైన కంపెనీ ఎప్పుడూ ఉద్యోగం కోసం డబ్బు అడగదని గుర్తుంచుకోండి.**
- **తెలియని ఉద్యోగ శోధన వెబ్‌సైట్లలో చెల్లింపులు చేయవద్దు.**

14. మనీ మ్యూల్స్

కార్యనిర్వహణ విధానం

- మనీ మ్యూల్ అనేది మోసగాళ్లచే అమాయక బాధితుల బ్యాంక్ ఖాతా/ల ద్వారా దొంగిలించబడిన / అక్రమ డబ్బును లాండరింగ్ చేయడానికి మోసగించబడిన విధానాన్ని వివరించే పదం.
- మోసగాళ్లు ఇమెయిల్‌లు, సోషల్ మీడియా మొదలైనవాటి ద్వారా వినియోగదారులను సంప్రదిస్తారు మరియు ఆకర్షణీయమైన కమీషన్‌లకు బదులుగా వారి బ్యాంక్ ఖాతాలకు డబ్బును స్వీకరించేలా

వారిని (మనీ మ్యూల్) ఒప్పిస్తారు.

- మనీ మ్యూల్ మరొక మనీ మ్యూల్ ఖాతాకు డబ్బును బదిలీ చేయమని నిర్దేశించబడుతుంది, ఒక గొలుసును ప్రారంభించడం ద్వారా చివరికి డబ్బు మోసగాడి ఖాతాకు బదిలీ చేయబడుతుంది.

- ప్రత్యామ్నాయంగా, మోసగాడు నగదును విత్‌డ్రా చేసి ఎవరికైనా అందజేయమని ఆదేశించవచ్చు మ్యూల్ని
- అటువంటి మోసాలు నివేదించబడినప్పుడు, మనీ లాండరింగ్ కోసం మనీ మ్యూల్ పోలీసుల విచారణ లక్ష్యంగా మారుతుంది.

ముందు జాగ్రత్తలు

- **రుసుము / చెల్లింపు కోసం డబ్బును స్వీకరించడానికి లేదా బదిలీ చేయడానికి మీ ఖాతాను ఉపయోగించడానికి ఇతరులను అనుమతించవద్దు.**
- **మీ బ్యాంక్ ఖాతా వివరాలను అడిగే ఇమెయిల్‌లకు ప్రతిస్పందించవద్దు.**
- **ఆకర్షణీయమైన ఆఫర్‌లు / కమీషన్‌ల ద్వారా మోసపోకండి మరియు అనధికారిక డబ్బును స్వీకరించడానికి మరియు వాటిని ఇతరులకు బదిలీ చేయడానికి లేదా నగదును విత్‌డ్రా చేసుకోవడానికి మరియు భారీ రుసుము ఆశతో ఇవ్వడానికి సమ్మతి ఇవ్వకండి.**
- **నిధుల మూలం అసలైనది కానట్లయితే, లేదా అంతర్లీన లావాదేవీకి సంబంధించిన హేతుబద్ధత అధికారులకు రుజువు**

కాకపోతే, డబ్బును స్వీకరించే వ్యక్తి పోలీసు మరియు ఇతర చట్ట అమలు సంస్థలతో తీవ్ర ఇబ్బందులకు గురయ్యే అవకాశం ఉంది.

కార్యనిర్వహణ విధానం మరియు మోసపూరిత లావాదేవీలకు వ్యతిరేకంగా తీసుకోవలసిన జాగ్రత్తలు – బ్యాంకింగేతర ఆర్థిక సంస్థలు (NBFCలు)

1. రుణాలు పొడిగించేందుకు మోసగాళ్ల ద్వారా నకిలీ ప్రకటనలు

కార్యనిర్వహణ విధానం

- చాలా ఆకర్షణీయమైన మరియు తక్కువ వడ్డీ రేట్లు లేదా సులభంగా తిరిగి చెల్లించే ఎంపికలు లేదా కొలేటరల్/సెక్యూరిటీ మొదలైన వాటి అవసరం లేకుండా వ్యక్తిగత రుణాలను అందిస్తామంటూ మోసగాళ్లు నకిలీ ప్రకటనలను జారీ చేస్తారు.

- మోసగాళ్లు అటువంటి ఆఫర్‌లతో ఇమెయిల్‌లను పంపుతారు మరియు రుణగ్రహీతలను సంప్రదించమని అడుగుతారు.

  మోసపూరిత రుణగ్రహీతలతో విశ్వసనీయతను పొందడానికి మరియు విశ్వాసం కలిగించడానికి, ఈ ఇమెయిల్-ఐడిలు ప్రసిద్ధ / నిజమైన నాన్-బ్యాంకింగ్ ఫైనాన్షియల్ కంపెనీల (NBFCలు) యొక్క వరిష్ఠ అధికారుల ఇమెయిల్‌ల IDల వలె కనిపించేలా తయారు చేయబడతాయి.

- రుణగ్రహీతలు రుణాల కోసం మోసగాళ్లను సంప్రదించినప్పుడు, మోసగాళ్లు ప్రాసెసింగ్ ఫీజులు, వస్తువులు మరియు సేవల పన్ను (GST), ఇంటర్‌సిటీ ఛార్జీలు, అడ్వాన్స్ ఈక్వేటెడ్ మంత్లీ ఇన్‌స్టాల్‌మెంట్ (EMI) మొదలైన వివిధ ముందస్తు ఛార్జీల పేరుతో రుణగ్రహీతల నుండి డబ్బు తీసుకుంటారు. రుణాలు ఇవ్వకుండా పరారీ అవుతారు.

- మోసగాళ్లు నకిలీ వెబ్‌సైట్ లింక్‌లను కూడా సృష్టిస్తారు. వ్యక్తులు రుణాలపై సమాచారం కోసం శోధించినప్పుడు శోధన ఇంజిన్‌లలో అవి చూపబడేలా.

ముందు జాగ్రత్తలు

- **ఎన్‌బిఎఫ్‌సిలు/బ్యాంకులు వసూలు చేసే లోన్ ప్రాసెసింగ్ రుసుము, మంజూరైన లోన్ మొత్తం నుండి తీసివేయబడుతుంది మరియు రుణగ్రహీత నుండి నగదు రూపంలో ముందస్తుగా డిమాండ్ చేయబడదు.**
- **ఎన్‌బిఎఫ్‌సిలు/బ్యాంకులు రుణ దరఖాస్తు ప్రాసెసింగ్‌కు ముందు, ముందస్తు రుసుమును ఎన్నటికీ అడగవు కాబట్టి ఎటువంటి ప్రాసెసింగ్ రుసుమును ముందుగానే చెల్లించవద్దు.**
- **వాస్తవ మూలాధారాల ద్వారా వివరాలను తనిఖీ చేయకుండా/ధృవీకరించకుండా, తక్కువ వడ్డీ రేట్లు, మొదలైన ఆన్‌లైన్ ఆఫర్‌కు వ్యతిరేకంగా చెల్లింపులు చేయవద్దు లేదా సురక్షిత ఆధారాలను నమోదు చేయవద్దు.**

2. SMS / ఇమెయిల్ / తక్షణ సందేశం / కాల్ స్కామ్‌లు

కార్యనిర్వహణ విధానం

- ఆకర్షణీయమైన రుణాలపై తక్షణ సందేశ యాప్‌లు / SMS / సోషల్ మీడియా ప్లాట్‌ఫారమ్‌లలో మోసగాళ్లు నకిలీ సందేశాలను ప్రసారం చేస్తారు మరియు వారు షేర్ చేసిన మొబైల్ నంబర్‌లో ఏదైనా తెలిసిన NBFC యొక్క లోగోను ప్రొఫైల్ చిత్రంగా విశ్వసనీయతను ప్రేరేపించడానికి ఉపయోగిస్తారు.

