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

unicef

For Virus Alerts,Incident & Vulnerability Reporting
cert-in
Handling Computer Security Incidents

www.InfoSecawareness.in

From the Desk

E Magesh
Director, C-DAC Hyderabad

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.

INDEX

చెడు భాషను మానుకోండి.............................. 04
వ్యక్తిగత సమచారం గోప్యంగా ఉంచడం........... 06
సంభాషణ జరిపేటప్పుడు.............................. 08
కాపీరైట్స్... 10
సంస్కృతులు.. 12
ఆన్‌లైన్ ప్రిడేటర్లు... 14
తక్షణ సందేశం... 16
ఇమెయిల్ అకౌంట్ హాక్ చేయడం.................. 18
సైబర్ బెదిరింపు... 20
సైబర్ స్టాకింగ్.. 22
మొబైల్ ఫోన్ భద్రత...................................... 24
మొబైల్ ఫోన్ వ్యసనాలు.............................. 26
రాన్సమ్‌వేర్.. 28
ఆన్‌లైన్‌లో అపరిచితులను కలవడం................. 30
ఆన్‌లైన్ గేమింగ్.. 32
సామాజిక నెట్వర్కింగ్.................................... 34
గుర్తింపును దొంగిలించడం 36
ఆన్‌లైన్ మోసం... 38
ఫిషింగ్ దాడులు... 40
పిక్చర్ మార్ఫింగ్.. 42
సైబర్ గ్రూమింగ్.. 44
నకిలీ సమీక్షలు... 46

చెడు భాషను మానుకోండి

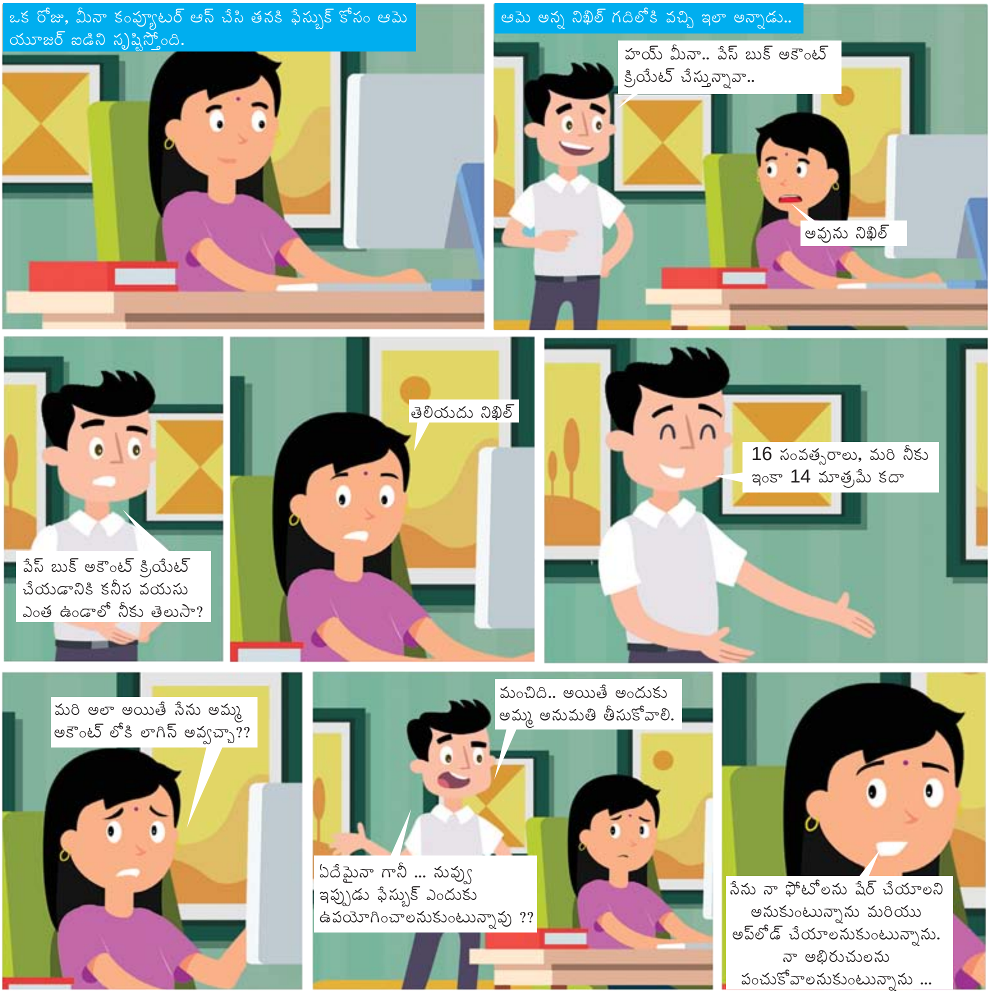
మీలో కొంతమందికి చెడు పదాలను సరదాగా వాడడం లేదా చెడ్డ భాషను ఉపయోగించే అలవాటు ఉండవచ్చు లేదా మీరు ఇష్టపడని మీ క్లాస్‌మేట్‌పై మీ కోపాన్ని చూపించవచ్చు. మీరు ఉపయోగించే పదాలు, ఇంకా మీరు పోస్ట్ చేసిన ఫోటోలు ప్రతీకారం తీర్చుకునే విధంగా ఉండడమే కాకుండా వాస్తవ ప్రపంచంలో కూడా అవి దుష్పరిణామాలకు దారి తీయవచ్చు. తన తరగతిలోని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

చిట్కాలు:

- మొరటుమాటలు లేదా చెడ్డ భాష వాడటం మానుకోండి.
- కంప్యూటర్లను ఇతరులకు హాని కలిగించడానికి ఉపయోగించకూడదు.
- మీరు ఇతరులతో చాట్ చేసేటప్పుడు మర్యాదపూర్వకంగా, సహనంతో ఉండాలి.
- సోషల్ నెట్‌వర్కింగ్ సైట్‌లను ఉపయోగిస్తున్నప్పుడు ఇతరుల అభిప్రాయాలను మరియు ఆసక్తులను గౌరవించండి.
- అపరిచితులతో చాటింగ్ చేయవద్దు.

వ్యక్తిగత సమాచారం గోప్యంగా ఉంచడం

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 వెళ్తే అది మిమ్మల్ని ఇబ్బందుల్లో పడేస్తుంది. తన సోదరి తన వ్యక్తిగత సమాచారాన్ని పంచుకోవడంలో జాగ్రత్తగా ఉండాలని నిఖిల్ ఆమెకు ఎలా వివరించాడో చూద్దాం.

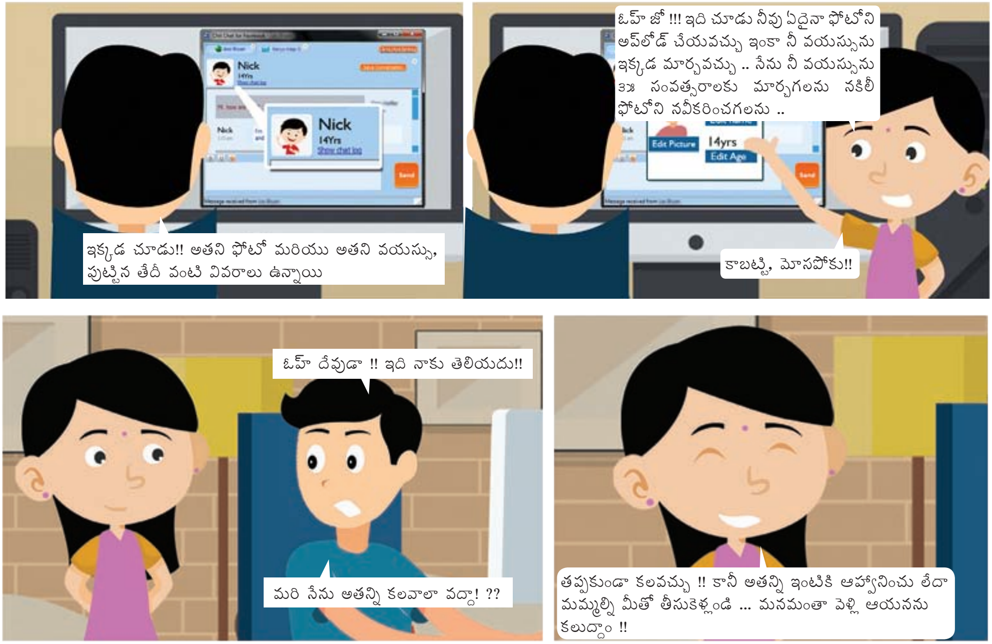


చిట్కాలు:

