ఆన్‌లైన్ భద్రతా అంశాలు మరియు సురక్షిత వినియోగ మార్గదర్శకాలు

మీ ఆన్‌లైన్ బ్యాంకింగ్‌ని సురక్షితంగా ఉంచడంలో మేము ఎలా సహాయపడగలమో ఇక్కడ పేర్కొనబడింది

బ్యాంకుగా భద్రత గురించి ఆలోచించడం అలవాటు చేసుకున్నాం. ఇంటర్నెట్ యొక్క పెరుగుదల మనందరికీ ఎక్కువ సౌలభ్యాన్ని అందించింది, అయితే ఇది కొత్త ప్రమాదాలను కూడా తెస్తుంది. HSBC వద్ద, మేము పరిశ్రమ ప్రామాణిక భద్రతా సాంకేతిక పరిజ్ఞానం మరియు అభ్యాసాలని ఉపయోగిస్తాము, మీ ఖాతాను ఏదైనా అనధికార ప్రాప్యత నుండి రక్షించుకోవడానికి గోప్యత, సాంకేతికత మరియు గుర్తింపు అనే మూడు ముఖ్య రంగాలపై దృష్టి పెడతాము. మీ ఆన్‌లైన్ ఇంటర్నెట్ బ్యాంకింగ్ రక్షించడానికి హెచ్ఎస్‌బిసి ఏమి చేస్తుందో మరియు మీ ఆన్‌లైన్ భద్రతను మెరుగుపరచడానికి మీరు వ్యక్తిగతంగా ఏ చర్యలు తీసుకోవచ్చో కనుగొనండి.

మీ ఆన్‌లైన్ బ్యాంకింగ్ మేము ఎలా రక్షిస్తామో మరియు మీ స్వంత ఆన్‌లైన్ భద్రత మెరుగుపరచడానికి మీరు ఏ చర్య తీసుకోవచ్చో చూడటానికి చదవండి.

మోసం రకాలు

మీ వ్యక్తిగత మరియు భద్రతా వివరాల ఇవ్వడానికి మోసగాడు మిమ్మల్ని మోసగించడానికి అనేక మార్గాలు ఉన్నాయి. అప్పుడు వారు బ్యాంకుతో మీ ఆర్థిక సమాచారాన్ని యాక్సెస్ చేయడానికి ఈ వివరాలని ఉపయోగిస్తారు మరియు మీరు ఖాతా నుండి వారి చెల్లింపులని ఏర్పాటు చేస్తారు.

మీరు ఎదుర్కొనే కొన్ని సాధారణ రకాల మోసాలు ఇక్కడ ఉన్నాయి.

క్రెడిట్ / డెబిట్ కార్డ్ స్కిమ్మింగ్ లేదా క్లోనింగ్

మోసగాళ్ళు మీ క్రెడిట్ లేదా డెబిట్ కార్డ్‌లోని మాగ్నెటిక్ స్ట్రిప్ నుండి సమాచారాన్ని దొంగిలించవచ్చు. ఎటిఎమ్ కార్డ్ యొక్క స్లాట్‌లో స్కిమ్మింగ్ పరికరాలను దాచడం ద్వారా లేదా మీరు వ్యాపారి చెల్లింపు టెర్మినల్స్ వద్ద శ్రద్ధ చూపనప్పుడు వారు దీన్ని చేస్తారు. ఈ పరికరాలు మీ కార్డ్ వివరాలని స్కాన్ చేసి నిల్వ చేస్తాయి. మీ పిన్‌ను దొంగిలించడానికి, మోసగాళ్ళు కెమెరాను వివేకం ఉన్న ప్రదేశంలో లేదా వ్యాపారి స్థాపనలో ఉంచవచ్చు.

