ఎక్కడ చూసినా మోసగాళ్లే

జాగ్రత్తగా ఉండండి, ఎక్కడా మోసపోకండి!

#BankingDhyaanSe 2.0

AXIS BANK

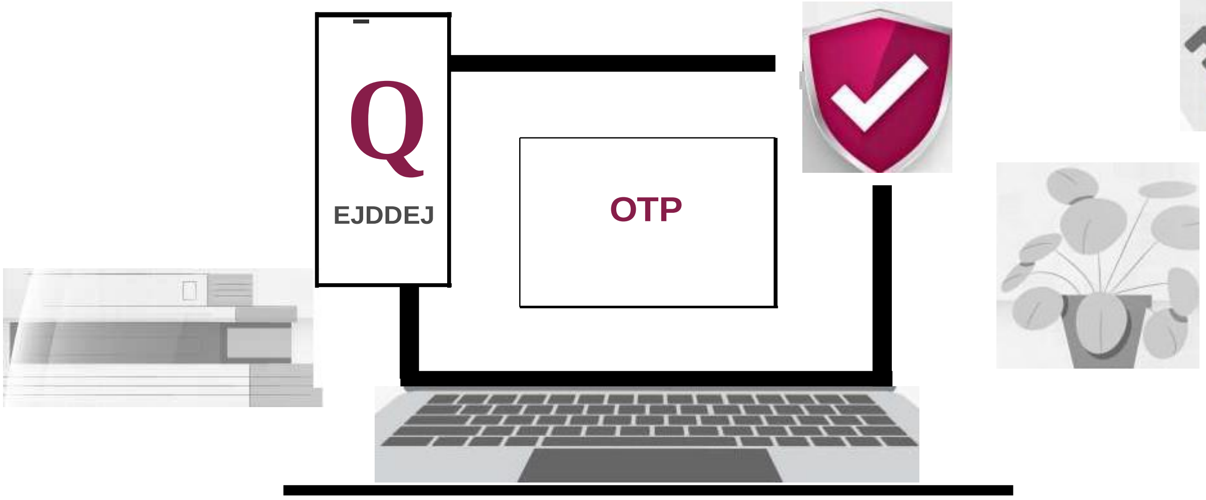
మీరు సంపాదించడానికి కష్టపడుతున్నారు, అయితే మీ సంపాదనను సురక్షితంగా ఉంచుకోకూడదా?

యాక్సిస్ బ్యాంక్ ఫ్రాడ్ అవేర్‌నెస్ బుక్ లెట్ #BankingDhyaanSe 2.0కు స్వాగతం,

ఆర్థిక మోసాలను అర్థం చేసుకోవడానికి మరియు వాటిని నివారించడానికి మీకు ఈ పుస్తకం ఉపయోగపడుతుంది. వేగంగా మారుతున్న డిజిటల్ యుగంలో, మోసగాళ్ల నుంచి రక్షణకు మీ జ్ఞానం నే మీ కవచం. ఈ మార్గదర్శక పుస్తకం మీ కష్టపడి సంపాదించిన డబ్బును కాపాడుకోవడానికి విశ్లేషణలు, వాస్తవ జీవన ఉదాహరణలు, మరియు అనువైన చిట్కాలను అందిస్తుంది

బ్యాంకింగ్ లో మీ నమ్మకమైన భాగస్వామిగా, యాక్సిస్ బ్యాంక్ డిజిటల్ ల్యాండ్ స్కేప్ ను ఆత్మవిశ్వాసంతో నావిగేట్ చేయడంలో మీకు సహాయపడటానికి అంకితం చేయబడింది. మోసానికి దూరంగా ఉంటూ ఉజ్వలమైన ఆర్థిక భవిష్యత్తును అందరం కలిసి భద్రపరుచుకుందాం.

OTP మోసాలు



వన్ టైమ్ పాస్ వర్డ్ అనేది మీ డిజిటల్ కింగ్ డమ్ ను యాక్సెస్ చేయడానికి గోల్డెన్ కీ.

మీ అమూల్యమైన కీ ని మోసగాళ్ల నుండి రక్షించాలంటే, మీరే కాపలాదారుగా ఉండాలి!"

II
lttl1
w
0

OTPలను గోప్యంగా ఉంచండి: ఫోన్ కాల్స్, ఇ-మెయిల్స్, టెక్స్ట్ మెసేజెస్ లేదా సోషల్ మీడియా ద్వారా ఎవరితోనైనా OTPలను పంచుకోవద్దు మరియు జాగ్రత్తగా కాపలా కాస్తున్న గార్డులా అప్రమత్తంగా ఉండండి.

అభ్యర్థనలను ధృవీకరించండి: విశ్వసించండి, కాని ధృవీకరించండి. ఆకస్మికంగా OTP రిక్వెస్ట్ వస్తే లేదా అనుమానాస్పదంగా అనిపిస్తే తొందరపడకండి. మీరు ప్రతిస్పందించే ముందు దాని ప్రామాణికతను రెండుసార్లు తనిఖీ చేయండి.

00

అధికారిక వెబ్సైట్లు లేదా యాప్స్ను ఉపయోగించండి: OTPలను పంచేటప్పుడు సురక్షితంగా ఉండండి. ఎప్పుడూ అధికారిక సైట్ లేదా యాప్‌కు నేరుగా వెళ్ళండి - ఎలాంటి షార్ట్‌కట్‌లకు పోవద్దు. లింక్ క్లిక్ చేయడం కన్నా టైప్ చేయడం ఎప్పటికీ మెరుగైనది.

తక్షణ అభ్యర్థనల విషయంలో జాగ్రత్తగా ఉండండి: మోసగాళ్లు చాలా సార్లు మీపై ఒత్తిడి తీసుకురావడానికి అత్యవసర పరిస్థితిని సృష్టిస్తారు, తద్వారా మీరు మీ OTPను పంచుకోవాలని ప్రయత్నిస్తారు. కొంచెం వెనక్కి తగ్గి, ఆలోచించండి, మరియు చర్య తీసుకునే ముందు స్వతంత్రంగా ఆ అభ్యర్థనను ధృవీకరించండి.

