



गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS



Indian
Cyber
Crime
Coordination
Centre

సైబర్ నేరాల

నివారణకు

తప్పనిసరిగా



చేయవలసిన మరియు చేయకూడని పనులు

ఆలోచించడం అపండి చర్చ మొదలు పెట్టండి



సూచిక పేజీలు

మోసం రకము

పేజీ సంఖ్య

KYC మోసం	4
ఆన్‌లైన్ జాబ్ మోసం	5
ఆన్‌లైన్ షాపింగ్ మోసం	6
డిజిటల్ అరెస్ట్	7
పెట్టుబడి మోసం	8
ఆన్‌లైన్ గేమింగ్	9
లాటరీ మోసం	10
ఫిషింగ్	11
స్పామ్/విషింగ్ కాల్స్	12
క్విషింగ్	13
సెర్చ్ ఇంజిన్ మోసం	14
సామాజిక మాధ్యమాలలో నకిలీ ఖాతాలు	15



సూచిక పేజీలు

మోసం రకము	పేజీ సంఖ్య
ఎస్.ఎం.ఎస్, ఇమెయిల్ & కాల్ మోసాలు	16
డెబిట్/క్రెడిట్ కార్డ్ మోసం	17
మొబైల్ అప్లికేషన్ APK మోసాలు	18
సైబర్ బానిసత్వం	19
సిమ్ స్వాపింగ్	20
మసీ మ్యూల్స్	21
జ్యూస్ జాకింగ్	22
డివైస్ స్టెబర్ నేరం	23
రిమోట్ యాక్సెస్ మోసం	24
సురక్షిత బ్రౌజింగ్	25
రాన్సమ్ వేర్	26
స్మార్ట్ఫోన్ మోసాలు	27



KYC మోసం



KYC మోసం అనేది సైబర్ నేరస్థులు వ్యక్తిగత సమాచారం, గుర్తింపు లేదా ఆర్థిక ఖాతాలను దొంగిలించడానికి KYC ప్రక్రియను దుర్వినియోగం చేయడం. ఇది వ్యక్తులు, సంస్థలు, బ్యాంకులకు ఆర్థిక నష్టాలు మరియు ప్రతిష్ఠకు నష్టాన్ని కలిగించవచ్చు. ప్రజలను మోసం చేయడం, నకిలీపత్రాలు తయారు చేయడం, నకిలీ గుర్తింపులు సృష్టించడం వంటి పద్ధతులు వాడతారు. ఇవి జాగ్రత్తగా గమనించి నివారించాలి.

✓ చేయవలసినవి:

- **అభ్యర్థనలను నిర్ధారించండి:** ఏదైనా KYC అప్డేట్ అభ్యర్థనలను నిర్ధారించడానికి మీ బ్యాంక్ లేదా ఆర్థిక సంస్థను నేరుగా సంప్రదించండి.
- **అధికారిక సంప్రదింపులను ఉపయోగించండి:** ఫోన్ నంబర్లు లేదా కస్టమర్ కేర్ వివరాలను అధికారిక వెబ్సైట్ లేదా నమ్మకమైన మూలాల నుండి మాత్రమే పొందండి.
- **సంఘటనలను నివేదించండి:** మీరు ఏదైనా సైబర్ మోసమని అనుమానిస్తే వెంటనే మీ బ్యాంక్ లేదా ఆర్థిక సంస్థకు తెలియజేయండి.
- **KYC అప్డేట్ పద్ధతులను తనిఖీ చేయండి:** KYC వివరాలను అప్డేట్ చేయడానికి అందుబాటులో ఉన్న పద్ధతుల గురించి మీ బ్యాంకును వాకబు చేయండి.

✗ చేయకూడనివి:

- **వ్యక్తిగత వివరాలు రక్షించుకోండి:** మీ ఖాతా లాగిన్ వివరాలు, కార్డ్ సమాచారం, పిన్లు, పాస్వర్డ్లు లేదా OTP లను ఎవరితోనూ లేదా అధికారిక వెబ్సైట్లు/ యాప్లలో కాకుండా మరెక్కడా ఉపయోగించరాదు.
- **పత్రాలను భద్రపరచండి:** KYC పత్రాలు లేదా వాటి కాపీలను తెలియని లేదా గుర్తించబడని వ్యక్తులు లేదా సంస్థలతో పంచుకోరాదు.
- **అనుమానాస్పద లింక్లను నివారించండి:** మొబైల్ లేదా ఇమెయిల్ ద్వారా అందుకున్న అనుమానాస్పద లేదా ధృవీకరించని లింక్లపై క్లిక్ చేయవద్దు.



ఆన్‌లైన్ జాబ్ మోసం

ఆన్‌లైన్ జాబ్ మోసాలు పనిని వెతుకుతున్న వారిని మోసం చేస్తాయి. మోసగాళ్లు వెబ్‌సైట్‌లు, సోషల్‌మీడియా లేదా ఇమెయిల్ ద్వారా నకిలీ ఉద్యోగాలను పోస్ట్ చేస్తారు, అధిక జీతం మరియు సులభమైన పని అందిస్తామని చెప్తారు. వారి లక్ష్యం బాధితుల డబ్బు లేదా వ్యక్తిగత సమాచారాన్ని దోంగిలించడం.

✓ చేయవలసినవి:

- **నమ్మకమైన మూలాలను ఉపయోగించండి:** ప్రైవేట్ మరియు ప్రభుత్వ ఉద్యోగ జాబితాల కోసం వార్తాపత్రికలు, జాబ్ పోర్టల్‌లు లేదా ప్రభుత్వ పోర్టల్‌లను ఉపయోగించండి.
- **వివరాలను తనిఖీ చేయండి:** అంతర్జాతీయ ఉద్యోగ ఆఫర్ కోసం, సంస్థ యొక్క వివరాలను సరిచూసుకోండి మరియు మీకు సరైన పని వీసా ఉన్నట్లు నిర్ధారించుకోండి.
- **ప్రశ్నలు అడగండి:** ఆన్‌లైన్ ఇంటర్వ్యూల సమయంలో, కంపెనీ మరియు ఇంటర్వ్యూయర్ గురించి వివరణాత్మక ప్రశ్నలు అడగండి.
- **ఇమెయిల్‌లను సరిచూడండి:** అసలైన కంపెనీలను అనుకరించే ఇమెయిల్ చిరునామాలను గమనించండి. ఉదాహరణకు, info@company.com కి బదులుగా info@company.net.

✗ చేయకూడనివి:

- **ముందస్తు ఫీజులను నివారించండి:** కంపెనీ చట్టబద్ధతను ధృవీకరించకుండా కన్సల్టింగ్ ఫీజులు చెల్లించవద్దు.
- **అనుమానం వ్యక్తం చేయండి:** ప్రాయోజిత శోధన ఫలితాలు లేదా అడగకుండా వచ్చిన ఉద్యోగ ఇమెయిల్‌లను గుడ్డిగా నమ్మకండి.
- **ప్రకటనలను ధృవీకరించండి:** ప్రకటనల యాథార్థ్యాన్ని ధృవీకరించకుండా, ముఖ్యంగా సోషల్ మీడియా ప్లాట్‌ఫార్మ్‌లు లేదా గ్రూప్‌లలో ఉద్యోగాల కోసం దరఖాస్తు చేయవద్దు.



ఆన్‌లైన్ షాపింగ్ మోసం



ఆన్‌లైన్ షాపింగ్ మోసం అనేది మోసగాళ్లు బాధితులను అక్రమ కొనుగోళ్లు చేయడానికి చేసే సైబర్ నేరం. వారు నకిలీ వెబ్‌సైట్‌లను సృష్టిస్తారు లేదా చట్టబద్ధమైన ప్లాట్‌ఫార్మ్‌లను తప్పుదారి పట్టిస్తారు, నమ్మకశక్యం కాని అద్భుతమైన ఆఫర్‌లను అందిస్తారు, వ్యక్తిగత మరియు ఆర్థిక సమాచారాన్ని దొంగిలిస్తారు, ఆర్థిక నష్టాలకు మరియు ఆన్‌లైన్ మార్కెట్‌ప్లేస్‌లపై నమ్మకం కోల్పోవడానికి దారితీస్తుంది.

