అప్రమత్తంగా ఉండండి మరియు సురక్షితంగా బ్యాంకింగ్ చేయండి

బ్యాంకింగ్ ధ్యాన్‌సే తో

AXIS BANK

ఇది యాక్సిస్ బ్యాంక్ అందిస్తున్న కస్టమర్ సర్వీస్

ఎక్నాలెడ్జ్‌మెంట్

ఈ విషయ వస్తువుపై ఆర్‌బిఐ ఒంబుడ్స్‌మన్ (ముంబయి–2) మహారాష్ట్ర, గోవా మరియు కొన్ని మా అంతర్గత పరిశోధన సంస్థల కార్యాలయం విడుదల చేసిన ‘ఆర్థిక మోసగాళ్ళు మోసాలకు పాల్పడే విధానంపై పుస్తకం’ లోని అంశాల ఆధారంగా ఈ డాక్యుమెంటు రూపొందించబడింది.

ముందుమాట

బ్యాంకింగ్ సిస్టమ్ డిజిటైజేషన్ కస్టమర్‌లు సుఖంగా మరియు వేగంగా తమ ఆర్థిక అవసరాలను తీర్చుకునేందుకు కొత్త మార్గాలను కల్పించింది. శారీరక మరియు సామాజిక కాంటాక్టును తగ్గించుకునేందుకు సాధ్యమైన మేర డిజిటల్ పద్ధతులు అవలంబించేలా ప్రస్తుత పరిస్థితి కూడా మనల్ని ప్రోత్సహిస్తోంది.

డిజిటల్ బ్యాంకింగ్‌లో సౌలభ్యాన్ని పెరగడం మనకు ఆనందకరమే అయినప్పటికీ, మనం సైబర్‌క్రైమ్ మరియు బ్యాంకింగ్ మోసాలకు కూడా ఎక్కువగా గురవుతున్నాము. అత్యధిక సమయం, కస్టమర్‌లు తెలియకుండానే ఇరుక్కుపోవచ్చు మరియు జాగ్రత్తగా లేకపోతే ఆర్థిక నష్టం వాటిల్లవచ్చు.

యాక్సిస్ బ్యాంక్‌లో, మేము మీ గురించి జాగ్రత్త తీసుకుంటాము మరియు ఎప్పటికప్పుడు ఉపయోగకరమైన సమాచారం పంచుకోవడం ద్వారా మీ ప్రయోజనాలను పరిరక్షించేందుకు మీకు సహాయపడే చర్యలను నిరంతరం ప్రవేశపెడుతుంటాము.

ఈ డాక్యుమెంటు ద్వారా మేము మీకు చైతన్యం కల్పిస్తున్నాము మరియు నేడు అమలులో ఉన్న అనుమానాస్పద మరియు మోసపూరిత కార్యకలాపాలను మీకు బాగా తెలిసేలా చేస్తున్నాము. ఇలాంటి యాక్టివిటిని ఎలా గుర్తించాలి, మీరు తీసుకోవలసిన ముందుజాగ్రత్తలు మరియు వాటిని ఎలా రిపోర్టు చేయాలి అనే విషయాలను అర్థంచేసుకునేందుకు మీకు సహాయపడటం కోసం మేము కొన్ని ప్రముఖ మోసపూరిత కార్యకలాపాల్లో కొన్నిటిని ఇక్కడ ఇస్తున్నాము. అప్రమత్తంగా ఉండటం వల్ల బలయ్యే అవకాశాలను మరియు ఆర్థిక నష్టం తగ్గించుకునేందుకు మీకు వీలు కలుగుతుంది.

మీరు శ్రద్ధగా బ్యాంకింగ్ చేసేటప్పుడు, ఈ సమాచారం మీకు ఉపయోగకరంగా ఉంటుందని మరియు సురక్షితమైన మరియు నిరాటంక బ్యాంకింగ్ అనుభవం పొందుతారని మేము ఆశిస్తున్నాము.

సురక్షితంగా ఉండండి!

కొన్ని సాధారణ ముందుజాగ్రత్త చర్యలు మరియు మంచి పద్ధతులను ఇక్కడ ఇస్తున్నాము.