టూ ఫ్యాక్టర్ అథెంటికేషన్ ఎనేబుల్ చేయండి: 2FA (టూ ఫ్యాక్టర్ ఆథెంటికేషన్)తో సెక్యూరిటీని రెట్టింపు చేయండి. యాప్ ఆధారిత లేదా హార్డ్వేర్ టోకెన్లు వంటి రాక్-సాలిడ్ ఎంపికలను ఎంచుకోండి. ఏ రోజైనా SMS, OTPలను అధికమిస్తాయి.

దయచేసి గుర్తుంచుకోండి, బ్యాంక్ మీ CVV, OTP, PIN, కార్డ్ నెంబరు, పాస్‌వర్డ్ లు మొదలైన వాటిని అడగదు. ఈ వివరాలను ఎవరితోనూ పంచుకోవద్దు.

క్రెడిట్ కార్డు మోసాలు

క్రెడిట్ కార్డ్ కుంభకోణాలను దాచిపెట్టే ఒక స్నీక్ గేమ్ గా ఊహించుకుందాం. ఒక స్కామర్ వారి నిజమైన ఉద్దేశాలను దాచడానికి ఎలా ప్రయత్నిస్తాడో, వారు మీ క్రెడిట్ కార్డ్ సమాచారాన్ని బహిర్గతం చేయడానికి మిమ్మల్ని మోసం చేయవచ్చు.

వారి ఉచ్చులో పడకుండా ఉండటానికి, ఈ చిట్కాలను గుర్తుంచుకోండి:

ఫిషర్ల పట్ల జాగ్రత్త: స్కామర్లు మీ బ్యాంకు లేదా తెలిసిన కంపెనీకి చెందిన వారిగా నటించవచ్చు. వారి ట్రిక్కులకు లొంగకండి. వారి గుర్తింపును ధృవీకరించండి.

మీ స్టేట్‌మెంట్లను తనిఖీ చేయండి: మీ క్రెడిట్ కార్డ్ స్టేట్‌మెంట్లను నిరంతరం సమీక్షించండి. అపరిచిత వ్యయాలు లేదా చార్జీలను గమనిస్తే, అది ఆటలో దాచిన ఆటగాళ్లను కనుగొన్నట్లే వాటిని వెంటనే పరిష్కరించండి.

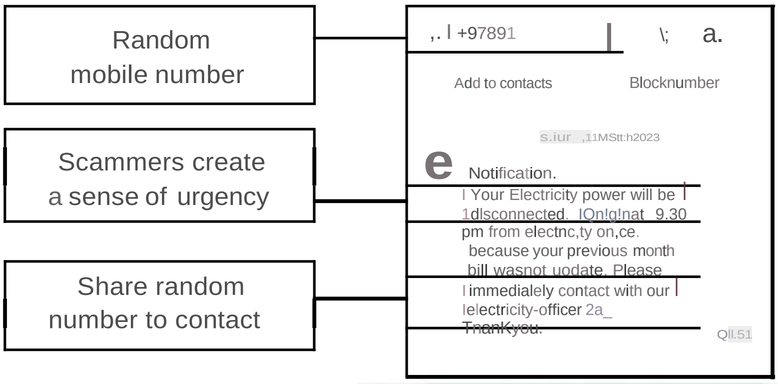
లావాదేవీ పరిమితులను సెట్ చేయండి: మీ అన్ని చెల్లింపు ఛానెళ్లలో లావాదేవీ పరిమితులను సెట్ చేయండి మరియు మీ అవసరానికి అనుగుణంగా 'వినియోగాన్ని నిర్వహించు' విభాగాన్ని అనుకూలీకరించండి.

సురక్షిత సైట్లు మాత్రమే: ఆన్‌లైన్‌లో షాపింగ్ చేసేటప్పుడు, వెబ్‌సైట్ సురక్షితంగా ఉందని నిర్ధారించుకోండి (URLలో "https" కోసం చూడండి). ఇది ఆట కోసం సురక్షితమైన ఆటస్థలాన్ని ఎంచుకోవడం వంటిది.

అప్‌డేట్‌గా ఉండండి: మీరు ఆటలో కొత్త వ్యూహాలను నేర్చుకున్నట్లే, తాజా స్కామ్ వ్యూహాలపై ఓ కన్నేసి ఉంచండి. ఈ విధంగా, మీరు స్కామర్లను అధిగమించడానికి సిద్ధంగా ఉంటారు.

విద్యుత్ బిల్లుల మోసాలు..

నకిలీ SMSను ఎలా గుర్తించాలి?



దీన్ని ఊహించండి: మీరు ఇంట్లో సాయంత్రం సేదతీరుతూ, మీ ఇష్టమైన షోను చూస్తూ ఆనందిస్తుంటే, మీ ఫోన్ బజ్ అవుతుంది, ఒక సందేశం వచ్చింది. అది మీ విద్యుత్ సరఫరాదారు నుండి వచ్చింది, మరియు వారు మీ తాజా బిల్లు కోసం అధిక మొత్తాన్ని మీరు బకాయి అని చెబుతున్నారు.

మీరు భయపడే ముందు, దీనిని పరిగణించండి: విద్యుత్ బిల్లు మోసం, ఒక రహస్య దెయ్యంలా, హెచ్చరిక లేకుండా మీ జీవితంలోకి చొచ్చుకుపోతుంది.

మీ గోప్యమైన వివరాలను ఎవరితోనూ పంచుకోవద్దు లేదా అవాంఛిత లింకులపై క్లిక్ చేయవద్దు.

బిల్లు చెల్లింపులు చేయడానికి అధికారిక మరియు సురక్షితమైన వెబ్‌సైట్‌లను మాత్రమే ఉపయోగించండి.

గుర్తుంచుకోండి, విద్యుత్ శాఖ ఎప్పుడూ వ్యక్తిగత వివరాలు లేదా చెల్లింపులను యాదృచ్ఛిక / నమోదు చేయని నంబర్ల ద్వారా అడగదు.

ఉద్యోగ మోసాలు

ఊహించండి మీరు ఉద్యోగ జాబితాలను స్క్రోల్ చేస్తుంటే, అకస్మాత్తుగా నిజం కావడం అసంభవంగా కనిపించే ఒక ఉద్యోగ ఆఫర్ మీ కంటబడింది. అసంఖ్యాక సెలవులు, పజామాల్లో పని చేయడం, మరియు డేటా ఎంట్రీ కోసం ఆరు అంకెల జీతం? సైన్ అప్ చేయండి!

