



Information Security Education & Awareness

Ministry of Electronics and Information Technology
Government of India

सी डैक
CDAC

సైబర్ భద్రత పై పిల్లలకు అవగాహన



పిల్లల కోసం సైబర్ భద్రతపై కథలు



For Virus Alerts, Incident & Vulnerability Reporting
certin
Handling Computer Security Incidents

www.
InfoSec
awareness.in

From the Desk

Children are now growing up in an internet connected world enjoying the benefits of being a part of cyber world. Considering the risks involved while using cyber space makes it important to educate children about cybercrimes and what they should do to protect themselves from the dangers of internet while being online. As part of Information Security Education & Awareness (ISEA) Project Phase II, under Ministry of Electronics and Information Technology (MeitY), many initiatives were undertaken to create cyber awareness among children. Keeping in view of the increased number of cybercrimes towards children, ISEA has created this handbook to help younger children to understand the various types of cyber-crimes that can happen to them and various ways cyber criminals may try to fraud them making them a victim of cyber-crimes. We hope that this handbook could be of use to children to make them a responsible cyber user and also help them to understand the cyber world in a better way. With immense pleasure we release cartoon handbook for children on cyber security awareness and congratulate the whole team of Information Security Education & Awareness Project for coming up with such a venture to promote cybersecurity awareness.



E Magesh
Director, C-DAC Hyderabad



INDEX

చెడు భాషను మానుకోండి.....	04
వ్యక్తిగత సమచారం గోప్యంగా ఉంచడం.....	06
సంభాషణ జరిపేటప్పుడు.....	08
కాపీరైట్స్.....	10
సంస్కృతులు.....	12
ఆన్‌లైన్ ప్రీడేటర్లు.....	14
తక్షణ సందేశం.....	16
ఇమెయిల్ అకౌంట్ హాక్ చేయడం.....	18
సైబర్ బిదిరింపు.....	20
సైబర్ స్వాకింగ్.....	22
మొబైల్ ఫోన్ భద్రత.....	24
మొబైల్ ఫోన్ వ్యసనాలు.....	26
రాస్‌షమ్‌వేర్.....	28
ఆన్‌లైన్‌లో ఆపరిచితులను కలవడం.....	30
ఆన్‌లైన్ గేమింగ్.....	32
సామాజిక నెట్వర్కింగ్.....	34
గుర్తింపును దొంగిలించడం	36
ఆన్‌లైన్ మోసం.....	38
ఫిషింగ్ దాడులు.....	40
పిక్చర్ మార్పింగ్.....	42
సైబర్ గ్లామింగ్.....	44
నకిలీ సమక్షలు.....	46



మీలో కొంతమందికి చెడు పదాలను సరదాగా వాడడం లేదా చెడ్డ భాషను ఉపయోగించే అలవాటు ఉండవచ్చు. లేదా మీరు ఇష్టపడని మీ క్లాస్ మేట్ పై మీ కోపాన్ని చూపించవచ్చు. మీరు ఉపయోగించే పదాలు, ఇంకా మీరు పోస్ట్ చేసిన ఫోటోలు ప్రతీకారం తీర్చుకునే విధంగా ఉండడమే కాకుండా వాస్తవ ప్రపంచంలో కూడా అవి దుష్ప్రణాళికలకు దారి తీయవచ్చు. తన తరగతిలోని సహవిద్యార్థితో "బబ్లు" చెడ్డ భాషను ఉపయోగించినప్పుడు ఏమి జరిగిందో చూద్దాం.

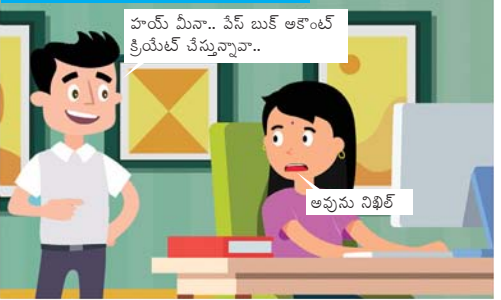


మీ వ్యక్తిగత ఫోటోలు, మిమ్మల్ని గురించిన మీ వ్యక్తిగత సమాచారం సోషల్ మీడియాలో పోస్ట్ చేయడం అంటే మీలో చాలా మందికి ఒక సరదా/ సంతోషం. కానీ ఈ వ్యక్తిగత సమాచారం తప్పుడు వ్యక్తుల చేతుల్లోకి వెళ్ళే అది మిమ్మల్ని ఇబ్బందుల్లో పడేస్తుంది. తన సోదరి తన వ్యక్తిగత సమాచారాన్ని పంచుకోవడంలో జాగ్రత్తగా ఉండాలని నిఖిల్ ఆమెకు ఎలా వివరించాడో చూద్దాం.

ఒక రోజు, మీనా కంప్యూటర్ ఆఫీస్ చేసి తనకి ఫ్రెండ్స్ కోసం ఆమె యూజర్ ఐడీని సృష్టించింది.

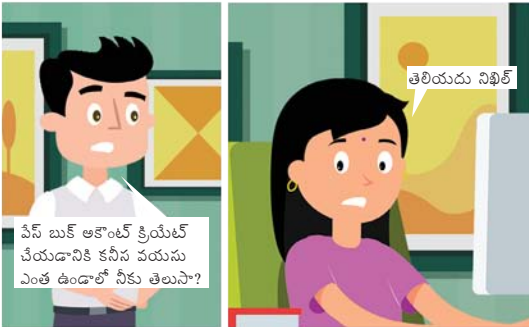


ఆమె అన్న నిఖిల్ గదిలోకి వచ్చి ఇలా అన్నాడు..



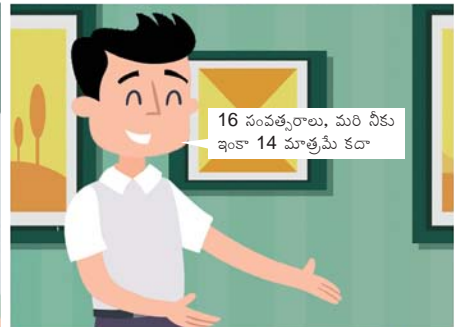
హాయ్ మీనా.. పేస్ బుక్ ఆకౌంట్ క్రియేట్ చేస్తున్నావా..

అవును నిఖిల్



పేస్ బుక్ ఆకౌంట్ క్రియేట్ చేయడానికి కనీస వయసు ఎంత ఉండాలి నీకు తెలుసా?

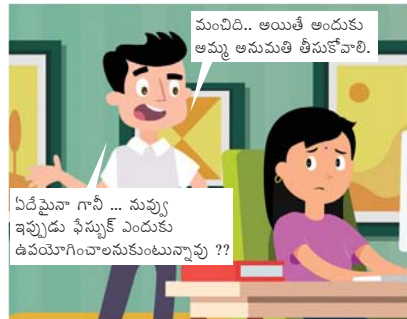
తెలియదు నిఖిల్



16 సంవత్సరాలు, మరి నీకు ఇంకా 14 మాత్రమే కదా



మరి అలా ఆయితే నేను అమ్మ ఆకౌంట్ లోకి లాగిన్ అవువా??



మంచిది.. ఆయితే అందుకు అమ్మ అనుమతి తీసుకోవాలి.

ఏదేమైనా గానీ ... నువ్వు ఇప్పుడు ఫ్రెండ్స్ కు ఎందుకు ఉపయోగించాలనుకుంటున్నావు ??



నేను నా ఫోటోలను షేర్ చేయాలని అనుకుంటున్నాను మరియూ ఆప్లోడ్ చేయాలనుకుంటున్నాను. నా ఆభిరుచులను పంచుకోవాలనుకుంటున్నాను ...

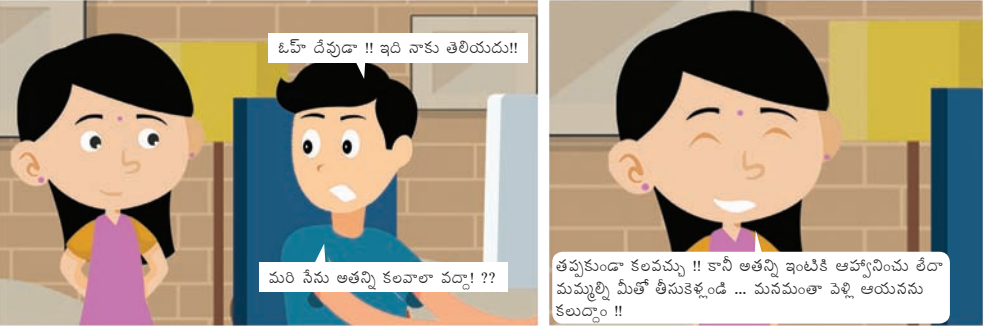
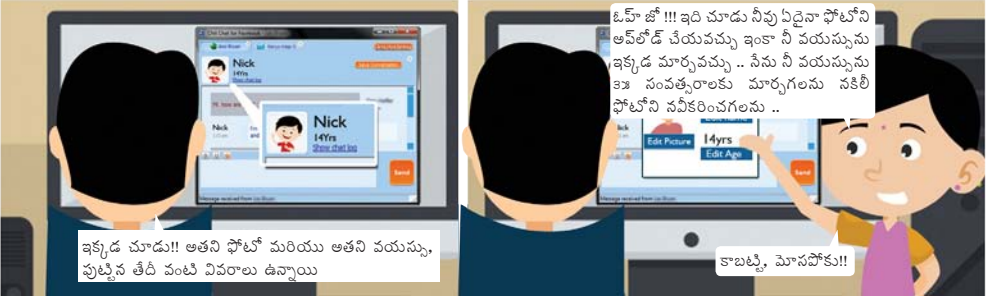


చిట్కాలు:

- మీకు తెలియకుండా అపరిచితులు మీ ప్రొఫైల్ ను ఉపయోగించుకోవచ్చు మరియు మీ సమాచారాన్ని దుర్వినియోగం చేయవచ్చు
- సోషల్ నెట్ వర్కింగ్ వెబ్ సైట్ లో అందుబాటులో ఉన్న గోప్యతా సెట్టింగ్ లను ఎల్లప్పుడూ ఉపయోగించుకోవడం మంచిది.
- మీ పేరు, పాఠశాల / ఇంటి చిరునామా, ఫోన్ నంబర్లు, వయస్సు, జండర్, క్రెడిట్ కార్డ్ వివరాల వంటి వ్యక్తిగత సమాచారాన్ని ఇవ్వవద్దు లేదా పోస్ట్ చేయవద్దు
- సైట్ లో నీవు ఇచ్చే సమాచారం కూడా నిన్ను బాధితురాలిగా మార్చే ప్రమాదంలోకి నెడుతుందని తెలుసుకో.
- సోషల్ నెట్ వర్కింగ్ సైట్ లో పరిచయం అయిన వారితో వ్యక్తిగతంగా కలవకు, ఎందుకంటే కొంతమంది వారు ఎవరో నిజాలు వారు చెప్పకపోవచ్చు.

ఆన్లైన్ చాటింగ్ చాలా సరదాగా ఉంటుంది, కానీ దీనిలో ప్రతికూలఅంశాలు కూడా ఉంటాయి. ఒక్కోసారి చాటింగ్ అపారాధకు దారితీస్తుంది. వచన సందేశాన్ని పంపే ముందు దాన్ని చదివి ఎలా ఆర్థం చేసుకోవచ్చో ఆలోచించడం మంచిది. ఆన్లైన్ చాటింగ్లో కూడా ఇమెయిల్ మర్యాదలు మరియు భద్రతా నియమాలు పాటించాల్సి ఉంటుంది.





చిట్కాలు:

- ౧. మీకు తెలియని వ్యక్తుల నుండి వచన సందేశాలను గురించి పట్టించుకోకు.
- ౨. ఆన్‌లైన్ సంభాషణలలో నీ వ్యక్తిగత వివరాలను పంచుకోవడం మానుకో.

