డిజిటల్ సేఫ్టీ & సెక్యూరిటీ

Samhita CGF

కార్యక్రమ పరిచయం

ప్రభుత్వ మరియు ప్రైవేట్ సేవల డిజిటలైజేషన్ మరియు డిజిటల్ కమ్యూనికేషన్లు, ముఖ్యంగా సోషల్ మీడియా రాక వినియోగదారుల ఆర్థిక సమగ్రత మరియు వ్యక్తిగత గోప్యతపై ముఖ్యమైన చిక్కులను కలిగి ఉంది. సైబర్ క్రైమ్ మరియు డిజిటల్ మోసాల వల్ల డిజిటల్ భద్రతకు కలిగే నష్టాలను గుర్తించడానికి మరియు నివారించడానికి గరిష్ట స్థాయి డిజిటల్ అక్షరాస్యత తప్పనిసరి అవుతుంది.

ఇంటర్నెట్ మరియు స్మార్ట్ఫోన్ల యొక్క పెరుగుతున్న పరిధి ఆన్లైన్ మోసాలకు గురయ్యేలా చేసింది మరియు మన డేటాకు సంభావ్య ఆన్లైన్ ప్రమాదాల కారణంగా మన భద్రతను ప్రమాదంలోకి నెట్టింది. మన వ్యక్తిగత సమాచారాన్ని ప్రమాదంలో పడేసే మరియు మన మానసిక శ్రేయస్సును కూడా ప్రభావితం చేసే ఈ ప్రమాదాల నుండి మనల్ని మనం రక్షించుకోవాలి.

- డిజిటల్ భద్రత మరియు భద్రత అంటే ఏమిటి?
- ఆర్థిక మోసాలు మరియు వాటి నివారణ
- సోషల్ మీడియా ప్లాట్‌ఫారమ్‌లు, స్కామ్‌లు మరియు మర్యాదలు
- గుర్తింపు దొంగతనం నుండి మనల్ని మనం రక్షించుకోవడం
- ఇంటర్నెట్ స్మార్ట్ గా ఉండటం
- డిజిటల్ హక్కులు, చట్టాలు మరియు పరిష్కార విధానాలు

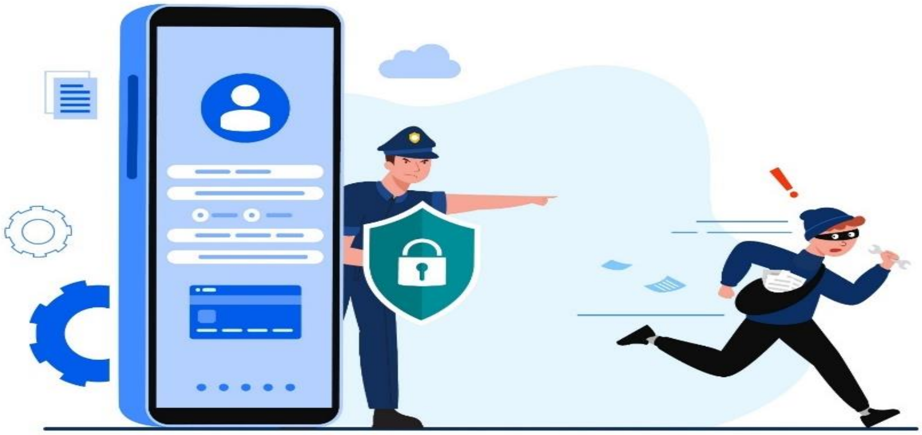
ఈ ప్రోగ్రామ్ లో, మనం వీటి గురించి నేర్చుకుంటాం:

ఈ హ్యాండ్ బుక్ ఆన్ లైన్ ప్రోగ్రామ్ లో కీలక భావనల అభ్యసనను పునఃసమీక్షించే ప్రయత్నం చేసింది. 20 ప్రాక్టికల్ యాక్టివిటీలు చివర్లో జాబితా చేయబడ్డాయి, 6 మాడ్యూల్స్ నుంచి నేర్చుకోవడాన్ని బలోపేతం చేయడం కొరకు వాటిని ప్రాక్టీస్ వర్క్ గా చేయమని మేం మిమ్మల్ని కోరుతున్నాం.

విషయ పట్టిక[మార్చు]

మాడ్యూల్ 1	1
డిజిటల్ సేఫ్టీ అండ్ సెక్యూరిటీ పరిచయం	1
మాడ్యూల్ 2	10
ఆర్థిక కుంభకోణాలు మరియు వాటి నివారణ	10
మాడ్యూల్ 3	16
సోషల్ మీడియా	16
మాడ్యూల్ 4	25
గుర్తింపు దొంగతనం	**36**
మాడ్యూల్ 5	**36**
ఇంటర్నెట్ స్మార్ట్36	**36**
మాడ్యూల్ 6	**45**
డిజిటల్ హక్కులు, చట్టాలు మరియు పరిష్కార యంత్రాంగాలు	**45**
సూచించిన ఆచరణాత్మక కార్యకలాపాలు	**54**

మాడ్యూల్ 1
డిజిటల్ సేఫ్టీ అండ్ సెక్యూరిటీ పరిచయం



డిజిటల్ భద్రత మరియు భద్రత అంటే ఏమిటి?

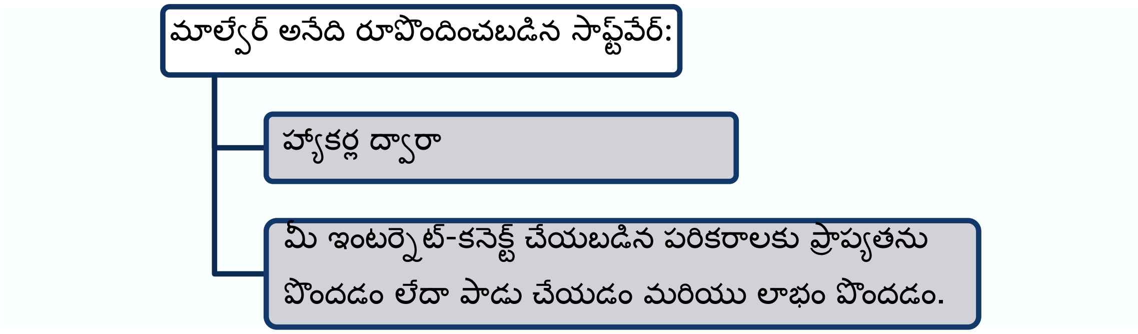
డిజిటల్ సేఫ్టీ అండ్ సెక్యూరిటీ అనేది కంప్యూటర్లు, మొబైల్ పరికరాలు, టాబ్లెట్లు మొదలైన ఇంటర్నెట్ కనెక్టెడ్ పరికరాలను సంరక్షించడాన్ని సూచిస్తుంది. చోరబాటుదారులు లేదా హ్యాకర్ల నుండి.

ఫిషింగ్

క్రెడిట్ కార్డ్ నంబర్, బ్యాంక్ సమాచారం వంటి వ్యక్తిగత సమాచారాన్ని బహిర్గతం చేయడానికి ప్రలోభాన్ని ఉపయోగించి ఒక వ్యక్తి యొక్క డబ్బు లేదా గుర్తింపును దొంగిలించడానికి ప్రయత్నించే డిజిటల్ మాధ్యమం ద్వారా దాడిని ఫిషింగ్ అంటారు.

ఇ-మెయిల్స్ మీ పరికరానికి హాని కలిగించే లేదా కార్డు వివరాలు, పాస్వర్డ్లు వంటి మీ సున్నితమైన డేటాను దొంగిలించే వైరస్లను తీసుకెళ్లగలవు. దీనిని **ఫిషింగ్** అని పిలుస్తారు, ఇది అనేక రకాల సైబర్ దాడులలో ఒకటి.

Malware:



డిజిటల్ భద్రత మరియు భద్రతను ధృవీకరించడం

స్పామ్ మెయిల్‌లపై లేదా తెలియని పంపినవారి నుండి వచ్చే మెయిల్‌లపై ఎప్పుడూ క్లిక్ చేయవద్దు

ఎల్లప్పుడూ మీ వ్యక్తిగత భద్రత

యాంటీ వైరస్ సాఫ్ట్‌వేర్‌లతో మీ పరికరాన్ని భద్రపరచండి

మీరు సైబర్ మోసాన్ని అనుమానించినట్లయితే, వెంటనే సంబంధిత సంస్థకు కాల్ చేయండి, ఫిర్యాదును నమోదు చేయండి మరియు మీ ఖాతా భద్రతను నిర్ధారించడానికి ఉత్తమమైన చర్య తీసుకోవాలని వారిని అడగండి

ప్రభుత్వంలో ఫిర్యాదు చేయండి. భారతదేశ ఆన్‌లైన్ సైబర్ క్రైమ్ సెల్

డిజిటల్ భద్రత మరియు భద్రత యొక్క ప్రయోజనాలు

- 24*7 సురక్షితమైన మరియు సురక్షితమైన బ్యాంకింగ్ అనుభవం
- మీ శాఖను సందర్శించకుండానే అవాంతరాలు లేని మరియు తక్షణ లావాదేవీలు
- ఆర్థిక నష్టాన్ని నివారిస్తుంది
- ఫిషింగ్, పాస్‌వర్డ్ దాడి మొదలైన సైబర్ దాడుల నుండి రక్షణ
- లావాదేవీల కోసం సురక్షితమైన/ప్రైవేట్ విండోను అందిస్తుంది

సైబర్ సెక్యూరిటీ మరియు గోప్యతాఅపోహలు

నెంబరు	పురాణం	వాస్తవికత
1.	బలమైన పాస్ వర్డ్ లు మన పరికరాలను మరియు వాటిలో నిల్వ చేయబడిన డేటాను రక్షిస్తాయి.	బలమైన పాస్ వర్డ్ లతో పాటు టూ ఫ్యాక్టర్ అథెంటికేషన్, డేటా మానిటరింగ్ ఉండాలి.
2.	హ్యాకర్లు లేదా సైబర్ నేరగాళ్లు చిన్న వ్యాపారాలు మరియు ఉద్యోగులు, గృహిణులు, స్వయం ఉపాధి వంటి వ్యక్తులపై దాడి చేయరు.	అధునాతన భద్రతా పరిష్కారాలు మరియు అవగాహన లేకపోవడం వల్ల, ఇటువంటి చిన్న వ్యాపారాలు మరియు ప్రజలు హ్యాకర్లు లేదా సైబర్ నేరగాళ్లకు మృదువైన లక్ష్యాలు.
3.	యాంటీ వైరస్/యాంటీ మాల్వేర్ సాఫ్ట్వేర్ మన డివైజ్లు లేదా డేటాను భద్రపరుచుకుంటే సరిపోతుంది.	యాంటీ-వైరస్/యాంటీ-మాల్వేర్ సాఫ్ట్వేర్ వైరస్లు మరియు మాల్వేర్ల నుండి పరికరాన్ని మాత్రమే రక్షిస్తుంది, కానీ సమాచారాన్ని తిరిగి పొందడానికి ఫేక్ కాల్ వంటి సైబర్ నేరాల యొక్క అనేక ఇతర మాధ్యమాలు ఉన్నాయి
4.	హ్యాకర్ల నుంచి మన డివైజ్లను కాపాడుకుంటే చాలు.	ఏదైనా అంతర్గత వ్యక్తి/ఉద్యోగి ఉద్దేశపూర్వకంగా లేదా పొరపాటున సమాచారాన్ని లీక్ చేయవచ్చు.
5.	ఇంటర్నెట్ సర్వీస్ ప్రొవైడర్ యొక్క ఐటి విభాగం మాత్రమే సైబర్ భద్రతకు బాధ్యత వహిస్తుంది.	హ్యాకర్ల నుండి మరియు వారి చుట్టూ ఉన్న చొరబాటుదారుల నుండి వారి వ్యక్తిగత లేదా వృత్తిపరమైన సమాచారం మరియు పరికరాన్ని రక్షించడం ప్రతి వ్యక్తి యొక్క సామాజిక బాధ్యత.
6.	యాప్ ను యాప్ స్టోర్ నుంచి డౌన్ లోడ్ చేసుకుంటే సురక్షితం.	యాప్ స్టోర్ లోని యాప్ లు వైరస్ లు/మాల్ వేర్ మరియు గోప్యతా విధానానికి వ్యతిరేకంగా టెస్టింగ్ మరియు వెరిఫికేషన్ కు వెళ్లాలి.
7.	పాస్ వర్డ్ రక్షిత వై-ఫై ఏదైనా సురక్షితం.	పాస్వర్డ్ కూడా ఏదైనా పబ్లిక్ వై-ఫై కనెక్షన్ మీ పరికరానికి ముప్పు కావచ్చు. పబ్లిక్ Wi-Fi కనెక్షన్ ద్వారా ఎలాంటి గోప్యమైన సమాచారం లేదా డాక్యుమెంట్ ని ఎప్పుడూ పంచుకోవద్దు.
8.	మీ స్వంత పరికరాన్ని తీసుకురండి లేదా పని వద్ద ఉపయోగించడం కొరకు బైఓడీ సురక్షితం	ఇంటర్నెట్ కు కనెక్ట్ చేయబడిన ఏ పరికరం అయినా డిజిటల్ బెదిరింపులకు గురయ్యే అవకాశం ఉంది.
9.	HTTPS వెబ్ సైట్ లు విశ్వసనీయమైనవి మరియు హ్యాక్ చేయబడవు	హ్యాకర్లు హెచ్ టిటిపిఎస్ ఎన్ క్రిప్షన్ ను దాటవేయవచ్చు; అందువల్ల, విశ్వసనీయమైన HTTPS వెబ్ సైట్ లను మాత్రమే

		ఉపయోగించండి, ఉదా. బ్యాంకు ద్వారా భాగస్వామ్యం చేయబడిన మీ బ్యాంక్ వెబ్ సైట్.
10.	ఏదైనా ఉల్లంఘనకు వ్యతిరేకంగా 100% సైబర్ భద్రత సాధించవచ్చు.	రోజుకో కొత్త ముప్పు పుట్టుకొస్తోంది. 100% సైబర్ సెక్యూరిటీ సాధించలేం.

ఈ **ఉత్తమ పద్ధతులను** అనుసరించడం ద్వారా, మీరు సైబర్ క్రైమ్ బాధితుడిగా ఉండకుండా ఉండవచ్చు:

- ✓ బ్రౌజర్ని ఉపయోగిస్తున్నప్పుడు ఎల్లప్పుడూ అజ్ఞాత మోడ్ని ఉపయోగించండి.
- ✗ బ్రౌజర్లో ఆధారాలను ఎప్పుడూ సేవ్ చేయవద్దు.
- ✗ మూడవ పక్షం లింక్ నుండి యాప్‌లను ఎప్పుడూ డౌన్‌లోడ్ చేయవద్దు.
- ✗ అసురక్షిత వెబ్‌సైట్/యాప్‌లో వ్యక్తిగత సమాచారాన్ని ఎప్పుడూ షేర్ చేయవద్దు.
- ✓ మీ యాంటీవైరస్ అప్‌డేట్‌గా ఉంచండి.
- ✗ వైరస్ స్కానింగ్ లేకుండా ఏ ఫైల్‌ను డౌన్‌లోడ్ చేయవద్దు.
- ✓ మీ డేటా యొక్క బ్యాకప్‌ను ఉంచండి.
- ✗ మీ పరికరాన్ని గమనించకుండా ఎప్పుడూ ఉంచవద్దు.
- ✗ మీ పాస్‌వర్డ్‌లను ఎప్పుడూ షేర్ చేయవద్దు.
- ✓ ఎల్లప్పుడూ రెండు-కారకాల ప్రమాణీకరణను ఉపయోగించండి.