ఒక్కసారి ఆలోచించండి "అప్లై నౌ" బటన్ నొక్కే ముందు!

కంపెనీని పరిశీలించండి: ఆన్‌లైన్‌లో కంపెనీని వెతికి, అది విశ్వసనీయమైనదో కాదో నిర్ధారించుకోండి. మోసగాళ్లు తరచుగా నమ్మించే వెబ్‌సైట్లతో నకిలీ కంపెనీలను సృష్టిస్తారు.

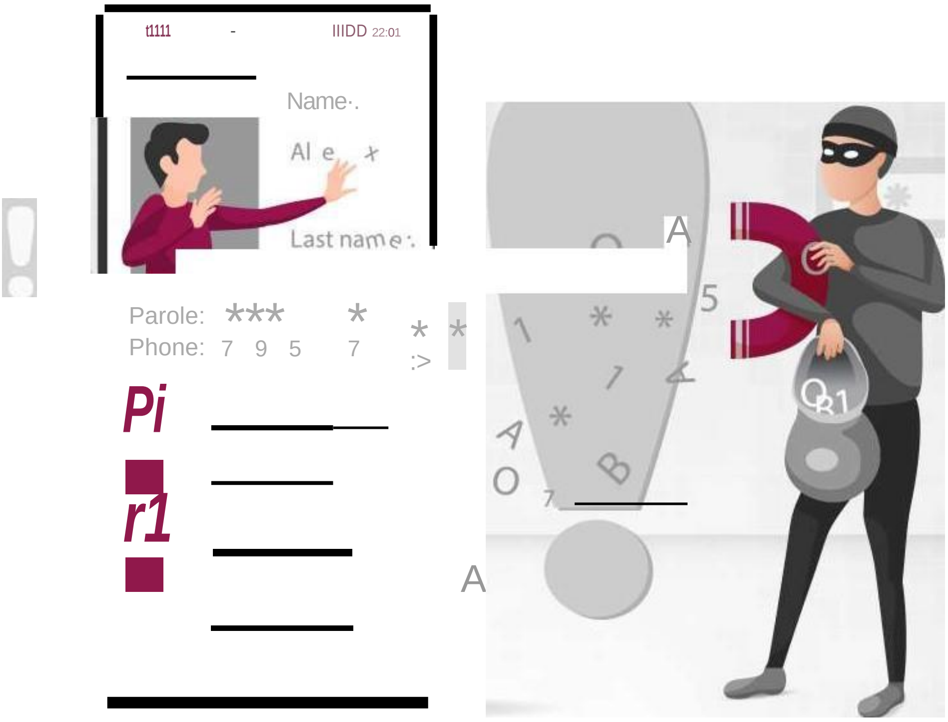
ముందస్తుగా చెల్లించవద్దు: మీరు పనిచేయడం ప్రారంభించడానికి ముందు శిక్షణ, మెటీరియల్స్ లేదా నేపథ్య తనిఖీల కోసం చెల్లించమని చట్టబద్ధమైన యజమానులు మిమ్మల్ని అడగరు.

రెడ్ ఫ్లాగ్స్ కోసం చూడండి: ఉద్యోగంలో మీ సోషల్ సెక్యూరిటీ నంబర్ లేదా ఆర్థిక వివరాలు వంటి సున్నితమైన సమాచారాన్ని వెంటనే అందించాల్సి వస్తే జాగ్రత్తగా ఉండండి.
చాలా త్వరగా ఉద్యోగంలో చేరండి: ఇంటర్వ్యూ లేదా ఎక్కువ సమాచారం మార్పిడి చేయకుండా మీకు అక్కడికక్కడే ఉద్యోగం ఆఫర్ చేస్తే, అది స్కామ్ కావచ్చు.

మీ అభిప్రాయాన్ని నమ్మండి: ఏదైనా అనుమానంగా అనిపిస్తే, మీ హృదయాన్ని నమ్మి జాగ్రత్తగా ముందుకు వెళ్లండి లేదా దానిని వదిలేయండి.

గుర్తుంచుకోండి, ఉద్యోగాలను వెతికేటప్పుడు మీ వ్యక్తిగత మరియు ఆర్థిక సమాచారాన్ని రక్షించుకోవడం మీ మొదటి ప్రాధాన్యత కావాలి.

నకిలీ కాల్ మోసాలు

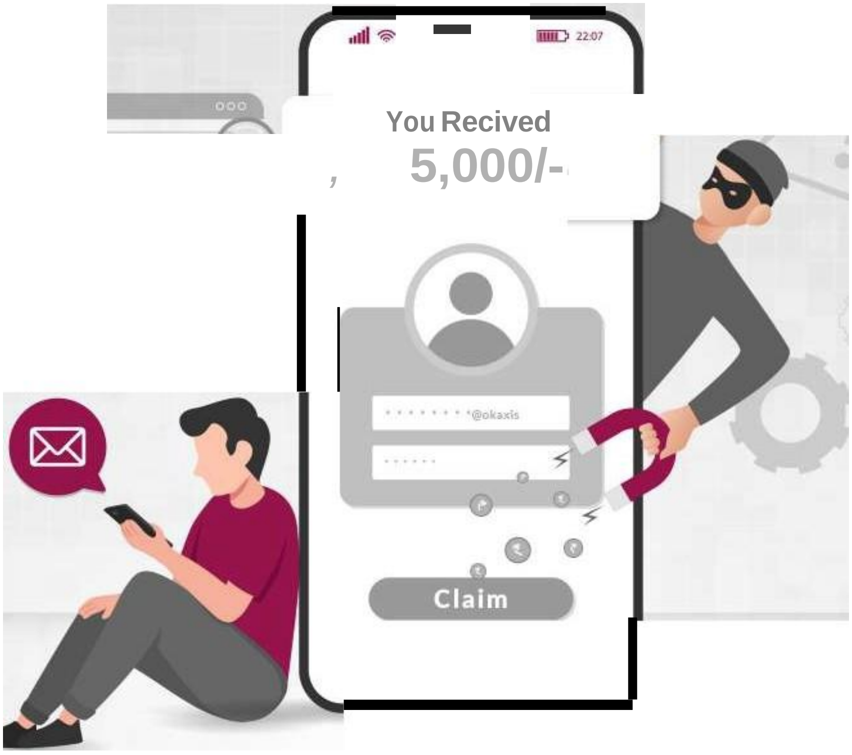


ఒక మాంత్రికుడు విషయాలను వాస్తవంగా ఉన్న దానికంటే భిన్నంగా ఎలా చూపించగలడో, స్కామర్లు మీకు తెలిసిన లేదా విశ్వసించే వ్యక్తిగా అనిపించడానికి మీ కాలర్ ఐడిని తారుమారు చేయవచ్చు - ఈ సందర్భంలో, వారిని మీ బ్యాంక్అధికారిలాగా చూపించగలరు. ఇది వారి నిజమైన గుర్తింపు కోసం డిజిటల్ మారువేషం లాంటిది.
ఈ స్నీకీ ట్రిక్ నుండి మిమ్మల్ని మీరు రక్షించుకోవడానికి, ఈ చిట్కాలను గుర్తుంచుకోండి:

జాగ్రత్తతో ధృవీకరించండి: కాలర్ ఐడీ పరిచితంగా అనిపించినా, సందేహంతో ఉండండి. ఎవరైనా సున్నితమైన సమాచారం అడిగితే, వారి గుర్తింపును ఇతర మార్గాల్లో రెండుసార్లు తనిఖీ చేయండి.
వ్యక్తిగత సమాచారం పంచవద్దు: కాలర్ నమ్మదగినవారిలా కనిపించినా, ఫోన్ ద్వారా వ్యక్తిగత లేదా ఆర్థిక సమాచారాన్ని ఎప్పుడూ పంచవద్దు. ఫోన్ పెట్టి, నమ్మకమైన నంబర్ ఉపయోగించి తిరిగి కాల్ చేయండి.
గోప్యతను కాపాడుకోండి: మీరు ఆన్‌లైన్ లేదా సోషల్ మీడియాలో పంచుకునే వ్యక్తిగత వివరాల విషయంలో జాగ్రత్తగా ఉండండి. మోసగాళ్లు తరచుగా ఈ వనరుల నుండి సమాచారాన్ని సేకరించి, తమ నకిలీ కాల్స్‌ను మరింత నమ్మదగినట్లుగా చూపిస్తారు.
కాల్ బ్లాకింగ్‌ను ఉపయోగించండి: మీ ఫోన్ క్యారియర్ అందించే కాల్-బ్లాకింగ్ యాప్స్ లేదా ఫీచర్లను పరిశీలించండి. అవి మోసపూరిత కాల్స్‌ను ఫిల్టర్ చేయడంలో సహాయపడతాయి.

గూగుల్ లో కానీ, సెర్చ్ ఇంజిన్ లో కానీ ఫోన్ నంబర్ల కోసం సెర్చ్ చేయవద్దు. ఒకవేళ మీరు అలా చేస్తే, సంస్థ లేదా వ్యాపారి మీకు పంపిన ఏదైనా లింక్ లను క్లిక్ చేయవద్దు.
అదనంగా, అధీకృత అప్లికేషన్ స్టోర్ ల నుండి మాత్రమే మీ పరికరాల్లో బ్యాంకింగ్ అప్లికేషన్ ల యొక్క తాజా వెర్షన్ లు డౌన్‌లోడ్ చేయబడ్డాయని దయచేసి ధృవీకరించుకోండి.
దయచేసి దీనిని క్రమానుగతంగా తనిఖీ చేయండి.
గుర్తుంచుకోండి, మీరు నిజ జీవితంలో ముసుగు ధరించిన అపరిచితుడిని నమ్మనట్లే, ఫోన్లో ముసుగు ధరించిన వ్యక్తిని నమ్మవద్దు. అప్రమత్తంగా ఉండండి!

UPI రిఫండ్ మోసాలు



ఊహించండి, మీరు మీ ఫోన్‌లో స్క్రోల్ చేస్తుండగా, UPI రిఫండ్ నోటిఫికేషన్ కనిపిస్తుంది, మరియు ఒక్కసారిగా మీరు ఆనందంలో మునిగిపోతారు! కానీ ఆగండి. ఇది UPI రిఫండ్ మోసం కావచ్చు!

UPI లేదా యూనిఫైడ్ పేమెంట్స్ ఇంటర్‌ఫేస్ మన రోజు వారీ జీవితంలో ఒక భాగమైంది. మీ సమీప కిరాణా దుకాణాల్లో చెల్లింపుల నుంచి, ఫోన్లను రీచార్జ్ చేయడం వరకు, విమాన టిక్కెట్లు బుక్ చేయడం వరకు, మేము UPI చెల్లింపులను అనేక విషయాలకు ఉపయోగిస్తున్నాం. కాబట్టి మోసగాళ్లు UPI యాప్స్‌ను ఉపయోగించి ప్రజలను మోసం చేయడానికి కొత్త పద్ధతులు అవలంబించడం ప్రారంభించారు.

వారి అధికారిక పదజాలం మరియు ప్రొఫెషనల్ భాషకు మోసపోవద్దు. ఈ క్రింది సూచనలను గుర్తుంచుకోండి:

లింకుల పట్ల జాగ్రత్త: రిఫండ్ క్లెయిమ్ చేసుకోవడానికి రిజిస్టర్ చేసుకోమని కోరుతూ స్కామర్లు మీకు ఒక లింక్ పంపవచ్చు.

అత్యవసరమైన పద్ధతులు: వారు మీపై ఒత్తిడి తీసుకొచ్చి బ్యాంక్ వివరాలు లేదా UPI PINను వెంటనే నమోదు చేయమని చెబుతారు. అర్హతను ధృవీకరించండి: మీరు రిఫండ్‌కు అర్హులా లేదా అని నిర్ధారించుకోండి. అర్హులైతే, నమ్మకమైన సోర్స్ తనిఖీ చేయండి.

అత్యవసరమైన పద్ధతులు: వారు మీపై ఒత్తిడి తీసుకొచ్చి బ్యాంక్ వివరాలు లేదా UPI PINను వెంటనే నమోదు చేయమని చెబుతారు. అర్హతను ధృవీకరించండి: మీరు రిఫండ్‌కు అర్హులా లేదా అని నిర్ధారించుకోండి. అర్హులైతే, నమ్మకమైన సోర్స్ తనిఖీ చేయండి.

గుర్తుంచుకోండి, బ్యాంక్ లేదా ఇతర అధికారికులు ఎప్పుడూ మీ సున్నితమైన వివరాలను అడగరు.