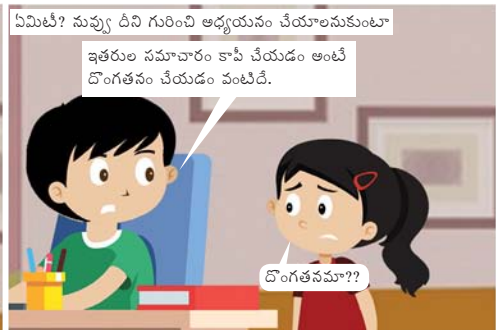
Social networking

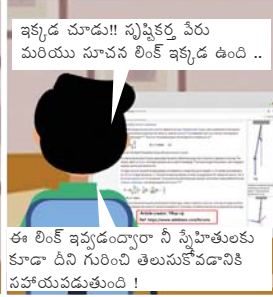
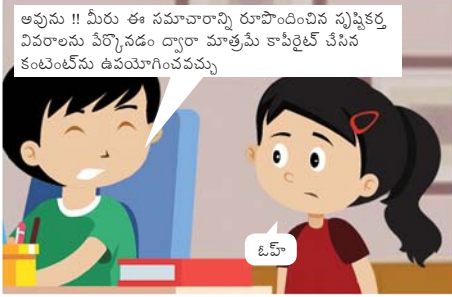
- Only add people as friends to your site if you know them in real life
- Do not post anything which harm to your family credibility
- Be aware that the information you give in the sites could also put you at risk of victimization
- Change your passwords frequently



కాపీరైట్ అనేది ఒకరు చేసిన స్వీయపనిని రక్షించే చట్టం. ఇది సాహిత్య, నాటకీయ, సంగీత, కళాత్మక మరియు కొన్ని ఇతర సృజనాత్మక రచనలకు సంబంధించినటువంటిది. వీటిని ఎక్కడైనా వాడుకున్నందుకు మనం కొంత మూల్యం చెల్లించాల్సి ఉంటుంది. కాపీరైట్ చట్టం ఏ వయస్సులో ఉన్న వారికైనా వర్తిస్తుంది. మనకి తెలియకుండానే చట్టాన్ని ఉల్లంఘించడం చాలా సులభం, చింటూ కాపీరైట్ల గురించి అతని స్నేహితుడికి అర్థమయ్యేలా ఎలా వివరిస్తున్నాడో చూద్దాం.

చింటూ తన కంప్యూటర్లో ఏదో టైపు చేస్తున్నాడు.





చిట్కాలు:

- నువ్వు చట్టాన్ని ఉల్లంఘించలేదని ముందుగా నిర్ధారించుకో
- కంటెంట్ యజమానికి క్రెడిట్‌లను ఎల్లప్పుడూ పేర్కొనండి.
- ఉపయోగించే ముందు నిబంధనలు మరియు షరతులను చదవడం మరచిపోవద్దు.
- రచయిత హక్కులను గౌరవించండి



BACKUP your files while working and store them in a separate location

సంస్కృతి మనకు ఒక గుర్తింపును ఇస్తుంది, మన ప్రవర్తనలను ప్రభావితం చేస్తుంది మరియు సాంస్కృతిక ప్రైవిడ్జ్యం మనల్ని ఇతర సంస్కృతులను కొంతవరకు అర్థం చేసుకునేలా చేయడం కాకుండా అంగీకరించేలా కూడా చేస్తుంది. పిల్లలు విభిన్న సంస్కృతులను అంగీకరించడం చాలా ముఖ్యం ఎందుకంటే ఇది పాఠశాలలో సమస్యలకు, బెదిరింపులకు కూడా దారితీస్తుంది. ఇతరుల సంస్కృతిని అర్థం చేసుకోవడం మరియు గౌరవించడం యొక్క విలువను మహిష్ తన సోదరికి అర్థం అయ్యేలా ఎలా చెప్పాడో చూద్దాం.

తన నమ్మకానికి సంబంధించిన కోట్ను పంచుకోవాలనుకుంటున్న మిస్సా తన ఫ్రెండ్ మిక్కు తిరిచింది.



ఆమె సోదరుడు మహిష్ అక్కడికి వచ్చాడు.

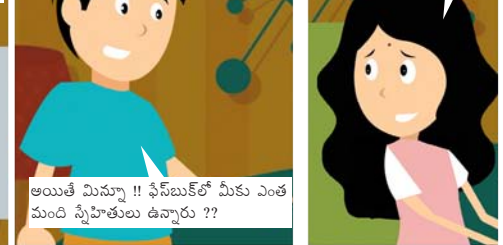


హయ్, మిస్సా.. ఏం చేస్తున్నావ్.

హయ్ మహిష్ !! నమ్మకాలు మరియు వాస్తవాలపై ఈ కోట్ను నా ఫ్రెండ్ మిక్కు తో పంచుకోవడానికి నేను నా ఫ్రెండ్ మిక్కు తిరిచాను ...

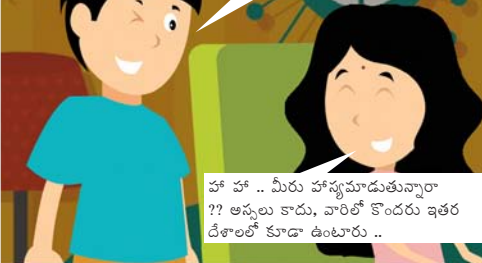


సుమారుగా 400 మంది ఉన్నారు మహిష్



అయితే మిస్సా !! ఫ్రెండ్ మిక్కు ఎంత మంది ఫ్రెండ్లు ఉన్నారు ??

వాళ్ళంతా ఒకే వ్రాంతం వారేనా??

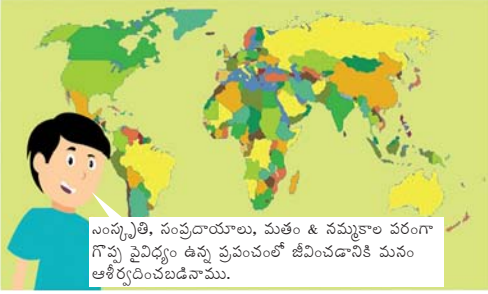


హా హా .. మీరు హాస్యమాడుతున్నారా ?? ఆస్యలు కాదు, వారితో కొందరు ఇతర దేశాలలో కూడా ఉంటారు ..

అలాంటప్పుడు నీ అభిప్రాయాలను మరియు నమ్మకాలను పంచుకోవడం వారికి బాధ కలిగించవచ్చు అవునా! ?



ఏమిటి? అలా ఎలా జరుగుతుంది ??



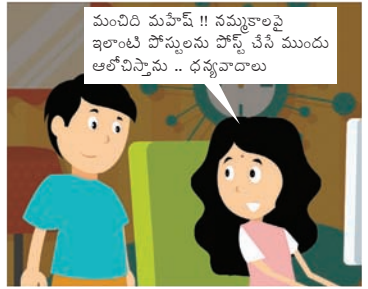
సంస్కృతి, సంప్రదాయాలు, మతం & నమ్మకాల పరంగా గొప్ప వైవిధ్యం ఉన్న ప్రపంచంలో జీవించడానికి మనం ఆశీర్వదించబడినాము.



మన వని, అధ్యయనంలో భాగంగా లేదా ఇంటర్నెట్ ఉపయోగిస్తున్నప్పుడు ప్రపంచవ్యాప్తంగా వారి వారి స్వంత సంప్రదాయాలు, మతాలు, సంస్కృతులు మరియు నమ్మకాలను కలిగి ఉన్న వ్యక్తులతో మనం సంభాషిస్తాము.



ఇంటర్నెట్ అందుబాటు అంది ప్రతి ఒక్కరికీ సరైనది ఇంకా అది వారి హక్కు కూడా కనుక, ప్రపంచవ్యాప్తంగా అనుసంధానించబడిన ఈ సెట్‌వర్క్ లో భాగంగా మనం ఇతరుల విలువలను, వారి నమ్మకాలను గౌరవించాలి.



మంచిది మహిష్ !! నమ్మకాలపై ఇలాంటి ధోస్తలను ధోక్త చేసే ముందు ఆలోచిస్తాను .. ధన్యవాదాలు

చిట్కాలు:

- మీ స్వంతమైనదే కాకుండా చాలా భిన్నమైన సంస్కృతులు ఉన్నాయని అంగీకరించండి.
- విభిన్న సంస్కృతుల గురించి తెలుసుకోవడానికి ఎప్పుడూ సుసేర్దులుగా ఉండండి
- వివిధ జాతులు, సంస్కృతులు మరియు మతాల నుండి స్నేహితులను సంపాదించడానికి ప్రయత్నించండి.
- ఇతరుల సంస్కృతి నుండి సానుకూల అంశాలను మాత్రమే అంగీకరించండి.
- మీ అభిప్రాయం లేదా నమ్మకాన్ని ఇతరులపై బలవంతంగా రుద్దకండి.

Possible Threats in WhatsApp

ఆన్లైన్ రాబందులు పిల్లలు మరియు టీనేజర్లను త్రింగిక మరియు హింసాత్మక ప్రయోజనాల కోసం దోపిడీ చేసే ఇంటర్నెట్ వినియోగదారులు. ఇందులో పిల్లల వస్త్రధారణ, త్రింగిక కార్యకలాపాల్లో పాల్గొనడం, ఫోటోలను, సమాచారాన్ని అవాంఛితంగా బహిష్కరణ చేయడం, ఆన్లైన్ వేధింపులు, భయం లేదా ఇబ్బంది కలిగించే బెదిరింపులు ఉండవచ్చు. ఒక ఆన్లైన్ ప్రాజెక్టు/రాబందు రిటూను ఎలా వేధించాడో చూద్దాం.

రిటూ 7 వ తరగతి చదువుతోంది, ఆమె ఆన్లైన్ చాట్ లో ఒక అవరచితుడిని కలుసుకుంది

ఆమె ఒక సంవత్సరం పాటు అతనితో చాలాసార్లు చాట్ చేసింది, తన వ్యక్తిగత సమాచారం, ఫోటోలు మరియు వీడియోలను కూడా అతనితో పంచుకుంది

ఒక సంవత్సరం తరువాత, ఆ వ్యక్తి ఆమెను సోషల్ నెట్వర్కింగ్ సైట్లో సప్రదించాడు

మీ తల్లిదండ్రులకు తెలియకుండా నన్ను ఒంటరిగా కలుపు, తీకపోతే మీ ప్రైవేట్ ఫోటోలను ఆన్లైన్లో అందరికీ విడుదల చేస్తాను.

నీ వ్యక్తిగత వివరాలు, మీ ఇల్లు, మీ పాఠశాల మరియు నీ స్నేహితులు నాకు తెలుసు.

ఆమె అతన్ని కంప్యూటింగ్ నిరాకరించడంతో, అతను ఆమె ఫోటోలను ఇంటర్నెట్ లో పోస్ట్ చేసాడు.

ఆమె తీవ్ర నిరాశకు గురై ఒంటరిగా ఉండిపోయింది.

ఆమె క్లాస్మేట్స్, స్నేహితులు ఆమెను బెదిరించడం, విస్మరించడం ఆమె గురించి మాట్లాడటం ప్రారంభించారు.

తన స్నేహితులు ఆమెను ఎలా విమర్శించారో ఆమె తన అంతర్గత భావాలను వెల్లడిస్తూ ఒక వీడియోను పోస్ట్ చేసింది.



ఆమె మునుపటి పాఠశాల నుండి బాలికలు ఆమె ప్రస్తుతం చదువుతున్న పాఠశాలకు వచ్చి తోటి విద్యార్థులు చూస్తూ, వీడియో తీస్తుండగా ఆమెను కొట్టారు...



ఆమె కష్టం మీద తను రోడ్డుపైకి పెళ్ళి మార్గాన్ని కనుగొనగలిగింది, అక్కడ ఆమె రోడ్డు పక్కన పడుకుని ఉండగా ఆమె తండ్రి చూసాడు



ఇంటికి తిరిగి వచ్చిన తరువాత ...ఆమె తన తండ్రికి అన్నీ వివరిస్తుంది.



దీనిపై సైబర్ పోలీసులకు ఫిర్యాదు చేద్దాం ...

తరువాత, రీటా మరియు ఆమె తండ్రి సైబర్ పోలీసులను సంప్రదించి ఫిర్యాదు చేసారు.



ఆమెను పేధించిన అవరిచితుడిని గుర్తించి తన సేరానికి అతనిపై కేసు నమోదు చేశారు...

చిట్కాలు:

- మీ ఆన్లైన్ అనుభవాల గురించి మీ తల్లిదండ్రులతో ఓవెన్ గా, నిజాయితీగా సంభాషణలు జరపండి/మాట్లాడండి.
- చాలా వ్యక్తిగతంగా ఉండాలనుకునే వారితో మాట్లాడకండి.
- వ్యక్తులు వారు ఎవరో, ఏమిటో ఎల్లప్పుడూ నిజాలు చెప్పరని గుర్తుంచుకోండి.
- ఫోన్ నంబర్లు, అడ్రసులు, పాఠశాల పేరు లేదా ఇతర వివరాలను ఎప్పుడూ పోస్ట్ చేయవద్దు
- అవరిచితుల నుండి ఎలాంటి బహుమతిని లేదా వస్తువులను ఎప్పుడూ అంగీకరించవద్దు.

