DCB BANK

అనుబంధం 7: వినియోగదారుల అవగాహన-సైబర్ బెదిరింపులు మరియు మోసాలు

సోషల్ మీడియా టెక్నిక్‌లు, మొబైల్ ఫోన్ కాల్‌లు మొదలైన వినూత్న కార్యకలాపాలను ఉపయోగించడం ద్వారా అసాంఘిక అంశాలు ప్రజలను మోసగించడం మరియు తప్పుదారి పట్టించడం గమనించబడింది. దీనిని దృష్టిలో ఉంచుకుని, మోసపూరిత సందేశాలు, నకిలీ కాల్‌లు, తెలియని వాటి గురించి ప్రజలు అప్రమత్తంగా ఉండాలని డిసిబి బ్యాంక్ హెచ్చరించింది. లింక్‌లు, తప్పుడు నోటిఫికేషన్‌లు, అనధికారిక క్యూఆర్ కోడ్‌లు మొదలైనవి, రాయితీలు పొందడంలో/ బ్యాంకులు మరియు ఆర్థిక సేవా ప్రదాతల నుండి ఏ పద్ధతిలోనైనా ప్రతిస్పందనను వేగవంతం చేయడంలో సహాయపడతాయి.

యూజర్ ఐడి, లాగిన్/లావాదేవీ పాస్‌వర్డ్ వన్ టైమ్ పాస్‌వర్డ్ (ఓటిపి), డెబిట్/క్రెడిట్ కార్డ్ వివరాలైన పిన్, సివివి, గడువు తేదీ మరియు ఇతర వ్యక్తిగత సమాచారం వంటి రహస్య వివరాలను పొందడానికి మోసగాళ్లు ప్రయత్నిస్తారు. మోసగాళ్లు ఉపయోగించే సాధారణ కార్యనిర్వహణ విధానం:

- కవైసి అప్‌డేట్ చేయడం, అకౌంట్ / సిమ్ కార్డ్‌ని అన్‌బ్లాక్ చేయడం, డెబిట్ చేసిన మొత్తాన్ని క్రెడిట్ చేయడం మొదలైన సాకులతో రహస్య వివరాలను షేర్ చేయడానికి కస్టమర్‌లను ఆకర్షించడానికి బ్యాంక్/నాన్-బ్యాంక్ ఇ-వాలెట్ ప్రొవైడర్లు/టెలికాం సర్వీస్ ప్రొవైడర్ల నుండి వచ్చినట్లు నటిస్తూ ఫిషింగ్-ఫోన్ కాల్‌లు.
- మోసపూరిత ఫిషింగ్ ఇమెయిల్‌లు మరియు/లేదా ఎస్‌ఎంఎస్‌లు కస్టమర్‌లను మోసగించడానికి రూపొందించిన వారి ఆలోచనలని కమ్యూనికేషన్ చేసేందుకు బ్యాంక్/ఇ-వాలెట్ ప్రొవైడర్ నుండి ఉద్భవించిందని మరియు రహస్య వివరాలను సేకరించేందుకు లింక్‌లను కలిగి ఉంది.
- రిమోట్ యాక్సెస్ – కస్టమర్లను ఆకర్షించడం ద్వారా కస్టమర్ల డివైజ్‌లోని డేటాను యాక్సెస్ చేయగల వారి మొబైల్ ఫోన్/కంప్యూటర్‌లో అప్లికేషన్‌ను డౌన్‌లోడ్ చేసుకునేలా చేస్తుంది.
- డబ్బును స్వీకరించడానికి 'మీ యుపిఐ పిన్‌ను నమోదు చేయండి' వంటి సందేశాలతో నకిలీ చెల్లింపు అభ్యర్థనలను పంపడం ద్వారా యుపిఐ యొక్క 'కలెక్ట్ రిక్వెస్ట్' ఫీచర్‌ను దుర్వినియోగం చేయండి.
- వెబ్‌పేజీలు/సోషల్ మీడియాలో బ్యాంకులు/ఇ-వాలెట్ ప్రొవైడర్ల నకిలీ సంప్రదింపు నంబర్‌లు మరియు శోధన ఇంజిన్‌లు మొదలైనవి ప్రదర్శించబడతాయి.