మానుకోవలసినవి

- భద్రతలేని వెబ్‌సైట్‌లు చూడటం లేదా తెలియని బ్రౌజర్‌లను ఉపయోగించడం
- పబ్లిక్ డివైస్‌ల్లో పాస్‌వర్డ్‌లను సేవ్ చేయడం
- పబ్లిక్ లేదా ఉచిత నెట్‌వర్క్‌ల్లో ఆర్థిక/గోప్యమైన ఈ-మెయిల్స్‌కి యాక్సెస్‌కావడం
- అపరిచితుల నుంచి వచ్చిన అనుమానాస్పదంగా కనిపించే పాప్ అప్‌లు, లింకులు మరియు ఈ-మెయిల్స్‌పై క్లిక్ చేయడం.
- సురక్షితమైన క్రెడెన్షియల్స్‌ని లేదా పాస్‌వర్డ్‌లను ఈ-మెయిల్స్ లేదా అపరిచిత వెబ్‌సైట్‌ల్లో భద్రపరచుకోవడం
- సోషల్ మీడియాలో అపరిచిత వ్యక్తులకు గోప్యమైన సమాచారం ఇవ్వడం
- ఒకే పాస్‌వర్డ్‌లను బ్యాంకింగ్ మరియు ఇతర లావాదేవీలకు ఉపయోగించడం
- అపరిచిత అప్లికేషన్‌లు లేదా సాఫ్ట్‌వేర్‌ని ఇన్‌స్టాల్ చేయడం
- మీ మొబైల్ లేదా ఇతర ఎలక్ట్రానిక్ డివైస్‌లు లేదా యాప్స్‌ని లాక్‌చేయకుండా వదిలేయడం

ఎప్పుడూ చేయకండి

- మీ పిన్ (పర్సనల్ ఐడెంటిఫికేషన్ నంబరు), పాస్‌వర్డ్, క్రెడిట్ లేదా డెబిట్ కార్డు నంబర్లు, సివివి, చెక్కు బుక్ కాపీలు, కెవైసి వివరాలు తదితర వాటిని ఎవ్వరికీ ఇవ్వకండి.
- అపరిచిత డివైస్‌ల్లో సున్నితమైన లేదా గోప్యమైన సమాచారం భద్రపరచకండి.

ఎల్లప్పుడూ

- బలమైన స్క్రీన్ పాస్‌వర్డ్‌తో మీ ఫోన్‌ని రక్షించుకోండి
- వర్తించిన చోట/లభించిన చోట టూ-ఫ్యాక్టర్ అథెంటికేషన్‌ని ఉపయోగించండి
- ఉపయోగించిన తరువాత వెంటనే ఇంటర్నెట్ బ్యాంకింగ్ సెషన్‌ని లాగ్ అవుట్ చేయండి
- ఎనేబుల్ లేదా డిజేబుల్ విశిష్టతను ఉపయోగించండి మరియు మీరు ఉపయోగించిన దాని ఆధారంగా మీ కార్డు లేదా అకౌంట్‌పై లావాదేవీ అయాన్ పరిమితులను సెటప్ చేయండి.
- ప్యాడ్‌లాక్ లేదా https లాంటి భద్రత గల చిహ్నాల కోసం చూడటం ద్వారా వెబ్‌సైట్ సురక్షితమైనదేనా అనే విషయం నిర్ధారించుకోండి.
- ఆన్‌లైన్ చెల్లింపుల కోసం సురక్షితమైన పేమెంట్ గేట్‌వేలు ఉపయోగించండి.
- అల్ఫాన్యూమరిక్ మరియు ప్రత్యేక కేరెక్టర్‌లు కలిసివున్న బలమైన పాస్‌వర్డ్‌లనునిర్వహించండి మరియు వాటిని రెగ్యులర్‌గా మార్చండి.
- పబ్లిక్ డివైస్‌ల్లో వర్చువల్ కీబోర్డు ఉపయోగించండి, ఎందుకంటే కాంప్రమైజ్‌డ్ డివైస్‌లు, కీబోర్డులు తదితర వాటి ద్వారా కూడా కీస్ట్రోక్‌లను పసిగట్టవచ్చు.
- మీ డివైస్‌ల్లో యాంటీవైరస్ మరియు యాంటీ-ఐ-స్పైవేర్‌ని ఇన్‌స్టాల్ చేయండి, వాటిని అప్‌డేట్‌గా ఉంచి వీలైనప్పుడల్లా అప్‌డేట్‌లను ఇన్‌స్టాల్ చేయండి.
- ఉపయోగించడానికి ముందు ఏవైనా యుఎస్‌బి డ్రైవ్స్/స్టోరేజ్ డివైస్‌లను స్కాన్ చేయండి.
- పాస్‌వర్డ్‌తో మీ మొబైల్ యాప్స్‌ని రక్షించండి లేదా మొబైల్ ఫోన్‌ల్లో దాగివున్న స్పేస్ ఫీచర్‌ని ఉపయోగించి మామూలుగా చూడకుండా వాటిని దాచిపెట్టండి.