IF YOU ARE THREATENED

Don't be scared to say no

If you are not willing to do things asked by predator don't be scared to say no

Inform to parents

If some one threatens you, immediately inform your parents

Don't fear

Be cool, stop chatting and get out of the chat room or log off

Contact cyber police

If someone threaten to harm family members, immediately contact cyber police

Don't log off

If someone tries to abuse you don't logoff immediately, inform parents

తక్షణ సందేశం (IM) ఇంటర్నెట్ ద్వారా అప్పటికప్పుడే నిజ సమయంలో 'చాట్' చేయడానికి మిమ్మల్ని అనుమతిస్తుంది. దూరంగా ఉన్న కుటుంబ సభ్యులు, స్నేహితులతో మాట్లాడడానికి గొప్ప సాధనం, కానీ దీంతో మీరు ఎల్లప్పుడూ జాగ్రత్తగా ఉండాలి. చింటూ తక్షణ సందేశ అనువర్తనం లేదా యాప్ ద్వారా అపరిచితులతో చాట్ చేసినప్పుడు ఏమి జరిగిందో చూద్దాం.



చింటూ క్రీడలలో చాలా మరుకుగా ఉండేవాడు, పాఠశాల మైదానంలో క్రమం తప్పకుండా ఫుట్ బాల్ ఆడేవాడు



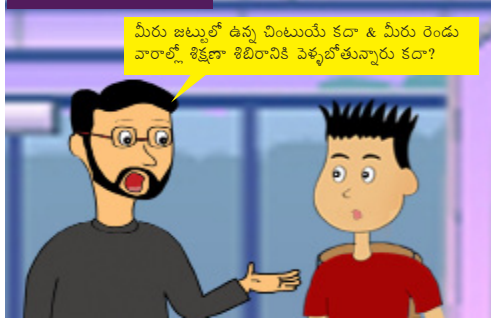
ఒక రోజు ఉదయం, ఫుట్ బాల్ శిక్షణ ముగిసిన తరువాత అతను బస్ స్టాప్ వద్ద వేచి ఉన్నాడు

అకస్మాత్తుగా ఒక వ్యక్తి వచ్చి అతనితో మాట్లాడటం మొదలుపెట్టాడు. ఆ వ్యక్తి అతని పేరు చింటూనా అని అడిగాడు. చింటూ అవును అని సమాధానం ఇచ్చాడు మరియు చింటూ అతనిని అడిగాడు



నా పేరు మీకు ఎలా తెలుసు??

ఆ వ్యక్తి సమాధానం ఇచ్చాడు.



మీరు జబ్బులో ఉన్న చింటూయే కదా & మీరు రెండు వారాల్లో శిక్షణా శిబిరానికి పెళ్ళబోతున్నారు కదా?

చింటూ ఆశ్చర్య పోయాడు, కానీ అతను ఆ వ్యక్తితో ఫుట్ బాల్ గురించి చర్చించడం ప్రారంభించాడు



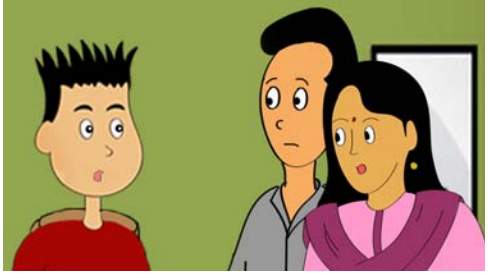
కొద్దిసేపటి తరువాత, ఆ వ్యక్తి చాలా దగ్గరగా వచ్చాడు ఇంకా అకస్మాత్తుగా తన మొబైల్ నంబర్ & వ్యక్తిగత సమాచారాన్ని అడగడం మొదలుపెట్టాడు.



అదృష్టవశాత్తూ, చింటూ పాఠశాల బస్సు రావడంతో చింటూ బస్సు ఎక్కడానికి వెళ్లాడు, ఆ అవరచితుడు బస్సును చూసి పారిపోయాడు



చింటూ తన తల్లిదండ్రులకు ఏమీ జరిగిందో వివరించాడు ... మాట్లాడుతున్నప్పుడు కొద్ది రోజుల క్రితం అతను క్రీడలపై ఆసక్తి ఉన్న మరో అబ్బాయిలో చాట్ చేస్తున్నాడని గుర్తు చేసుకున్నాడు ..



వారు ఫుట్బాల్ గురించి చర్చించేవారు. వాళ్ళు చూడానికి ఎలా ఉంటారో తెలుసుకోవాలని అనుకున్నారు. ఒకరినొకరు ముందే చూస్తే అప్పుడు క్యాంపులో గుర్తు పట్టడం సులువవుతుందని కూడా అనుకున్నారు.



చింటూ, అతని తల్లిదండ్రులు కలిసి చాట్ సెషన్ ఆ వ్యక్తి బస్ స్టాప్ వద్ద ఉండటానికి కారణం అయిందని గ్రహించారు. వారు ఈ సేనాన్ని పోలీసులకు నివేదించారు.



చిట్కాలు:

- మీ ప్రైవేట్ మరియు వ్యక్తిగత సమాచారాన్ని ఎవరికీ వెల్లడించవద్దు ..
- మీరు చాటింగ్ చేసే వ్యక్తులతో జాగ్రత్తగా ఉండండి.
- మీకు తెలియని వ్యక్తి పంపిన వెబ్ లింక్లపై క్లిక్ చేయకండి, తెలియని వ్యక్తులు పంపిన అటాచ్మెంట్లను ఓపెన్ చేయద్దు.
- మీ తక్షణ సందేశం యాప్ ను క్రమం తప్పకుండా అప్ డేట్ చేస్తుండండి/నవీకరించండి.
- ప్రొఫైల్ ఫోటో ఆప్షన్ ఖాళీగా ఉంచడం మంచిది.



ఇమెయిల్ అకౌంట్ హాక్ చేయడం



ఈ రోజుల్లో అందరికీ ఇమెయిల్ ఖాతా ఉంటోంది. ఇమెయిల్ ఖాతాను సృష్టించడానికి స్వస్థమైన వయో పరిమితులు లేవు. మీలో చాలామంది ఇమెయిల్ ఖాతాను సృష్టించడం ద్వారా ఇంటర్నెట్ ప్రపంచంలోకి ప్రవేశించి ఉండవచ్చు. కానీ దీనివల్ల కూడా చాలా ప్రమాదాలు ఉన్నాయి అని మీరు తెలుసుకోవాలి. సోనీ ఇమెయిల్ ఖాతాతో ఏమి జరిగిందో చూద్దాం.

సోనీ ఒక ప్రసిద్ధ అంతర్జాతీయ పాఠశాలలో (ఇంటర్నెషనల్ స్కూలు) ఉపాధ్యాయురాలు.

ఆమె పిల్లల రికార్డులు పాఠశాల సంబంధిత పత్రాలు, పిల్లల ఫ్రోగ్రెస్ షీట్స్ ని క్రమం తప్పకుండా చదవ్వవేక్షించేది మరియు ఆమెకు కొత్త బిక్రాంజింను నేర్చుకునే అలవాటు కూడా ఉంది .

ఒక రోజు ఉదయం, ఆమె పాఠశాల ప్రిన్సిపాల్ నివేదికలను ఒక క్లిక్తో స్వయంచాలకంగా ట్రాక్ చేసి పరిష్కారాన్ని పేర్ను డాన్లోడ్ చేసింది.

ఒక రోజు ఆమెకు తన స్నేహితుడి నుండి కాల్ వచ్చింది..

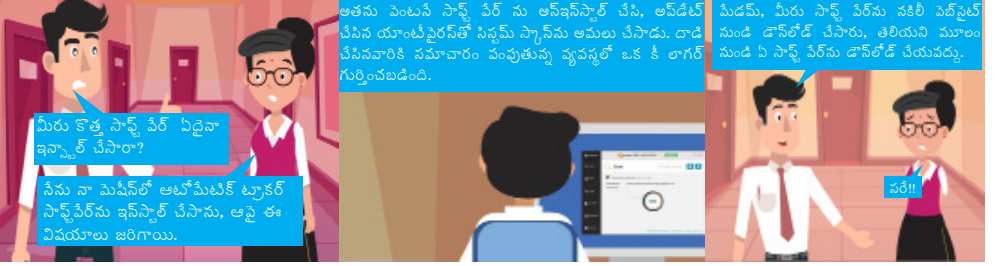
సోనీకి తన బంధువులు, స్నేహితుల నుండి తన ఆర్థిక అవసరం గురించి చాలా కాల్స్ వచ్చాయి.

ఆమె తన ఇమెయిల్ ఖాతాను తనిఖీ చేసిన తర్వాత ఆమె షాక్ అయ్యింది.

అప్పుడు ఆమె వెంటనే ఈ సమస్య గురించి సైబర్ పోలీసుల వద్ద కేసు నమోదు చేసింది.

ఈ విషయం గురించి ఆమె వారి ఐటి సపోర్ట్ టీంను సంప్రదించింది.

ఆమె కంప్యూటర్ల ద్వారా అనుమానాస్పద ప్రక్రియ నడుస్తుందా అని ఐటి బృందం నిశితంగా పరిశీలించింది. ఆమె యాంటీవైరస్ సాఫ్ట్ వేర్ & డెస్క్ టాప్ షిల్డ్ వాల్ నిలిపివేయబడిందని వారు కనుగొన్నారు.



చిట్కాలు:

- మీ మెయిల్ అకౌంట్ వివరాలను అపరిచితులకు ఇవ్వవద్దు.
- మీరు మీ ఇమెయిల్‌ను తనిఖీ చేసిన తర్వాత లాగ్ అవుట్ చేసి అలవాటు చేసుకోండి
- స్కామ్ లేదా ఫ్యార్యార్డ్ చైన్ ఇమెయిల్‌లకు రిప్లై ఇవ్వవద్దు.
- అపరిచితుల నుండి వచ్చిన ఇమెయిళ్ళను అనుమానాస్పద మైనవిగా చూడండి.
- మీరు యాప్/అనువర్తనాన్ని డౌన్‌లోడ్ చేయడానికి ముందు అనువర్తనం యొక్క సమీక్షలను తనిఖీ చేయండి మరియు మూడవ పార్టీ సోఫ్ట్ నుండి అనువర్తనాలను డౌన్‌లోడ్ చేయడంలో జాగ్రత్తగా ఉండండి.

Safety tips for blogging

Check out what your friends write about you.

Keep identifying details to yourself and close friends

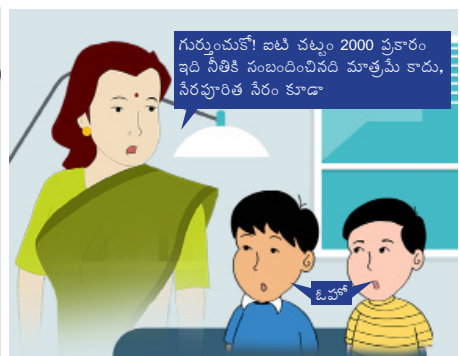
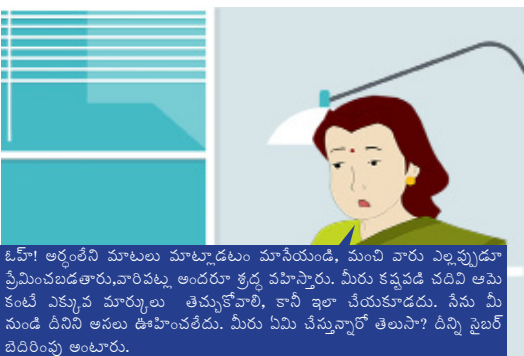
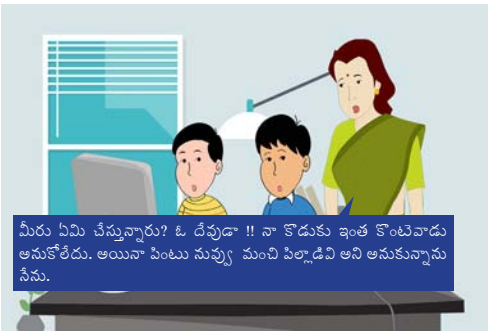
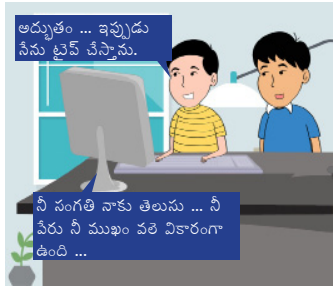
If you think there's a problem, report it immediately.

