సైబర్ జ్ఞాన్

Supported by:

INFORMATION SECURITY EDUCATION & AWARENESS

CYBERSECURITY CENTRE of EXCELLENCE
A joint initiative of DSCI & Government of Telangana

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

www.isea.gov.in

https://ccoe.dsci.in/

www.endnowfoundation.org

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

ఎండ్ నౌ ఫౌండేషన్ భారతదేశం యొక్క మొట్టమొదటి లాభాపేక్ష లేని స్వచ్ఛంద సేవ సంస్థ. మహిళలు, యువత మరియు పిల్లల్లో బాధ్యతాయుతమైన అంతర్జాల ప్రవర్తనను మరియు డిజిటల్ సంరక్షణను ప్రోత్సహించడం ఈ సంస్థ యొక్క లక్ష్యం.

ఈ సైబర్ జ్ఞాన్ మా గౌరవనీయ
వ్యవస్థాపక ధర్మకర్త, దివంగత శ్రీ కాశీనాథ్ బత్తిన,
ఐపిఎస్ గారి జ్ఞాపకార్థం అంకితం చేయబడినది.

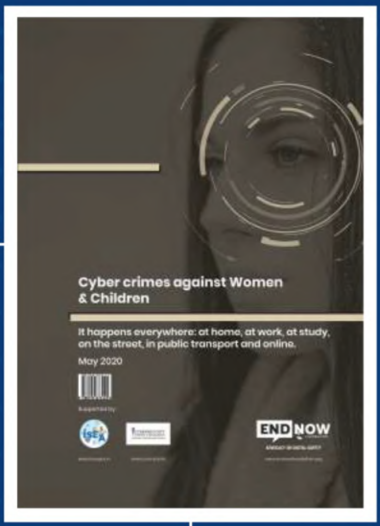
23 February 1938 - 26 July 2020

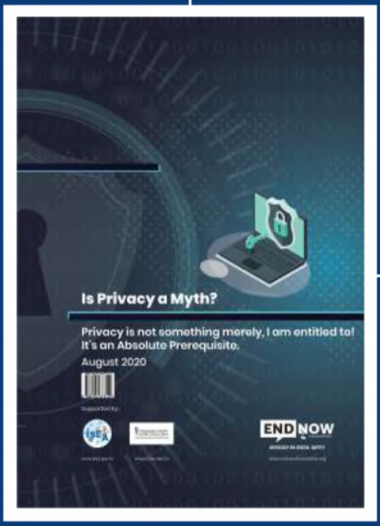
https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

మా ప్రచురణలు

(అమేజాన్‌లో లభ్యమగును)





https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

చరవాణి (స్మార్ట్‌ఫోన్స్)

21వ శతాబ్దంలో అతిపెద్ద మాదకద్రవ్యం కాని వ్యసనం

మీ చరవాణిలో మిమ్మల్ని బానిసలుగా చేసుకుంటే, మీ బానిసత్వం నుండి విముక్తి పొందడానికి కొన్ని మార్గదర్శకాలు

- మీ చరవాణిలో ప్రకటనలు నిలిపివేయండి.
- మీ చరవాణిని పడకగది వెలుపలే చార్జ్ చేయండి.
- మీ చరవాణికి బదులుగా మీ కంప్యూటర్ నుండి సాంఘిక ప్రసార మాధ్యమాన్ని ఉపయోగించండి.
- మీ చరవాణికి హెూం తెర (హెూం స్క్రీన్) పై ముఖ్యమైన అనువర్తనాలను మాత్రమే ఉంచండి.
- స్నేహితులు మరియు కుటుంబ సభ్యులతో భోజనం చేసేటప్పుడు మీ చరవాణిని దూరంగా ఉంచండి.
- పరికరాలు లేని సమావేశాలలో పాల్గొనండి.
- మీ చరవాణిలో "బూడిద స్థాయి" (గ్రే స్కేల్) విధానమును ఉపయోగించండి.
- సాంకేతిక పరిజ్ఞానాన్ని ఉపయోగించడాన్ని నియంత్రించడానికి, ఐఓఎస్ పరికరాలకోసం తెర సమయాన్ని (స్క్రీన్‌టైమ్) మరియు ఆండ్రాయిడ్ పరికరాలకోసం డిజిటల్ శ్రేయస్సు (డిజిటల్ వెల్‌బీయింగ్) ను అవలంబించండి

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

ఆన్‌లైన్ ఆటలు చాలా ప్రమాదాలతో కూడినవి

అంతర్జాల ఆటల ప్రతికూల ప్రభావాలను

తెలుసుకోవడానికి ఇది చదవండి.

- అంతర్జాల ఆటలు ఒక వ్యసనం
- ఈ వ్యసనం వల్ల కుటుంబం మరియు స్నేహితులకు దూరమవుతారు.
- నిద్రలేమికి గురి అవుతారు .
- ఆక్రోశం పెరుగుతుంది.
- ఆరోగ్యంపై చెడు ప్రభావాలు పడతాయి
- విలువైన సమయం వృధా అవుతుంది.
- ఖరీదైన అభిరుచి పెరుగుతుంది.
- కంటిచూపుపై ప్రభావం పడుతుంది.

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

మీరు భద్రతపై శ్రద్ధ చూపినప్పుడే సోషల్ మీడియా చాలా సరదాగా ఉంటుంది.

అంతర్జాల లోకంలో సురక్షితంగా ఉండడానికి ఇక్కడ కొన్ని చిట్కాలు ఉన్నాయి

- క్లిష్టమైన పాస్‌వర్డ్‌ను ఉపయోగించండి.
- మీ ప్రతి సామాజిక మాధ్యమం ఖాతాలకు వేరు వేరు పాస్‌వర్డ్లు ఉపయోగించండి.
- మీ భద్రతా జవాబులను ఎంపిక చేసుకోండి (ఈ ఎంపిక చాలా సోషల్ మీడియా ప్లాట్‌ఫాంలలో లభిస్తుంది).
- కంప్యూటర్ నుండి మాత్రమే సామాజిక మాధ్యమం ఉపయోగించండి.
- తెలియని వ్యక్తుల స్నేహపూర్వక అభ్యర్థనలను అంగీకరించేటప్పుడు జాగ్రత్త వహించండి.
- షార్ట్‌లింక్స్ క్లిక్ చేసేప్పుడు ఆలోచించి చేయండి.
- మీ వ్యక్తిగత సమాచారాన్ని ఇతరులకు పంచేప్పుడు జాగ్రత్త వహించండి.
- సామాజిక మాధ్యమం చానెల్ యొక్క గోప్యతా విధానాలతో పరిచయం కలిగి ఉండండి.
- వైరస్ నివారణ (యాంటివైరస్) సాఫ్ట్‌వేర్‌ను ఉపయోగించుకొని మీ కంప్యూటర్‌ను రక్షించుకోండి.
- మీ పని పూర్తికాగానే మీ కంప్యూటర్‌ని ఆపివేయండి (లాగ్ ఆఫ్ చేయండి).

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

సైబర్ బెదిరింపుల రకాలు

ప్రతిరూపం :-

ఆన్‌లైన్‌లో వేరొకరిలా నటిస్తూ,

బెదిరిస్తూ ఇబ్బందుల్లో పడేయడం.

సైబర్ స్టాకింగ్

తరచుగా సందేశాలను

పంపిస్తూ భయపెట్టడం

మినహాయింపు :-

ఉద్దేశ్యపూర్వకంగా ఆన్‌లైన్ గ్రూపు నుండి

(వాట్సప్) ఒకరిని మినహాయించడం

(తీసివేయడం).

వేదింపు :-

పదేపదే అప్రియమైన మాటలు,

మొరటుగా మరియు అవమానకర

సందేశాలు పంపడం.

పుకార్లు :-

ఆన్‌లైన్‌లో ఒక వ్యక్తికి లేదా అతని

ప్రతిష్టకు లేదా అతని స్నేహానికి

హాని కలిగించేలా చెడు పుకార్లు

ప్రచారం చేయడం.

ఫ్లేమింగ్ :-

కోపంతో, అసహ్యంతో ఎలక్ట్రానిక్

సందేశాలను ఉపయోగించి

ఆన్‌లైన్‌లో పోరాటాలు చేయడం

రహస్యాలు బయల్పరచడం :-

ఒకరి రహస్య లేదా ఇబ్బందికరమైన

సమాచారాన్ని ఆన్‌లైన్‌లో బయట పెట్టడం.

అందంగా లేవు,

ఓడిపోయావు, వైఫల్యం, స్వార్థపరుడు,

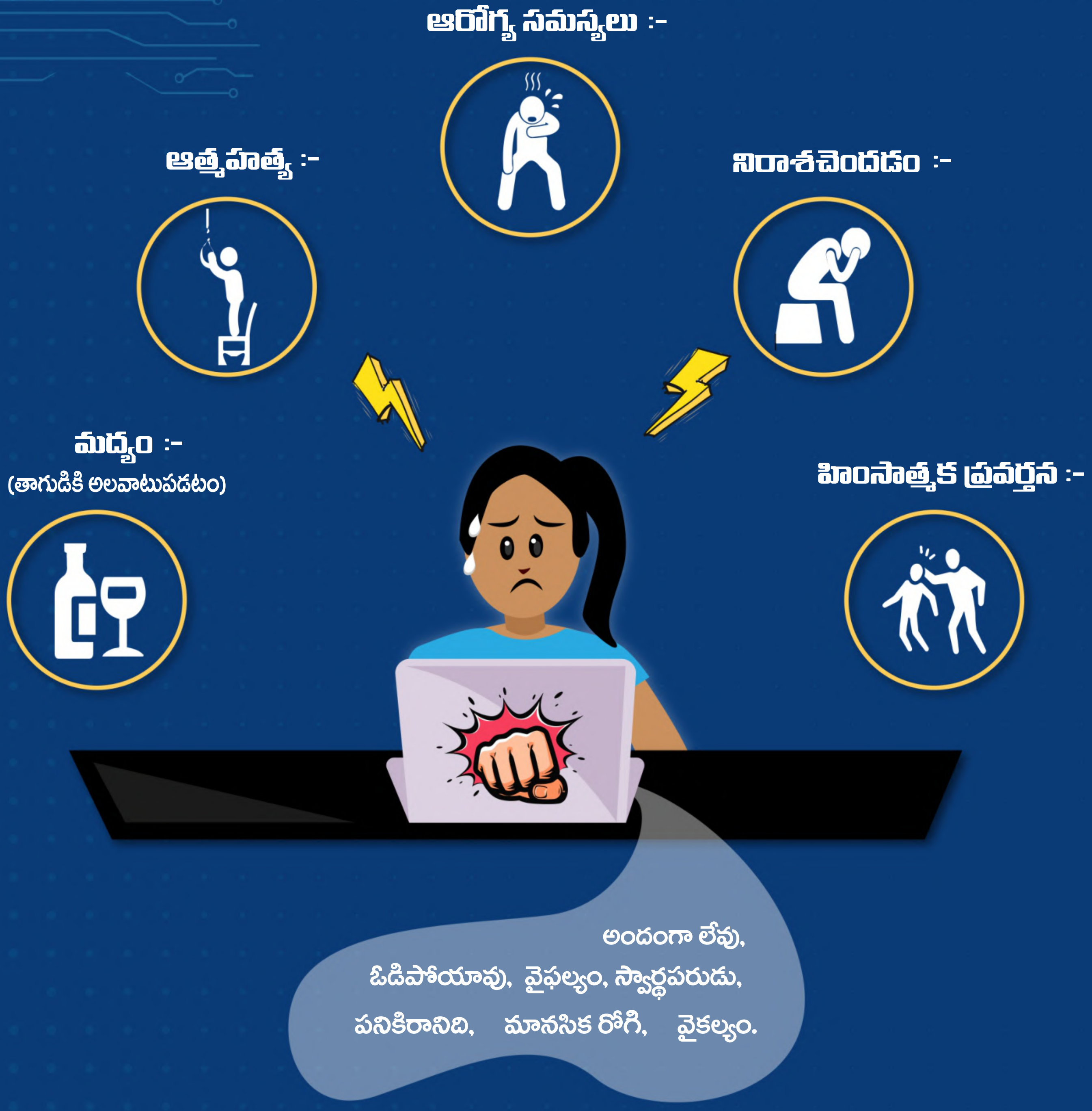
పనికిరానిది, మానసిక రోగి, వైకల్యం.