- మీకు తెలియకుండా అపరిచితులు మీ ప్రొఫైల్‌ను ఉపయోగించుకోవచ్చు మరియు మీ సమాచారాన్ని దుర్వినియోగం చేయవచ్చు
- సోషల్ నెట్‌వర్కింగ్ వెబ్‌సైట్లలో అందుబాటులో ఉన్న గోప్యతా సెట్టింగ్‌లను ఎల్లప్పుడూ ఉపయోగించుకోవడం మంచిది.
- మీ పేరు, పాఠశాల / ఇంటి చిరునామా, ఫోన్ నంబర్లు, వయస్సు, జండర్, క్రెడిట్ కార్డ్ వివరాల వంటి వ్యక్తిగత సమాచారాన్ని ఇవ్వవద్దు లేదా పోస్ట్ చేయవద్దు
- సైట్లలో నీవు ఇచ్చే సమాచారం కూడా నిన్ను బాధితురాలిగా మార్చే ప్రమాదంలోకి నెడుతుందని తెలుసుకో.
- సోషల్ నెట్‌వర్కింగ్ సైట్‌లో పరిచయం అయిన వారితో వ్యక్తిగతంగా కలవకు, ఎందుకంటే కొంతమంది వారు ఎవరో నిజాలు వారు చెప్పకపోవచ్చు.

చాటింగ్ చేసేటప్పుడు

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



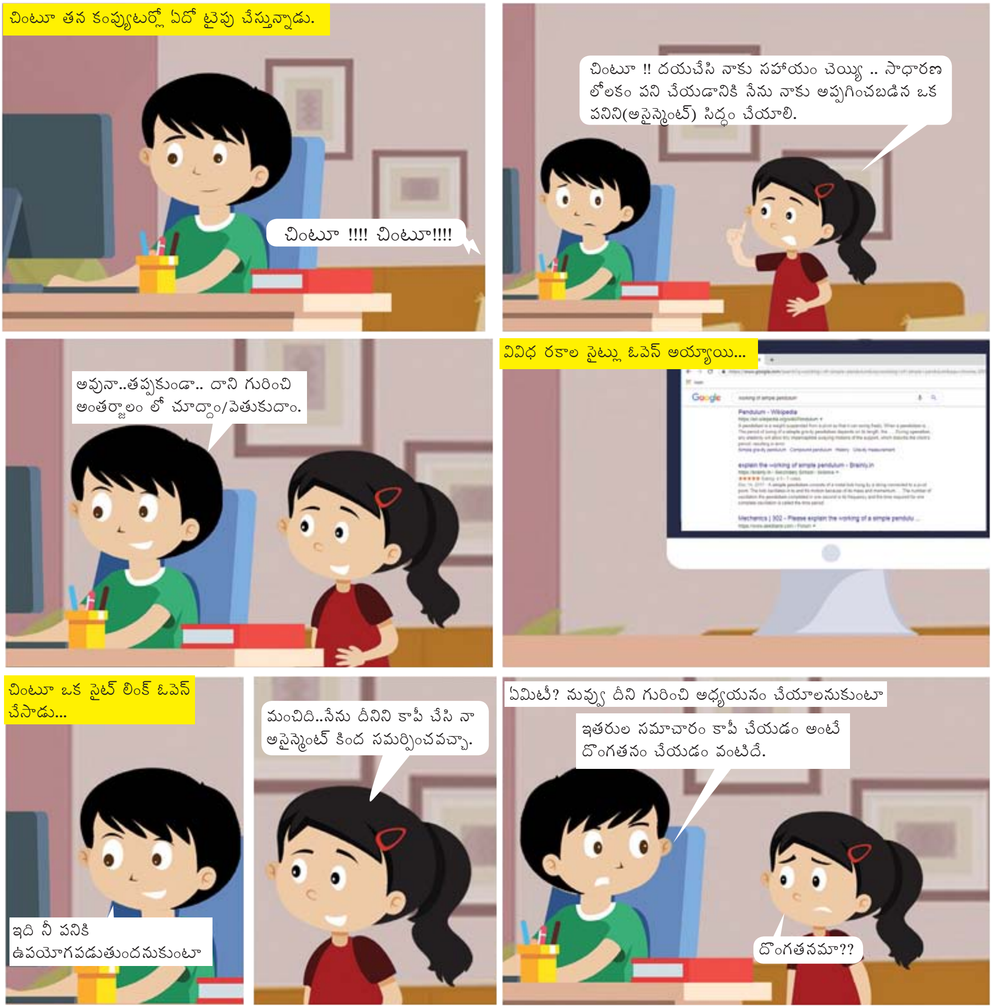
చిట్కాలు:

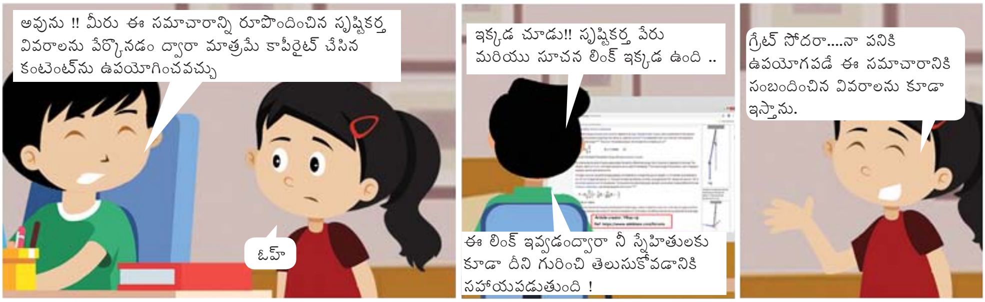
౧. మీకు తెలియని వ్యక్తుల నుండి వచన సందేశాలను గురించి పట్టించుకోకు.

౨. ఆన్‌లైన్ సంభాషణలలో నీ వ్యక్తిగత వివరాలను పంచుకోవడం మానుకో.

కాపీరైట్స్

కాపీరైట్ అనేది ఒకరు చేసిన స్వీయపనిని రక్షించే చట్టం. ఇది సాహిత్య, నాటకీయ, సంగీత, కళాత్మక మరియు కొన్ని ఇతర సృజనాత్మక రచనలకు సంబందించినటువంటిది. 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.