✓ చేయవలసినవి:

- **ధరలను పోల్చండి:** వివిధ ఇ-కామర్స్ వెబ్‌సైట్‌లలో ధరలను పోల్చండి.
- **క్యాష్-ఆన్-డెలివరీని ఉపయోగించండి:** ఒక వెబ్‌సైట్ అనుమానాస్పదంగా కనిపిస్తే, క్యాష్-ఆన్-డెలివరీ చెల్లింపు పద్ధతిని ఎంచుకోండి.
- **ధృవీకరించబడిన విక్రేతలను ఎంచుకోండి:** ఇ-కామర్స్ వెబ్‌సైట్‌లలో "ధృవీకరించబడిన" లేదా "నమ్మకమైన" విక్రేతల నుండి కొనుగోలు చేయడానికి ప్రాధాన్యత ఇవ్వండి.
- **ఆఫర్‌లను ధృవీకరించండి:** నిజమనిపించని ఆఫర్‌ల పట్ల జాగ్రత్తగా ఉండండి.
- **సురక్షితమైన లావాదేవీలు:** డబ్బు స్వీకరించడానికి మీరు PIN, పాస్‌వర్డ్ లేదా OTP ని నమోదు చేయవలసిన అవసరం లేదని గుర్తుంచుకోండి.

✗ చేయకూడనివి:

- **పబ్లిక్ నెట్‌వర్క్‌లను నివారించండి:** పబ్లిక్ కంప్యూటర్‌లు లేదా నెట్‌వర్క్‌లను ఉపయోగించి ఇ-షాపింగ్ లావాదేవీలు చేయవద్దు.
- **మీ సమాచారాన్ని రక్షించండి:** మీ కార్డ్ వివరాలు, పుట్టిన తేదీ, ఫోన్ నంబర్ మొదలైన వాటిని నమ్మకం లేని ఇ-షాపింగ్ వెబ్‌సైట్‌లలో సేవ్ చేయవద్దు.
- **విక్రేతలను ధృవీకరించండి:** విక్రేత వివరాలు ధృవీకరించకుండా OLX, Quikr మొదలైన C2C ప్లాట్‌ఫార్మ్‌లలో ముందస్తు చెల్లింపులు చేయవద్దు.
- **QR కోడ్‌ల గురించి జాగ్రత్త వహించండి:** WhatsApp లేదా Telegram లో తెలియని వ్యక్తి అడిగితే డబ్బు 'స్వీకరించడానికి' QR కోడ్‌లను స్కాన్ చేయవద్దు.



డిజిటల్ అరెస్ట్

డిజిటల్ అరెస్ట్ అంటే సాంప్రదాయ భౌతిక అరెస్ట్ పద్ధతులకు బదులుగా డిజిటల్ మార్గాల ద్వారా (వీడియో కాల్స్ వంటివి) ఒక వ్యక్తిని నిర్బంధించడం లేదా పరిమితం చేయడం. దీనిలో తరచుగా మోసగాళ్లు ప్రభుత్వ అధికారులుగా మారువేషం వేసి డబ్బు దోచుకుంటారు.



✓ చేయవలసినవి:

- **నిజాలను తెలుసుకోండి:** పోలీసులు లేదా ప్రభుత్వ అధికారులు వీడియో కాల్స్ ద్వారా ఎప్పుడూ విచారణలు నిర్వహించరు.
- **వ్యక్తిగత సమాచారాన్ని భాగస్వామ్యం చేయవద్దు:** ఏ ప్రభుత్వ అధికారి కూడా వీడియో కాల్స్ ద్వారా డబ్బు లేదా వ్యక్తిగత వివరాలను అడగరు.
- **ప్రశాంతంగా ఉండండి:** మీరు అటువంటి కాల్స్ అందుకుంటే, వెంటనే "రిపోర్ట్ సెన్సిట్వ్ ట్రాబ్" cybercrime.gov.in లోనివేదించండి.
- **చట్టాన్ని అర్థం చేసుకోండి:** భారతదేశంలో "డిజిటల్ అరెస్ట్" ప్రక్రియ అనేది లేదు.

✗ చేయకూడనివి:

- **భయపడవద్దు:** ప్రశాంతంగా ఉండండి మరియు మోసాలకు లోనుకాకుండా జాగ్రత్తపడండి.
- **మోసగాళ్లకు తల ఒగ్గవద్దు:** ఎవరైనా వీడియో కాల్ ద్వారా ఒత్తిడి చేస్తే డబ్బు పంపవద్దు.
- **దీర్ఘకాలిక నిమగ్నం కావద్దు:** అనుమానాస్పదంగా అనిపించే దీర్ఘకాలిక వీడియో కాల్ లలో చిక్కుకోకుండా జాగ్రత్తపడండి.
- **ధృవీకరించని కాల్ లను నమ్మవద్దు:** డబ్బు అడిగే ప్రభుత్వ అధికారుల నుండి వచ్చే అని చెప్పుకునే వీడియో కాల్ లను పట్టించుకోకండి.



పెట్టుబడి మోసం



పెట్టుబడి మోసం అంటే అధిక రాబడులను వాగ్దానం చేసే మోసపూరిత పథకాలు, తరచుగా నమ్మలేనంత మంచివి. ఈ మోసాలు చట్టబద్ధమైన ఆర్థిక కార్యకలాపాల ద్వారా లాభాలను సృష్టించడానికి బదులుగా కొత్త పెట్టుబడిదారుల డబ్బుతో ముందరి పెట్టుబడిదారులకు చెల్లిస్తాయి. దీనిని పోంజీ స్కీమ్ అని కూడా అంటారు.

✓ చేయవలసినవి:

- **నమోదిత సంస్థలతో పెట్టుబడి పెట్టండి:**
పెట్టుబడులకు SEBI-నమోదిత మధ్యవర్తులతో మాత్రమే పెట్టుబడి పెట్టండి.
- **పెట్టుబడి ఉత్పత్తులను ధృవీకరించండి:**
ఎల్లప్పుడూ నియంత్రిత ఆర్థిక సంస్థల ద్వారా పెట్టుబడి పెట్టండి.
- **సమాచారం పొందండి:** నియంత్రిత సంస్థలు మరియు ఆర్థిక ఉత్పత్తుల విశ్లేషనీయ సమాచార వనరులను అనుసరించండి.
- **అనుమానిత కార్యకలాపాన్ని నివేదించండి:**
1930కి కిట్ చేయండి లేదా cybercrime.gov.in లో నివేదించండి.

✗ చేయకూడనివి:

- **భయపడవద్దు:** ప్రశాంతంగా ఉండి ఆఫర్ ను ధృవీకరించుకోండి.
- **నమ్మశక్యం కాని రాబడులను నమ్మవద్దు:**
రిస్క్ లేకుండా అధిక రాబడులను వాగ్దానం చేసే పథకాలను నివారించండి.
- **అనుమానాస్పద గ్రూపులలో చేరవద్దు:**
అనుమానిత ట్రేడింగ్ యాప్ లను ప్రమోట్ చేసే సోషల్ మీడియా గ్రూప్ లకు దూరంగా ఉండండి.
- **రెడ్ ఫ్లాగ్ లను నిర్లక్ష్యం చేయవద్దు:**
రాబడులు కాలక్రమేణా చాలా స్థిరంగా లేదా చాలా ఎక్కువగా అనిపిస్తే జాగ్రత్తగా ఉండండి.



ఆన్‌లైన్ గేమింగ్



ఆన్‌లైన్ గేమింగ్ సైబర్ నేరస్థలకు ముఖ్యమైన స్థానంగా మారింది, వర్చువల్ దొంగతనం మరియు ఖాతా ఛేదనల నుండి వాస్తవ ప్రపంచ ఆర్థిక మోసం మరియు గుర్తింపు దొంగతనం వరకు వివిధ రకాల ముప్పులు ఉన్నాయి. దాడిచేసేవారు ప్లాట్‌ఫారమ్ లోపాలను ఆసరాగా తీసుకుంటారు మరియు ఫిషింగ్ మోసాలు, మాల్వేర్స్ మరియు సోఫిస్టర్డ్ ఇంజనీరింగ్ ద్వారా ఆటగాళ్లను లక్ష్యంగా చేసుకుంటారు.

✓ చేయవలసినవి:

- **యాక్సెస్‌ను పర్యవేక్షించండి:** మీరు తల్లిదండ్రులైతే, పర్యవేక్షణ కింద ఆన్‌లైన్ గేమింగ్‌కు యాక్సెస్‌ను అందించండి.
- **రియల్ మనీ యావ్‌ల విషయంలో జాగ్రత్తగా ఉండండి:** చాలా రియల్ మనీ గేమింగ్ యావ్‌లు మోసపూరితంగా ఉండవచ్చు. జాగ్రత్తగా ఉండండి మరియు అనుమానాస్పదంగా కనిపించే యావ్‌లను నివారించండి.
- **వివేకవంతమైన యావ్ అనుమతులు:** కాంటాక్ట్స్, స్టోరేజ్ మరియు లోకేషన్ వంటి అనుమతులను యావ్‌కు ఇచ్చే ముందు జాగ్రత్తగా ఉండండి.
- **వ్యక్తిగత సమాచారాన్ని రక్షించండి:** మీ పూర్తి పేరు, చిరునామా లేదా బ్యాంక్ ఖాతా వివరాలు వంటి సున్నితమైన వ్యక్తిగత సమాచారాన్ని సురక్షితంగా ఉంచండి.