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

సైబర్ బెదిరింపుల దుష్ప్రభావాలు

సైబర్ బెదిరింపుల వల్ల ఎదురయ్యే దుష్పరిణామాలు



సాధారణ సైబర్ బెదిరింపులు, మోసాలు

సైబర్ బెదిరింపులు, మోసాల నుండి రక్షించుకోవడానికి కొన్ని సాధారణ పద్ధతులు.

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

రాన్‌సంవేర్ :-

వినియోగదారుని లాక్ చేసే మెలవెలెంట్ (కపటంతో కూడిన) సాఫ్ట్‌వేర్ ఉపయోగించి డేటాను దాచి జాగ్రత్త చేయండి. క్రిప్టో వైరాలజీ దోపిడీ చేస్తున్నప్పుడు బాధితుడి నుండి చెల్లింపు ఫైళ్ళను డిక్రిప్ట్ చేసి పునరుద్ధరించండి.

మాల్వేర్ :-

హానికరమైన సాఫ్ట్‌వేర్ యంత్రంలో ఇన్‌స్టాల్ చేస్తే థర్డ్‌పార్టీ కోసం మనకు తెలియకుండానే నేరపూరిత చర్యలను చేస్తుంది.

బోట్‌నెట్స్ :-

నేర ప్రయోజనాలకోసం దాడి చేసేవాడు పరికరాలకు ప్రవేశాన్ని అందించే 'రహస్య కీ' మరియు కనెక్షన్లు నియంత్రిస్తాడు.

స్పూఫింగ్ :-

మోసపూరిత ఖాతా నుండి చట్టబద్ధమైనదిగా పంపిన ఈమెయిల్ సందేశాలు మరియు విశ్వసనీయమైన మూలం వినియోగదారు వ్యవస్థకు లాభం చేకూర్చే ప్రయత్నం.

వార్మ్ :-

ఇది స్వతంత్ర సాఫ్ట్‌వేర్ ప్రోగ్రామ్, అవసరం లేకుండా సిస్టమ్, నెట్‌వర్క్‌లోకి చొరబడి విస్తరిస్తూ, డూప్లికేట్స్ సృష్టించుకుంటూ డేటాను మరియు ఇతర సాఫ్ట్‌వేర్‌లను నాశనం చేస్తుంది.

ట్రోజన్స్ :-

విధ్వంసకతను కలిగివున్న కంప్యూటర్ ప్రోగ్రామ్ హాని చేయని ప్రోగ్రామింగ్‌వలె మారువేషంలో దాగిఉన్న కోడ్.

డెనియల్ ఆఫ్ సర్వీస్ :- (డిడిఓఎస్)

వరదలా వెల్లువెత్తే బ్యాండ్‌విడ్త్ అటాక్స్ ద్వారా ఆన్‌లైన్ సిస్టమ్స్ అందుబాటులో లేకుండా చేయడం.

వైరస్ :-

ఒకరకమైన మాల్వేర్ కంప్యూటర్ నుండి దాని ప్రోగ్రామింగ్‌ను ప్రతిబింబించడం ద్వారా మరియు వినియోగదారు ప్రోగ్రామ్‌లు మరియు ఫైళ్ళకు సంక్రమించడం ద్వారా అవి పనిచేసే విధానాన్ని మార్చడానికి లేదా పూర్తిగా పనిచేయడం మానేయడం ద్వారా వ్యాపిస్తుంది.

ఫిష్షింగ్ :-

DNS సర్వర్ సాఫ్ట్‌వేర్ దుర్బలత్వం బహిర్గతమవుతుంది లేదా హోస్ట్‌ఫైల్ మార్చుకోబడుతుంది మరియు చట్టబద్ధమైన వెబ్‌సైట్ హానికరంగా స్కామ్‌సైట్‌కు మళ్ళించబడుతుంది. అక్కడ తెలియని సందర్శకులు వారి రహస్య సమాచారాన్ని నమోదు చేస్తారు.

స్పైవేర్ :-

వినియోగదారు కార్యకలాపాలను రహస్యంగా పర్యవేక్షించడానికి ఉపయోగించే హార్డ్‌డ్రైవ్‌లోని క్రిమినల్ మాల్వేర్.

ఫార్మింగ్ :-

DNS సర్వర్ సాఫ్ట్‌వేర్ దుర్బలత్వం బహిర్గతమవుతుంది. లేదా హోస్ట్‌ఫైల్ మార్చుకోబడి చట్టబద్ధమైన వెబ్‌సైట్ హానికరంగా స్కామ్‌సైట్‌కు మళ్ళిస్తుంది. ఇక్కడ తెలియని వారు వారి రహస్య సమాచారానికి ప్రవేశించవచ్చు.

యాడ్‌వేర్ :-

శోధన అభ్యర్థనలను మళ్ళించగల లేదా కొన్నింటిని స్వయంచాలకంగా అందిస్తుంది. దాని సృష్టికర్తకు ఆదాయాన్నిచ్చే ప్రక్రియ.

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

ఫిషింగ్ దాడి హెచ్చరికలు

సైబర్ నేరగాళ్ల నుండి నిన్ను నీవు రక్షించుకునే విధానాలు

ముఖ్యమైన 5 సంకేతాలు :-

వెబ్‌లింక్‌లు తెలియని వెబ్‌సైట్‌లకు దారితీస్తాయి. (వెబ్‌సైట్ URL ను జాగ్రత్తగా గమనించాలి).

ఊహించని అదనపు సమాచారాలు వస్తూ ఉంటాయి (ఈమెయిల్, సందేశాల ద్వారా).

పేలవమైన వ్యాకరణాన్ని మరియు పదాల అచ్చు తప్పులను గమనించాలి.

వ్యక్తిగత సమాచారాన్ని అడుగుతారు (పాస్‌వర్డ్, OTP సమాచారం మొ॥) వ్యక్తిగతంగా మీ పేరు ప్రస్తావించకుండా పంపే సందేశాలు.

వ్యక్తిగతంగా మీ పేరు ప్రస్తావించకుండా పంపే సందేశాలు.

రక్షించుకునే విధానాలు

1. మీరు ధృవీకరించలేని వెబ్‌లింక్‌లు లేదా ఏదైనా అదనపు సమాచారాన్ని తెరవవద్దు.

2. సమాచారాన్ని ధృవీకరించుకోవడానికి అవతలి వ్యక్తికి కాల్ చేయండి (మీకు తెలిసిన వారి నుండి వచ్చినా).

3. సందేహం వచ్చినప్పుడు, ఎల్లప్పుడూ సహాయం కోసం సరైన వారిని సంప్రదించండి.

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

బ్లూలైట్ ఎక్స్‌పోజర్ (చూడటం) ద్వారా మీ మెదడు మరియు శరీరంపై ఎలాంటి ప్రభావం చూపుతుంది

మెలటోనిన్‌కు అంతరాయం కలిగించడం ద్వారా స్మార్ట్‌ఫోన్ లైట్ నిద్రను నాశనం చేస్తుంది. అన్నిరకాల ఆరోగ్య సమస్యలకు దారితీస్తుంది.

మీ నిద్రకు అంతరాయం, మిమ్మల్ని పరధ్యానంలో ఉంచవచ్చు మరియు మరుసటి రోజు మీ జ్ఞాపకశక్తిని కూడా బలహీనపరుస్తుంది.

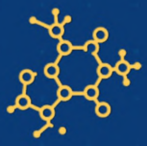
బ్లూలైట్ మనల్ని దెబ్బతీస్తుందని కొన్ని ఆధారాలు ఉన్నాయి. కాలక్రమేణా రెటీనాకు హాని కలుగుతుంది. దీని మీద ఇంకా పరిశోదనలు చేయవలసి ఉంది.

రాత్రిపూట స్మార్ట్‌ఫోన్ లైట్‌వల్ల నిద్రలేకపోవడంతో నేర్చుకోవడం కష్టమవుతుంది.

బ్లూలైట్ కంటి శుక్లానికి దారితీస్తుందా లేదా అనే దానిపై పరిశోధనలు, దర్యాప్తు చేస్తున్నారు.

దీర్ఘకాలికంగా తగినంత నిద్ర రాకపోవడం న్యూరోటాక్సిన్ నిర్మాణానికి దారితీస్తుంది. ఇది మీకు మంచి నిద్రరాకుండా చేస్తుంది.

రాత్రిపూట వచ్చే కాంతి మరియు దానితో వచ్చే చెదిరిన నిద్రవలన రొమ్ము మరియు ప్రోస్టేట్ క్యాన్సర్లు వచ్చే ప్రమాదం ఎక్కువగా ఉంది.



కాంతి బహిర్గతం ద్వారా మెలటోనిన్ స్థాయిలు తగ్గడం ద్వారా వ్యక్తులలో డిప్రెషన్ పెరిగే అవకాశం ఉంది.

మెలటోనిన్ మరియు నిద్రకు అంతరాయం కలిగించడం ద్వారా స్మార్ట్‌ఫోన్ లైట్ ఆకలిని నియంత్రించగల హార్మోన్లను గందరగోళానికి గురిచేస్తుంది మరియు ఊబకాయం వచ్చే ప్రమాదాన్ని పెంచుతుంది.

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

నకిలీ వార్తల వ్యాప్తికోసం ప్రజలు సామానిక మాధ్యమాన్ని, సందేశాల్ని
మరియు అంతర్జాలాన్ని దుర్వినియోగం చేస్తున్నారు.

నకిలీ వార్తలు

మీరు నకిలీ వార్తలు కనిపెట్టుటకు మార్గాలు :-

- మూలాలు మరియు URL ను తనిఖీ చేయండి.
- ముందు శీర్షిక (హెడ్‌లైన్)ను చదవండి.
- తేదీని తనిఖీ చేయండి.
- అసాధారణ వ్రాతలపై దృష్టిపెట్టండి.
- వాస్తవాలను తనిఖీచేసే సైట్‌లను చూడండి. ఉదాహరణకు (www.factly.in)
- ఒకవేళ ఇది వేళాకోళమా, కాదా అని తనిఖీ చేయండి.
- మీ అభిప్రాయాన్ని చెప్పేముందు ఒకసారి తనిఖీ చేయండి.
- వచ్చిన ఎటువంటి బొమ్మలైనా సరే గూగుల్ ఇమేజెస్‌లో తనిఖీ చేయండి.

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

నకిలీ వార్తలు

సోషల్ మీడియా మరియు ఇంటర్నెట్‌లో నకిలీ వార్తలను కనుగొనడం

మూలాన్ని పరిగణించటం

నమ్మదగినదా లేదా బాగా తెలిసినదా అని పేరున్న న్యూస్ ఛానెల్ లేదా ఆన్‌లైన్ న్యూస్ వెబ్‌సైట్ నుండి వచ్చిన మూలాన్ని పరిగణించండి.

URL తనిఖీ చేయండి

.IO, CO. Com తో ముగిసే ఇలాంటి సైట్‌లను చాలా మంది ఉపయోగిస్తున్నారు. ఇది చట్టబద్ధమైనదిగా అనిపిస్తుందా? వెబ్‌సైట్ విశ్వసనీయమైనదిగా ట్రాక్ రికార్డ్ ఉందా అని గమనించాలి.

రచయిత ఎవరు?

ఈ రచయిత నమ్మదగిన వారా, గౌరవించదగిన వారా అని ఆన్‌లైన్‌లో శోధించాలి. చాలా నకిలీ సైట్లు రచయిత పేరును ఉపయోగించవు.