- మోసగాళ్లు వారి ఆధార్ కార్డ్ / పాన్ కార్డ్ మరియు నకిలీ NBFC ID కార్డును కూడా పంచుకోవచ్చు.
- అటువంటి బల్క్ సందేశాలు / SMS / ఇమెయిల్‌లు పంపిన తర్వాత, మోసగాళ్ళు యాదృచ్ఛిక

వ్యక్తులకు కాల్ చేసి, నకిలీ మంజూరు లేఖలు, నకిలీ చెక్కుల కాపీలు మొదలైనవాటిని పంచుకుంటారు మరియు వివిధ ఛార్జీలు డిమాండ్ చేస్తారు. ఒకసారి రుణగ్రహీతలు వీటిని చెల్లించిన తరువాత, మోసగాళ్లు డబ్బుతో పరారీ అవుతారు.

ముందు జాగ్రత్తలు

- **టెలిఫోన్‌లు / ఇమెయిల్‌లు మొదలైనవాటి ద్వారా వ్యక్తులు సొంతంగా చేసే రుణ ఆఫర్‌లను ఎప్పుడూ నమ్మవద్దు.**
- **అటువంటి ఆఫర్‌లకు వ్యతిరేకంగా ఎటువంటి చెల్లింపులు చేయవద్దు లేదా ఇతర మూలాధారాల ద్వారా ఇది నిజమైనదా అని నిర్ధారణ చేసుకోకుండా అటువంటి ఆఫర్‌లకు వ్యతిరేకంగా ఏదైనా వ్యక్తిగత / ఆర్థిక ఆధారాలను భాగస్వామ్యం చేయవద్దు.**
- **SMS / ఇమెయిల్‌ల ద్వారా పంపబడిన లింక్‌లపై ఎప్పుడూ క్లిక్ చేయవద్దు లేదా ప్రచార SMS / ఇమెయిల్‌లకు ప్రత్యుత్తరం ఇవ్వకండి.**
- **అనుమానాస్పద అటాచ్‌మెంట్ లేదా ఫిషింగ్ లింక్‌లను కలిగి ఉన్న తెలియని మూలాల నుండి వచ్చే ఇమెయిల్‌లను ఎప్పుడూ తెరవవద్దు / ప్రతిస్పందించవద్దు.**

3. OTP ఆధారిత మోసాలు

కార్యనిర్వహణ విధానం

- మోసగాళ్లు NBFCల వలె నటించి, రుణాలు అందజేస్తామని SMS / సందేశాలు పంపడం లేదా NBFC/బ్యాంక్ కస్టమర్ల రుణ ఖాతాలపై క్రెడిట్ పరిమితిని

పెంచడం వంటి వాటితో వినియోగదారులను మొబైల్ నంబర్‌లో సంప్రదించమని అడుగుతారు.

- వినియోగదారులు అలాంటి నంబర్‌లకు కాల్ చేసినప్పుడు, మోసగాళ్లు వారి ఆర్థిక ఆధారాలను సేకరించేందుకు ఫారమ్‌లను నింపమని అడుగుతారు. మోసగాళ్లు OTP లేదా PIN వివరాలను పంచుకోవడానికి మరియు కస్టమర్ల ఖాతాల నుండి అనధికారిక బదిలీలను నిర్వహించడానికి కస్టమర్‌లను ప్రేరేపిస్తారు / ఒప్పిస్తారు.

ముందు జాగ్రత్తలు

- **OTP / PIN / వ్యక్తిగత వివరాలు మొదలైనవాటిని మీ స్వంత స్నేహితులు మరియు కుటుంబ సభ్యులతో సహా ఎవరితోనూ ఏ రూపంలోనూ భాగస్వామ్యం చేయవద్దు.**
- **మీకు ముందస్తు సమాచారం లేకుండా OTP ఉత్పన్నం కాలేదని నిర్ధారించుకోవడానికి SMS / ఇమెయిల్‌లను క్రమం తప్పకుండా తనిఖీ చేయండి.**
- **ఎల్లప్పుడూ బ్యాంక్ / ఎన్‌బిఎఫ్‌సి / ఇ-వాలెట్ ప్రొవైడర్ యొక్క అధికారిక వెబ్‌సైట్‌ను యాక్సెస్ చేయండి లేదా వారి సేవలను పొందడానికి మరియు / లేదా వస్తువు మరియు సేవలకు సంబంధించిన సమాచారం మరియు వివరణలను పొందడానికి శాఖ ని సంప్రదించండి.**

4. నకిలీ రుణ వెబ్‌సైట్‌లు / యాప్ మోసాలు

కార్యనిర్వహణ విధానం

- తక్షణ మరియు స్వల్పకాలిక రుణాలను అందించే నిష్కపటమైన రుణ యాప్‌లను మోసగాళ్లు సృష్టిస్తారు. ఈ యాప్‌లు రుణగ్రహీతలను మోసం చేస్తాయి మరియు గణనీయంగా ఎక్కువ వడ్డీ

రేట్లను కూడా వసూలు చేస్తాయి.

- మోసపూరిత రుణగ్రహీతలను ఆకర్షించడానికి, మోసగాళ్ళు "పరిమిత కాలపు ఆఫర్లు" అని ప్రచారం చేస్తారు మరియు ఒత్తిడి వ్యూహాలను ఉపయోగించి అత్యవసర నిర్ణయాలు తీసుకోమని రుణగ్రహీతలను అడుగుతారు.