✗ చేయకూడనివి:

- **అనుమానాస్పద మూలాలను నివారించండి:** నమ్మదగని మూలాల నుండి గేమింగ్ యావ్‌లను డౌన్‌లోడ్ చేయవద్దు.
- **హామీ ఇవ్వబడిన రాబడుల గురించి జాగ్రత్తగా ఉండండి:** సోషల్ మీడియాలో లేదా ప్రకటనల ద్వారా హామీ ఇవ్వబడిన రాబడులను వాగ్దానం చేసే గేమింగ్ యావ్‌లను ఇన్‌స్టాల్ చేయవద్దు.
- **సమాచారాన్ని ప్రైవేట్‌గా ఉంచండి:** తెలియని సహ ఆటగాళ్లతో గోప్యమైన సమాచారాన్ని భాగస్వామ్యం చేయవద్దు.
- **సోషల్ మీడియాలో షేర్ చేయడాన్ని పరిమితం చేయండి:** వేధింపులు లేదా సైబర్ దాడుల బారిన పడకుండా ఉండేందుకు మీ గేమింగ్ విజయాలను సోషల్ మీడియాలో షేర్ చేయడం నివారించండి.



లాటరీ మోసం



లాటరీ మోసాలు ప్రజలు ఒక బహుమతి గెలిచారని నమ్మించి, డబ్బు పంపడానికి లేదా వ్యక్తిగత సమాచారాన్ని దోచుకోడానికి చేసే మోసం. ఈ పథకాలు ఆర్థిక లాభం పొందే ఆశ పెడతాయి కానీ అవి ఎప్పటికీ నమ్మదగినవిగా ఉండవు.

✓ చేయవలసినవి:

- **ఫీజులు చెల్లించవద్దు:** మోసగాళ్లు తరచుగా పన్నులు, షిప్పింగ్ ఫీజులు లేదా నకిలీ బహుమతుల కోసం నిర్వహణ ఛార్జీలను డిమాండ్ చేస్తారు. ఏ లాటరీల కోసం డబ్బులు పంపవద్దు.
- **అడగని క్లెయిమ్లను ప్రశ్నించండి:** ఊహించని లాటరీ గెలుపు సందేశాలు లేదా కాల్స్ పట్ల జాగ్రత్తగా ఉండండి.
- **మోసాన్ని నివేదించండి:** లాటరీ స్కామ్ గురించి అనుమానిస్తే అధికారులకు తెలియజేయండి.
- **అనుమానంగా ఉండండి:** ఎవరూ ఉచితంగా పెద్ద మొత్తంలో డబ్బును ఇవ్వరని గుర్తుంచుకోండి.

✗ చేయకూడనివి:

- **ఆధారాలను పంచుకోవద్దు:** లాటరీ క్లెయిమ్ల కోసం భద్రతా వివరాలను అందించవద్దు లేదా చెల్లింపులు చేయవద్దు.
- **నకిలీ అధికారుల పట్ల జాగ్రత్తగా ఉండండి:** RBI ప్రజా ఖాతాలను కలిగి ఉండదు, డిపాజిట్లను అభ్యర్థించదు, లేదా వ్యక్తిగత/బ్యాంక్ వివరాలను అడగదు.
- **నకిలీ సందేశాలను విస్మరించండి:** బహుమతి డబ్బు, ప్రభుత్వ సహాయం లేదా బహుమతులకు సంబంధించిన KYC అప్డేట్ల వంటి వాగ్దానం చేసే ఆఫర్లకు ప్రతిస్పందించడాన్ని నివారించండి.



ఫిషింగ్ మోసం



ఫిషింగ్ అనేది సాధారణ సైబర్ నేర ఎత్తుగడ, ఇది బాధితులను నకిలీ లింక్లపై క్లిక్ చేయడం ద్వారా మోసం చేస్తుంది. ఈ లింకులు నమ్మకమైన మూలాల నుండి ఇమెయిల్లు లేదా వెబ్సైట్లుగా కనిపిస్తాయి, కానీ వినియోగదారులను లాగిన్ క్రెడిన్షియల్స్, వ్యక్తిగత సమాచారం లేదా ఆర్థిక వివరాల వంటి సున్నితమైన డేటాను దొంగిలించడానికి రూపొందించబడిన మోసపూరిత సైట్లకు దారి మళ్లిస్తాయి. ఫిషింగ్ మాల్వేర్స్ను కూడా ఇన్స్టాల్ చేయవచ్చు, సైబర్ నేరగాళ్లకు మీ పరికరానికి అనధికారిక ప్రాప్తిని అందిస్తుంది.

✓ చేయవలసినవి:

- **అనుమానంగా ఉండండి:** తెలిసిన మూలాల నుండి వచ్చిన అనుకోని సందేశాలను జాగ్రత్తగా పరిగణించండి.
- **URLలను తనిఖీ చేయండి:** నిజమైన గమ్యస్థానాన్ని బహిర్గతం చేయడానికి మరియు వ్యత్యాసాలను గుర్తించడానికి లింక్లపై పైకి మౌస్ తీసుకెళ్లడం చేయండి.
- **పంపిన వారిని ధృవీకరించండి:** సందేశం యొక్క ప్రామాణికత గురించి మీకు నిశ్చయత లేకపోతే, నమ్మకమైన పద్ధతి ద్వారా పంపిన వారిని సంప్రదించండి.
- **క్రమం తప్పకుండా నవీకరించండి:** భద్రతా లోపాలను మూసివేయడానికి మీ సాఫ్ట్వేర్ మరియు సిస్టమ్లను నవీకృతంగా ఉంచండి.
- **ఫిషింగ్ నివేదిక:** ఫిషింగ్ ప్రయత్నాలను ఎదుర్కొంటే సంబంధిత అధికారులు లేదా ప్లాట్ఫారమ్లకు నివేదించండి.

✗ చేయకూడనివి:

- **లింక్లపై క్లిక్ చేయడాన్ని నివారించండి:** అనుమానాస్పద లింక్లపై క్లిక్ చేయవద్దు; తెలియని వారి నుండి వచ్చిన సందేశాలను వెంటనే తొలగించండి.
- **సబ్స్క్రిప్షన్ రద్దు చేయండి & బ్లాక్ చేయండి:** అనుమానాస్పద లింక్లతో ఇమెయిల్ల నుండి సబ్స్క్రిప్షన్ రద్దు చేయండి మరియు పంపిన వారి ఇమెయిల్స్ను బ్లాక్ చేయండి.
- **అధికారిక వెబ్సైట్లను సందర్శించండి:** ఆర్థిక లావాదేవీల కోసం ఎప్పుడూ నేరుగా అధికారిక వెబ్సైట్లకు వెళ్లండి మరియు వెబ్సైట్ భద్రతను ధృవీకరించండి (HTTPS లాక్ తో).



స్పామ్/విషింగ్ కాల్స్



స్పామ్/విషింగ్ కాల్స్ సైబర్ నేరం యొక్క మోసపూరిత రూపం. మోసగాళ్లు బాధితులను వ్యక్తిగత లేదా ఆర్థిక డేటా వంటి సున్నితమైన సమాచారాన్ని బహిర్గతం చేయడానికి సామాజిక ఇంజనీరింగ్ని ఉపయోగిస్తారు. వారు తరచుగా బ్యాంకులు లేదా ప్రభుత్వ ఏజెన్సీల వంటి చట్టబద్ధమైన సంస్థలను అనుకరిస్తారు, కాలర్ ID సూపింగ్ మరియు అత్యవసర పద్ధతులను ఉపయోగించి విశ్వాసాన్ని పొంది సమాచారాన్ని దొంగిలిస్తారు.

✓ చేయవలసినవి:

- **కాల్ బ్లాకర్లను ఉపయోగించండి:** కాల్-బ్లాకింగ్ యాప్లను ఇన్స్టాల్ చేయండి మరియు స్పామ్ కాల్లను నివేదించండి.
- **జాగ్రత్తగా ఉండండి:** తెలియని నంబర్ల నుండి వచ్చే కాల్లకు సమాధానమిచ్చేటప్పుడు జాగ్రత్తగా ఉండండి.
- **అవగాహన వ్యాప్తి చేయండి:** సాధారణ ఫోన్ స్కామ్ల గురించి ఇతరులకు అవగాహన కల్పించండి.
- **భద్రతను ప్రారంభించండి:** అదనపు రక్షణ కోసం వాయిస్మెయిల్ పాస్వర్డ్లను ఉపయోగించండి.