యుపిఐ యాప్స్‌లో స్కామ్ లేదా చెల్లింపు మోసాలు

మోసగాళ్ళు మీకు మెసేజింగ్ యాప్స్ ద్వారా క్యూఆర్ కోడ్‌లని పంపవచ్చు, క్యూఆర్ కోడ్ స్కాన్ చేయమని లేదా వారి ఖాతాలోకి డబ్బును బదిలీ చేయడానికి అభ్యర్థనను ఆమోదించమని అడుగుతుంది. మీరు విక్రయిస్తున్న ఉత్పత్తిని వారు కొనాలకుంటున్నారని చెప్పడం వంటి నకిలీ కథను చెప్పడం ద్వారా వారు మిమ్మల్ని మోసగించడానికి ప్రయత్నించవచ్చు. వారు మీ కోసం బ్యాంక్ లేదా షాపింగ్ కంపెనీ ఎగ్జిక్యూటివ్ వలె నటించవచ్చు, వాపసు, క్లెయిమ్ చేయని క్యాష్‌బ్యాక్ ఆఫర్‌లు లేదా రివార్డ్ పాయింట్లను ప్రాసెస్ చేయడానికి ఆఫర్ చేయవచ్చు. సందేహించని బాధితులు అప్పుడు క్యూఆర్ కోడ్‌ను స్కాన్ చేయవచ్చు లేదా వారి UPI పిన్ ఉపయోగించి అభ్యర్థన ఆమోదించవచ్చు, మోసగాడి ఖాతాలోకి డబ్బు బదిలీ అవుతుంది.

వ్యాపార ఇమెయిల్ మరియు మెసేజింగ్ యాప్స్ ద్వారా చెల్లింపు మోసాలు

మోసగాళ్ళు మీ ఇమెయిల్ లేదా చాట్‌లని హ్యాక్ చేయవచ్చు లేదా మీ గురించి మరింత తెలుసుకోవడానికి గుప్తీకరించని సందేశాలని అడ్డగించవచ్చు. వారు మీ గురించి మరింత తెలుసుకున్న తర్వాత, వారు హ్యాక్ చేయబడిన / రాజీపడిన /స్పూఫ్ చేసిన ఐడి నుండి సందేశాలను పంపవచ్చు, ప్రియమైన వ్యక్తిని ఆసుపత్రిలో చేర్చడం లేదా క్రొత్తగా చెల్లించాల్సిన అత్యుత్తమ బిల్లు వంటి చట్టబద్ధమైన ప్రయోజనాల కోసం అత్యవసర చెల్లింపు చేయమని మిమ్మల్ని అడుగుతుంది. ఖాతా. బాధితుల అభ్యర్థన యొక్క ఆవశ్యకత కారణంగా లేదా వారు అభ్యర్థనను విశ్వసించవచ్చని భావించినందున చెల్లింపు చేయడానికి మోసపోవచ్చు. బాధితుడు స్వయంగా చెల్లింపు చేసినందున, బ్యాంక్ వారికి పంపే లావాదేవీ హెచ్చరికల వల్ల వారు అప్రమత్తంగా ఉండరు. ఈ రకమైన మోసాన్ని గుర్తించడం కష్టమవుతుంది.

నకిలీ సంప్రదింపు సంఖ్యలు

మోసగాళ్ళు బ్యాంకులు మరియు సేవా ప్రదాత సంప్రదింపు కేంద్రాల కోసం నకిలీ సంప్రదింపు వివరాలను అందించవచ్చు. సందేహించని బాధితులు సెర్చ్ ఇంజిన్ ఉపయోగించి సంప్రదింపు వివరాల కోసం వెతకవచ్చు మరియు నకిలీ నంబర్‌కు కాల్ చేయవచ్చు. అప్పుడు వారు 'ధృవీకరణ ప్రక్రియ' ద్వారా తీసుకోబడతారు, అక్కడ వారు వారి డెబిట్ / క్రెడిట్ కార్డ్‌లు మరియు బ్యాంక్ ఖాతాల గురించి సున్నితమైన సమాచారాన్ని పంచుకుంటారు.

మీకు అవసరమైన సంప్రదింపు వివరాల కోసం మీరు ఎల్లప్పుడూ బ్యాంక్ లేదా సేవా ప్రదాత యొక్క అధికారిక వెబ్‌సైట్‌ను సందర్శిస్తున్నారని నిర్ధారించుకోవడం ద్వారా మిమ్మల్ని మీరు రక్షించుకోవచ్చు. అప్రమత్తంగా ఉండండి మరియు శోధన ఫలితాల్లో ప్రదర్శించబడే కాల్ నంబర్లను ముందుగా తనిఖీ చేయకుండా నివారించండి, ప్రత్యేకించి అవి మొబైల్ నంబర్ కావచ్చు.