రెండవ అభిప్రాయాన్ని పొందండి

ఒక కథ మిమ్మల్ని చాలా కోపంగా మరియు లోతుగా ఆలోచింపజేస్తే, ఫార్వర్డ్ చేయడానికి ముందు తెలిసిన వారిని సంప్రదించండి లేదా డీబంకింగ్ సైట్‌లను ఉపయోగించండి

మీ పక్షపాతాన్ని విస్మరించండి

మీ అంతర్గత అభిప్రాయాలను తెలియజేసే కథలను నమ్మడం సులభం కాని మీరు తరువాత సామాజిక మాధ్యమాల్లో చూసినపుడు మీ రాజకీయ జాతి లేదా మతపరమైన అభిప్రాయాలను కలిగి ఉన్న పోస్టులను చూస్తారు.

శీర్షికను మించి చదవండి

వార్తలను విమర్శనాత్మకంగా అధ్యయనం చేయండి. స్వరం యొక్క దృక్కోణాన్ని గుర్తించండి. అప్పుడే వ్యాసం యొక్క సమతుల్య, సరసమైన మరియు లక్ష్యం కనిపిస్తుంది.

https://linktr.ee/endnowfoundation

ADVOCACY ON DIGITAL SAFETY

నకిలీ వార్తలను గుర్తించడం

తప్పుడు సమాచారం మరియు నిర్వహణ యొక్క 9 రకాలు

తప్పుడు కనెక్షన్

ముఖ్యాంశాలు, విజువల్స్ లేదా శీర్షికలు కంటెంటుకు మద్దతు ఇవ్వనప్పుడు.

తప్పుడు సందర్భం

నిజమైన కంటెంట్ తప్పుడు సందర్భోచిత సమాచారంతో పంచుకున్నప్పుడు.

విషయాన్ని మార్చడం

కొన్ని నిజమైన సమాచారం లేదా చిత్రాలను మోసగించడానికి తారుమారు చేసినప్పుడు.

వ్యంగ్యం లేదా అనుకరణ

ముఖ్యాంశాలు, విజువల్స్ లేదా శీర్షికలు కంటెంటుకు మద్దతు ఇవ్వనప్పుడు.

తప్పుదారి పట్టించే విషయం

సమస్యను లేదా వ్యక్తిని ఫ్రేమ్ చేయడానికి సమాచారాన్ని ఉపయోగించడాన్ని తప్పదారి పట్టించడం.

మోసపూరిత విషయం

నిజమైన విషయాలకు ప్రతిరూపం చేసినపుడు.

కల్పించిన విషయం

100శాతం తప్పుడు విషయం మోసగించడానికి మరియు హాని చేయడానికి రూపొందించబడింది.

ప్రచారం

వైఖరులు, విలువలు మరియు జ్ఞానాన్ని నిర్వహించడానికి విషయాన్ని ఉపయోగించినప్పుడు

ప్రాయోజిత విషయం

ప్రకటన లేదా ప్రజా సంబంధాల విషయాలను మరోరూపంలో సంపాదకీయంలా ప్రదర్శించడం

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

ఛాయాచిత్ర ధృవీకరణలో నకిలీవార్తలను గుర్తించడం

అసలు విషయాన్ని మరియు మూలాన్ని గుర్తించండి మరియు ధృవీకరించండి (దీనిలో స్థానం, తేది మరియు సుమారు సమయం ఉంటుంది).

కెమెరా మోడల్ / టైమ్‌స్టాంప్ సమాచారం కోసం ఎల్లప్పుడూ ఫోటో ఫోరెన్సిక్స్ / ఫైండెక్సిఫ్ వంటి సాధనాలను ఉపయోగించండి.

బహుళ వనరులను ప్రయత్నించండి నిజాయితీని నిరూపించడానికి అసలు మూలాన్ని సవాలు చేయండి. తదుపరి ప్రశ్నలను అడగండి.

వోల్ఫ్రామ్ ఆల్ఫాను ఉపయోగించి ఫోటోను తీసిన వాతావరణం (ఉదా :- ఎండ, వర్షం, మేఘావృతం) వాస్తవానికి ఆ ప్రాంత వాతావరణం కాదా అని తనిఖీ చేయండి.

టిన్ ఐ (www.TinEye.com) లేదా గూగుల్ ఇమేజ్ సెర్చ్ (www.images.google.com) వంటి సాధనాలను ఎల్లప్పుడు వాడండి.

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

వీడియో ధృవీకరణలో నకిలీ వార్తలను గుర్తించడం

అసలు విషయాన్ని మరియు మూలాన్ని గుర్తించండి మరియు ధృవీకరించండి (దీనిలో స్థానం, తేది మరియు సుమారు సమయం ఉంటుంది).

బహుళ వనరులను ప్రయత్నించండి. నిజాయితీని నిరూపించడానికి అసలు మూలాన్ని సవాలు చేయండి తదుపరి ప్రశ్నలను అడగండి.

ఆమ్నెస్టీ ఇంటర్నేషనల్ యొక్క డేటా వ్యూయర్‌ను ఉపయోగించండి.

అప్‌లోడ్ పేరు మరియు అప్‌లోడ్ చేసిన తేదీని పరిశీలించండి.

సాంఘిక మాధ్యమాలు వాటి సంబంధిత ఖాతాల అప్లోడర్ యొక్క స్థానం, కార్యాచరణ, విశ్వసనీయత, పక్షపాతం లేదా ఎజెండాను సూచిస్తాయి.

ఈ ఖాతాలు ఎంతకాలం చురుకుగా ఉన్నాయి? వారు ఎంత చురుకుగా ఉన్నారు?

వ్యక్తి ఆన్‌లైన్ డేటాబేస్ లేదా నెట్‌వర్కింగ్ ప్లాట్‌ఫాంలో జాబితా చేయబడ్డారా?

సామాజిక మాధ్యమాలు, బ్లాగ్ లేదా వెబ్‌సైట్‌తో సహా ఇతర ఖాతాలు అప్‌లోడ్‌లో అనుబంధంగా ఉన్నాయా?

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

ఇంటి నుండి పని చేయడం కోసం
10 భద్రతా చిట్కాలు

అన్ని భద్రతా జాగ్రత్తలు ఉన్న మీ కార్యాలయ పరికరాన్ని ఉపయోగించండి.

అన్ని ఖాతా మరియు పరికరాల కోసం ఎల్లప్పుడూ OTP మరియు కఠినమైన పాస్‌వర్డ్‌లను ఉపయోగించండి.

సురక్షితమైన కనెక్షన్ ద్వారా డేటాను వాడడానికి VPN ను ఉపయోగించండి.

సున్నితమైన డేటాను కోల్పోకుండా ఉండటానికి డేటా లాస్ ప్రివెన్షన్ (DLP) సాధనాలను ఎల్లప్పుడూ వాడడం ప్రారంభించండి,

మాల్వేర్ దాడుల నుండి రక్షించడానికి ఆపరేటింగ్ సిస్టమ్ మరియు యాంటీ వైరస్‌లను క్రమం తప్పకుండా నవీకరించండి.

కోవిడ్-19 మోసాలు, ఫిషింగ్ ఈమెయిల్స్, హానికరమైన డొమైన్లు మరియు నకిలీ అనువర్తనాల గురించి తెలుసుకోండి.

సురక్షితంగా లేనటువంటి, ఉచిత, పబ్లిక్ వైఫై లేదా మరి ఏ ఇతర నెట్‌వర్క్‌ను ఉపయోగించడం మానుకోండి

ధృవీకరించబడిన మరియు ప్రామాణికమైన ? మాత్రమే వాడబడ్డాయని నిర్ధారించుకోండి.

మీ సిస్టమ్ మరియు క్లౌడ్‌లోని డేటాను తరచుగా బ్యాకప్ చేసుకోండి (వన్ డ్రైవ్, జి డ్రైవ్ మొదలైనవి)

ఖాళీ పోర్ట్‌లు మరియు సిస్టమ్ బ్లూటూత్ కనెక్టివిటీని నిలిపివేయండి.

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

అంతర్జాల ఉద్యోగ కుంభకోణాలు

ప్రతిరోజూ వేలాది మంది అంతర్జాల ఉద్యోగ కుంభకోణాలతో
మోసపోతున్నారు... మీరు కూడా చిక్కుకోకండి

ఈ అంతర్జాల ఉద్యోగ కుంభకోణాల నుండి కాపాడుకొనుటకు మార్గాలు

మీరు తక్షణమే ఎంపిక చేయబడ్డారు అని వస్తే నమ్మవద్దు.

అస్పష్టమైన ఉద్యోగ అవసరం మరియు ఉద్యోగ వివరణ ఉన్నట్లయితే.

అస్పష్టమైన ఈమెయిల్ వ్రాయబడితే.

సంప్రదింపు సమాచారం లేకుండా లేదా సంస్థ యొక్క సంకేతం లేకుండా ఈమెయిల్ వ్రాయబడితే.

తక్షణ సందేశ వేదిక (వాట్సప్)పై ఇంటర్వ్యూ ఏర్పాటు చేయబడితే.

సంస్థ లేదా పని గురించిన సమాచారం శోధన ఫలితాల్లో కనిపించకుంటే.

మీ యొక్క రహస్య సమాచారాన్ని అందించమని మిమ్మల్ని అడిగితే.

మిమ్మల్ని ఎటువంటి డబ్బు పంపమని అడిగినా.

https://linktr.ee/endnowfoundation

మోసపోకండి

మోసాన్ని నివారించడానికి కొన్ని మార్గాలు

DO NOT

ముందుగానే చెల్లించవద్దు.

చెల్లింపు అభ్యర్థనలను ఆమోదించే ముందు ఒకసారి తనిఖీ చేసుకోండి.

వ్యక్తిగత వివరాలు, పిన్ నంబర్, OTP, ఖాతా సంఖ్యలు మొదలైనవి ఇతరులతో పంచుకోవద్దు.

అనుమానాస్పద ఖాతాలుంటే వెంటనే స్పందించి నివేదించండి.

చరవాణితో మాట్లాడుతూ ఉన్నప్పుడు ఎటువంటి డబ్బుతోకూడిన లావాదేవీలు జరపవద్దు.

జాగ్రత్త : అంతర్జాల వేదికల ద్వారా చెల్లింపులు దృఢంగా ఉంటాయి. కాని 99 శాతం చెల్లింపులు ఫిషింగ్ మరియు సోషల్ ఇంజనీరింగ్ నేరాలకు లోనయ్యే అవకాశం ఉంది.

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

డెబిట్ / క్రెడిట్ కార్డు మోసం

డెబిట లేదా క్రెడిట్ కార్డు మోసాలను నివారించడానికి కొన్ని మార్గాలు

ఎల్లప్పుడు మీ కార్డు మరియు కార్డు వివరాలను సురక్షితంగా ఉంచుకోండి.

లావాదేవీలు చేసేటప్పుడు మీ కార్డుపై మీ దృష్టి సారించి ఉంచండి.

మీ కార్డు ద్వారా డెబిట్ చేసిన మొత్తాన్ని నిర్ధారించుకుని చిల్లర వ్యాపారులను అడగండి.

క్రొత్త కార్డులు మీకు చేరిన వెంటనే సంతకం చేయండి.

మీ రసీదులను ఆన్‌లైన్ స్టేట్‌మెంట్లతో పోల్చి చూసుకోండి.

కార్డు నుండి జరిపిన ఆర్థిక లావాదేవీల రసీదులను, సమాచారాన్ని జాగ్రత్తగా చించి పడేయండి.

మీ కార్డులను బహిరంగ ప్రదేశాలలో ఉంచవద్దు. వ్యక్తిగత వస్తువులను ఎప్పుడైనా మీ వద్దనే ఉంచుకోండి.