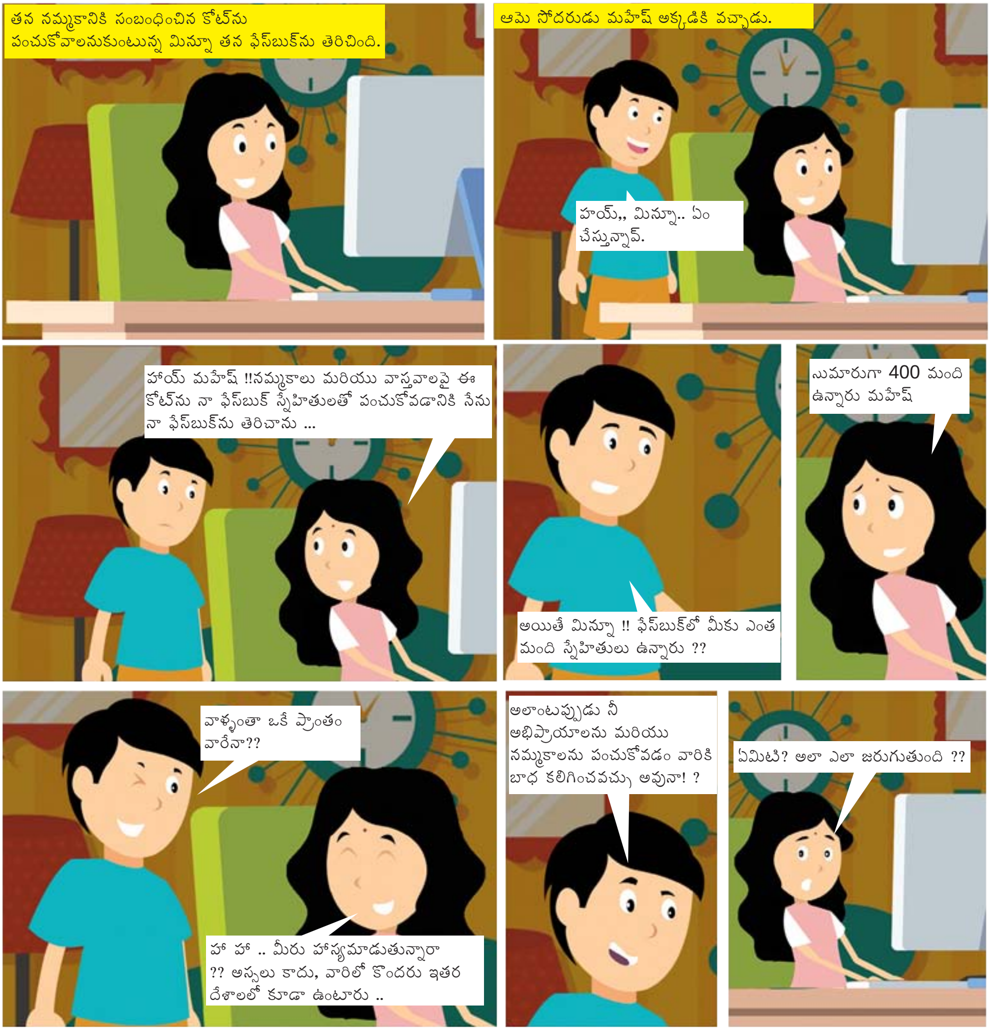


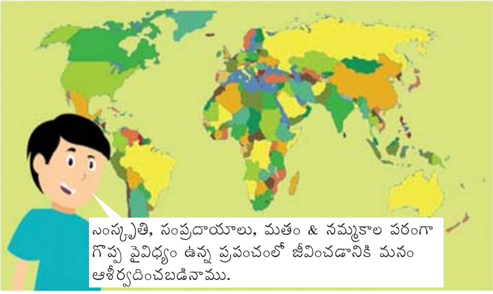
చిట్కాలు:

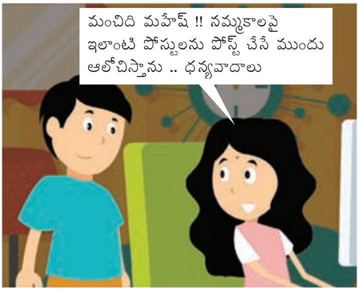
- నువ్వు చట్టాన్ని ఉల్లంఘించలేదని ముందుగా నిర్ధారించుకో
- కంటెంట్ యజమానికి క్రెడిట్‌లను ఎల్లప్పుడూ పేర్కొనండి.
- ఉపయోగించే ముందు నిబంధనలు మరియు షరతులను చదవడం మరచిపోవద్దు.
- రచయిత హక్కులను గౌరవించండి

సంస్కృతులు

సంస్కృతి మనకు ఒక గుర్తింపును ఇస్తుంది, మన ప్రవర్తనలను ప్రభావితం చేస్తుంది మరియు సాంస్కృతిక వైవిధ్యం మనల్ని ఇతర సంస్కృతులను కొంతవరకు అర్థం చేసుకునేలా చేయడమే 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 మహేష్ తన సోదరికి అర్థం అయ్యేలా ఎలా చెప్పాడో చూద్దాం.





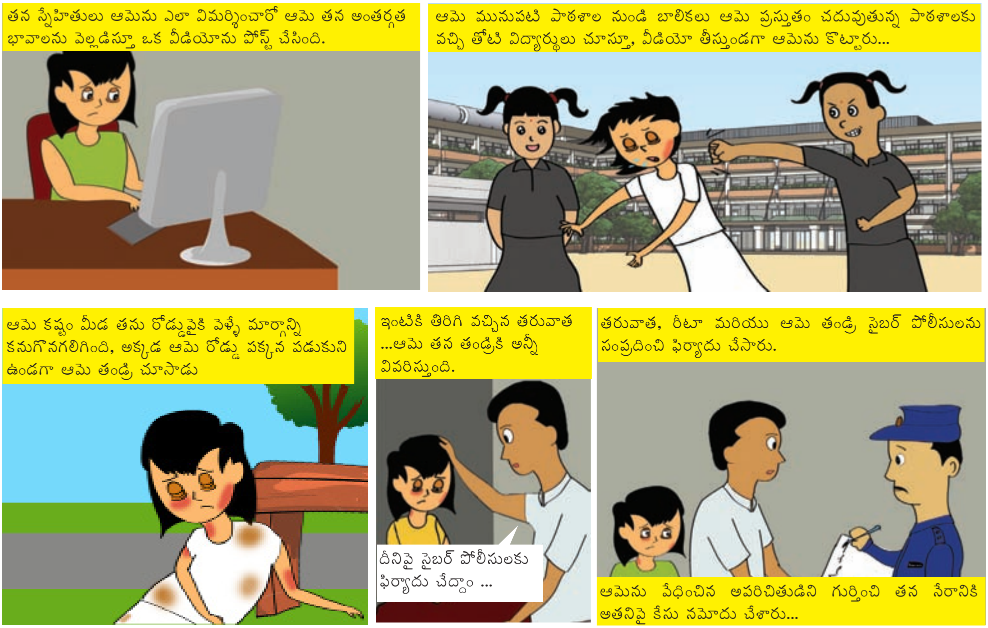


చిట్కాలు:

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

ఆన్‌లైన్ ప్రిడేటర్లు

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

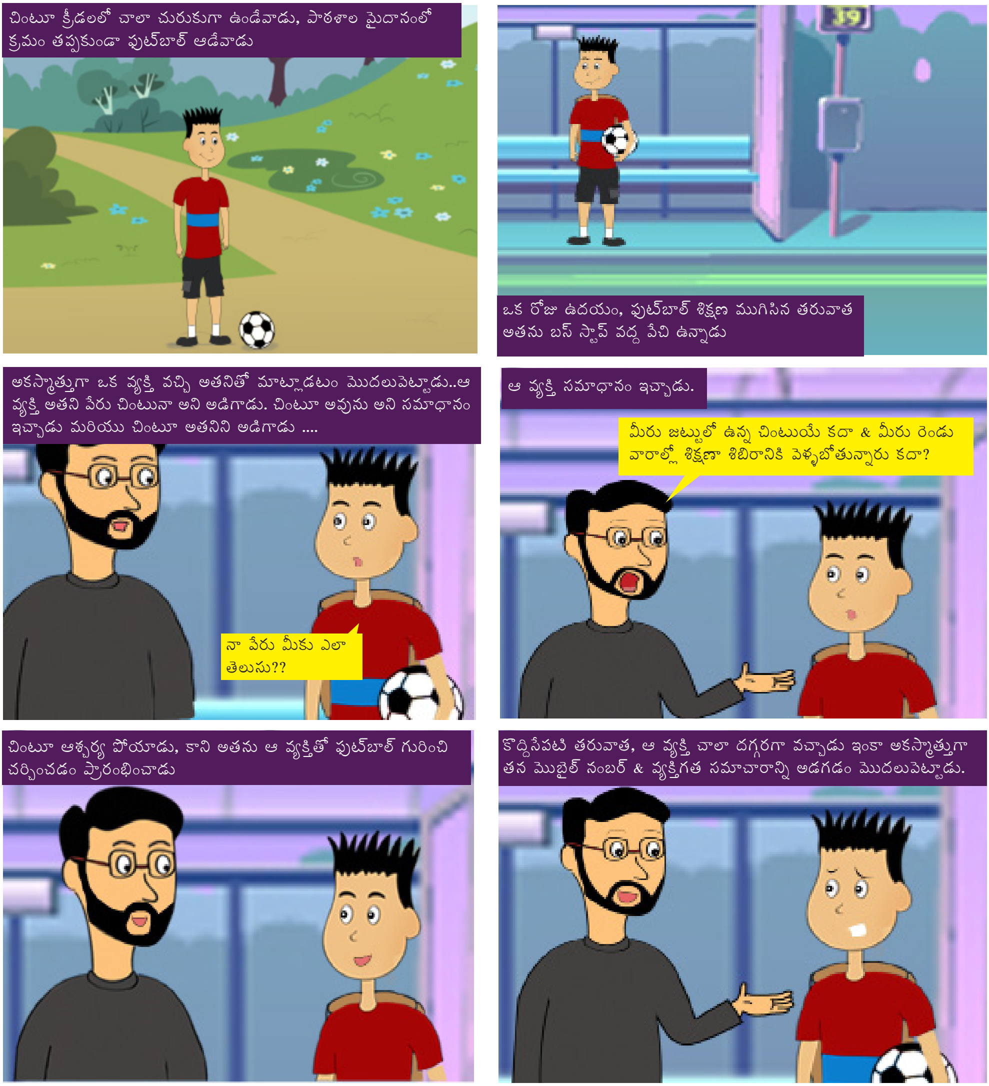


చిట్కాలు:

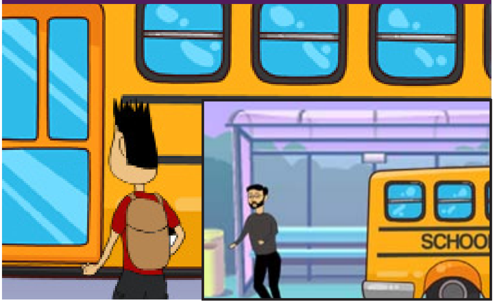
- మీ ఆన్‌లైన్ అనుభవాల గురించి మీ తల్లిదండ్రులతో ఓపెన్ గా, నిజాయితీగా సంభాషణలు జరపండి/మాట్లాడండి.
- చాలా వ్యక్తిగతంగా ఉండాలనుకునే వారితో మాట్లాడకండి.
- వ్యక్తులు వారు ఎవరో, ఏమిటో ఎల్లప్పుడూ నిజాలు చెప్పరని గుర్తుంచుకోండి.
- ఫోన్ నంబర్లు, అడ్రసులు, పాఠశాల పేరు లేదా ఇతర వివరాలను ఎప్పుడూ పోస్ట్ చేయవద్దు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

తక్షణ సందేశం

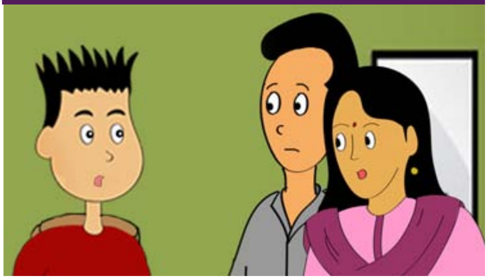
తక్షణ సందేశం (IM) ఇంటర్నెట్ ద్వారా అప్పటికప్పుడే నిజ సమయంలో ‘చాట్’ చేయడానికి మిమ్మల్ని అనుమతిస్తుంది. దూరంగా ఉన్న కుటుంబ సభ్యులు, స్నేహితులతో మాట్లాడ డానికి గొప్ప సాధనం, కానీ దీంతో మీరు ఎల్లప్పుడూ జాగ్రత్తగా ఉండాలి. చింటూ తక్షణ సందేశ అనువర్తనం లేదా యాప్ ద్వారా అపరిచితులతో చాట్ చేసినప్పుడు ఏమి జరిగిందో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



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



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



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

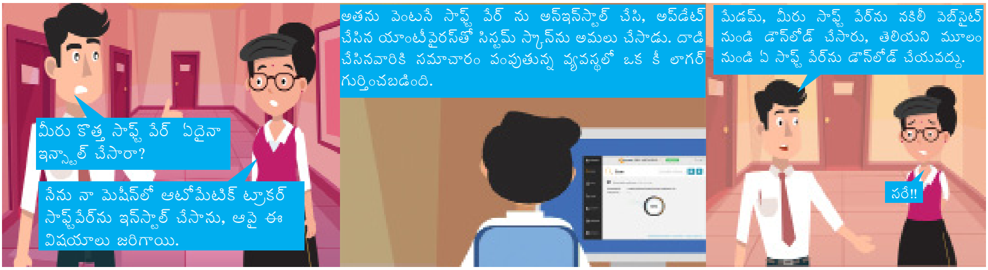
చింటూ, అతని తల్లిదండ్రులు కలిసి చాట్ సెషన్ ఆ వ్యక్తి బస్ స్టాప్ వద్ద ఉండటానికి కారణం అయిందని గ్రహించారు. వారు ఈ నేరాన్ని పోలీసులకు నివేదించారు.

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 చేయొద్దు.
- మీ తక్షణ సందేశం యాప్ ను క్రమం తప్పకుండా అప్ డేట్ చేస్తుండండి/నవీకరించండి.
- ప్రొఫైల్ ఫోటో ఆప్షన్ ఖాళీగా ఉంచడం మంచిది.

ఇమెయిల్ అకౌంట్ హాక్ చేయడం

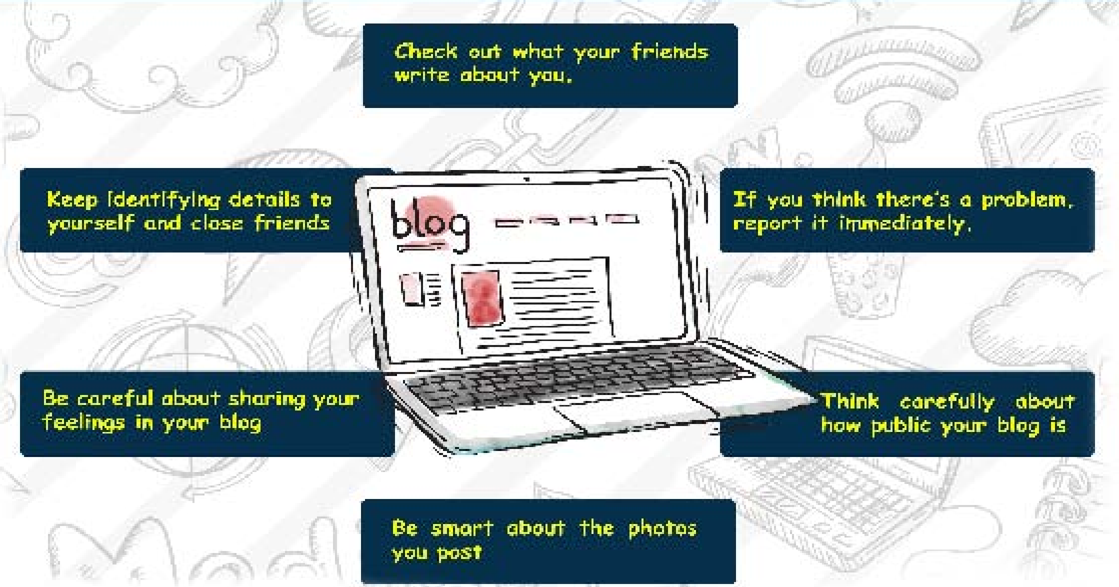
ఈ రోజుల్లో అందరికీ ఇమెయిల్ ఖాతా ఉంటోంది. ఇమెయిల్ ఖాతాను సృష్టించడానికి స్పష్టమైన వయో పరిమితులు లేవు. మీలో చాలామంది ఇమెయిల్ ఖాతాను సృష్టించడం ద్వారా ఇంటర్నెట్ ప్రపంచంలోకి ప్రవేశించి ఉండవచ్చు. కానీ దీనివల్ల కూడా చాలా ప్రమాదాలు ఉన్నాయి అని మీరు తెలుసుకోవాలి. సోనీ ఇమెయిల్ ఖాతాతో ఏమి జరిగిందో చూద్దాం.



చిట్కాలు:

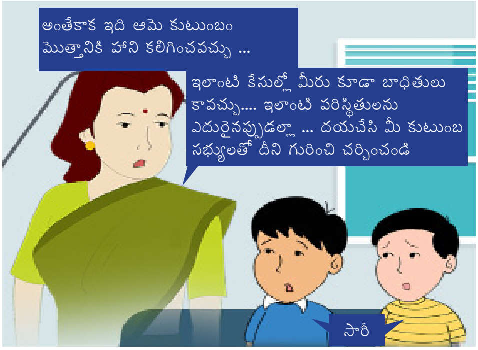
- మీ మెయిల్ అకౌంట్ వివరాలను అపరిచితులకు ఇవ్వవద్దు.
- మీరు మీ ఇమెయిల్‌ను తనిఖీ చేసిన తర్వాత లాగ్ అవుట్ చేసే అలవాటు చేసుకోండి
- స్పామ్ లేదా ఫార్వార్డ్ చైన్ ఇమెయిల్‌లకు రిప్లై ఇవ్వవద్దు.
- అపరిచితుల నుండి వచ్చిన ఇమెయిళ్ళను అనుమానాస్పద మైనవిగా చూడండి.
- మీరు యాప్/అనువర్తనాన్ని డౌన్‌లోడ్ చేయడానికి ముందు అనువర్తనం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

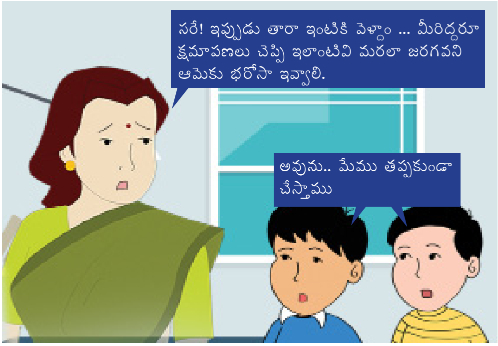
Safety tips for blogging



సైబర్ బెదిరింపు

సైబర్ బెదిరింపు అనేది ఒక వ్యక్తిని వేధించడానికి, బెదిరించడానికి, ఇబ్బంది పెట్టడమే లక్ష్యంగా చేసుకోవడానికి సాంకేతిక పరిజ్ఞానాన్ని ఉపయోగించడం. సరళంగా చెప్పాలంటే, ఇది ఆన్‌లైన్‌లో జరిగేది. వేరొకరిని 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 పెద్దలతో మాట్లాడండి
- బెదిరింపు ముఠాలో చేరి సైబర్ రౌడీగా ఉండకండి.