ఏదైనా డిజిటల్ (ఆన్‌లైన్/మొబైల్) బ్యాంకింగ్/చెల్లింపు లావాదేవీలను నిర్వహించేటప్పుడు, అన్ని జాగ్రత్తలు తీసుకోవడం ద్వారా సురక్షితమైన డిజిటల్ బ్యాంకింగ్‌ను అభ్యసించాలనిడిసిబి బ్యాంక్ ప్రజలను కోరుతోంది. ఇవి ఆర్థిక మరియు/లేదా ఇతర నష్టాలను నివారించడంలో సహాయపడతాయి.

సురక్షితమైన డిజిటల్ బ్యాంకింగ్ పద్ధతులు

- ఖాతా నంబర్, లాగిన్ ఐడి, పాస్‌వర్డ్, పిన్, యుపిఐ-పిన్, ఓటిపి, ఏటిఎం/డెబిట్ కార్డ్/క్రెడిట్ కార్డ్ వివరాలను ఎవ్వరితోనూ షేర్ చేయవద్దు, బ్యాంకు అధికారులతో కూడా పంచుకోవద్దు, అవి వాస్తవమైనవిగా అనిపించినా కూడా.
- అప్‌డేట్ చేయలేదనే సాకుతో మీ ఖాతా బ్లాక్ చేయబడుతుందని బెదిరించే ఏదైనా ఫోన్ కాల్/ఇమెయిల్ మరియు దానిని అప్‌డేట్ చేయడానికి లింక్‌ను క్లిక్ చేయమని సూచించడం మోసగాళ్ల సాధారణ కార్యకలాపం. కవైసి అప్‌డేట్ చేయబడిన/వేగవంతంగా పొందడం కోసం ఆఫర్‌లకు ప్రతిస్పందించవద్దు . మీ బ్యాంక్/ఎన్‌బిఎఫ్‌సి/ ఈ-వాలెట్ ప్రొవైడర్ యొక్క అధికారిక వెబ్‌సైట్‌ను ఎల్లప్పుడూ యాక్సెస్ చేయండి లేదా బ్రాంచ్‌ని సంప్రదించండి.
- మీ ఫోన్ లేదా పరికరంలో తెలియని యాప్‌ను డౌన్‌లోడ్ చేయవద్దు. యాప్ మీ గోప్యమైన డేటాను రహస్యంగా యాక్సెస్ చేయవచ్చు.
- డబ్బు రసీదుతో కూడిన లావాదేవీలకు బార్‌కోడ్‌లు లేదా క్యూ ఆర్ కోడ్‌లను స్కాన్ చేయడం లేదా ఎంపిన్‌ని నమోదు చేయడం అవసరం లేదు. అందువల్ల, అలా చేయమని అడిగితే జాగ్రత్త వహించండి.
- సంప్రదింపు వివరాల కోసం ఎల్లప్పుడూ బ్యాంక్/ఎన్‌బిఎఫ్‌సి/ ఈ-వాలెట్ ప్రొవైడర్ యొక్క అధికారిక వెబ్‌సైట్‌ను యాక్సెస్ చేయండి. ఇంటర్నెట్ శోధన ఇంజిన్‌లలోని సంప్రదింపు నంబర్‌లు మోసపూరితంగా ఉండవచ్చు.
- స్పెల్లింగ్ లోపాల కోసం ఇమెయిల్‌లు మరియు ఎస్‌ఎంఎస్‌లో స్వీకరించినయుఆర్‌ఎల్‌లు మరియు డొమైన్ పేర్లను తనిఖీ చేయండి. ఆన్‌లైన్ బ్యాంకింగ్ కోసం ధృవీకరించబడిన, సురక్షితమైన మరియు విశ్వసనీయ వెబ్‌సైట్‌లు మరియు యాప్‌లను మాత్రమే ఉపయోగించండి, అంటే "https"తో ప్రారంభమయ్యే వెబ్‌సైట్‌లు. అనుమానాస్పద యుఆర్‌ఎల్ లేదా వెబ్‌సైట్ వెంటనే స్థానిక పోలీసు/సైబర్ క్రైమ్ శాఖకు తెలియజేయాలి.