ఇమెయిళ్ళని ఫిషింగ్ లేదా స్పూఫింగ్ చేయడం

మోసగాళ్ళు బాధితులని తమకు వీలైనన్ని ఇమెయిల్ చిరునామాలకు పంపడం ద్వారా ఫిష్ చేయవచ్చు. బ్యాంక్, ఆన్‌లైన్ చెల్లింపు సేవ, చిల్లర లేదా ఇతర సారూప్య సేవ వంటి చట్టబద్ధమైన సంస్థలో భాగమని నటిస్తూ వారు తరచుగా ఇలా చేస్తారు. వారు తమ ఐడిని స్పూఫ్ చేయవచ్చు కాబట్టి ఇమెయిల్ మోసగాడు కాకుండా వేరొక పంపినట్లు కనిపిస్తుంది.

వ్యక్తిగత లేదా ఆర్థిక సమాచారం అడిగే ఇమెయిల్‌లకు ప్రతిస్పందించకుండా ఫిషింగ్ మోసాలకు వ్యతిరేకంగా మిమ్మల్ని మీరు రక్షించుకోవచ్చు. మీరు ఎప్పుడూ అనుమానాస్పద ఇమెయిల్‌లలో లింక్‌లని ఎన్నుకోకూడదు.

మీ వ్యక్తిగత లేదా భద్రతా వివరాలని ఇమెయిల్ ద్వారా వెల్లడించమని హెచ్ఎస్‌బిసి మిమ్మల్ని ఎప్పుడూ అడగదు. మీ హెచ్ఎస్‌బిసి నుండి వచ్చినట్లు చెప్పుకుంటూ అలాంటి ఇమెయిల్ స్వీకరిస్తే, దానికి స్పందించకండి. ఇమెయిల్ వెంటనే తొలగించండి. గుర్తుంచుకోండి, మీ వినియోగదారుల పేరు, పాస్‌వర్డ్ లేదా ఇతర భద్రతా వివరాలు వంటి మీ ఆధారాలని ఎవరితో పంచుకోవద్దు.

మనీ మ్యూల్ లేదా అదనపు ఆదాయం ఇమెయిల్ మోసాలు

మనీ మ్యూల్ కుంభకోణంలో, మోసగాళ్ళు మిమ్మల్ని బదిలీకి సహాయం కోసం అడగవచ్చు. వారు మీ ఖాతాలోకి డబ్బు బదిలీ చేయమని ఆఫర్ చేయవచ్చు, కాబట్టి మీరు దానిని మరొక ఖాతాకు బదిలీ చేయడంలో వారికి సహాయపడగలరు. ప్రతిగా, వారు మీకు కమీషన్ ఇస్తారని వారు చెపుతారు.

మనీలాండరింగ్ వంటి నేరాలకు వారు తరచూ పాల్పడుతున్నందున మీ అలాంటి అభ్యర్థనల విస్మరించాలి. తెలిసి పాల్గొనే ఎవరైనా నేరానికి సహచరుడిగా పరిగణించబడతారు మరియు ప్రాసిక్యూషన్ ఎదుర్కొనవచ్చు. ఇది నిజమని చాలా బావుంది అనిపిస్తే, అది బహుశా భ్రమ కావచ్చు.

అడ్వాన్స్ ఫీజు మోసం ('419' మోసాలు)

మోసగాళ్ళు అవాంఛనీయ లేఖ లేదా ఇమెయిళ్ళను మీకు పంపవచ్చు, సాధారణంగా యుఎస్ డాలర్లలో, పెద్ద మొత్తంలో డబ్బును తరలించడానికి వారికి సహాయం చేసినందుకు మీకు ఉదారంగా బహుమతి ఇస్తారు. ఈ మోసగాళ్ళు నిజంగా మీ బ్యాంకింగ్ వివరాలు. ఒప్పందాన్ని పూర్తి చేయడానికి వారు సాధారణంగా రుసుము, కొన్ని పన్నులు లేదా లంచం చెల్లించమని అడుగుతారు – ఇది ముందస్తు రుసుము. బాధితులు సాధారణంగా మోసగాళ్ళతో దీన్ని కోల్పోతారు.