BEST PRACTICES & GUIDELINES FOR STRENGTHENING YOUR BROWSING SECURTY

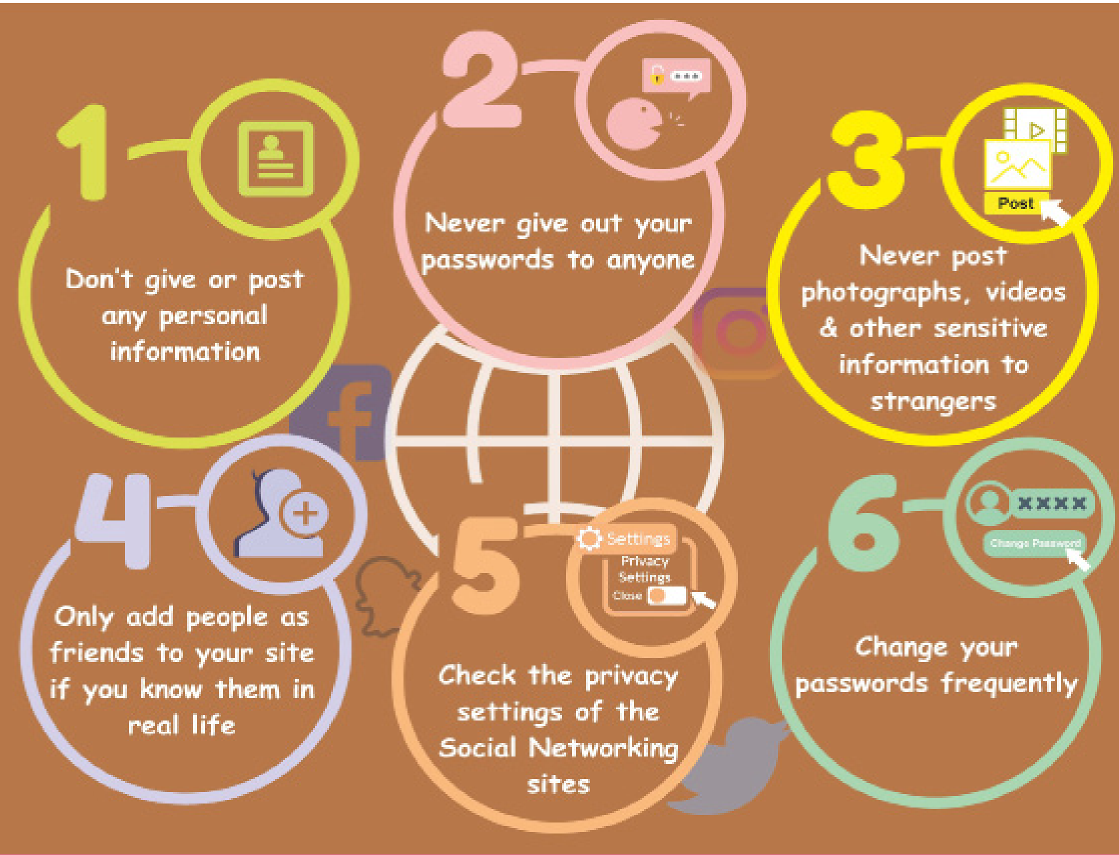
సైబర్ స్టాకింగ్

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

చిట్కాలు:

- ఆన్‌లైన్ లో మీ సమాచారం ఏమిటో సమీక్షించండి వీలయినంత తక్కువ సమాచారం ఉంచండి.
- మీ గోప్యత, భద్రతా సెట్టింగ్‌లను అన్నిటిని సమీక్షించండి
- మీరు హాజరయ్యే ఈవెంట్ల 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



మొబైల్ ఫోన్ భద్రత

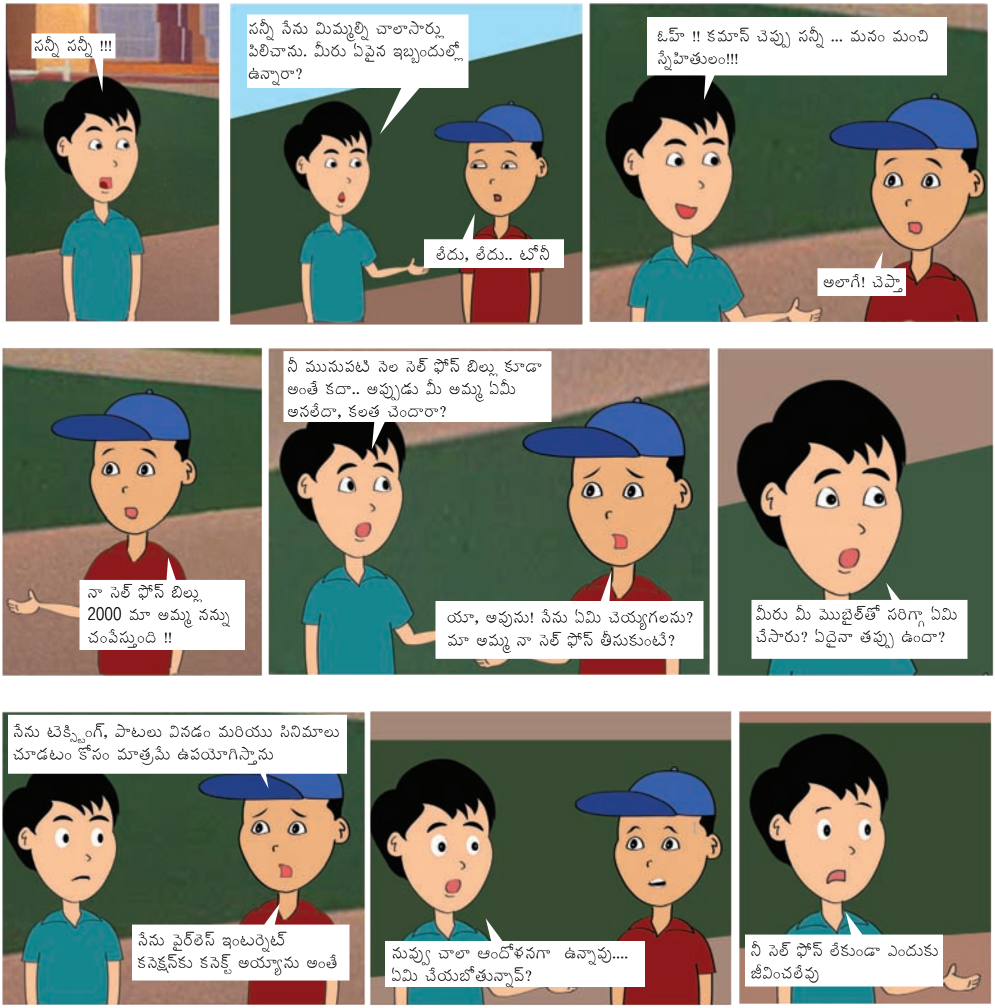
ఈ రోజుల్లో మొబైల్ ఫోన్‌ను ఎలా ఉపయోగించాలో తెలియని పిల్లవాడిని కనుగొనడం కష్టం. ఇది అందించే ఫైఖరులు, సామర్థ్యాలు మరియు వినోదం కాకుండా మీరు బాధ్యత వహించాల్సిన అవసరం ఉందని మరియు సురక్షితంగా ఉండటానికి కొన్ని నియమాలు భద్రతా చర్యలను అనుసరించాలని మీరు తెలుసుకోవాలి. బన్నీ తన కొత్త మొబైల్ ఫోన్‌లో చాలా తెలియని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

చిట్కాలు:

- మొబైల్ ఆపరేటింగ్ సిస్టమ్‌ను క్రమం తప్పకుండా నవీకరించండి.
- ఆపరేటింగ్ సిస్టమ్‌ను దాని తాజా వెర్షన్‌కు అప్‌గ్రేడ్ చేయండి.
- విశ్వసనీయ మూలాల నుండి అనువర్తనాలను ఎల్లప్పుడూ ఇన్‌స్టాల్ చేయండి.
- పేరున్న ప్రొవైడర్ నుండి భద్రతా సాఫ్ట్‌వేర్‌ను ఇన్‌స్టాల్ చేయడానికి మొగ్గు చూపండి. వాటిని క్రమం తప్పకుండా నవీకరించండి.
- అనువర్తనాన్ని డౌన్‌లోడ్ చేయడానికి ముందు దాని ఫీచర్లను తనిఖీ చేయడం ఎప్పుడూ శ్రేయస్కరం. కొన్ని అనువర్తనాలు/యాప్స్ మీ వ్యక్తిగత డేటాను ఉపయోగించవచ్చు.
- మీరు మూడవ పక్షం నుండి అనువర్తనాన్ని డౌన్‌లోడ్ చేస్తుంటే, అది మంచి పేరున్నదా లేదా అని నిర్ధారించుకోవడానికి కొద్దిగా పరిశోధన చేయండి.