ముందు జాగ్రత్తలు

- **ప్రభుత్వం / రెగ్యులేటర్ / అధీకృత ఏజెన్సీలతో రుణదాత నమోదు చేయబడిందో లేదో ధృవీకరించుకోండి.**
- **భౌతిక చిరునామా లేదా సంప్రదింపు సమాచారాన్ని రుణదాత అందించారో లేదో తనిఖీ చేయండి, తర్వాత వారిని సంప్రదించడం కష్టం కాదు.**
- **క్రెడిట్ స్కోర్‌లను తనిఖీ చేయడం కంటే వ్యక్తిగత వివరాలను పొందడంలో రుణదాత ఎక్కువ ఆసక్తి చూపితే జాగ్రత్త వహించండి.**
- **ఏదైనా పేరున్న NBFC/బ్యాంక్ రుణ దరఖాస్తును ప్రాసెస్ చేసే ముందు చెల్లింపు కోసం అడగదని గుర్తుంచుకోండి.**
- **నిజమైన లోన్ ప్రొవైడర్లు రుణగ్రహీతల పత్రాలు మరియు ఇతర ఆధారాలను ధృవీకరించకుండా ఎప్పుడూ డబ్బును అందించరు.**
- **ఈ NBFC-ఆధారిత రుణ యాప్‌లు నిజమైనవో కాదో ధృవీకరించుకోండి.**

5. మనీ సర్క్యులేషన్ / పోంజీ / మల్టీ-లెవల్ మార్కెటింగ్ (MLM) పథకాల మోసం

కార్యనిర్వహణ విధానం

- మోసగాళ్లు MLM / చైన్ మార్కెటింగ్ / పిరమిడ్ స్ట్రక్చర్ స్కీమ్‌లను

ఉపయోగించి సభ్యుల నమోదు / జోడించిన తర్వాత సులభంగా లేదా త్వరగా డబ్బును వాగ్దానం చేస్తారు.

- ఈ పథకాలు అధిక రాబడికి హామీ ఇవ్వడమే కాకుండా మోసపూరిత వ్యక్తుల విశ్వాసాన్ని పొందడానికి మరియు నోటి ప్రచారం ద్వారా ఎక్కువ మంది పెట్టుబడిదారులను ఆకర్షించడానికి మొదటి కొన్ని వాయిదాలను (EMIలు) కూడా చెల్లిస్తాయి.
- ఈ పథకాలు గొలుసు/ సమూహానికి ఎక్కువ మంది వ్యక్తులను చేర్చడాన్ని ప్రోత్సహిస్తాయి. ఉత్పత్తుల విక్రయం కోసం కాకుండా పథకంలో చేరిన వ్యక్తుల సంఖ్య ఆధారంగా ఎన్‌రోలర్‌కు కమీషన్ చెల్లించబడుతుంది.
- పథకంలో చేరే వ్యక్తుల సంఖ్య తగ్గడం ప్రారంభించిన కొంత సమయం తర్వాత ఈ మోడల్ నిలకడగా ఉండదు. ఆ తర్వాత, మోసగాళ్లు పథకాన్ని మూసివేసి, అప్పటి వరకు ప్రజలు పెట్టుబడి పెట్టిన డబ్బుతో అదృశ్యమవుతారు.

ముందు జాగ్రత్తలు

- **రిటర్న్‌లు రిస్క్‌లకు అనులోమానుపాతంలో ఉంటాయి. రిటర్న్ ఎక్కువగా ఉంటే గా , రిస్క్ కూడా ఎక్కువగా ఉంటుంది.**
- **ఏదైనా పథకం అసాధారణంగా అధిక రాబడిని (40-50%p.a) నిలకడగా అందిస్తే, సంభావ్య మోసానికి మొదటి సంకేతం కావచ్చు మరియు జాగ్రత్త అవసరం.**
- **వస్తువులు/సేవ యొక్క అసలు విక్రయం లేకుండా ఏదైనా చెల్లింపు**

/ కమీషన్ / బోనస్ / లాభం శాతం అనుమానాస్పదంగా మరియు మోసానికి దారితీయవచ్చని ఎల్లప్పుడూ గమనించండి.

- మల్టీ-లెవల్ మార్కెటింగ్ / చైన్ మార్కెటింగ్ / పిరమిడ్ స్ట్రక్చర్ పథకాలను అమలు చేస్తున్న సంస్థలు అందించే అధిక రాబడుల వాగ్దానాలతో ప్రలోభాలకు గురికావద్దు.
- మనీ సర్క్యులేషన్ / మల్టీ-లెవల్ మార్కెటింగ్ / పిరమిడ్ నిర్మాణాల క్రింద డబ్బును అంగీకరించడం అనేది ప్రైజ్ చిట్స్ మరియు మనీ సర్క్యులేషన్ పథకాల (నిషేధింపు) చట్టం, 1978 ప్రకారం గుర్తించదగిన నేరం.
- అటువంటి ఆఫర్లు లేదా అటువంటి పథకాల సమాచారం విషయంలో, వెంటనే రాష్ట్ర పోలీసులకు ఫిర్యాదు చేయాలి.

6. నకిలీ పత్రాలతో మోసపూరిత రుణాలు

కార్యనిర్వహణ విధానం

- ఆర్థిక సంస్థల నుండి సేవలను పొందేందుకు మోసగాళ్లు నకిలీ పత్రాలను ఉపయోగిస్తారు.

- మోసగాళ్లు గుర్తింపు విధానంగా దొంగతనాలకు పాల్పడతారు, గుర్తింపు కార్డులు, బ్యాంక్ ఖాతా వివరాలు మొదలైన వినియోగదారుల వ్యక్తిగత సమాచారాన్ని దొంగిలిస్తారు మరియు ఆర్థిక సంస్థ నుండి ప్రయోజనాలను పొందేందుకు ఈ సమాచారం లేదా ఆధారాలను ఉపయోగిస్తారు.
- మోసగాళ్లు NBFC ఉద్యోగులుగా వ్యవహరిస్తారు మరియు

వినియోగదారుల నుండి KYC సంబంధిత పత్రాలను సేకరిస్తారు.

మ◌ు◌ందు జాగ్రత్తలు

- **ఏదైనా సంస్థ నుండి రుణం మంజూరు / క్రెడిట్ సౌకర్యాన్ని పొందడం కోసం నేషనల్ ఆటోమేటెడ్ క్లియరింగ్ హౌస్ (NACH) ఫారమ్‌తో సహా KYC మరియు ఇతర వ్యక్తిగత పత్రాలను అందించేటప్పుడు తగిన జాగ్రత్తలు మరియు అప్రమత్తతను పాటించండి, ప్రత్యేకించి ఈ సంస్థలకు ప్రతినిధులుగా వ్యవహరిస్తున్న వ్యక్తులతో.**
- **ఇటువంటి పత్రాలు సంస్థ యొక్క అధీకృత సిబ్బందితో లేదా సంస్థల అధీకృత ఇమెయిల్ IDలతో మాత్రమే భాగస్వామ్యం చేయబడాలి.**
- **రుణం మంజూరు చేయనప్పుడు మరియు/లేదా రుణ ఖాతాను మూసివేసిన తర్వాత మీరు భాగస్వామ్యం చేసిన డాక్యుమెంట్‌లను వారు వెంటనే అవి ఇక ఉపయోగపడకుండా ప్రక్షాళన చేస్తారని నిర్ధారించుకోవడానికి సంబంధిత సంస్థలతో సంప్రదింపుల్లో ఉండండి.**

ఆర్థిక లావాదేవీల విషయంలో తీసుకోవాల్సిన సాధారణ జాగ్రత్తలు

సాధారణ జాగ్రత్తలు

- అంతర్జాలంలో మీ బ్రౌజింగ్ సెషన్‌లలో కనిపించే అనుమానాస్పదంగా కనిపించే పాప్ అప్‌ల పట్ల జాగ్రత్తగా ఉండండి.
- ఆన్‌లైన్ చెల్లింపులు / లావాదేవీలు చేసే ముందు ఎల్లప్పుడూ సురక్షిత చెల్లింపు గేట్‌వే (https:// - ప్యాడ్ లాక్ చిహ్నంతో URL) కోసం తనిఖీ చేయండి.