మీ పిన్ నెంబర్‌ను ఎవ్వరి ముందు ఎప్పుడై న రాయకండి మరియు ఎవరికీ చెప్పకండి.

ఆన్‌లైన్ లావాదేవీలు చేస్తున్నప్పుడు మీరు యాంటివైరస్ సాఫ్ట్‌వేర్ మరియు ఆపరేటింగ్ సిస్టిమ్‌ను నవీకరించారని నిర్ధారించుకోండి.

నమ్మదగిన మూలాల (Source) నుండి మాత్రమే కొనుగోలు చేయండి. అంతర్జాల కొనుగోళ్ళ కోసం 3D సురక్షిత పద్ధతులను (ప్రోటోకాల్) ఉపయోగించండి.

భర్తీ (రిప్లేస్‌మెంట్) కార్డు వచ్చినప్పుడు, గడవు ముగిసిన / ఉపయోగించని/ నిరోధించబడిన కార్డును ముక్కలు ముక్కలుగా కత్తిరించండి. అయస్కాంత గీత లేదా మైక్రోచిప్‌ను కూడ విచ్ఛిన్నం చేయండి.

ద్రవ్య యంత్రాలు (ఏటిఎం)

మీ చుట్టూ ఉన్న ఇతరుల పట్ల ఎల్లప్పుడూ జాగ్రత్త వహించండి.

మీ కార్డు మోసానికి గురి అవుతున్నట్లు సంకేతాలు ఉంటే మీ ఎటిఎం ఉపయోగించవద్దు.

ATM

ఎటిఎం నుండి మీ కార్డు తిరిగి రాకపోతే మీ బ్యాంకుకు వెంటనే తెలియజేయండి.

మీ పిన్ నంబర్‌ను జాగ్రత్తగా కాపాడుకోండి.

చెల్లింపు టెర్మినల్స్ (పిఓఎస్)

చిల్లర దుకాణాలలో ముఖ్యంగా మద్యం దుకాణాలు, ఆహార దుకాణాలు, పార్కింగ్ టికెట్ యంత్రాలు మరియు పెట్రోలు నింపే స్థలాల వద్ద కార్డు మోసానికి (Skimming) గురి అవుతుంది. కాబట్టి జాగ్రత్త వహించండి.

కార్డుతో చెల్లింపు జరుపు సమయంలో కార్డుపై మీ దృష్టి సారించి ఉంచండి. (మరియు కార్డును తాకండి).

మీ కార్డు మీకు ఎప్పుడూ కనిపించేలా లావాదేవీలు జరపండి.

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

KYC కుంభకోణం (స్కామ్) జరుగు విధానం

1. మీ వాలెట్ లేదా బ్యాంక్ KYC చెల్లదని మీకు కాల్ వస్తుంది.

2. మీ ఆన్‌లైన్ ఖాతాను తిరిగి పనిచేసేలా సరిచేయవచ్చు అని కాల్ చేసిన వ్యక్తి చెప్తారు.

3. మిమ్మల్ని ఒక అనువర్తనాన్ని (App) డౌన్‌లోడ్ చేయమని చెప్తూ ఎలా చేయాలో దశల వారిగా మార్గనిర్దేశం చేస్తారు.

4. మీరు ఆ అనువర్తనాన్ని (యాప్‌ను) ఉపయోగించినప్పుడు ఆ ఫోన్ చేసినవారు మీ చరవాణి తెరను (స్క్రీన్) చూడగలుగుతారు.

5. అతను మీ వాలెట్‌కు కొద్ది మొత్తాన్ని బదిలీ చేయమని అడుగుతాడు.

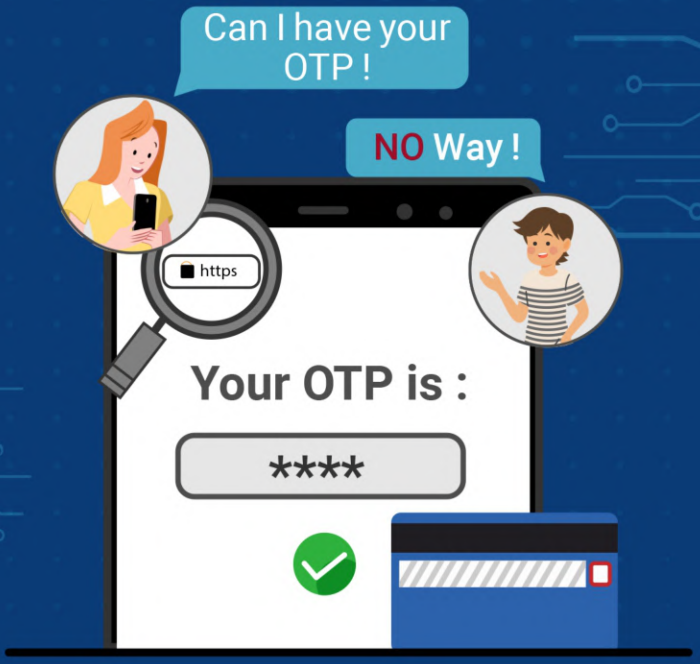
6. మీరు బదిలీ లావాదేవీలు చేసేటప్పుడు, అతడు మీ పాస్‌వర్డ్ మరియు ఇతర వివరాలు చూస్తాడు.

7. అతను మీ పాస్‌వర్డ్ మరియు ఇతర వివరాలను ఉపయోగించి మీ బ్యాంకు నుండి పెద్దమొత్తాన్ని బదిలీ చేస్తాడు.

8. బాధితుడు (మీరు) అన్ని నగదు బదిలీల కోసం OTP ని అందుకుంటారు. కాని ఈ అనువర్తనం (యాప్) ద్వారా మోసగాడు వాటిని చూడగలడు.

9. ఈ అనువర్తనం (App) ద్వారా మోసగాళ్ళు మీ బ్యాంక్ ఖాతాను నిమిషాల్లో ఖాళీ చేస్తారు.

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY



OTP (వన్‌టైమ్ పాస్‌వర్డ్) ను రక్షించుకోండి

మీ బ్యాంకు ఖాతా నుండి డబ్బును దొంగిలించడానికి మీ వన్‌టైమ్ పాస్‌వర్డ్ ఉపయోగించవచ్చు. మీరు ఇబ్బంది పడకుండా ఉండాలంటే OTP ని ఎవరితో పంచుకోవద్దు.

- మీ కు బ్యాంకు ద్వారా వచ్చిన వన్‌టైమ్ పాస్‌వర్డ్ (OTP) ని ఎవరితోనూ పంచుకోవద్దు.
- మీ ఎటిఎం (ATM) పిన్‌ను తరచుగా మారుస్తూ ఉండండి.
- మీ కార్డు వెనక ఉండే మూడు అంకెల సంఖ్య (CVV) ను ఎవరితోనూ పంచుకోవద్దు.
- సురక్షితమైన ఆన్‌లైన్ కోసం (http://) తనిఖీ చేయండి మరియు లాక్ గుర్తును చూసి లావాదేవీలు చేయండి.
- మీ యొక్క డెబిట్ / క్రెడిట్ కార్డు వివరాలను ఈ-కామర్స్ వెబ్‌సైట్‌లో ఎప్పుడు సేవ్ చేయవద్దు.

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

మీరు మీ పిన్ (PIN) ఎంటర్ చేసేముందు ఆలోచించండి

వీటికి "NO" చెప్పండి

- ముందస్తు చెల్లింపులు.
- వ్యక్తిగత వివరాలను, పిన్ నెంబర్, OTP, ఖాతా సంఖ్య మొదలైనవి ఇతరులతో పంచుకోవడం.
- చరవాణిలో మాట్లాడుతూ ఉన్నప్పుడు ద్రవ్యలావాదేవీలు జరపడం.

క్రింద పేర్కొన్న యాప్‌లలో UPI పేమెంట్ పొందేప్పుడు PIN ఎంటర్ చేయాల్సిన అవసరం లేదు

Paytm | PhonePe | G Pay

జాగ్రత్త : అంతర్జాల వేదికలద్వారా చెల్లింపులు ఖచ్చితమైనవై ఉంటాయి.

కాని 99శాతం చెల్లింపులు ఫిషింగ్ మరియు సోషల్ ఇంజనీరింగ్ నేరాలకు లోనయ్యే అవకాశం ఉంది.

https://linktr.ee/endnowfoundation

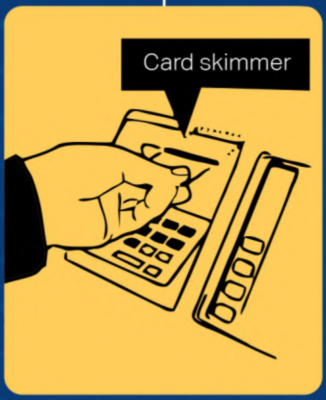
ENDNOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

కార్డు స్కిమ్మింగ్ (SKIMMING) ఎలా జరుగుతుంది.

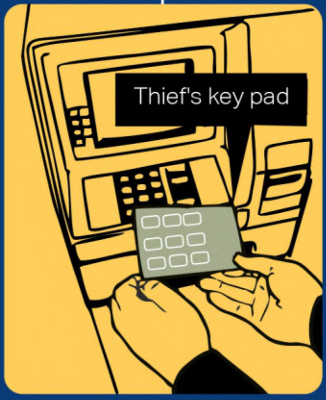
ATM ల నుండి బ్యాంకు సమాచారాన్ని దొంగిలించే మార్గాలు ఇక్కడ ఉన్నాయి.

మొసగాళ్ళు మొత్తం పరికరాన్ని మారుస్తారు.

మొసగాళ్ళు స్కిమ్మర్ ను ఇన్‌స్టాల్ చేస్తారు.



మొసగాళ్ళు కొత్త కీపాడ్‌ను ఇన్‌స్టాల్ చేస్తారు.



మొసగాళ్ళు కెమెరాను ఇన్‌స్టాల్ చేస్తారు.

ఈ మోసగాళ్ళ బారినుండి మిమ్మల్ని మీరు రక్షించుకునే మార్గాలు

- గ్యాస్ స్టేషన్లు, పెట్రోలు బంకులు మరియు దుకాణాల కంటే బ్యాంకుల వద్ద ATM లు సురక్షితంగా ఉండవచ్చు.
- మీ కార్డును స్లాట్ నుండి తీసేటప్పుడు దాన్ని కదిలించండి. దాని వలన స్కిమ్మర్‌ను కూడా తీసివేయవచ్చు.
- మీరు మీ పిన్‌ను నమోదు చేస్తున్నప్పుడు 'కీ'ప్యాడ్‌ను మీ మరో చేతితో కవర్ చేయండి.
- అనువర్తనాలు (యాప్‌లు) మారినట్లయితే ATM లేదా చెల్లింపు యంత్రాన్ని ఉపయోగించవద్దు.
- ATM ఉపయోగించడంలో సమస్య ఉంటే, అపరిచితుల సహాయాన్ని అంగీకరించవద్దు.
- మీ బ్యాంక్ స్టేట్‌మెంట్‌లను క్రమం తప్పకుండా తనిఖీ చేస్తూ, అనుమానాస్పద నగదు బదిలీలు ఏవైనా జరిగాయేమో తెలుసుకోండి.

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

స్విమ్ స్వాప్ మోసం అంటే ఏమిటి?

స్టెప్ - 1

మోసగాళ్ళు ఫిషింగ్, విషింగ్, స్మిషింగ్ లేదా మరే ఇతర మార్గాల ద్వారా కస్టమర్ యొక్క వ్యక్తిగత సమాచారాన్ని సేకరిస్తారు.

స్టెప్ - 3

వారు మొబైల్ ఆపరేటర్‌ను సంప్రదించి సిమ్ పనిచేయకుండా నిరోధించడానికి అసలైన కస్టమర్‌గా ఐడి ప్రూఫ్ సేకరించి మొబైల్ ఆపరేట్ యొక్క రిటైల్ అవుట్‌లెట్లను సందర్శిస్తారు.