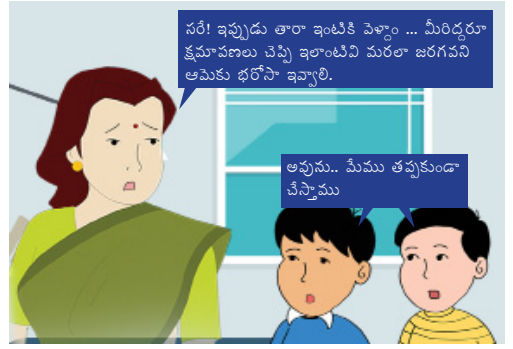
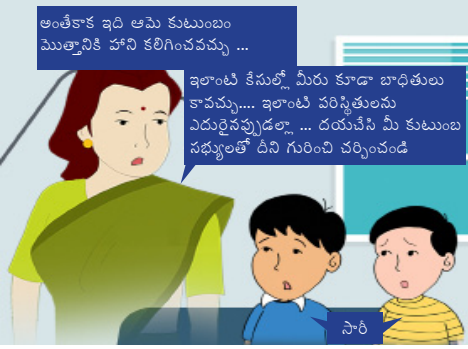
Be careful about sharing your feelings in your blog

Think carefully about how public your blog is

Be smart about the photos you post

సైబర్ బెదిరింపు అనేది ఒక వ్యక్తిని వేధించడానికి, బెదిరించడానికి, ఇబ్బంది పెట్టడమే లక్ష్యంగా చేసుకోవడానికి సాంకేతిక పరిజ్ఞానాన్ని ఉపయోగించడం. సరళంగా చెప్పాలంటే, ఇది ఆన్‌లైన్‌లో జరిగేది. పేరొకరిని బాధపెట్టడం, వేధించడం లేదా ఆందోళనకు గురి చేయడం. సైబర్ బెదిరింపు గురించి చింటు తల్లి అతనికి ఎలా వివరిస్తుందో ఇప్పుడు చూద్దాం.





చిట్కాలు:

- ఒకే విధంగా స్పందించవద్దు లేదా ప్రతీకారం తీర్చుకోకండి.
- సాక్ష్యాలను సేవ్ చేయండి.
- ఇకపై ఇలాంటి పనులు ఎప్పుడూ చేయమని, ఏ బెదిరింపులకు పాల్పడమని నమ్మకంతో ఉండండి.
- మీకు నమ్మకమైన వెద్దలతో మాట్లాడండి
- బెదిరింపు ముఠాలో చేరి వైబర్ రౌడీగా ఉండకండి.

BEST PRACTICES & GUIDELINES FOR STRENGTHENING YOUR BROWSING SECURITY



సైబర్ స్టాకింగ్ ఆన్లైన్ స్టాకింగ్ అని నిర్వచించబడింది. ఇది ఒక వ్యక్తిని లేదా సమూహాన్ని భయపెట్టడానికి లేదా బాధపెట్టడానికి ఇంటర్నెట్ లేదా ఇతర ఎలక్ట్రానిక్ మార్గాలను పడిపడి ఉపయోగించడం. సైబర్ స్టాకింగ్లో మిమ్మల్ని భయపెట్టడానికి ఇమెయిల్, తక్షణ సందేశాలు, ఫోన్ కాల్స్ మరియు ఇతర కమ్యూనికేషన్ మోడ్లను ఉపయోగించవచ్చు.

జావీయా ఒక ఎన్ఆర్ఐ, యుఎస్ నుండి పాఠశాల విద్యను పూర్తి చేసింది మరియు ఇప్పుడు భారతదేశంలో ఆమె ఇంజనీరింగ్ చదువుతోంది. ఆమె తన జీవితాన్ని పూర్తిస్థాయిలో గడిపింది.



ఆమె ఏమి చేసినా, సోషల్ మీడియాలో ఆన్లోడ్ చేసింది. ఓహో, ఆమెకు 10 పేజీల వైగా అనుచరులు ఉన్నారు



ఆమె తన జీవితం మరియు కనీస గోప్యత గురించి ఆమె స్నేహితులు, అనుచరులకు తెలియజేయడానికి తన ఫేస్ బుక్ లోని ఫీచర్ ను తనిఖీ చేస్తుంది.



ఒక రోజు, ఆమె గోవాకు ఒంటరిగా ట్రిప్ వెళ్ళాలని నిర్ణయించుకుంటుంది. ఆమె తన ఫేజ్ బుక్ తన ప్రణాళికలను ప్రయాణ వివరాలతో సవరిస్తుంది.



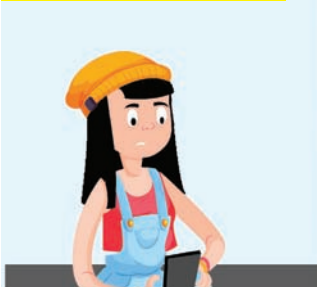
కిరణ్ అనే స్టాకర్ ఆమె వివరాన్నింటినీ బ్రాక్ చేసేవాడు. అతను ఇలాంటి వాటికి అలవాటుపడి, ఇటీవలే బెయిల్ మీద వచ్చిన అవరాధి.



అతను బస్సులో గోవాకు చేరుకొని తన హోటల్ గది నుండి జావీరియాను కలవాలనే కోరికను వ్యక్తం చేస్తూ ఆమెకు వ్రాసాడు



అతని ప్రొఫైల్ తనిఖీ చేసిన తర్వాత, తన వెబుక్ ఏమి ప్లాన్ జరుగుతుందో తెలియని జావీరియా అతన్ని వెంటనే బ్లాక్ చేసింది.



కిరణ్ ఆమె ప్రయాణవివరాలను ముందే సేకరించి ఉన్నందున, అతను ఆమెను బీచ్ దగ్గర అనుసరిస్తాడు ఇంకా చుట్టూ ఎవరూ లేనప్పుడు ఆమెను పేదించి అక్కడనుండి పారిపోతాడు.



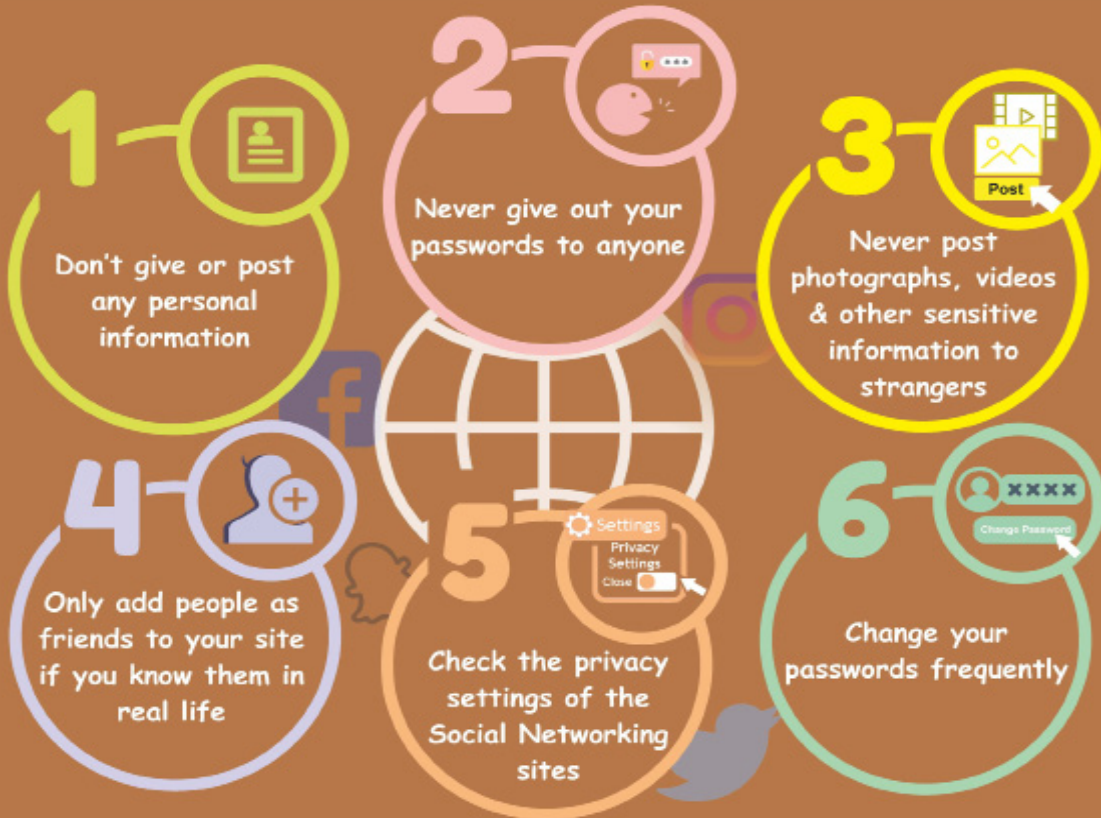
భయపడేపోయిన జావీరియా తన చిత్రాలను గోప్యంగా ఉంచనందుకు సోషల్ మీడియాలో తన వివరాలు మరియు ఇతర సంబంధిత పోస్టులను తనిఖీ చేయనందుకు విచారస్తుంది.



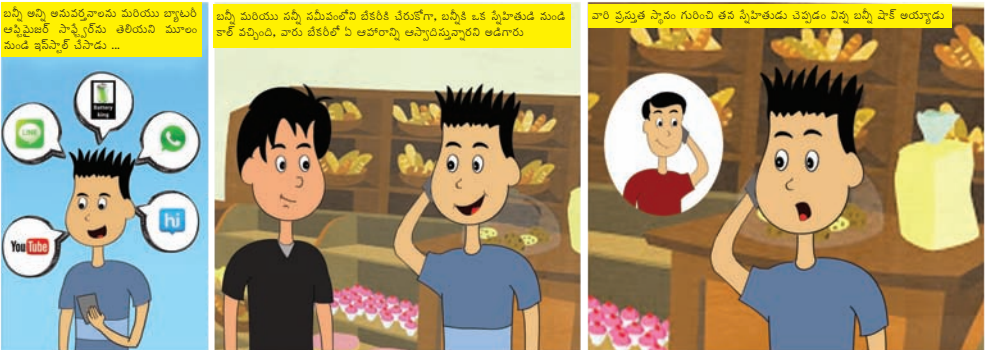
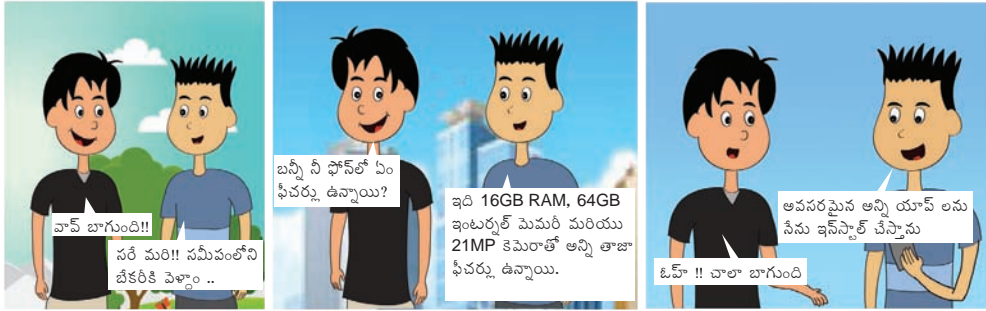
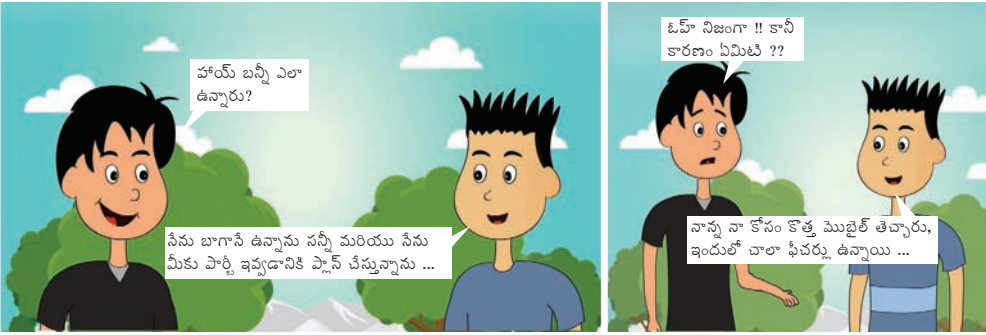
చిట్కాలు:

- ఆన్‌లైన్ లో మీ సమాచారం ఏమిటో సమీక్షించండి వీలయినంత తక్కువ సమాచారం ఉంచండి.
- మీ గోప్యత, భద్రతా సెట్టింగ్‌లను అన్నిటిని సమీక్షించండి
- మీరు హాజరయ్యే ఈవెంట్లు వివరాలను బహిరంగంగా పంచుకోవడం గురించి జాగ్రత్తగా ఉండండి
- మీ తల్లిదండ్రులకు స్టాకింగ్ గురించి చెప్పండి. పోలీసులకు రిపోర్ట్ చేయమని వారిని అడగండి
- నవీకరించబడిన యాంటీవైరస్ సాఫ్ట్‌వేర్‌ను మాత్రమే ఎప్పుడూ ఉపయోగించండి.