మీ ఆన్‌లైన్ బ్యాంకింగ్ వివరాలు ఎవరికైనా ఉన్నాయని మీరు అనుమానించినట్లయితే, మీరు ఆన్‌లైన్ బ్యాంకింగ్‌కు లాగిన్ అయి వెంటనే మీ పాస్‌వర్డ్ మార్చాలి. అప్రమత్తం చేయడానికి మీరు వీలైనంత త్వరగా మాకు కాల్ చేయాలి. మా పంక్తులు 24/7* తెరిచి ఉన్నాయి. మీరు మా హాట్‌లైన్ సంఖ్యల జాబితాను ఇక్కడ చూడవచ్చు.

సోషల్ మీడియా హక్స్

ఫేస్‌బుక్, వాట్సాప్ లేదా ఇన్‌స్టాగ్రామ్ వంటి సోషల్ మీడియా ప్లాట్‌ఫామ్‌లలో మోసగాళ్ళు సన్నిహితుడు లేదా బంధువు వలె నటించవచ్చు, డబ్బును అత్యవసరంగా వారికి బదిలీ చేయమని అడుగుతారు. మీకు తెలిసిన వారి నుండి కాల్ ఇవ్వడం ద్వారా లేదా ఇతర ఛానెల్‌ల ద్వారా వారిని సంప్రదించడం ద్వారా అభ్యర్థన చట్టబద్ధమైనదా అని మీరు తనిఖీ చేయవచ్చు.

విషింగ్ కాల్స్

మోసగాళ్ళు బ్యాంక్ సిబ్బంది లేదా కస్టమర్ సర్వీస్ ఎగ్జిక్యూటివ్ వలె నటించవచ్చు మరియు సంభావ్య బాధితులని వారి బ్యాంక్ ఖాతా వివరాలు వంటి సున్నితమైన సమాచారాన్ని దొంగిలించడానికి పిలుస్తారు. బాధితుడి నమ్మకాన్ని గెలవడానికి, నేరస్థులు బాధితుడికి సోషల్ ఇంజనీరింగ్ ద్వారా దొంగిలించబడిన వ్యక్తిగత సమాచారాన్ని అందించవచ్చు. వారు కొంత నమ్మకాన్ని ఏర్పరచుకున్న తరువాత, మోసగాళ్ళు వారి బ్యాంక్ వివరాలు మరియు వన్-టైమ్ పాస్ కోడ్స్ (OTP) లు వంటి వారి రహస్య సమాచారాన్ని అందిస్తారనే ఆశతో, కొన్ని ప్రత్యేక సేవ లేదా ఉత్పత్తిని అందించవచ్చు.

ట్రోజన్ వైరసలు

మీరు తెరవమని అడిగిన ఫైల్స్, పేజీలు లేదా జోడింపులని కలిగి ఉన్న అవాంఛనీయ ఇమెయిల్‌లను మోసగాళ్ళు మీకు పంపవచ్చు. కానీ వాటిని తెరవడం అంటే మీ ఆన్‌లైన్ కార్యాచరణను పర్యవేక్షించే ప్రోగ్రామ్‌ను మీ కంప్యూటర్‌లో రహస్యంగా ఇన్‌స్టాల్ చేస్తుంది మరియు మీ వివిధ వెబ్‌సైట్లలో టైప్ చేసేవి కూడా. కాబట్టి ఆన్‌లైన్‌లో షాపింగ్ చేసేటప్పుడు మీరు మీ క్రెడిట్ కార్డ్ వివరాలను నమోదు చేసినప్పుడు, మోసగాళ్ళు మీరు నమోదు చేసిన సమాచారాన్ని చూడగలరు.

ఆన్‌లైన్ భద్రత కోసం హెచ్ఎస్‌బిసి తీసుకున్న చర్యలు

మల్టి-లేయర్ లాగ్ ఆన్ ధృవీకరణ

మీ ఆర్థిక సమాచారం ప్రత్యేకమైన వినియోగదారుడు పేరు మరియు పాస్‌వర్డ్ యొక్క అధునాతన కలయికతో పాటు మీ భౌతిక భద్రతా పరికరం లేదా డిజిటల్ సురక్షిత కీ ద్వారా ఉత్పత్తి చేయబడిన ఒక-సమయం భద్రతా కోడ్ ద్వారా రక్షించబడుతుంది.