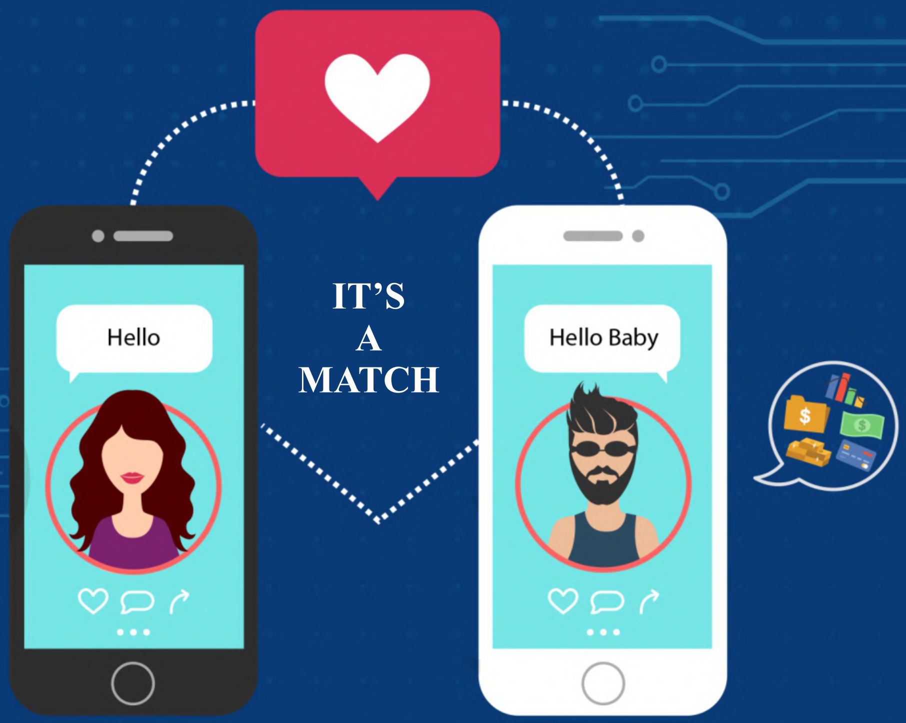
స్టెప్ - 2

మోసగాడు కొత్తగా పొందిన సిమ్‌కార్డు ద్వారా వన్‌టైమ్ పాస్‌వర్డ్ (OTP) ను ఉత్పత్తి చేసి ఆ OTP ద్వారా దొంగిలించబడిన బ్యాంకింగ్ సమాచారాన్ని ఉపయోగించి లావాదీవేలు చేస్తాడు.

స్టెప్ - 4

మొబైల్ ఆపరేటర్ ప్రస్తుతం ఉన్న సిమ్ కార్డును పనిచేయకుండా కొత్త సిమ్ కార్డును తెలియకుండా మోసగాడికి ఇస్తాడు.

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY



అంతర్జాలంలో 'ప్రేమ' పేరుతో మోసానికి గురికాకుండా ఉండండి

- అంతర్జాల ఖాతాదారుల నిజాయితీని ధృవీకరించకుండా అంతర్జాల చాటింగ్/డేటింగ్‌కు మానసికంగా సంసిద్ధులు కాకూడదు.
- అంతర్జాల అపరిచితుడు / సామాజిక మాధ్యమ స్నేహితులకు డబ్బు లేదా మీ వివరాలను ఎప్పుడూ పంపవద్దు.
- అంతర్జాల స్నేహితుడు కొన్ని పరిచయాలు లేదా సంభాషణల వెనువెంటనే డేటింగ్ వెబ్‌సైట్ / ప్లాట్‌ఫాంలలో కాకుండా వేరే వెబ్‌సైట్‌లలో, చాటింగ్‌లలో కలవమని అడుగుతాడు.

- మీ అంతర్జాల అభిమాని ఎవరు అని నిర్ణయించడంలో సహాయపడటానికి www.tineye.com లేదా https://images.google.com తో ఇమేజ్‌ని చెక్ చేయండి.
- సన్నిహిత లేదా వ్యక్తిగత చిత్రాలు లేదా వీడియోలను అంతర్జాలంలో భాగస్వామ్యం చేయకూడదు. ఇతరులు చూడకూడదు అనుకునే మీ గత భాగస్వామ్య చిత్రాలు లేదా వీడియోలను ఉపయోగించి స్కామర్లు మిమ్మల్ని బెదిరించి వారి లక్ష్యాలను చేరుకునేందుకు ప్రయత్నిస్తారు.

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

మ్యాట్రిమోనియల్ మోసాల నివారణ

అంతర్జాల పెళ్ళిసంబంధాల మోసానికి గురికాకుండా

మిమ్మల్ని మీరు ఎలా కాపాడుకోవాలి :

- పూర్తి వివరాలు తనిఖీ చేయండి.
- వివాహ పోర్టల్‌లో ఎల్లప్పుడూ ధృవీకరించబడిన సరియైన వివరాలకోసం మాత్రమే చూడండి.
- ఎవరికీ రుసుము ఇవ్వకండి.
- మీ పోర్టల్ ఖాతా సమాచారాన్ని ఎప్పుడూ బహిర్గతం (పబ్లిక్) చేయవద్దు.
- వ్యక్తిగతంగా కలిసేటప్పుడు అప్రమత్తంగా ఉండండి.
- ఏదైనా పత్రంలో సంతకం చేసేటప్పుడు అప్రమత్తంగా ఉండండి.

https://linktr.ee/endnowfoundation

‘రుణం’ మోసం నుండి జాగ్రత్త

హెచ్చరిక సంకేతాలు :

- క్రెడిట్ చెక్ (తనిఖీ) అవసరం లేదు.
- రుణదాత చట్టబద్ధంగా ప్రభుత్వంలో నమోదు కాకపోవడం.
- భౌతిక చిరునామా లేకపోవడం.
- ముందస్తు చెల్లింపు.
- కొన్ని రోజులు మాత్రమే ఆఫర్ గడువు ఉండటం.

సురక్షిత చిట్కాలు :

- సురక్షితమైన చెల్లింపు కోసం చూడండి (ప్యాడ్ లాక్ చిహ్నంతో https://URL)
- OTP / PIN నంబర్లను కొనుగోలుదారు లేదా విక్రేతకు ఎప్పుడూ చెప్పవద్దు
- మీరు ఫోన్ మాట్లాడేటప్పుడు ఎటువంటి బ్యాంక్ లావాదేవీలు (చెల్లింపులు) చేయకూడదు.
- కొనుగోలుదారులు లేదా విక్రేతలు అందించిన ఏ చిన్న లింకును కూడా క్లిక్ చేయవద్దు.

- కొనుగోలుదారులు లేదా విక్రేతలు అందించిన ఎటువంటి గూగుల్ ఫారమ్‌ను నింపవద్దు.
- QR కోడ్‌ను స్కాన్ చేయవద్దు.
- ఏ రుణాలకైనా ముందస్తు రుణ రుసుమును ఎప్పుడూ చెల్లించవద్దు.

లాటరీ మోసానికి గురికాకుండా మిమ్మల్ని మీరు రక్షించుకోండి

కొన్ని రకాల మోసాలు

- కౌన్ బనేగా కరోడ్ పతి
- స్క్రాచ్ కార్డ్ గిఫ్ట్
- ఆర్.బి.ఐ. లాటరీ
- యూరోపియన్ లాటరీ

భద్రతా చిట్కాలు

- ఈమెయిల్ మరియు SMS ల ద్వారా పంపిన లింక్‌లను క్లిక్ చేయవద్దు.
- https:// ప్రారంభమయ్యే వెబ్‌సైట్‌లపై క్లిక్ చేయండి (దానిపై తాలం గుర్తు ఉంటుంది)
- మీరు ఊహించని అనుబంధం (అటాచ్‌మెంట్) వస్తే దానిని తెరవకండి.
- ఈమెయిల్ మరియు SMS లు పంపించినవారు మీ పేరు ద్వారా మిమ్మల్ని గుర్తించకపోతే వాటిని తెరవకండి.
- లాటరీ బహుమతి గెలుచుకున్నందుకు ముందస్తుగా రుసుము చెల్లించాల్సిన అవసరం లేదు.
- మీరు వ్యక్తిగతంగా కొనుగోలు చేయకపోతే లేదా పాల్గొనకపోతే లాటరీ లేదా పోటీలో డబ్బులు గెలవలేరు.

- పోటీలలో మరియు లాటరీలలో మీరు గెలుపొందినవి వసూలు చేయడానికి ముందస్తు రుసుము చెల్లించాల్సిన అవసరం లేదు.
- అధిక రాబడిని ఊహించి, తెలియని వ్యక్తికి లేదా సంస్థలకు నిధులను ఎప్పుడూ బదిలీ చేయవద్దు.

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

ఐడెంటిటీ మోసం నుండి సురక్షితంగా ఉండండి

గుర్తింపు (ఐడెంటిటీ) మోసం నుండి మిమ్మల్ని మీరు కాపాడుకోడానికి మార్గాలు :

- ఈమెయిల్ ద్వారా లేదా SMS ద్వారా పంపిన లింకులను తెరవవద్దు.

- కంప్యూటర్ మరియు మొబైల్ ఫోన్‌లో యాంటీవైరస్ సాఫ్ట్‌వేర్‌ను నవీకరించండి.

- ఈమెయిల్ లేదా SMS లో ఆర్థిక సమాచారం / పాస్‌వర్డ్ సమాచారం గురించి ఎవరితో పంచుకోవద్దు.
- సామాజిక మాధ్యమంలో జన్మదినం, జన్మస్థలం మరియు ఇంటి చిరునామాను పోస్ట్ చేయవద్దు.

- పాస్‌వర్డ్‌లను క్రమంగా మార్చండి.

- అన్ని అనువర్తనాల (యాప్) కోసం ఒకే రకమైన పాస్‌వర్డ్‌ను కలిగి ఉండకండి.
- క్రమంగా బ్యాంక్ స్టేట్‌మెంట్స్ మరియు క్రెడిట్ కార్డ్ స్టేట్‌మెంట్లను తనిఖీ చేసుకోండి.
- మీరు పాన్‌కార్డు మరియు ఆధార్‌కార్డ్ యొక్క జిరాక్స్ కాపీని ఇచ్చినప్పుడు ఆ జిరాక్స్ కాపీపై మీ ఉద్దేశ్యాన్ని రాయండి.

https://linktr.ee/endnowfoundation

ENDNOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

సైబర్ భద్రత

అంతర్జాలాన్ని వినియోగిస్తున్నప్పుడు భద్రత కోసం ఇలా చేయండి

ఎల్లప్పుడూ మీ సమాచారాన్ని మరియు పాస్‌వర్డ్‌ను గోప్యంగా ఉంచండి.

మీరు అంతర్జాలంలో చేర్చే విషయాలపట్ల జాగ్రత్త వహించండి.

మీరు గోప్యంగా ఉంచే విషయాలను ఎప్పటికప్పుడు తనిఖీ చేస్తూ ఉండండి.

నమ్మకమైన వెబ్‌సైట్‌లలో సురక్షితంగా వస్తువులు కొనుగోలు చేసుకోండి.

ఖచ్చితమైన పాస్‌వర్డ్‌ను ఎంచుకోండి.

మీ అన్ని ఎలక్ట్రానిక్ పరికరాలలో వైరస్ నివారణ ప్రోగ్రామ్‌ను (యాంటీవైరస్) చేర్చండి.

పని పూర్తికాగానే మీ అకౌంట్‌ను మూసివేయాలని (లాగ్‌ఆఫ్) గుర్తుంచుకోండి.

వెబ్‌సైట్ డొమైన్ URL ను తనిఖీ చేయండి.

ఎల్లప్పుడు మీ ఈమెయిల్ తెరిచే ముందు ఒకసారి తనిఖీ చేయండి.