✗ చేయకూడనివి:

- **వ్యక్తిగత సమాచారాన్ని పంచుకోవద్దు:** తెలియని కాలర్లకు వ్యక్తిగత లేదా ఆర్థిక సమాచారాన్ని ఎప్పటికీ అందించవద్దు.
- **కాలర్ IDని నమ్మవద్దు:** కాలర్ IDని స్కాప్ చేయవచ్చు, కాబట్టి దానిపై ఆధారపడవద్దు.
- **తెలియని నంబర్లను నివారించండి:** తెలియని లేదా అంతర్జాతీయ నంబర్ల నుండి కాల్లకు సమాధానం ఇవ్వవద్దు.
- **మీ డేటాను రక్షించండి:** నిజమైన సంస్థలు యూజర్నేమ్లు, పాస్వర్డ్లు లేదా OTPలు వంటి సున్నితమైన సమాచారాన్ని ఎప్పుడూ అడగవు. కుటుంబంతో సహా వీటిని ఎప్పటికీ పంచుకోవద్దు.



Scan this QR
to redeem money



క్విషింగ్



క్విషింగ్ స్కామ్లు పెరుగుతున్నాయి. మోసగాడు QR కోడ్లను స్కాన్ చేయమని అడగడం ద్వారా డీల్లు లేదా సాకర్స్ వాగ్దానాలతో బాధితులను ఆకర్షిస్తారు, కానీ చివరికి అనధికారిక ఆర్థిక లావాదేవీలను ప్రారంభిస్తారు. హానికరమైన కోడ్లు వినియోగదారులను ఫిషింగ్ సైట్లకు మళ్లించవచ్చు, లాగిన్ క్రెడెన్షియల్లను దొంగిలించవచ్చు లేదా డబ్బును నేరుగా మోసగాడి ఖాతాకు బదిలీ చేయవచ్చు.

✓ చేయవలసినవి:

- **నమ్మకమైన మూలాలను స్కాన్ చేయండి:** అధికారిక వెబ్సైట్లు లేదా ధృవీకరించబడిన వ్యాపారాల నుండి మాత్రమే QR కోడ్లను స్కాన్ చేయండి.
- **చర్య తీసుకునే ముందు ధృవీకరించండి:** మోసగాళ్లు తరచుగా తొందరపాటు కు గురిచేస్తారు – తగిన సమయం తీసుకొని ధృవీకరించుకోండి.
- **అనుమానాస్పద కోడ్లను నివేదించండి:** మీరు మోసాన్ని అనుమానిస్తే, కోడ్ను చట్టబద్ధమైన మూలానికి మరియు సంబంధిత అధికారులకు నివేదించండి.

✗ చేయకూడనివి:

- **చెల్లింపులతో జాగ్రత్తగా ఉండండి:** చెల్లింపు యాప్లతో QR కోడ్లను స్కాన్ చేయడాన్ని నివారించండి, ఎందుకంటే అవి మోసపూరిత డబ్బు బదిలీల కోసం ఖాతా వివరాలను కలిగి ఉండవచ్చు.
- **డబ్బు స్వీకరించడానికి స్కాన్ చేయవద్దు:** నిధులను స్వీకరించడానికి QR కోడ్లను ఎప్పుడూ స్కాన్ చేయవద్దు. చట్టబద్ధమైన లావాదేవీలకు కోడ్లను స్కాన్ చేయడం లేదా m-PIN లేదా పాస్‌వర్డ్ల వంటి బ్యాంకింగ్ వివరాలను నమోదు చేయడం అవసరం లేదు.
- **తెలియని మూలాలను నివారించండి:** ఇమెయిల్లు, సందేశాలు లేదా తెలియని మూలాల నుండి కోడ్లను స్కాన్ చేయవద్దు.



శోధన యంత్రం మోసం



శోధన యంత్రం మోసం మోసగాళ్లు చట్టబద్ధమైన సంస్థలుగా నటిస్తూ నకిలీ సంప్రదింపు సమాచారాన్ని ప్రదర్శించడానికి శోధన ఫలితాలను తారుమారుచేసినపుడు జరుగుతుంది. బాధితులు ఈ నంబర్లకు తెలియకుండా కాల్ చేసినపుడు పాస్‌వర్డ్‌లు మరియు ఖాతా వివరాల వంటి సున్నితమైన సమాచారాన్ని బహిర్గతం చేయవచ్చు, ఇది ఆర్థిక నష్టం, గుర్తింపు దొంగతనం మరియు ఇతర తీవ్రమైన పరిణామాలకు దారితీస్తుంది.

✓ చేయవలసినవి:

- **అధికారిక వెబ్‌సైట్‌లను సందర్శించండి:** శోధన ఫలితాలపై ఆధారపడకుండా, సంప్రదింపు వివరాల కోసం ఎప్పుడూ అధికారిక వెబ్‌సైట్‌ను తనిఖీ చేయండి.
- **కాంటాక్ట్‌లను ధృవీకరించండి:** వ్యక్తిగత సమాచారాన్ని షేర్ చేయడానికి ముందు కాలర్ ID లేదా నమ్మకమైన డైరెక్టరీలను ఉపయోగించి ఫోన్ నంబర్లు మరియు వెబ్‌సైట్‌లను డబుల్-చెక్ చేయండి.
- **ప్రమాదాలను గమనించండి:** అత్యవసరం, భయపెట్టి ఎత్తుగడలు లేదా అనుమానాస్పద ఆఫర్ల పట్ల జాగ్రత్తగా ఉండండి. చట్టబద్ధమైన కంపెనీలు తక్షణ చర్యకు ఒత్తిడి చేయవు.

✗ చేయకూడనివి:

- **శోధన ఫలితాలను నమ్మవద్దు:** శోధన యంత్రం ఫలితాల్లో జాబితా చేయబడిన నంబర్లకు ఎప్పుడూ కాల్ చేయవద్దు; మోసగాళ్లు తరచుగా తమను తాము అక్రమ సంస్థగా మారుస్తారు.
- **సమాచారాన్ని విచారించకుండా పంచుకోవద్దు:** మీరు సంప్రదింపును ప్రారంభించినట్లయితే మాత్రమే ఫోన్‌లో వ్యక్తిగత వివరాలను షేర్ చేయండి.



సోషల్ మీడియా నకిలీకరణ



సోషల్ మీడియా నకిలీకరణ అనేది ఎవరైనా నిజమైన వ్యక్తి లేదా సంస్థను అనుకరిస్తూ నకిలీ ఖాతాను ఏర్పాటు చేసినప్పుడు జరుగుతుంది. ఈ మోసపూరిత ఖాతాలు ఇతరులను మోసం చేయడానికి ఉపయోగించబడతాయి, తరచుగా గుర్తింపు దొంగతనం, ఆర్థిక స్కామ్లు, ప్రతిష్ట నష్టం మరియు తప్పుడు సమాచార వ్యాప్తికి దారితీస్తుంది.

✓ చేయవలసినవి:

- **ఖాతాలను ధృవీకరించండి:** ప్రామాణికతను నిర్ధారించడానికి నీలి చెక్మార్కులు, స్థిరమైన వినియోగదారు పేర్లు మరియు పరిచితమైన ప్రొఫైల్ చిత్రాల కోసం చూడండి.
- **జాగ్రత్తగా ఉండండి:** అడగని సందేశాలను నివారించండి మరియు వ్యక్తిగత వివరాలను పంచుకోవద్దు లేదా అనుమానాస్పద లింక్లపై క్లిక్ చేయవద్దు.
- **నకిలీకరణను నివేదించండి:** ప్లాట్‌ఫారమ్ మరియు నకిలీ అయిన నిజమైన వ్యక్తి లేదా సంస్థకు తెలియజేయండి.
- **నిధుల అభ్యర్థనలను నిర్ధారించండి:** స్నేహితుల లేదా బంధువుల నుండి డబ్బు కోసం అభ్యర్థనలను ఫోన్ కాల్ లేదా వ్యక్తిగత సమావేశం ద్వారా ధృవీకరించండి

✗ చేయకూడనివి:

- **చెల్లింపులు చేయవద్దు:** తెలియని వ్యక్తులకు ఆన్‌లైన్‌లో చెల్లించడాన్ని మరియు నమ్మకం లేని / ధృవీకరించని చారిటీలను నివారించండి.
- **సమాచారాన్ని ప్రైవేట్‌గా ఉంచండి:** సోషల్ మీడియాలో వ్యక్తిగత లేదా రహస్య వివరాలను ఎప్పుడూ పంచుకోవద్దు.



ఎస్.ఎం.ఎస్, ఇమెయిల్ & కాల్ స్కామ్లు

ఎస్.ఎం.ఎస్, ఇమెయిల్ మరియు కాల్ స్కామ్లు నకిలీ ఆఫర్లతో బాధితులను మోసం చేయడానికి మోసగాళ్లు ఉపయోగిస్తారు. వారు వారి లోగోలు మరియు నకిలీ IDలను ఉపయోగించి నమ్మకమైన నాన్-బ్యాంకింగ్ ఫైనాన్సియల్ కంపెనీలను అనుకరిస్తారు, విశ్వసనీయతను పొందుతారు. మోసగాళ్లు ముందస్తు చెల్లింపులను అడుగుతూ నకిలీ మంజూరు లేఖలు లేదా చెక్లను పంపవచ్చు. చెల్లింపు చేసిన తర్వాత, మోసగాళ్లు డబ్బుతో మాయమైపోతారు.