లావాదేవీ ధృవీకరణ

కార్డులపై 3డి సురక్షత లావాదేవీలు, భద్రతా లావాదేవీలు మరియు చెల్లింపు వ్యవస్థపై నమ్మకాన్ని పొందటానికి సహాయపడతాయి. లావాదేవీల కోసం ఉత్పత్తి చేయబడిన OTP లను ఎవరితో పంచుకోవద్దు.

128-బిట్ సెక్యూర్ సాకెట్ లేయర్ (ఎస్ఎస్ఎల్) ఎన్క్రిప్షన్

ఇంటర్నెట్ బ్యాంకింగ్ సెషన్‌లో ప్రసారం చేయబడిన సమాచారం కోసం హెచ్ఎస్‌బిసి 128-బిట్ సెక్యూర్ సాకెట్ లేయర్ (ఎస్ఎస్ఎల్) గుప్తీకరణ ఉపయోగిస్తుంది, ఇది గుప్తీకరణకు ఇండస్ట్రీ స్టాండర్డ్ ప్రమాణంగా అంగీకరించబడుతుంది.

స్వయంచాలక 'టైం-అవుట్' అంశాలు

భద్రతా ప్రమాణంగా, మీ ఇంటర్నెట్ బ్యాంకింగ్ సెషన్ ఉపయోగించబడని కాలం తర్వాత స్వయంచాలకంగా మూసివేయబడడం లేదా టైం-అవుట్ అవుతుంది. మీరు పూర్తి చేసిన తర్వాత మీ ఇంటర్నెట్ బ్యాంకింగ్ సెషన్‌ను ఎల్లప్పుడూ మూసివేయాలి.

భద్రతా పరికరం / డిజిటల్ సురక్షితమైన కీ

మీ భౌతిక భద్రతా పరికరం/డిజిటల్ సురక్షిత కీ ఆన్‌లైన్ భద్రతని ఉన్నత స్థాయికి తీసుకువెళుతుంది. మీ ఖాతాకు లాగిన్ అవ్వడానికి మీరు యధావిధిగా మీ ప్రస్తుత వినియోగదారుడు పేరు మరియు పాస్‌వర్డ్‌ను నమోదు చేయాలి, తరువాత మీ భౌతిక భద్రతా పరికరం లేదా మీ డిజిటల్ సురక్షిత కీ ద్వారా సృష్టించబడిన ప్రత్యేకమైన భద్రతా కోడ్‌ను నమోదు చేయాలి. ఈ 2 దశల ప్రామాణీకరణ ప్రక్రియ మీరు మీ ఇంటర్నెట్ బ్యాంకింగ్‌ని యాక్సెస్ చేసినపుడు మెరుగైన స్థాయి భద్రతను అందిస్తుంది.

ఆన్‌లైన్ భద్రతలో మీ పాత్ర

ఇంటర్నెట్ బ్యాంకింగ్ భద్రతని నిర్ధారించుకోవడానికి చేయవలసినవి మరియు చేయకూడని వాటిని అనుసరించండి