#BankingDhyaanSe

ఆన్‌లైన్/వెబ్‌సైట్ మోసాల గురించి (1)

మోసం చేసే విధానం

మీరు ఎలా జాగ్రత్తగా మరియు సురక్షితంగా ఉండొచ్చు?

ఆన్‌లైన్ ఫిషింగ్

దీనిని ఎలా చేస్తారు

- మోసగాళ్ళు బ్యాంక్ యొక్క అసలైన వెబ్‌సైట్‌ని కచ్చితంగా పోలివుండే వెబ్‌సైట్‌ని రూపొందిస్తారు.
- ఈ వెబ్‌సైట్ లింకులను ఎస్ఎంఎస్, సామాజిక మాధ్యమాలు, ఈ-మెయిల్ తదితర వాటి ద్వారా పంపిణీ చేస్తారు.
- చూడటానికి ప్రామాణిక వెబ్‌సైట్ మాదిరిగా కనిపించేలా ఈ లింకులకు మాస్క్ చేస్తారు మరియు వివరమైన యుఆర్ఎల్‌ని చెక్ చేయకుండానే మరియు లింకును చూడటం ద్వారా మాత్రమే మీ క్రెడెన్షియల్స్ లేదా సున్నితమైన మరియు గోప్యమైన సమాచారం నమోదు చేసేలా పురిగొల్పుతారు.
- మీరు ఈ వెబ్‌సైట్‌ల్లో ఈ క్రెడెన్షియల్స్‌ని నమోదు చేసినప్పుడు, మోసగాళ్ళు వీటిని తీసుకుని దుర్వినియోగం చేసే అవకాశం ఉంది.

సురక్షిత సూచనలు

- చూడటానికి ప్రామాణికంగా ఉన్నప్పటికీ అపరిచిత లింకులపై క్లిక్ చేయకండి
- ఆర్థిక వివరాలను నమోదు చేయడానికి ముందు వెబ్‌సైట్ వివరాలను నిర్ధారించుకోండి.

ఆన్‌లైన్ మోసాలు

వీటిని ఎలా చేస్తారు

- మోసగాళ్ళు ఆన్‌లైన్, ఈ-కామర్స్ ప్లాట్ ఫారాల్లో చట్టబద్ధ కొనుగోలుదారులు/విక్రేతలుగా నటిస్తారు.
- వీళ్ళు మీ ఉత్పాదన పట్ల ఆసక్తి చూపిస్తారు లేదా భారీ డిస్కౌంట్లు లేదా ప్రోత్సాహకాలు అందించడం ద్వారా వాళ్ళ నుంచి మీరు కొనేలా పురిగొల్పుతారు.
- డబ్బు చెల్లించడానికి బదులుగా, మీ బ్యాంక్ అకౌంట్ నుంచి డబ్బు గుంజుకోవడానికి యుపిఐ ‘రిక్వెస్ట్ మనీ’ ఆప్షన్‌ని పూర్తిచేసేలా వాళ్ళు మిమ్మల్ని ప్రలోభపెడతారు.

సురక్షిత సూచనలు

- ఆన్‌లైన్ ఉత్పాదనల కోసం ఆర్థిక లావాదేవీలు చేసేటప్పుడు జాగ్రత్తగా ఉండండి
- డబ్బు పొందడానికి మీ పిన్ లేదా పాస్‌వర్డ్‌ని ఎప్పుడూ నమోదు చేయవద్దని మిమ్మల్ని అడుగుతారు.