ఫిషింగ్ మోసాలు

ఊహించండి, మీరు ఒక చేపలా స్పష్టమైన చెరువులో ప్రశాంతంగా ఈదుతుంటారు, మీ పని మేమీ చూసుకుంటూ ఉంటారు. అకస్మాత్తుగా, ఒక మెరుస్తున్న, ఆకర్షణీయమైన ఎర మీ ముందు తేలుతుంది. మీరు ఆశక్తి చూపుతారు, కాని ఆగండి – ఏదో అనుమానంగా ఉంది!
ఫిషింగ్ కుంభకోణాలతో డిజిటల్ రంగంలో సరిగ్గా ఇదే జరుగుతుంది.

సైబర్ నేరగాళ్లు ఒక చేప ఎరకు ప్రలోభపెట్టినట్లు సున్నితమైన సమాచారాన్ని బహిర్గతం చేయడానికి మిమ్మల్ని మోసం చేయడానికి నమ్మదగిన వ్యక్తులుగా నటిస్తారు. వారు నకిలీ ఇమెయిల్స్, సందేశాలు లేదా వెబ్సైట్లను పంపుతారు, అవి చట్టబద్ధమైనవిగా కనిపిస్తాయి, ఇవి ఎక్కువగా బ్యాంకులు, సోషల్ మీడియా లేదా మీ బాస్‌ల పేరుతో ఉంటాయి.
ఈ డిజిటల్ హుక్లను నివారించడానికి, ఈ చిట్కాలను గుర్తుంచుకోండి:

URLలను రెండుసార్లు తనిఖీ చేయండి: లింక్‌లపై మౌస్ ఉంచి, అవి నిజంగా ఎక్కడికి తీసుకెళ్తాయో చూడండి.

వ్యక్తిగత సమాచారాన్ని పంచకండి: నిజమైన సంస్థలు ఇమెయిల్ ద్వారా సున్నితమైన విషయాలు అడగవు.

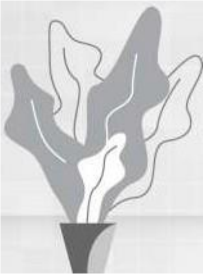
rl2J అనుమానాస్పదంగా ఉండండి: అనుకోని అభ్యర్థనలు? చర్య తీసుకునే ముందు ఇతర మార్గాల ద్వారా ధృవీకరించుకోండి.

l@l:"\,. భద్రతా సాఫ్ట్‌వేర్‌ను అప్‌డేట్ చేయండి: మీ డిజిటల్ ఆస్తిని తాజా రక్షణలతో సంరక్షించండి.

జాగ్రత్తగా ఉండే చేపలా, జాగ్రత్తగా ఉండండి మరియు ఇంటర్నెట్ యొక్క విశాలమైన సముద్రంలో తెలివిగా ఈత కొట్టండి!

ఫోన్ ద్వారా మోసం చేసే కాల్స్

a



మీ ఫోన్ మోగింది, మరియు ఇది మీ ఖాతా హ్యాకింగ్ కు గురైందని 'అర్జెంట్' కాల్ తో మీ బ్యాంకు అని పిలువబడేది, లేదా ఇది మీ లక్కీ డే అని చెప్పే 'విన్నింగ్' కాల్ కావచ్చు, మరియు మీరు బహుమతిని గెలిచారని చెప్పే కాల్ అవ్వచ్చు!
ఫోన్ పెట్టేయండి (తక్షణమే)!

అటువంటి మోసాల నుండి సురక్షితంగా ఉండటానికి, ఈ క్రింది చిట్కాలను గుర్తుంచుకోండి:

L

మీ వ్యక్తిగత వివరాలను ఎప్పుడూ ఫోన్లో బహిర్గతం చేయవద్దు.