చేయవలసినవి

- మీ కంప్యూటర్ అన్ని సమయాల్లోఇటీవలి యాంటీ-వైరస్ మరియు ఫైర్‌వాల్ రక్షణ సాఫ్ట్‌వేర్‌తో రక్షించబడిందని నిర్ధారించుకోండి. మీకు తాజా రక్షణ ఉందని నిర్ధారించడానికి క్రమం తప్పకుండా నవీకరణల డౌన్‌లోడ్ చేయండి.
- మీకు గుర్తుండిపోయే పాస్‌వర్డ్‌ని ఎంచుకోండి, కానీ మరొకరు ఊహించగలిగే పాస్‌వర్డ్‌ని ఎంచుకోవద్దు. ఆల్ఫా మరియు సంఖ్యా అక్షరాల కలయికల కలిగి ఉన్న పాస్‌వర్డ్ సాధారణంగా ఊహించడం కష్టం (ఉదా. A7g3cy91)
- మీ ఇతర సేవలకు ఉపయోగించే పాస్‌వర్డ్‌ని ఎంచుకోవద్దు. మీ పాస్‌వర్డ్ ఇంటర్నెట్ బ్యాంకింగ్ కొరకు ప్రత్యేకంగా ఉండాలి.
- ఫిషింగ్ ఇమెయిళ్ళ పట్ల జాగ్రత్త వహించండి. అన్ని అక్షరాలు మరియు కారక్టర్స్‌తో సహా మొత్తం ఇమెయిల్ అడ్రస్‌ని ఎల్లప్పుడూ జాగ్రత్తగా చదవండి.
- ఫిషింగ్ ఇమెయిల్ చిరునామాలని పోలి ఉంటుంది. ఉదా. hsdc.co.in లేదా hsbcbank.com. మీ మౌస్ పాయింటర్‌ని దాని నిజమైన గమ్యాన్ని బహిర్గతం చేయడానికి URL పై రోల్ చేయండి; ఇది మీ బ్రౌజర్ దిగువ ఎడమ మూలలో ప్రదర్శించబడుతుంది. అసమతుల్యత ఉంటే లింక్‌పై క్లిక్ చేయవద్దు. URL లోని స్పెల్లింగ్ తప్పులు, చెడు వ్యాకరణం లేదా అక్షరాల గందరగోళం వంటి సంకేతాల కోసం చూడండి
- మీ ఖాతా అవసరం లేకపోతే అదనపు లబ్ధిదారులను తొలగించండి
- మీ కంప్యూటర్ లేదా లాగాన్ వివరాలని గుర్తుంచుకునే బ్రౌజర్‌లలో కార్యాచరణ నిలిపివేయండి
- మీ సిస్టమ్ మరియు వెబ్ బ్రౌజర్ నవీకరించండి. తయారీదారులు తమ వ్యవస్థలు మరియు బ్రౌజర్‌లలో బలహీనతలని కనుగొన్నప్పుడు భద్రతా పాచెస్‌ని క్రమం తప్పకుండా విడుదల చేస్తారు. ఈ నవీకరణల కోసం రోజూ మీ సాఫ్ట్‌వేర్ ప్రొవైడర్‌తో తనిఖీ చేయండి.
- బ్యాంక్ వెబ్‌సైట్ చేరుకోవడానికి ఎల్లప్పుడూ బ్రౌజర్‌లో బ్యాంక్ URL ని టైప్ చేయండి.
- ప్యాడ్‌లాక్‌తో మరియు సైట్ ప్రమాణపత్రాన్ని తనిఖీ చేయండి. సైట్ సర్టిఫికేట్ HSBC కి చెందినదని నిర్ధారించడానికి మీ HSBC ఆన్‌లైన్ బ్యాంకింగ్‌కు లాగిన్ అయినప్పుడు మీ బ్రౌజర్ దిగువన ఉన్న ప్యాడ్‌లాక్ గుర్తుపై రెండుసార్లు క్లిక్ చేయండి. 'నకిలీ' సైట్‌లో మీ వివరాలని నమోదు చేయడంలో మీరు మోసపోకుండా ఇది నిర్ధారిస్తుంది.