- PIN (వ్యక్తిగత గుర్తింపు సంఖ్య), పాస్‌వర్డ్ మరియు క్రెడిట్ లేదా డెబిట్ కార్డ్ నంబర్, CVV మొదలైన వాటిని ప్రైవేట్‌గా ఉంచండి మరియు రహస్య ఆర్థిక సమాచారాన్ని బ్యాంకులు/ఆర్థిక సంస్థలు, స్నేహితులు లేదా కుటుంబ సభ్యులతో కూడా పంచుకోవద్దు.
- వెబ్‌సైట్‌లు / పరికరాలు / పబ్లిక్ ల్యాప్‌టాప్ / డెస్క్‌టాప్‌లలో కార్డ్ వివరాలను సేవ్ చేయడం మానుకోండి.
- అటువంటి సదుపాయం అందుబాటులో ఉన్న చోట రెండు-కారకాల ప్రమాణీకరణను ఆన్ చేయండి.
- తెలియని మూలాధారాలు అనుమానాస్పద జోడింపు లేదా ఫిషింగ్ లింక్‌లను కలిగి ఉండవచ్చు. అట్టి ఇమెయిల్‌లను ఎప్పుడూ తెరవవద్దు / ప్రతిస్పందించవద్దు;
- అపరిచితులతో చెక్కుబుక్, KYC పత్రాల కాపీలను పంచుకోవద్దు.

పరికరం / కంప్యూటర్ భద్రత కోసం

- క్రమ వ్యవధిలో పాస్‌వర్డ్‌లను మార్చండి.
- మీ పరికరాల్లో యాంటీవైరస్‌ని ఇన్‌స్టాల్ చేయండి మరియు

అందుబాటులో ఉన్నప్పుడల్లా అప్‌డేట్‌లను ఇన్‌స్టాల్ చేయండి.

- వినియోగానికి ముందు ఎల్లప్పుడూ తెలియని యూనివర్సల్ సీరియల్ బస్ (USB) డ్రైవ్‌లు / పరికరాలను స్కాన్ చేయండి.
- మీ పరికరాన్ని అన్‌లాక్ చేసి ఉంచవద్దు.

- నిర్దిష్ట సమయం తర్వాత పరికరం యొక్క స్వీయ లాక్‌ని కాన్ఫిగర్ చేయండి.
- మీ ఫోన్ / ల్యాప్‌టాప్‌లో తెలియని అప్లికేషన్‌లు లేదా సాఫ్ట్‌వేర్‌లను ఇన్‌స్టాల్ చేయవద్దు.
- పరికరాలలో పాస్‌వర్డ్‌లు లేదా రహస్య సమాచారాన్ని నిల్వ చేయవద్దు.

సురక్షితమైన ఇంటర్నెట్ బ్రౌజింగ్ కోసం

- సురక్షితం కాని/అసురక్షిత/తెలియని వెబ్‌సైట్‌లను సందర్శించడం మానుకోండి.
- తెలియని బ్రౌజర్‌లను ఉపయోగించడం మానుకోండి.

- పబ్లిక్ పరికరాలలో పాస్‌వర్డ్‌లను ఉపయోగించడం / సేవ్ చేయడం మానుకోండి.
- తెలియని వెబ్‌సైట్‌లు/పబ్లిక్ పరికరాలలో సురక్షిత ఆధారాలను నమోదు చేయడం మానుకోండి.
- వ్యక్తిగత సమాచారాన్ని ఎవరితోనూ, ముఖ్యంగా తెలియని వ్యక్తులతో సోషల్ మీడియాలో పంచుకోవద్దు.
- ఏదైనా వెబ్‌పేజీ (https:// - ప్యాడ్ లాక్ గుర్తుతో URL) భద్రతను ఎల్లప్పుడూ ధృవీకరించుకోండి, అలాగే ఇమెయిల్ లేదా SMS లింక్ అటువంటి పేజీలకు దారి మళ్లించబడినప్పుడు.

సురక్షితమైన ఇంటర్నెట్ బ్యాంకింగ్ కోసం

- పబ్లిక్ పరికరాలలో ఎల్లప్పుడూ వర్చువల్ కీబోర్డ్‌ను ఉపయోగించండి, ఎందుకంటే కీస్ట్రోక్‌లను పరికరాలు, కీబోర్డ్ రాజీ ద్వారా కూడా సంగ్రహించవచ్చు
- వినియోగం తర్వాత వెంటనే ఇంటర్నెట్ బ్యాంకింగ్ సెషన్ నుండి లాగ్ అవుట్ చేయండి.
- కాలానుగుణంగా పాస్‌వర్డ్‌లను నవీకరించండి.
- మీ ఇమెయిల్ మరియు ఇంటర్నెట్ బ్యాంకింగ్ కోసం ఒకే పాస్‌వర్డ్‌లను ఉపయోగించవద్దు.
- ఆర్థిక లావాదేవీల కోసం పబ్లిక్ టెర్మినల్స్ (అంటే సైబర్ కేఫ్, మొదలైనవి) ఉపయోగించడం మానుకోండి.

ఫోన్ గూఢచర్యం జరుగుతోందని సూచించే అంశాలు

- ఫోన్‌లో తెలియని అప్లికేషన్‌లు డౌన్‌లోడ్ చేయబడుతున్నాయి.
- ఫోన్ బ్యాటరీ సాధారణం కంటే వేగంగా అయిపోతుంది.

- ఫోన్ వేడెక్కడం అనేది, నేపథ్యంలో స్పైవేర్‌ను అమలు చేయడం ద్వారా ఎవరైనా గూఢచర్యం చేస్తున్నారనే సంకేతం కావచ్చు.
- డేటా వినియోగంలో అసాధారణ పెరుగుదల, కొన్నిసార్లు నేపథ్యంలో స్పైవేర్ రన్ అవుతుందనడానికి సంకేతం కావచ్చు.
- స్పైవేర్ యాప్‌లు కొన్నిసార్లు ఫోన్ షట్‌డౌన్ ప్రాసెస్‌లో జోక్యం చేసుకోవచ్చు, తద్వారా పరికరం సరిగ్గా ఆఫ్ చేయడంలో విఫలమవుతుంది లేదా అలా చేయడానికి అసాధారణంగా ఎక్కువ సమయం పడుతుంది.
- డేటాను పంపడానికి మరియు స్వీకరించడానికి స్పైవేర్ మరియు మాల్వేర్ ద్వారా వచన సందేశాలను ఉపయోగించవచ్చని గమనించండి.

