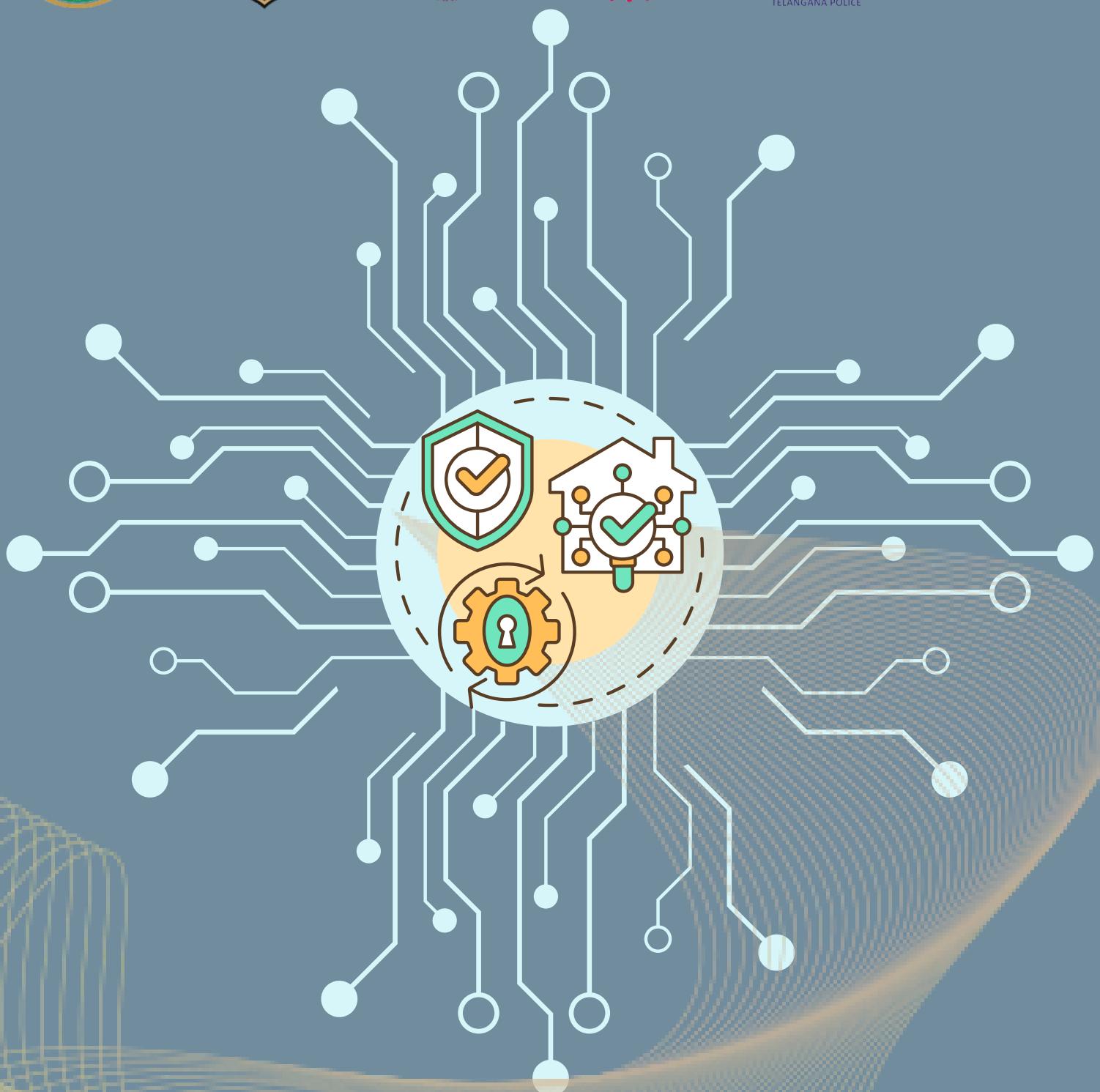


సైబర్ అంబాసిడరకు సాధికారత కల్పించేడం

సైబర్ అంబాసిడర్ ప్రోగ్రామ్ ద్వారా ఒక పయాణం



విషయ సూచిక

1. సైబర్ పరిశుభ్రత
2. నెట్‌కెట్లు
3. ఆన్‌లైన్ క్లాస్ నెట్‌క్వోర్ట్లు
4. పబ్లిక్ కంప్యూటర్లు మరియు వైఫై
5. సురక్షిత డౌన్‌లోడ్లు
6. మాల్వేర్ మరియు వైరస్
7. ఉమెన్ సెఫ్టీ వింగ్
8. ఆన్‌లైన్ గేమ్స్
9. సైబర్ అడిక్షన్
10. ఆన్‌లైన్ ప్రైడేటర్స్ మరియు చైల్డ్ ఆన్‌లైన్ యాక్టివిటీ ప్రాటెక్షన్
11. సైబర్ స్ప్యుస్ మరియు నివారణ చర్యలు
12. సైబర్ ప్యాకింగ్
13. ఆన్‌లైన్ గ్రూమింగ్
14. ఇమెయిల్ బెదిరింపులు
15. పాస్‌వర్డ్ బెదిరింపులు
16. క్రెడిట్ కార్డ్ స్చామ్లు
17. ఫిజింగ్
18. ఇమెయిల్ లాటరీ
19. సైబర్ బెదిరింపు
20. మొబైల్ సెక్యూరిటీ
21. సామాజిక నెట్‌వర్కింగ్
22. నకిలీ అప్లికేషన్‌లను గుర్తించడం ఎలా
23. డెస్క్‌టాప్ సెక్యూరిటీ
24. వెరబుల్ గాడ్జెట్‌లపై భద్రత అవగాహన
25. ఆరోగ్యం సమస్యలు(కష్టాలు)
26. మానసిక ఆరోగ్య
27. శారీరక ఆరోగ్యం
28. కంప్యూటర్లను ఆఫ్ చేయడం
29. సైబర్ లా-ఇండియా



Hello Students,

Welcome to the Cyber Ambassador Platform, Phase-III a training program on Cyber Safety and Security. Women Safety Wing, Telangana Police as a part of Cyber Ambassador Platform so far trained around 12000 Students from 4000 Govt schools on Cyber Safety who in turn created awareness among all other students of the schools and also community at large. Now it is your turn to get trained on Cyber Safety which is the need of the hour. You are lucky enough to have innovative way of training in digital mode in the form of captivating Videos, Infographics, Comics and Quiz.

This course will help you to find all the positive practices of our day-to-day lives while using the internet. It is designed in a fun, interactive manner to allow you to assimilate the material easily. The entire course is covered over the span of five days where you will learn about Cyber Hygiene, Netiquettes, Online games, Cyber addiction, Online predators, Child online activity protection, Cyber Stalking, email and password threats, Credit card scams, Phishing, Mobile security, Social networking and many more.

Once you undergo this training you will be identified as **CYBER AMBASSADOR** and with the knowledge gained, you will be made to create awareness on Cybercrimes, Cyber safety and cyber security among other students of the school and also in your neighborhood by organizing community outreach programs in coordination with She teams thus creating a safe cyber space to all citizens. Our SHE teams will be coordinating with you through your mentor teachers and in case of any doubt you should feel free to contact them though the mentor teachers. Hope you will learn keenly and get benefit of the course. Upon successful completion of the course, you will receive a course completion certificate from Women Safety Wing, Hyderabad police department.



Dear Cyber Ambassadors,

Congratulations on completing Phase III of the Cyber Ambassador Program! Your dedication and commitment to enhancing cyber awareness among your peers are commendable. As you embark on your journey as Cyber Ambassadors, equipped with knowledge and skills to navigate the digital world responsibly, we present to you "Empowering Cyber Ambassdors: A Journey Through Cyber Ambassador Program Phase III."

This book serves as a comprehensive resource, encapsulating the vital lessons and insights gained throughout your Cyber Ambassador journey. Through engaging infographics and concise explanations, it revisits the fundamental concepts and practices of cybersecurity, ensuring that you retain and reinforce your understanding of crucial topics.

In this digital era where technology permeates every aspect of our lives, the need for cyber awareness and vigilance has never been more critical. As Cyber Ambassadors, you play a pivotal role in promoting a safer online environment within your school community and beyond. This book not only aids in revising the materials covered in Phase III but also empowers you to continue educating others about cyber threats, data privacy, online safety, and responsible digital citizenship.

Remember, knowledge is power, and with it comes the responsibility to act. Let this book be your companion as you advocate for cyber awareness, inspire your peers to adopt secure online practices, and champion a culture of digital responsibility.

We applaud your dedication to becoming proactive agents of change in the digital landscape. Together, let us strive to create a safer and more secure cyber world for all.

Best wishes,
Dr. Vishnu Ramdeo,
Chief Executive Officer,
Cyber Secura Pvt. Ltd.

సైబర్

పరిశుభ్రత (HYGIENE)



సైబర్ పరిశుభ్రత అనగా ముఖ్యమైన దేటాను సురక్షితంగా ఉంచడం మరియు నెట్వర్క్లను భద్రపరచడం.



సైబర్ పరిశుభ్రత అనేది ఇప్పుడు చాలా తక్కువగా అంచనా వేయబడిన విషయాలలో ఒకটి. ప్రజలు వినోదం లేదా పని ప్రయోజనాల కోసం ఇంటర్నెట్‌ని ఉపయోగిస్తున్నారు, అయితే కొత్తమంది తమ క్రీమ్ ఆక్షిఫిట్స్ కోసం ఇంటర్నెట్‌ని ఉపయోగిస్తున్నారు.

సైబర్ పరిశుభ్రత కోసం చేయవలసినవి



తలియని వెబ్‌సైట్‌ను ఎప్పుడూ చూడొద్దు.

వెబ్‌సైట్ పెరిఫన్స్ లేదా దాని కుక్కీలు లేదా దేటా యాక్సెస్‌ని ఎల్లప్పుడూ చెక్ చేయండి.

తలియని వెబైప్పీ ఎల్లప్పుడూ VPN ఉపయోగించి అక్సెస్ చేయుండి.

ఇంటర్నెట్ నుండి ప్రోగ్రామ్లను డాన్లోడ్ చేయడానికి ముందు ఎల్లప్పుడూ చెక్ చేయండి.

సైబర్ పరిశుభ్రత కోసం చేయవద్దు



తలియని వెబ్‌సైట్‌లలో మీ బ్యాంక్ వివరాలను ఎప్పుడూ ఫేర్ చేయవద్దు.

ఇంటర్నెట్‌లో ఎవరితోనూ పర్సనల్ ఇన్ఫోర్మేషన్‌ను ఎప్పుడూ పంచుకోవద్దు.

డిస్కసనరీలో అందుబాటులో ఉన్న సులభంగా ఉపయోగించి ప్రాస్‌వర్ట్‌లను ఎప్పుడూ ఉపయోగించవద్దు.