- మీ ఖాతాలని క్రమం తప్పకుండా తనిఖీ చేయండి. ఏదైనా లావాదేవీలపై అనుమానం ఉంటే, వివరాలని గమనించండి మరియు మాకు కాల్ చేయండి.
- ఆన్‌లైన్ బ్యాంకింగ్ ఉపయోగించిన తర్వాత ఎల్లప్పుడూ లాగ్-అవుట్ చేయండి. లాగ్-అవుట్ బటన్ ఎంచుకోండి మరియు మీ సేవకు లాగిన్ అయినప్పుడు మీ PC ని ఎప్పుడూ గమనించకుండా ఉంచండి.
- మీ బ్యాంకుల కస్టమర్ కేర్ నంబర్లు, ఆన్‌లైన్ షాపింగ్ వెబ్‌సైట్ మొదలైన వాటి కోసం చూసుక ఎన్నట్లయితే ఇంటర్నెట్‌లో తెలివిగా శోధించండి. మోసపూరిత శోధనలు వాటిని నిర్వహించే మొబైల్ నంబర్లతో ఫలితాలని ఇవ్వడానికి తారు మారు చేస్తాయి. బ్యాంక్ కస్టమర్ కేర్ నంబర్ లేదా ఇ-కామర్స్ వెబ్‌సైట్‌కు బదులుగా మోసగాడిని పిలవడానికి మీరు మోసపోవచ్చు.
- మీ పరికరాల్లో మీ బ్యాంక్ సంప్రదింపు కేంద్రం సంఖ్య నిల్వ చేయండి లేదా మీ క్రెడిట్ / డెబిట్ కార్డ్ వెనుక వ్రాసిన సంఖ్యని చూడండి.
- మీ వ్యక్తిగత కంప్యూటర్ లేదా మొబైల్ పరికరాల్లో స్క్రీన్ షేరింగ్ అప్లికేషన్ల విషయంలో జాగ్రత్తగా ఉండండి. అటువంటి అవర్తనాల డౌన్‌లోడ్ చేయడానికి మోసగాడు మిమ్మల్ని మోసగించి, మీ నుండి కోడ్ కోరడం ద్వారా ప్రాప్యత పొందండి. ప్రాప్యత అనుమతించబడిన తర్వాత, వారు మీ పరికరాన్ని రిమోట్‌గా చూస్తారు, నియంత్రిస్తారు మీ ఖాతాల నుండి చెల్లింపుల కూడా అమలు చేయవచ్చు.
- మీ ఇంటర్నెట్ కనెక్షన్‌ను భద్రపరచండి. పాస్‌వర్డ్‌తో మీ ఇంటి వైర్‌లెస్ నెట్‌వర్క్ ఎల్లప్పుడూ రక్షించండి
- కమీషన్ లేదా సహాయం కోసం కూడా మీ ఖాతాలో డబ్బు వసూలు చేయాల్సిన పథకం / ఆఫర్‌ల పట్ల జాగ్రత్తగా ఉండండి. వారు మోసగాళ్ళు మీ ఖాతాలోకి వచ్చిన నేరాల పంపవచ్చు మరియు డబ్బును బదిలీ చేయమని లేదా వారికి నగదు అందించమని మిమ్మల్ని అడగవచ్చు. మోసగాడు డబ్బు బాటలో తమని తాము కోరుకోరు మరియు మిమ్మల్ని డబ్బు పుట్టగా ఉపయోగించుకోవచ్చు.
- మోసాన్ని తెలియపరచడానికి వెంటనే బ్యాంకు సంప్రదించండి.