మొబైల్ ఫోన్ వ్యసనాలు

నిజమైన వ్యక్తులతో సంభాషించడానికి బదులుగా సోషల్ మీడియాను ఉపయోగించడం లేదా ఆటలను ఆడటం కోసం మీరు మీ మొబైల్‌తో ఎక్కువ సమయం గడిపినప్పుడు, మీ జీవితంలో ప్రతికూల పరిణామాలు ఎదురైనప్పుడు కూడా, ఇమెయిల్‌లు లేదా అనువర్తనాలను పదేపదే తనిఖీ చేయకుండా మీరు ఆపలేరు. దీన్నే మొబైల్ ఫోన్ వ్యసనం అని పిలుస్తారు. మొబైల్ ఫోన్‌కు బానిస అయినప్పుడు సన్నికి ఏమి జరిగిందో చూద్దాం.



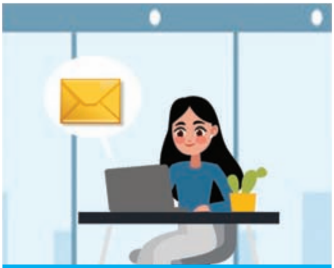
చిట్కాలు:

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

రాన్సమ్‌వేర్

రాన్సమ్‌వేర్ అనేది ఒక రకమైన హానికరమైన సాఫ్ట్ వేర్, క్రయధనం చెల్లించే వరకు కంప్యూటర్ సిస్టమ్ లేదా డేటా అందుబాటును తిరస్కరించడానికి రూపొందించబడింది. రాన్సమ్‌వేర్ సాధారణంగా ఫిషింగ్ ఇమెయిల్‌ల ద్వారా లేదా తెలియకుండా వైరస్ సోకిన వెబ్‌సైట్‌ను సందర్శించడం ద్వారా వ్యాపిస్తుంది. రాన్సమ్‌వేర్ అలీషా ల్యాప్‌టాప్‌ను ఎలా ప్రభావితం చేసిందో చూద్దాం.

అలీషా ఒక వ్యవస్థాపకురాలు/పారిశ్రామికవేత్త. ఆమె సంస్థలో 50 మంది ఉద్యోగులు & 60 కంప్యూటర్స్ ఉన్నాయి


ఒక రోజు, ఆమె తన విక్రేత నుండి అటాచ్మెంట్ కలిగి ఉన్న ఇమెయిల్‌ను అందుకుంటుంది

అలీషా అటాచ్‌మెంట్‌ను డౌన్‌లోడ్ చేస్తుంది. ఆమె యాంటీవైరస్ నవీకరించబడలేదు, కాబట్టి ఎలాంటి హెచ్చరికలు లేవు

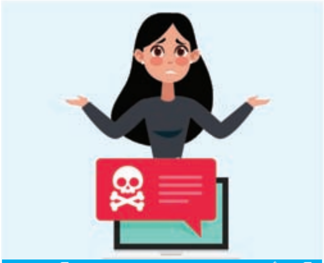
ఫైల్‌ను తెరిచిన తర్వాత, ఆమె సిస్టమ్ లాక్ అవుతుంది మరియు అన్ని ఫైల్స్ గుప్తీకరించబడతాయి. యాక్సెస్ చేయలేకపోయింది

స్క్రీన్‌పై ఒక హెచ్చరిక సందేశం స్క్రీన్‌ను అన్‌లాక్ చేయడానికి బిట్‌కాయిన్‌లో లక్ష రూపాయలు చెల్లించాలని కోరుతుంది

అలీషా ఇవ్వబడిన బిట్‌కాయిన్ వాలెట్ చిరునామాకు చెల్లింపు చేస్తుంది

హ్యాకర్ ప్రైవేట్ కీని పంపలేదు. ఫైల్స్ గుప్తీకరించబడ్డాయి (రహస్యలిపిలోకి మార్చబడినాయి) అందుబాటులో లేవు

తనకు వచ్చింది రాన్సమ్‌వేర్ తో ఉన్న ఫిషింగ్ ఇమెయిల్ అని ఆమె కంపెనీ మేనేజర్ అలీషాకు చెప్పాడు.


ఇమెయిల్‌ను తొలగించకపోవడం, యాంటీవైరస్ మరియు ఆపరేటింగ్ సిస్టమ్‌ను అప్‌డేట్ చేయనందుకు అలీషా బాధ పడింది.

చిట్కాలు:

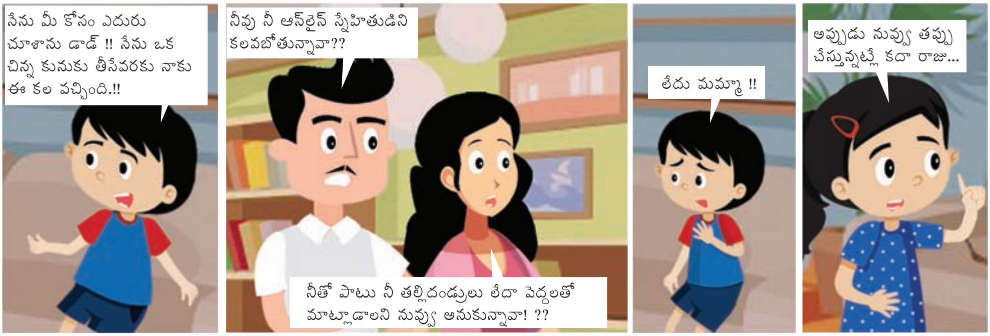
- మొట్టమొదట, మీ అతి ముఖ్యమైన ఫైళ్ళను రోజూ బ్యాకప్ చేయండి.
- అనుమానాస్పదంగా కనిపించే అటాచ్మెంట్లను తెరవడం మానుకోండి.
- క్లిక్ చేయడానికి ముందు రెండుసార్లు ఆలోచించండి.
- నేరస్థులచే బలవంతంగా ఓపెన్ చేయలేని బలమైన పాస్‌వర్డ్ లను ఉపయోగించండి.
- విండోస్ ఫైర్‌వాల్‌ను ఎప్పుడు ఆన్ చేసి, ప్రతిసారి సరిగ్గా కన్ఫిగర్ చేయండి.