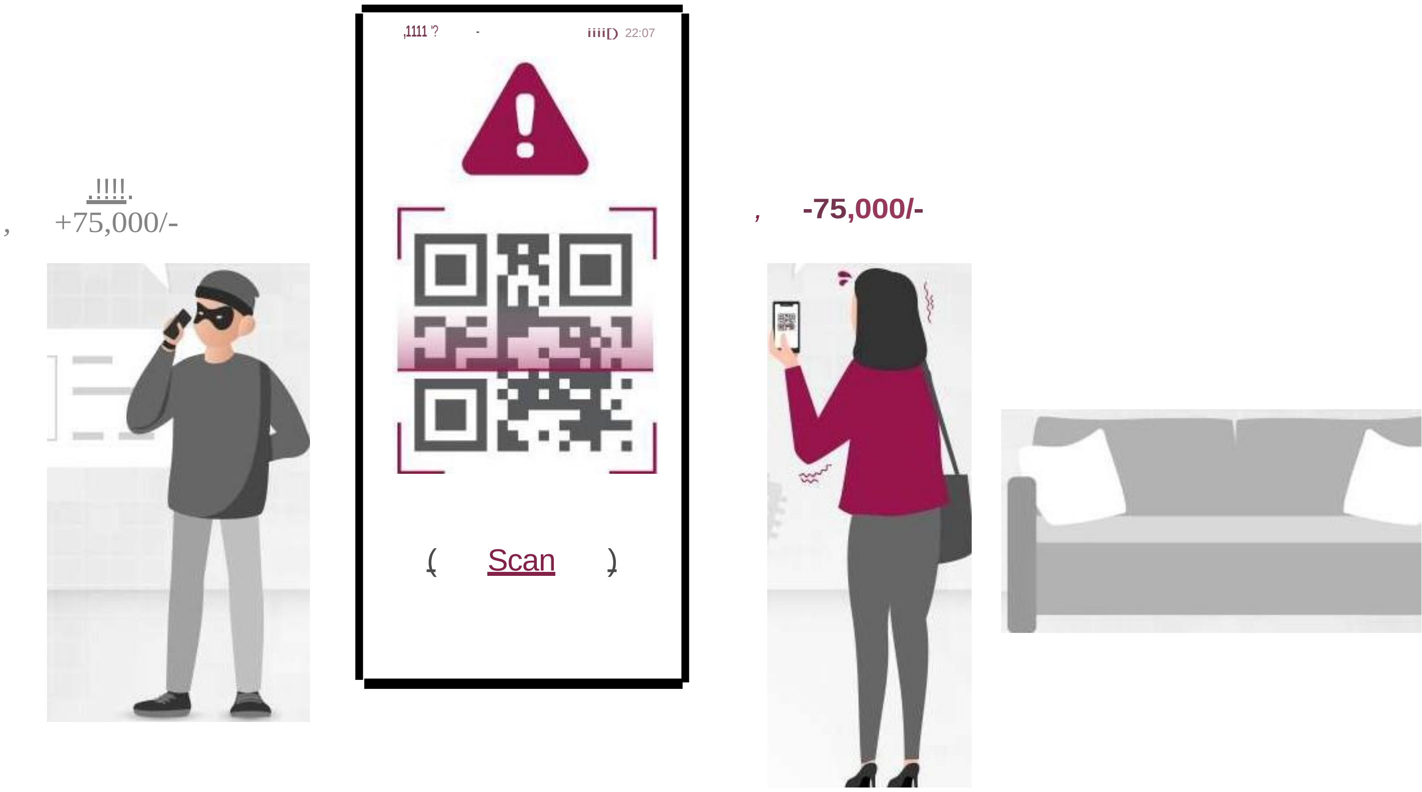
,..,
<@)>
L .J

తెలివిగా ఉండండి మరియు కాల్ చేసిన వ్యక్తి యొక్క గుర్తింపును ధృవీకరించండి.

"వారి నాటకానికి మోసపోవద్దు! వారు ఒత్తిడి తెచ్చినప్పుడు శాంతంగా ఉండండి.

ఆన్లైన్లో అన్యులకి మీ సమాచారాన్ని పంచేటప్పుడు జాగ్రత్తగా ఉండండి - తెలివిగా ఉంటే మీ సమాచారాన్ని సురక్షితంగా ఉంచగలరు!

UPI మోసాలు - డబ్బును అభ్యర్థించు ఆప్షన్



స్నేహ తన ఫర్నీచర్‌ను ఒక ఆన్‌లైన్ కొనుగోలు మరియు అమ్మకపు యాప్‌లో ప్రచారం చేసింది. ఒక కొనుగోలుదారు, అతను పరామిలిటరీ సిబ్బంది అని చెబుతూ, WhatsAppలో పేమెంట్ కోసం QR కోడ్ పంపాడు. స్నేహ దాన్ని స్కాన్ చేసి, ₹75,000 కోల్పోయింది.

ఇది సుపరిచితమేనా? మీరు తరచుగా UPI పేమెంట్ ప్లాట్‌ఫామ్‌లను ఉపయోగించడం వల్ల UPI మోసాలకు గురవుతారని భయపడుతున్నారా?

ఎల్లప్పుడూ గుర్తుంచుకోండి:

UPI పిన్ కేవలం పేమెంట్ చేయడానికి మాత్రమే అవసరం మరియు ఎటువంటి చెల్లింపును స్వీకరించడానికి కాదు..

పేమెంట్ రిసీవ్ చేసుకోమని మీ UPI PIN అడిగిన మరుక్షణమే ఆపండి! ఇది వాస్తవానికి చెల్లింపు అభ్యర్థన కావచ్చు మరియు సేకరణ అభ్యర్థన కాదు.

మీ OTP, UPI పిన్, రహస్య వివరాలను ఎవరితోనూ పంచుకోవద్దు.

ఏదైనా చెల్లింపును ప్రారంభించే ముందు UPI యాప్‌లో మొబైల్ నంబర్ మరియు పేరు ధృవీకరించడం తప్పనిసరి.

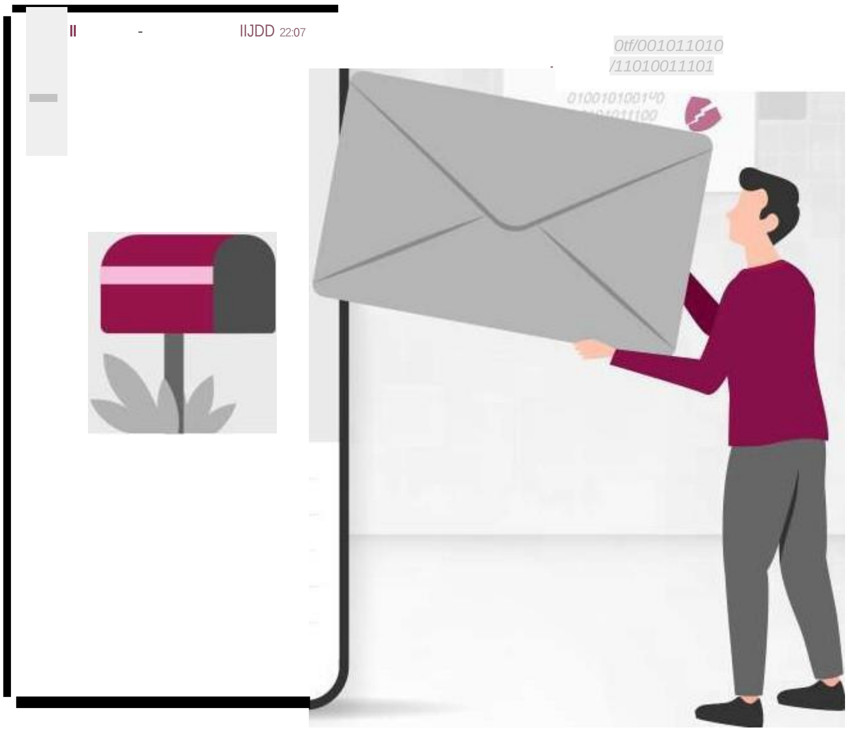
QR కోడ్ స్కాన్ మోసం

పేమెంట్ యాప్‌లపై క్యూఆర్ కోడ్‌లను జాగ్రత్తగా స్కాన్ చేయండి. అవి డబ్బు బదిలీ కోసం ఖాతా వివరాలను కలిగి ఉంటాయి.

డబ్బులు స్వీకరించడానికి QR కోడ్లను స్కాన్ చేయవద్దు; డబ్బులు తీసుకునే లావాదేవీలలో QR కోడ్లను స్కాన్ చేయడం, మొబైల్ బ్యాంకింగ్ పిన్ (m-PIN), పాస్‌వర్డ్‌లు మొదలైనవి నమోదు చేయడం అవసరం లేదు.