ఆన్‌లైన్/వెబ్‌సైట్ మోసాల గురించి (2)

మోసం చేసే విధానం
మీరు సురక్షితగంగా మరియు జాగ్రత్తగా ఎలా ఉండొచ్చు?

సందేహాస్పద సెర్చ్ ఇంజిన్ ఫలితాలు

వీటిని ఎలా చేస్తారు?

- మోసగాళ్ళు కంపెనీల యొక్క కస్టమర్ కేర్ కోఆర్డినేట్‌లను మార్చుతారు మరియు సామాజిక మాధ్యమాల వేదికల్లో సెర్చ్ ఫలితాల్లో టాప్‌లో తమ ఫేక్ నంబరును ఉంచేందుకు సెర్చ్ ఇంజిన్ ఆప్టిమైజేషన్‌ని (ఎస్‌ఇఒ) ఉపయోగిస్తారు.
- మీబ్యాంకు లేదా ఇతర ఆర్థిక సమాచారం/సంస్థల యొక్క కస్టమర్ కేర్ సంప్రదింపు వివరాల కోసం ఆన్‌లైన్‌లో సెర్చ్ చేసేటప్పుడు, అసలైనవిగా భావించి, ఇలాంటి నిర్ధారించుకోని/నకిలీ నంబర్లను మీరు పొరబాటుగా కాంటాక్టు అవ్వవచ్చు.
- మీరు మీ వ్యక్తిగత లేదా గోప్యమైన మరియు ఆర్థిక వివరాలను ఇవ్వవచ్చు మరియు మోసానికి గురవ్వవచ్చు.

సురక్షిత సూచనలు

- సెర్చ్ ఇంజిన్‌లో కస్టమర్ కేర్ సంప్రదింపు వివరాల కోసం సెర్చ్ చేయకండి ఎందుకంటే బాధితులను ఆకర్షించేందుకు మోసగాళ్ళు వాటికి ముసుగువేయవచ్చు.
- ఎల్లప్పుడూ బ్యాంకుల/కంపెనీల యొక్క అధికారిక వెబ్‌సైట్‌ల యొక్క అసలైన సంప్రదింపు వివరాల కోసం చూడండి.

స్క్రీన్ షేరింగ్/రిమోట్ యాక్సెస్

దీనిని ఎలా చేస్తారు?

- మోసగాళ్ళు మిమ్మల్ని స్క్రీన్ షేరింగ్ యాప్స్‌ని డౌన్‌లోడ్ చేసుకునేలా చేసి, మీ ల్యాప్‌టాప్/మొబైల్ డివైస్‌ల్లో మీ వ్యక్తిగత డేటా మరియు ఆర్థిక క్రెడెన్షియల్స్‌కి యాక్సెస్ పొందుతారు మరియు ఆ తరువాత మీ బ్యాంకింగ్ మరియు పేమెంట్ యాప్స్‌ని ఉపయోగించి చెల్లింపులు చేస్తారు.

సురక్షిత సూచనలు

- అపరిచిత వ్యక్తులెవరైనా సిఫారసు చేసిన స్క్రీన్ షేరింగ్ యాప్స్‌ని డౌన్‌లోడ్ చేసుకోకండి.
- ఏదైనా బ్యాంకింగ్ లేదా ఆర్థిక యాప్ లేదా వెబ్‌సైట్‌లోకి లాగిన కావడానికి ముందు స్క్రీన్ షేరింగ్ అప్లికేషన్ దేనినైనా మీరు తప్పకుండా డీయాక్టివేట్ చేయండి.

కాల్/మొబైల్ మోసాల గురించి (1)

మోసం చేసే విధానం

మీరు ఎలా జాగ్రత్తగా మరియు సురక్షితంగా ఉండొచ్చు?

విషింగ్ కాల్స్

దీనిని ఎలా చేస్తారు?