STAGES OF RANSOMWARE INFECTION

HOW TO PROTECT AGAINST RANSOMWARE

ఆన్‌లైన్‌లో అపరిచితులను కలవడం

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



చిట్కాలు:

- మీరు నెట్‌వర్కింగ్ సైట్‌లో కలిసిన వ్యక్తిని కలవాలనుకుంటే మీ తల్లిదండ్రుల అనుమతి తీసుకోండి
- నిజ జీవితంలో మీకు తెలిస్తే మాత్రమే వారిని మీ సైట్‌కు స్నేహితులుగా చేర్చండి
- 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

ఆన్‌లైన్ గేమింగ్

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

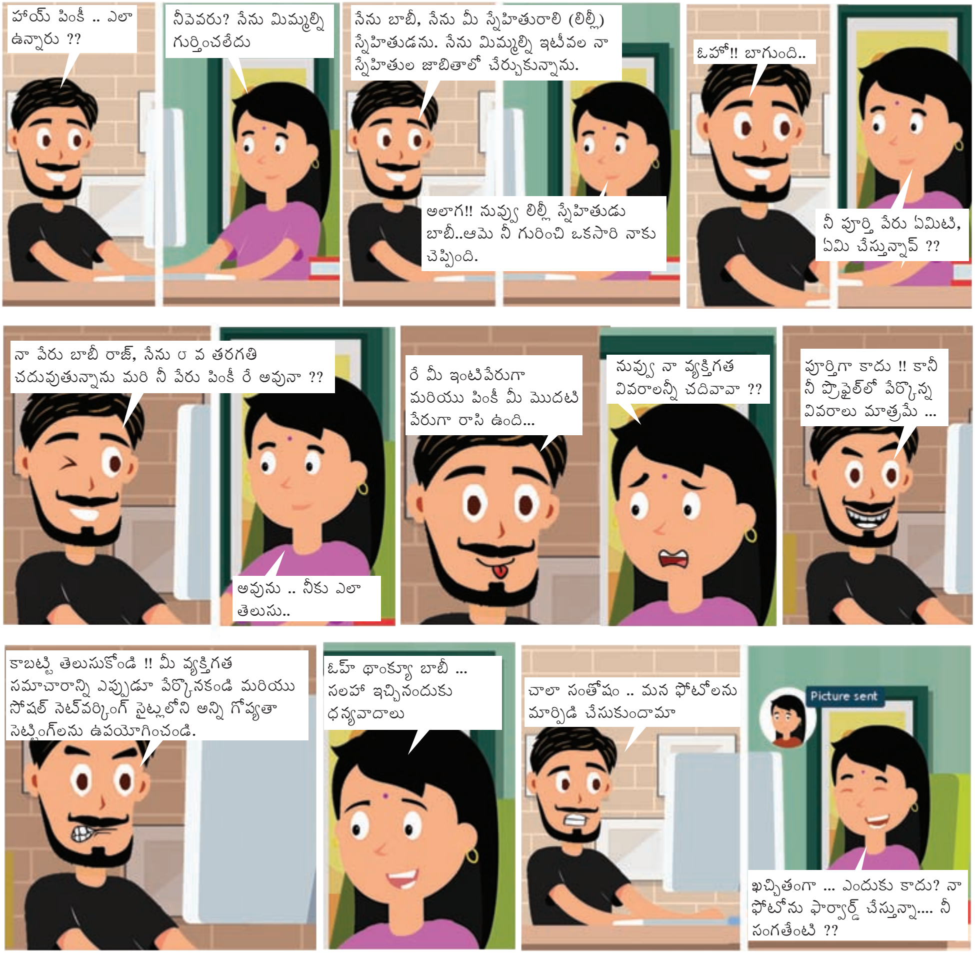
చిట్కాలు:

- 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

సామాజిక నెట్వర్కింగ్

స్నేహితులు మరియు కుటుంబ సభ్యులతో కనెక్ట్ అవ్వడానికి, మీడియా కంటెంట్‌ను పంచుకోవడానికి మరియు ఇలాంటి అభిరుచులను పంచుకునే వ్యక్తులతో సోషల్ నెట్‌వర్క్ లను రూపొందించడానికి సోషల్ నెట్‌వర్కింగ్ సైట్‌లు ముఖ్యమైన పాత్ర పోషిస్తాయి. ఇతర ఆన్‌లైన్ కార్యాక్రమాల మాదిరిగానే సోషల్ నెట్‌వర్కింగ్ కూడా ప్రమాదాలను కలిగి ఉంటుంది. సైబర్ మోసం యొక్క ఉచ్చు నుండి లిల్లీ తన స్నేహితుడు పింకీని ఎలా కాపాడుతుందో చూద్దాం.



చిట్కాలు:

- అపరిచితులను ఆన్‌లైన్‌లో ఎప్పుడూ జోడించవద్దు
- మీ స్నేహితుల సమాచారాన్ని నెట్‌వర్కింగ్ సైట్లలో పోస్ట్ చేయవద్దు, అది వారిని ప్రమాదంలో పడేసే అవకాశం ఉంది.
- గ్రూప్ ఫోటోలు, పాఠశాల పేర్లు, ప్రాంతాలు, వయస్సు, జండర్ మొదలైనవి పోస్ట్ చేయకుండా మీ స్నేహితులను రక్షించండి.
- మీరు చేయబోయే ప్రణాళికలు మరియు కార్యక్రమాలను నెట్‌వర్కింగ్ సైట్లలో పోస్ట్ చేయకండి.

గుర్తింపును దొంగిలించడం

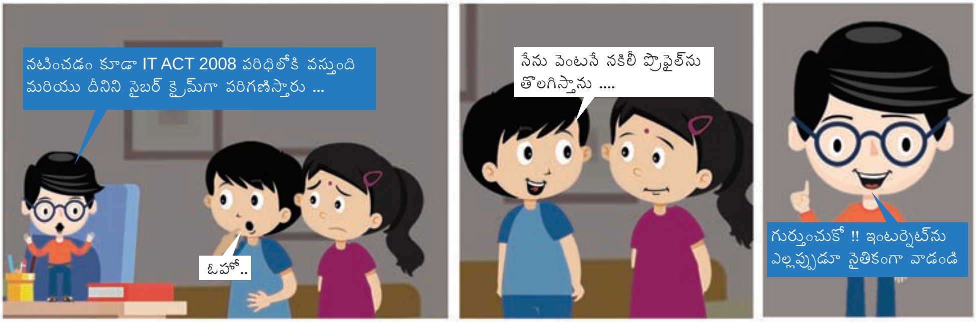
గుర్తింపు దొంగతనం అంటే ఇతరుల వ్యక్తిగత సమాచారాన్ని దొంగిలించడం. ఇతరుల గుర్తింపును ఉపయోగించడం నేరంగా పరిగణించబడుతుంది. సన్నిహితులు మరియు కుటుంబ సభ్యుల నుండి కూడా గుర్తింపు దొంగతనం జరుగుతుంది. రాజు తన క్లాస్‌మేట్‌పై ప్రతీకారం తీర్చుకోవడానికి తన వ్యక్తిగత సమాచారాన్ని పట్టుకోవడం ద్వారా ఎలా ప్రయత్నించాడో చూద్దాం.

చిట్కాలు:

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

ఆన్‌లైన్ మోసం

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



చిట్కాలు:

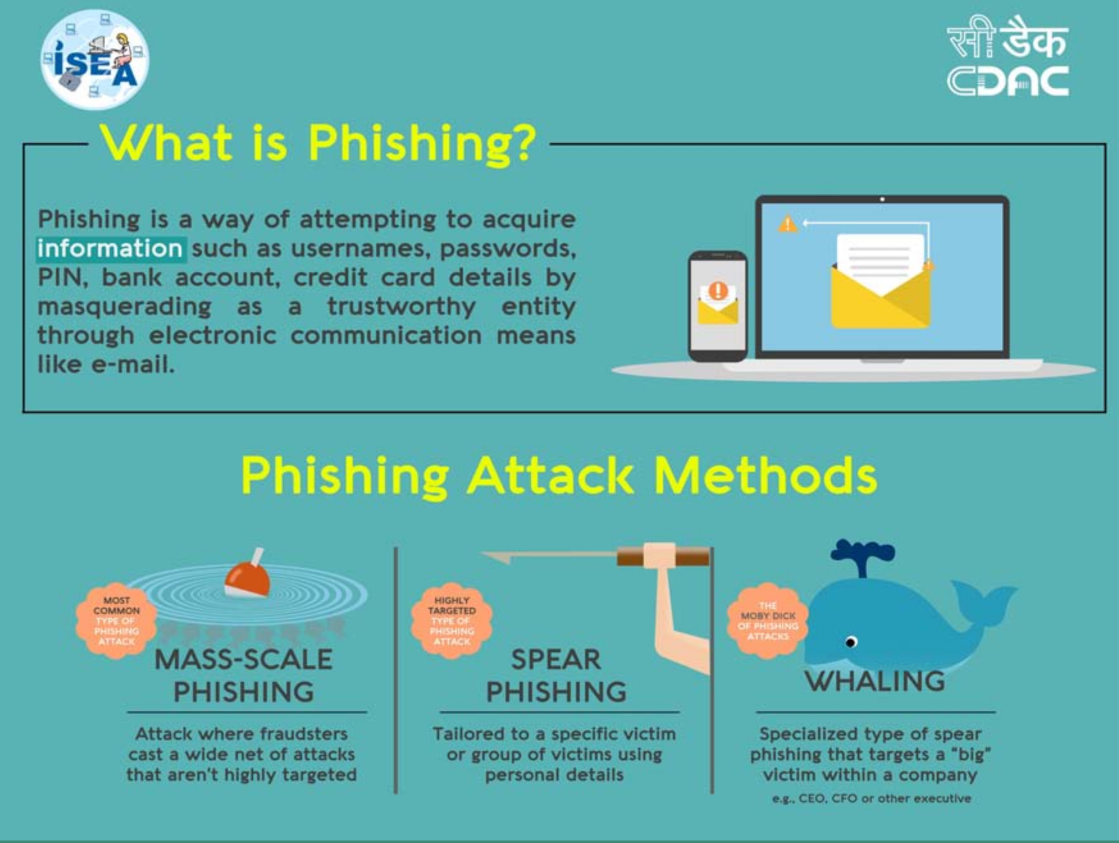
- మీరు మోసగించబడినట్లయితే, వెంటనే ఖాతాను సంబంధిత అధికారులకు నివేదించండి
- సోషల్ నెట్‌వర్క్ సైట్లలో తెలియని వ్యక్తులకు ఛాయాచిత్రాలు, వీడియోలు మరియు ఇతర సున్నితమైన సమాచారాన్ని ఎప్పుడూ పంపించవద్దు
- సోషల్ నెట్‌వర్కింగ్ సైట్‌ల గోప్యతా సెట్టింగ్‌లను తనిఖీ చేయండి, మీరు ఆమోదించినట్లయితే మాత్రమే ఇతరులను మీ స్నేహితుడిగా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