కొనుగోలుదారు/అమ్మకందారు అనవసరంగా తొందర లేదా అత్యవసరాన్ని చూపిస్తే, అతను మోసగాడు అయ్యే అవకాశం ఎక్కువ. శాంతంగా ఉండండి, ఎప్పుడూ వివరణ కోరండి మరియు అవసరమైన ప్రశ్నలు అడగండి.

ధృవీకరించని మొబైల్ యాప్ మోసాలు



మీకు ఒక SMS, ఇమెయిల్, లేదా ఎప్పుడూ చూడని బంధువు నుంచి ఒక లింక్ తో సందేశం వస్తుంది. అది మీకు తెలిసిన సంస్థ నుంచి నిజమైన యాప్ లింక్‌లా కనిపిస్తుంది. ఆగండి! ఇవి నిజమైనవి కావు, ఇవి మోసం చేసే డిజిటల్ ట్రాప్.

ఒక్కసారి ఆగండి! ఇవి స్నేహపూర్వకమైన డౌన్‌లోడ్లు కావు; ఇవి మీకు అస్సలు వెళ్లకూడని డిజిటల్ మోసానికి ఆహ్వానాలు!

మోసగాళ్లు SMS, ఇమెయిల్ లేదా సోషల్ మీడియాలో నకిలీ యాప్ లింక్‌లు పంపుతారు, ఇవి నిజమైనవిగా కనిపిస్తాయి. వారు యూజర్లను అవి క్లిక్ చేయమని ఒప్పిస్తారు, దాంతో తెలియని యాప్‌లు డౌన్‌లోడ్ అవుతాయి. ఒకసారి ఇన్‌స్టాల్ అయిన తర్వాత, మోసగాళ్లు మీ ఫోన్, సున్నితమైన సమాచారం, మరియు OTPలకు యాక్సెస్ పొందుతారు.

తెలియని మూలాల నుండి లేదా అపరిచిత వ్యక్తుల అభ్యర్థన మేరకు యాప్ లను డౌన్ లోడ్ చేయడం మానుకోండి.

యాప్ డౌన్‌లోడ్ చేసేముందు యాప్ పబ్లిషర్‌లు మరియు యూజర్ రేటింగ్‌లను నిర్ధారించండి.

యాప్ అనుమతులు మరియు యాప్ అభ్యర్థనలను (ఉదాహరణకు: కాంటాక్ట్స్, ఫోటోలు) సమీక్షించండి, అవసరమైన వాటికే అనుమతించండి.

గుర్తుంచుకోండి, బ్యాంకులు లేదా ఇతర అధికారులు ఇలాంటి సున్నితమైన వివరాల కోసం మిమ్మల్ని ఎప్పుడూ అడగరు.

ATM కార్డు నుంచి డబ్బు దొంగిలించే మోసం

ATM స్కిమ్మింగ్‌ను డిజిటల్ జేబుదొంగలాగా ఊహించండి. మీరు ATM ఉపయోగించి డబ్బు తీసుకుంటున్నప్పుడు లేదా మీ బ్యాలెన్స్ చూసినప్పుడు, మోసగాళ్లు మీ కార్డ్ సమాచారం రికార్డ్ చేసేందుకు యంత్రంపై దాచిన పరికరాలను అమరిస్తారు. ఈ పరికరాలు నకిలీ కార్డ్ స్లాట్ లేదా చిన్న కెమెరాల్లా ఉండవచ్చు.

ATM ఉపయోగించే ముందు, కార్డ్ స్లాట్ మరియు కీప్యాడ్‌పై ఏదైనా అన్యమైన పరికరాలు, సడలిన భాగాలు లేదా దాచిన కెమెరాలు ఉన్నాయా అని చెక్ చేయండి.

మీ PINను ఎంటర్ చేసేటప్పుడు, మీ చేతితో లేదా మీ శరీరంతో కవర్ చేయండి, తద్వారా కెమెరాలు లేదా ఇతరులు చూడలేరు.

మీ బ్యాంక్ స్టేట్‌మెంట్లు మరియు లావాదేవీలను తరచుగా తనిఖీ చేయండి. ఏదైనా అన్యమైన కార్యకలాపాలు కనబడితే, వెంటనే మీ బ్యాంక్‌కు సమాచారం ఇవ్వండి.

కాల్స్ పట్ల జాగ్రత్త: మీ బ్యాంకుకు చెందిన వారు ఎవరైనా ఫోన్ చేసి సున్నితమైన సమాచారం అడిగితే జాగ్రత్తగా ఉండండి. బ్యాంకులు చాలా అరుదుగా ఫోన్ ద్వారా పిన్ లు లేదా పూర్తి కార్డు నంబర్లను అడుగుతాయి.

సురక్షితమైన ATMలు వాడండి: సురక్షిత ప్రాంతాల్లో ఉన్న లేదా బ్యాంకు బ్రాంచ్‌లకు అనుబంధంగా ఉన్న ATMలను ఎంచుకోండి, ఎందుకంటే ఇవి మోసపూరితంగా మార్పులు చెయ్యబడే అవకాశం తక్కువగా ఉంటుంది.

అప్‌డేట్‌గా ఉండండి: మిమ్మల్ని మీరు మెరుగ్గా రక్షించుకోవడానికి తాజా మోసాలు మరియు మోసం వ్యూహాల గురించి తెలుసుకోండి.

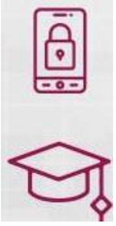
గుర్తుంచుకోండి, జాగ్రత్తగా ఉండటం మరియు ఈ సూచనలను పాటించడం ATM కార్డ్ స్కిమ్మింగ్ మోసానికి బలవ్వకుండా ఉండటానికి మరియు మీ ఆర్థిక సమాచారాన్ని సురక్షితంగా ఉంచడానికి సహాయపడతాయి.