- అప్పుడప్పుడు మీ బ్యాంక్ యొక్క టోల్ ఫ్రీ లేదా కస్టమర్ కేర్ నంబరును స్పూఫ్ చేస్తూ, బ్యాంకింగ్ ఎగ్జిక్యూటివ్స్ తదితరుల మాదిరిగా చెప్పుకుంటూ టెలిఫోన్ కాల్/సామాజిక మాధ్యమం ద్వారా కస్టమర్‌ల కాంటాక్టులు పొందుతారు.
- సర్వీసులను వెంటనే నిలిపివేయడం, కెవైసిని అనువర్తించకపోవడం, అకౌంట్/కార్డు మూసివేయడం లాంటి వివిధ అత్యవసర కారణాలను ఉదహరిస్తూ క్రెడెన్షియల్ వివరాలు లేదా ఒటిపిని చెప్పేలా కస్టమర్‌పై కాలర్ ఒత్తిడి తీసుకొస్తారు.
- మీ అకౌంట్‌లో మోసపూరిత కార్యకలాపాలు చేసేందుకు వాళ్ళు ఈ క్రెడెన్షియల్స్‌ని దుర్వినియోగం చేస్తారు.

సురక్షిత సూచనలు

- యూజర్‌నేమ్, పాస్‌వర్డ్, కార్డు వివరాలు, పిన్, సివివి, ఒటిపి, తదితర లాంటి గోప్యమైన సమాచారాన్ని పంచుకోవలసిందిగా బ్యాంక్/ఏదైనా యథార్థ సంస్థ ఎప్పుడూ మిమ్మల్ని అడగదు.

మొబైల్ యాప్ మోసాలు

వీటిని ఎలా చేస్తారు?

- నిర్ధారించుకోని యాప్‌ని మీ మొబైల్, ల్యాప్‌టాప్ లేదా డెస్క్‌టాప్‌లో డౌన్‌లోడ్ చేసుకునేలా మిమ్మల్ని ప్రలోభపెట్టడం జరుగుతుంది.
- ఈ యాప్‌లకు లింకులను ఎస్ఎంఎస్, సోషల్ మీడియా ప్లాట్ ఫామ్‌లు, తదితర వాటి ద్వారా పంచుకోవడం మరియు ప్రమోట్ చేయడం జరుగుతుంది.
- ఇవి మీ డివైస్‌కి పూర్తి యాక్సెస్ పొందేలా మోసగాళ్ళను అనుమతించే ద్రోహచింతన గల అప్లికేషన్‌లు.

సురక్షిత సూచనలు

- నిర్ధారించుకోని/అపరిచిత మూలాల నుంచి ఎప్పుడూ అప్లికేషన్‌ని డౌన్‌లోడ్ చేసుకోకండి.
- డౌన్‌లోడ్ లింక్‌పై ఉద్దేశరహితంగా క్లిక్ చేయకుండా ఉండేందుకు, అపరిచిత మూలాల నుంచి అందిన ఎస్ఎంఎస్/ఈ–మెయిల్‌ని డిలీట్ చేయండి.

కాల్/మొబైల్ మోసాల గురించి (2)

మోసం చేసే విధానం

మీరు ఎలా జాగ్రత్తగా మరియు సురక్షితంగా ఉండొచ్చు?

ఒటిపి ఆధారిత మోసం

దీనిని ఎలా చేస్తారు?

- లోన్స్ ఇస్తున్న బ్యాంకుగా లేదా క్రెడిట్ పరిమితిని పెంచుతున్నట్లుగా మరియు మెసేజ్‌లో పేర్కొన్న నంబరును సంప్రదించవలసిందిగా మిమ్మల్ని అడుగుతున్నట్లుగా మోసగాడి నుంచి మీకు ఎస్ఎంఎస్ అందవచ్చు.
- మీరు ఆ నంబరుకు కాల్ చేసినప్పుడు, కొద్ది ఫారాలు నింపవలసిందిగా (ఆన్‌లైన్‌లో కూడా) మిమ్మల్ని అడుగుతారు, దీనిలో మీ ఆర్థిక వివరాలు ఉంటాయి. ఒటిపి లేదా పిన్ వివరాలను పంచుకోవలసిందిగా మీకు నచ్చజెప్పడాన్ని వాళ్ళకు సులభతరం చేస్తాయి. దీనివల్ల మీకు ఆర్థిక నష్టం కలుగుతుంది.