చేయకూడనివి

- మీ ఇతర సేవలకు ఉపయోగించే పాస్‌వర్డ్‌ని ఎంచుకోవద్దు. మీ పాస్‌వర్డ్ ఇంటర్నెట్ బ్యాంకింగ్ కొరకు ప్రత్యేకంగా ఉండాలి.
- ఇమెయిల్ / SMS లోని లింక్ అనుకోకుండా క్లిక్ చేసినప్పుడు తెరవబడే వెబ్‌పేజీలలో యూజర్‌ఐడి, పాస్‌వర్డ్, కార్డ్ నంబర్, గడువు తేదీ సివివి మొదలైన వివరాలని వెల్లడించవద్దు.
- బ్యాంక్ ఉద్యోగుల నుండి లేదా I.T వంటి ప్రభుత్వ సంస్థల నుండి వచ్చినట్లు పేర్కొన్నప్పటికీ, అటువంటి వివరాలను అడిగే సందేశాలకు స్పందించవద్దు. డిపార్ట్మెంట్, ఆర్ బి

ఐ మొదలైనవి. హెచ్ఎస్‌బిసి మెంబర్ మీకు ఎప్పుడూ కాల్ చేయరు మరియు వీటిని అడగరు.

- మీ ఇంటర్నెట్ బ్యాంకింగ్ వినియోగదారుని పేరు తర్వాత మీ పాస్‌వర్డ్‌ని కలిసి వ్రాయవద్దు. మీ పాస్‌వర్డ్‌ని గుర్తించదగిన ఆకృతిలో వ్రాయవద్దు మరియు మీ భౌతిక భద్రతా పరికరం / డిజిటల్ సురక్షిత కీతో మీ లాగాన్ వివరాలని ఎప్పుడూ ఉంచవద్దు.
- మీ మొబైల్ బ్యాంకింగ్ అప్లికేషన్‌ని నవీకరించండి. దీన్ని డౌన్‌లోడ్ చేయడానికి మరియు దానిపై ఏదైనా నవీకరణలు చేయడానికి, మీ పరికరం యొక్క అధికారిక యాప్ స్టోర్‌ని చూడండి
- ఆన్‌లైన్ వెబ్‌సైట్లలో కార్డ్ నంబర్ మరియు గడువు తేదీల నిల్వ చేయడంలో జాగ్రత్తగా ఉండండి. అరుదుగా ఉపయోగించే వెబ్‌సైట్ల యొక్క నమ్మదగని వెబ్‌సైట్లలో ఈ వివరాలను నిల్వ చేయవద్దు.
- నమ్మకం లేని సోర్సెస్ నుండి ఇమెయిల్‌లలోని లింక్‌ల నుండి మొబైల్ బ్యాంకింగ్ / చెల్లింపు అవర్తనాలను ఎప్పుడూ డౌన్‌లోడ్ చేయవద్దు

మీ యుపిఐ పిన్‌ని ఎవరైనా అడిగితే, గుర్తుంచుకోండి, మీరు చెల్లింపు చేస్తున్నారు. చెల్లింపుని స్వీకరించడానికి మీకు యుపిఐ పిన్ అవసరం లేదు.

పబ్లిక్ కంప్యూటర్ల ఉపయోగిస్తున్నప్పుడు అప్రమత్తంగా ఉండండి

ఎల్లప్పుడూ

- మీరు కంప్యూటర్ ఆపేయాలనుకుంటే లాగవుట్ అవ్వండి, ఒక్క క్షణం అయినా లాగ్ అవుట్ అవ్వాలి. వీలైతే, మీరు లాగిన్ అయినప్పుడు కంప్యూటర్ గమనించకుండా వదిలి వెళ్ళద్దు.
- మీరు కంప్యూటర్ నుండి లాగ్ అవుట్ అవ్వడానికి ముందు మీ బ్రౌజింగ్ చరిత్రను తొలగించండి: ఇంటర్నెట్ బ్రౌజర్ మీ పాస్‌వర్డ్ మరియు మీ సందర్శించే పేజీల గురించి సమాచారాన్ని నిల్వ చేస్తాయి. ఇంటర్నెట్ బ్రౌజర్ యొక్క సాధనాల మెనుకి వెళ్లి ఎంపిక లేదా ఇంటర్నెట్ ఎంపికలని ఎంచుకోండి. బ్రౌజర్‌లో ఏదైనా ఆటో కంప్లీట్ ఫంక్షన్ ఆపివేయబడిందని నిర్ధారించుకోండి, ఏదైనా కుకీస్ ఉంటే తొలగించండి మరియు హిస్టరీని క్లియర్ చేయండి.
- లైబ్రరీలు, ఇంటర్నెట్ కేఫ్‌లు మరియు పాఠశాలలతో సహా మీ బ్యాంకింగ్‌కు సహాయం చేయగలిగితే పబ్లిక్ కంప్యూటర్లని ఉపయోగించకుండా ఉండటానికి ప్రయత్నించండి.

సున్నితమైన సమాచారాన్ని టైప్ చేయడం మానుకోండి. మీరు అన్ని జాగ్రత్త పాటిస్తున్నప్పటికీ, పబ్లిక్ కంప్యూటర్‌లో కీస్ట్రోక్ లాగర్ అని పిలువబడే హానికరమైన సాఫ్ట్‌వేర్ ఉండవచ్చు. ఈ ప్రోగ్రామ్‌లు మీ పాస్‌వర్డ్, క్రెడిట్ కార్డ్ నంబర్ మరియు బ్యాంక్ వివరాలను దొంగిలించగలవు. సున్నితమైన సమాచారాన్ని బహిర్గతం చేసే ఆర్థిక లావాదేవీ చేయకుండా ఉండండి.

ముఖ్యమైన విషయం – మీరు ఎప్పుడైనా హెచ్ఎస్‌బిసి అని చెప్పుకునే నమ్మదగని మూలం నుండి ఇమెయిల్ లేదా వ్యక్తిగత సమాచారం కోరుతున్న అయాచిత ఇమెయిల్ నుండి అందుకుంటే; మరింత దర్యాప్తు చేయడానికి వాటిని **phishing@hsbc.com** కు రిపోర్ట్ చేయండి.