ఫిషింగ్ మరియు మోసాలకు దూరంగా ఉండండి

మీ పిల్లలు అంతర్జాలాన్ని వినియోగిస్తున్నప్పుడు సురక్షితంగా ఉండేలా చూడండి.

మీరు అంతర్జాలాన్ని వినియోగిస్తున్నప్పుడు మిమ్మల్ని గౌరవించు కోండి. అలాగే ఇతరులను గౌరవించండి.

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

మీ చరవాణిలు మరియు టాబ్లెట్ ల భద్రత కోసం ఇలా చేయండి !

మీ డెస్క్‌టాప్ పరికరాల కంటే మీ చరవాణులు మరియు టాబ్లెట్‌లకు భద్రత ఎక్కువ అవసరం.

మీ పరికరాల్లో స్వయంగా నవీకరించు (ఆటో అప్‌డేట్) అన్న విషయాన్ని చేర్చుకుని, దాన్ని ఉపయోగిస్తూ మీ పరికరాల్లో ఉన్న అన్ని అనువర్తనాలను (యాప్స్) ఎప్పటికప్పుడు నవీనంగా ఉంచండి.

మీ చరవాణివంటి పరికరాల భద్రత మరియు గుర్తింపు కోసం పిన్/ పాస్‌వర్డ్ / వేలిముద్ర / ఏదైనా భద్రతా గుర్తింపు చిహ్నాలను ఉపయోగించండి.

బహిరంగ ప్రదేశాల్లో పబ్లిక్ వైఫైని వాడవద్దు. మీ చరవాణిలో ఉన్న 3జి లేదా 4జిని మాత్రమే ఉపయోగించండి లేదా వర్చువల్ ప్రైవేట్ నెట్‌వర్క్ (VPN) ను ఉపయోగించండి.

మీ చరవాణి పరికరాలను మీరు ఎక్కడి నుంచైనా ట్రాక్ చేయగల మరియు ఆఫ్ చేయగల లేదా వాటిని పూర్తిగా తొలగించగల ఏర్పాటు చేసుకోండి.

ఎక్కువకాలం మన్నికలేని మరియు తయారీదారుల మద్దతులేని పరికరాలను ఎప్పటికప్పుడు కొత్త పరికరాలతో మార్చండి.

https://linktr.ee/endnowfoundation

ENDNOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

మీ డేటాని బ్యాకప్ చేసుకోండి

బ్యాకప్ చేసుకునేందుకు ఈ క్రింది విధానాలను పాటించడం ఉత్తమం !

మీ ముఖ్యమైన డేటాను తరచుగా బ్యాకప్ చేయండి మరియు వాటిని పునరుద్ధరించ వచ్చునా లేదా అని పరీక్షించండి.

డేటా పునరుద్ధరించ వచ్చునా లేదా అన్న విషయాన్ని ప్రత్యామ్నాయ పరికరాల్లో నిర్దిష్ట వ్యవధుల్లో పరీక్షించండి.

ఏమి బ్యాకప్ చేయాలో అనగా పత్రాలు, ఛాయాచిత్రాలు, ఈమెయిల్, క్యాలెండర్ మరియు సంపర్కాలు (కాంటాక్ట్స్) మొదలగునవి గుర్తించాలి.

క్లౌడ్‌పై డేటా బ్యాకప్ చేయడాన్ని పరిగణించండి, తద్వారా మీరు డేటాను ఎక్కడి నుంచైనా ఉపయోగించుకో గలరు.

బ్యాకప్ ఉన్న పరికరాన్ని నిర్ధారించుకొని శాశ్వతంగా ఏదైనా నెట్‌వర్క్‌కి జతచేయబడలేదు అని నిర్ధారించుకోండి.

ADVOCACY ON DIGITAL SAFETY

మాల్‌వేర్ నష్టం నివారణ మార్గం

ఊహించని పాప్-అప్‌లు, తెలియని ఈమెయిల్ మరియు .
exe పాడగింపు ఫైల్‌ల నివారణ మార్గాలు

అన్ని పరికరాలలో వైరస్ నివారణ (యాంటీవైరస్) సాఫ్ట్‌వేర్‌ను ఉపయోగించండి మరియు ఆమోదించిన సాఫ్ట్‌వేర్‌ను మాత్రమే మీ పరికరాల్లో చేర్చండి.

తొలగించగల ప్రసారమాధ్యమాలను (రిమూవబుల్ మీడియా) నియంత్రించండి. ఫైళ్ళను, ఈమెయిల్ లేదా క్లౌడ్ నిల్వల ద్వారా బదిలీ చేయమని ప్రోత్సహించండి.

తెలియని మూలం(సోర్స్) నుండి ఇతర పార్టీ అనువర్తనాలను (యాప్) ఎప్పుడూ డౌన్‌లోడ్ చేయవద్దు.

మీ నెట్‌వర్క్ మరియు అంతర్జాలం మధ్య బఫర్ మండలాన్ని (బఫర్ జోన్) సృష్టించడానికి మీ ఫైర్‌వాల్‌ను ఆన్ చేయండి.

'స్వయంగా నవీకరించు' (ఆటోఅప్‌డేట్) అన్న ఎంపికను ఉపయోగించి అన్ని సాఫ్ట్‌వేర్ మరియు ఫర్మ్‌వేర్‌లను నవీకరించుకోండి.

ENDNOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

పాస్‌వర్డ్‌ను ఉపయోగించడం

మీ డేటాను రక్షించడానికి పాస్‌వర్డ్‌ను ఉపయోగించండి !

బూట్ చేసుకునేందుకు పాస్‌వర్డ్ అవసరమయ్యే ఎన్‌క్రిప్టెడ్ ఉత్పత్తులను ఉపయోగించేలా ఏర్పాటుచేసుకోండి.

నిర్దిష్ట వ్యవధుల్లో పాస్‌వర్డ్ మార్పు చేస్తూ ఉండండి.

అన్ని పరికరాల్లో పాస్‌వర్డ్/పిన్ లేదా వేలిముద్ర వంటి గుర్తింపు చిహ్నాలను పెట్టుకోండి.

కొత్త పరికరాల్లో తయారీదారులు ఇచ్చిన పాస్‌వర్డ్‌ను తప్పనిసరిగా మార్చాలి.

బ్యాంకింగ్, ఈమెయిల్ మరియు సాంఘిక ప్రసార మాధ్యమం సైట్ల కోసం ద్వికారక ప్రామాణికీకరణ (2 ఫాక్టర్ అథంటికేషన్ - 2FA) విధానాన్ని ఉపయోగించండి.

వాడకందారు (యూజర్) సులభంగా పాస్‌వర్డ్‌ను రీసెట్ చేసుకునేలా సురక్షిత స్టోరేజీని అందించండి.

సులభంగా ఊహించగల పాస్‌వర్డ్‌లను ఉపయోగించడం మానుకోండి (అనగా కుటుంబం, పెంపుడు జంతువులు, మొదటి పేర్లు మొదలగునవి).

'మాస్టర్ పాస్‌వర్డ్' వంటి పాస్‌వర్డ్ మేనేజర్ సాధనాన్ని ఉపయోగించండి (ఇవి అన్ని ఇతర పాస్‌వర్డ్‌లను నియంత్రించడానికి ఉపయోగపడుతుంది).

ENDNOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

క్యారిమినాటి యూట్యూబ్ చానెల్ (క్యారీస్‌లైవ్) హ్యాక్ అయ్యింది

ద్వికారక ప్రామాణికీకరణ (2 ఫ్యాక్టర్ అథెంటికేషన్ 2FA) విధానాన్ని ప్రారంభించండి

వీరి ఖాతాలు హ్యాక్ చేయబడినప్పుడు మీ ఖాతాలు కూడా సులభంగా హ్యాక్ చేయవచ్చు.

→

CARRYISLIVE

→

WHO IS NEXT ?

ద్వికారక ప్రామాణికీకరణ కోసం ఈ క్రింది దశలను అనుసరించండి

- Instagram: సెట్టింగ్స్ → సెక్యూరిటీ → టు ఫ్యాక్టర్ అథెంటికేషన్.
- Facebook: సెట్టింగ్స్ → సెక్యూరిటీ & లాగిన్ → టు ఫ్యాక్టర్ అథెంటికేషన్.
- Twitter: సెట్టింగ్స్ & ప్రైవసీ → అకౌంట్స్ సెక్యూరిటీ → టెక్స్ట్ మెసేజ్ →
- LinkedIn: సెట్టింగ్స్ & ప్రైవసీ → లాగిన్ & సెక్యూరిటీ → టూ స్టెప్ వెరిఫికేషన్
- YouTube: గూగుల్ అకౌంట్ → సెక్యూరిటీ → టూ స్టెప్ వెరిఫికేషన్.

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

తల్లిదండ్రుల కోసం 10 ఆన్‌లైన్ భద్రతా చిట్కాలు

డిజిటల్ పౌరసత్వం మరియు ఆన్‌లైన్ భద్రత

టెక్నాలజీ అన్ని మార్గాలను నిరోధించవద్దు. టెక్నాలజీని సురక్షితంగా మరియు సానుకూలంగా ఉపయోగించుకోవడం నేర్చుకోవడానికి మీ పిల్లలకు సహాయపడండి.

మీ పిల్లలకు ఇష్టమైన అనువర్తనాలు (Apps) లేదా సైట్‌లపై ఆసక్తి చూపండి. వారికి సహకరించండి.

అంతర్జాలం యొక్క సరిహద్దులను నిర్ణయించండి మరియు ఫిల్టరింగ్ సాఫ్ట్‌వేర్‌ని ఉపయోగించడాన్ని పరిగణించండి. ఇది తల్లిదండ్రులుగా మీరు తీసుకోవాల్సిన బాధ్యత.

కార్లు, బెడ్‌రూములు మరియు భోజనం వంటి సమయాల్లో టెక్నాలజీ వాడకూడదని కుటుంబంతో ఒప్పందాన్ని చేసుకోండి.

అంతర్జాలంలో బహిర్గతం చేయకూడని వ్యక్తిగత సమాచారాన్ని మీ పిల్లలకు ఎల్లప్పుడూ నేర్పండి.

ఆన్‌లైన్ సమాచారాన్ని తెలుసుకోవడానికి మీ పిల్లలకు సహాయపడండి మరియు కల్పన నుండి వాస్తవాన్ని గ్రహింపజేయండి.

మీ పిల్లలకు డిజిటల్ సంధిగ్ధతల్లో సూచనలు ఇవ్వండి. బహుమతులుగా లేదా శిక్షలుగా వస్తువులను ఉపయోగించడం మానుకోండి.

ఇంట్లో ఉన్నప్పుడు గ్రీన్ సమయం మరియు స్క్రీన్ సమయాన్ని సమతుల్యం చేయండి. ప్రాథమిక అవసరాలపై దృష్టిపెట్టండి.

తక్కువ వయస్సు ఉన్న మీ పిల్లలకు వయస్సు పరిమిత వెబ్‌సైట్‌లను సైన్‌అప్ చేయడానికి వారికి అనుమతి ఇవ్వద్దు.

మరింత నేర్చుకోండి :
తల్లిదండ్రుల కోసం నమ్మదగిన వనరులను అన్వేషించండి. తద్వారా మీకు మీరే అవగాహన చేసుకోవచ్చు.

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

పిల్లల కోసం 10 ఆన్‌లైన్ భద్రతా చిట్కాలు

డిజిటల్ పౌరసత్వం మరియు ఆన్‌లైన్ భద్రత

చట్టాలు : 13 సంవత్సరాల వయస్సు పైబడిన పిల్లలకు చాలాసైట్లు, వెబ్ సాధనాలు మరియు చిత్రాలు ఆన్‌లైన్ పని కాపీరైట్ ద్వారా రక్షించబడతాయి.