సురక్షిత సూచనలు

- ఎవ్వరితోనూ ఏ రూపంలోనూ ఎప్పుడూ మీ ఒటిపి, పిన్ లేదా వ్యక్తిగత వివరాలను పంచుకోకండి.
- మీకు తెలియకుండా ఒటిపి ఏదీ జెనరేట్ కాకుండా చూసేందుకు మీ ఎస్ఎంఎస్/ఈ-మెయిల్స్‌ని రెగ్యులర్‌గా చెక్ చేయండి.

జ్యూస్ జాకింగ్

దీనిని ఎలా చేస్తారు?

- జ్యూస్ జాకింగ్ అనేది ఒక రకం సైబర్ దొంగతనం. మీ మొబైల్‌ని ఏవైనా అపరిచిత/నిర్ధారించుకోని చార్జింగ్ పోర్టులకు కనెక్ట్ చేసేందుకు, కొన్ని అపరిచిత యాప్స్/మాల్‌వేర్‌ని మీ డివైస్‌లో ఇన్‌స్టాల్ చేస్తే, మోసగాళ్ళు దీనితో సున్నితమైన డేటా, ఈ-మెయిల్, ఎస్ఎంఎస్ లేదా సేవ్‌చేసిన పాస్‌వర్డ్‌లను దొంగిలించవచ్చు.

సురక్షిత సూచనలు

- ఎల్లప్పుడూ పబ్లిక్/అపరిచిత చార్జింగ్ పోర్టులు/కేబుల్స్‌ని ఉపయోగించడం మానుకోండి

కాల్/మొబైల్ మోసాల గురించి (3)

మోసం చేసే విధానం

మీరు ఎలా జాగ్రత్తగా మరియు సురక్షితంగా ఉండొచ్చు?

సిమ్ స్వాప్ మోసాలు

వీటిని ఎలా చేస్తారు?

- మీ అకౌంట్ వివరాలు మరియు ప్రామాణీకత మీ రిజిస్టర్డు మొబైల్ నంబరుకు కనెక్ట్ చేయబడతాయి. మీ నంబరుకు కొత్త రీప్లేస్‌మెంట్ సిమ్ కార్డు పొందడం ద్వారా ఆర్థిక లావాదేవీలు నిర్వహించేందుకు ఒటిపికి మరియు ఎలర్ట్‌లకు యాక్సెస్ పొందడానికి మోసగాళ్ళు ప్రయత్నిస్తారు.
- మీ ఒరిజినల్ సిమ్‌ని బ్లాక్ చేయించేందుకు మరియు మీ మొబైల్ నంబరుతో కొత్త సిమ్‌ని సేకరించేందుకు నకిలీ ఐడి ప్రూఫ్‌తో మీరే వెళ్ళినట్లుగా మోసగాడు మీ మొబైల్ ఆపరేటర్ యొక్క రిలైట్ అవుట్‌లెట్‌ని సందర్శిస్తారు.
- ప్రత్యామ్నాయంగా, మీ ఆపరేటర్‌కి మోసగాడు ఇచ్చిన ఎస్ఎంఎస్‌ని పంపడం ద్వారా మీ సిమ్ కార్డును అప్‌గ్రేడ్ చేసేలా వాళ్ళు మిమ్మల్ని భయపడతారు లేదా ఎత్తుగడ వేస్తారు.

సురక్షిత సూచనలు

- మీ గోప్యమైన మరియు వ్యక్తిగత డేటాను దొంగిలించడం సామాజిక ఇంజినీరింగ్ స్కామ్‌ల లక్ష్యమనే విషయం తెలుసుకోండి.
- మీ మొబైల్ ఫోన్ అకస్మాత్తుగా నెట్‌వర్క్ కనెక్టివిటి దేనినీ చూపించకపోతే, మీ సిమ్‌కి డూప్లికేట్ సిమ్ జారీచేయబడలేదని నిర్ధారించుకునేందుకు మీ సర్వీసు స్థితి గురించి వెంటనే మీ మొబైల్ సర్వీస్ ప్రొవైడర్‌ని విచారించండి.

ఇతర రకాల మోసాల గురించి (1)

మోసం చేసే విధానం

మీరు ఎలా జాగ్రత్తగా మరియు సురక్షితంగా ఉండొచ్చు?