పాస్వర్డ్లు

పాస్ వర్డ్ అనేది కంప్యూటర్ సిస్టమ్ లేదా సేవకు ప్రాప్యతను అనుమతించే అక్షరాల స్ట్రింగ్. ప్రత్యేకమైన పాస్ వర్డ్ సృష్టించడానికి

1. వరుస అక్షరాలు లేదా సంఖ్యలను పరిహరించండి
2. వ్యక్తిగత సమాచారాన్ని నివారించండి
3. పొడవైన పాస్ వర్డ్ లు తయారు చేయండి
4. సంబంధం లేనిపదాలను ఉపయోగించండి

విభిన్న అప్లికేషన్ ల కొరకు విభిన్న పాస్ వర్డ్ లను ఉపయోగించండి మరియు మీ పాస్ వర్డ్ లను తరచుగా మార్చండి.

సమాచారానికి అనధికారిక ప్రాప్యత గుర్తింపు దొంగతనం, ఆర్థిక నష్టం, డిజిటల్ కుంభకోణాలకు పెరిగిన బలహీనత లేదా వేధింపులతో సహా ప్రమాదాలకు దారితీస్తుంది.

వన్-టిపాస్ వర్డ్ (OTP):

ఒటిపిలు వన్ టైమ్ పాస్ వర్డ్ లు, ఇవి ఆన్ లైన్ ఆర్థిక లావాదేవీలకు భద్రతన
మీ ఒటీపీని గోప్యంగా ఉంచడానికి

1. మీ ఒటీపీని ఎప్పుడూ షేర్ చేయకండి.
2. లావాదేవీ పూర్తయిన తర్వాత ఒటీపీని డిలీట్ చేయండి.
3. ఎల్లప్పుడూ అధికారిక వెబ్సైట్ల ద్వారా లాగిన్ అవ్వండి.
4. తెలియని యాప్ లను ఎప్పుడూ డౌన్ లోడ్ చేసుకోవద్దు.

ఒటిపిలను దొంగిలించడానికి కొన్ని సాధారణ మార్గాలు:

1. బ్యాంకు అధికారులుగా నటించి మీ ఖాతా వివరాలను వెరిఫై చేయమని అడగడం ద్వారా.
2. ఎస్ ఎంఎస్ లేదా వాట్సప్ ద్వారా లింక్ లు పంపడం, వాటిని క్లిక్ చేసినప్పుడు మాల్ వేర్ ను వ్యాప్తి చేయడం ద్వారా.
3. స్క్రీన్ షేరింగ్ యాప్ ను డౌన్ లోడ్ చేసుకోమని మిమ్మల్ని అడగడం ద్వారా మీ డేటాకు రిమోట్ యాక్సెస్ పొందవచ్చు.

క్రెడిట్/డెబిట్ కార్డు మోసాలు:

ఎవరైనా మీకు తెలియకుండా ఆర్థిక లావాదేవీల కోసం మీ క్రెడిట్ కార్డు సమాచారాన్ని చట్టవిరుద్ధంగా ఉపయోగించినప్పుడు క్రెడిట్ / డెబిట్ కార్డు మోసం జరుగుతుంది.

డెబిట్/క్రెడిట్ కార్డు మోసాల నుండి సురక్షితంగా ఉండటం:

1. మీ కార్డును ఎల్లప్పుడూ మీతో ఉంచుకోండి.
2. మీ పిన్ ను క్రమం తప్పకుండా మార్చుకోండి.
3. మీ పిన్ ను ఎవరితోనూ పంచుకోవద్దు.
4. మీ నెలవారీ క్రెడిట్ కార్డ్ స్టేట్ మెంట్ ని జాగ్రత్తగా చెక్ చేయండి
5. తెలియని వెబ్ సైట్లు లేదా యాప్ లలో మీ కార్డును ఉపయోగించడం మానుకోండి.
6. అనుమానాస్పద లింకులను క్లిక్ చేయవద్దు.
7. మీ కార్డు దొంగిలించబడినా లేదా పోయినా వెంటనే మీ బ్యాంకుకు తెలియజేయండి.

డాక్యుమెంట్ ఫ్రాడ్ ప్రీ-ఎంప్షన్

మోసగాళ్లు వివిధ కారణాలతో ఆధార్, పాన్ కార్డు వంటి నకిలీ పత్రాలను నకిలీ చేస్తున్నారు. వారు నకిలీ పత్రాలను ఉపయోగిస్తారు:

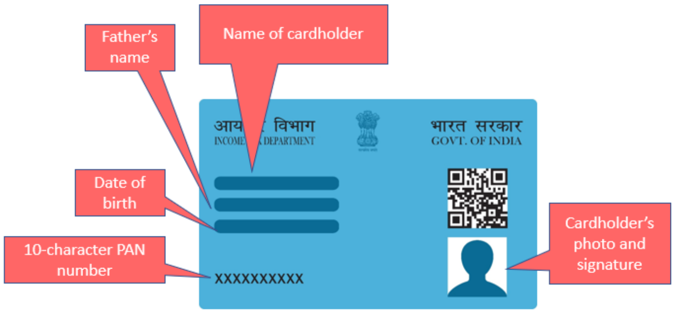
1. కొత్త బ్యాంకు ఖాతా తెరవండి
2. రుణాల కోసం దరఖాస్తు చేసుకోండి
3. ప్రాపర్టీ కొనుగోలు చేయండి
4. ఆదాయపు పన్ను రిటర్న్స్/ ఇన్సూరెన్స్ ఫైలింగ్స్ ఫైల్ చేయండి

ఆధార్ కార్డు ఎంత ముఖ్యమో..

1. ప్రతి నివాస భారతీయుడిని గుర్తించడానికి వీలు కల్పిస్తుంది.
2. చిరునామా రుజువుగా పనిచేస్తుంది.
3. గుర్తింపు రుజువుగా పనిచేస్తుంది.
4. హోల్డర్లు ప్రభుత్వ సబ్సిడీలను పొందడానికి వీలు కల్పిస్తుంది.
5. బ్యాంకు ఖాతా తెరిచేటప్పుడు గుర్తింపు కోసం ఉపయోగించవచ్చు.
6. ఉద్యోగాలకు దరఖాస్తు చేసేటప్పుడు గుర్తింపు కోసం ఉపయోగించవచ్చు.

ఈ క్రింది లావాదేవీలలో దేనినైనా నిర్వహించడానికి మాకు **పాన్** కార్డు అవసరం:

1. బ్యాంకు ఖాతా తెరిచి..
2. పన్ను రిటర్నులు దాఖలు చేయడం..
3. కొత్త రుణం కోసం దరఖాస్తు చేసుకుంటారు.
4. కొత్త ప్రాపర్టీ క్రయవిక్రయాలు.
5. డెబిట్/క్రెడిట్ కార్డుల కొనుగోలు..
6. బీమా ప్రీమియం చెల్లింపులు చేయడం



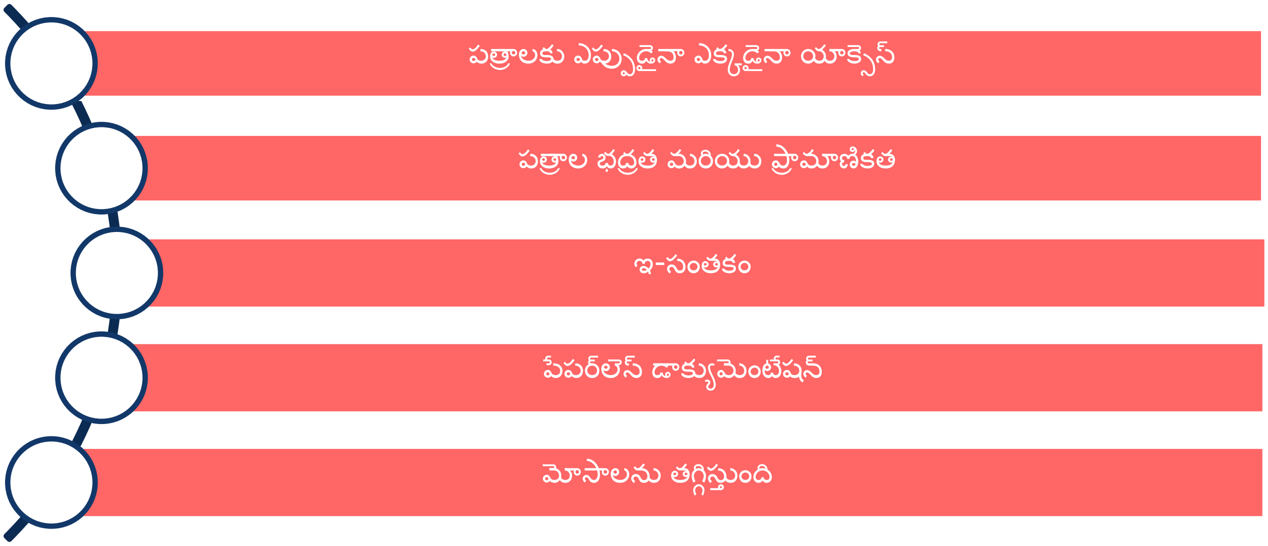
ఆధార్/పాన్ కార్డు మోసాల నుంచి సురక్షితంగా ఉండాలంటే..

1. సాధారణ లావాదేవీల కోసం మీ ఆధార్ లేదా పాన్ కార్డును ఉపయోగించవద్దు.
2. ఆధార్, పాన్ కార్డు వివరాలను ఇతరులతో పంచుకోవద్దు.
3. మీ ఆధార్ లేదా పాన్ కార్డుల యొక్క సంతకం చేసిన ఫోటో కాపీలను మాత్రమే ఉపయోగించడానికి నిర్దిష్ట కారణం మరియు ఉపయోగించిన తేదీతో సమర్పించడానికి ప్రయత్నించండి.
4. ఆన్లైన్ పోర్టళ్లలో మీ పూర్తి పేరు, పుట్టిన తేదీని నమోదు చేయవద్దు.

ముఖ్యమైన డాక్యుమెంట్లను సురక్షితంగా ఉంచడం

డిజిలాకర్ అనేది డిజిటల్ లాకర్, ఇది ఆధార్, పాన్, డ్రైవింగ్ లైసెన్స్, పాస్పోర్ట్, మార్క్ షీట్లు, ఎలక్టోరల్ ఓటరు గుర్తింపు కార్డు వంటి అధికారిక పత్రాల స్కాన్ చేసిన కాపీలను నిల్వ చేయడానికి మిమ్మల్ని అనుమతిస్తుంది. ఈ డాక్యుమెంట్లను మీరు ఎక్కడైనా, ఎప్పుడైనా యాక్సెస్ చేసుకోవచ్చు.

డిజిలాకర్ ప్రయోజనాలు



రిఫరెన్స్ రీడింగ్:

- సైబర్ స్వచ్ఛతా కేంద్రం : https://www.csk.gov.in/
- భారతదేశంలో సైబర్ నేరాలపై పూర్తి గైడ్ : https://indiaforensic.com/compcrime.htm
- జి 20 ప్రెసిడెన్సీ యొక్క భారతదేశం యొక్క సైబర్ సెక్యూరిటీ ప్రాధాన్యతలు : https://www.orfonline.org/expert-speak/indias-cybersecurity-priorities-for-g20-presidency/
- ఇండియన్ సైబర్ క్రైమ్ కోఆర్డినేషన్ సెంటర్ వివరాలు: https://www.mha.gov.in/en/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme

మాడ్యూల్ 2

ఆర్థిక కుంభకోణాలు మరియు వాటి నివారణ

ఆర్థిక నష్టాన్ని నిరోధించడం కొరకు తెలియని నంబర్లు మరియు అంతర్జాతీయ కాల్ ల నుంచి కాల్ లను నిర్వహించడం:

కాల్ చేసిన వ్యక్తి ఫోన్ చేసి ఒక రింగ్ తర్వాత ఫోన్ ను హ్యాంగ్ చేసినప్పుడు వన్-రింగ్ **స్కామ్** జరుగుతుంది. తమ డబ్బును ఇవ్వడానికి ప్రజలను మోసం చేయడం ఒక స్కామ్.

వన్-రింగ్ స్కామ్ ఎలా పనిచేస్తుంది:

1. స్కామర్ ఇంటర్నేషనల్ ప్రీమియం రేట్ నంబర్ (ఐపీఆర్ఎన్)ను అద్దెకు తీసుకుంటాడు.
2. స్కామర్ మీకు ఒక ఉంగరం ఇస్తాడు మరియు తరువాత కాల్ ను డిస్ కనెక్ట్ చేస్తాడు.
3. మీరు ఒక ముఖ్యమైన కాల్ మిస్ అయ్యారని మీరు అనుకుంటారు మరియు అదే నంబర్ కు తిరిగి కాల్ చేస్తారు.
4. మీ కాల్ తీసుకోబడుతుంది, కానీ, అవతలి వైపు నుండి ఎవరూ మీతో మాట్లాడరు.
5. సమాధానం రాన తరువాత, మీరు మీ కాల్ ని డిస్ కనెక్ట్ చేస్తారు.
6. కాల్ చేసిన తరువాత, ఒక అంతర్జాతీయ కాల్ చేసినందుకు మీరు పెద్ద మొత్తంలో డబ్బును కోల్పోయారని మీరు గ్రహిస్తారు.

వన్-రింగ్ స్కామ్ నుండి సురక్షితంగా ఉండటానికి:

వన్ రింగ్ స్కామ్ నుంచి సురక్షితంగా ఉండాలంవన్..

- మీరు గుర్తించని నంబర్ల నుండి ఎలాంటి కాల్‌లకు సమాధానం ఇవ్వవద్దు లేదా తిరిగి ఇవ్వవద్దు.
- తెలియని నంబర్‌లకు కాల్ చేసే ముందు, ఏరియా కోడ్ అంతర్జాతీయంగా ఉందో లేదో తనిఖీ చేయండి.
- మీ ఫోన్ ఆపరేటర్‌కు అన్ని అనుమానాస్పద కాల్‌లను నివేదించండి.

ఆర్థిక స్కామ్‌ల రకం

ఆర్థిక స్కామ్‌ల రకాలు

- ఫిషింగ్
- స్పియర్-ఫిషింగ్
- తిమింగలం
- CEO మోసం
- గుర్తింపు దొంగతనం
- లాటరీ ఫీజు మోసాలు
- ఆన్‌లైన్ షాపింగ్ మోసం
- ఇంటి నుండి పని చేసే మోసాలు
- దొంగిలించబడిన కార్డుల స్కామ్
- ఇన్వాయిస్ మోసం

క్రెడిట్ కార్డు నంబర్లు, బ్యాంక్ సమాచారం వంటి వ్యక్తిగత సమాచారాన్ని బహిర్గతం చేయడానికి ఒక వ్యక్తి యొక్క డబ్బు లేదా గుర్తింపును దొంగిలించడానికి ప్రయత్నించే డిజిటల్ మాధ్యమం ద్వారా దాడిని ఫిషింగ్ అంటారు.

స్పియర్-ఫిషింగ్ అనేది ఒక రకమైన ఫిషింగ్, ఇది చాలా నిర్దిష్ట మరియు వ్యక్తిగతీకరించిన సందేశాలను ఉపయోగించి ఒక వ్యక్తి యొక్క డబ్బు లేదా గుర్తింపును దొంగిలించడానికి ప్రయత్నిస్తుంది.

స్పియర్-ఫిషింగ్ మాదిరిగానే, **తిమింగల వేట** సిఇఒలు మరియు సెలబ్రిటీలు వంటి ఉన్నత-ప్రొఫైల్, ప్రసిద్ధ మరియు సంపన్న వ్యక్తులను లక్ష్యంగా చేసుకుంటుంది.