చర్చ : మీరు ఆన్‌లైన్‌లో ఏమి చేస్తున్నారో మీ తల్లిదండ్రులకు చెప్పండి. మీకు ఏదైనా తెలియకపోతే ఎల్లప్పుడు మీరు విశ్వసించే పెద్దవారిని అడగండి.

స్నేహితులు : తల్లిదండ్రుల అనుమతి లేకుండా ఆన్‌లైన్ స్నేహితులను కలవకండి స్నేహితులు మీకు చెప్పే ప్రతి విషయాన్ని నిజమని నమ్మకండి.

గోప్యత: మీ వ్యక్తిగత సమాచారాన్ని గోప్యంగా ఉంచండి. మీ పూర్తి చిరునామాను, ఫోన్ నెంబర్, మీ ప్రణాళికలు, పాస్‌వర్డ్ మరియు పుట్టినరోజు మొదలగునవి.

కీర్తి : ఉపాధ్యాయులు, కుటుంబం, స్నేహితులు మరియు భవిష్యత్ యజమానులకు అపకీర్తి తెచ్చేవి ఏదైనా పోస్ట్ చేయవద్దు.

ప్రశ్నించడం: ఆన్‌లైన్‌లో చాలా తప్పుడు మరియు ప్రతికూల సమాచారం ఉన్నందున మీరు చదివిన మరియు చూసిన ప్రతీ విషయాన్ని నమ్మకూడదు.

బెదిరింపు: సైబర్ బెదిరింపు మీకు లేదా మరొకరికి జరుగుతుందని మీరు అనుకుంటే, ఒక వేళ చూస్తే, మీకు తెలిసిన వ్యక్తులకు చెప్పండి.

ఖాతాలు: కొన్ని సున్నితమైన ఈమెయిల్ చిరునామాలు మరియు వినియోగదారుల పేర్లను ఎంచుకోండి. ఖచ్చితమైన పాస్‌వర్డ్‌లను ఉపయోగించండి మరియు వాటిని ఇతరులతో పంచుకోవద్దు.

మర్యాద : అన్ని సమయాల్లో మర్యాదగా, గౌరవంగా ఉండండి. మీరు ఆన్‌లైన్‌లో ఎలా మర్యాద పొందాలనుకుంటున్నారో ఇతరులతో అలాగే వ్యవహరించండి.

అన్‌ప్లగ్: మీ స్క్రీన్ సమయం మరియు గ్రీన్ సమయాలన్ని సమతుల్యం చేయండి. ఇంటి బయటకు వెళ్ళండి, తిరగండి, ఆడుకోండి మరియు ఇతరులతో ముఖాముఖి మాట్లాడండి.

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

సైబర్ నేరాలు రక్షకబట నిలయం

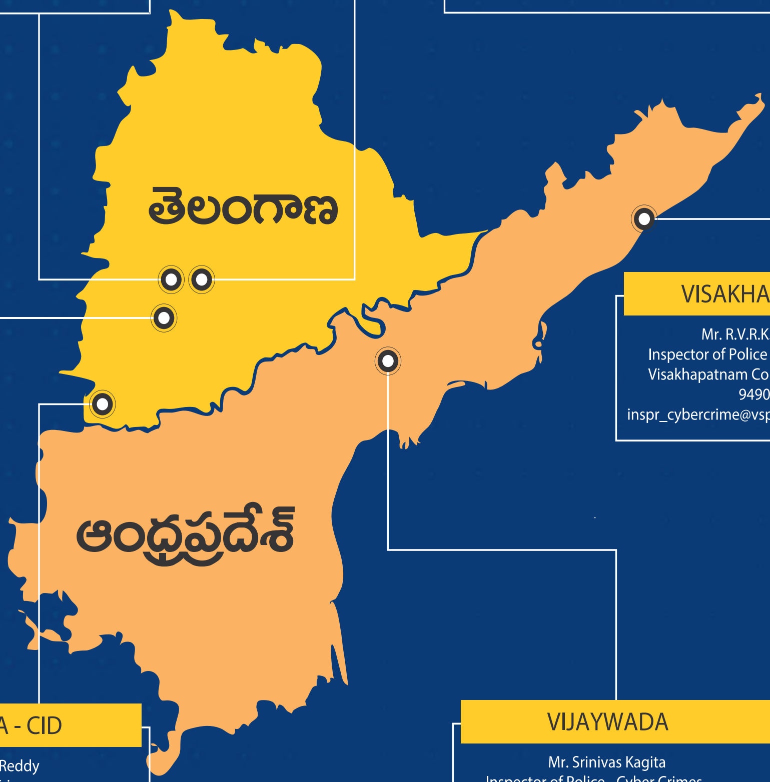
ఆంధ్రప్రదేశ్ మరియు తెలంగాణ

సైబర్ నేరాలు ఫిర్యాదు చేసే పోర్టల్

www.cybercrime.gov.in

CYBERABAD
Mr. Bala Krishna Reddy
A.C.P – Cyber Crimes
Cyberabad Commissionerate
9490617310
sho-cybercrimes@tspolice.gov.in

HYDERABAD
Mr. K.V.M. Prasad
A.C.P – Cyber Crimes
Hyderabad Commissionerate
040-27852412, 9490616152
cybercell-hyd@tspolice.gov.in



RACHAKONDA
Mr. S. Harinath
A.C.P – Cyber Crimes
Rachakonda Commissionerate
040-27854044, 9490617437
acp-cybercrimes-rck@tspolice.gov.in

VISAKHAPATNAM
Mr. R.V.R.K. Chowdary
Inspector of Police – Cyber Crimes
Visakhapatnam Commissionerate
9490617917
inspr_cybercrime@vspc.appolice.gov.in

TELANGANA - CID
B. Ravi Kumar Reddy
D.S.P - Cyber Crimes
Telangana - CID
+91 94406 27982
ccps.cid@tspolice.gov.in

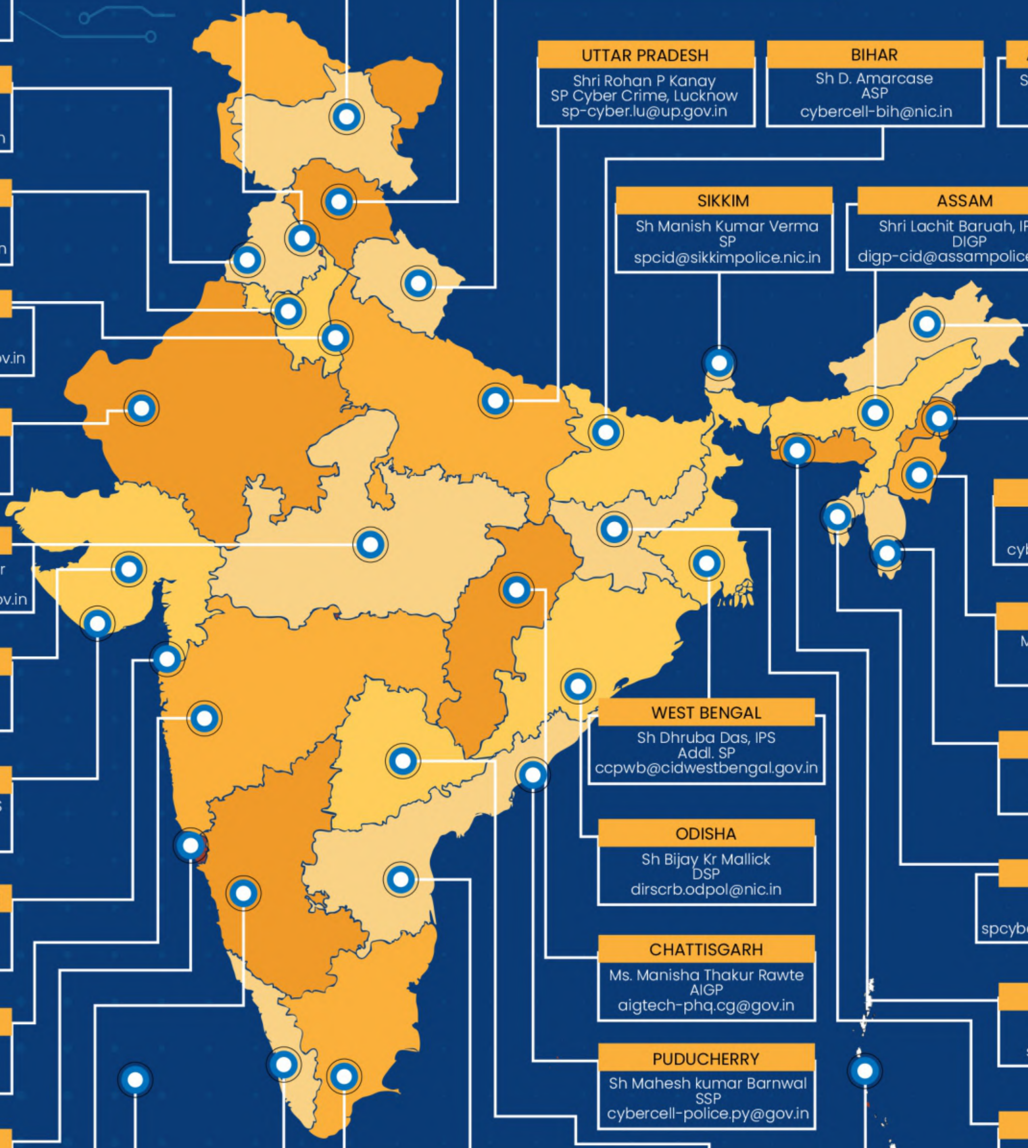
VIJAYWADA
Mr. Srinivas Kagita
Inspector of Police - Cyber Crimes
Vijaywada Commissionerate
0866-2970433, 9490619462
cyberpolicingcellvza@gmail.com