Guidelines for Social networking



ఈ రోజుల్లో ముబైల్ ఫోన్‌ను ఎలా ఉపయోగించాలో తెలియని పిల్లవాడిని కనుగొనడం కష్టం. ఇది అందించే పైఖరులు, సామర్థ్యాలు మరియు వినోదం కాకుండా మీరు బాధ్యత వహించాల్సిన అవసరం ఉందని మరియు సురక్షితంగా ఉండటానికి కొన్ని నియమాలు భద్రతా చర్యలను అనుసరించాలని మీరు తెలుసుకోవాలి. బట్టి తన కొత్త ముబైల్ ఫోన్‌లో చాలా తెలియని యాప్స్ ఇన్‌స్టాల్ చేసినప్పుడు ఏమి జరిగిందో చూద్దాం.

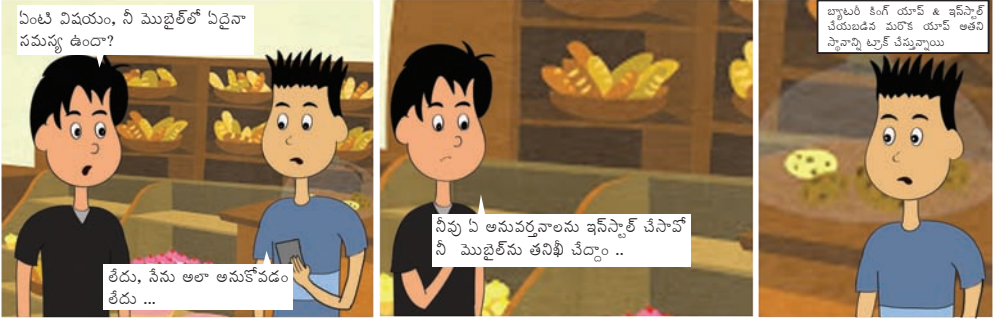


బట్టి అన్ని అవసరాలను మరియు బ్యాటరీ ఆప్టిమైజర్ సాఫ్ట్వేర్ను తిరియని మూటం నుండి ఇన్‌స్టాల్ చేసాడు ...

బట్టి మరియు బట్టి సమీపంలోని బేకరీకి చేరుకోగా, బట్టికి ఒక ఫ్రీహాతుడి ముడి కార్ వచ్చింది, వారు బేకరీలో ఏ ఆహారాన్ని ఆస్వాదిస్తున్నారని అడగారు

వారి ప్రస్తుత స్థానం గురించి తన ఫ్రీహాతుడు చెప్పడం చివ్వి బట్టి షాక్ అయ్యాడు

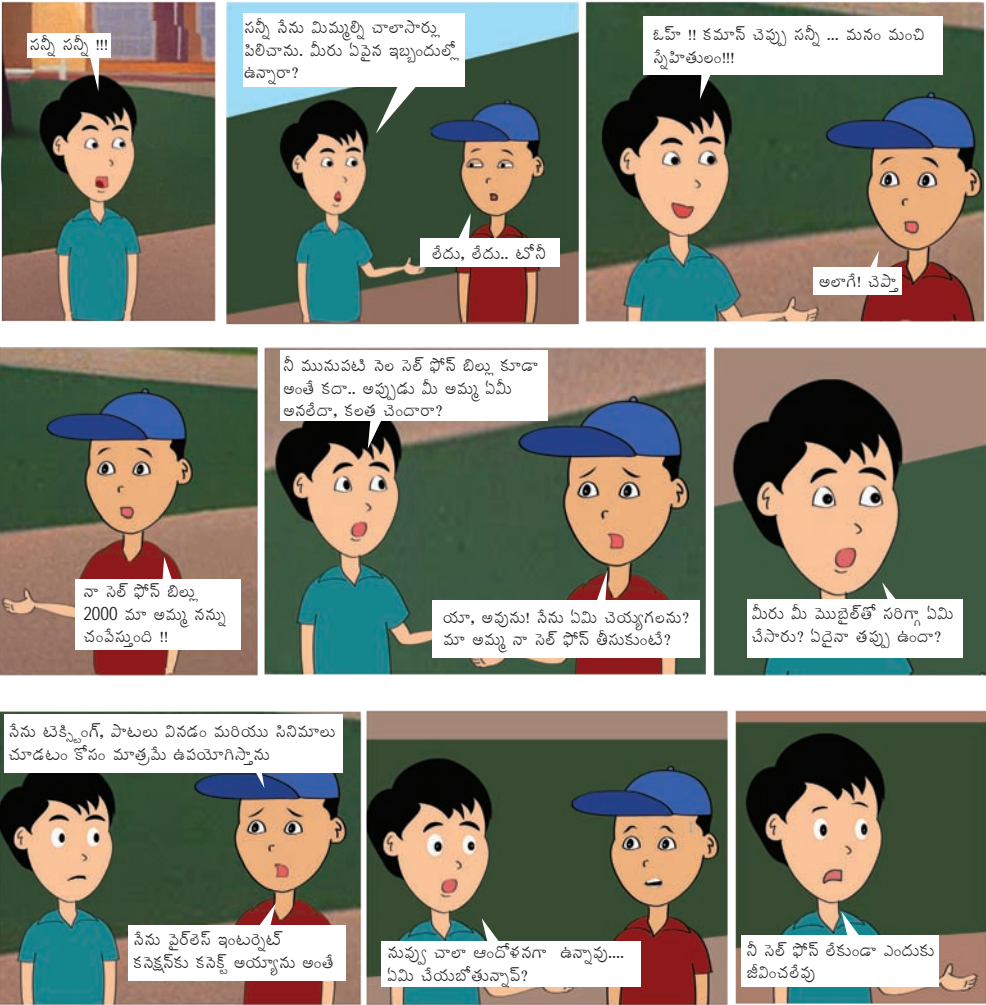




చిట్కాలు:

- మొబైల్ ఆపరేటింగ్ సిస్టమ్ ను క్రమం తప్పకుండా నవీకరించండి.
- ఆపరేటింగ్ సిస్టమ్ ను దాని తాజా వెర్షన్ కు అప్ గ్రేడ్ చేయండి.
- విశ్వసనీయ మూలాల నుండి అనువర్తనాలను ఎల్లప్పుడూ ఇన్స్టాల్ చేయండి.
- పేరున్న ప్రొవైడర్ నుండి భద్రతా సాఫ్ట్ వేర్ ను ఇన్స్టాల్ చేయడానికి మొగ్గు చూపండి. వాటిని క్రమం తప్పకుండా నవీకరించండి.
- అనువర్తనాన్ని డౌన్ లోడ్ చేయడానికి ముందు దాని ఫీచర్లను తనిఖీ చేయడం ఎప్పుడూ శ్రేయస్కరం. కొన్ని అనువర్తనాలు/యాప్స్ మీ వ్యక్తిగత డేటాను ఉపయోగించవచ్చు.
- మీరు మూడవ పక్షం నుండి అనువర్తనాన్ని డౌన్ లోడ్ చేస్తుంటే, అది మంచి పేరున్నదా లేదా అని నిర్ధారించుకోవడానికి కొద్దిగా పరిశోధన చేయండి.

నిజమైన వ్యక్తులతో సంభాషించడానికి బదులుగా సోషల్ మీడియాను ఉపయోగించడం లేదా ఆటలను ఆడటం కోసం మీరు మీ మొబైల్ తో ఎక్కువ సమయం గడిపినప్పుడు, మీ జీవితంలో ప్రతికూల పరిణామాలు ఎదురైనప్పుడు కూడా, ఇమెయిల్ లు లేదా అనువర్తనాలను వదలవడం తనిఖీ చేయకుండా మీరు ఆపలేరు. దీన్ని మొబైల్ ఫోన్ వ్యసనం అని పిలుస్తారు. మొబైల్ ఫోన్ కు బానిస అయినప్పుడు సన్నిధి ఏమి జరిగిందో చూద్దాం.



చిట్కాలు:

- మీ మొబైల్ ఫోన్‌ను ఉపయోగించడానికి పరిమితులను సెట్ చేయండి
- పడుకునే ముందు ఫోన్ ఆఫ్ చేయండి
- అనవసరమైన యాప్స్/అనువర్తనాలను తొలగించు.
- మీరు మాట్లాడుతున్న వ్యక్తిపై దృష్టి వెట్టడం మంచిది.
- తిసిటప్పుడు మొబైల్ వాడటం మానుకో.





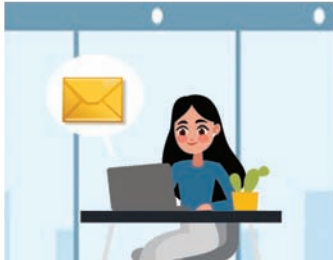
రాన్సమ్ వేర్



రాన్సమ్ వేర్ అనేది ఒక రకమైన హానికరమైన సాఫ్ట్ వేర్, క్రయధనం చెల్లించే వరకు కంప్యూటర్ సిస్టమ్ తీదా డేటా అందుబాటును తిరస్కరించడానికి రూపొందించబడింది. రాన్సమ్ వేర్ సాధారణంగా ఫిషింగ్ ఇమెయిల్ల ద్వారా తీదా తెలియకుండా ఫైరెస్ సోకిన వెబ్ సైట్లను సందర్శించడం ద్వారా వ్యాపిస్తుంది. రాన్సమ్ వేర్ అతీషా ల్యాప్ టాప్ ను ఎలా ప్రభావితం చేసిందో చూద్దాం.



అతీషా ఒక వ్యవస్థాపకురాలు/పారిశ్రామిక పిత్ర. ఆమె సంస్థలో 50 మంది ఉద్యోగులు & 60 కంప్యూటర్స్ ఉన్నాయి



ఒక రోజు, ఆమె తన విక్రీత నుండి అటామ్మెట్ కలిగి ఉన్న ఇమెయిల్ ను అందుకుంటుంది



అతీషా అటామ్మెట్ ను డౌన్ లోడ్ చేస్తుంది. ఆమె యాంటీ ఫైరెస్ నవీకరించబడలేదు, కాబట్టి ఎలాంటి హెచ్చరికలు లేవు



ఫైర్ ను తెరిచిన తర్వాత, ఆమె సిస్టమ్ లాక్ అవుతుంది మరియు అన్ని ఫైల్స్ గుప్తీకరించబడతాయి. యాక్సిస్ చేయలేకపోయింది



స్కీన్ పై ఒక హెచ్చరిక సందేశం స్క్రీన్ ను అన్ లాక్ చేయడానికి బిట్ కాయిన్ లో లక్ష రూపాయలు చెల్లించాలని కోరుతుంది



అతీషా ఇవ్వబడిన బిట్ కాయిన్ వాలెట్ చిరునామాకు చెల్లింపు చేస్తుంది



హ్యాకర్ ఫైల్ లో కీని పంపలేదు, ఫైల్స్ గుప్తీకరించబడ్డాయి (రహస్యలిపిలోకి మార్చబడినాయి) అందుబాటులో లేవు



తనకు వచ్చింది రాన్సమ్ వేర్ తో ఉన్న ఫిషింగ్ ఇమెయిల్ అని ఆమె కంపెనీ మేనేజర్ అతీషాకు తెలివిచ్చాడు.

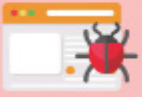


ఇమెయిల్ ను తొలగించకపోవడం, యాంటీ ఫైరెస్ మరియు ఆపరేటింగ్ సిస్టమ్ ను అప్ డేట్ చేయనందుకు అతీషా బాధ పడింది.

చిట్కాలు:

- మొట్టమొదట, మీ అతి ముఖ్యమైన వైళ్ళను రోజూ బ్యాకప్ చేయండి.
- అనుమానాస్పదంగా కనిపించే అటాచ్మెంట్లను తెరవడం మానుకోండి.
- ఫ్లోక్ చేయడానికి ముందు రెండుసార్లు ఆలోచించండి.
- సేరస్థలచే బలవంతంగా ఓపెన్ చేయలేని బలమైన పాస్వర్డ్లను ఉపయోగించండి.
- విండోస్ ఫైర్వాలను ఎప్పుడు ఆన్ చేసి, ప్రతిసారి సరిగ్గా కన్ఫిగర్ చేయండి.

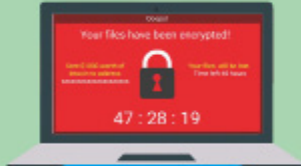
STAGES OF RANSOMWARE INFECTION



Visit suspicious Websites



Open suspicious emails



Files are encrypted



Data is lost

HOW TO PROTECT AGAINST RANSOMWARE



Do not open suspicious emails



Keep your Anti-virus up-to-date



Backup data frequently and keep them offline



Never click on Website links or ads



Install the latest patches for software



Disable macros for office applications

అపరిచితులు ఎల్లప్పుడూ ప్రమాదం. మీ తల్లిదండ్రులు మీకు నేర్పించిన మొదటి భద్రతా నియమం ఇదే కావచ్చు. కానీ ఇంటర్నెట్ & సోషల్ మీడియా మనల్ని రక్షించడానికి ఉపయోగించిన కొన్ని అడ్డంకులను కూల్చివేసింది. తన ఆన్లైన్ స్నేహితుడిని కలవాలనుకున్నప్పుడు రాజుకు ఏమి జరిగిందో చూద్దాం



ఒక ఆడవిలో... ఒక రోజు



రాజు తలుపు దగ్గరకు వెళ్ళాడు...