ఇంటర్నెట్‌లో ఎవరినీ ఎప్పుడూ ట్రోల్ చేయవద్దు.



**సైబర్!
సైబర్!**





నటికెట్టు

నెటికెట్టును నేర్చుకోవడం ద్వారా, గౌరవప్రదమైన అన్లైన్ వాతావరణాన్ని స్ఫోట్ చేయగలిగిన అన్లైన్ కమ్యూనికేషన్ నిర్మించడానికి మర్యాద, గౌరవంతో కమ్యూనికేట్ చేయడానికి కృషి చేస్తాం.



ఇమెయిల్ మర్యాదలు:

- ప్రాథమిక్ టోన్ మరియు సరైన శుభాకాంక్షలను ఉపయోగించండి.
- ఇమెయిల్లను సంక్లిషించగా మరియు సూచిగా ఉంచండి.
- స్పృష్టమైన మరియు సంబంధిత సంజ్ఞీల్లోను ఉపయోగించండి.

సోషల్ మీడియా మర్యాద:

- మీ పరస్పర చర్యలలో గౌరవంగా మరియు శ్రద్ధగా ఉండండి.
- అభ్యంతరకర్మనైన భావ మరియు వ్యక్తిగత దాడులను నివారించండి.
- ఇతరుల గోప్యత మరియు అనుమతులను గౌరవించండి.



అన్లైన్ కమ్యూనికేషన్:

- స్పృష్టతను మెరుగుపరచడానికి సరైన వ్యాకరణం మరియు స్పెల్టింగ్ ఉపయోగించండి.
- అన్ని కౌపినల్లోను ఉపయోగించడం మానుకోరిడి, ఇది గ్లోగ్ అరవడాన్ని సూచిస్తుంది.
- సాంస్కృతిక భేదాలు మరియు జాపా సూక్ష్మ వైపులాయిలను గుర్తుంచుకోరిడి.



సైబర్ బెదిరింపు నివారణ:

- అన్లైన్లో ఇతరులతో దయ మరియు సానుభూతిలో వ్యవహరించండి.
- దుర్దినియోగ ప్రవర్తనను రిపోర్ట్ చేయండి మరియు నిరోధించండి.
- హానికరమైన కంటింట్లో పాల్టోనవద్దు లేదా పీర్ చేయవద్దు.



కాపీరైట్ మరియు క్రెడిబిలిట్:

- కాపీరైట్ చట్టాలు మరియు మేధి సంపత్తిని గౌరవించండి.
- ఇతరుల కంటింట్ని ఉపయోగిస్తున్నప్పుడు లేదా భాగస్వామ్యం చేస్తున్నప్పుడు సరైన క్రెడిట్ మరియు క్రెడిబిలిట్ ఇవ్వుండి.



పైవసీ మరియు భద్రత:

- అన్లైన్లో మీ వ్యక్తిగత సమాచారం మరియు పైవసీ రాళ్చించండి.
- బలమైన, ప్రత్యేకమైన పాస్‌వర్డ్లను ఉపయోగించండి మరియు టు ఫాక్ట్ అతేంబేక్సన్ ఉపయోగించండి.
- ఫిషింగ్ అటాక్ మరియు అన్లైన్ స్మార్ట్లల పట్ల జార్గతగా ఉండండి.



అన్లైన్ కమ్యూనికేషన్ మర్యాద:

- వైవిధ్యాన్ని స్వీకరించండి మరియు విభిన్న అభిప్రాయాలను గౌరవించండి.
- ద్వేషపూరిత ప్రసంగం లేదా వివక్షతతో కూడిన భావనను నివారించండి.
- నిర్వాచార్యులకు పాల్టోనండి మరియు చర్చలకు సానుకూలంగా సహకరించండి.

ఆన్‌లైన్ క్లాస్ నెటీకెట్స్



ఆన్‌లైన్ తరగతులలో నెటీకెట్ సాధన చేయడం ద్వారా, మీరు సానుకూల మరియు అనుకూలమైన అభ్యాస వాతావరణాన్ని స్పృష్టించవచ్చు. ఆన్‌లైన్ తరగతి అనుభవాన్ని ఎక్కువగా ఉపయోగించుకోవడానికి మర్యాద, గౌరవం మరియు వృత్తి సైఫుణ్ణంతే శాశ్వతించాం.



వీడియో కాన్సెర్ట్స్ మర్యాద



- బ్యార్క్‌రోడ్ నాయిన్ ను తగ్గించడానికి మాట్లాడనప్పుడు మిమ్మట్టి మీరు మూళ్లొ చేసుకోడి.
- కెమరా ఫైపు మీ దృష్టిని కొనసాగించండి.
- వీడియో కాన్సెర్ట్స్ లో ప్రాఫేషనల్ దుస్తులు ధరించండి.



చర్చల్ పాల్టొనటం

- మీ ప్రతిస్థాపనలలో సహచరులను మరియు బోధకులను గౌరవించండి.
- అంకానికి పరిమతపై చర్చలకు అర్థవంతగా సహార్థించండి.
- ఇతరులైన మాట్లాడటం లేదా అనుభితమైన భావము ఉపయోగించడం వంటి అంతరాయం కలిగించే ప్రవర్తనను నివారించండి.



సమయపాలన మరియు సంసిద్ధత

- సమయానికి తరగతికి లాగ్ అవ్యాపి మరియు అవసరమైన పస్ట్సులలో స్థిరంగా ఉండండి.
- అన్నిమొట్టిలు గడువులో పూర్తి దేయ్యాండి.
- గడువు తెదీలోగా పూర్తి చేయడంలో ఏప్లొ సహాను మీరు ఉపయోగించినట్టుయితే మందుగానే తెలియజేయండి.



ప్రాఫేషనల్ కమ్యూనికేషన్

- మీ ఆన్‌లైన్ కమ్యూనికేషన్లో స్పృష్టమైన మరియు సంక్లిష్ట భాషను ఉపయోగించండి.
- సదైన వ్యక్తరణం, స్పృష్టింగ్ మరియు విరామ చిహ్నాలను ఉపయోగించండి.
- అసభికారిక భాష రేదా అధిక సంక్లిష్ట పదాలను ఉపయోగించడం మానుకోడి.



సహచరులను మరియు బోధకులను గౌరవించడం

- ఇతరుల అభిభ్రాయాలను జాగ్రత్తగా విసండి.
- అభిప్రాయ సైఫ్ట్‌వెర్క్‌పేటి విలువ ఇచ్చుండి మరియు నిర్మాణాత్మక చర్చలలో పాల్టొనండి.
- అన్ని పదస్పర చర్యలలో గౌరవప్రదమైన భాష మరియు స్పృష్టి ఉపయోగించండి.



టెక్నికల్ ట్రబుల్-పూటింగ్ (Trouble Shooting)

- మీ ఇంటర్వెన్షన్ కెష్ట్స్‌నీ తనిఖి చేయండి మరియు అది స్థిరగా ఉండని నిర్మాణించింది.
- మీ సాఫ్ట్‌వెర్ మరియు అస్ట్రేట్‌స్‌ను అమ్-డెబ్ల్యూగా ఉంచండి.
- వెద్దినా సాంకేతిక సమస్యలకు సాంకేతిక సహాయ కెంట్రాన్ని సంప్రదించండి.



పబ్లిక్ కంప్యూటర్లు మరియు Wi-Fi యొక్క ప్రయోజనాలు

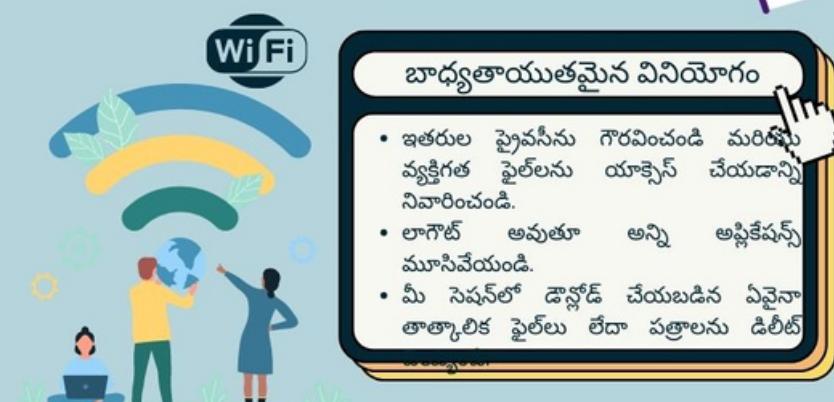
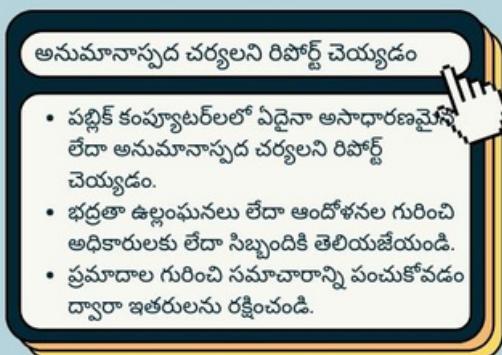
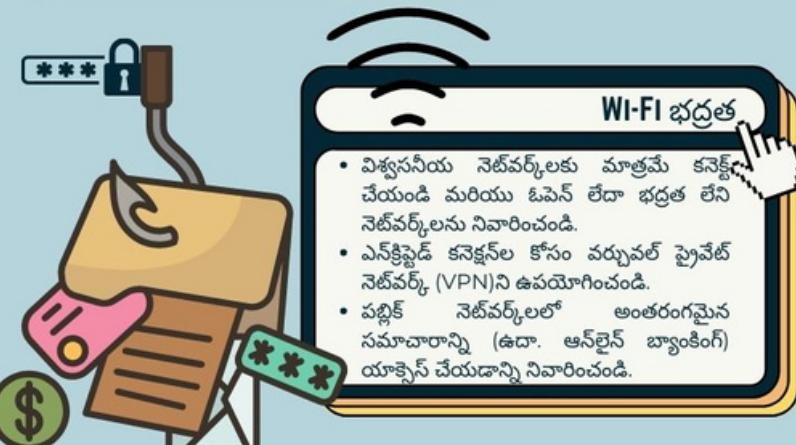
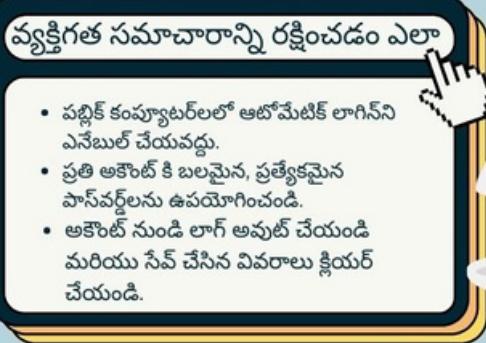
- ఇంటర్వెన్ మరియు డిజిటల్ వనరులకు అనుకూలమైన యాక్సైస్ ఉంటుంది.
- పని, అధ్యయనం మరియు కమ్యూనికేషన్ కోసం కనెక్టివిటీ పెరుగుతుంది.