ఒక CEO ఫ్రాడ్ లో, మోసగాళ్లు మీరు పనిచేసే కంపెనీ యొక్క CEO లేదా మరొక అథారిటీ ఫిగర్ గా నటించి డబ్బు పంపమని లేదా మీ సున్నితమైన సమాచారానికి ప్రాప్యత ఇవ్వమని మిమ్మల్ని అడుగుతారు.

గుర్తింపు దొంగతనంలో, మోసగాళ్లు పేరు, చిరునామా, ఇమెయిల్ చిరునామా, అలాగే క్రెడిట్ కార్డ్ లేదా ఖాతా సమాచారం వంటి మీ వ్యక్తిగత సమాచారాన్ని లక్ష్యంగా చేసుకుంటారు. అప్పుడు వారు మీ పేరుతో ఆన్లైన్లో వస్తువులను ఆర్డర్ చేసి, మీ క్రెడిట్ కార్డు సమాచారాన్ని ఉపయోగించి చెల్లింపులు చేస్తారు.

లాటరీ ఫీజు స్కామ్ లో, మీరు లాటరీ గెలుచుకున్నట్లు మీకు నోటిఫికేషన్ వస్తుంది మరియు మీ బహుమతిని క్లెయిమ్ చేయడానికి రుసుమును జమ చేయమని మిమ్మల్ని అడుగుతారు.

ఆన్లైన్ షాపింగ్ మోసంలో, ఒక నకిలీ షాపింగ్ పోర్టల్ ఆకర్షణీయమైన ధరలకు ఉత్పత్తులను ప్రదర్శిస్తుంది. పేమెంట్ చేసిన తర్వాత, మీరు నకిలీ ఉత్పత్తిని అందుకుంటారు లేదా ఉత్పత్తి లేదు.

వర్క్ ఫ్రమ్ హోమ్ స్కామ్ లలో మోసగాళ్లు ఇంటి నుంచి పనిచేస్తే మంచి జీతం వస్తుందని చెప్పి ప్రజలను మోసం చేస్తున్నారు. నిర్ణీత మొత్తాన్ని డిపాజిట్ చేయాలని ఉద్యోగార్థులను కోరుతున్నారు. డబ్బులు జమ అయ్యాక యజమానుల జాడ ఉండదు.

మీకు తెలియకుండా ఎవరైనా మీ **డెబిట్/క్రెడిట్ కార్డు** సమాచారాన్ని చట్టవిరుద్ధంగా ఆర్థిక లావాదేవీల కోసం ఉపయోగించినప్పుడు డెబిట్/క్రెడిట్ కార్డు స్కామ్ సంభవిస్తుంది.

ఇన్ వాయిస్ మోసంలో, మోసగాళ్లు సరఫరాదారులుగా నటించి, ఇన్ వాయిస్ లు చెల్లించిన బ్యాంక్ ఖాతా వివరాలను అప్ డేట్ చేయమని అడగడం ద్వారా వ్యాపారాలను లక్ష్యంగా చేసుకుంటారు.

ఆర్థిక కుంభకోణాల పర్యవసానాలు:

- ఆర్థిక నష్టం
- భావోద్వేగ ఒత్తిడి
- అవకాశాలు కోల్పోయారు
  - వ్యక్తుల కోసం
  - వ్యాపారాల కోసం

ఆన్ లైన్ ఫైనాన్షియల్ స్కామ్ ల నుంచి సురక్షితంగా ఉండండి:

1. అన్ని వ్యక్తిగత సమాచారం, గుర్తింపు కార్డులు మరియు బ్యాంకు కార్డులను ఎల్లప్పుడూ సురక్షితంగా ఉంచండి.
2. మీ పిన్ నంబర్లను గోప్యంగా ఉంచండి.
3. మీ పిన్ నెంబర్లు రాసుకోవద్దు లేదా వాటిని బ్యాంకు కార్డులతో నిల్వ చేయవద్దు.
4. బ్యాంకు ఖాతా వివరాలు లేదా ఇతర భద్రతా సమాచారాన్ని ఏ వ్యక్తికి ఇవ్వవద్దు.
5. మీ తరఫున బ్యాంకులో పెట్టడానికి ముందుకు వచ్చే వ్యక్తులకు మీ డబ్బును ఎప్పుడూ ఇవ్వవద్దు.
6. మీ ఏటీఎం కార్డును మరెవరూ ఉపయోగించవద్దు.
7. అనుమానాస్పద లావాదేవీల కోసం నెలవారీ క్రెడిట్ కార్డ్ స్టేట్మెంట్లు మరియు ఇతర బ్యాంక్ స్టేట్మెంట్లను జాగ్రత్తగా తనిఖీ చేయండి.
8. మీ కార్డు చోరీ లేదా నష్టాన్ని వెంటనే నివేదించండి.
9. ఇంటర్నెట్ లో చెల్లింపులు చేయడానికి మీ కార్డును ఉపయోగించేటప్పుడు జాగ్రత్తగా ఉండండి.
10. సురక్షిత చెల్లింపు వెబ్ సైట్ లపై మాత్రమే మీ కార్డు ధృవీకరణ విలువను (CVV) వెల్లడించండి
11. ఏదైనా ఆర్థిక ఒప్పందంపై డిజిటల్ సంతకం చేసేటప్పుడు జాగ్రత్తగా ఉండండి.

12. విదేశీ బ్యాంకులో భారీ మొత్తంలో డబ్బు పెట్టడానికి మీ సహాయం కోరుతూ కాల్స్, లేఖలు, ఇ-మెయిల్స్ లేదా ఫ్యాక్స్ల పట్ల జాగ్రత్త వహించండి.
13. మీకు ఉద్యోగం లేదా మరేదైనా ప్రయోజనం ఇస్తామని హామీ ఇచ్చే స్పామ్ లేదా అవాంఛిత ఇ-మెయిల్స్ కు సమాధానం ఇవ్వవద్దు.

మీ ఆన్లైన్ బ్యాంకింగ్ వివరాలు హ్యాకింగ్కు గురైతే ఈ కింది చర్యలు తీసుకోండి...

1. వెంటనే మీ బ్యాంకుకు తెలియజేయండి
2. మీ క్రెడిట్/డెబిట్ కార్డు లేదా యుపిఐ యాప్ ను బ్లాక్ చేయండి
3. నెట్ బ్యాంకింగ్ కోసం మీ పాస్ వర్డ్ లను మార్చండి
4. మీ యుపిఐ, డెబిట్ కార్డ్ మరియు క్రెడిట్ కార్డ్ PIN లను మార్చండి
5. ప్రస్తుత డెబిట్/క్రెడిట్ కార్డులను రద్దు చేయండి మరియు రీప్లేస్ మెంట్ లను అడగండి.
6. కొత్త సెక్యూరిటీ ఫీచర్ ని సెటప్ చేయండి (మల్టీ-స్టెప్ ఆథెంటికేషన్)

రిఫరెన్స్ రీడింగ్:

- ఆర్థిక మోసాల గురించి మరింత: https://cybercrime.gov.in/pdf/Financial%20Fraud%20Brochures%20final.pdf

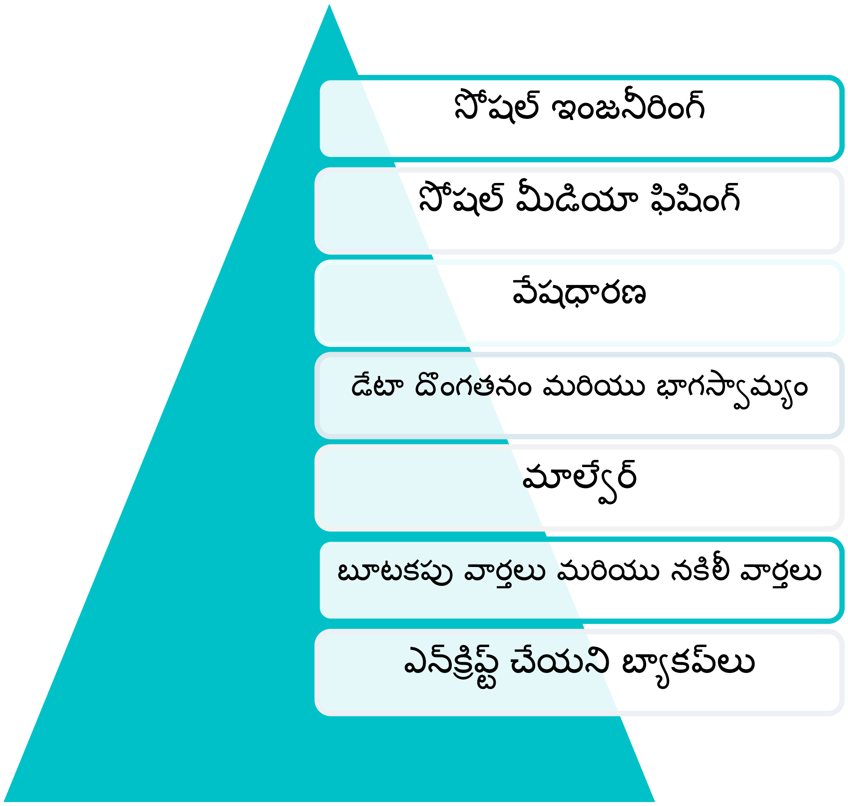
మాడ్యూల్ 3
సోషల్ మీడియా

విరివిగా ఉపయోగించే సోషల్ మీడియా ప్లాట్ ఫామ్ లు

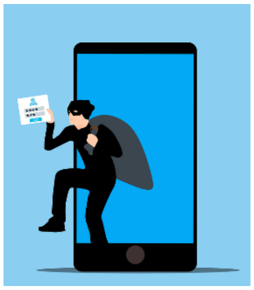
1. వాట్సప్..
2. ఇన్ స్టాగ్రామ్
3. ఫేస్ బుక్
4. ట్విట్టర్
5. Sharechat
6. Snapchat

సోషల్ మీడియా ప్లాట్ఫామ్లు వినియోగదారులకు చిత్రాలను ప్రదర్శించడానికి మరియు బహిరంగంగా పోస్ట్ చేయడానికి అనుమతిస్తాయి. మోసగాళ్లు యూజర్ కు తెలియకుండా రహస్యంగా సమాచారాన్ని సేకరిస్తారు. సేకరించిన సమాచారంతో మోసగాళ్లు వివిధ మార్గాల్లో యూజర్లను సంప్రదిస్తారు.

మోసగాళ్లు సోషల్ మీడియా యూజర్లను మోసం చేసే వివిధ మార్గాలు:



సోషల్ ఇంజనీరింగ్



ఈ దాడిలో అనధికార ప్రాప్యత, నెట్వర్క్ మరియు ఆర్థిక లాభం పొందడానికి మానిప్యులేషన్ ఉంటుంది. మోసగాళ్లు లావాదేవీ లేదా డబ్బు బదిలీ చేయడానికి బ్యాంకు లేదా ఇతర సంస్థ యొక్క ప్రామాణిక ప్రతినిధులుగా తమను తాము ప్రాతినిధ్యం వహించడం ద్వారా వినియోగదారును మోసం చేస్తారు.

మిమ్మల్ని మీరు రక్షించుకోవడానికి, ఫోన్ కాల్స్ ఆధారంగా లావాదేవీలు చేయవద్దు లేదా బ్యాంకు వివరాలు ఇవ్వవద్దు.

సోషల్ మీడియా ఫిషింగ్

ఫిషింగ్ యొక్క ఉద్దేశ్యం వ్యక్తిగత డేటాను పొందడం లేదా వినియోగదారు యొక్క సోషల్ మీడియా ఖాతాలను యాక్సెస్ చేయడం.

తారుమారు[మారు]

ఈ స్కామ్ లో మోసగాళ్లు సున్నితమైన సమాచారాన్ని దొంగిలించడానికి వినియోగదారుడిని నమ్మే వ్యక్తిగా నటిస్తారు.

సోషల్ మీడియా స్క్రాపింగ్

ఇది సోషల్ మీడియా ఫిషింగ్ మరియు ఇంప్రెషన్ కు ఒక ఉదాహరణ. వ్యక్తిగత సమాచారాన్ని తిరిగి పొందడానికి మోసగాళ్లు కస్టమర్ ఎగ్జిక్యూటివ్ గా నకిలీ కాల్స్ చేస్తారు. ఇందులో పేర్లు, పుట్టిన తేదీలు, వ్యక్తిగత ఫోటోలు, లొకేషన్ ఉంటాయి. మోసగాళ్లు భవిష్యత్తులో డేటా/గుర్తింపు దొంగతనం కోసం ఈ సమాచారాన్ని ఉపయోగిస్తారు

సోషల్ మీడియా నుంచి మిమ్మల్ని మీరు రక్షించుకోవడానికి:

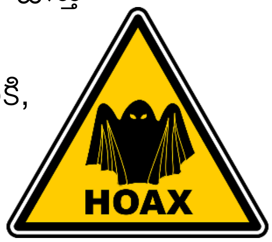
1. మీ వ్యక్తిగత వివరాలను ఎప్పుడూ పంచుకోవద్దు
2. అటువంటి కాల్స్ గురించి వెంటనే రిపోర్ట్ చేయండి
3. అనుమానాస్పద ప్రొఫైల్ ని రిపోర్ట్ చేయండి మరియు బ్లాక్ చేయండి

డేటా చోరీ..

ఈ స్కామ్ లో మోసగాళ్లు రహస్య సమాచారాన్ని అక్రమంగా బదిలీ చేస్తారు. మాల్వేర్ సాధారణంగా లైక్ బటన్, ఆడియో క్లిప్స్, వీడియోలు లేదా సోషల్ మీడియాలోని లింక్లలో మారువేషంలో ఉంటుంది.

ఫేక్ న్యూస్, ఫేక్ న్యూస్..

ఈ స్కామ్ లో మోసగాళ్లు తప్పుడు సమాచారాన్ని ప్రచారం చేస్తూ వినియోగదారులను తప్పుదోవ పట్టిస్తున్నారు.



ఫేక్ కాల్స్ మరియు సందేశాల నుండి మనల్ని మనం రక్షించుకోవడానికి, మనం వీటిని చేయాలి:

1. ఫోటోలు మరియు మీడియాను ఎల్లప్పుడూ జాగ్రత్తగా తనిఖీ చేయండి.
2. విశ్వసనీయ వర్గాల నుంచి సమాచారాన్ని సరిచూసుకోవాలి.
3. చట్టవిరుద్ధమైన మరియు ప్రమాదకరమైన సంభాషణా సమూహాలను బ్లాక్ చేయండి మరియు నివేదించండి.
4. అవాంఛిత సమూహాలకు మమ్మల్ని జోడించకుండా నిరోధించడానికి సమూహ గోప్యతా సెట్టింగ్ లను ఉపయోగించండి.

Unencrypted Backups

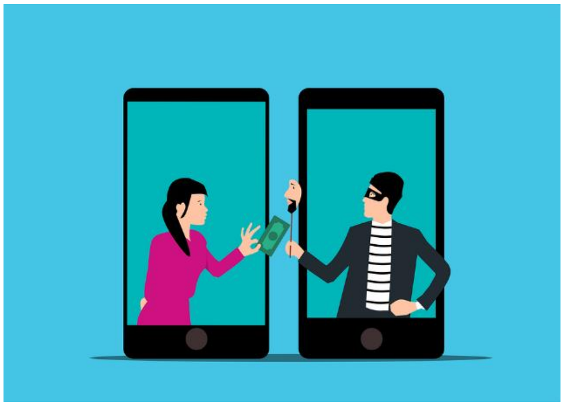
ఈ స్కామ్ లో, డేటా అల్గోరిథం ద్వారా ఎన్ కోడ్ చేయబడదు మరియు ఎవరైనా చదవవచ్చు.