మోసం జరిగిన తర్వాత తీసుకోవలసిన చర్యలు

- మీ శాఖను సందర్శించడం ద్వారా లేదా బ్యాంక్ వెబ్‌సైట్‌లో అందుబాటులో ఉన్న అధికారిక కస్టమర్ కేర్ నంబర్‌కు కాల్ చేయడం ద్వారా డెబిట్ కార్డ్/క్రెడిట్ కార్డ్‌ను మాత్రమే కాకుండా కార్డ్‌కి లింక్ చేసిన బ్యాంక్ ఖాతాలోని డెబిట్‌ను కూడా నిలుపుదల చేయండి. అలాగే, డెబిట్/క్రెడిట్ కార్డ్‌లు, మోసం జరిగిన తర్వాత బ్లాక్ చేయబడిన తర్వాత మోసం శాశ్వతంగా జరగకుండా నిరోధించడానికి నెట్ బ్యాంకింగ్, మొబైల్ బ్యాంకింగ్ మొదలైన ఇతర బ్యాంకింగ్ ఛానెల్‌ల భద్రతను తనిఖీ చేయండి మరియు నిర్ధారించుకోండి.
- హెల్ప్‌లైన్ నంబర్ 155260 లేదా 1930కి డయల్ చేయండి లేదా నేషనల్ సైబర్ క్రైమ్ రిపోర్టింగ్ పోర్టల్ (www.cybercrime.gov.in)లో సంఘటనను నివేదించండి.

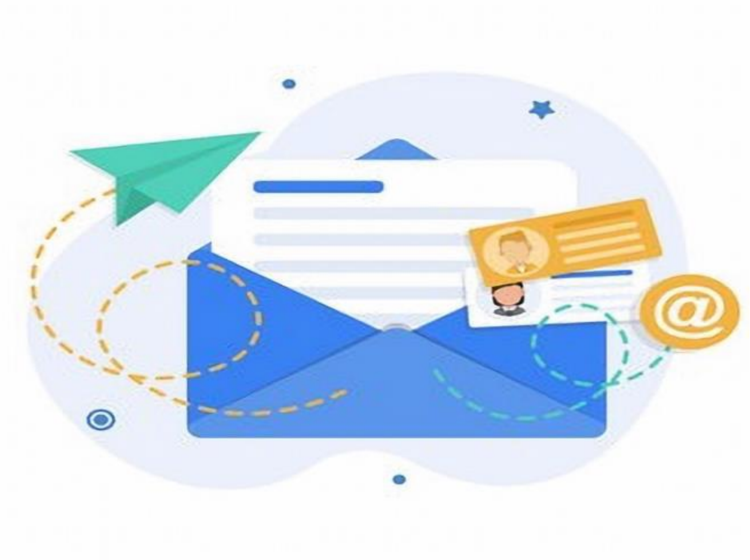
మొబైల్‌ని రీసెట్ చేయండి: మొబైల్ నుండి డేటా లీక్ కారణంగా మోసం జరిగితే మొబైల్ రీసెట్ చేయడానికి (సెట్టింగ్-రీసెట్-ఫ్యాక్టరీ డేటా)ని ఉపయోగించండి.

డెబిట్ / క్రెడిట్ కార్డ్‌లకు సంబంధించిన జాగ్రత్తలు

- మీరు క్రెడిట్ / డెబిట్ కార్డ్ యొక్క వివిధ ఫీచర్లను డియాక్టివేట్ చేయాలి, అనగా, దేశీయ మరియు అంతర్జాతీయ లావాదేవీల కోసం ఆన్‌లైన్ లావాదేవీలు, మీరు కార్డును కొంతకాలం ఉపయోగించనట్లయితే మరియు కార్డ్ వినియోగం అవసరమైనప్పుడు మాత్రమే సక్రియం చేయాలి.
- అదేవిధంగా, కార్డ్‌ని ఉపయోగించకూడదనుకుంటే, నియర్ ఫీల్డ్ కమ్యూనికేషన్ (NFC) ఫీచర్‌ను డీయాక్టివేట్ చేయాలి.
- ఏదైనా పాయింట్ ఆఫ్ సేల్ (POS) సైట్‌లో PINని నమోదు చేయడానికి ముందు లేదా NFC రీడర్‌లో కార్డ్‌ని ఉపయోగిస్తున్నప్పుడు, మీరు POS మెషీన్ స్క్రీన్ మరియు NFC రీడర్‌లో ప్రదర్శించబడే మొత్తాన్ని జాగ్రత్తగా తనిఖీ చేయాలి.
- లావాదేవీ చేస్తున్నప్పుడు స్వైపింగ్ కోసం వ్యాపారి మీ దృష్టి నుండి కార్డ్‌ని దూరంగా తీసుకెళ్లనివ్వవద్దు.
- POS సైట్ / ATMలో PINని నమోదు చేస్తున్నప్పుడు మీ మరో చేత్తో కీప్యాడ్‌ను కవర్ చేయండి.

ఇమెయిల్ ఖాతా భద్రత కోసం

- తెలియని చిరునామాలు / పేర్ల నుండి ఇమెయిల్‌ల ద్వారా పంపబడిన లింక్‌లపై క్లిక్ చేయవద్దు.
- పబ్లిక్ లేదా ఉచిత నెట్‌వర్క్‌లలో ఇమెయిల్‌లను తెరవడం



మానుకోండి.

- సురక్షిత ఆధారాలు / బ్యాంక్ పాస్‌వర్డ్‌లు మొదలైన వాటిని ఇమెయిల్‌లలో నిల్వ చేయవద్దు.

పాస్‌వర్డ్ భద్రత కోసం

- మీ పాస్‌వర్డ్‌లో ఆల్ఫాన్యూమరిక్ మరియు ప్రత్యేక అక్షరాల కలయికను ఉపయోగించండి.
- అటువంటి సదుపాయం అందుబాటులో ఉన్నట్లయితే, మీ అన్ని ఖాతాలకు రెండు కారకాల ప్రమాణీకరణను ఉంచండి.
- మీ పాస్‌వర్డ్‌లను ఎప్పటికప్పుడు మార్చుకోండి.
- మీరు పుట్టిన తేదీ, జీవిత భాగస్వామి పేరు, కారు నంబర్ మొదలైనవాటిని పాస్‌వర్డ్‌లుగా ఉంచడం మానుకోండి.

NBFC అంగీకరించే డిపాజిట్ నిజమైనదా కాదా అని మీకు ఎలా తెలుస్తుంది?