HTTPS://



పబ్లిక్ కంప్యూటర్లు మరియు Wi-Fi ప్రైవ్యాడాలు

- మాల్టీప్లాట్‌ఫారమ్ మరియు హెక్సింగ్ ప్రయత్నాలు వంటి భద్రతా బెదిరింపులు ఉంటాయి.
- పేర్ డైవెన్ మరియు నెట్వర్క్‌ల కారణంగా ప్రైవ్యాస్ సమస్యలు.
- ఫిషింగ్ దాడులు మరియు స్క్రోపులకు గురవ్యే అవకాశం.





CYBER SECURA

సురక్షిత డోనలోడ్

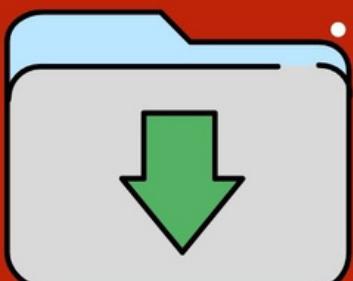
సురక్షితమైన ఆనలైన్ ప్రాపింగ్ కోసం మీరు ఎలాంటి జాగ్రత్తలు తీసుకుంటారో, మీరు మీ డివైస్ లో ఫైల్లను డోనలోడ్ చేసేటప్పుడు కూడా అంతే జాగ్రత్తగా ఉండాలి. వైరస్లు, మాల్వేర్ మరియు ట్రోజన్లు (తప్పుదోవ పట్టించే మాల్వేర్) గతంలో కంట్ ఎక్కువగా ఉన్నాయి-అందుకే మీరు ఏదైనా డోనలోడ్ చేసే ముందు జాగ్రత్త వహించాలి.



సురక్షితంగా డోనలోడ్ చేయడం ఎలా?



- ప్రసిద్ధ సైట్లు మరియు సోర్స్ నుండి మాత్రమే డోనలోడ్ చేసుకోండి



- ఎక్జెక్యూటిభల్ ఫైల్లను (.exe) చాలా జాగ్రత్తగా డోనలోడ్ చేయండి. ఇవి మీ కంప్యూటర్లో రన్ చేయడానికి ప్రోగ్రామ్లు ఉపయోగించే ఫైల్లు. అయినప్పటికీ, అవి సాధారణంగా వైరస్లు కూడి ఉంటాయి.



మాల్వెర్

VS

వైరస్

వినియోగదారుడి అనుమతి లేకుండా, సాధారణంగా హ్యోకర్ ప్రయోజనం కోసం కంప్యూటర్ యొక్క యూట్సెస్ పొందడానికి రూపొందించబడిన ప్రోగ్రామ్.



మాల్వెర్ అనగా హనికరమైన సాఫ్ట్‌వేర్ (MALicious softWARE).

Trojan, Worm, Spyware, Addware మరియు Ransomware వివిధ రకాల మాల్వెర్.



మాల్వెర్ నుండి కంప్యూటర్ను ఎలా కాపాడాలి?



వైరస్‌ల రకాలు Boot Sector, Multi Partite, Space filler, File infector, Resident, Direct action, Macro.



1. యాంటీ మాల్వెర్ ప్రోగ్రామ్ ను ఉపయోగించండి.

2. హనికరమైన ప్రోగ్రామ్లను ఎలా గుర్తించాలో తెలుసుకోండి. అనుమానాన్ని దంగా అనిపించే అప్లికేషన్లు, అలాగే మీ కంప్యూటర్ నెమ్ముదిగా నడుస్తున్నట్లు లేదా వేడెక్కడం వంటివి అనిపించినా అప్రమత్తంగా ఉండండి.

3. అనురక్షిత వెబ్‌సైట్ల నుండి డోనలోడ్ లను నివారించండి.



4. ఫైర్‌వాల్ వంటి యాంటీవైరస్ ప్రోగ్రామ్లను ఉపయోగించండి.



విమెన్ సెట్‌ట్రీ వింగ్

తెలంగాణ పోలీస్

మిషన్

భాగస్వాములు స్వాపలంబన తో మరియు వారి స్వంత అభివృద్ధి ప్రయాణాలకు నాయకత్వం ప్రహించే సామర్థ్యాన్ని కలిగి ఉండటానికి మద్దతు ఇవ్వడం మా లక్ష్యం. సంఘరశా పరిధిని తగ్గించడం, అవసరమైన మద్దతును అందించడం మరియు లావాదేవీల నేరాలు మరియు ఇతర భద్రతా సమస్యలను తగ్గించడం ద్వారా మేము ఈ దిశగా పురోగతి సాధిస్తాము. మేము నైపుణ్య శిక్షణ మరియు ఇతర అవసరమైన సహాయక వ్యవస్థల ద్వారా మహిళల క్రేయస్వను ప్రోత్సహిస్తాము.

విజన్



మహిళలు పురోగతిలో భాగస్వాములై లీంగ్-సమాన రాష్ట్రాన్ని నెలకొల్పడమే మా విజన్. TSWSW కౌనికంగా మరియు జాతీయ సంకీర్ణాల భాగస్వాములతో కలిసి పని చేసి లింగ వివక్ష లేని క్రేషణును ప్రోత్సహించే వ్యవస్థను సృష్టించడానికి ప్రయత్నిస్తుంది.

నేటి సమస్యలు మరియు మీ భద్రతకు సంబంధించి మీకు ఎప్పుడైనా సహాయం లేదా మార్గదర్శకత్వం అవసరమైతే, సోషల్ మీడియాలో మమ్మల్ని సంప్రదించడానికి వెనుకాడకండి.



TELANGANA STATE POLICE
For You With You Always



FACEBOOK :

<https://www.facebook.com/tswomensafety>
<https://www.facebook.com/TelanganaSheTeams>
<https://www.facebook.com/TSAHTofficialPage>
<https://www.facebook.com/PridePlace.WSW.TS/>
<https://www.facebook.com/BharosaWomenSafetyWing/>

TWITTER :

https://twitter.com/ts_womensafety
https://twitter.com/TS_SheTeams
<https://twitter.com/TSAHTofficial>
https://twitter.com/PridePlace_WSW
https://twitter.com/Bharosa_TSWSW



INSTAGRAM :

https://instagram.com/womensafetywing_ts
<https://www.instagram.com/tsahtofficial/>
<https://www.instagram.com/telanganasheteams/>
<https://www.instagram.com/prideplace.wsw.ts/>

Website:

<https://www.womensafetywing.telangana.gov.in/>

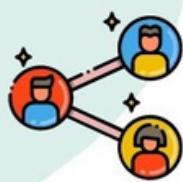
She team state what's app number: 9441669988

Reception number: 9440700906



WOMEN SAFETY WING
TELANGANA POLICE

ఆన్‌లైన్ గేములు



ఆన్‌లైన్ గేముల వ్యసనం యొక్క కారణాలు

సులభమైన యాక్షిప్స్:

- ఆన్‌లైన్ గేముల విష్టుతమైన లజ్యత వల్ల పిల్లలకు సులభంగా అందుబాటులో ఉన్నాయి.
- వివిధ పరికరాలలో గేమ్స్ ఆడకునే సాలజ్యం వ్యసనానికి దోహదం చేస్తుంది.

సామాజిక ఇంటరాక్షన్ :

- ఆన్‌లైన్ గేముల తరచుగా సాంఘికంగా కలిసి ఆడకునేందుకు వేదిక అందిస్తాయి, ఇది సహాద్యం మరియు ఇతరులతో కలిసిపోవాలని కోరుకునే పిల్లలను వ్యసనపరుస్తుంది.



ఆన్‌లైన్ గేముల వ్యసనం యొక్క లక్షణాలు

ఉపసంఖ్యారణ లక్షణాలు:

- ఆన్‌లైన్ గేముల ఆడనప్పుడు అశాంతి, చిరాకు మరియు మానసిక అందోళన చూపిస్తారు.
- అటలు ఆడకుండా ఉండటానికి స్నీయ నియంత్రణ కోర్సీతారు.

వ్యక్తిగత పరిశ్రమ మరియు నిద్ర సమయాలకు నిర్దిశ్కృతం:

- మితిమీరిన గేమింగ్ కారణంగా వ్యక్తిగత పరిశ్రమ నిర్దిశ్కృతం చేయడం, భోజనం మానేయడం మరియు సక్కమంగా నిర్దిశ్కాపోవడం.

విధ్య పురోగతిలో క్షీణితః:

- పారశాల పనితీరులో గుర్తించడిన క్షీణిత, చదువులపై ఆసక్తి తగ్గడం మరియు ఏకార్థ తగ్గడం.

సమాజంలోకి వెళ్తుండా విడిగా ఉండడం:

- కుటుంబం మరియు స్నీహితులతో తక్కువ సమయం గడువడం, సామాజిక కార్బోకలాపాల నుండి ఉపసంహరించుకోవడం మరియు నిజ జీవిత కెట్టుల కంటే ఆన్‌లైన్ పరస్పర చర్యలకు ప్రాధాన్యత ఇవ్వడం.



నివారణ చిట్టాలు

సృష్టితమైన సరిపూడ్లలను పెట్టండి:

- స్మిగ్నెన్ సమయం మరియు గేమింగ్ షైడ్యూల్స్ లకు సంబంధించి సృష్టితమైన నియమాలను ఏర్పాటు చేయండి.
- ఇతర కార్బోకలాపాలతో గేమింగ్ ను సమతుల్యం చేసుకునేలా పిల్లలను ప్రోత్సహించండి.

ప్రత్యామ్నాయ కార్బోకలాపాలని ప్రోత్సహించండి:

- ఆన్‌లైన్ గేముల నుండి దృష్టినీ మల్లించడానికి ఆరీరక కార్బోకలాపాలు, అభిరుచులు మరియు సామాజిక పరస్పర చర్యలలో పాల్ఫోన్‌డాన్స్ ప్రోత్సహించండి.

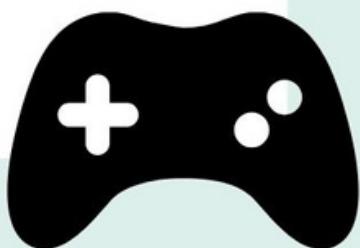
బహిరంగ సంభాషణను ప్రోత్సహించండి:

- పిల్లలు తమ గేమింగ్ అలవాట్లు మరియు ఆందోళనల గురించి చర్చించడానికి వీలుగా ఉండే వాతావరణాన్ని సృష్టించండి.
- మితిమీరిన గేమింగ్ యొక్క పరిణామాల గురించి తెలియజేయండి.