నకిలీ ఖాతాలను గుర్తించడం కొరకు, సోషల్ మీడియాలో మోసగాడి యొక్క ఈ క్రింది ప్రవర్తనలను గమనించండి:

1. కాల్స్ మరియు మీటింగ్ లు తీసుకోవడం మానుకోండి.
2. ఆన్ లైన్ ఉనికి లేదు
3. పరిమిత స్నేహితులు/అనుచరులు
4. చాలా ఇటీవలి ప్రొఫైల్
5. ప్రొఫెషనల్ చిత్రాలు
6. దొంగిలించిన చిత్రాలు
7. డబ్బులు అడుగుతాడు.
8. స్పష్టమైన చిత్రాలు లేదా వీడియో కోసం అడుగుతుంది

సోషల్ మీడియా మోసం యొక్క అత్యంత సాధారణ రూపం **క్యాట్ఫిషింగ్**.

క్యాట్ఫిషింగ్ అనేది ఆన్లైన్ మోసం యొక్క ఒక రూపం. మోసగాడు నకిలీ గుర్తింపును ఉపయోగించడం ద్వారా వేరొకరిగా నటిస్తాడు మరియు శృంగార సంబంధాన్ని ఏర్పరచుకోవడం ద్వారా సులభమైన లక్ష్యాలను మోసం చేస్తాడు



1. ఫేక్ ఐడెంటిటీకి మద్దతుగా ఓ క్యాట్ ఫిషర్ మేకప్ స్టోరీలు, ఫేక్ ఫోటోలను ఉపయోగిస్తుంటాడు.
2. పిల్లి-ఫిషర్ సాధారణంగా డబ్బు మరియు వ్యక్తిగత సమాచారాన్ని అడుగుతుంది

అన్ని సోషల్ మీడియా ప్లాట్ఫారమ్లు "**రిపోర్ట్**" మరియు "**బ్లాక్**" లక్షణాలను కలిగి ఉంటాయి, ఇది మరొక సమస్యాత్మక లేదా నకిలీ వినియోగదారు నుండి వినియోగదారును రక్షించే ఇలాంటి విధిని కలిగి ఉంటుంది.

అడ్డగించు

కాంటాక్ట్ ని బ్లాక్ చేయడం వల్ల యూజర్ నుంచి మెసేజ్ లు రిసీవ్ చేసుకోవడాన్ని నిలిపివేస్తారు.

నివేదిక

వినియోగదారు లేదా ఒక సమూహం ద్వారా నిబంధనలు మరియు షరతులు ఉల్లంఘించబడుతున్నట్లయితే కంపెనీకి తెలియజేయడానికి రిపోర్టింగ్ సహాయపడుతుంది.

వాట్సాప్ యొక్క ఉపయోగాలు:

1. పాప్-అప్ ప్రకటనలు లేవు
2. ఉపయోగించడం సులభం
3. ఛార్జ్ మెసేజింగ్ సర్వీస్ లేదు
4. మీడియా, స్థానం మరియు స్థితి భాగస్వామ్యం
5. సమూహాలు సామూహిక పరస్పర చర్యను అనుమతిస్తాయి
6. వీడియో కాలింగ్

వాట్సాప్ వల్ల కలిగే నష్టాలు:

7. అనేక గోప్యతా సమస్యలు ఉన్నాయి
8. ధృవీకరించని సమాచార భాగస్వామ్యం చాలా ఉంది
9. వాట్సాప్ చాలా వ్యసనపరుడు.

సోషల్ మీడియా మర్యాద:

సోషల్ మీడియా వేదికలు మరియు వినియోగదారులు ఆన్లైన్లో తమ ఖ్యాతిని కాపాడుకోవడానికి ఉపయోగించే మార్గదర్శకాలు సోషల్ మీడియా మర్యాద.

సోషల్ మీడియా చేయాల్సినవి

- తెలిసిన పరిచయాలతో కమ్యూనికేట్ చేయండి
- అనుమతి కోసం అడగండి మరియు సరిహద్దులను గౌరవించండి
- సమూహ నియంత్రణలను ఉపయోగించండి
- సరైన ఫోటోలు మరియు వీడియోలను మాత్రమే భాగస్వామ్యం చేయండి
- తగిన ఫోటోలు మరియు వీడియోలను పోస్ట్ చేయండి
- సోషల్ మీడియా ప్లాట్‌ఫారమ్‌ల మార్గదర్శకాలను అనుసరించండి.

సోషల్ మీడియా చేయకూడనివి

- ఇతర వినియోగదారులను స్పామ్ చేయండి
- ఇతరుల వ్యక్తిగత సమాచారాన్ని ఉపయోగించండి లేదా భాగస్వామ్యం చేయండి
- బల్క్ సందేశం
- అసభ్యకరమైన భాషను ఉపయోగించడం
- నకిలీ వార్తలు మరియు తప్పుదారి పట్టించే సమాచారాన్ని ప్రోత్సహించడం
- ఓవర్-షేర్

వాట్సాప్ చేయాల్సినవి..:

- మీకు తెలిసిన పరిచయాలకు ప్రొఫైల్ ఫోటోలు, స్థితి మరియు సమాచారం గురించిన దృశ్యమానతను పరిమితం చేయండి.
- యాదృచ్ఛిక సమూహాలలో జోడించబడకుండా ఉండటానికి సమూహ గోప్యతా సెట్టింగ్‌లను ఉపయోగించండి.
- ఎండ్-టు-ఎండ్ ఎన్క్రిప్షన్ ఉపయోగించండి.
- చాట్‌లో లైవ్ లొకేషన్‌ను ఆఫ్ చేయండి.
- మిమ్మల్ని సంప్రదించడానికి ప్రయత్నిస్తున్న తెలియని వినియోగదారులను బ్లాక్ చేయండి.

వాట్సాప్

- ❌ అపరిచితులతో మీ వ్యక్తిగత సమాచారాన్ని పంచుకోండి.
- ❌ మీ గోప్యతా సెట్టింగ్‌ని పబ్లిక్‌గా సెట్ చేయండి.
- ❌ ఇతర వినియోగదారు గోప్యతను అగౌరవపరచండి.

చేయకూడనివి..

ఇన్ స్టాగ్రామ్ చేయాల్సినవి

- ✓ మీ ఫాలోవర్లలో తెలిసిన వ్యక్తులను జోడించండి.
- ✓ తగిన ఫోటోలు, వీడియోలు, సమాచారాన్ని పోస్ట్ చేయండి.
- ✓ ఇతర వినియోగదారు గోప్యతను గౌరవించండి.
- ✓ మోసగాళ్ల కోసం బ్లాక్/రిపోర్ట్ ఉపయోగించండి.

ఇన్ స్టాగ్రామ్ చేయకూడనివి

- పబ్లిక్ ఖాతాలపై సున్నితమైన సమాచారాన్ని షేర్ చేయండి.
- అనుమతి లేకుండా ఇతరుల పోస్ట్‌ను ఉపయోగించండి.
- అనుచరులను కొనుగోలు చేయండి.
- ఇతరులను అగౌరవపరచండి

ఫేస్ బుక్ చేయాల్సినవి

- ధృవీకరించబడిన వార్తలు మరియు సమాచారాన్ని భాగస్వామ్యం చేయండి.
- మీ డేటా మరియు సమాచారాన్ని భద్రపరచడానికి గోప్యతా సెట్టింగ్‌లను ఉపయోగించండి.
- సరైన మీడియాను మాత్రమే షేర్ చేయండి.
- తెలిసిన వినియోగదారులతో పరస్పర చర్య చేయండి.

ఫేస్ బుక్ చేయకూడనివి

- ధృవీకరించని వార్తలను భాగస్వామ్యం చేయండి.
- యాదృచ్ఛిక లింక్‌లపై క్లిక్ చేయండి.
- ఏదైనా ప్రకటనలో బ్యాంక్ ఖాతా వివరాలు వంటి మీ ఆధారాలను పూరించండి.

ట్విట్టర్ చేయాల్సినవి

- మీ డేటా మరియు ట్వీట్‌లను దుర్వినియోగం కాకుండా రక్షించడానికి గోప్యత మరియు భద్రత ఎంపికను ఉపయోగించండి.
- ట్వీట్ల ద్వారా మీ ఆలోచనలను వ్యక్తీకరించడానికి తగిన భాషను ఉపయోగించండి.
- తెలిసిన వినియోగదారుల అభ్యర్థనలను మాత్రమే ఆమోదించండి.

ట్విట్టర్ చేయకూడనివి

- మీ అభిప్రాయాలను ఇతరులపై బలవంతంగా రుద్దండి.
- అసభ్యకరమైన భాషను ఉపయోగించండి.
- మీ ప్రత్యక్ష స్థానాన్ని పబ్లిక్‌గా షేర్ చేయం

కమ్యూనికేషన్ లో సోషల్ మీడియా ఎంతగానో ఉపయోగపడుతుంది మరియు ప్రపంచంతో మనల్ని అప్ డేట్ చేస్తుంది. కానీ దాన్ని బాధ్యతాయుతంగా వాడాలి. సోషల్ మీడియాలో ఎన్నో ఆసక్తికర విషయాలు, వార్తలు చక్కర్లు కొడుతున్నాయి. వాటిని సర్క్యులేట్ చేసే ముందు జాగ్రత్తగా ఉండాలి.

రిఫరెన్స్ రీడింగ్:

- సైబర్ జాగృతి దివస్: https://www.youtube.com/watch?v=6whmq4EwIIo
- సైబర్ బుల్లీయింగ్ వాస్తవాలు : https://www.youtube.com/watch?v=oXo8N9qlJtk

మాడ్యూల్ 4
గుర్తింపు దొంగతనం

పాస్ వర్డ్ లు మరియు ఆథెంటికేషన్

పాస్ వర్డ్ అనేది ఆథెంటికేషన్ ప్రాసెస్ సమయంలో యూజర్ యొక్క గుర్తింపును ధృవీకరించడానికి ఉపయోగించే అక్షరాల స్ట్రింగ్.

మీ స్మార్ట్ పరికరాలు మరియు వ్యక్తిగత సమాచారానికి అనధికారిక ప్రాప్యతకు వ్యతిరేకంగా పాస్ వర్డ్ లు మొదటి **రక్షణను** అందిస్తాయి.

1. పాస్ వర్డ్ లు కనీసం పది అక్షరాలను కలిగి ఉండాలి మరియు ఇలాంటి అక్షరాల కలయికను

ప్రత్యేక పాత్రలు	పెద్ద అక్షరాలు మరియు చిన్న అక్షరాలు	సంఖ్యలు

1. "12345" లేదా "క్వెర్టీ" వంటి సీక్వెన్స్ లను ఉపయోగించడం మానుకోండి.
1. మీరు అక్షరాలకు బదులుగా ఒకేలా కనిపించే సంఖ్యలను ఉపయోగించవచ్చు–ఒక

Zoom	ఇలా వ్రాయండి	Zoom
Trick	ఇలా వ్రాయండి	Tr1ck
Basket	ఇలా వ్రాయండి	845KE7
Ball	ఇలా వ్రాయండి	8411

1. మీరు మీ కీబోర్డులోని సంఖ్యలతో పాటు పేర్కొన్న ప్రత్యేక అక్షరాలతో సంఖ్యలను కూడా భర్తీ చేయవచ్చు.

ధృవీకరణ ఈ క్రింది కారకాలను కలిగి ఉంటుంది:

1. పాస్ వర్డ్, పిన్ వంటి యూజర్ కు తెలిసిన విషయాలు
2. వినియోగదారుని డెబిట్ కార్డ్ మరియు క్రెడిట్ కార్డ్ వంటి ఏదైనా
3. బయోమెట్రిక్ లక్షణాలు వంటి యూజర్ కు ప్రత్యేకమైన ఏదైనా

యుపిఐ పిన్, బ్యాంకింగ్ కార్డు పిన్లు మరియు బయోమెట్రిక్ ఆథెంటికేషన్లు

1. UPI ధృవీకరణ

UPI Stands for Unified Payments Interface

A payment system that allows you to transfer funds across banks

To use UPI you need:

- A smartphone
- An active bank account
- A mobile number linked with bank account
- Internet connection
- UPI ID
- UPI PIN

UPI ID

- Automatically Generated
- Required to access UPI account

UPI PIN

- Unique, 4 or 6-digit passcode created by the user
- Safeguards your UPI account

1. బ్యాంకింగ్ కార్డుల ఆథెంటికేషన్

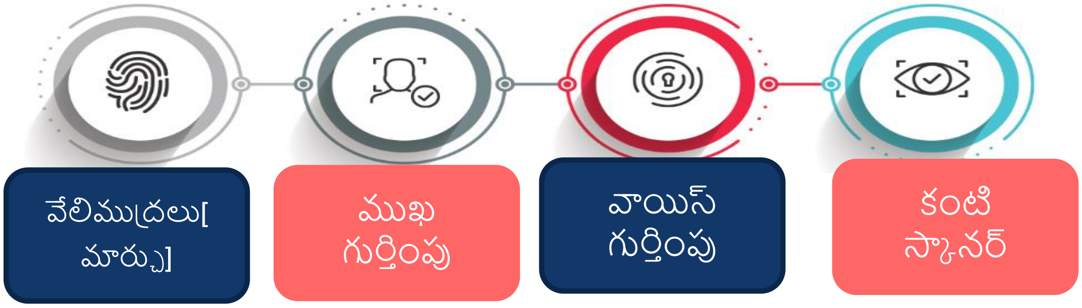
బ్యాంకింగ్ కార్డు పిన్ లో దేనికి పిన్ ఉంటుంది:

P	I	N
Personal	Identification	Number

ఖాతాదారుడి కార్డుకు ప్రత్యేకమైన నాలుగు అంకెల కోడ్.

2. బయోమెట్రిక్ ప్రమాణీకరణ

బయోమెట్రిక్ ఆథెంటికేషన్ ఈ క్రింది బయోమెట్రిక్ తో సరిపోలుతుంది స్మార్ట్ పరికరం లేదా మీ బ్యాంకింగ్ ఖాతాను యాక్సెస్ చేయడానికి ఫీచర్లు.



3. రెండు-కారకాల ప్రమాణీకరణ

Two-factor authentication is also referred to as 2FA

Safeguards your online accounts by verifying user details and passcode

Monitors and helps safeguard your online account credentials and data

హానికరమైన వెబ్ సైట్ లు మరియు యాప్ లు

టూ-ఫ్యాక్టర్ అథెంటికేషన్ అనేది ఒక పాస్ వర్డ్ మరియు వన్-టైమ్ పాస్ కోడ్/ఆథెంటికేషన్ కోడ్ ని ఉపయోగిస్తుంది. SMS ద్వారా మొబైల్ ఫోన్, ఇది నమోదు చేయబడినప్పుడు వినియోగదారు చివరికి ఖాతాను యాక్సెస్ చేయడానికి అనుమతిస్తుంది.

యూజర్ నేమ్ నమోదు చేయండి | ప్రమాణీకరణ కోడ్ | ప్రామాణీకరణ నమోదు

హానికరమైన వెబ్ సైట్ లు మరియు యాప్ లు

హానికరమైన వెబ్సైట్లు మరియు అనువర్తనాలు సైబర్ దాడి యొక్క అత్యంత సాధారణ రూపాలలో ఒకటి.

హ్యాకర్లు మీ సోషల్ మీడియా ఖాతాలలో ప్రదర్శించబడే SMS, ఇమెయిల్ లు లేదా ప్రకటనల ద్వారా మీకు లింక్ లను పంపుతారు

ఒక్క క్లిక్ తో మీ వ్యక్తిగత సమాచారం మొత్తం హ్యాకర్లకు లీక్ అవుతుంది కాబట్టి అప్రమత్తంగా ఉండాలి.