- https://rbi.org.inలో అందుబాటులో ఉన్న డిపాజిట్‌లను అంగీకరించే అర్హత కలిగిన డిపాజిట్ తీసుకునే NBFCల జాబితాలో సదరు NBFC పేరు కనిపిస్తుందో లేదో ధృవీకరించుకోండి మరియు డిపాజిట్‌లను స్వీకరించకుండా నిషేధించబడిన కంపెనీల జాబితాలో అది

కనిపించడం లేదని నిర్ధారించుకోండి.

- NBFCలు తప్పనిసరిగా రిజర్వ్ బ్యాంక్ జారీ చేసిన రిజిస్ట్రేషన్ సర్టిఫికేట్ (CoR)ని దాని సైట్‌లో / దాని కార్యాలయంలో తప్పనిసరిగా ప్రదర్శించాలి. ఈ సర్టిఫికేట్, డిపాజిట్లను ఆమోదించడానికి RBI ద్వారా NBFCకి ప్రత్యేకంగా అధికారం ఉందని కూడా ప్రతిబింబించాలి. డిపాజిట్‌లను ఆమోదించడానికి NBFCకి అధికారం ఉందని నిర్ధారించుకోవడానికి సర్టిఫికేట్‌ను పరిశీలించండి.

- NBFCలు 12-నెలల కంటే తక్కువ మరియు 60 నెలల కంటే ఎక్కువ కాలం డిపాజిట్‌లను అంగీకరించవు మరియు NBFC ఒక డిపాజిటర్‌కు చెల్లించగల గరిష్ట వడ్డీ రేటు 12.5% మించకూడదు.

- రిజర్వ్ బ్యాంక్ వడ్డీ రేట్లలో మార్పును https://rbi.org.in → సైట్‌మ్యాప్ → NBFC జాబితా → FAQలలో ప్రచురిస్తుంది.

డిపాజిటర్లు తీసుకోవాల్సిన జాగ్రత్తలు

- డబ్బును డిపాజిట్ చేసేటప్పుడు, బ్యాంక్/ఎన్‌బీఎఫ్‌సీ/కంపెనీతో చేసిన ప్రతి డిపాజిట్‌కి సరైన రసీదు కోసం పట్టుబట్టండి.

- రసీదుపై సంస్థచే అధికారం పొందిన అధికారి సంతకం చేయాలి మరియు ఇతరత్రా, డిపాజిట్ తేదీ, డిపాజిటర్ పేరు, అంకెలు మరియు వ్రాతతో మొత్తం, చెల్లించాల్సిన వడ్డీ రేటు, పరిపక్వత తేదీ మరియు మొత్తాన్ని పేర్కొనాలి.

- NBFCల తరపున పబ్లిక్ డిపాజిట్లను సేకరిస్తున్న బ్రోకర్లు / ఏజెంట్లు

మొదలైన వాటి విషయంలో, సంబంధిత NBFC ద్వారా బ్రోకర్లు / ఏజెంట్లు సక్రమంగా అధికారం పొందారని ధృవీకరించండి.

- NBFCల డిపాజిటర్లకు డిపాజిట్ ఇన్సూరెన్స్ సౌకర్యం అందుబాటులో లేదని గుర్తుంచుకోండి.

ఫిర్యాదు ప్రక్రియ

RBI అంబుడ్స్‌మన్‌కు ఫిర్యాదు

- ఆన్‌లైన్ ఫిర్యాదుల కోసం, దయచేసి https://cms.rbi.org.in/ లింక్‌ని సందర్శించండి
- ఇమెయిల్ ద్వారా ఫిర్యాదులను crpc@rbi.org.in కు పంపవచ్చు.
- భౌతిక / పేపర్ రూపంలో ఫిర్యాదులను CRPC, భారతీయ రిజర్వు బ్యాంకు, సెంట్రల్ విస్టా, సెక్టార్ -17, చండీగఢ్ -160 017కు పంపవచ్చు.

సెక్యూరిటీస్ అండ్ ఎక్స్ఛేంజ్ బోర్డ్ ఆఫ్ ఇండియా (SEBI)కి ఫిర్యాదు

- దయచేసి https://www.sebi.gov.in/ లింక్‌ని సందర్శించండి

ఇన్సూరెన్స్ రెగ్యులేటరీ అండ్ డెవలప్‌మెంట్ అథారిటీ ఆఫ్ ఇండియా (IRDAI)కి ఫిర్యాదు

- దయచేసి https://www.irdai.gov.in/ లింక్‌ని సందర్శించండి

నేషనల్ హౌసింగ్ బ్యాంక్ (NHB)కి ఫిర్యాదు

- దయచేసి https://nhb.org.in/ లింక్‌ని సందర్శించండి

సైబర్ పోలీస్ స్టేషన్‌లో ఫిర్యాదు

- దయచేసి https://cybercrime.gov.in/ని సందర్శించండి

....

పదకోశం

- **ముందస్తు రుసుము/ప్రాసెసింగ్ రుసుము/టోకెన్ రుసుము**: డాక్యుమెంటేషన్ ఛార్జీలు, సమావేశ ఖర్చులు, ప్రాసెసింగ్ ఫీజులు, రుణగ్రహీతకు రుణం పంపిణీకి వర్తించే ఇతర ఛార్జీలు వంటి ప్రాథమిక చెల్లింపులు వీటిలో ఉంటాయి.
- **రెండు-కారకాల ప్రమాణీకరణ**: ప్రామాణీకరణ పద్ధతులు మూడు ప్రాథమిక 'కారకాలు' కలిగి ఉంటాయి- వినియోగదారుకు తెలిసినవి (ఉదా., పాస్‌వర్డ్, పిన్- స్టాటిక్ లేదా ఒక సారి రూపొందించబడినవి); వినియోగదారు కలిగి ఉన్నవి (ఉదా., ATM/ స్మార్ట్ కార్డ్ నంబర్, గడువు తేదీ మరియు కార్డ్‌పై ముద్రించిన CVV); మరియు వినియోగదారువి ఏదైనా (ఉదా., వేలిముద్ర వంటి బయోమెట్రిక్ లక్షణం). రెండు-కారకాల ప్రమాణీకరణ (దీనిని 2FA అని కూడా పిలుస్తారు) రెండు వేర్వేరు భాగాల కలయిక ద్వారా వినియోగదారుల గుర్తింపును అందిస్తుంది - లావాదేవీని పూర్తి చేయడానికి వినియోగదారుకు ఏమి ఉంది మరియు వినియోగదారుకు తెలిసినవి.