నిపుణుల సహాయాన్ని కోరండి:

- నివారణ చర్యలు తీసుకున్నప్పటిక వ్యసనం కొనసాగితే లేదా అధ్యాస్యంగా ఉంటే, గేమింగ్ వ్యసనంలో ప్రెపుణ్యం కలిగిన థరపిస్ట్లు లేదా కాన్సెలల్డ్ వంటి నిపుణుల నుండి మార్గదర్శకత్వం తీసుకోండి.



సైబర్ వ్యసనం



సైబర్ వ్యసనం అంటే ఏమిటి?

- సైబర్ వ్యసనం డీజిటల్ పరికరాలు మరియు ఆన్‌లైన్ కార్బూకలాపాల యొక్క అధిక మరియు నిర్వంధ వినియోగాన్ని సూచిస్తుంది.
- ఇది ఒకరి ఆన్‌లైన్ ప్రవర్తనల్ని నియంత్రణ కోల్పువడానికి దారితీస్తుంది మరియు జీవితంలోని వివిధ అంశాలను ప్రతికూలంగా ప్రభావితం చేస్తుంది.



సైబర్ వ్యసనం సంకేతాలు

- ఆన్‌లైన్‌లో ఎక్కువ సమయం గడపడం, వ్యక్తిగత బాధ్యతలను విస్థరించడం.
- డీస్కాన్‌ల అయినప్పుడు మాడ్ స్మార్ట్ సైగ్నల్లు, చిలాకు లేదా చంచలతను అనుభవించడం
- నిజ జీవిత సామాజిక పరస్పర చర్యల నుండి ఉపసంహరించుకోవడం మరియు ఎక్కువగా ఆన్‌లైన్ లో మాట్లాడడానికి ప్రాధాన్యత ఇవ్వడం.



సైబర్ వ్యసనం యొక్క ప్రమాదాలు

- మానసిక ఆరోగ్యంపై ప్రభావం:
 - నిరాశ, అందోళన మరియు బంటరీగా ఉండాలనే భావం పెరిగే ప్రమాదం.
 - భావేద్వ్యాగాలను నిర్వహించడంలో ఇబ్బంది కలుగుతుంది మరియు ఆత్మగౌరవాన్ని తగ్గిస్తుంది.
- శారీరక ఆరోగ్యంపై ప్రభావం:
 - నిశ్చల జీవనసైలి, బయలు పెరగడం మరియు శారీరక ద్యుద్యుమ్మెన్లో కోల్పువడం.
 - అధిక స్మార్ట్ సమయం కారణంగా నిద్రక అటుంకాలు మరియు నిద్ర విధానాలకు అంతరాయం ఏర్పడుతుంది.



బ్యాలెన్స్ చేయడానికి మ్యాహాలు

- ఆఫ్‌లైన్ ఆక్టివిటీస్ లోపాల్నాడం:
 - శారీరక కార్బూకలాపాయ, అబిరుమలు మరియు సామాజిక పరస్పర చర్యలలో పాల్టోన్స్‌న్ని ప్రోత్సహించడం.
 - కొత్త అనుకూలను అన్వేషించడి మరియు డీజిటల్ పరికరాలలో సంబంధం లేని కార్బూకలాపాలలో పాల్టోన్సించడి.
- డీజిటల్ డెటోక్స్ (Detox) సాధనాలు:
 - డీజిటల్ పరికరాల నుండి క్రమంగా విరామం తీసుకోండి.
 - విక్రాంతి, ధ్యాన లేదా ఆఫ్‌లైన్ కార్బూకలాపాలను కొనుసాగించడం కోసం సమయాన్ని కెట్టాయించాడి.
- సహాయక నెల్వర్న్సు నిర్మించడం:
 - డీజిటల్ అలవాట్ల గురించి కుటుంబం మరియు స్నేహితులతో బహిరంగ సంభాషణను ప్రోత్సహించడి.
 - ఆరోగ్యకరమైన డీజిటల్ జీవనసైలిని నిర్వహించడానికి అనుభవాలు, సప్ట్యూ మరియు మ్యాహాలను పంచుకోండి.



ఆన్‌లైన్ ప్రిడేటర్స్ మరియు చైల్డ్ ఆన్‌లైన్ యాక్షివిటీ ప్రాటెక్షన్



1

ఆన్‌లైన్ ప్రిడేటర్స్ అంటే ఎవరు?

- ఆన్‌లైన్ ప్రిడేటర్లు అంటే పిల్లలను లక్ష్యంగా చేసుకుని, ఇంటర్వ్యూన్లని ఉపయోగించి, గ్రామంగా, దశాధిక్రమాలలో గుర్తింపు వివరాలను దొంగతనంచేసే వ్యక్తులు.
- వారు తరచుగా తమ నిజమైన గుర్తింపు వివరాలను మరియు ఉద్యోగాలను పిల్లల నమ్మకం పొందడానికి మరియు ఏమార్గుడానికి దాచిపెడతారు.



2

ఆన్‌లైన్ దోషికి గురైనప్పుడు ఉండే సంకేతాలు:

రహస్య ప్రవర్తన, ఆన్‌లైన్లో ఎక్కువ సమయం గడపడం, తెలియని వ్యక్తుల నుండి బహుమతులు లేదా ఉబ్బు స్వీకరించడం లేదా మానసిక స్థితి లేదా ప్రవర్తనలో ఆట్స్ట్రోక్ మార్పులు ఉండవచ్చు.



3

ఆన్‌లైన్లో పిల్లలను రళ్చించడం ఎలా:

- ఇంటర్వ్యూల్ వినియోగం కోసం స్వప్తమైన సరిప్పులు మరియు మార్గదర్శకాలను నియమించండి.
- బలమైన, ప్రత్యేకమైన పాన్‌వెర్టీలు మరియు సురక్షితమైన ఆభ్యాసాల వినియోగాన్ని ప్రోత్సహించండి.
- సొఫ్ట్‌వర్ మీడియా స్టాటిస్టాటిక్స్ పారమ్ లలో ప్రైవెట్ సెట్‌టింగ్‌లను క్రమం తప్పుండా పర్యవేక్షించండి.
- ఆన్‌లైన్లో అపరిచితులతో సంబంధాలు పెట్టుకోవడం వల్ల కలిగే నష్టాల గురించి పిల్లలకు అవగాహన కల్పించండి.



4

పెరంటల్ కంట్లోల్ & మానిటరింగ్

- అనుచిత కంటెంట్‌కి ప్రవేశం పరిమితం చేయండి.
- ఆన్‌లైన్ కార్బూకలాపాలు మరియు స్క్యూన్ సమయాన్ని భ్రాక్ చేయండి.
- ప్రమాదాలను కలిగించగల లేదా హానికరమైన ప్రవర్తన కోసం ఆర్ట్రోలను ఆక్రమించి చేయండి.
- నిర్దిష్ట వెబ్‌సైట్లు లేదా అప్లికేషన్లను భ్రాక్ చేయడానికి లేదా పరిమితం చేయడానికి ఫిల్టరింగ్ స్సిమ్స్‌లను ఉపయోగించండి.



5

కమ్యూనికేషన్ మరియు ట్రైప్స్:

- పిల్లలు వారి ఆన్‌లైన్ అనుభవాలను వర్ణించడానికి సురక్షితమైన మరియు తప్పుప్పుని వాతావరణాన్ని సృష్టించండి.
- ఆన్‌లైన్లో అసాకర్యంగా లేదా బెదిరింపులకు గురైనట్లు భావించి సహాయం కోరమని వారిని ప్రోత్సహించండి.
- మర్దతు మరియు మార్గదర్శకట్టు కోసం వారు మీపై అధారపడగలరని వారికి భరోసా ఇవ్వండి.



6

అనుమానాస్పద కార్బూకలాపాలని రిపోర్ట్ చేయడం

- సందేశాలు లేదా స్క్యూన్‌ఫాల్స్ ల వంటి పిల్లెనా సాక్షాత్కారాలను భద్రపరచమని వారికి సూచించండి.
- స్క్యూనిక పట్టాల అమలు లేదా తప్పుపోయిన మరియు దొషించి గురైన పిల్లల కోసం జాతీయ కేంద్రం (NCMEC) వంటి సంబంధిత రిపోర్ట్‌గా ధానెలలు లేదా సంస్థలకు సమాచారాన్ని అందించండి.



సైబర్ స్పెష్స్ మరియు నివారణ చర్యలు



1 సైబర్ స్పెష్స్ అంటే ఏమిటి?

- సైబర్ స్పెష్స్ అనేది కనెక్ట్ చేయబడిన డిజిటల్ ప్రపంచాన్ని సూచిస్తుంది. ఇక్కడ సమాచారం పంచుకోవడం, యూట్యూబ్ మరియు ఫేర్ చెయ్యడం జరుగుతుంది.
- ఇది ఇంటర్వెట్, నెట్వర్క్లు, పరికరాలు మరియు డిజిటల్ కమ్యూనికేషన్ ప్లాటఫారమ్లను కలిగి ఉంటుంది.



2 వ్యక్తిగత సమాచారాన్ని రక్షించడం ఎలా:

- సోషల్ మీడియా ప్లాటఫారమ్లలో ఒపర్షెరింగ్స్ ను నివారించడం.
- గోవ్యంగా ఉండవలసిన ఆక్షిషన్స్ కోసం సురక్షితమైన Wi-Fi కనెక్ట్లను ఉపయోగించడం.
- ఆన్‌లైన్ ట్రాన్సక్షన్స్ (transaction) తో జార్ట్రుల్గా ఉండటం మరియు విశ్వసనీయమైన వెబ్‌సైట్లకు అవసరమైన సమాచారాన్ని మాత్రమే అందించడం.



3 సోషల్ మీడియా భద్రత:

- మీ ప్రైవ్యూల్ మరియు పోస్ట్లను ఎవరు చూడవచ్చే నియంత్రణ చేయడానికి ప్రైవ్యెస్చి సెట్టింగ్లను ఉపయోగించడం.
- మీరు బహిరంగంగా ఇతరులతో పంచుకునే వాటి గురించి జార్ట్రుల్ పహించడం మరియు వాటిద్వారా వచ్చే ప్రమాదాలను పరిగణనలోకి తీసుకోవడం.
- తెలియని వ్యక్తులతో మాట్లాడుకోవడం నివారించడం మరియు అపరిచితుల నుండి ప్రైవ్యెస్చి రిక్వెషన్ లేదా మెనేజెంట్ పట్ల జార్ట్రుల్గా ఉండటం.