హానికరమైన వెబ్ సైట్ లు ఈ క్రింది వాటిని చేయమని మిమ్మల్ని ఆదేశించవచ్చు:

1. సాఫ్ట్ వేర్/ఏదైనా ఇన్ వాయిస్/ఫైల్/యాప్ డౌన్ లోడ్ చేసుకోండి
2. ఒక ఫైలును సేవ్ చేయండి
3. ఒక ప్రోగ్రామ్ ను రన్ చేయండి

హానికరమైన వెబ్ సైట్ లు/యాప్ లు ఎలా పనిచేస్తాయి?

ఒక హానికరమైన లింక్/ఫైల్/అటాచ్ మెంట్ యూజర్ కు పంపబడుతుంది.

యూజర్ లింక్ క్లిక్ చేశాడు

మీ సున్నితమైన డేటా మొత్తాన్ని దొంగిలించే మాల్వేర్ పరికరంలో ఇన్స్టాల్ చేయబడింది.

మీరు మీ వాలెట్ లో 5000INR బోనస్ పాయింట్ లను గెలుచుకున్నారు. క్లెయిమ్ చేయడానికి ఇక్కడ క్లిక్ చేయండి !!! మరో 15 నిమిషాల్లో గడువు

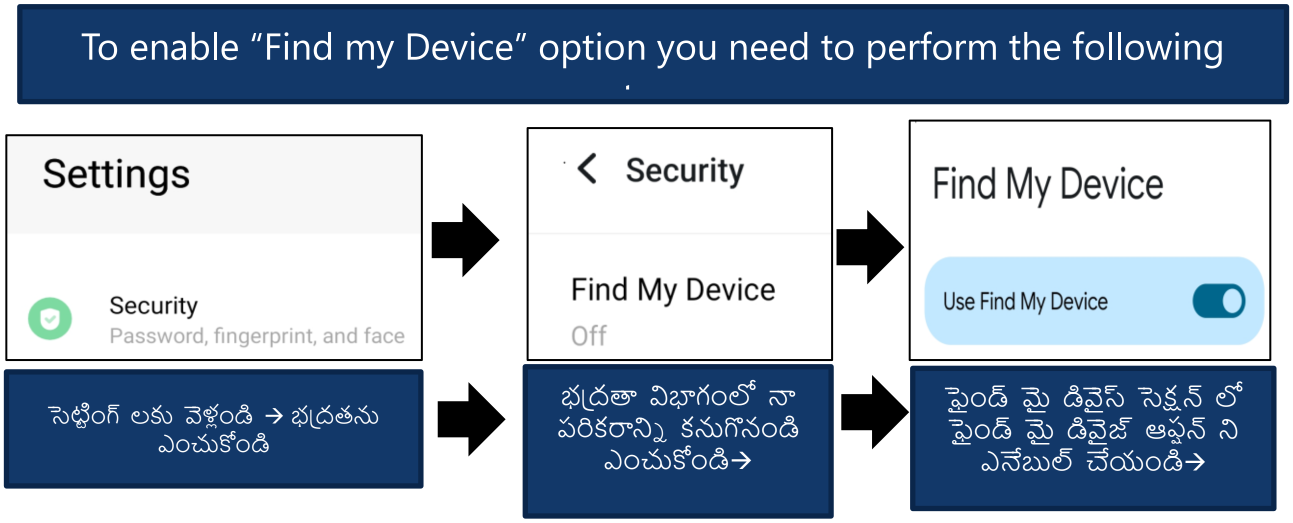
హానికరమైన వెబ్ సైట్ లు మరియు యాప్ ల నుండి మీ పరికరాన్ని రక్షించడంలో సహాయపడే కొన్ని అంశాలు ఇక్కడ ఉన్నాయి:

1. ఇమెయిల్ లో పొందుపరిచిన లింక్ పై ఎప్పుడూ క్లిక్ చేయవద్దు
2. ఏదైనా బాహ్య తృతీయ పక్ష సందేశం నుండి అందుకున్న లింక్ పై ఎప్పుడూ క్లిక్ చేయవద్దు.
3. మీ వ్యక్తిగత సున్నితమైన సమాచారాన్ని అడిగే యాదృచ్ఛిక అనువర్తనాన్ని ఎన్నడూ ఇన్ స్టాల్ చేయవద్దు
4. ఏదైనా ఆన్ లైన్ చెల్లింపులు చేసేటప్పుడు ఎల్లప్పుడూ URLలో "https" కోసం తనిఖీ చేయండి.
5. URLను జాగ్రత్తగా చదవండి. వెబ్సైట్ స్పెల్లింగ్లో చిన్న ట్విస్ట్ ప్రమాదాన్ని కలిగిస్తుంది.
6. బ్యాంక్ ద్వారా అందించబడ్డ లింక్ నుంచి మీ బ్యాంకింగ్ యాప్ ని ఇన్ స్టాల్ చేసుకోండి.
7. ఏదైనా వెబ్ సైట్ ను యాక్సెస్ చేయడానికి ముందు ఎల్లప్పుడూ URL చెక్ చేయండి.
8. విశ్వసనీయ వెబ్సైట్లలో మాత్రమే షాపింగ్ చేయండి మరియు అందుకున్న యాదృచ్ఛిక లింక్ల ద్వారా కాదు.
9. నమ్మకమైన ప్లే స్టోర్ నుండి సురక్షిత అనువర్తనాలను వ్యవస్థాపించండి.
10. వాటిని తెరవడానికి ముందు ఇమెయిల్ లను తనిఖీ చేయండి. పంపిన వ్యక్తి మీకు తెలిస్తేనే తెరవండి.
11. ఒకవేళ మీరు ఆన్ లైన్ లో ఏదైనా ఖాతాకు లాగిన్ అయినట్లయితే, వెబ్ సైట్ ని విడిచిపెట్టడానికి ముందు ఎల్లప్పుడూ లాగిన్ అవ్వండి.
12. మీ యాంటీవైరస్ ను క్రమం తప్పకుండా అప్ డేట్ చేయండి.

పోయిన ఫోన్ లను రిమోట్ గా నిర్వహించడం

ఈ క్రింది **పరిస్థితులలో** మాత్రమే, పోగొట్టుకున్న ఫోన్ ను రిమోట్ గా యాక్సెస్ చేయవచ్చు

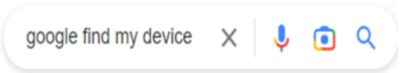
1. ఫోన్ ఆన్ చేయబడింది
2. ఐఫోన్ విషయంలో గూగుల్ అకౌంట్ (ఆండ్రాయిడ్ అయితే) లేదా ఐక్లౌడ్ కు సైన్ ఇన్ చేయండి.
3. ఇంటర్నెట్ కు కనెక్ట్ చేయబడింది
4. నా పరికరాన్ని కనుగొనండి ప్రారంభించబడింది



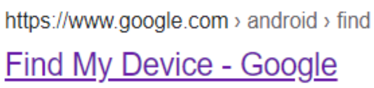
ఇది పోయినప్పుడు లేదా దొంగతనం జరిగినప్పుడు మీ ఫోన్ను రిమోట్గా యాక్సెస్ చేయడానికి మిమ్మల్ని

మీ కోల్పోయిన స్మార్ట్ ఫోన్ డేటాను రిమోట్ గా తుడిచివేయడానికి, మీరు చూపించిన దశలను నిర్ధారించాలి:

మీ అకౌంట్ లోకి గూగుల్ క్రోమ్ మరియు సైన్ ఇన్ ఓపెన్ చేయండి

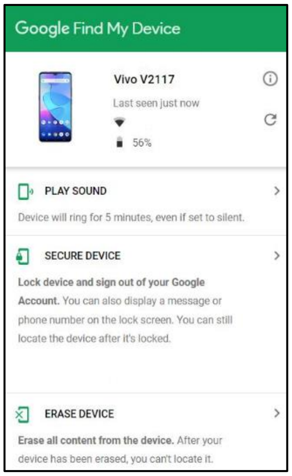


సెర్చ్ బార్ లో గూగుల్ ఫైండ్ మై డివైస్ అని టైప్ చేయండి



చూపించిన లింక్ పై క్లిక్ చేయండి. గూగుల్ ఫైండ్ మై డివైజ్ స్క్రీన్ కనిపిస్తుంది.

ఇప్పుడు, స్క్రీన్ పై చూపించిన విధంగా తగిన ఎంపికను ఎంచుకోవడం ద్వారా మీరు మీ పరికరాన్ని సురక్షితంగా ఉంచవచ్చు లేదా దానిపై ఉన్న కంటెంట్ ను తుడిచివేయవచ్చు.



ఫిషింగ్ మరియు ఆన్ లైన్ ఫారాలు

ఆన్లైన్ ఫారాలు మనందరికీ తెలుసు:

1. బహుళ ప్రశ్నలతో కూడిన సర్వే ఫారాలను రూపొందించడానికి ఉపయోగించబడుతుంది.
2. సర్వే ఫలితాలను రియల్ టైమ్ లో విశ్లేషించడానికి ఉపయోగిస్తారు.
3. ఏదైనా పరికరం నుండి ప్రాప్యత

కానీ వాటిని హ్యాకర్లు తరచుగా మీ వ్యక్తిగత సమాచారాన్ని హ్యాక్ చేయడానికి ఉపయోగిస్తారు. హ్యాకర్లు మీ బ్యాంకు సిబ్బందిగా నటించవచ్చు మరియు వారు మీకు ఒక ఫారం జత చేసిన ఇమెయిల్ పంపారని మీకు తెలియజేస్తారు, మీ పొదుపు పథకాన్ని పునరుద్ధరించడానికి నింపి పంపమని అడుగుతారు.

ఇలాంటి ఫిషింగ్ కుంభకోణాల జోలికి వెళ్లొద్దు. మీరు మీ బ్యాంక్ నుండి ఆన్లైన్ ఫారమ్ నింపాల్సిన అవసరం ఉందా అని వెంటనే ధృవీకరించండి.

ఫిషింగ్ ఆన్లైన్ ఫారం ఇమెయిల్స్ యొక్క నమూనా ఇక్కడ ఉంది.

Phishing Form e-mail

శ్రద్ధ: అత్యవసరం | బాహ్య ఇమెయిల్ ప్రియమైన అకౌంట్ హోల్డర్ మీ KYCకి సంబంధించి కొంత తప్పిపోయిన సమాచారం ఉందని మీకు తెలియజేయడానికి ఇది. దయచేసి జతచేయబడిన ఫారాన్ని నింపండి మరియు ఈ రోజులోగా సబ్మిట్ చేయండి, లేకపోతే తదుపరి నోటీసు వచ్చే వరకు మీ ఖాతా స్తంభింపజేయబడుతుంది మరియు మీరు ఈ ఖాతా నుండి ఎటువంటి ఆర్థిక లావాదేవీలు చేయలేరు. మీ ఖాతాను అప్ డేట్ చేయడం కొరకు దయచేసి దిగువ లింక్ మీద క్లిక్ చేయండి: ఇప్పుడు నవీకరించండి మేము మీ గోప్యతను గౌరవిస్తాము! ధన్యవాదాలు మరియు అభినందనలు MSN20002 555555 పేరు పెట్టలేదు.png	వివరాలను నింపండి: మొదటి పేరు:* ___________ చివరి పేరు:* చిరునామా 1:* చిరునామా 2 ఇమెయిల్ ఐడి:* రిజిస్టర్డ్ మొబైల్ నెంబరు:* ఆధార్ నెంబరు:*

సురక్షితంగా ఉండటానికి ఆన్లైన్ ఫారాలలో చేయవలసినవి మరియు చేయకూడనివి:

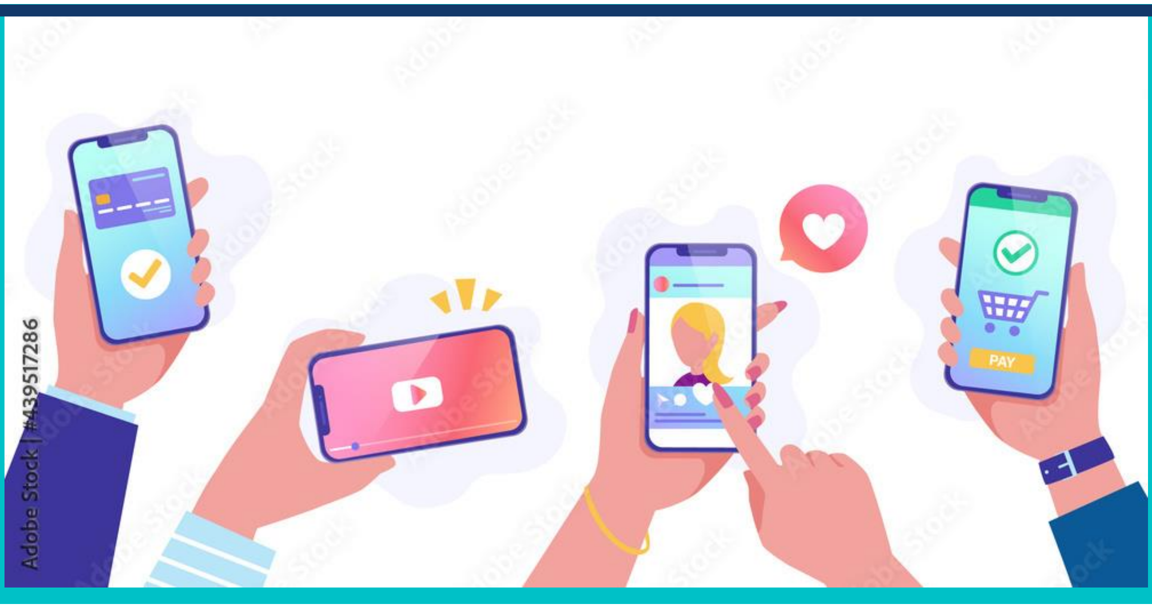
- ✗ ఫారాన్ని పంపే మూలం గురించి మీకు ఖచ్చితంగా తెలిసే వరకు ఆన్లైన్ ఫారాల ద్వారా సున్నితమైన సమాచారాన్ని అందించవద్దు.
- ✓ మీరు ఇ-మెయిల్ ద్వారా ఫారమ్ అందుకోవడం గురించి ఎల్లప్పుడూ మీ బ్యాంకు లేదా సంబంధిత అధికారితో క్రాస్ చెక్ చేయండి.
- ✗ బాహ్య థర్డ్ పార్టీ వెండర్ నుండి ఇమెయిల్ ను ఎప్పుడూ తెరవవద్దు.
- ✓ వాటికి రిప్లై ఇచ్చే ముందు పంపిన వారి ఈమెయిల్ ఐడీని చదివి గుర్తించండి.

రిఫరెన్స్ రీడింగ్:

- మీ యూపీఐ పిన్ రీసెట్ చేయడం ఎలా? : https://www.youtube.com/watch?v=ZoEqpKF_Sjw
- టూ ఫ్యాక్టర్ ఆథెంటికేషన్ తో మీ ఇన్ స్టాగ్రామ్ ఖాతాను సురక్షితం చేయడం: https://help.instagram.com/566810106808145
- టూ ఫ్యాక్టర్ అథెంటికేషన్ తో మీ ఫేస్ బుక్ ఖాతాను భద్రపరచడం: https://www.facebook.com/help/148233965247823
- పోయిన ఐఫోన్ ను రిమోట్ గా నిర్వహించడం : https://support.apple.com/en-in/guide/security/secc46f3562c/web
- మాల్వేర్ ఇన్ఫెక్షన్ల కోసం వెబ్సైట్ను ఎలా తనిఖీ చేయాలి : https://www.sitelock.com/blog/check-website-for-malware/
- మీ స్మార్ట్ఫోన్కు హాని కలిగించే హానికరమైన యాప్స్: https://www.91mobiles.com/hub/malicious-apps-malware-google-play-store/

మాడ్యూల్ 5

ఇంటర్నెట్ స్మార్ట్ గా ఉండటం



సురక్షిత బ్రౌజింగ్ చిట్కాలు:

ఆన్ లైన్ బ్రౌజింగ్ సురక్షితంగా ఉండటానికి కొన్ని మార్గాలు ఉన్నాయి.