✓ చేయవలసినవి:

- **ప్రామాణికతను ధృవీకరించండి:** ఎల్లప్పుడూ పంపిన వారి వివరాలను క్రాస్-చెక్ చేయండి మరియు అధికారిక మూలాలను నేరుగా సంప్రదించండి.
- **అనుమానాస్పద సందేశాలను నివేదించండి:** ఏదైనా నకిలీ సందేశాలను అధికారిక నివేదిక చానెళ్లకు ఫిర్యాద్ చేయండి మరియు ఇతరులను హెచ్చరించండి.

✗ చేయకూడనివి:

- **అడగని ఆఫర్లను నమ్మవద్దు:** ధృవీకరణ లేకుండా ఫోన్, ఇమెయిల్ లేదా టెక్స్ ద్వారా రుణ ఆఫర్లను ఎప్పుడూ నమ్మవద్దు.
- **సున్నితమైన సమాచారాన్ని పంచుకోవద్దు:** ఆఫర్ యొక్క చట్టబద్ధతను నిర్ధారించకుండా వ్యక్తిగత లేదా ఆర్థిక వివరాలను ఇవ్వడాన్ని నివారించండి.
- **లింక్లపై క్లిక్ చేయవద్దు లేదా అనుమానాస్పద ఇమెయిల్లను తెరవవద్దు:** అటాచ్మెంట్లు లేదా లింక్లతో తెలియని మూలాల నుండి లింక్లపై క్లిక్ చేయవద్దు లేదా ఇమెయిల్లను తెరవవద్దు.
- **ముందస్తు ఫీజులు చెల్లించవద్దు:** నిజమైన రుణదాతలు రుణ ప్రాసెసింగ్ కోసం ముందస్తు చెల్లింపులను కోరుకోరు.



డెబిట్/క్రెడిట్ కార్డ్ మోసం



డెబిట్ మరియు క్రెడిట్ కార్డ్ మోసం అంటే మీ అనుమతి లేకుండా మీ కార్డు వివరాలను అనధికారిక లావాదేవీలకు ఉపయోగించడం. నేరస్థులు మీ భౌతిక కార్డును దొంగిలించవచ్చు, మీ వివరాలను స్క్రిమ్ చేయవచ్చు, లేదా ఫిషింగ్ స్కాములద్వారా సునిశితమైన సమాచారాన్ని పంచుకోవడానికి మిమ్మల్ని మోసగించవచ్చు.

✓ చేయవలసినవి:

- **వాడని ఫీచర్లను నిష్క్రియం చేయండి:** అవసరం లేనప్పుడు ఆన్‌లైన్, అంతర్జాతీయ లేదా NFC లావాదేవీలను ఆఫ్ చేయండి.
- **చెల్లించే ముందు తనిఖీ చేయండి:** మీ PIN నమోదు చేసే ముందు స్క్రీన్‌పై మొత్తాన్ని ధృవీకరించండి మరియు స్క్రిమ్మింగ్ పరికరం కోసం POS మెషిన్‌ను తనిఖీ చేయండి.
- **మీ కార్డును కంటికి కనిపించేలా ఉంచుకోండి:** లావాదేవీల సమయంలో మీ కార్డును ఎప్పుడూ గమనిస్తూ ఉండండి.
- **మీ PIN ను సురక్షితంగా ఉంచుకోండి:** ATM లేదా POS మెషిన్లలో మీ PIN నమోదు చేసేటప్పుడు కీప్యాడ్‌ను కప్పండి.

✗ చేయకూడనివి:

- **వివరాలను షేర్ చేయకండి:** మీ కార్డు సమాచారం లేదా PIN ని ఎవరితోనూ పంచుకోకండి.
- **PIN ని నిల్వ చేయకండి:** సులభంగా యాక్సెస్ చేయగలిగే ప్రదేశాలలో మీ PIN ని రాయడం లేదా సేవ్ చేయడం చేయకండి.
- **పబ్లిక్ వైఫైని వాడకండి:** భద్రత లేని నెట్‌వర్క్‌లలో మీ కార్డును ఉపయోగించవద్దు.
- **అలర్ట్‌లను విస్మరించవద్దు:** అనుమానాస్పద లావాదేవీలను వెంటనే మీ బ్యాంకుకు నివేదించండి.



మొబైల్ అప్లికేషన్ APK స్కామ్



సైబర్ నేరగాళ్లు నకిలీ మొబైల్ బ్యాంకింగ్ అప్లికేషన్లను సృష్టిస్తారు, అవి అసలైన వాటిని పోలి ఉంటాయి, ఇందులో సమాన లోగోలు మరియు ఇంటర్‌ఫేస్‌లు ఉపయోగిస్తారు. ఈ అప్లికేషన్లు అనధికారిక అప్ డ్లైన్లు లేదా ఫిషింగ్ లింక్‌ల వంటి అనధికారిక ఛానెల్‌ల ద్వారా పంపిణీ చేయబడతాయి. ఒకసారి ఇన్స్టాల్ చేసిన తర్వాత, అవి మీ బ్యాంకింగ్ క్రెడిన్షియల్స్ మరియు వ్యక్తిగత డేటాను దోగిస్తాయి, ఆర్థిక మోసం మరియు గుర్తింపు దొంగతనానికి దారితీస్తుంది.

✓ చేయవలసినవి:

- అధికారిక స్టోర్ల నుండి డౌన్‌లోడ్ చేయండి: Google Play Store లేదా Apple App Store లేదా బ్యాంకు వెబ్‌సైట్‌ల వంటి విశ్వసనీయ మూలాల నుండి బ్యాంకింగ్ అప్‌లను ఎల్లప్పుడూ డౌన్‌లోడ్ చేయండి.
- అప్లికేషన్ ప్రామాణికతను ధృవీకరించండి: ఏదైనా బ్యాంకింగ్ అప్‌ని ఇన్‌స్టాల్ చేయడానికి ముందు డెవలపర్ వివరాలను తనిఖీ చేసి సమీక్షలను చదవండి.
- సాఫ్ట్‌వేర్‌ని నవీకరించి ఉంచండి: మీ ఫోన్ OS మరియు భద్రతా సాఫ్ట్‌వేర్ ఎల్లప్పుడూ తాజాగా ఉన్నాయని నిర్ధారించుకోండి.
- టూ-ఫ్యాక్టర్ ఆథెంటికేషన్ (2FA)ని ప్రారంభించండి: మీ ఖాతాలకు అదనపు భద్రతను జోడించండి.
- బ్యాంకు ఖాతాలను క్రమం తప్పకుండా పర్యవేక్షించండి: ఏదైనా అనధికారిక లావాదేవీల కోసం మీ బ్యాంకు ఖాతా స్టేట్‌మెంట్‌లను క్రమం తప్పకుండా సమీక్షించండి.

✗ చేయకూడనివి:

- అధికారికం కాని లింక్‌ల నుండి డౌన్‌లోడ్ చేయకండి: అనుమానాస్పద ఇమెయిల్‌లు లేదా వెబ్‌సైట్‌ల నుండి లింక్‌లను క్లిక్ చేయడం లేదా అప్‌లను డౌన్‌లోడ్ చేయడాన్ని నివారించండి.
- తెలియని అప్‌లలో సునిశితమైన సమాచారాన్ని నమోదు చేయకండి: అపరిచిత అప్‌లు లేదా సైట్‌లలో బ్యాంకింగ్ వివరాలను ఎప్పుడూ షేర్ చేయకండి.
- మీ పరికరాన్ని జైల్‌బ్రేక్ చేయకండి: మీ పరికరాన్ని రూటింగ్ చేయడం వల్ల మాల్వేర్ మరియు దాడులకు అది బలహీనంగా మారుతుంది.
- క్రెడిన్షియల్స్‌ని షేర్ చేయకండి: మీ బ్యాంకింగ్ PIN లేదా OTP ని ఎవరికీ షేర్ చేయకండి, వారు సపోర్ట్ సిబ్బంది అని చెప్పుకున్నప్పటికీ.



సైబర్ బానిసత్వం



సైబర్ బానిసత్వం అనేది డిజిటల్ ప్లాట్‌ఫారమ్ల ద్వారా వ్యక్తుల దోపిడీని కలిగి ఉంటుంది, అక్కడ వారు నిష్పక్షపాతమైన పరిహారం లేకుండా పని చేయడానికి బలవంతం చేయబడతారు లేదా మానిప్యూలేట్ చేయబడతారు. ఇది మానవ అక్రమ రవాణా మరియు బలవంతపు కార్మిక వ్యవస్థతో ఓవర్‌లాప్ అవుతుంది కానీ ప్రత్యేకంగా దోపిడీ కోసం ఇంటర్నెట్ మరియు డిజిటల్ సాధనాలను ఉపయోగిస్తుంది.