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

నోడల్ సైబర్ సెల్ అధికారులు

సైబర్ నేరాలు ఫిర్యాదు చేసే పోర్టల్

www.cybercrime.gov.in



JAMMU & KASHMIR
Sh Mukesh Singh
(IGP)
igcrime-jk@nic.in

HIMACHAL PRADESH
Sh Narveer Rathore
DSP
polcyberps-shi-hp@nic.in

UTTARAKHAND
Ms. Riddhima Aggarwal
DIG
ccps.deh@uttarakhandpolice.uk.gov.in

CHANDIGARH
Sh Omvir Singh Bishnoi
DIG
dig-chd@nic.in

PUNJAB
Sh Inderbir Singh
AIG
aigcc@punjabpolice.gov.in

HARYANA
Shri Pankaj Nain, IPS
SP/Cyber Crime
shocyberpkl.pol-hry@gov.in

DELHI
Sh Anyesh Roy
DCP
acp.cybercell@delhipolice.gov.in

RAJASTHAN
Sh Umesh Nitharwal
Dy. SP CCPS
ccps-raj@nic.in

MADHYA PRADESH
Sh Niranjan B Vayangankar
DIGP
mpcyberpolice@mppolice.gov.in

GUJARAT
Sh Rajesh Gadhiya
SP
cc-cid@gujarat.gov.in

DAMAN AND DIU
Sh. Hareshwar V. Swami,IPS
SP
sp-diu-dd@nic.in

DADRA & NAGAR HAVELI
Ms. Manasvi Jain
Dy. SP
itcell-dnhp@mha.gov.in

MAHARASHTRA
Sh Balsing Rajput
SP
sp.cbr-mah@gov.in

GOA
Sh Pankaj Kumar Singh
DIGP
picyber@goapolice.gov.in

KARNATAKA
Sh S. Badrinath
Dy. SP
badri@ksp.gov.in

LAKSHADWEEP
Sh Ramdulesh Meena
DSP
lak-sop@nic.in

KERALA
Sh Sreejith
IGP
igpcrimes.pol@kerala.gov.in

UTTAR PRADESH
Shri Rohan P Kanay
SP Cyber Crime, Lucknow
sp-cyber.lu@up.gov.in

BIHAR
Sh D. Amarcase
ASP
cybercell-bih@nic.in

ARUNACHAL PRADESH
Shri Navdeep Singh Brar
SP
spcr@arunpol.nic.in

SIKKIM
Sh Manish Kumar Verma
SP
spcid@sikkimpolice.nic.in

ASSAM
Shri Lachit Baruah, IPS
DIGP
digp-cid@assampolice.gov.in

NAGALAND
Sh Zekotso Mero
IGP
cybercrimeps-ngl@gov.in

MANIPUR
Ms. Joyce Lalremmawi
SP
cidcb-mn@nic.in

MIZORAM
Sh Lalhuliana.Sanai
SP
cidcrime-mz@nic.in

TRIPURA
Sh. Ajit Pratap Singh
SP Crime
spcybercrime@tripurapolice.nic.in

MEGHALAYA
Sh M.G.T Sangma
SP
sspcid-meg@gov.in

JHARKHAND
Ms. Vijaya Laxmi
SP
cyberps@jhpolice.gov.in

WEST BENGAL
Sh Dhruba Das, IPS
Addl. SP
ccpwb@cidwestbengal.gov.in

ODISHA
Sh Bijay Kr Mallick
DSP
dirscrb.odpol@nic.in

CHATTISGARH
Ms. Manisha Thakur Rawte
AIGP
aigtech-phq.cg@gov.in

PUDUCHERRY
Sh Mahesh kumar Barnwal
SSP
cybercell-police.py@gov.in

ANDHRA PRADESH
Ms. G. Radhika
SP
cybercrimes-cid@ap.gov.in

TELANGANA
Sh B. Ravi Kumar Reddy
DySP
ccps.cid@tspolice.gov.in

ANDAMAN & NICOBAR
Sh. Madhup Tiwari
IGP
igpint.and@nic.in

TAMIL NADU
Sh G Shashank Sai (for OTHER CYBER CRIMES)
SP
spl-ccdtnpolice@gov.in

Smt. Jayashree V. (for Women and Children related)
SP
spl-cwctnpolice@gov.in

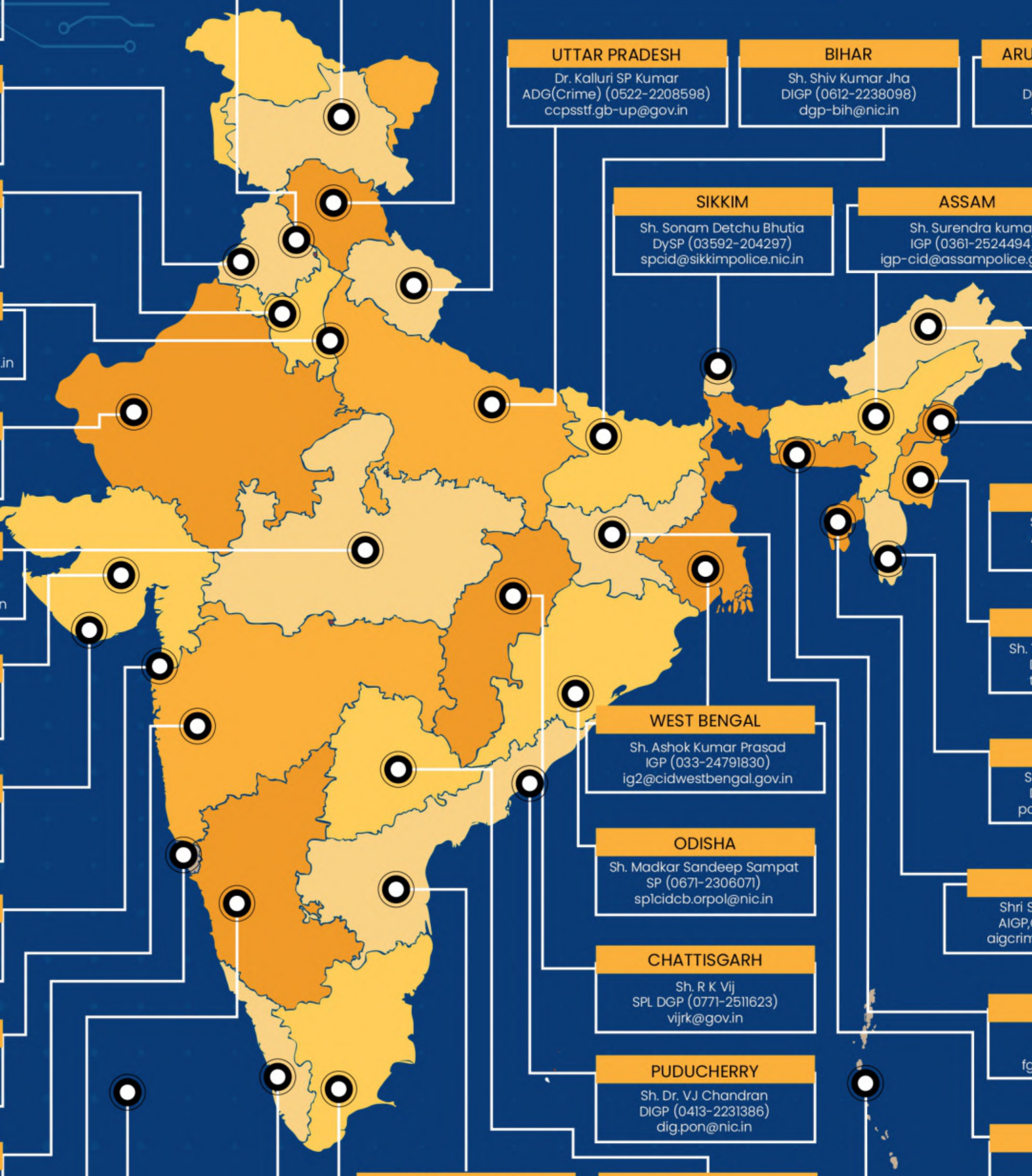
https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

గ్రీవెన్స్ అధికారులు - సైబర్ సెల్

సైబర్ నేరాలు ఫిర్యాదు చేసే పోర్టల్

www.cybercrime.gov.in



JAMMU & KASHMIR
Sh. B Srinivas
ADGP (0191-2582996)
adgpcidjk@jkpolice.gov.in

HIMACHAL PRADESH
Sh. Sandeep Dhawal
SP (0177-2627955)
sp-cybercr-hp@nic.in

UTTARAKHAND
Sh. Deepam Seth
IGP (0135-2712563)
dgc-police-ua@nic.in

CHANDIGARH
Ms. Nilambari Jagadale
SSP (0172-2760001)
pssput-chd@nic.in

PUNJAB
Sh. Hardial Singh Mann
DIGP (0172-2226258)
aigcc@punjabpolice.gov.in
shocc@punjabpolice.gov.in

HARYANA
Shri Desh Raj Singh, IPS
ADGP(Crime) (01733-253230)
adgp.crime@hry.nic.in

DELHI
Mr. Prem Nath
Addl.CP (011-20892633)
addlcp.cybertech@delhipolice.gov.in

UTTAR PRADESH
Dr. Kalluri SP Kumar
ADG(Crime) (0522-2208598)
ccpsstf.gb-up@gov.in

BIHAR
Sh. Shiv Kumar Jha
DIGP (0612-2238098)
dgp-bih@nic.in

ARUNACHAL PRADESH
Sh. Take Ringu
DIGP (0360-2215518)
sit@arunpol.nic.in

SIKKIM
Sh. Sonam Detchu Bhutia
DySP (03592-204297)
spcid@sikkimpolice.nic.in

ASSAM
Sh. Surendra kumar
IGP (0361-2524494)
igp-cid@assampolice.gov.in

RAJASTHAN
Sh. Abhijeet Singh
SP SOG (0141-2309547)
singh.kadian@ips.gov.in

MADHYA PRADESH
Smt. Aruna Mohan Rao
SPL DGP (0755-2770248)
spl.dgp-cybercell@mppolice.gov.in

NAGALAND
Sh. Renchamo P. Kikon
ADGP (0370-2223897)
renchamo.p@gov.in

GUJARAT
Dr. Shamsher Singh
ADGP (079-23250798)
cc-cid@gujarat.gov.in

MANIPUR
Sh. Themthing Ngashangva
DIGP (0385-2450573)
themthing.ng@gov.in

WEST BENGAL
Sh. Ashok Kumar Prasad
IGP (033-24791830)
ig2@cidwestbengal.gov.in

DAMAN AND DIU
Sh. Vikramjit Singh IPS
SP (0260-2250942)
sp-dmn-dd@nic.in

MIZORAM
Sh.Balaji Srivastava IPS
DGP (0389-2334682)
polmizo@rediffmail.com

ODISHA
Sh. Madkar Sandeep Sampat
SP (0671-2306071)
splcidcb.orpol@nic.in

DADRA & NAGAR HAVELI
Sh. Sharad Bhaskar
SP (0260-2643022)
sp-sil-dnh@nic.in

TRIPURA
Shri Subrata Chakraborty
AIGP,Crime (0381-2321741)
aigcrime@tripurapolice.nic.in

CHATTISGARH
Sh. R K Vij
SPL DGP (0771-2511623)
vijrk@gov.in

MAHARASHTRA
Sh. Brijesh Singh
SPL IGP/ DGP (022-22160080)
ig.cbr-mah@gov.in

MEGHALAYA
Sh. F G Kharshiing
DIGP (364-2550141)
fg.kharshiing@ips.gov.in

PUDUCHERRY
Sh. Dr. VJ Chandran
DIGP (0413-2231386)
dig.pon@nic.in

GOA
Sh. Paramaditya
DIGP (0832-2420883)
digpgoa@goapolice.gov.in

JHARKHAND
Sh. Ranjit Prasad
IGP (0651-2490046)
ig-orgcid@jhpolice.gov.in

ANDHRA PRADESH
Shri M.Sunil Kumar Naik IPS
DIGP (0863-2340152)
cybercrimes-cid@ap.gov.in

TELANGANA
Smt. Swathi Lakra IPS
ADGP (040-23147604)
igp_wpc@cid.tspolice.gov.in

KARNATAKA
Sh. T D Pawar
DIGP (080-22251817)
digadmincod@ksp.gov.in

LAKSHADWEEP
Sh. Shibesh Singh
SSP (04896-262258)
lak-sop@nic.in

TAMIL NADU
Shri Shankar K. (FOR OTHER CYBER CRIMES)
IGP (044-28447712)
spl-ccdtnpolice@gov.in

Shri Shankar K. (FOR WOMEN & CHILDREN RELATED)
IGP (044-28447620)
spl-cwctnpolice@gov.in

ANDAMAN & NICOBAR
Sh.Deependra Pathak
DGP (03192-230216)
dgp.and@nic.in

KERALA

KERALA
Sh. Dr. Shaik Darvesh
ADGP (0471-2722215)
adgpcrimes.pol@kerala.gov.in

https://linktr.ee/endnowfoundation

END NOW FOUNDATION
ADVOCACY ON DIGITAL SAFETY

సహకారం :

శ్రీమతి ఐరేణి శైలజ
తెలుగు భాషోపాధ్యాయురాలు

శ్రీమతి ఐరేణి చిత్రప్రియ
తెలుగు భాషోపాధ్యాయురాలు

శ్రీ మొగిలి రఘునాథ్ గౌడ్
అపర్ణా గ్రాఫిక్స్

https://www.canva.com/ | https://slidesgo.com/ | https://linktr.ee/ | https://www.freepik.com/ | https://internshala.com/

https://linktr.ee/endnowfoundation

END NOW FOUNDATION

ADVOCACY ON DIGITAL SAFETY

www.endnowfoundation.org

Hyderabad – 500018

Telangana, India. (Reg. No: 86/IV/2017)

Advocacy by News Paper | Research & Development | Advocacy by Digital Safety Advocates | Advocacy by FM Radio | Advocacy by Student Ambassadors | Advocacy By Organisations