ఇంటర్నెట్ స్మార్ట్ గా ఉండండి

1. **సంరక్షణతో భాగస్వామ్యం చేయండి**
   వార్తలుశరవేగంగా వ్యాపిస్తాయి. దీని పర్యవసానాలు ప్రజలపై ఎలా ఉంటాయో ముందుగానే ఆలోచించాలి
   .
2. **బాధ్యతాయుతంగా కమ్యూనికేట్ చేయండి**
   1. ముఖాముఖి కమ్యూనికేషన్ మాదిరిగానే ఆన్ లైన్ కమ్యూనికేషన్ ద్వారా ఆలోచనాత్మక భాగస్వామ్యాన్ని పెంపొందించండి.
   2. తగిన కమ్యూనికేషన్ కొరకు మార్గదర్శకాలను రూపొందించండి.
   3. కుటుంబం, స్నేహితుల వివరాలను భద్రపరుచుకోండి.
3. **ఇంటర్నెట్ అలర్ట్ గా ఉండండి**
   1. ఫేక్ వార్తల జోలికి పోవద్దు.
   2. ప్రజలు అర్థం చేసుకోవడంలో సహాయపడటం చాలా ముఖ్యం
      1. డబ్ల్యూటోపీ నిజమైనది మరియు ఏది నకిలీ అనేది ఆన్లైన్ భద్రతలో చాలా ముఖ్యమైన పాఠం.
      2. ఆన్లైన్లో వ్యక్తులు మరియు పరిస్థితులు ఎల్లప్పుడూ కనిపించే విధంగా ఉండవు.
4. **ఇంటర్నెట్ స్ట్రాంగ్ గా ఉండండి**
   1. మీ రహస్యాలను సురక్షితం చేసుకోండి

      1. ఆఫ్లైన్లో ఎంత ముఖ్యమో ఆన్లైన్లో ప్రైవసీ, సెక్యూరిటీ కూడా అంతే ముఖ్యం.
      2. వ్యక్తిగత సమాచారాన్ని సంరక్షించడం అనేది వినియోగదారులు తమ పరికరాలు, ప్రతిష్ఠలు మరియు సంబంధాలను దెబ్బతీయకుండా ఉండటానికి సహాయపడుతుంది.
5. **ఇంటర్నెట్ దయగా ఉండండి**
   1. దయగా ఉండటం బాగుంది
   2. సానుకూలతతో పాటు ప్రతికూలతను వ్యాప్తి చేయడానికి ఇంటర్నెట్ ఒక శక్తివంతమైన సాధనం. వినియోగదారుడు "ఇతరులతో ఎలా వ్యవహరించాలని అనుకుంటున్నారో అలాగే వ్యవహరించండి" అనే భావనను ఆన్లైన్లో వారి

చర్యలకు తీసుకెళ్లవచ్చు, ఇతరులపై సానుకూల ప్రభావాన్ని పెంచవచ్చు మరియు అనుచిత ప్రవర్తనను తొలగించవచ్చు.

6. **ఇంటర్నెట్ ధైర్యంగా ఉండండి**
   1. వినియోగదారులు ఇంట్లో మరియు బహిరంగ ప్రదేశంలో బహిరంగ కమ్యూనికేషన్ను పెంపొందించడం ద్వారా ప్రశ్నార్థకమైన దాని గురించి మాట్లాడుకోవడం సౌకర్యవంతంగా ఉంటుంది.

SMART చురుకు బ్రౌజింగ్:

సోషల్ ప్రొఫైల్స్ నుంచి సేకరించిన సమాచారం ఆధారంగా హ్యాకర్లు ఫిషింగ్ స్కామ్ లను రూపొందించవచ్చు. మోసాల నుండి మిమ్మల్ని మీరు రక్షించుకోవడానికి ఇక్కడ కొన్ని స్మార్ట్ చిట్కాలు ఉన్నాయి.

S-Safe	M-Meeting	A-Ask	R-Reliable	T-Tell
సురక్షితంగా ఉండటానికి, మీ వ్యక్తిగత సమాచారాన్ని ఆన్‌లైన్‌లో అపరిచితులతో ఎప్పుడూ షేర్ చేయండి.	మీకు వ్యక్తిగతంగా తెలిసిన వారిని మాత్రమే కలవండి. మీరు ఆన్‌లైన్‌లో కలుసుకున్న అపరిచితుడిని ఎప్పుడూ కలవకండి.	భద్రత గురించి సందేహం ఉంటే, సహాయం కోసం పరిజ్ఞానం ఉన్న వ్యక్తిని అడగండి. స్నేహితుల అభ్యర్థనలను ఎప్పుడూ అంగీకరించవద్దు లేదా అపరిచితుల నుండి ఇమెయిల్‌లను తెరవవద్దు.	ఏదైనా వెబ్‌సైట్‌ను ఉపయోగించే ముందు లేదా ఏదైనా యాప్‌ని డౌన్‌లోడ్ చేసే ముందు విశ్వసనీయత తనిఖీ అవసరం	మీ ఆన్‌లైన్ ఖాతాతో ఏవైనా చట్టవిరుద్ధ కార్యకలాపాలు గమనించినట్లయితే సంబంధిత అధికారులకు తెలియజేయండి

1. ప్రయాణ ప్రణాళికలు లేదా కుటుంబ వివరాలు వంటి మీ వ్యక్తిగత సమాచారాన్ని పంచుకోవద్దు. హ్యాకర్లు ఆ పోస్ట్ లోని సమాచారాన్ని మీకు వ్యతిరేకంగా ఉపయోగించవచ్చు
2. మీ ఇ-మెయిల్ మరియు కాంటాక్ట్ నెంబరును ఆన్ లైన్ లో పోస్ట్ చేయవద్దు, భాగస్వామ్యం చేయవద్దు లేదా ట్వీట్ చేయవద్దు.
3. అపరిచితుల స్నేహితుల అభ్యర్థనలను అంగీకరించవద్దు.
4. మీ వర్క్ స్టేషన్ నుండి ఫోటోలను భాగస్వామ్యం చేసేటప్పుడు, మీ కంప్యూటర్ సిస్టమ్ నుండి ఏదైనా బహిర్గతం కాకుండా చూసుకోండి.
5. విభిన్న సోషల్ మీడియా ప్లాట్‌ఫారమ్లలో ఎల్లప్పుడూ వేర్వేరు ప్రొఫైల్ చిత్రాలను ఉపయోగించడానికి ప్రయత్నించండి.

సురక్షిత బ్రౌజింగ్ టూల్స్

ఫైర్ వాల్: ఫైర్ వాల్ అనేది నెట్ వర్క్ కు అనధికారిక ప్రాప్యతను నిరోధించడానికి మరియు భద్రతా ప్రమాదాలను తగ్గించడానికి కొన్ని నిబంధనలను ఉపయోగించి ట్రాఫిక్ ను తనిఖీ చేయడానికి మొదటి రక్షణ మార్గంగా పనిచేసే సాఫ్ట్ వేర్.

యాంటీవైరస్:

కంప్యూటర్ వైరస్ అనేది హానికరమైన కోడ్ లేదా ప్రోగ్రామ్, ఇది తనను తాను ప్రతిబింబిస్తుంది మరియు కంప్యూటర్ పనిచేసే విధానాన్ని అంతరాయం కలిగించడానికి రూపొందించబడింది. చట్టబద్ధమైన ప్రోగ్రామ్కు చొప్పించడం లేదా జతచేయడం ద్వారా వైరస్ పనిచేస్తుంది. డేటాను కరప్ట్ చేయడం లేదా నాశనం చేయడం ద్వారా సిస్టమ్ సాఫ్ట్ వేర్ ను దెబ్బతీసే లేదా హాని కలిగించే సామర్థ్యాన్ని వైరస్ కలిగి ఉంటుంది.
యాంటీ వైరస్ అనేది వైరస్ లు మరియు వార్మ్ లు వంటి మాల్ వేర్ ల ద్వారా సంక్రమణను నిరోధించడానికి మీ కంప్యూటర్ లేదా మొబైల్ పరికరంలో ఇన్ స్టాల్ చేయబడిన భద్రతా ప్రోగ్రామ్.

మీ పరికరం లేదా సిస్టమ్ లో యాంటీ వైరస్ ఇన్ స్టాల్ చేయడం వల్ల కలిగే ప్రయోజనాలు:

- వైరస్లను గుర్తించడం, నిరోధించడం మరియు తొలగించడం.
- గుర్తింపు దొంగతనాన్ని నిరోధించడం మరియు ఫిషింగ్ను నిరోధించడం.
- హానికరమైన వెబ్సైట్లు మరియు లింక్ల గురించి హెచ్చరిక.
- సురక్షిత పాస్వర్డ్ ఎన్క్రిప్షన్తో ఆన్లైన్ ఖాతాలను సురక్షితంగా ఉంచడం.
- కంప్యూటర్ స్మూత్ రన్నింగ్.

ఇంటర్నెట్ అనేది సమాచారం, దృష్టి మరల్చే ప్రకటనలు, ప్రమాదకరమైన మాల్వేర్ మరియు మోసపూరిత క్లిక్-బెయిట్ లింక్ల సంక్లిష్ట మిశ్రమం, ఇది అనుమానాస్పద వినియోగదారులను సైబర్ పీడకలలలోకి తీసుకువెళుతుంది. మాల్వేర్ మరియు ఇతర బ్రౌజర్ ఆధారిత దాడుల గురించి ఆందోళన చెందకుండా వెబ్ యొక్క గమ్మత్తైన భూభాగాన్ని నావిగేట్ చేయడానికి, బ్రౌజర్ విక్రేతలు అనేక సహాయక భద్రతా లక్షణాలను అందిస్తారు.

ఇంటర్నెట్ లో Safety కొరకు**Browsers** అందించే ఫీచర్లు

1. గూగుల్ క్రోమ్ నుంచి సేఫ్ బ్రౌజింగ్ ఫీచర్
2. మైక్రోసాఫ్ట్ ద్వారా స్మార్ట్ స్క్రీన్ ఫిల్టర్
3. మొజిల్లా ఫైర్ ఫాక్స్ ద్వారా ఫిషింగ్ ఫిల్టర్

2. ఈ ఫీచర్లు ఫిషింగ్ దాడులు మరియు మాల్వేర్ నుండి కంప్యూటర్లను రక్షించడంలో సహాయపడతాయి.

ఆన్లైన్లో మిమ్మల్ని సురక్షితంగా ఉంచగల మరియు ఆన్లైన్లో రక్షణ కవచాన్ని నిర్మించడంలో మీకు సహాయపడే కొన్ని దశలు ఇక్కడ ఉన్నాయి.

1. **సెన్సిటివ్ బ్రౌజింగ్**: బ్యాంకు లావాదేవీల కోసం కేఫ్ లు మొదలైన వాటిలో ఓపెన్ నెట్ వర్క్ లను తరచుగా ఉపయోగిస్తాం. సైబర్ నేరగాళ్లు మీ బ్యాంక్ వివరాలను క్షణాల్లో కాపీ చేసి మీరు కష్టపడి సంపాదించిన డబ్బును దోచుకుంటారు.

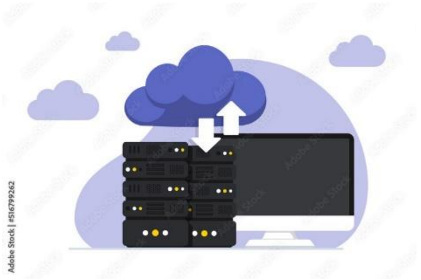
2. **స్పామ్** సందేశాలను గుర్తించడం మరియు నివారించడం సులభం. 'ఆర్బీఐ నుంచి సందేశం' లేదా 'మీ సహాయం అవసరం' వంటి పదాలు. ఈ సందేశాలలో ఉపయోగించబడతాయి. వాటికి దూరంగా ఉండాలని, ఇలాంటి అనుమానాస్పద లింకులు ఓపెన్ చేయొద్దన్నారు.

3. **స్ట్రాంగ్ పాస్ వర్డ్ లను** క్రాక్ చేయడం కష్టం. ప్రతి విభిన్న ఆన్ లైన్ ఖాతాకు ఎల్లప్పుడూ వేర్వేరు పాస్ వర్డ్ లను ఉపయోగించడానికి ప్రయత్నించండి. వెబ్సైట్ల పాస్వర్డ్ పాలసీ ప్రకారం మీరు ఎల్లప్పుడూ మీ పాస్వర్డ్లను సెట్ చేయాలి. పాస్ వర్డ్ లు ఆల్ఫా-న్యూమరిక్ గా ఉండాలి మరియు వాటిని బలంగా చేయడానికి ప్రత్యేక అక్షరాలను కలిగి ఉండాలి.

- **మీ ఖాతాలు/సెషన్ ల నుంచి సైన్ అవుట్** చేయండి: మేము సాధారణంగా మా పరికరాల్లో మా మెయిల్ లేదా సోషల్ మీడియా ఖాతాలు లేదా బ్యాంకింగ్ సెషన్ లకు లాగిన్ అవుతాము. కానీ ఇది మన సైబర్ భద్రతకు కూడా ముప్పుగా పరిణమించవచ్చు.

ఎల్లప్పుడూ మీ ఖాతాల నుండి లాగ్ అవుట్ చేయండి మరియు మీ పరికరాల్లో మీ బ్యాంక్ లాగిన్ లు.

1. **సోషల్ మీడియాలో భద్రత**:ఫేస్ బుక్ లేదా ఇన్ స్టాగ్రామ్ మరియు ఇతర సోషల్ సైట్లలో చిత్రాలను అప్ లోడ్ చేయడం ఈ రోజుల్లో చాలా సాధారణం, కానీ ఈ చిత్రాలను దుర్వినియోగం చేయవచ్చు. మీ ఆన్ లైన్ డేటాను స్టాకర్లు మరియు ఇతర ప్రమాదాల నుండి సురక్షితంగా ఉంచడానికి, మీరు మీ ఖాతా సెట్టింగ్ లను పబ్లిక్ నుండి ప్రైవేట్ కు మార్చాలి.



2. **డేటా బ్యాకప్**: ఫిజికల్ డ్రైవ్ లు లేదా ఆన్ లైన్ స్టోరేజ్ అంటే క్లౌడ్ స్టోరేజ్ సహాయంతో మీ డేటాను ఎల్లప్పుడూ బ్యాకప్ చేయండి. ఈ విధంగా, మీ పరికరానికి ఏదైనా జరిగితే మీ డేటా సురక్షితంగా ఉంటుంది.
3. **వెబ్ సైట్ల భద్రతా హెచ్చరిక** : మెకాఫీ సైట్ అడ్వైజర్ వంటి అనేక సైట్ భద్రతా పొడిగింపులు వెబ్ సైట్ బ్రౌజింగ్ యొక్క భద్రత గురించి మిమ్మల్ని హెచ్చరిస్తాయి.