4 సైబర్ పరిశుభ్రత:

- సఫ్టాప్ ర్యాంసాంసర్ (Ransomware) దాడుల నుండి రక్షించడానికి మీ డేటాను క్రమం తప్పకుండా బ్యాక్‌పుప్ (Backup) చేయండి.
- బలమైన పాస్‌వర్డ్లు, బయామెట్రిక్ లాక్ లేదా ఎన్‌ఎస్‌ఎఫ్ (Encryption) ఉపయోగించడం ద్వారా మీ పరికరాలను సురక్షితంగా నిర్వహించవచ్చు.
- సురక్షితమైన పైల్ ఫెరింగ్, మాల్వేర్ కోసం అటాచ్‌మెంట్లను (Attachments) స్టోర్ చేయడం మరియు ఇంటర్వెట్ నుండి పైల్లను డౌన్‌లోడ్ చేసేటప్పుడు జార్ట్రుల్గా ఉండటం.
- ప్రసిద్ధ వెబ్‌సైట్లను ఉపయోగించడం మరియు వాటికి సురక్షితమైన ట్రాన్సక్షన్ గెట్‌వేలు (Transaction Gateway) ఉన్నాయని నిర్దారించుకోవడం ("https" మరియు ప్యాడ్లాక్ చిహ్నం గమనించండి).



5 సైబర్ సంఘటనలను రిపోర్ట్ చేయండి:

- మీ స్టానిషిక చట్ట అమలు లేదా సైబర్ క్యూమ్ రిపోర్ట్‌ఇంగ్ ఏజెన్సీలను సంప్రదించండి.
- మీ ఇంటర్వెట్ సర్వీస్ ప్లాటఫారమ్ వంటి సంబంధిత సంస్థలకు తెలియజేయండి.



సైబర్ స్టాకింగ్



సైబర్ స్టాకింగ్ అంటే ఏమిటి?

- సైబర్ స్టాకింగ్ అనేది డిజిటల్ మార్కెట్లను ఉపయోగించి ఒక వ్యక్తిని పొనికర్చున మరియు నిరంతర వేధింపులు, బెదిరింపులు లేదా ట్ర్యాకింగ్ చేయడం.
- ఇది ఆన్‌లైన్ ప్లాటఫారమ్లు, ఇమెయిల్లు, సోషల్ మీడియా లేదా మెసేజింగ్ యాప్ల ద్వారా నిర్వహించబడే అవాంధిత మరియు అనుచిత ప్రవర్తనలను కలిగి ఉంటుంది.



సైబర్ స్టాకింగ్ ప్రభావం:

- భావోద్వేగ బాధ: బూధితులు భయం, ఆందోళన మరియు గోప్యతను కోల్పువచ్చాడు.
- మానసిక హాని: ఇది ఒత్తిడి, నిరాశ మరియు శక్తిహీనత యొక్క భావానికి దారిత్పిస్తుంది.
- సామాజిక ఒంటరితనం: భయం లేదా అపంపుకుం కారణంగా బూధితులు స్నేహితులు, కుటుంబ సభ్యులు మరియు ఆన్‌లైన్ కార్బూకలాపాల నుండి వెనకడవచ్చు.



సైబర్ స్టాకింగ్ ను గుర్తించడం

- స్టాకింగ్ బిహీవియర్: ఆన్‌లైన్ కార్బూకలాపాలు, వ్యాఖ్యలు మరియు పరస్పర చర్యలను తరచుగా పర్యవేక్షించడం.
- గోప్యతన్ని దాడి: అనుమతి లేకుండా వ్యక్తిగత సమాచారం లేదా చిత్రాల అవాంధిత వాయిష్టి.



మిమ్మల్ని మీరు రక్షించుకోవడం

- బలమైన ప్రైవెసీ సెట్టింగ్లను ఉపయోగించండి: సోషల్ మీడియా ప్లాటఫారమ్లలో ప్రైవెసీ సెట్టింగ్లను క్రమం తప్పకుండా చెక్ చేయండి మరియు అప్-డేల్ట్ చేయండి.
- వ్యక్తిగత సమాచారాన్ని పంచుకోవడంలో జార్గుత్త వహించండి: సున్నితమైన వివరాలను బహిరంగంగా లేదా తెలియని వ్యక్తులతో పంచుకోవడం మానుకోండి.



ఆన్‌లైన్ కమ్యూనికేషన్ భద్రత

- బలమైన పాస్‌వర్డ్లను స్థాపించండి: సురక్షితమైన పాస్‌వర్డ్ల కోసం అశ్వరాలు, సంఘయలు మరియు చిప్సుల కలయికను ఉపయోగించండి.
- లింక్లను క్లిక్ చేయడంతో జార్గుత్తగా ఉండండి: ఇమెయిల్లు, సందేశాలు లేదా సోషల్ మీడియాలో తెలియని లేదా అనుమానాస్వర్ద లింక్లపై క్లిక్ చేయడం మానుకోండి.
- ఫిషింగ్ ప్రయత్నాల పట్ల జార్గుత్త వహించండి: తెలియని మూలాల నుండి వ్యక్తిగత సమాచారం లేదా ఆర్థిక వివరాల కోరే అభ్యర్థుల పట్ల జార్గుత్త వహించండి.

సైబర్ స్టాకింగ్ నీ నివేదించండి

- డాక్యుమెంట్ ఎవిడెన్స్: స్ట్రోప్పులు, మెనేజ్మెంట్లు లేదా సైబర్ స్టాకింగ్ సంఘటనలకు సంబంధించి ఏడైనా సాక్షాత్కారి బధపరచండి.
- అధికారులకు నివేదించుట: సంఘటనలను రిపోర్ట్ చేయండి ఫోనిక చట్ట అమలు లేదా ప్రత్యేక సైబర్ క్రైమ్ విభాగాలను సంప్రదించండి.
- ఆన్‌లైన్ రిపోర్ట్సింగ్ సాధనాలను ఉపయోగించండి: సైబర్ స్టాకింగ్ సంఘటనలను సంబంధిత ప్లాటఫారంలు లేదా సోషల్ మీడియా నెట్‌వర్క్లకు రిపోర్ట్ చేయండి.



ప్రజలను అవగాహన కలిగి, అప్రమత్తంగా ఉండటానికి మరియు వారి ఆన్‌లైన్ భద్రతకు ప్రాధాన్యతనివ్యవస్థ ప్రోత్సహించండి.



ఆన్‌లైన్ వేషధారణ (GROOMING)



ఆన్‌లైన్ గ్రామింగ్ అంటే ఏమిటి?

ఆన్‌లైన్ గ్రామింగ్ అనేది ఆన్‌లైన్లో ప్రాడెటర్ మానసికంగా, లెంగికంగా లేదా ఆరికంగా దోషించి చేసే ఉండేశ్యంతో బాధితుడిలో నమ్మకాన్ని పెంచికొనే ప్రక్రియ.



గ్రామింగ్ మ్యాప్లోలు:



- తప్పుడు గురించు వివరాలు: ప్రాడెటర్ నకిలీ ప్రోఫైల్లను స్థాపిస్తారు లేదా విశ్వసనీయంగా కనిపించడానికి దిగెలించబడిన గుర్తింపులను ఉపయోగిస్తారు.
- బిల్డింగ్ ట్రైస్: ప్రాడెటర్ బాధితుడిలో జంధాన్ని పెంపొదించుకొవడానికి సమయం మరియు కృషిని పెట్టుబడినా పెడతారు, వారి విశ్వసాన్ని పొంచుతారు.
- ఎమోషనల్ మానిప్యూలేషన్: ప్రాడెటర్ వారి బాధితులని వారిపై ఎమోషనల్ గా ఆధారపడేలా చేస్తారు.
- గోప్యత మరియు బంటరితనం: ప్రాడెటర్ బాధితులతో వారి సంబంధాన్ని రహస్యంగా ఉంచబడానికి ప్రోత్సహిస్తారు మరియు స్నేహితులు కుటుంబ సభ్యులతో సంబంధాలను తెంచుకునేలా చేస్తారు.
- దోషి: విశ్వసు ఏర్పడిన తుల్యత ప్రాడెటర్ లైంగిక వేధింపులకు పాల్సినప్పుడు లేదా ఆఫ్సైన్ కలవడానికి ప్రయత్నించవచ్చు.



గ్రామింగ్ సంకేతాలు:

- ఆన్‌లైన్ ఆఫ్సివిటీస్ గురించి అధిక ప్రైవేసీ.
- కుటుంబం మరియు స్నేహితుల నుండి దూరమయ్యటం వంటి ప్రవర్తన మరియు తీవ్రమైన మార్పులు.
- తెలియని వ్యక్తి నుండి ఒహుమతులు లేదా డబ్బులు నుండి వెచ్చికించడం.
- ఆన్‌లైన్లో ఎక్కువ సమయం గడువుడం.
- ఆన్‌లైన్లో మాత్రమే తెలిసిన వారితో మానసికంగా అనుబంధం ఏర్పరుచుకోవడం.

3



4 గ్రామింగ్ నుండి మిమ్మల్ని మరు రక్షించుకోవడం ఎలా:

- విద్యుత మరియు అవగాహన: ఆన్‌లైన్ గ్రామింగ్
- యొక్క ప్రమాదాల గురించి తెలుసుకోడి మరియు ఈ జ్ఞానాన్ని ఇతరులతో పంచుకోండి.
- గోప్యతా సెట్టింగ్లు: సిపల్ మీడియా స్టాపివర్మెలు మరియు ఆన్‌లైన్ ఖాతాలలో మీ ప్రైవేసీ సెట్టింగ్లను కుటుంబ తుల్యతండా పర్యవ్హక్క చేయించి మరియు సద్గులూ చేయించి.
- బలమైన ప్సౌన్‌వర్క్షులు: మీ ఆన్‌లైన్ ఖాతాల కోసం ప్రత్యేకమైన, కుటుంబ ప్సౌన్‌వర్క్షును ఉపయోగించి మరియు వాటిని కుటుంబ తుల్యతండా అవ్వడిట్ చేయిండి.
- షేర్ చేయడానికి ముందు ఆలోచించండి: ఆన్‌లైన్లో అపరిచితులతో వ్యక్తిగత సమాచారం, ఫోటోలు లేదా మీడియాలను షేర్ చేయడం జూర్తుగా ఉండండి.
- మీ స్యూపాన్ని విశ్వసించండి: ఏదో అసాక్షర్యగా లేదా అనుమానస్థదగా అనిపిస్తే మీ అలోచనను నమ్మండి మరియు నమ్మగలిగి పెద్దల నుండి సహాయం తీసుకోండి.
- కిమెన్ కమ్యూనికేషన్: మీ ఆన్‌లైన్ కార్బుకలాపాల గురించి మీ తల్లిదండ్రులు, సంక్రములు లేదా ఉపాధ్యాయులతో బహిరంగంగా నిజాయాతీత్ కూడిన సంఘర్షణను నిర్వహించండి.