- మీరు ప్రారంభించని లావాదేవీ కోసం మీ ఖాతాను డెబిట్ చేయడానికి OTPని స్వీకరించినట్లయితే, వెంటనే మీ బ్యాంక్/ఇ–వాలెట్ ప్రొవైడర్‌కు తెలియజేయండి. లావాదేవీ జరగని కారణంగా మీరు డెబిట్ SMSని స్వీకరిస్తే, వెంటనే మీ బ్యాంక్/ఇ–వాలెట్ ప్రొవైడర్‌కు తెలియజేయండి మరియు యుపిఐతో సహా అన్ని డెబిట్ మోడ్‌లను బ్లాక్ చేయండి. మీరు మీ ఖాతాలో ఏదైనా మోసపూరిత కార్యకలాపాన్ని అనుమానించినట్లయితే, ఇంటర్నెట్/మొబైల్ బ్యాంకింగ్ కోసం ప్రారంభించబడిన లబ్ధిదారుల జాబితాకు అదనంగా తనిఖీ చేయండి.
- మీ బ్యాంక్/ఇ–వాలెట్ ఖాతాకు లింక్ చేయబడిన మీ ఇమెయిల్ పాస్‌వర్డ్‌ను షేర్ చేయవద్దు. ఇ–కామర్స్ /సోషల్ మీడియా సైట్‌ల కోసం సాధారణ పాస్‌వర్డ్‌లు మరియు మీ బ్యాంక్ ఖాతా మరియు ఇమెయిల్‌లు మీ బ్యాంక్ ఖాతాకు లింక్ చేయవద్దు. పబ్లిక్, ఓపెన్ లేదా ఫ్రీ వై–ఫై లేదా ఇంటర్నెట్ నెట్‌వర్క్‌ల ద్వారా బ్యాంకింగ్ చేయడాన్ని నివారించండి.
- ఏదైనా వెబ్‌సైట్/అప్లికేషన్‌లో మీ ఇమెయిల్‌ను యూజర్ ఐడీగా నమోదు చేస్తున్నప్పుడు మీ ఇమెయిల్ పాస్‌వర్డ్‌ను పాస్‌వర్డ్ అనే పదంగా సెట్ చేయవద్దు. మీ ఇమెయిల్‌ను యాక్సెస్ చేయడానికి ఉపయోగించే పాస్‌వర్డ్ ప్రత్యేకించి మీ బ్యాంక్ ఖాతాతో లింక్ చేయబడి ఉంటే, ప్రత్యేకంగా ఉండాలి మరియు ఇమెయిల్ యాక్సెస్ కోసం మాత్రమే ఉపయోగించాలి మరియు ఏదైనా ఇతర వెబ్‌సైట్ లేదా అప్లికేషన్‌ను యాక్సెస్ చేయడానికి కాదు.
- కమీషన్ రసీదులు లేదా లాటరీ విజయాల కోసం ఖాఐలో మీ తరపున డబ్బు డిపాజిట్ చేయమని సలహా ఇవ్వడం ద్వారా తప్పుదారి పట్టించకండి.
- మీ ఆర్థిక సేవా ప్రదాత నుండి హెచ్చరికల కోసం మీ ఇమెయిల్ మరియు ఫోన్ సందేశాలను క్రమం తప్పకుండా తనిఖీ చేయండి. తదుపరి నష్టాన్ని నివారించడానికి కార్డ్ ఖాతా, వాలెట్‌ను బ్లాక్ చేయడం కోసం మీ ఖాతాలో ఏదైనా అధీకృత లావాదేవీని వెంటనే మీ బ్యాంక్/ఎన్‌బిఎఫ్‌సి/సర్వీస్ ప్రొవైడర్‌కు నివేదించండి.
- మీ ఏటిఎం, డెబిట్ మరియు క్రెడిట్ కార్డ్‌లను సురక్షితం చేయండి మరియు లావాదేవీల కోసం రోజువారీ పరిమితిని సెట్ చేయండి. మీరు గృహ/అంతర్జాతీయ ఉపయోగం కోసం పరిమితులను కూడా సెట్ చేయవచ్చు మరియు యాక్టివేట్/నిష్క్రియం చేయవచ్చు. ఇది మోసం వల్ల కలిగే నష్టాన్ని పరిమితం చేయవచ్చు.