- **ఆథరైజేషన్**: చెల్లింపు సమాచారం చెల్లుబాటు అయ్యేదని మరియు కస్టమర్ క్రెడిట్ కార్డ్‌లో నిధులు అందుబాటులో ఉన్నాయని సూచిస్తూ వ్యాపారి లావాదేవీ అధికార అభ్యర్థనకు కార్డ్ జారీ చేసే బ్యాంక్ నుండి ప్రతిస్పందన.
- **కార్డ్ నంబర్**: క్రెడిట్ కార్డ్ అసోసియేషన్ లేదా కార్డ్ జారీ చేసే బ్యాంక్ కార్డ్‌కి కేటాయించిన నంబర్. క్రెడిట్ కార్డ్ చెల్లింపు చేయడానికి ఈ సమాచారాన్ని కస్టమర్ తప్పనిసరిగా వ్యాపారికి అందించాలి కానీ ఇతరులతో పంచుకోకూడదు. కార్డుపై అంకెల స్ట్రింగ్ ప్రింట్ చేయబడుతుంది.
- **క్రెడిట్ కార్డ్**: ఆర్థిక సంస్థ నుండి అసురక్షిత/సురక్షిత క్రెడిట్‌ని పొందడం ద్వారా ఉత్పత్తులు లేదా సేవలకు చెల్లింపును అనుమతించే

కార్డ్.

- **క్రెడిట్ పరిమితి**: ఈ పదం ఒక ఆర్థిక సంస్థ కస్టమర్‌కు విస్తరించే గరిష్ట క్రెడిట్ మొత్తాన్ని సూచిస్తుంది. క్రెడిట్ కోరే దరఖాస్తుదారు ఇచ్చిన సమాచారం యొక్క విశ్లేషణ ఆధారంగా రుణం ఇచ్చే సంస్థ క్రెడిట్ కార్డ్‌పై క్రెడిట్ పరిమితిని పొడిగిస్తుంది. క్రెడిట్ పరిమితి కస్టమర్ యొక్క క్రెడిట్ స్కోర్‌లను మరియు భవిష్యత్తులో క్రెడిట్ పొందే వారి సామర్థ్యాన్ని ప్రభావితం చేస్తుంది.
- **CVV:** కార్డ్ వెరిఫికేషన్ విలువను సూచిస్తుంది. ఇది చాలా ఆన్‌లైన్ లావాదేవీలను పూర్తి చేయడానికి తప్పనిసరిగా కార్డ్‌పై ముద్రించబడిన 3-అంకెల సంఖ్య. ఈ వివరాలు గోప్యంగా ఉంచాలి మరియు ఎవరితోనూ భాగస్వామ్యం చేయకూడదు.
- **డెబిట్ కార్డ్**: కార్డ్ హోల్డర్ యొక్క బ్యాంక్ ఖాతాలో అందుబాటులో ఉన్న నిధుల వాడకం ద్వారా ఉత్పత్తులు లేదా సేవలకు చెల్లించడానికి అనుమతించే కార్డ్.
- **ఇ-కామర్స్ ప్లాట్‌ఫారమ్**: ఇది డిజిటల్ మరియు ఎలక్ట్రానిక్ నెట్‌వర్క్ ద్వారా డిజిటల్ ఉత్పత్తులతో సహా వస్తువులు మరియు సేవలను కొనుగోలు చేయడం మరియు విక్రయించడం ప్రారంభించే ప్లాట్‌ఫారమ్/వెబ్‌సైట్.
- **EMI:** ఇది సమానమైన నెలవారీ వాయిదాను సూచిస్తుంది. రుణగ్రహీత తన రుణదాత/క్రెడిటర్‌కి (బ్యాంక్/ఎన్‌బిఎఫ్‌సి వంటివి) ప్రతి నెలా రుణదాత/క్రెడిటర్ నుండి తీసుకున్న వడ్డీతో సహా పూర్తిగా చెల్లింపు జరిగేవరకు చెల్లించాల్సిన స్థిరమైన నెలవారీ చెల్లింపు (అసలు మరియు వడ్డీతో సహా).

- **ఎన్క్రిప్షన్:** ప్రాసెసింగ్ సమాచారాన్ని దాని గోప్యతను నిర్వహించడానికి ఎలక్ట్రానిక్ కోడ్‌గా మార్చే ప్రక్రియ.

- **గడువు తేదీ**: కార్డు, ఒప్పందం, పత్రం మొదలైన వాటి చెల్లుబాటు

గడువు ముగిసే తేదీ. ఇంకా గడువు ముగియని కార్డ్లు లేదా డాక్యుమెంట్లకు సంబంధించి మాత్రమే లావాదేవీలు ఆమోదించబడతాయి.

- **గేట్‌పే:** ఇది నేరుగా ప్రమేయం లేకుండా లావాదేవీల బేస్ మేనేజ్‌మెంట్, రిస్క్ మేనేజ్‌మెంట్ మొదలైన సేవలను మార్గం మరియు సులభతరం చేయడానికి సాంకేతిక మౌలిక సదుపాయాలను అందించే మధ్యవర్తి. చెల్లింపు గేట్‌వేలు అనేది నిధుల నిర్వహణలో ఎటువంటి ప్రమేయం లేకుండా ఆన్‌లైన్ చెల్లింపు లావాదేవీలను నిర్వహించడానికి మరియు సులభతరం చేయడానికి సాంకేతిక మౌలిక సదుపాయాలను అందించే సంస్థలు.
- **తక్షణ చెల్లింపు సేవలు** (IMPS): ఇది నేషనల్ పేమెంట్స్ కార్పొరేషన్ ఆఫ్ ఇండియా (NPCI) ద్వారా అందించబడిన మొబైల్ ఫోన్‌ల ద్వారా తక్షణ ఇంటర్‌బ్యాంక్ ఎలక్ట్రానిక్ ఫండ్ బదిలీ సేవ (పరిమితి వరకు).
- **KYC:** మీ వినియోగదారుని తెలుసుకోండి. పత్రాను పొందడం ద్వారా మరియు తగిన శ్రద్ధతో కస్టమర్‌తో సంబంధాన్ని కొనసాగించడంలో ఉన్న గుర్తింపు, అనుకూలత మరియు నష్టాలను ధృవీకరించడానికి ఆర్థిక సంస్థ ప్రయత్నం చేసే ప్రక్రియ ఇది.
- **మనీ మ్యూల్**: ఇది వారి బ్యాంక్ ఖాతా(ల) ద్వారా దొంగిలించబడిన / అక్రమ డబ్బును లాండరింగ్ చేయడానికి మోసగాళ్లచే దోపిడీకి గురైన బాధితులను వివరించడానికి ఉపయోగించే పదం.
- **మల్టీ-లెవల్ మార్కెటింగ్**: కంపెనీ తరపున వస్తువులు లేదా సేవలను విక్రయించే విధానం, దీని ద్వారా పాల్గొనేవారు తమ విక్రయాలపై కమీషన్‌ను అందుకుంటారు, అలాగే వారు రిక్రూట్ చేసిన భాగస్వాముల విక్రయాలపై.
- **నేషనల్ ఆటోమేటెడ్ క్లియరింగ్ హౌస్ (NACH):** ఇది నేషనల్ పేమెంట్స్ కార్పొరేషన్ ఆఫ్ ఇండియా (NPCI) ద్వారా నిర్వహించబడే

కేంద్రీకృత ఎలక్ట్రానిక్ క్లియరింగ్ సర్వీస్ (ECS) సిస్టమ్.