హలో !! అక్కడ ఎవరైనా ఉన్నారా ??

రఘు !!! మీరు అక్కడ ఉన్నారా ??



అప్పుడు అతను తన స్నేహితుడిని పిలుస్తాడు...

రఘు !!! తలుపు తెరవండి... సీను రాజుని !!!



అకస్మాత్తుగా, తలుపు తెరుచుకుంటుంది మరియు ఒక అపరిచితుడు అతనిని లోపలికి లాగుతారు....

తేడు!!! నన్ను వదిలేయండి!!!



తలుపు మూసివేయబడింది...

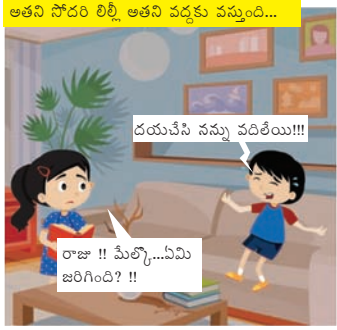


అతను ఇదంతా కల కన్నాడు మరియు అకస్మాత్తుగా బిగ్గరగా పలకడం ప్రారంభించాడు ...

నన్ను వదిలేయ!!!

దయచేసి నన్ను వదిలేయ!!!

నన్ను వదిలేయ!!!



అతని దొంగరి లిల్లి అతని వద్దకు వస్తుంది...

దయచేసి నన్ను వదిలేయ!!!

రాజు !! మీల్లో...ఏమి జరిగింది ??



నువ్వు కలలు కంటున్నావా ??



రాజు ... ఏమైంది...మీకు పీడకల గానీ వచ్చిందా??.



అవును నాన్న !! సీను నా ఆన్లైన్ స్నేహితుడు రఘుని కలవడానికి వెళ్ళాను

సీను తలుపు తట్టాను...ఎవరో నన్ను పట్టుకున్నారు...నాకు చాలా భయం వేసింది !!



అతను ఈ రోజు తన ఆన్లైన్ స్నేహితుడిని కలవడానికి వెళ్ళున్నాడు.

సీను అతనిని ఆపి, పెళ్ళి ముందు మీ అనుమతి కోరమని చెప్పాను

నేను మీ కోసం ఎదురు చూశాను డాడ్ !! నేను ఒక చిన్న కుమకు తీసేవరకు నాకు ఈ కల వచ్చింది!!



నీవు నీ ఆన్లైన్ స్నేహితుడిని కలవబోతున్నావా??



నీతో పాటు నీ తల్లిదండ్రులు లేదా పెద్దలతో మాట్లాడాలని నువ్వు అనుకున్నావా??

లేదు మమ్మా !!



అప్పుడు నువ్వు తప్పు చేస్తున్నట్లే కదా రాజు...



చిట్కాలు:

- మీరు నెట్‌వర్కింగ్ సైట్‌లో కలిసిన వ్యక్తిని కలవాలనుకుంటే మీ తల్లిదండ్రుల అనుమతి తీసుకోండి
- నిజ జీవితంలో మీకు తెలిస్తే మాత్రమే వారిని మీ సైట్‌కు స్నేహితులుగా చేర్పండి
- ఎవరైనా మీకు కోపం తెప్పిస్తే, రుజువు కోసం సందేశాలను స్క్రీన్‌షాట్ చేసి, ప్రొఫైల్‌గురించి రిపోర్ట్ చేయండి
- సైట్లలో మీరు ఇచ్చే సమాచారం కూడా మిమ్మల్ని బాధితులుగా చేసే ప్రమాదం ఉందని తెలుసుకోండి
- మీ పాస్‌వర్డ్‌ను తరచుగా మార్చండి



THINK BEFORE YOU POST

కొంతమంది ఇంటర్నెట్ వినియోగదారులు ఆన్లైన్ స్నేహితులు మరియు వారి కంప్యూటర్ స్క్రీన్లో వారు సృష్టించే కార్యకలాపాలవల్ల భావోద్వేగ అనుబంధాన్ని పెంచుకోవచ్చు. ఇది మీ జీవితంలో అభిరుచులు మరియు కార్యకలాపాల ఆరోగ్యకరమైన సమతుల్యతను నాశనం చేస్తుంది. ఇంటర్నెట్ ఉపయోగించడంలో చాలా ఆసక్తి ఉన్న విజయ్ కు ఏమి జరిగిందో చూద్దాం



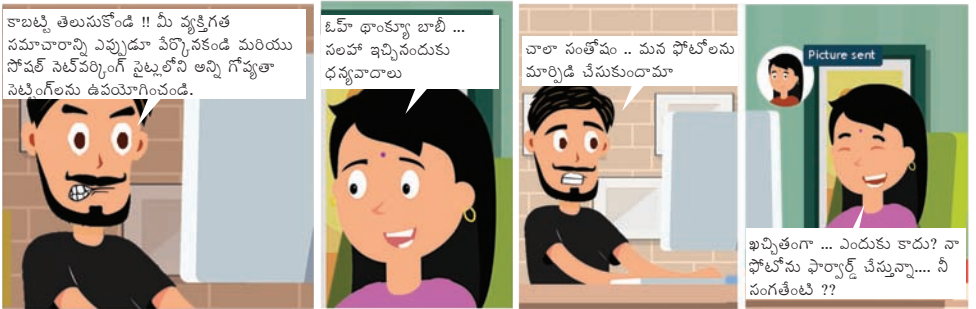
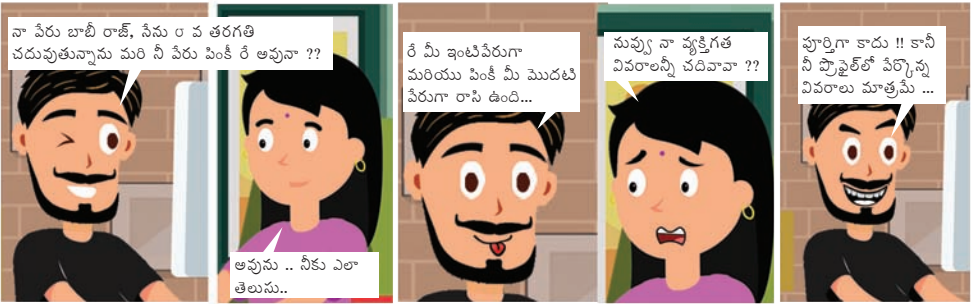
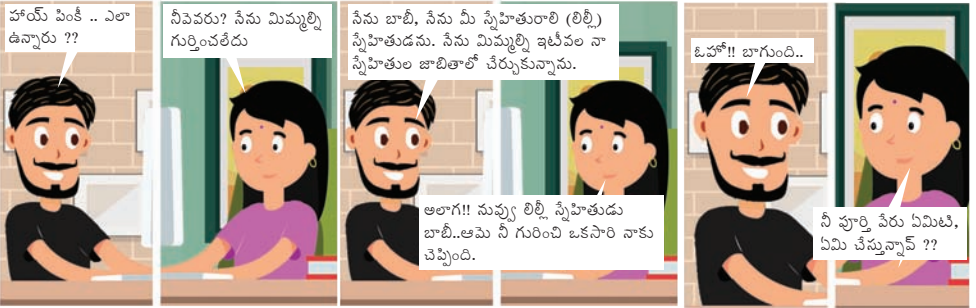
చిట్కాలు:

- మీరు ఆన్‌లైన్‌లో ఎక్కువ సమయం గడపవద్దు. ఆ సమయాన్ని పరిమితం చేయండి
- ఆటలు లేదా యాప్స్ తల్లిదండ్రుల / పెద్దల అనుమతి లేకుండా డౌన్‌లోడ్ చేయవద్దు, అవి ఉచితంగా ఉన్నప్పటికీ. ఆటలు లేదా యాప్స్ అనుచితమైన కంటెంట్ కలిగి ఉండవచ్చు

HOW TO STOP TEXTING ADDICTION

<p>Avoid texting/ chatting at late nights</p> 	<p>Never chat with Unknown persons</p> 	<p>Respond only when it is really required</p> 
<p>Uninstall the texting APPS which you no longer use</p> 	<p>Fix a time to access and be selective to reply</p> 	<p>Prefer to make a call and talk rather than texting</p> 
<p>Avoid spreading gossips or rumours through texting</p> 	<p>Carry your phone in your bag or pocket. don't carry it in your hand</p> 	<p>Turn off the notifications</p> 

స్నేహితులు మరియు కుటుంబ సభ్యులతో కనెక్ట్ అవ్వడానికి, మీడియా కంటెంట్స్ను పంచుకోవడానికి మరియు ఇలాంటి అభిరుచులను పంచుకునే వ్యక్తులతో సోషల్ నెట్వర్క్ లను రూపొందించడానికి సోషల్ నెట్వర్కింగ్ సైట్లు ముఖ్యమైన పాత్ర పోషిస్తాయి. ఇతర ఆన్లైన్ కార్యక్రమాల మాదిరిగానే సోషల్ నెట్వర్కింగ్ కూడా ప్రమాదాలను కలిగి ఉంటుంది. వైబర్ మోసం యొక్క ఉచ్చు నుండి లిల్లి తన స్నేహితుడు పింకిని ఎలా కాపాడుతుందో చూద్దాం.





చిట్కాలు:

- అపరిచితులను ఆన్ లైన్ లో ఎప్పుడూ జోడించవద్దు
- మీ స్నేహితుల సమాచారాన్ని సెట్ వర్కింగ్ సైట్లలో పోస్ట్ చేయవద్దు, అది వారిని ప్రమాదంలో పడేసి అవకాశం ఉంది.
- గ్రూప్ ఫోటోలు, పాఠశాల పేర్లు, ప్రాంతాలు, వయస్సు, జండర్ మొదలైనవి పోస్ట్ చేయకుండా మీ స్నేహితులను రక్షించండి.
- మీరు చేయబోయే ప్రణాళికలు మరియు కార్యక్రమాలను సెట్ వర్కింగ్ సైట్లలో పోస్ట్ చేయకండి.

గుర్తింపు దొంగతనం అంటే ఇతరుల వ్యక్తిగత సమాచారాన్ని దొంగిలించడం. ఇతరుల గుర్తింపును ఉపయోగించడం సేరంగా పరిగణించబడుతుంది. సన్నిహితులు మరియు కుటుంబ సభ్యుల నుండి కూడా గుర్తింపు దొంగతనం జరుగుతుంది. రాజా తన క్లాస్ మేట్ పై ప్రతీకారం తీర్చుకోవడానికి తన వ్యక్తిగత సమాచారాన్ని పట్టుకోవడం ద్వారా ఎలా ప్రయత్నించాడో చూద్దాం.



రాజా క్లాసులో చాలా అల్లరి పిల్లవాడు



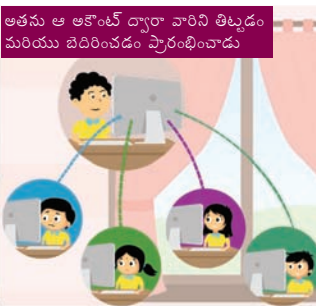
ఒక రోజు, క్లాస్ రీడర్ అతని గురించి ఫిర్యాదు చేయడంతో అతని టీచర్ అతనిని తిట్టండి



వీటన్నిటికీ తన క్లాస్ రీడర్ కారణమని రాజా భావించాడు. అతను ఆమె ఐడి కార్డును దొంగిలించి దానిపై వివరాలను తీసుకున్నాడు



అతను fb లో ఒక నకిలీ అకౌంట్ ను సృష్టించాడు, క్లాస్ మేట్స్ ను అందరిని దానికి జోడించాడు



అతను ఆ అకౌంట్ ద్వారా వారిని తిట్టడం మరియు బెదిరించడం ప్రారంభించాడు



ఆమె స్నేహితులు క్లాస్ రీడర్ వద్దకు వచ్చి, ఆమె ఎందుకు ఇలా ప్రవర్తించారని అడగారు, అప్పుడు ఆమె ఎస్ బిలో తనకి అసలు అకౌంట్ తేదని చెప్పింది.