✓ చేయవలసినవి:

- **ధృవీకరించబడిన ఏజెంట్ల ద్వారా అప్లై చేయండి:** ప్రభుత్వం ఆమోదించిన ఏజెన్సీల ద్వారా మాత్రమే ఉద్యోగాలకు దరఖాస్తు చేయండి.
- **ఉద్యోగ ఆఫర్లను ధృవీకరించండి:** ఉద్యోగ ఆఫర్లను అంగీకరించడానికి ముందు వాటి చట్టబద్ధతను జాగ్రత్తగా తనిఖీ చేయండి.
- **ఆకర్షణీయంకా ఉండే ఉద్యోగ ఆఫర్ల పట్ల జాగ్రత్తగా ఉండండి:** తక్కువ పని కోసం అధిక జీతం ఇస్తామని హామీ ఇచ్చే ఆన్‌లైన్ అవకాశాల పట్ల జాగ్రత్తగా ఉండండి.
- **యజమానులను పరిశోధించండి:** ఉద్యోగాన్ని అందిస్తున్న కంపెనీ లేదా ప్లాట్‌ఫారమ్‌ను ఎల్లప్పుడూ పరిశోధించండి.
- **అనుమానాస్పద కార్యకలాపాన్ని నివేదించండి:** మీకు ఏదైనా మోసం లేదా దోపిడీ అనుమానం ఉంటే, cybercrime.gov.in యొక్క "రిపోర్ట్ సస్పెక్ట్ ట్యాబ్"పై వెంటనే నివేదించండి.

✗ చేయకూడనివి:

- **తక్కువ ప్రయత్నం గల ఆఫర్లను నివారించండి:** తక్కువ ప్రయత్నం లేదా పారదర్శకత కలిగి సులభంగా డబ్బు సంపాదించే అవకాశాలను నమ్మకండి.
- **పని కోసం టూరిస్ట్ వీసాను ఎప్పుడూ ఉపయోగించవద్దు:** టూరిస్ట్ వీసాలో విదేశాలలో పని చేయకండి.
- **ధృవీకరించబడని సోషల్ మీడియా ప్రకటనలు లేదా ఆఫర్లను నమ్మకండి:** సోషల్ మీడియాలో తెలియని వ్యక్తులు లేదా సమూహాల నుండి వచ్చే ప్రకటనలు లేదా ఆఫర్లను నమ్మకండి.



సిమ్ స్వాపింగ్



SIM స్వాపింగ్ అనేది మీ ఫోన్ నంబర్ను వారి SIM కార్డుకి బదిలీ చేసే సైబర్ నేరం. ఇది వారికి మీ కాల్స్, మెసేజ్లు మరియు ప్రమాణీకరణ కోడ్లకు ప్రాప్యతను ఇస్తుంది, గుర్తింపు దొంగతనం, ఖాతా హైజాకింగ్ మరియు ఆర్థిక మోసానికి అనుమతిస్తుంది. స్కామర్లు వ్యక్తిగత వివరాలను వెల్లడించడానికి మిమ్మల్ని మోసగించడానికి తరచుగా అప్గ్రేడ్లు లేదా ప్రయోజనాలను అందిస్తున్న నెట్వర్క్ సిబ్బందిగా మాట్లాడుతారు.

✓ చేయవలసినవి:

- **2-ఫ్యాక్టర్ ఆథెంటికేషన్ని ప్రారంభించండి:** మీ ఖాతాలకు అదనపు భద్రతను జోడించండి.
- **బలమైన PIN లను ఉపయోగించండి:** మీ ఖాతాలు మరియు SIM కోసం ప్రత్యేకమైన మరియు ఊహించడం కష్టమైన PIN లను సెట్ చేయండి.
- **అప్డేట్గా ఉండండి:** మీ ఫోన్ సాఫ్ట్వేర్ మరియు అప్లను క్రమం తప్పకుండా నవీకరించి ఉంచండి.
- **అనుమానాస్పద కార్యకలాపాన్ని నివేదించండి:** మీరు అసాధారణ కార్యకలాపాలను గమనిస్తే లేదా మీ SIM ని కోల్పోతే వెంటనే మీ నెట్వర్క్ ప్రొవైడర్ను సంప్రదించండి.

✗ చేయకూడనివి:

- **సమాచారాన్ని రక్షించుకోండి:** కాల్స్ లేదా మెసేజ్ల ద్వారా అపరిచితులతో సునిశితమైన డేటాను నిల్వ చేయకండి లేదా OTPలను పంచుకోకండి.
- **బలమైన PINలను ఉపయోగించండి:** మీ ఖాతాల కోసం సులభంగా ఊహించదగిన PINలను నివారించండి.
- **SIM నష్టాన్ని నివేదించండి:** మీ SIM కార్డ్ పోయినట్లయితే వెంటనే మీ నెట్వర్క్ ప్రొవైడర్కు తెలియజేయండి.
- **కార్యకలాపాన్ని పర్యవేక్షించండి:** అసాధారణ మొబైల్ కార్యకలాపాలు లేదా ఎక్కువ సమయం నెట్వర్క్ యాక్సెస్ లేకపోవడాన్ని గమనించి వెంటనే చర్య తీసుకోండి.
- **క్రెడిన్షియల్స్ను సురక్షితం చేయండి:** మీ SIM కార్డుకు సంబంధించిన గుర్తింపు వివరాలను ఎప్పుడూ షేర్ చేయకండి.



మనీ మ్యూల్స్



మనీ మ్యూల్స్ అనేవి చట్టవిరుద్ధంగా పొందిన నిధులను పెద్ద మొత్తం లో బదిలీ చేయడానికి తెలిసి లేదా తెలియకుండా ఉపయోగించే వ్యక్తులు. స్కామర్లు వారిని కమీషన్ల మారుగా దొంగిలించిన డబ్బును స్వీకరించడానికి మరియు బదిలీ చేయడానికి ఒప్పిస్తారు. మోసగాడి గుర్తింపును అస్పష్టం చేయడానికి ఈ నిధులు అనేక ఖాతాల ద్వారా తరలించబడతాయి. ఉద్దేశపూర్వకంగా లేదా లేకపోయినా, అటువంటి కార్యకలాపాల్లో పాల్గొనడం చట్టవిరుద్ధం మరియు తీవ్రమైన న్యాయపరమైన పరిణామాలు ఎదుర్కోవాల్సి ఉంటుంది.

✓ చేయవలసినవి:

- **ఉద్యోగ ఆఫర్లను పరిశీలించండి:** డబ్బు బదిలీలను కలిగి ఉన్న అడగని ఉద్యోగాల పట్ల జాగ్రత్తగా ఉండండి. కంపెనీ లేదా వ్యక్తి యొక్క చట్టబద్ధతను పరిశోధించండి.
- **ఆర్థిక సమాచారాన్ని కాపాడండి:** తెలియని పక్షాలతో బ్యాంకు ఖాతా వివరాలు లేదా వ్యక్తిగత సమాచారాన్ని ఎప్పుడూ పంచుకోకండి.
- **అనుమానాస్పద కార్యకలాపాన్ని నివేదించండి:** మీరు మనీ మ్యూల్ పథకంను అనుమానిస్తే అధికారులను సంప్రదించండి.

✗ చేయకూడనివి:

- **ఖాతాలను పంచుకోకండి:** నిధులను స్వీకరించడానికి లేదా బదిలీ చేయడానికి ఇతరులను మీ ఖాతాను ఉపయోగించనివ్వకండి.
- **కమీషన్లను తిరస్కరించండి:** ఫీజు కోసం అనధికార డబ్బును నిర్వహించడానికి ఆఫర్లను తిరస్కరించండి.
- **రిస్కులను తెలుసుకోండి:** చట్టబద్ధం కాని నిధులను బదిలీ చేయడం వల్ల తీవ్రమైన చట్టపరమైన చర్యలు ఎదుర్కోవాల్సి ఉంటుంది.