ఫిషింగ్ దాడులు

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 విక్కీ ఎలా పడిపోయాడో చూద్దాం

చిట్కాలు:

- 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.
- అటాచ్మెంట్లను ప్రత్యేకంగా జిప్ ఫైల్‌లను తెరవవద్దు మరియు .ఎలీం ఫైల్‌లను అమలు చేయవద్దు.
- మీకు ఏమైనా అనుమానం ఉంటే ఇ-మెయిల్ తెరవకండి. ఒకవేళ చట్టబద్ధమైనదైన మరియు మిమ్మల్ని సంప్రదించడానికి ప్రయత్నిస్తున్న వ్యక్తికి నిజంగా అవసరమైతే, వారు మరొక మార్గాన్ని ప్రయత్నిస్తారు.



పిక్చర్ మార్ఫింగ్

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

చిట్కాలు:

- నిజ జీవితంలో మీకు తెలిస్తే మాత్రమే వారిని మీ ఖాతాకు స్నేహితులుగా చేర్చండి
- ఫోటోలు, వీడియోలు మరియు ఇతర సున్నితమైన సమాచారాన్ని అపరిచితులకు సోషల్ సెట్‌వర్క్ 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.

సైబర్ గ్రూమింగ్

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.

చిట్కాలు:

- సోషల్ 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 వెబ్‌క్యామ్‌ను ఎప్పుడూ షేర్ చేయవద్దు

- మీరు ఆన్‌లైన్‌లో కలిసిన వ్యక్తిని కలవడానికి ఒంటరిగా వెళ్లవద్దు. మీతో పాటు ఎల్లప్పుడూ స్నేహితుడిని లేదా పెద్ద వారిని తీసుకెళ్ళండి.

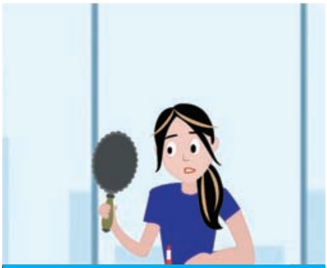
- సోషల్ నెట్‌వర్క్ సైట్లలో తెలియని వ్యక్తులకు ఫోటోలు, వీడియోలు మరియు ఇతర సున్నితమైన సమాచారాన్ని ఎప్పుడూ షేర్ చేయవద్దు

నకిలీ సమీక్షలు

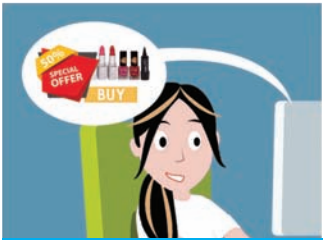
ఆన్‌లైన్ ప్రోడక్ట్ సమీక్షలు దుకాణదారులకు ప్రోడక్ట్ గురించి తెలుసుకోవటానికి ఒక మార్గం. వినియోగ దారులు నిర్ణయం తీసుకోవడంలో అవి గణనీయమైన ప్రభావాన్ని చూపుతాయి. మనలో చాలామంది కొనుగోలు చేయడానికి ముందు ఉత్పత్తి యొక్క సమీక్షలు మరియు రేటింగ్‌ల కోసం తనిఖీ చేస్తారు. కానీ మీరు ఆన్‌లైన్‌లో చదివిన ప్రతి సమీక్ష నిజమైనది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

నిక్కీ అండర్ గ్రాడ్యుయేట్ విద్యార్థి ఇంకా కాబోయే మోడల్

ఆమె వెలుగులో ఉందని నిర్ధారించుకోవడానికి ఆమె చాలా పేజీ 3 పార్టీలకు హాజరయ్యేది

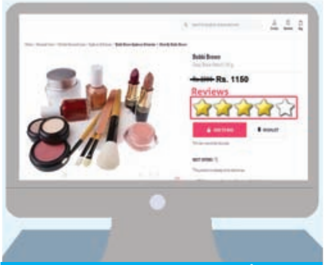


ఆమె ధరించిన సౌందర్య సాధనాలు మరియు పరిమళ ద్రవ్యాలు చాలా ఖరీదైనవి, ఇవి పార్టీ ముగిసే వరకు కొనసాగేవి.



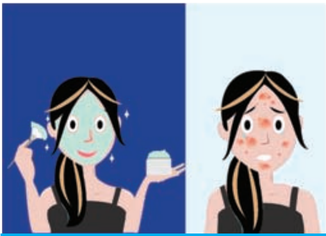
ఆమె మరిన్ని పార్టీలకు హాజరుకావడం ప్రారంభించగానే, సౌందర్య సాధనాలు త్వరలోనే అయిపోయాయి. ఆమె ఆన్‌లైన్‌లో చౌకగా కొనడానికి అన్వేషించడం ప్రారంభించింది

అవే ఉత్పత్తులను 50% తక్కువకు అందించే వెబ్‌సైట్‌ను ఆమె చూసింది



ఇది నమ్మదగనిదిగా అనిపించినప్పటికీ, ఆమె ఇతర్లు 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 ఇంటివద్దే అందుకుంటుంది. వాటిని ఉపయోగించిన తరువాత, ఆమె చర్మంపై దద్దుర్లు వస్తాయి, అవి తీవ్రం కావడంతో, ఆమె ఆసుపత్రిలో చేరాల్సి వచ్చింది

నిక్కీ నకిలీ సమీక్షలను నమ్మడం మానేసింది. చాలా వెబ్‌సైట్లు అద్భుతమైన సమీక్షలను రాయడానికి ప్రసిద్ధి చెందాయి. మీరు వెబ్‌సైట్‌లు & సమీక్షలను జాగ్రత్తగా గమనించాలి, లేకపోతే పొరపాటుకు మూల్యం చెల్లించాలల్సి వస్తుంది.

చిట్కాలు:

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

Special thanks to

Hon. Prof. N Balakrishnan
(IISc, Bangalore)

Prof. R. K. Shyamsundar
(IIT, Bombay)

Prof. Sukumar Nandi
(IIT, Guwahati)

Prof. V. Kamakoti
(IIT, Madras)

Manoj Singh Gaur
(Director, IIT Jammu)

Dr. Sanjay Bahl
(Director General, Cert-In)

Arvind Kumar
(Scientist G, Group Coordinator, MeitY)

Rakesh Maheshwari
(Scientist G, Group Coordinator, MeitY)

Shri. Sitaram Chamarthy
(Principal Consultant, TCS)

Dr. Bishwajit Saha
Additional Director (ATR & I), CBSE

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

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

Anil Kumar Pipal
Head, HRD Division, MeitY

Sanjay Kumar Vyas
Scientist E & OSD to Secretary, MeitY

Surendra Singh
Scientist "D"
HRD Division, MeitY

Dr Ananth Prabhu G
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 Jahnavi
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.

ISEA
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.

सी डैक
CDAC

Supported by

www.cyberswachhtakendra.gov.in

http://cert-in.org.in/

Subscribe us on YouTube

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

Like us on Facebook

https://www.facebook.com/infosecawareness

Follow us on Twitter

https://twitter.com/InfoSecAwa

Follow us on Instagram

@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