- **నియర్ ఫీల్డ్ కమ్యూనికేషన్ (NFC):** ఇది NFC అమర్చిన పరికరం నుండి సామర్థ్యం గల టెర్మినల్‌కు డేటాను ప్రసారం చేయడానికి ఉపయోగించే కమ్యూనికేషన్ టెక్నాలజీ. NFC సాంకేతికత NFC ప్రారంభించబడిన మెషీన్ దగ్గర స్మార్ట్‌ఫోన్/కార్డ్‌ను ఉంచడం ద్వారా నిర్వహించబడే కాంటాక్ట్‌లెస్ చెల్లింపును చేయడానికి ఉపయోగించబడుతుంది.
- **నేషనల్ ఎలక్ట్రానిక్ ఫండ్ ట్రాన్స్‌ఫర్ (NEFT):** ఇది RBI యాజమాన్యంలో నిర్వహించబడే దేశవ్యాప్త కేంద్రీకృత చెల్లింపు వ్యవస్థ, ఇది భారతదేశంలోని బ్యాంక్ కస్టమర్‌లు ఏదైనా రెండు NEFT-ప్రారంభించబడిన బ్యాంక్ ఖాతాల మధ్య నిధులను బదిలీ చేయడానికి వీలు కల్పిస్తుంది.
- **OTP:** వన్ టైమ్ పాస్‌వర్డ్ అనేది ధృవీకరణ పద్ధతిలోని కారకాలలో ఒకటి, ఇది కస్టమర్‌కు తెలుసు మరియు ఆన్‌లైన్ లావాదేవీలను నిర్వహించడానికి తరచుగా ఉపయోగించబడుతుంది. ఇది గోప్యమైనది మరియు ఎవరితోనూ భాగస్వామ్యం చేయకూడదు.

- **ఫిషింగ్:** ఇది తమ బ్యాంక్ / ఇ-వాలెట్ ప్రొవైడర్ నుండి కమ్యూనికేషన్ ఉద్భవించిందని మరియు రహస్య వివరాలను సేకరించేందుకు లింక్‌లను కలిగి ఉందని కస్టమర్‌లను మోసగించడానికి రూపొందించిన మోసపూరిత ఇమెయిల్‌లు మరియు / లేదా SMSలను సూచిస్తుంది.
- **పాయింట్ ఆఫ్ సేల్ పరికరం (POS) / అంగీకార పరికరం (mPOS):** ఇది మర్చంట్ ఎస్టాబ్లిష్‌మెంట్‌లలో ఇన్‌స్టాల్ చేయబడిన ఏదైనా పరికరం / టెర్మినల్ / మెషీన్‌ను సూచిస్తుంది, ఇది చెల్లింపు కార్డ్‌ల (క్రెడిట్ కార్డ్‌లు, డెబిట్ కార్డ్‌లు, గిఫ్ట్ కార్డ్‌లు మొదలైనవి) ద్వారా చెల్లింపులను అంగీకరించడానికి వ్యాపారులను అనుమతిస్తుంది. .
- **క్విక్ రెస్పాన్స్ (QR) కోడ్**: QR కోడ్ అనేది రెండు డైమెన్షనల్ బార్ కోడ్

రకం. ఇది తెలుపు నేపథ్యంలో ఒక చదరపు గ్రిడ్‌లో అమర్చబడిన నలుపు చతురస్రాలను కలిగి ఉంటుంది. ఈ కోడ్‌లను చదవడానికి మరియు అర్థం చేసుకోవడానికి స్మార్ట్‌ఫోన్ కెమెరాల వంటి ఇమేజింగ్ పరికరాలను ఉపయోగించవచ్చు. QR కోడ్ చెల్లింపుదారుని గురించిన సమాచారాన్ని కలిగి ఉంటుంది మరియు కస్టమర్ ఖాతా నుండి డెబిట్ చేయడం ద్వారా పాయింట్ ఆఫ్ సేల్ వద్ద మొబైల్ చెల్లింపులను సులభతరం చేయడానికి ఉపయోగించబడుతుంది.

- **రిమోట్ యాక్సెస్**: ఇది కస్టమర్‌ని వారి మొబైల్ ఫోన్/కంప్యూటర్‌లో ఒక అప్లికేషన్‌ను డౌన్‌లోడ్ చేయమని ఆకర్షిస్తుంది, ఇది ఆ కస్టమర్ పరికరంలోని కస్టమర్ల డేటా మొత్తాన్ని యాక్సెస్ చేయగలదు.

- **UPI:** యూనిఫైడ్ పేమెంట్ ఇంటర్‌ఫేస్ అనేది ఒక బ్యాంక్ నుండి డబ్బును బదిలీ చేయడానికి అనుమతించే ప్లాట్‌ఫారమ్/ ఇంటర్నెట్ యాక్సెస్ ఉన్న మొబైల్ ఫోన్‌ని ఉపయోగించి ఇతరులకు వాలెట్ ఖాతా. కస్టమర్ UPI కోసం బ్యాంక్‌లో నమోదు చేసుకున్న తర్వాత, చెల్లింపును ప్రారంభించడానికి ఒక ప్రత్యేకమైన వర్చువల్ ఐడెంటిఫైయర్ సృష్టించబడుతుంది మరియు కస్టమర్ మొబైల్ ఫోన్‌కు మ్యాప్ చేయబడుతుంది. ఇది UPI-PIN రూపంలో ప్రమాణీకరణను ఉపయోగిస్తుంది, ఇది గోప్యమైనది మరియు ఎవరితోనూ భాగస్వామ్యం చేయకూడదు.
- **విషింగ్:** ఇది బ్యాంక్ / నాన్-బ్యాంక్ ఇ-వాలెట్ ప్రొవైడర్ల నుండి టెలికాం సర్వీస్ ప్రొవైడర్లు KYC-అప్‌డేషన్, ఖాతా / SIM-కార్డ్‌ని అన్‌బ్లాక్ చేయడం, డెబిట్ చేసిన మొత్తాన్ని క్రెడిట్ చేయడం మొదలైన సాకులతో రహస్య వివరాలను పంచుకోవడానికి కస్టమర్‌లను ఆకర్షించే ఫోన్ కాల్‌లను సూచిస్తుంది.

- **వాలెట్:** వాలెట్ అనేది దానిలో నిల్వ చేయబడిన విలువకు వ్యతిరేకంగా వస్తువులు మరియు సేవలను కొనుగోలు చేయడానికి

ఉపయోగించే ఖాతా లాంటిది. వాలెట్ వర్చువల్ (ఉదా. మొబైల్ వాలెట్) లేదా భౌతిక (ప్రీపెయిడ్ కార్డ్డులు) కావచ్చు.

****