ఇమెయిల్ బెదిరింపులు



ఇమెయిల్ బెదిరింపులు అనేది వ్యక్తిగత సమాచారానికి అనధికారిక యూక్సెన్స్ ని పొందడానికి లేదా మాల్వైర్ తో సిస్టమ్లకు హాని కలిగించడానికి సైబర్ నేరస్తులు ఉపయోగించే సాధారణ పద్ధతి. ఈ బెదిరింపుల గురించి తెలుసుకోవడం మరియు మిమ్మల్ని మీరు ఎలా రక్షించుకోవాలో తెలుసుకోవడం చాలా ముఖ్యం.



1

ఫిషింగ్ దాడులు:

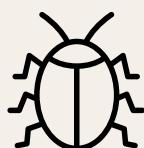
- ఫిషింగ్ దాడులు చట్టబడ్డంగా కనిపించే ఇమెయిల్లను కలిగి ఉంటాయి, అయితే సున్నితమైన సమాచారాన్ని బహిర్జతం చేసేలా రెసిపిఎంట్స్ ని మోసరించడం లక్ష్యంగా పెట్టుకున్నాయి.
- భూతా ఆధారాలు, ఆర్థిక వివరాలు లేదా వ్యక్తిగత సమాచారం కోసం అడిగే అనుమానాస్పద ఇమెయిల్ల పట్ల జాగ్రత్త వహించండి.
- అత్యవసర లేదా బెదిరింపు భావ వ్యక్తిగత లోపాలు లేదా అసాధారణ ఇమెయిల్ చిరునామాల పట్ల జాగ్రత్తగా ఉండండి.

2

మాల్వైర్ మరియు జోడింపులు

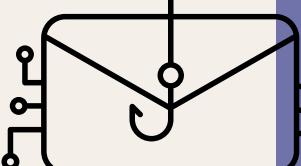
(Attachments):

- హనికరమైన జోడింపులు మాల్వైర్, వైరస్లు లేదా ర్యాంసోవర్ కలిగి ఉండవచ్చు.
- తెలియని లేదా అనుమానాస్పద మూలాల నుండి జోడింపులు తెరవడం మానుకోండి.
- .exe, .zip లేదా .bat వంటి అసాధారణ ఫైల్ పొడిగింపులతో ఇమెయిల్ జోడింపుల పట్ల జాగ్రత్తగా ఉండండి.



3 మోసపూరిత ఇమెయిల్లు:

- మోసపూరిత ఇమెయిల్లు చట్టబడ్డమైన మూలాలను అనుకరిస్తాయి, రెసిపిఎంట్స్ నమ్మదగిన మూలం నుండి వచ్చినప్పని భావించేలా చేస్తాయి.
- ఏవైనా అనుమానతలు లేదా మార్పులు కోసం పంపినవారి ఇమెయిల్ చిరునామాను ధృవీకరించండి.
- లింక్లపై క్లిక్ చేయడానికి ముందు అవి చట్టబడ్డమైన వెబ్సైట్లకు దారితీస్తిన్నాయో లేదో చెక్ చేయండి.



4 ఇమెయిల్ స్క్రోమ్లు:

- ఇమెయిల్ స్క్రోమ్లు రెసిపిఎంట్స్ ను డబ్బు లేదా సున్నితమైన సమాచారాన్ని అందించమని మోసరించడానికి ప్రయత్నిస్తాయి.
- బహుమతులు, వారసత్వం లేదా లాటరీ విజయాలను వాగ్గానం చేసే ఇమెయిల్ల పట్ల సందేహస్పదంగా ఉండండి.
- తెలియని వ్యక్తుల నుండి ఆర్థిక సహాయం లేదా షైర్ ట్రాన్స్ఫర్ కోసం రిక్వెస్ట్ లను నిరాకరించండి.



5 మిమ్మల్ని మీరు రక్షించుకోండి:

- తెలిసిన ఒగ్గు నుండి రక్షించడానికి మీ ఇమెయిల్ సాఫ్ట్వేర్ మరియు యాంటీవైర్స్ ప్రోగ్రామ్లను అప్ డేట్ చేయండి.
- అదనపు భద్రత కల్పించడానికి మీ ఇమెయిల్ భూతాల కోసం మల్టీపుల్ ఫాక్టర్ అంటెంటీప్రోవ్ (MFA)ని ప్రారంభించండి.
- మీ ఇన్బాస్ నుండి అనుమానాస్పద ఇమెయిల్లను క్రమం తప్పకుండా తెలగించండి.

6 అనుమానాస్పద ఇమెయిల్లను రిపోర్ట్ చేయుడం:

- బాధితుల నుండి ఇతరులను రక్షించడంలో సహాయపడటానికి ఫిషింగ్ ఇమెయిల్లను మీ ఇమెయిల్ ప్రావైడర్ లేదా IT బిభాగానికి రిపోర్ట్ చేయుండి.
- అనుమానాస్పద ఇమెయిల్లను యాంటీ ఫిషింగ్ వర్క్‌ఐమ్ ర్యాప్కు పారావ్రాత్ చేయండి (reportphishing@apawg.org) or the Federal Trade Commission (spam@uce.gov).





పాస్వర్డ్ బెదిరింపులు



సాధారణ పాస్వర్డ్ బెదిరింపులు

- బ్రూట్ ఫోర్స్ అట్కేట్ (Brute force attacks): హోకట్లు వివిధ కలయికలను ప్రయత్నించడం ద్వారా పాస్వర్డ్లను ఉపయోగించడానికి అటోమేటిడ్ స్వీచ్‌వేర్స్ ను ఉపయోగిస్తారు.
- పాస్వర్డ్ క్రైకింగ్: సైబర్ నేరథులు ఎన్జెప్లెట్ (Encrypted) పాస్వర్డ్లను డెక్షిప్ చేయడానికి అధునాతన పద్ధతులను ఉపయోగిస్తారు.
- ఫిషింగ్ డాడలు: మొసపురిత ఇమెయిల్లు లేదా వెబ్‌సైట్ల ద్వారా వారి పాస్వర్డ్లను ఒప్పాల్తతం చేసేలా స్క్రూమర్లు వినియోగారులను మొసిస్తారు.
- పాస్వర్డ్ పునర్వినియాగం: బహిల భాతాలలో ఒక పాస్వర్డ్ ను ఉపయోగించడం ప్రమాదాన్ని పెచుతుంది.

బలమైన పాస్వర్డ్లను సృష్టించడం



- పాస్వర్డ్ పాడము: కాంప్లెక్సీటీ పిండానికి కెసిసం 12 అక్షరాల పాడము ఉండే పాస్వర్డ్ ను ఎంచుకోండి.
- కాంప్లెక్సీటీ: పెద్ద అక్షరాలు మరియు చిన్న అక్షరాలు, సంఖ్యలు మరియు ప్రత్యేక అక్షరాల మత్తుమాన్ని ఎంచుకోండి.
- వ్యక్తిగత సమాచారాన్ని నివారించండి: వెద్దు, పుట్టిన తేదీలు లేదా సులభంగా ఉపయోగించగలగే సమాచారాన్ని ఉపయోగించవద్దు.
- పాస్వర్డ్ అప్లోడ్: పదాల మధ్య భాషీలు లేదా ప్రత్యేక అక్షరాలతో గుర్తుండిపోయే పదబంధాన్ని ఉపయోగించడాన్ని పరిగణించండి.



టు ఫాక్టర్ అతేంట్కేషన్ (2FA)

- అంయబాటులో ఉన్నప్పుడ్లా 2FAని పూర్ణంగా ఉదాహరించండి. ఇది రెండవ దృవీకరణ దశను కోరడం ద్వారా అదనపు భద్రత పొను జోడిస్తుంది.
- సాధారణ పద్ధతులలో SMS కోడ్లు, ప్రామాణికరణ యాప్లు లేదా బయోమెట్రిక్ దృవీకరణ ఉన్నాయి.



- బలమైన పాస్వర్డ్లను సురక్షితంగా నిల్వ చేయడానికి మరియు రూపొందించడానికి ప్రసిద్ధ పాస్వర్డ్ మేనేజర్ ఉపయోగించండి.
- సంక్లిష్టమైన పాస్వర్డ్లను గుర్తుంచుకోవడానికి మరియు అవసరమైనప్పుడు వాచిని స్క్రోయం చేసుంది.
- అదనపు భద్రత కోసం పాస్వర్డ్ మేనేజర్ బలమైన ఎన్క్రిప్షన్ మరియు మాస్టర్ పాస్వర్డ్ ఉండిని నిర్మాంచుకోండి.

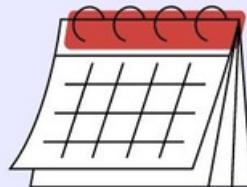


పాస్వర్డ్ మేనేజర్



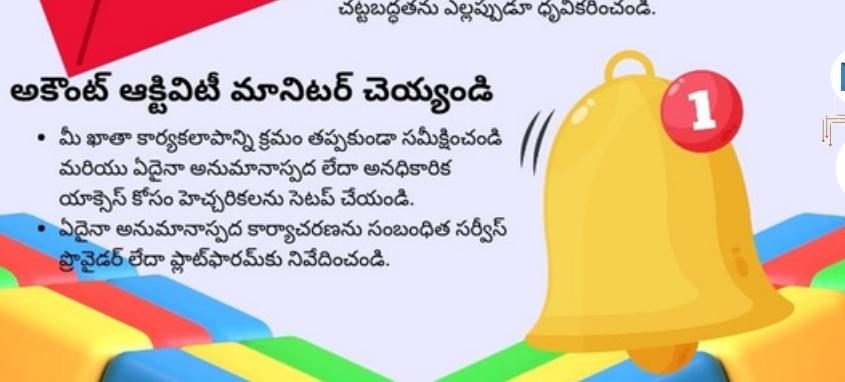
రెగ్యులర్ పాస్వర్డ్ అప్డేట్లు

- ముఖ్యంగా స్క్రీన్‌సెప్ట్ ఫాలాల కోసం పాస్వర్డ్లను క్రమం తప్పకుండా మార్చండి.
- ఎక్స్‌ప్రో కాలం ఒకే పాస్వర్డ్ నీ ఉపయోగించడం మానుకోండి.
- పాస్వర్డ్లను అప్డేట్ చేయడంలో మీకు సహాయపడచానికి రిమైండర్లను ఉపయోగించండి.



అకౌట్ ఆక్షిట్ మానిటర్ చెయ్యండి

- మీ భాతా కార్బూకలాపాన్ని క్రమం తప్పకుండా సమీక్షించండి మరియు ఏడైనా అనుమానస్వద లేదా అనందికారిక యాక్సెస్ కోసం హెచ్చరికలను నెట్‌వర్క్ చేయండి.
- ఏడైనా అనుమానస్వద కార్బూపరణను సంబంధిత సర్వీస్ ప్రోటోకాల్ లేదా స్టాటిషార్మెక్ నివేదించండి.