ఆమె వెంటనే సహాయం కోసం తన టీచర్ ని సంప్రదించింది



తరవాత, ఈ అకౌంట్ ను రాజు సృష్టించినట్లు తెలిసింది



అకౌంట్ తొలగించబడింది, అతని టీచర్ అతని ప్రవర్తనకు కఠినంగా హెచ్చరించారు

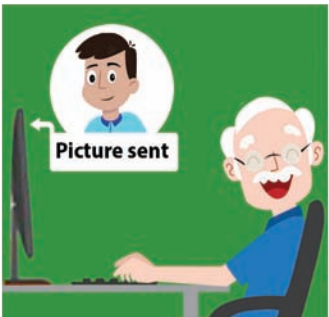
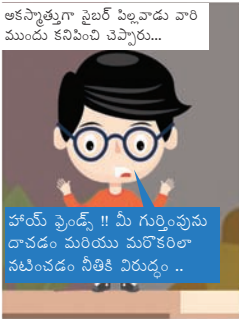
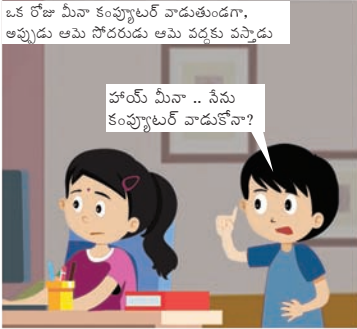
చిట్కాలు:

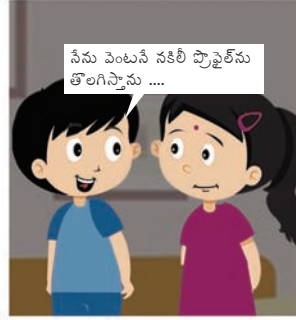
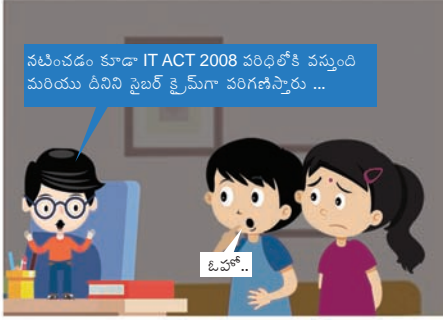
- పుస్తకాలపై మీ వ్యక్తిగత సమాచారాన్ని రాయడం తగ్గించండి
- మీ వస్తువులను జాగ్రత్తగా చూసుకోండి.
- అపరిచితులతో మాట్లాడటం మానుకోండి
- సోషల్ మీడియాలో వ్యక్తిగత సమాచారాన్ని షేర్ చేయకండి.

FOUR INTERNET SAFETY TIPS FOR KIDS



పేరొకరి పేరుతో ఇమెయిల్ వంపడం, మెటిరియల్ పోస్ట్ చేయడం, సోషల్ నెట్వర్కింగ్ ఖాతాలను సృష్టించడం లేదా ఇతర వ్యక్తులను ఏ విధంగానైనా సంప్రదించడానికి ప్రయత్నించడం ఆన్లైన్ వంచన లేదా ఇ-వ్యక్తిగతం అంటారు. వంచన సేరం అని రాజు ఎలా గ్రహించాడో చూద్దాం





చిట్కాలు:

- మీరు మోసగించబడినట్లయితే, వెంటనే భాతాను సంబంధిత అధికారులకు నివేదించండి
- సోషల్ నెట్ వర్క్ సైట్లలో తెలియని వ్యక్తులకు ఛాయాచిత్రాలు, వీడియోలు మరియు ఇతర సున్నితమైన సమాచారాన్ని ఎప్పుడూ పంపించవద్దు
- సోషల్ నెట్ వర్కింగ్ సైట్ల గోప్యతా సెట్టింగ్లను తనిఖీ చేయండి, మీరు ఆమోదించినట్లయితే మాత్రమే ఇతరులను మీ స్నేహితుడిగా చేర్చగలిగే విధంగా సెట్టింగ్లను సెట్ చేయండి



HOW TO AVOID BEING A TARGET

- Ask for separate locker at hostel to keep your documents
- Avoid sharing your personal or financial information with your hostel mates or friends
- Avoid using Aadhaar card/ Pan card/ Internet banking etc in front of anyone



ఫిషింగ్ దాడులు చిన్న పిల్లలను లక్ష్యంగా చేసుకుంటాయి ఎందుకంటే వారు సాధారణంగా మరింత అజాగ్రత్తగా ఉంటారు, అతిగా నమ్ముతారు; ఇంకా సాంకేతిక పరిజ్ఞానం తల్లిదండ్రుల నియంత్రణలు మరియు పరిమితులను సులభంగా తప్పించుకోవచ్చు. ఫిషింగ్ ఉచ్చులో విక్రీ ఎలా పడిపోయాడో చూద్దాం

విక్రీ తన సాతహాలో చాలా చురుకైన కుర్చుడు



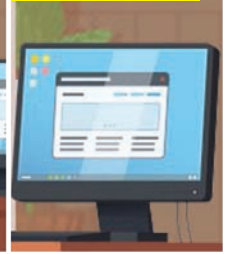
అతను ఆన్లైన్ ఆటలను ఆడటానికి ఇష్టపడతాడు వాటిని చాలా సవాలగా భావిస్తాడు



ఒక రోజు, అతను "గేమ్ ఆఫ్ కింగ్స్" అనే ఆటను డౌన్లోడ్ చేసి ఆట పూర్తి చేశాడు



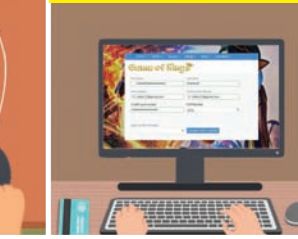
ఆట యొక్క పూర్తి వెర్షన్ కోసం డౌన్లోడ్ లింక్తో పాస్వర్డ్ తరస్థితి వచ్చింది



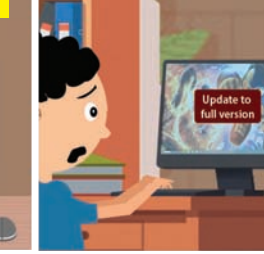
అతను అది నిజమని భావించి డౌన్లోడ్ లింక్పై క్లిక్ చేశాడు



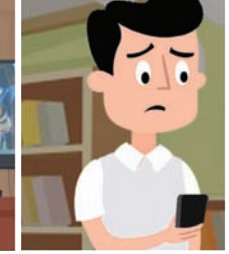
ఇది క్రెడిట్ కార్డుతో సహా వివరాలను పూరించడానికి ఒక ఫార్మ్ను చూపించే వెబ్సైట్ మళ్ళించింది, అతను తన తండ్రి వివరాలను నింపాడు



తరువాత, అతను ఆట యొక్క పూర్తి వెర్షన్ కోసం ఎటువంటి సవకరణను పొందలేదు



ఇంతలో, అతని తండ్రి క్రెడిట్ కార్డు నుండి డబ్బు తీయబడిన మెసేజ్ వచ్చింది



అతను తన అనుమతి లేకుండా తన క్రెడిట్ కార్డును ఉపయోగించాడా అని విక్రీని అడిగాడు



విక్రీ క్షమాపణలు చెప్పి, ఆట డౌన్లోడ్ కోసం కార్డు వివరాలను ఆన్లైన్ రూపంలో ఉపయోగించానని చెప్పాడు



విక్రీ తండ్రి కార్డును బ్యాంక్ చేసినందుకు బ్యాంక్ కస్టమర్ కేర్ కి సంప్రదించి ఫిర్యాదు చేశారు.



ఎంటనీ బ్యాంకు అధికారి స్పందించి కార్డును బ్యాంక్ చేశారు



చిట్టాలు:

- అనుమతి లేకుండా మీ తల్లిదండ్రుల క్రెడిట్ / డెబిట్ కార్డు వివరాలను ఎప్పుడూ ఉపయోగించవద్దు.
- వ్యక్తిగత లేదా ఆర్థిక సమాచారం అడిగే ఇ-మెయిల్ లేదా పాప్-అప్ సందేశానికి ప్రత్యుత్తరం ఇవ్వవద్దు.
- స్పామ్ ఇ-మెయిల్‌ను తెరవవద్దు.
- అటాన్యెంట్లను ప్రత్యేకంగా జిప్ ఫైల్‌లను తెరవవద్దు మరియు .లీం ఫైల్‌లను అమలు చేయవద్దు.
- మీకు ఏమైనా అనుమానం ఉంటే ఇ-మెయిల్ తెరవకండి. ఒకవేళ చట్టబద్ధమైనదైన మరియు మిమ్మల్ని సంప్రదించడానికి ప్రయత్నిస్తున్న వ్యక్తికి నిజంగా అవసరమైతే, వారు మరొక మార్గాన్ని ప్రయత్నిస్తారు.



What is Phishing?

Phishing is a way of attempting to acquire **information** such as usernames, passwords, PIN, bank account, credit card details by masquerading as a trustworthy entity through electronic communication means like e-mail.



Phishing Attack Methods



MOST COMMON TYPE OF PHISHING ATTACK

MASS-SCALE PHISHING

Attack where fraudsters cast a wide net of attacks that aren't highly targeted



HIGHLY TARGETED TYPE OF PHISHING ATTACK

SPEAR PHISHING

Tailored to a specific victim or group of victims using personal details

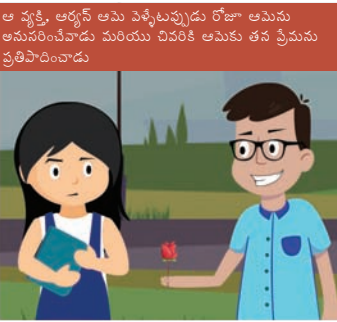


THE MOBY DICK OF PHISHING ATTACKS

WHALING

Specialized type of spear phishing that targets a "big" victim within a company
e.g., CEO, CFO or other executive

ఒక వ్యక్తి యొక్క ముఖాన్ని మరొకరి శరీరానికి మార్పింగ్ చేయడం మరియు దానిని బ్లాక్ మెయిల్ చేయడానికి లేదా వ్యక్తిని బెదిరించడం కోసం ప్రచురించడం సోషల్ నెట్వర్కింగ్ సైట్లలో ఫోటోలను అవేలోడ్ చేసే వ్యక్తులను దోషిణి చేసే మార్గాలలో ఒకటి. రవీనాకి ఏమి జరిగిందో చూద్దాం.



చిట్కాలు:

- నిజ జీవితంలో మీకు తెలిస్తే మాత్రమే వారిని మీ భాతాకు స్నేహితులుగా చేర్చండి
- ఫోటోలు, వీడియోలు మరియు ఇతర సున్నితమైన సమాచారాన్ని అపరిచితులకు సోషల్ నెట్వర్క్ సైట్లలో ఎప్పుడూ షేర్ చేయవద్దు
- మీ సమాచారాన్ని వీక్షించడానికి మీరు ఎవరిని అనుమతించాలనుకుంటున్నారో దాని ప్రకారం మీరు గోప్యతా సెట్టింగ్లను కూడా సెట్ చేయవచ్చు.
- ఏ ధోరణులను గుడ్డిగా అనుసరించవద్దు, వాటితో తెలివిగా ఉండండి.

Public Computer Safety

A public computer(or public access computer) may be available public places like Internet cafes, libraries, schools or facilities run by private or Government

Check whether there are any key loggers installed in the system

Do's

Don'ts

Don't save logon information

Be careful who is watching over your shoulder & check for spywares

Don't enter sensitive information into a public computer

Ensure to use the browser tools to delete files, cookies & to clear browsing history

Don't leave the computer unattended



సైబర్ వస్త్రధారణ అనేది ఎవరైనా లైంగిక వేధింపులకు లేదా దోపిడీకోసం పిల్లలను వారి నమ్మకాన్ని పొందే లక్ష్యంతో సోషల్ మీడియా లేదా మెసేజింగ్ ప్లాట్‌ఫామ్ల ద్వారా పిల్లలతో భావోద్వేగ బంధాన్ని ఏర్పరచుకోవడం. రోజీ విషయంలో ఏమి జరిగిందో చూద్దాం.

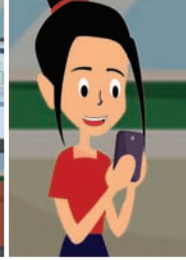
రోజీ 14 ఏళ్ల అమ్మాయి & ముంబైలో నివసించేది.