సామాజిక మాధ్యమం ద్వారా మోసాలు

వీటిని ఎలా చేస్తారు?

- మోసగాళ్ళు మిమ్మల్ని అభినయిస్తారు మరియు జనాదరణ పొందిన సామాజిక మాధ్యమ వేదికలపై నకిలీ అకౌంట్‌లు సృష్టిస్తారు.
- అన్‌లాక్ చేయని మీ ఫోన్‌ని పొరబాటున అప్పగించినప్పుడు (అత్యవసర కాల్ చేసేందుకు లేదా మరమ్మతులు చేసేందుకు) లేదా ఫోన్‌ని అలా వదిలేసి వెళ్ళినప్పుడు, మీ ప్రొఫైల్‌కి యాక్సెస్ పొందేందుకు మీ మొబైల్‌కి పంపిన ఓటిపిని మోసగాడు పొందగలుగుతారు మరియు మీ కాంటాక్టులు, ఆన్‌లైన్ ప్రొఫైల్ మరియు చాట్ మెసేజ్‌లకు తమకు యాక్సెస్ ఇస్తూ కొన్ని అప్లికేషన్‌ల యొక్క డెస్క్‌టాప్ వెర్షన్‌ని జెనరేట్ చేస్తారు.
- అత్యవసర వైద్య సహాయం, తదితర వాటికి డబ్బు అడుగుతూ మీ స్నేహితులకు వాళ్ళు అభ్యర్థనలు పంపుతారు.

సురక్షిత సూచనలు

- ఏదైనా చెల్లింపు చేయడానికి ముందు స్వయంగా లేదా ఫోన్ ద్వారా మీ కాంటాక్టులను చేరుకోవడం ద్వారా అభ్యర్థన యొక్క ప్రామాణికతను నిర్ధారించుకోండి.
- లాక్ చేయని ఫోన్‌ని మీరు ఎప్పుడూ ఎక్కడా వదిలేసి వెళ్ళకూడదు.

క్యూఆర్ స్కాన్-ఆధారిత మోసాలు

వీటిని ఎలా చేస్తారు?

- మోసగాళ్ళు వివిధ ముసుగుల్లో మిమ్మల్ని సంప్రదించవచ్చు లేదా పేమెంట్ యాప్స్‌ని ఉపయోగించి క్యూఆర్ కోడ్‌లను స్కాన్ చేసేలా మరియు పేమెంట్ ప్రక్రియను పూర్తిచేసేలా మిమ్మల్ని ప్రలోభపెట్టవచ్చు.
- మీ అకౌంట్ నుంచి డబ్బు బదిలీని పూర్తిచేయడం ద్వారా మిమ్మల్ని ట్రిక్ చేసేందుకు మోసగాడు ఎంచుకున్న ఏదైనా నిర్దిష్ట అకౌంట్‌కి డబ్బు బదిలీ చేసేందుకు ఈ క్యూఆర్ కోడ్‌లకు ముందుగా నిర్ణయించిన అకౌంట్ వివరాలు ఉంటాయి.

సురక్షిత సూచనలు

- పేమెంట్ యాప్స్‌ని ఉపయోగించి ఏవైనా క్యూఆర్ కోడ్‌లను స్కాన్ చేసేటప్పుడు జాగ్రత్తగా ఉండండి.

ఇతర రకాల మోసాల గురించి (2)

మోసం చేసే విధానం

మీరు ఎలా జాగ్రత్తగా మరియు సురక్షితంగా ఉండొచ్చు?

లాటరీ లేదా జాబ్ మోసం స్కామ్‌లు

వీటిని ఎలా చేస్తారు?

- మీరు భారీ లాటరీ/బహుమతి గెలుచుకున్నారని లేదా ఉద్యోగం ఇస్తున్న ప్రఖ్యాత కంపెనీ అధికారినని చెప్పుకుంటూ మోసగాళ్ళు మీకు ఈ-మెయిల్ పంపుతారు లేదా ఫోన్ కాల్స్ చేస్తారు.
- అయితే, డబ్బు/బహుమతి పొందడానికి లేదా ఎంపిక ప్రక్రియను పూర్తిచేసేందుకు, మీ డబ్బులో కొంత మొత్తాన్ని ముందుగా చెల్లించాలని మిమ్మల్ని అడగవచ్చు.
- అడిగిన డబ్బు లాటరీ/బహుమతిలో చాలా కొద్ది శాతం ఉంటుంది కాబట్టి లేదా ఉద్యోగం పొందడానికి కీలకంగా పరిగణిస్తారు కాబట్టి, అడిగిన మొత్తాన్ని మీరు చెల్లిస్తారు.