క్రెడిట్ కార్డ్ మొనూల పట్ల జాగ్రత్తవహించండి:

మిమ్మల్ని మీరు రక్షించుకోండి



1 క్రెడిట్ కార్డ్ స్ట్రోమ్ ల రకాలు

1. ఫిషింగ్:

- స్ట్రోమ్ లు మిమ్మల్ని మొనించే ఇమెయిల్లు లేదా వెబ్సైట్లను ఉపయోగించి క్రెడిట్ కార్డ్ వివరాలను తీసుకుంటారు.



2. స్క్రోమ్ లో బెంగ్లు:

- ATMలు లేదా పాయింట్ ఆప్ సెర్ టిప్పున్టీ వద్ద క్రెడిట్ కార్డ్ వివరాలను దొగ్గిలింపడానికి నేర్చులు పరికరాలను జాగ్రత్తగా ఉండండి మరియు ట్ర్యాంపరింగ్ కోసం డెక్ చేయండి.



3. కార్డ్ సాట్ ప్రైవెట్ మొనం:

- స్ట్రోమ్ లు అన్టెన్ లేదా ఫోన్ ద్వారా కొమగ్గే కోసం దొగ్గిలింపబడిన క్రెడిట్ కార్డ్ సమాచారాన్ని ఉపయోగిస్తారు.



4. గుర్తింపు దొగ్గతనం:

- మొసమూరిత క్రెడిట్ కార్డ్ భాతాలను తెరవడానికి దొగ్గలు వ్యక్తిగత సమాచారాన్ని దొగ్గిస్తారు.



3 నివారణ చిట్టాలు

- మీ భాతాలో అనధికార ధార్యీలు లేదా అనాధారణ కార్యాదరణ జరుగుట.
- వ్యక్తిగత లేదా క్రెడిట్ కార్డ్ సమాచారాన్ని అడుగుతూ అనుమాన్సుద ఇమెయిల్లు లేదా కాల్లు వచ్చుట.
- ఉపయోగించని క్రెడిట్ కార్డ్ ఆఫర్లు లేదా భాతా నోటిఫికేషన్లు అందుట.



4 మీరు బాధితుడు అయితే ఏమి చేయాలి

- అనధికార ధార్యీలను రిపోర్ట్ చేయడానికి క్రెడిట్ కార్డ్ జారీదేసేవారిని లేదా బ్యాంక్ ను సంప్రదించండి.
- తదుపరి మొసమూరిత కార్యకలాపాలను నిరోధించాలనికి మీ క్రెడిట్ నివేదికలపై మొసమూరిత లావాదేవిల పోట్టికును ఉంచండి.
- ప్రానిక వట్ట అమలు సంస్థలో రిపోర్ట్ ను షైల్ చేయండి.
- కొత్త భాతాలు తెరవుండా నిరోధించాలనికి మీ క్రెడిట్ రిపోర్ట్ లను స్టుటింపబేయడాన్ని పరిగణించండి.



5 ముగింపు:

క్రెడిట్ కార్డ్ స్ట్రోమ్ ల నుండి మిమ్మల్ని మీరు రక్షించుకోవడంలో అప్రమత్తొగా మరియు సద్గున్హాన్తో ఉండడం ద్వారా కీలకం. ఈ చిట్టాలను అనుసరించడం ద్వారా మరియు ఎదురుగాల ముఖ్యుల గురించి తెలుసుకోవడం ద్వారా, మీరు మీ ఆర్థిక శైయస్సును కాపాడుకోవచ్చు.

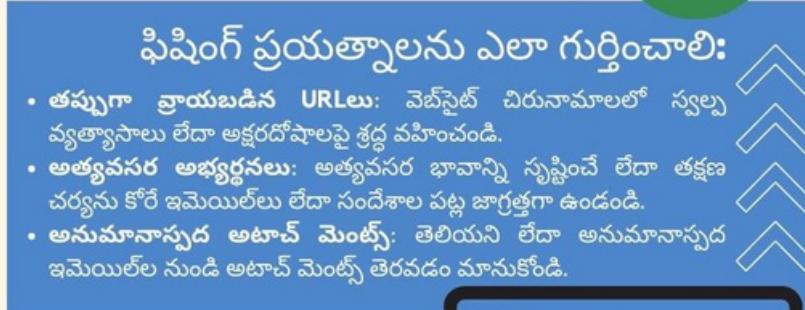


ఫిబీంగ్: ఆన్‌లైన్ స్క్రోమ్ల నుండి మిమ్మల్ని మీరు రక్షించుకోండి



సాధారణ ఫిబీంగ్ పద్ధతులు:

- ఇమెయిల్ స్ప్యాఫింగ్: పేరున్న మూలం నుండి వచ్చినట్లుగా ఇమెయిల్లను పంపడం నిజానికి అవి మోసపూరితమైనది.
- మోసపూరిత లింక్లు: నకిలీ వెబ్‌సైట్లకు దారి మళ్ళించే ఇమెయిల్లు లేదా సందేశాలలో హెనికరమైన లింక్లను పొందుపరచడం.
- నకిలీ లాగిన్ పేజీలు: వినియోగదారు పేర్లు, పాస్‌వర్డ్లు లేదా ఇతర వ్యక్తిగత సమాచారాన్ని దీంగిలించడానికి నకిలీ లాగిన్ పేజీలను సృష్టించడం.



ఫిబీంగ్ ప్రయత్నాలను ఎలా గుర్తించాలి:

- తప్పుగా ప్రాయబడిన URLలు: వెబ్‌సైట్ చిరునామాలలో స్వల్ప వ్యక్తిగత స్క్రోమ్లను లేదా అక్షరదోషాలపై శ్రద్ధ వహించండి.
- అత్యవసర అభ్యర్థనలు: అత్యవసర భావాన్ని సృష్టించే లేదా తక్షణ చర్యను కోరే ఇమెయిల్లు లేదా సందేశాల పట్ల జార్జుతగా ఉండండి.
- అనుమానాస్కర అట్టాచ్ మెంట్స్: తెలియని లేదా అనుమానాస్కర ఇమెయిల్ల నుండి అట్టాచ్ మెంట్స్ తెరవడం మానుకోండి.



ఫిబీంగ్ నుండి మిమ్మల్ని మీరు రక్షించుకోవడం:

- మూలాన్ని ట్రైఫిక్‌రించండి: ఏదైనా వ్యక్తిగత సమాచారాన్ని అందించే ముందు ఇమెయిల్లు, సందేశాల లేదా వెబ్‌సైట్ల వ్యవస్థలను ఒకటికి రెండుసార్లు డెక్ చేయండి.
- లింక్లు మరియు అట్టాచ్ మెంట్స్ తో జార్జుతగా ఉండండి: అను URL ను వీడింగచానికి లింక్లను చేరుకోండి మరియు వాటిని తెరవడానికి ముందు మాల్‌వెర్స్ కోసం జోడింపులను స్క్రోమ్ చేయండి.
- మి వ్యక్తిగత సమాచారాన్ని భద్రపరచండి: ఆన్‌లైన్లో లేదా అనురక్షిత థాసెలల ద్వారా సున్నితమైన డెటాను పంచుకోవడం మానుకోండి.

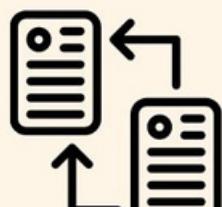


సెక్యూరిటీ స్టాప్‌వేర్‌తో అప్‌డేట్ అవ్వండి:

- మీ పరకరాల్ యాంటీ-వైరస్ మరియు యాంటీ-మాల్‌వెర్ స్టాప్‌వేర్లను ఇన్స్టాల్ చేయండి మరియు క్రమం తప్పకుండా అప్‌డేట్ చేయండి.
- అనధికార యాక్సెస్ నుండి రక్షించడానికి సమ్మక్షమైన ప్రెర్వాల్సును ఉపయోగించండి.

అనుమానాస్కర కార్బోవరణను రిపోర్ట్ చేయండి:

- మీరు ఫిబీంగ్ ప్రయత్నాలను ఎదుర్కొంటే, వాటిని తగిన అధికారులకు లేదా సంస్థలకు రిపోర్ట్ చేయండి.
- మీ ఇమెయిల్ ప్రాఫైడర్ లేదా యాంటీ-ఫిబీంగ్ వర్గం గ్రూప్ (APWG)కి అనుమానాస్కర ఇమెయిల్లు లేదా సందేశాలను పార్ట్‌వర్డ్ చేయండి.





ఇమెయిల్ లాటరీ

నైజీరియన్ లెటర్ స్క్యూమ్ అని కూడా అంటారు



ఈ స్క్యూమ్, బహుశా చాలా కాలంగా
నడుస్తున్న ఇంటర్వెట్ మోసాలలో ఒకటి,
మీరు ఒక అధికారిక ప్రభుత్వ ఉద్యోగి,
వ్యాపారవేత్త అని చెప్పుకునే వ్యక్తి నుండి
ఎమోషనల్ మేసేజ్ అందుకుంటారు,
లేదా సంపన్న విదేశీ కుటుంబ
సభ్యుడు విదేశీ బ్యాంకు నుండి పెద్ద
మొత్తంలో డబ్బును తిరిగి పొందడంలో
వారికి సహాయం చేయమని మిమ్మల్ని
అడుగుతాడు. బదులుగా, వ్యక్తి మీకు
కొంత డబ్బు ఇస్తానని వాగ్గానం
చేస్తాడు. వారు ఒప్పందాన్ని
చట్టబద్ధంగా కనిపించేలా చేసే నకిలీ
అగ్రిమెంట్ కూడా పంపించవచ్చు.



అటువంటి స్క్యూమ్ను నివారించడానికి ఏమి
చేయవచ్చు?



ఈ మేసేజ్ ని
పట్టించుకోకుండా,
రిపోర్ట్ చెయ్యడం
ఉత్తమం



REPORT SCAM



సైబర్ వేదింపు



ఎవరైనా వేరొకరి గురించి చెడుగా, హానికరమైన, తప్పుడు కంటింట్సు పేర్ చేసినప్పుడు సైబర్ వేదింపు జరుగుతుంది. ఇది సెల్ ఫోన్సు, కంప్యూటర్లు మరియు టాబ్లెట్లు వంటి డిజిటల్ పరికరాలలో జరుగుతుంది.

సైబర్ వేదింపులు



2019 స్కూల్ క్లైమ్ సప్లిమెంట్ ప్రకారం 9-12 తరగతులలో

16% మంది విద్యార్థులు సైబర్ వేదింపును అనుభవిస్తున్నారని సూచిస్తుంది.



2019 యూత్ రిస్క్ బిహీవియర్ సరైన్ లెన్స్ సిస్టమ్ ప్రకారం

15.7% ప్రాస్కూల్ విద్యార్థులు అన్లైన్ లో వేదింపులకు గురయ్యారు.