దూరం నుంచి యాక్సెస్ చేసే మోసం

మోసగాళ్లు కస్టమర్లను స్క్రీన్-షేరింగ్ యాప్ డౌన్‌లోడ్ చేసుకోవాలని ప్రలోభపెడతారు. ఆ యాప్‌తో వారు మీ డివైస్‌లోకి చొరబడి, మీపై నిఘా ఉంచి, మీ ఆర్థిక సమాచారాన్ని దొంగిలిస్తారు. తర్వాత, వారు మీ డబ్బుతో షాపింగ్‌కి వెళ్తారు! ఇలాంటి మోసాల నుండి దూరంగా ఉండటానికి ఈ సూచనలను గుర్తుంచుకోండి:

కాలర్లను ధృవీకరించండి: వారు ప్రాతినిధ్యం వహిస్తున్నట్లు చెప్పుకునే సంస్థ యొక్క అధికారిక సంప్రదింపు సమాచారాన్ని స్వతంత్రంగా చూడటం ద్వారా కాల్ చేసిన వ్యక్తి యొక్క గుర్తింపును ఎల్లప్పుడూ రెండుసార్లు తనిఖీ చేయండి.

ఒత్తిడిలో వెంటనే నిర్ణయాలు తీసుకోకండి: ఎవరైనా ఒత్తిడి తీసుకువస్తే, ఆలోచనకు సమయం తీసుకోండి మరియు అనుమతులు ఇవ్వడం లేదా సున్నితమైన సమాచారాన్ని పంచేముందు ధృవీకరించండి.



మీ పరికరాలను సురక్షితంగా ఉంచండి: తాజా భద్రతా అప్‌డేట్‌లతో మీ పరికరాలను అప్‌డేట్ చేయండి మరియు ప్రతి ఖాతాకు బలమైన, ప్రత్యేకమైన పాస్‌వర్డ్‌లను ఉపయోగించండి.

మిమ్మల్ని మీరు అర్థం చేసుకోండి: సాధారణ మోసాలు మరియు వ్యూహాల గురించి తెలుసుకోండి, తద్వారా అవి సంభవించినప్పుడు మీరు వాటిని గుర్తించవచ్చు.

వ్యక్తిగత సమాచారాన్ని రక్షించండి: ఫోన్, ఇమెయిల్ లేదా ఆన్‌లైన్‌లో వ్యక్తిగత లేదా ఆర్థిక వివరాలను పంచేటప్పుడు జాగ్రత్తగా ఉండండి, అభ్యర్థన నిజమా అని మీరు పూర్తిగా నమ్మినప్పుడు మాత్రమే పంచండి. మీ డిజిటల్ జీవితంలోకి చొరబడటానికి ప్రయత్నించే రిమోట్ యాక్సెస్ మోసగాళ్ల నుంచి రక్షించడానికి అప్రమత్తంగా ఉండండి.

దయచేసి గమనించండి - ఒకవేళ మీరు నలుపు/ఖాళీ స్క్రీన్ ని గమనించినట్లయితే, దయచేసి మీ సిస్టమ్ పై ఏదైనా చర్యతో ముందుకు సాగవద్దు. ఇది మీ స్క్రీన్ ఇతరులకు కనిపించే సంకేతం కావచ్చు.

సిమ్ మార్పుతో డబ్బు దోచే

ఊహించండి, మోసగాళ్లు ఫోన్ దొంగతనం చేస్తున్నారు! వారు మీరు లాగా నటిస్తూ, తమ సిమ్ కార్డ్ పోయిందని చెప్పి మీ నంబర్‌ను తమ చేతుల్లోకి తీసుకుంటారు. ఆ నంబర్‌తో, వారు మీ బ్యాంక్ లేదా ఇమెయిల్ వంటి ఆన్‌లైన్ ఖాతాల్లో చొరబడి గందరగోళం సృష్టిస్తారు!

స్వాప్ మోసం నుండి రక్షించుకోండి! ఈ సూచనలను గుర్తుంచుకోండి.

సిమ్ కార్డు గుర్తింపు వివరాలను పంచుకోవద్దు.

మీ ఫోన్ నెట్‌వర్క్ యాక్సెస్‌ను పర్యవేక్షించండి.

కొంతసేపు నెట్‌వర్క్ లేకపోతే, డూప్లికేట్ సిమ్ ఉందేమో అని తనిఖీ చేయడానికి మీ ఆపరేటర్‌ను సంప్రదించండి.

మీ డిజిటల్ జీవితంలోకి చొరబడి దొంగిలించడానికి ప్రయత్నించే రిమోట్ యాక్సెస్ మోసగాళ్ల నుంచి రక్షించడానికి జాగ్రత్తగా ఉండండి.

మోసపూరిత లావాదేవీని ఎలా రిపోర్ట్ చేయాలి?

www.axisbank.com వెబ్‌సైట్‌కి వెళ్లండి > Support విభాగాన్ని ఎంచుకోండి > 'Reach us here' విభాగం వరకు స్క్రోల్ చేయండి > Speak with us ఎంపిక చేయండి > 'Report a fraud or Dispute' ఎంచుకోండి > Report a Fraud పై క్లిక్ చేయండి > మీ ప్రశ్నకు సంబంధించి డ్రాప్‌డౌన్ నుండి సంబంధిత ఎంపికను ఎంచుకోండి > కాల్ పై క్లిక్ చేయండి.

RBIకి ఫిర్యాదు చేయడానికి, https://cms.rbi.org.in వెబ్‌సైట్‌కి వెళ్లండి.

టోల్-ఫ్రీ నంబర్ 14448కి కాల్ చేయండి (సోమవారం నుండి శుక్రవారం, ఉదయం 9:30 నుండి సాయంత్రం 5:15 వరకు, జాతీయ సెలవులు మినహా).

ఫిజికల్ కంప్లైంట్: 'సెంట్రలైజ్డ్ రిసిప్ట్ అండ్ ప్రాసెసింగ్ సెంటర్, 4వ అంతస్తు, రిజర్వ్ బ్యాంక్ ఆఫ్ ఇండియా, సెక్టార్ -17, సెంట్రల్ విస్టా, చండీగఢ్ - 160 017'కు లేఖ/ పోస్ట్ పంపండి. అవసరమైన ఫార్మాట్ పై మరిన్ని వివరాల కొరకు దయచేసి https://cms.rbi.org.in సందర్శించండి.

సైబర్ నేరాన్ని నివేదించడానికి, హెల్ప్‌లైన్ నంబర్ **155260** లేదా **1930**కి కాల్ చేయండి లేదా జాతీయ సైబర్ క్రైమ్ రిపోర్టింగ్ పోర్టల్ (**www.cybercrime.gov.in**) లో సంఘటనను నివేదించండి.