పబ్లిక్ మరియు ఉచిత వై-ఫై

పబ్లిక్ వై-ఫై అసురక్షితమైనది మరియు ప్రమాదకరమైనది. పబ్లిక్ వై-ఫై యొక్క అసురక్షిత కనెక్షన్ల నుండి కొన్ని సంభావ్య ప్రమాదాలు

1. మిడిల్ ఎటాక్ లో వ్యక్తి..
2. అన్ ఎన్ క్రిప్టెడ్ నెట్ వర్క్ లు
3. మాల్వేర్ పంపిణీ
    1. వైరస్ లు
    2. పురుగులు
    3. ట్రోజన్ గుర్రాలు
    4. రాన్సమ్వేర్
    5. యాడ్ వేర్
4. స్నూపింగ్ & స్నిఫింగ్
5. వ్యక్తిగత సమాచారం చోరీ
    1. లాగిన్ క్రెడెన్షియల్
    2. ఆర్థిక సమాచారం
    3. వ్యక్తిగత డేటా
    4. చిత్రాలు[మార్చు]
6. సెషన్ హైజాకింగ్

పబ్లిక్ వై-ఫై ఉపయోగిస్తున్నప్పుడు సురక్షితంగా ఉండటం

నివారించండి

సున్నితమైన పత్రాలు/ఫైళ్లను తెరవడం

వాడు

పబ్లిక్ Wi-Fi ద్వారా గుప్తీకరణను ఉపయోగించి VPN సురక్షిత కనెక్షన్‌లు

తెరవండి

https వెబ్‌సైట్‌లు మాత్రమే

ప్రారంభించు

సురక్షిత బ్రౌజర్ సెట్టింగ్‌లు

వా డు

గోప్యతా స్క్రీన్

ఆపి వేయి

ఫైల్ షేరింగ్

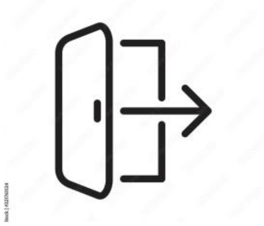
వాడు

రెండు-కారకాల ప్రమాణీకరణ

నిర్ధారించడానికి

మీ ఆపరేటింగ్ సిస్టమ్

గుర్తుంచుకోండి



పబ్లిక్ Wi-Fi నుండి లాగ్ అవుట్ చేయడానికి

సైబర్ నేరాల రకాలు:

1. **కాపీరైట్లను ఉల్లంఘించడం**: అనుమతి లేకుండా ఒకరి కాపీరైట్ చేసిన పనిని ఉపయోగించడం. ఉదాహరణకు, ఒక కంపెనీ వెబ్సైట్ నుండి ఒక చిత్రాన్ని ఉపయోగించడం మరియు దానిని మీ వ్యక్తిగత ఖాతాలో పోస్ట్ చేయడం.
2. **రాన్సమ్ వేర్ దాడులు**: దాడి చేసిన వ్యక్తికి రాన్సమ్ రుసుం చెల్లించే వరకు ఎన్ క్రిప్ట్ చేయడం ద్వారా డేటా లేదా పరికరానికి ప్రాప్యతను ప్రచురించడం లేదా నిరోధించడం మాల్ వేర్.

3. **అక్రమ జూదం**: ఆన్ లైన్ జూదం అంతర్జాలం ద్వారా కాసినోలు లేదా క్రీడలపై బెట్టింగ్ కు పాల్పడుతోంది.
4. **సైబర్ గూఢచర్యం**: సైబర్ గూఢచర్యం అనేది పోటీలో ప్రయోజనాలను పొందడానికి కంప్యూటర్ పరికరాల నుండి లేదా ద్వారా డేటా, సున్నితమైన సమాచారం లేదా మేధో సంపత్తిని ఉద్దేశపూర్వకంగా దొంగిలించడం. ఉదాహరణకు, రాజకీయ పార్టీలు ఎన్నికల సమయంలో పోటీదారుల డేటాను దొంగిలిస్తాయి.
5. **ఇమెయిల్ మరియు ఇంటర్నెట్ మోసం**
6. **గుర్తింపు మోసం**
7. **ఫైనాన్షియల్ లేదా కార్డ్ పేమెంట్ డేటా చోరీ**
8. క్రిప్టోజాకింగ్: క్రిప్టోజాకింగ్ అనేది ఒక రకమైన సైబర్ నేరం, ఇది క్రిప్టోకరెన్సీ కోసం మైనింగ్ చేయడానికి సైబర్ నేరగాళ్లు ప్రజల పరికరాలను (కంప్యూటర్లు, స్మార్ట్‌ఫోన్లు, టాబ్లెట్లు లేదా సర్వర్లు) అనధికారికంగా ఉపయోగించడం. అనేక రకాల సైబర్ నేరాల మాదిరిగానే, ఉద్దేశ్యం లాభం, కానీ ఇతర బెదిరింపుల మాదిరిగా కాకుండా, ఇది బాధితుడి నుండి పూర్తిగా దాచి ఉంచడానికి రూపొందించబడింది.
9. **సైబర్ డిటెక్షన్:** దాడిని ఆపడానికి బదులుగా డబ్బు డిమాండ్ లేదా మరేదైనా ప్రతిస్పందనతో కూడిన దాడి లేదా బెదిరింపుతో కూడిన నేరాన్ని సైబర్ ఎక్స్‌ప్రెస్ అంటారు.

హ్యాకర్ల నుండి మీ పరికరాన్ని రక్షించే పద్ధతులు:

- ఫైర్‌వాల్ ఉపయోగించండి
- యాంటీ-వైరస్‌ని ఇన్‌స్టాల్ చేయండి
- బలమైన పాస్‌వర్డ్‌లను ఉపయోగించండి
- తాజా బ్రౌజర్‌లను ఉపయోగించండి
- మీ నెట్‌వర్క్‌ను సురక్షితం చేయండి
- రెండు-కారకాల ప్రమాణీకరణను ఉపయోగించండి
- యాప్‌లు మరియు వ్యక్తిగత సమాచారం కోసం సెక్యూరిటీ పిన్‌లను ఉపయోగించండి

రిఫరెన్స్ రీడింగ్:

- **వ్యక్తిగత గోప్యత: ఇంటర్నెట్లో సురక్షితమైన బ్రౌజింగ్ కోసం టాప్ 12 చిట్కాలు:** https://cybersecurityventures.com/12-tips-for-safer-browsing/
- **మహిళలు మరియు బాలికలు ఆన్లైన్లో సురక్షితంగా ఉండటానికి సహాయపడే 5 చిట్కాలు:** https://www.globalcitizen.org/en/content/tips-to-help-women-girls-stay-safe-online/
- **పబ్లిక్ వైఫై భద్రతా ప్రమాదాలను ఎలా నివారించాలి:** https://www.kaspersky.co.in/resource-center/preemptive-safety/public-wifi-risks

మాడ్యూల్ 6

డిజిటల్ హక్కులు, చట్టాలు మరియు పరిష్కార యంత్రాంగాలు

డిజిటల్ సిటిజన్: ఇంటర్నెట్, ఇతర డిజిటల్ టెక్నాలజీలను బాధ్యతాయుతంగా ఉపయోగించే వ్యక్తిని డిజిటల్ సిటిజన్ అంటారు.

డిజిటల్ పౌరుడి పాత్ర:

1. మీ వ్యక్తిగత సమాచారాన్ని సంరక్షించండి
2. మీ డిజిటల్ పాదముద్రను జాగ్రత్తగా నిర్వహించండి (వారి ఆన్ లైన్ యాక్టివిటీ ఫలితంగా ఇంటర్నెట్ లో ఉన్న ఒక నిర్దిష్ట వ్యక్తి గురించిన సమాచారం)
3. ఆన్ లైన్ లావాదేవీ చట్టాలకు కట్టుబడి ఉండండి
4. చట్టవ్యతిరేక కార్యకలాపాలకు అండగా నిలబడండి
5. డిజిటల్ సిటిజన్ గా మీ హక్కులను తెలుసుకోండి

వ్యక్తిగత సమాచారాన్ని భాగస్వామ్యం చేసేటప్పుడు బాధ్యతాయుతమైన SMART డిజిటల్ పౌరులుగా ఉండండి:

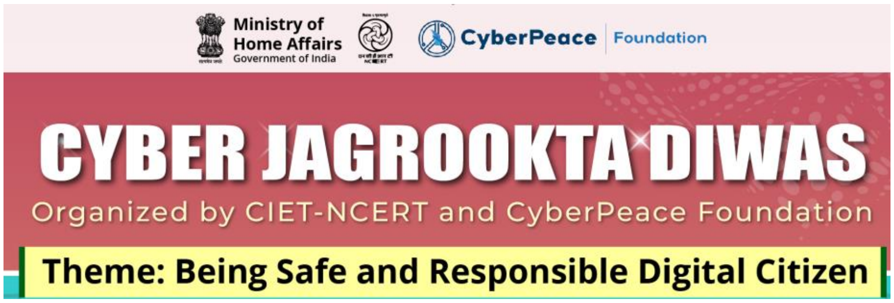
S-Safe	M-Meeting	A-Ask	R-Reliable	T-Tell
ఆన్‌లైన్‌లో సురక్షితంగా ఉండటానికి, మీ వ్యక్తిగత సమాచారాన్ని ఆన్‌లైన్‌లో అపరిచితులతో ఎప్పుడూ షేర్ చేయండి.	మీకు వ్యక్తిగతంగా తెలిసిన వారిని మాత్రమే కలవండి. మీరు ఆన్‌లైన్‌లో కలుసుకున్న అపరిచితుడిని ఎప్పుడూ కలవకండి.	భద్రత గురించి సందేహం ఉంటే, సహాయం కోసం పరిజ్ఞానం ఉన్న వ్యక్తిని అడగండి. స్నేహితుల అభ్యర్థనలను ఎప్పుడూ అంగీకరించవద్దు లేదా అపరిచితుల నుండి ఇమెయిల్‌లను తెరవవద్దు.	ఏదైనా వెబ్‌సైట్‌ను ఉపయోగించే ముందు లేదా ఏదైనా యాప్‌ని డౌన్‌లోడ్ చేసే ముందు విశ్వసనీయత తనిఖీ అవసరం	మీ ఆన్‌లైన్ ఖాతాతో ఏవైనా చట్టవిరుద్ధ కార్యకలాపాలు గమనించినట్లయితే సంబంధిత అధికారులకు తెలియజేయండి

ఆన్ లైన్ లో బ్యాంక్ ఖాతాను ఉపయోగించేటప్పుడు బాధ్యతలు

చే	వద్దు
బ్యాంకు జారీ చేసిన లాగిన్ క్రెడెన్షియల్స్ ను ఎల్లప్పుడూ ఉపయోగించండి.	మీ బ్యాంక్ ఖాతాలోకి లాగిన్ అవ్వడానికి బాహ్య లింక్స్ ఎప్పుడూ ఉపయోగించలేరు
ఏదైనా సమస్య ఉంటే బ్యాంకు డాక్యుమెంట్లు లేదా వారి అధికారిక వెబ్సైట్లో పేర్కొన్న నంబర్లకు కాల్ చేయండి.	ఏ ఎస్ఎంఎస్ లో పేర్కొన్న నంబర్ కు కాల్ చేయవద్దు. అది ఫేక్ మెసేజ్ కావొచ్చు.
మీ బ్యాంకులో మీ కేవైసీ (నో యువర్ కస్టమర్ వివరాలు) అప్ డేట్ అయ్యేలా చూసుకోండి.	మీ KYC వివరాలను ఏ బాహ్య పక్షం/వ్యక్తితోనూ పంచుకోవద్దు.

డిజిటల్ పౌరుల బాధ్యతల దిశగా ప్రభుత్వ చొరవ

1. పాఠశాలలు, కళాశాలల విద్యార్థులు, ఉపాధ్యాయులు, తల్లిదండ్రుల్లో అవగాహన కల్పించేందుకు ప్రతి నెలా మొదటి బుధవారం 'సైబర్ జాగృతి దివస్'ను పాటించాలని ప్రతిపాదించారు.
2. **డిజిటల్ పౌరుల హక్కులు మరియు బాధ్యతల గురించి అవగాహన కల్పించడానికి ప్రారంభించబడింది**



డిజిటల్ పౌరుల హక్కులు:

1. **యాక్సెస్ హక్కు:** ప్రతి పౌరుడికి ఇంటర్నెట్ పొందే హక్కు ఉంది. భావ ప్రకటనా స్వేచ్ఛకు ఇది ఒక ముఖ్యమైన హక్కుగా పరిగణించబడుతుంది. సుప్రీంకోర్టు ప్రకారం ఇంటర్నెట్ యాక్సెస్ ప్రాథమిక హక్కు.

2. **రైట్ టు ఫ్రీడమ్ ఆఫ్ ఇఎక్స్ప్రెషన్, ఐఎన్ ఫార్మేషన్ మరియు సి కమ్యూనికేషన్:** ప్రతి పౌరుడికి ఏదైనా సమాచారాన్ని వ్యక్తీకరించడానికి, యాక్సెస్ చేయడానికి లేదా కమ్యూనికేట్ చేయడానికి సోషల్ మీడియా నెట్ వర్క్ ను ఉపయోగించే హక్కు ఉంది.

3. **గోప్యత హక్కు మరియు డేటా రక్షణ:** సామాజిక మాధ్యమాల ద్వారా అందించే వారి వ్యక్తిగత సమాచారాన్ని సంరక్షించుకునే హక్కు వినియోగదారునికి ఉంది. అన్ని సోషల్ మీడియా ప్లాట్ఫారమ్లు గోప్యత మరియు డేటా సంరక్షణ సెట్టింగ్స్ అందించడం తప్పనిసరి, ఎందుకంటే యూజర్ మీ ప్రొఫైల్ను ఎవరు చూడవచ్చో ఎంచుకోవచ్చు లేదా వారి ప్రొఫైల్ను ప్రైవేట్గా ఉంచవచ్చు.

4. **రక్షణ హక్కు:** సామాజిక మాధ్యమాల ద్వారా ఇంటర్నెట్ వినియోగదారులకు రక్షణ కల్పించేలా ప్రభుత్వం చర్యలు తీసుకోవాలి. అలాగే, వినియోగదారులు 1930 కు కాల్ చేయడం ద్వారా ఇంటర్నెట్ ద్వారా ఏదైనా చట్టవ్యతిరేక కార్యకలాపాలను నివేదించడానికి సైబర్ సెల్కు సులభంగా యాక్సెస్ చేయవచ్చు.

పౌరుల ఆన్ లైన్ భద్రత కోసం డిజిటల్ టూల్స్ - ఆన్ లైన్ లావాదేవీలు

- మనీ-యూనిఫైడ్ పేమెంట్స్ ఇంటర్‌ఫేస్ కోసం భారత్ ఇంటర్‌ఫేస్ (BHIM-UPI)
- తక్షణ చెల్లింపు సేవ (IMPS)
- ప్రీ-పెయిడ్ చెల్లింపు సాధనాలు (PPIలు)
- నేషనల్ ఎలక్ట్రానిక్ టోల్ కలెక్షన్ (NETC)
- రియల్-టైమ్ గ్రాస్ సెటిల్మెంట్ (RTGS)

అనువర్తనాలను డౌన్ లోడ్ చేయడానికి, ఈ క్రింది సురక్షితమైన ఆన్ లైన్ స్టోర్లను ఉపయోగించండి:

GET IT ON Google Play

Download on the App Store

అక్రమ సైబర్ కార్యకలాపాలు:
అత్యంత సాధారణ చట్టవ్యతిరేక సైబర్ కార్యకలాపాలు:

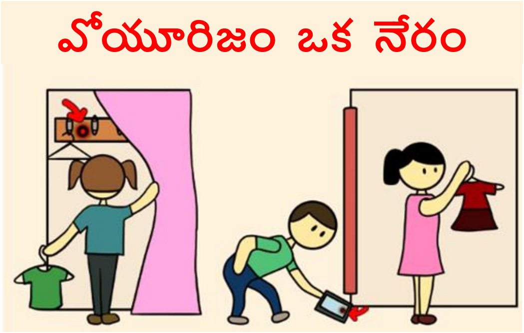
1. **సైబర్ స్టాకింగ్ -** సైబర్ స్టాకింగ్ అనేది ఎలక్ట్రానిక్ మీడియాను ఉపయోగించి ఏ వ్యక్తినైనా వెంబడించడాన్ని సూచిస్తుంది. ఇందులో ఇవి ఉన్నాయి:
    1. గుర్తింపు దొంగతనం చేయాలనే ఉద్దేశంతో సమాచారం రాబట్టారు.
    2. అవాంఛిత, భయపెట్టే లేదా అశ్లీల ఇమెయిల్స్ లేదా సందేశాలను పంపడం.
    3. సోషల్ మీడియాలో వేధించడం లేదా బెదిరించడం..