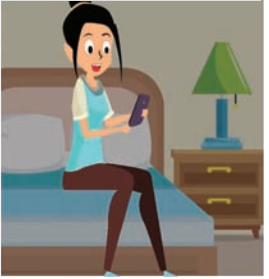
ఆమెకు సోషల్ నెట్‌వర్కింగ్ ఖాతా ఉంది మరియు ఒక రోజు ఆమెకు నటాషా అనే అమ్మాయి నుండి తెలియని ఫ్రెండ్ రిక్విస్ట్ వచ్చింది



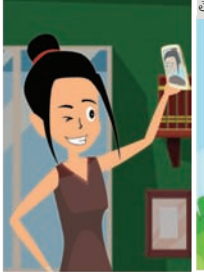
ఆమె అభ్యర్థనను అంగీకరించి, ఆమెతో చాట్ చేయడం ప్రారంభించింది



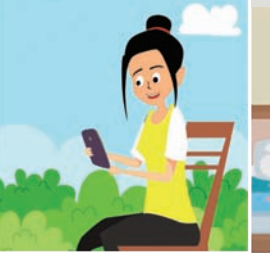
రోజీ నటాషా యొక్క స్నేహపూర్వక ప్రవర్తనను ఇష్టపడింది, ఇద్దరూ రోజూ చాట్ చేసేవారు



రోజీ తన విత్తాంశ నటాషాకి పంపించేది



నటాషా రోజీ చాలా ఆందంగా మరియు ముద్దుగా ఉందని రోజీ కి అభినందనలు తెలిపేది



ఒక రోజు, రోజీ ఒక ఫంక్షన్ కోసం సిద్ధమవుతున్నది. ఇంతలో ఆమెకు నటాషా నుండి ఒక టెక్స్ట్ వచ్చింది



ఆకస్మాత్తుగా, నటాషా రోజీని తన నగ్న చిత్రాన్ని పంపమని ఆడగడం ప్రారంభించింది. రోజీ ఈ సందేశం చూసి షాక్ అయింది



రోజీ బెదిరిపోయి ఏమి జరిగిందో తల్లికి చెప్పింది



ఆమె తల్లి వెంటనే అకౌంట్ గురించి రిపోర్టు చేసింది.



అకౌంట్ బ్లాక్ చేయబడింది...



చిట్కాలు:

- సోఫట్ మీడియా ప్లాట్‌ఫామ్‌లలో తెలియని వ్యక్తుల నుండి స్నేహితుల అభ్యర్థనను అంగీకరించవద్దు. సైబర్ గ్రూమర్ బాధితులతో స్నేహం చేయడానికి నకిలీ ఖాతాను కూడా సృష్టించవచ్చు.
- మీ పరిచయానికి తక్కువ వ్యవధిలో మీ గురించి మీ చాట్ భాగస్వామి మీకు చాలా అభినందనలు తెలిపినప్పుడు వారితో జాగ్రత్తగా ఉండండి.
- తెలియని వ్యక్తులతో చాట్ చేస్తున్నప్పుడు మీ పెబ్‌క్యామ్‌ను ఎప్పుడూ షీర్ చేయవద్దు
- మీరు ఆన్‌లైన్‌లో కలిసిన వ్యక్తిని కలవడానికి ఒంటరిగా వెళ్లవద్దు. మీతో పాటు ఎల్లప్పుడూ స్నేహితుడిని లేదా వెద్ద వారిని తీసుకెళ్ళండి.
- సోఫట్ సెట్‌వర్క్ సైట్లలో తెలియని వ్యక్తులకు ఫోటోలు, వీడియోలు మరియు ఇతర సున్నితమైన సమాచారాన్ని ఎప్పుడూ షీర్ చేయవద్దు



WHAT TO DO WHEN YOUR SYSTEM IS COMPROMISED ?



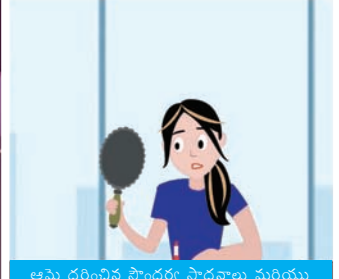
ఆన్లైన్ ప్రొడక్ట్ సమీక్షలు దుకాణదారులకు ప్రొడక్ట్ గురించి తెలుసుకోవటానికి ఒక మార్గం. వినియోగ దారులు నిర్ణయం తీసుకోవడంలో అవి గణనీయమైన ప్రభావాన్ని చూపుతాయి. మనలో చాలామంది కొనుగోలు చేయడానికి ముందు ఉత్పత్తి యొక్క సమీక్షలు మరియు రీటింగ్ల కోసం తనిఖీ చేస్తారు. కానీ మీరు ఆన్లైన్లో చదివిన ప్రతి సమీక్ష నిజమైనది కాదు. నకిలీ సమీక్ష ద్వారా నికీ ప్రభావితమైనప్పుడు ఆమెకు ఏమి జరిగిందో తనిఖీ చేద్దాం.



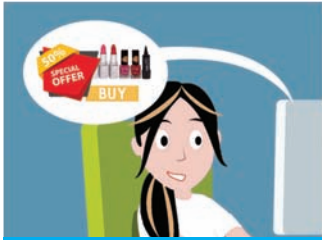
నికీ అండర్ గ్రాడ్యుయేట్ విద్యార్థి ఇంకా కాబోయే మోడల్



ఆమె వెలుగులో ఉండని నిర్ధారించుకోవడానికి ఆమె చాలా షీ 3 పార్టీలకు హాజరయ్యింది



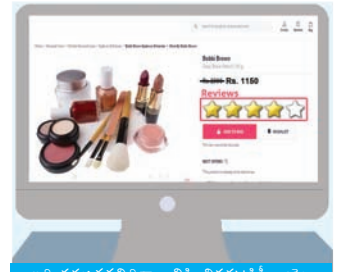
ఆమె ధరించిన సౌందర్య సాధనాలు మరియు పరిమళ ద్రవ్యాలు చాలా ఖరీదైనవి, ఇవి పార్టీ ముగిసే వరకు కొనసాగివి.



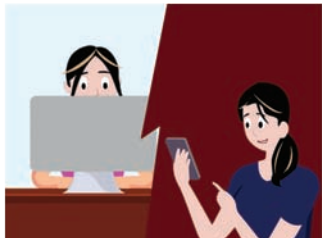
ఆమె మరిన్ని పార్టీలకు హాజరుకావడం ప్రారంభించగానే, సౌందర్య సాధనాలు త్వరలోనే అయిపోయాయి. ఆమె ఆన్లైన్లో చోకగా కొనడానికి అస్సెంబ్లీ వద్ద ప్రారంభించింది



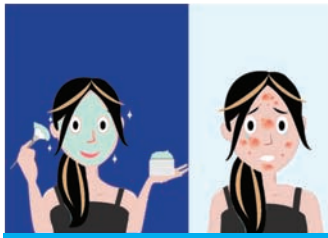
అనే ఉత్పత్తులను 50% తక్కువకు అందించే వెబ్సైట్ను ఆమె చూసింది



ఇది నమ్మదగనిదిగా అనిపించినప్పటికీ, ఆమె ఇతర ధృవీకరించిన సమీక్షలను తనిఖీ చేస్తుంది. వాటికి సగటున 4 స్టార్ రేటింగ్ ఉంది.



ఆమె సౌందర్య మరియు పెర్ఫ్యూమ్ ప్రొడక్ట్స్ కొనాలని నిర్ణయించుకుంటుంది. ఆన్లైన్లో చెల్లిస్తుంది మరియు ఆర్డర్ నిర్ధారణ కోసం SMS పొందుతుంది.



ఆమె ప్రొడక్ట్స్ ఇంటవర్టీ అందుకుంటుంది. వాటిని ఉపయోగించిన తరువాత, ఆమె చర్మంపై దద్దుర్లు వచ్చాయి, అవి తీవ్రం కావడంతో, ఆమె ఆసుపత్రిలో చేరాల్సి వచ్చింది



నికీ నకిలీ సమీక్షలను నమ్మడం మానేసింది. చాలా వెబ్సైట్లు అద్భుతమైన సమీక్షలను రాయడానికి ప్రసిద్ధి చెందాయి. మీరు వెబ్సైట్లు & సమీక్షలను జాగ్రత్తగా గమనించాలి. లేకపోతే పొరపాటుకు మూఱ్ఱం చెల్లించాల్సి వస్తుంది.

చిట్కాలు:

- సమీక్ష యొక్క పొడవు మరియు స్వరాన్ని పరిగణించండి
- సమీక్షకుడు ఇతర సమీక్షలను వ్యాశారో లేదో చూడండి
- ఇతర సమీక్షల కోసం చూడండి
- మధ్యస్థంగా రేట్ చేసిన ప్రొడక్ట్ సమీక్షలను చూడండి. ఉదా: (3***/5****)



Online shopping threats



Expensive branded products at low cost

In social networking sites very often we get advertisements showing expensive branded products at unbelievable prices. This catches attention of customer's most likely women and they may end up paying money for those products which are not genuine. For example branded bags, clothes, costly phone and beauty products.

Special thanks to



Hon. Prof. M. Banikrishnan
(IISc, Bangalore)



Prof. R. K. Shyam Sundar
(IIT, Bombay)



Prof. Sukumar Narub
(IIT, Guwahati)



Prof. V. Kamaakshi
(IIT, Madras)



Manoj Singh Gaur
(Director, IIT Jammu)



Dr. Sangay Bhatt
(Director General,
Cent-In)



Arvind Kumar
(Scientist G, Group
Coordinator, MeitY)



Rajesh Malhotra
(Scientist G, Group
Coordinator, MeitY)



Shri. Sitaram Chamarthy
(Principal Consultant, TCS)



Dr. Bishwajit Saha
Additional Director
(AIR & I), CSIR



Dr. Amarendra Prasad
Bhatnagar (Ph.D.)
Joint Director, CIET



Smt. U Rama Mohan Rao
SP, Cyber Crimes, CID,
Andhra Pradesh



Anil Kumar Pugal
Head, HRD Division, MeitY



Sangay Kumar Vyas
Scientist E & OSD to
Secretary, MeitY



Surendra Singh
Scientist - D
HRD Division, MeitY



Dr. Anandh Prabhug
Software Engineer &
Cyber Security Expert



Mr. Vivek Shetty
Entrepreneur & Social
activist

Supported & Reviewed by

K Indra Veni
M Jagadish Babu
E Naresh
M Soumya
T Sandeep
M Sandeep
Tyeb Naushad
B Nandeeshwar
Y Soumya

T Sushma
T Vishnu Priya
S Priya Darshini
Sheetal Mishra
Danish Inamdar
G Prashanth Reddy
Santhosh
Krapesh Bhatt
Shital Mahajan

S Amani
Ankush Sharma
Pooja Jadhav
U V Sudharshan
K S Jahnvi
Prem Prakash
P Keerthi Chandana
V Ashishya

Multimedia Team

Indra Keerthi V V L
P S S Bharadwaj

Concept by

Ch A S Murty

About ISEA

Looking at the growing importance for Information Security, Ministry of Electronics & Information Technology has identified this as a critical area. Information Security Education and Awareness (ISEA) Project was formulated and launched by Ministry of Electronics & Information Technology, Government of India. One of the activities under this programme is to spread Information Security Awareness among children, teachers, home users, IT and non-IT professionals throughout the country. C-DAC Hyderabad has been assigned the responsibility of executing this project. As part of this activity C-DAC, Hyderabad has been preparing Information Security Awareness material, coordinating with Participating Institutes (PI's) in organizing the various Information Security Awareness events.



INFORMATION SECURITY
EDUCATION AND AWARENESS
Project-Phase II

About C-DAC

C-DAC established its Hyderabad Centre in the year 1999 to work in Research, Development and Training activities embracing the latest Hardware & Software Technologies. The centre is a Knowledge Centre with the components of Knowledge Creation, Knowledge Dissemination and Knowledge Application to grow in the areas of Research & Development, Training and Business respectively. The R & D areas of the centre are e-Security, Embedded Systems, Ubiquitous Computing, e-Learning and ICT for Rural Development. The centre has developed over a period of time a number of products and solutions and has established a number of labs in cutting edge technologies. In line with these R&D strengths, the centre also offers Post Graduate level diploma courses. Centre is also actively involved in organizing faculty training programs. The centre regularly conducts skill based training and information security awareness programmes.



Supported by



Subscribe us on



<https://www.youtube.com/c/InformationSecurityEducationandAwareness>

Like us on



<https://www.facebook.com/infosecawareness>

Follow us on



<https://twitter.com/InfoSecAwa>

Follow us on



[@infosec_awareness](https://www.instagram.com/infosec_awareness)

For queries on Information security Call us on Toll Free No.

1800 425 6235

ISEA Whatsapp Number for Incident Reporting

+91 9490771800

To Share Tips/Latest News/feedback mail us to

isea@cdac.in

isea.gov.in

www.infosecawareness.in



प्रगत संगणन विकास केन्द्र
CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING
इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी विभाग का वैज्ञानिक संस्था, भारत सरकार
A Scientific Society of the Ministry of Electronics and Information Technology, Government of India
Plot No. 8 & 7, Indira Park, 5th No. 11, Stralokm Highway, Noida Building No. 1 Shalooji Subbaraj Theatre Road, Anandpur, Hyderabad - 500076, Bangalore (INDIA)