జ్యూస్ జాకింగ్



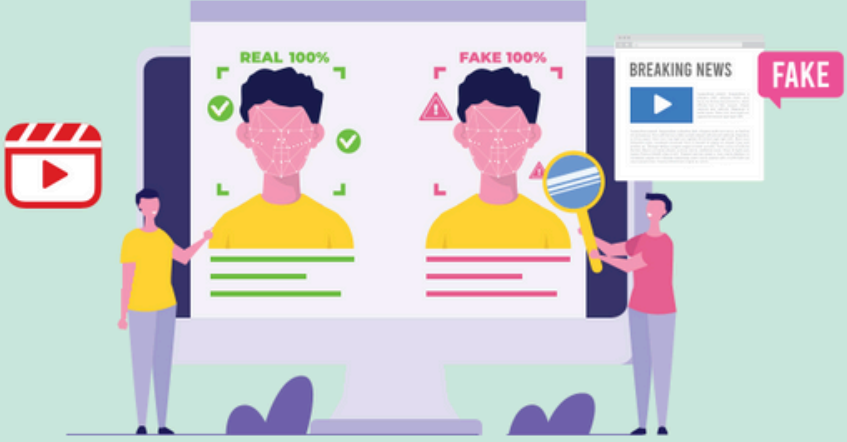
జ్యూస్ జాకింగ్ అంటే కంప్యూటర్ పబ్లిక్ USB ఛార్జింగ్ స్టేషన్లతో సంబంధం ఉన్న సైబర్ సెక్యూరిటీ రిస్క్. హ్యాకర్లు ఛార్జ్ మరియు డేటాను బదిలీ చేసే USB పోర్ట్లను ఉపయోగించుకోవచ్చు, మాల్వేర్స్ను ఇన్స్టాల్ చేయడానికి లేదా సునిశితమైన సమాచారాన్ని దొంగిలించడానికి వాటిని ఉపయోగించుకోవచ్చు. నిర్ధారించబడిన కేసులు లేకపోయినప్పటికీ, జాగ్రత్తగా ఉండటం అవసరం.

✓ చేయవలసినవి:

- **మీ ఛార్జర్ని తీసుకెళ్లండి:** అనుమానిత ప్రదేశాలలో పబ్లిక్ పోర్ట్లను నివారించడానికి మీ స్వంత ఛార్జర్ మరియు కేబుల్ని ఉపయోగించండి.
- **ప్రాంప్ట్లను ధృవీకరించండి:** "ఈ పరికరాన్ని నమ్మండి" ప్రాంప్ట్ల పట్ల జాగ్రత్తగా ఉండండి మరియు విశ్వసనీయ మూలాల నుండి మాత్రమే అంగీకరించండి.
- **AC ఔట్లెట్ల కోసం ఎంచుకోండి:** సాధ్యమైనప్పుడల్లా ప్రామాణిక విద్యుత్ ఔట్లెట్లను ఎంచుకోండి.

✗ చేయకూడనివి:

- **పబ్లిక్ పోర్ట్లను నివారించండి:** తెలియని లేదా పబ్లిక్ USB పోర్ట్లు లేదా కేబుల్లను ఉపయోగించవద్దు.



డిప్ ఫేక్ సైబర్ కైమ్



డిప్ ఫేక్ మోసంలో, సైబర్ నేరగాళ్లు అధునాతన AI ని ఉపయోగించి నకిలీ వీడియో/ఆడియో క్లిప్లను సృష్టిస్తారు, వాటిని సోషల్ మీడియా ద్వారా వ్యాప్తి చేస్తారు. వారు ప్రజలను మోసగించడానికి, అభిప్రాయాలను మానిప్యులేట్ చేయడానికి మరియు తప్పుడు సమాచారాన్ని వ్యాప్తి చేయడానికి సోషల్ ఇంజనీరింగ్ పద్ధతులను ఉపయోగిస్తారు.

✓ చేయవలసినవి:

- **సమాచారం తెలుసుకుంటూ ఉండండి:** డిప్ ఫేక్ టెక్నాలజీ మరియు దాని ప్రమాదాల గురించి తెలుసుకోండి.
- **కంటెంట్ ని ధృవీకరించండి:** పంచుకోవడానికి లేదా నమ్మడానికి ముందు మీడియా ప్రామాణికతను ఎల్లప్పుడూ తనిఖీ చేయండి.
- **విశ్వసనీయ మూలాలను ఉపయోగించండి:** వార్తలు మరియు అప్ డేట్ కోసం ప్రతిష్టాత్మక ప్లాట్ ఫారమ్లపై ఆధారపడండి.
- **అనుమానాస్పద కంటెంట్ ని నివేదించండి:** మీరు సంభావ్య డిప్ ఫేక్ లను కనుగొంటే అధికారులు లేదా ప్లాట్ ఫారమ్లకు హెచ్చరిక చేయండి.

✗ చేయకూడనివి:

- **ధృవీకరించని మీడియాను షేర్ చేయకండి:** దాని సత్యాన్ని తనిఖీ చేయకుండా కంటెంట్ ను వ్యాప్తి చేయకండి.
- **అనుమానాస్పద మూలాలను నమ్మకండి:** డిప్ ఫేక్ లను షేర్ చేయగల అవిశ్వసనీయ మూలాల నుండి దూరంగా ఉండండి.
- **గుడ్డిగా నమ్మకండి:** అతిశయోక్తిగా లేదా భావోద్వేగంగా అనిపించే కంటెంట్ పట్ల జాగ్రత్తగా ఉండండి.
- **గోప్యతను విస్మరించవద్దు:** గోప్యతా సెట్టింగ్ లను సమీక్షించండి మరియు మీరు ఆన్ లైన్ లో షేర్ చేసే వ్యక్తిగత సమాచారాన్ని తగ్గింపు చేయండి.



రిమోట్ యాక్సెస్ మోసం



రిమోట్ యాక్సెస్ మోసం నమ్మకమైన సంస్థలను సైబర్ నేరగాళ్లు నకిలీ చేసినప్పుడు జరుగుతుంది. వారు స్క్రీన్-షేరింగ్ అప్లికేషన్ల ద్వారా వారి పరికరాలకు అనధికారిక ప్రవేశాన్ని మంజూరు చేయడానికి వ్యక్తులను మోసగిస్తారు. ప్రవేశం ఇచ్చిన తర్వాత, వారు సున్నితమైన డేటాను దొంగిలించగలరు, ఖాతాలపై నియంత్రణను తీసుకోగలరు మరియు మోసపూరిత లావాదేవీలను నిర్వహించగలరు.

✓ చేయవలసినవి:

- **జాగ్రత్తగా ఉండండి:** మీకు తెలియని మరియు నమ్మకం లేని ఎవరికీ రిమోట్ యాక్సెస్ ని అనుమతించవద్దు.
- **గుర్తింపును నిర్ధారించండి:** కాలర్ గుర్తింపును మీరే నేరుగా నిర్ధారించుకోండి (వారు అందించిన నంబర్ల ద్వారా కాదు).
- **తెలియని సాఫ్ట్వేర్ ను నివారించండి:** మీకు నిశ్చయంగా తెలియకపోతే ఎవరి అభ్యర్థన మేరకు సాఫ్ట్వేర్ ను డౌన్లోడ్ చేయవద్దు.
- **జాగ్రత్తగా ఉండండి:** అనవసరమైన కాల్స్, సందేశాలు లేదా ఇమెయిల్ ల విషయంలో జాగ్రత్తగా ఉండండి.
- **భద్రతను పెంచండి:** బలమైన పాస్ వర్డ్ లను ఉపయోగించండి మరియు బహుళ-కారక ప్రమాణీకరణను ప్రారంభించండి.

✗ చేయకూడనివి:

- **సురక్షితంగా డౌన్లోడ్ చేయండి:** అవసరమైనప్పుడు మాత్రమే అధికారిక మూలాల నుండి స్క్రీన్-షేరింగ్ అప్లికేషన్లను ఇన్స్టాల్ చేయండి.
- **చెల్లింపు అప్లికేషన్లను సురక్షితం చేయండి:** ఏదైనా స్క్రీన్-షేరింగ్ సాఫ్ట్వేర్ ను డౌన్లోడ్ చేయడానికి ముందు అన్ని చెల్లింపు-సంబంధిత అప్లికేషన్ల నుండి లాగ్ అవుట్ చేయండి.
- **ఉపయోగం తర్వాత తొలగించండి:** పని పూర్తయిన తర్వాత స్క్రీన్-షేరింగ్ అప్లికేషన్ ను అన్ ఇన్స్టాల్ చేయండి.
- **మీ డేటాను రక్షించండి:** వ్యక్తిగత లేదా ఆర్థిక సమాచారాన్ని రిమోట్ గా పంచుకోవద్దు మరియు ఎవరికైనా స్క్రీన్ యాక్సెస్ ఉన్నప్పుడు ఖాతా వివరాలను నమోదు చేయడం నివారించండి.



సురక్షిత బ్రౌజింగ్



సురక్షిత బ్రౌజింగ్ అంటే ఇంటర్నెట్‌లో సర్పింగ్ చేసేటప్పుడు ఫిషింగ్, మాల్వేర్ మరియు గుర్తింపు దొంగతనం వంటి ఆన్‌లైన్ ముప్పుల నుండి మిమ్మల్ని రక్షించడానికి పద్ధతులు మరియు సాధనాలను ఉపయోగించడం. ఇది వెబ్‌సైట్‌లతో సురక్షితమైన పరస్పర చర్యలను నిర్ధారిస్తుంది మరియు సైబర్ ప్రమాదాలను తగ్గిస్తుంది.