2. గోప్యత/గోప్యత ఉల్లంఘన మరియు ఉల్లంఘన

1. వ్యక్తి యొక్క సమ్మతి లేకుండా ఏదైనా వ్యక్తిగత సమాచారం లేదా చిత్రాన్ని సోషల్ మీడియా/ ఏదైనా ప్లాట్ ఫామ్ పై ప్రచురించడం లేదా ప్రసారం చేయడం ఇందులో ఉంటుంది.
2. చట్టప్రకారం అవసరమైనప్పుడు మాత్రమే బ్యాంకులు, సోషల్ మీడియా ప్లాట్ఫామ్లు ఒకరి వ్యక్తిగత సమాచారాన్ని పంచుకోగలవు.

3. Voyeurism

1. **ఇది వ్యక్తిగత చర్యలో నిమగ్నమైన వ్యక్తి** యొక్క చిత్రాలు లేదా వీడియోలను **వారి** ప్రమేయం లేకుండా చూడటం, క్యాప్చర్ చేయడం లేదా భాగస్వామ్యం **చేయడాన్నిసూచిస్తుంది.**
2. **ఐపీసీ సెక్షన్ 354(సీ)** ప్రకారం ఇది శిక్షార్హమైన చర్య.
3. **వెంటనే సి.వైబర్ సెల్/ఉమెన్ సెల్/సమీపంలోని పోలీస్ స్టేషన్ కు తెలియజేయాలి.**



4. **సి** నుండి **మిమ్మల్ని మీరు పరీక్షించుకోవడానికి దశలు:**

1. సైబర్ సెల్/ఉమెన్ సెల్ కు రిపోర్ట్ చేయండి.
2. వాటిని బ్లాక్ చేయండి
3. ఏం జరుగుతోందో కుటుంబ సభ్యులకు చెప్పండి
4. మీ ఖాతాపై గోప్యతా ఫిల్టర్ లను సెట్ చేయండి
5. అన్ని సాక్ష్యాలను సేవ్ చేయండి
6. ఆపమని వారికి చెప్పండి.

చట్టవ్యతిరేక డిజిటల్ కార్యకలాపాలకు చట్టపరమైన నిబంధనలు

భారత శిక్షాస్మృతి 1860 ప్రకారం ఈ క్రింది కొన్ని చట్టపరమైన నిబంధనలు ఉన్నాయి.

సెక్షన్	చట్టవ్యతిరేక కార్యకలాపాలు	దండన
సెక్షన్ 354A	• మహిళల సమ్మతి లేకుండా లైంగిక కంటెంట్ ను చూపించడం లేదా పంచుకోవడం • లైంగిక కోరికలు అడగడం • లైంగిక గుర్తింపులు/సందేశాలను పోస్ట్ చేయడం/పంపడం	• మూడేళ్ల వరకు కఠిన కారాగార శిక్ష, లేదా జరిమానా లేదా రెండూ విధించవచ్చు.
సెక్షన్ 354సీ	• వాయురిజం	• మొదటి నేరం రుజువైతే జరిమానాతో పాటు మూడేళ్ల వరకు జైలు శిక్ష • ఆ తర్వాత ఏడేళ్ల తర్వాత శిక్షలు పడ్డాయి.
సెక్షన్ 354డి	• సైబర్ స్టాకింగ్	• మొదటి నేరానికి మూడేళ్ల వరకు జైలు శిక్ష • నేరం రుజువైతే జరిమానా, ఐదేళ్ల జైలు శిక్ష

ఇన్ఫర్మేషన్ టెక్నాలజీ యాక్ట్, 2008 ప్రకారం ఈ క్రింది కొన్ని చట్టపరమైన నిబంధనలు ఉన్నాయి.

ఐటి చట్టంలోని సెక్షన్	చట్టవ్యతిరేక కార్యకలాపాలు	దండన
సెక్షన్ 66ఈ	1. గోప్యత ఉల్లంఘన • వారి అనుమతి లేకుండా ఏదైనా వ్యక్తి యొక్క ప్రైవేట్ ప్రాంతం యొక్క చిత్రాన్ని క్యాప్చర్ చేయడం, ప్రచురించడం లేదా ప్రసారం చేయడం	• ఇది మూడు సంవత్సరాల వరకు జైలు శిక్ష మరియు/ లేదా జరిమానా విధించవచ్చు.
సెక్షన్ 66సీ	1. గుర్తింపు దొంగతనం 2. సైబర్ హ్యాకింగ్ • ఎలక్ట్రానిక్ సంతకం దుర్వినియోగం	1. మూడేళ్ల వరకు జైలు శిక్ష • రూ.లక్ష వరకు జరిమానా
సెక్షన్ 67	• అశ్లీల కంటెంట్ యొక్క ప్రచురణ లేదా ప్రసారం.	1. మొదటి నేరానికి మూడేళ్ల వరకు జైలు శిక్ష, జరిమానా • రెండోసారి నేరం రుజువైతే ఐదు నుంచి ఏడేళ్ల వరకు జరిమానా

కాపీరైట్ చట్టం ప్రకారం, మీరు మీ సృజనాత్మక రచనను సోషల్ మీడియాలో పోస్ట్ చేసినప్పుడు, దాని కాపీరైట్ మీకు ఉంటుంది. మీ అనుమతి లేకుండా ఎవరూ పనిని ఉపయోగించలేరు, ప్లాట్ఫామ్ యాజమాన్యాన్ని తీసుకోదు.

చట్టవ్యతిరేక డిజిటల్ కార్యకలాపాల కొరకు పరిష్కార యంత్రాంగాలు

ఏదైనా సైబర్ చట్టవ్యతిరేక కార్యకలాపాలకు వ్యతిరేకంగా మీరు ఈ క్రింది వాటిలో మీ ఫిర్యాదును నమోదు చేయవచ్చు. :

- https://cybercrime.gov.in/Default.aspx

నేషనల్ సైబర్ క్రైమ్ రిపోర్టింగ్ హెల్ప్‌లైన్ నంబర్-1930 (9.00 AM to 6 PM)

- https://ncrb.gov.in/en/node/2318

UMANG (న్యూ-ఏజ్ గవర్నెన్స్ కోసం ఏకీకృత మొబైల్ అప్లికేషన్)

- https://web.umang.gov.in/landing/department/cybercrime-reporting-portal.html

సైబర్ పోలీస్ పోర్టల్

- https://cyberpolice.nic.in/

సైబర్ క్రైమ్ పీలో ఫిర్యాదు చేయడానికి చర్యలు

1. **లింక్ లోకి వెళ్లండి: https://cybercrime.gov.in/**
2. **వెబ్ సైట్ యొక్క దిగువ విభాగానికి దిగువకు స్క్రోల్ చేయండి మరియు తరువాత ఫైల్ ఎ కంప్లయింట్ బటన్** మీద క్లిక్ చేయండి.
3. **రిపోర్ట్ అజ్ఞాతంగా ఉండే బటన్** మీద క్లిక్ చేయండి.
4. **ఫారం యొక్క అన్ని విభాగాలను నింపండి మరియు తదుపరి ప్రాసెసింగ్ కోసం సబ్మిట్ చేయండి. స్క్రీన్ షాట్లు వంటి సాక్ష్య పత్రాలను మీ వద్ద సిద్ధంగా ఉంచుకోండి.**
5. **మీ కంప్లైంట్ రిజిస్టర్ అవుతుంది. ఏదైనా సహాయం కోసం మీరు 1930 కు కాల్ చేయవచ్చు లేదా ఫిర్యాదును నమోదు చేయవచ్చు.**

రిఫరెన్స్ రీడింగ్:

- సైబర్ జాగృతి దివస్ గురించి మరింత తెలుసుకోవడానికి ఈ క్రింది లింకులు చూడండి:
  [Cyber Jaagrookta (Awareness) Diwas (Day 1 - Day 5)]
- సోషల్ మీడియా ప్లాట్ ఫారమ్ యొక్క మరింత సురక్షిత ఉపయోగం తెలుసుకోవడం కొరకు ఈ క్రింది లింక్ లను చూడండి.:
  [Be Careful While Using Social Media Platforms]
- ఆన్ లైన్ సైబర్ క్రైమ్ ని ఎలా రిపోర్ట్ చేయాలో తెలుసుకోవడానికి ఈ క్రింది లింక్ లను చూడండి:
  [Cyber Crime Helpline Number]
- భారతదేశంలో ఇ-కామర్స్ చట్టాలు మరియు నిబంధనలు ఎలా ఉన్నాయో తెలుసుకోవడానికి ఈ క్రింది లింక్ లను చూడండి:
  [E-Commerce Laws and Regulations in India]

- నా ఆన్ లైన్ లావాదేవీ సురక్షితమేనా అని నేను ఎలా చెప్పగలనో తెలుసుకోవడం కొరకు దిగువ లింక్ లను చూడండి.?
  [Is My Online Transaction Secure]

సూచించిన ఆచరణాత్మక కార్యకలాపాలు

డిజిటల్ సేఫ్టీ అండ్ సెక్యూరిటీ ప్రోగ్రామ్ యొక్క ఆన్ లైన్ లెర్నింగ్ మాడ్యూల్స్ ని మీరు పూర్తి చేశారని తెలుసుకోండి, మీ నిజ జీవితంలో అభ్యాసాన్ని ప్రాక్టీస్ చేయడానికి మరియు అన్వయించడానికి దయచేసి ఈ కార్యకలాపాలను ప్రయత్నించండి. ఈ కార్యకలాపాలు మీ అభ్యసనను బలోపేతం చేస్తాయని మేము ఆశిస్తున్నాము.

1. మీ అన్ని సోషల్ మీడియా, బ్యాంకింగ్, ఇ-కామర్స్ మరియు ఇమెయిల్ ఖాతాలకు ప్రత్యేకమైన మరియు బలమైన 10 అక్షరాల ఆస్కీ పాస్ వర్డ్ లను సృష్టించండి
2. ప్రతిరోజూ మీ డేటాను బ్యాకప్ చేయండి లేదా ఆటోమేటిక్ బ్యాకప్ సదుపాయాన్ని సెటప్ చేయండి
3. మీ ఆపరేటింగ్ సిస్టమ్ సాఫ్ట్ వేర్ ను క్రమం తప్పకుండా తనిఖీ చేయండి మరియు అప్ డేట్ చేయండి (విండోస్/ఐఓఎస్/ఆండ్రాయిడ్)
4. ఇంటర్నెట్ బ్రౌజ్ చేసేటప్పుడు అజ్ఞాత మోడ్ ఉపయోగించండి మరియు దానిలో తేడా ఏమిటో తెలుసుకోండి
5. మీ బ్యాంక్ వెబ్ సైట్ లపై సురక్షితమైన ఆర్థిక లావాదేవీలను సులభతరం చేయడం కొరకు బ్యాంకింగ్ మరియు పేమెంట్ ప్రొటెక్షన్ ని ఎనేబుల్ చేయడం కొరకు మీ యాంటీ వైరస్ సాఫ్ట్ వేర్ ని సెటప్ చేయండి.
6. చిన్న పిల్లలు మీ పరికరాలను ఉపయోగిస్తున్నప్పుడు ప్రమాదకరమైన మరియు అభ్యంతరకరమైన వెబ్ సైట్ లను నిరోధించడానికి తల్లిదండ్రుల నియంత్రణను ప్రారంభించడానికి మీ యాంటీవైరస్ సాఫ్ట్ వేర్ ను సెటప్ చేయండి
7. మీ ఫోన్ లోని తెలియని నంబర్ల నుండి వచ్చే కాల్ లను నిశితంగా గమనించండి మరియు అవి అంతర్జాతీయ తెలియని నంబర్ల నుండి వచ్చినట్లయితే సమాధానం ఇవ్వవద్దు.
8. ఆధార్/పాన్ సంతకం చేసిన ఫోటోకాపీలను మాత్రమే సబ్మిట్ చేయండి మరియు మీరు ఫోటోకాపీలను ఎవరికి సమర్పిస్తున్నారు మరియు వాటిని సబ్మిట్ చేసే ఉద్దేశ్యాన్ని కూడా పేర్కొనండి.
9. డిజిలాకర్ అకౌంట్ క్రియేట్ చేసి మీ ఆధార్, పాన్, డ్రైవింగ్ లైసెన్స్, ఎడ్యుకేషన్ సర్టిఫికేట్లను అప్లోడ్ చేయండి.
10. గ్రూప్ లకు యాడ్ కాకుండా ఉండేందుకు వాట్సాప్ లో సెట్టింగ్స్ మార్చుకోండి.
11. మీకు పదేపదే సందేశాలు పంపే గుర్తుతెలియని వ్యక్తి (లేదా నంబర్) కోసం వాట్సాప్ లోని "బ్లాక్" ఫీచర్ ను ప్రయత్నించండి
12. ఫేస్ బుక్/ఇన్ స్టాగ్రామ్/ఇతర సోషల్ మీడియా సెట్టింగ్ లను ప్రైవేట్ గా మార్చండి
13. మీ మెయిల్ ఐడి కోసం 2-ఫ్యాక్టర్ ఆథెంటికేషన్ సృష్టించండి

14. మీ గూగుల్ అకౌంట్/ఐఓఎస్ అకౌంట్ లో ఫైండ్ మై ఫోన్ ను ఎనేబుల్ చేయండి
15. మీ వెబ్ బ్రౌజర్ లో భద్రతా ఫీచర్లను ప్రారంభించండి (గూగుల్ క్రోమ్/మైక్రోసాఫ్ట్ ఎడ్జ్/మొజిల్లా ఫైర్ ఫాక్స్/Opera/IoS)
16. వారానికి ఒకసారి మీ పరికరం నుండి బ్రౌజింగ్ చరిత్రను తొలగించండి
17. సైబర్ స్టాకింగ్ లేదా ఏదైనా చట్టవిరుద్ధమైన సైబర్ కార్యకలాపాలను ఎదుర్కొంటున్న ఎవరైనా/చిన్న పిల్లలను గమనించండి, మద్దతు ఇవ్వండి మరియు సహాయపడండి.
18. నేషనల్ సైబర్ క్రైమ్ రిపోర్టింగ్ పోర్టల్ (https://cybercrime.gov.in/Default.aspx) లో పంచుకోబడిన వివిధ సేవలు మరియు జాగ్రత్తలను అన్వేషించండి
19. Explore UMANG Website (https://web.umang.gov.in/landing/department/cybercrime-reporting-portal.html)
20. జాతీయ మహిళా కమిషన్ పోర్టల్ (http://ncw.nic.in/ncw-cells) లో పరిష్కారానికి వివిధ సెల్ లను అన్వేషించండి

గమనికలు