సురక్షిత సూచనలు

- ఏవైనా లాటరీ కాల్స్/ఈ-మెయిల్స్ కోసం మీ సురక్షితమైన క్రెడెన్షియల్స్‌ని పంచుకోకండి లేదా చెల్లింపులు చేయకండి.
- నమ్మశక్యంకాని ఏవైనా లాటరీ లేదా ఆఫర్‌ల ప్రామాణికతను ఎల్లప్పుడూ ప్రశ్నించండి.
- జాబ్ ఇవ్వజూపిన యథార్థ కంపెనీ ఎప్పుడూ డబ్బు అడగదనే విషయం గుర్తుంచుకోండి.

ఎటిఎం కార్డు స్కిమ్మింగ్

దీనిని ఎలా చేస్తారు?

- డేటాను దొంగిలించేందుకు, డూప్లికేట్ కార్డు సృష్టించేందుకు మరియు మీ అకౌంట్ నుంచి డబ్బు విత్‌డ్రా చేసుకునేందుకు ఎటిఎం మెషీన్‌ల్లో స్కిమ్మింగ్ డివైస్‌లు ఇన్‌స్టాల్ చేస్తారు.
- మీరు నమోదు చేసిన సమాచారం తీసుకునేందుకు వాళ్ళు డమ్మీ కీప్యాడ్‌లు లేదా చిన్న కెమెరాలు కూడా ఇన్‌స్టాల్ చేయవచ్చు.
- ఒకవేళ మీరు నగదు విత్‌డ్రా చేయలేకపోతే, మీరు పిన్‌ని నమోదు చేసేటప్పుడు లేదా మీ లావాదేవీని పూర్తిచేయడానికి మీకు సహాయపడేందుకు, మీ పిన్‌ని చూసేందుకు ఎటిఎం సర్వీసులు ఉపయోగించి కస్టమర్‌గా కూడా వాళ్ళు వ్యవహరించవచ్చు.

సురక్షిత చిట్కాలు

- అప్రమత్తంగా ఉండండి మరియు కార్డు పెట్టిన స్లాట్‌లో లేదా ఎటిఎం మెషీన్ యొక్క కీప్యాడ్‌కి సమీపంలో అదనపు డివైస్ జతచేయలేదని నిర్ధారించుకోండి.
- మీకు సమీపంలో నిలబడిన ఎవ్వరి సమక్షంలోనూ కార్డు వివరాలను నమోదు చేయకండి.
- పిన్‌ని నమోదు చేసేటప్పుడు కీప్యాడ్‌కి ఆచ్ఛాదన పెట్టండి మరియు ఎవ్వరికీ మీ పిన్ లేదా కార్డు వివరాలు చెప్పకండి.
- మీకు ఏదైనా అనుమానాస్పదంగా అనిపిస్తే వెంటనే ఎటిఎం ప్రాంగణం నుంచి వెళ్ళిపోండి.

అనుమానాస్పద లేదా మోసపూరిత లావాదేవీని యాక్సిస్ బ్యాంక్‌కి రిపోర్టు చేయండి

ఒకవేళ అనుమానాస్పద లావాదేవీ మీ దృష్టికి వస్తే లేదా మోసపూరిత లావాదేవీ చేస్తే, ఈ కింద పేర్కొన్న చానల్స్‌లో మీరు సంప్రదించవచ్చు:

- మా ఫోన్ బ్యాంకింగ్ నంబర్లకు కాల్ చేయండి: 1860 419 5555 / 1860 500 5555
- మాకు రాయండి https://www.axisbank.com/support/కి
- యాక్సిస్ బ్యాంక్ బ్రాంచి దేనినైనా సందర్శించండి

మీరు సమయం కేటాయించినందుకు మరియు శ్రద్ధపెట్టినందుకు ధన్యవాదాలు.

#BankingDhyaanSe