✓ చేయవలసినవి:

- సురక్షిత బ్రౌజర్‌లను ఉపయోగించండి: ఎప్పుడూ నవీకరించబడిన, సురక్షిత బ్రౌజర్‌లతో బ్రౌజ్ చేయండి మరియు సైట్‌లు HTTPS ని ఉపయోగిస్తున్నాయని నిర్ధారించుకోండి.
- యాంటీవైరస్‌ని ఇన్‌స్టాల్ చేయండి: మీ పరికరాన్ని విశ్వసనీయమైన యాంటీవైరస్ సాఫ్ట్‌వేర్‌తో రక్షించండి.
- URL లను ధృవీకరించండి: సున్నితమైన సమాచారాన్ని నమోదు చేయడానికి ముందు వెబ్‌సైట్ లింక్‌లను తనిఖీ చేయండి.
- ఫైర్‌వాల్‌లను ప్రారంభించండి: అదనపు భద్రతా కొరకు ఫైర్‌వాల్‌లను ఉపయోగించండి.

✗ చేయకూడనివి:

- తెలియని లింక్‌లను క్లిక్ చేయడాన్ని నివారించండి: ధృవీకరించబడని లేదా అనుమానాస్పద లింక్‌ల నుండి దూరంగా ఉండండి.
- పబ్లిక్ వైఫైలో జాగ్రత్తగా ఉండండి: రక్షణ లేకుండా అసురక్షిత పబ్లిక్ వైఫైని ఉపయోగించవద్దు.
- పబ్లిక్ పరికరాలలో పాస్‌వర్డ్‌లను సేవ్ చేయవద్దు: షేర్ చేసిన లేదా పబ్లిక్ కంప్యూటర్‌లలో లాగిన్ క్రెడిన్షియల్స్‌ను నిల్వ చేయడాన్ని నివారించండి.
- అసురక్షిత సైట్‌లను దాటవేయండి: బ్రౌజర్ హెచ్చరికలను విస్మరించవద్దు మరియు ప్లాగ్ చేయబడిన లేదా అసురక్షిత వెబ్‌సైట్‌లను సందర్శించడాన్ని నివారించండి.



రాన్సమ్వేర్



రాన్సమ్వేర్ అనేది హానికరమైన సాఫ్ట్వేర్, ఇది బాధితుల ఫైల్లను లాక్ చేస్తుంది, వాటిని యాక్సెస్ చేయలేకుండా చేస్తుంది. ఫైల్లను అన్లాక్ చేయడానికి వారు డబ్బులు డిమాండ్ చేస్తారు. రాన్సమ్వేర్ ఫిషింగ్ ఇమెయిల్లు, హానికరమైన సాఫ్ట్వేర్ డౌన్లోడ్లు మరియు భద్రతా లోపాల ద్వారా వ్యాప్తి చెందుతుంది. ఇది వ్యక్తులు మరియు సంస్థలకు తీవ్రమైన ముప్పు కలిగిస్తుంది, గణనీయమైన డేటా నష్టం మరియు ఆర్థిక నష్టాన్ని కలిగిస్తుంది.

✓ చేయవలసినవి:

- **డేటాను బ్యాకప్ చేయండి:** నష్టాన్ని నివారించడానికి మీ డేటాను క్రమం తప్పకుండా బ్యాకప్ చేయండి.
- **కంటెంట్ స్కానింగ్ని ఉపయోగించండి:** హానికరమైన ఫైల్లను గుర్తించడానికి సకాలంలో కంటెంట్ స్కానింగ్ మరియు ఫిల్టరింగ్ని అమలు చేయండి.
- **సిస్టమ్లను అప్డేట్ చేయండి:** భద్రతా లోపాలను సరిదిద్దడానికి మీ సిస్టమ్లు మరియు సాఫ్ట్వేర్ని నవీకరించి ఉంచండి.
- **ఉద్యోగి శిక్షణ:** ఫిషింగ్ ప్రయత్నాలు మరియు ఇతర హానికరమైన కార్యకలాపాలను గుర్తించడానికి మరియు నివారించడానికి ఉద్యోగులకు శిక్షణ ఇవ్వండి.

✗ చేయకూడనివి:

- **రాన్సమ్ చెల్లించడాన్ని నివారించండి:** రాన్సమ్ చెల్లించవద్దు, ఎందుకంటే ఇది డేటా తిరిగి వస్తుందని హామీ ఇవ్వదు మరియు మరిన్ని దాడులను ప్రోత్సహిస్తుంది.
- **వ్యక్తిగత సమాచారాన్ని రక్షించండి:** అపరిచిత వనరులకు వ్యక్తిగత సమాచారాన్ని అందించవద్దు.
- **దాడిని కంట్రీన్ చేయండి:** దాడి వ్యాప్తి చెందడానికి అనుమతించవద్దు. ప్రభావిత వ్యవస్థలను వెంటనే ఐసోలేట్ చేయండి.
- **దాడి సమయంలో బ్యాకప్లను అమలు చేయడాన్ని నివారించండి:** దాడి సమయంలో బ్యాకప్లను అమలు చేయవద్దు, ఎందుకంటే అవి కూడా లాక్ కావచ్చు.



స్మార్ట్ఫోన్ స్కామ్లు



మొబైల్ స్కామ్లు పెరుగుతున్నాయి, మోసగాళ్లు డేటా మరియు డబ్బును దొంగిలించడానికి నకిలీ కాల్లు, హానికరమైన అప్లికేషన్లు మరియు సిమ్-సంబంధిత మోసాలను ఉపయోగిస్తున్నారు. మోసగాళ్లు తరచుగా వ్యక్తిగత వివరాలను పంచుకోవడానికి వినియోగదారులను మోసం చేయడానికి చట్టబద్ధమైన ఏజెన్సీలుగా తమను తాము మారాకాల్పిస్తారు. ఈ భద్రతా చర్యలను పాటించడం ద్వారా మిమ్మల్ని మీరు రక్షించుకోండి.

✓ చేయవలసినవి:

- **దొంగిలించబడిన ఫోన్లను నివేదించండి:** పోలీసులకు మరియు <https://sancharsaathi.gov.in/> కి పోగొట్టుకున్న లేదా దొంగిలించబడిన ఫోన్లను వెంటనే నివేదించండి.
- **సిమ్ రిజిస్ట్రేషన్లను తనిఖీ చేయండి:** మీ పేరుతో నమోదు చేయబడిన సిమ్ల సంఖ్యను క్రమం తప్పకుండా తనిఖీ చేయండి.
- **స్వామ్ కాల్లను నివేదించండి:** స్వాఫింగ్ కాల్లను నివేదించండి మరియు స్వామ్ కాల్లను బ్లాక్ చేయడానికి DND లో నమోదు చేయండి.
- **ధృవీకరించబడిన స్టోర్లను మాత్రమే ఉపయోగించండి:** ఫ్లే స్టోర్ లేదా యాప్ స్టోర్ వంటి అధికారిక స్టోర్ల నుండి మాత్రమే అప్లికేషన్లను డౌన్లోడ్ చేయండి.
- **IMEI నంబర్ను ట్రాక్ చేయండి:** <https://sancharsaathi.gov.in/> పోర్టల్ని ఉపయోగించి మీ IMEI నంబర్ను రికార్డు చేయండి.

✗ చేయకూడనివి:

- **తెలియని మూలాలను నివారించండి:** సోషల్ మీడియా గ్రూప్లలో లేదా ధృవీకరించబడని మూలాల నుండి స్వీకరించిన అప్లికేషన్లను డౌన్లోడ్ చేయడాన్ని నివారించండి.
- **సిమ్ పరిమితిని తనిఖీ చేయండి:** మీరు అనుమతించబడిన పరిమితి 9 సిమ్లు (జమ్ము & కాశ్మీర్, అస్సాం కోసం 6) మించలేదని నిర్ధారించుకోండి.
- **స్వామ్ కాల్లను విస్మరించండి:** స్వామ్ కాల్కు ఎప్పటికీ సమాధానం ఇవ్వకండి. వాటిని వెంటనే బ్లాక్ చేయండి.
- **అనవసరమైన సిమ్ కనెక్షన్లను తొలగించండి:** మీ పేరుతో అడగని సిమ్ కనెక్షన్లను ఉంచవద్దు.
- **WhatsApp సెట్టింగ్లను మార్చండి:** స్వామ్ కాల్లను నివారించడానికి WhatsAppలో "అపరిచిత కాలర్లను నిశ్చలం చేయండి" ని ప్రారంభించండి.



ఇలాంటి సైబర్ నేరాలను
www.cybercrime.gov.in లో
లేదా

1930 కు



కాల్ చేసి నివేదించండి.