ఎవరైనా అన్లైన్ లో నీచమైన, బాధక లింగించే లేదా ఇబ్బందికరమైన కామెంట్స్ లేదా పుకాద్దను పోస్ట్ చేయడం.

వేరొకరి గురించి వ్యక్తిగత లేదా తప్పుడు సమాచారాన్ని పోస్ట్ చేయడం కోసం అన్లైన్ లో మరొకరిలా నటిస్తున్నారు.

ఎవరిషైనా బాధపెడతామని బెదిరించడం లేదా ఆత్మహత్య చేసుకుంటామని చెప్పడం.

మృత్యు పోలు

బకరి గురించి బాధ కలిగించే వెబ్జెషన్ స్పృష్టించడం.



నివారణ

డాక్యుమెంట్



ఏదు జరుగుతుందో మరియు ఎక్కడ జరుగుతుందో రికార్డ్ చేయండి. వీలైతె హానికరమైన పోస్ట్సులు లేదా కంటింట్సు స్పీఫ్స్ ఫాట్లును తీయండి. వేదింపు అనేది మళ్ళీ మళ్ళీ జరిగే విషయాలు అని చాలా చట్టాలు మరియు విధానాలు గమనించాయి, కాబట్టి దానిని డాక్యుమెంట్ చేయడానికి రికార్డ్లు సహాయపడతాయి.

సపోర్ట్



పీట్లల గురించి చెడుగా లేదా హానికరమైన కంటింట్సు పోస్ట్లు పరిస్థితిని సరి చేయడానికి సహాయాలు, సలహారూలు బహిరంగంగా జోక్యూ చేసుకుంటారు. ఇలాంటి స్థితిలో బాధపడినవారికి మరింత తైపుఱుట సహాయం అవసరమని కనుగొనడానికి ప్రయత్నించండి.

రిపోర్ట్



సోప్లెట్ మీడియా ఫ్లాట్ ఫారమ్లు మరియు రిపోర్ట్‌లింగ్ ప్రక్రియలను కలిగి ఉంటాయి. పీట్లలకి శారీరకంగా వేదింపులు వచ్చినట్లుయితే లేదా నేరం లేదా చట్టానిర్దారింపున ప్రవర్తన సంభవించినట్టుయితే, దానని పోలీసులకు రిపోర్ట్ చేయుండి.



మొబైల్ భద్రత

మీ పరికరాన్ని లాక్ చేయండి

- అనధికార యాక్సెస్‌ను నిరోధించడానికి బల్లైన్ PIN, పాస్‌వర్డ్ లేదా బయోమెట్రిక్ ప్రమాణీకరణ (వేలిముర్ద లేదా ముఖ గుర్తింపు) సెట్ చేయుండి.
- అదనపు భద్రత కోసం కోఠ సమయం తర్వాత ఆఫ్-లాక్ అయ్యేల సెట్ చేయుండి.
- అవడేట్లు తరచూ బగ్గు పరిష్కరించే భద్రతా ప్యాచ్‌లను కలిగి ఉంటాయి.

విశ్వసనీయ యాప్‌లను ఇన్స్టాల్ చేయండి మరియు పథ్థిక్ WI-FI పథ్థ జార్జుత్తగా ఉండం

- అధికారిక యాప్ ప్టోర్ల నుండి మాత్రమే యాప్‌లను డౌన్‌లో చేసుకోండి (ఉదా., Google Play Store, Apple App Store).
- ఇన్స్టాల్ చేసి ముందు వినియోగదారు సమీళ్లు, రెటీంగ్లు మరియు యాప్ అనుమతులను వెక్ చేయండి.
- ఎన్క్రిప్షన్ చేసి అనురక్షిత పథ్థిక్ Wi-Fi నెట్‌వర్క్‌లను వాడటం నిపారించండి.
- పథ్థిక్ నెట్‌వర్క్‌లలో సురక్షిత ప్రొజింగ్ కోసం వర్ధువల్ ప్రొవెట్ నెట్‌వర్క్ (VPN)ని ఉపయోగించండి.

మొబైల్ బ్రోజింగ్‌ని సురక్షితం చేయుండి మరియు ప్రండ ప్రై డివైస్ ఎనెబుల్ చేయుండి

- వ్యక్తిగత సమాచారాన్ని నమోదు చేసేటప్పుడు లేదా ఆర్టిక్ లాప్‌టాప్‌లేవీలు నిర్వహించేటప్పుడు సురక్షిత వెబ్‌సైట్లను (HTTPS) ఉపయోగించండి.
- ఇమెయిల్లు, సదేశాలు లేదా వెబ్‌సైట్లలో అనుమానస్వర లింక్లపై క్లిక్ చేయడం పథ్థ జార్జుత్తగా ఉండండి.
- ప్రండ ప్రై డివైస్ ఫీఫర్ మీ డేటాను రక్షించడంలో మరియు అనధికారిక యాక్సెస్‌ను నిరోధించడంలో సహాయపడుతుంది.

యాప్ అనుమతులు

- ఏ సమాచారాన్ని యాప్‌లు యాక్సెస్ చేయవచ్చే నియంత్రించడానికి యాప్ అనుమతులను సమీక్షించండి.
- మీరు విశ్వసించే యాప్‌లకు అవసరమైన అనుమతులను మాత్రమే మంజూరు చేయండి.
- అనుమానస్వర లింక్లపై క్లిక్ చేయడం లేదా తెలియని మూలాలకు వ్యక్తిగత సమాచారాన్ని అందించడం మానుకోండి.

మీ డేటాను బ్యాక్‌ప్యూప్ చేయండి

- దొంగతనం, నష్టం లేదా సిస్టమ్ ఫేల్‌యూం సంభవించినప్పుడు డేటా నష్టాన్ని నిపారించడానికి మీ మొబైల్ పరికరాన్ని కుమం తప్పకుండా బ్యాక్‌ప్ప్ చేయండి.
- ముఖ్యమైన పైల్లులను బ్యాక్‌ప్ప్ చేయడానికి క్లోడ్ ను ఉపయోగించండి లేదా కంప్యూటర్కు కనెక్ట్ చేయండి.

ఎమ్ముల్ని మీరు వైతన్యవంతులను చేసుకోండి

- ఆజ్ఞా మొబైల్ భద్రతా బెదిరింపులు మరియు ఉత్తమ అబ్యోసాల గురించి ఎప్పటిక్పుడు తెలుసుకోండి.
- మొబైల్ వినియోగదారులను లక్ష్యంగా చేసుకునే సాప్లెర్ ఇంజనీరీంగ్ వ్యాప్కలు మరియు స్కూల్మ్స్ ల పథ్థ జార్జుత్తగా వ్యాపారండి.

సోషల్ నెట్వర్కింగ్



1. బలమైన ప్రైవెచ్చ సెట్టింగ్లను ఎంచుకోడి

- సోషల్ నెట్వర్కింగ్ ఫ్లాట్ ఫారమ్లలో మీ గోప్యతా సెట్టింగ్లను సమీక్షించండి. మరియు సద్గుబాటు చేయండి.
- విశ్వసనీయ కనెక్షన్లకు మాత్రమే వ్యక్తిగత సమాచారం పరిమితం చేయండి.



2. మీరు పంచుకునే వాటిని గుర్తుంచుకోడి



- మీరు పోస్ట్ చేసే ముందు ఆలోచించండి: మీకు వ్యతిరేకంగా ఉపయోగించగలిగే నున్నితమైన సమాచారాన్ని పేర్ చేయండి.
- వ్యక్తిగత వివరాలు, ఆర్టికల్స్ సమాచారం లేదా ప్రయాణ ప్రచారికలను పట్టింగ్ కా పంచుకోవడంలో జాగ్రత్తగా ఉండండి.



3. ప్రైండ్ రిక్వెస్ట్ తో జాగ్రత్తగా ఉండండి

- మీకు తెలిసిన మరియు విశ్వసించే వ్యక్తుల నుండి ప్రైండ్ రిక్వెస్ట్ లను మాత్రమే అంగీకరించండి.
- మీ వ్యక్తిగత సమాచారానికి ఆక్స్సెస్ కోరే అనుమతాస్వద లేదా నక్కలీ ప్రొఫైల్ పట్ల జాగ్రత్తగా ఉండండి.



5. క్లిక్ చేసే ముందు ఆలోచించండి

- అనుమతాస్వద లింక్లను క్లిక్ చేయడం మానుకోండి, అవి స్నేహితుల ద్వారా పేర్ చేయబడినపుటికీ లేదా ప్రసిద్ధ సైట్ల నుండి వచ్చినవిగా కనిపించినపుటికీ జాగ్రత్తగా ఉండండి.
- లింక్లను వాడడానికి ముందు వాటి ప్రామాణికతను ధృవీకరించండి.



4. ఫిషింగ్ ప్రయత్నాల గురించి తెలుసుకోడి

- సోషల్ నెట్వర్క్లలో సందేశాలు, వ్యాఖ్యలు లేదా లింక్ల ద్వారా ఫిషింగ్ స్క్రోమ్లు ఉన్నాయేమా చూడండి.
- వ్యక్తిగత సమాచారం లేదా లాగిన్ ఆధారాల కోసం అభ్యర్థనలపై సందేశాలను ఉండండి.



6. యాప్ అనుమతులను క్రమం తప్పకుండా సమీక్షించండి

- మీ సోషల్ నెట్వర్కింగ్ ఫ్లాట్ ఫారమ్ల గోప్యతా విధానాలపై అప్పటికీ గా ఉండండి.
- ఫ్లాట్ ఫారమ్ ద్వారా మీ డేటా ఎలా సేకరించబడింది, ఉపయోగించబడుతుంది మరియు పేర్ చేయబడిందో అర్థం చేసుకోండి.



7. గోప్యత గురించి సమాచారంతో ఉండండి

- సోషల్ నెట్వర్కింగ్ ఫ్లాట్ ఫారమ్లలో మీ ఫ్లాణాన్ని పేర్ చేయడంలో జాగ్రత్తగా ఉండండి.
- సోషల్ నెట్వర్కింగ్ ఫ్లాట్ ఫారమ్ ద్వారా మీ డేటా ఎలా సేకరించబడింది, ఉపయోగించబడుతుంది మరియు పేర్ చేయబడిందో అర్థం చేసుకోండి.

- సోషల్ నెట్వర్కింగ్ ఫ్లాట్ ఫారమ్లలో మీ ఫ్లాణాన్ని పేర్ చేయడంలో జాగ్రత్తగా ఉండండి.



- ఫ్లాణ సేవలను నిలిపివేయండి లేదా విశ్వసనీయ కనెక్షన్లకు మాత్రమే యాక్సెస్ ని పరిమితం చేయండి.



నకిలీ అప్పికేషన్సును ఎలా గుర్తించాలి



డెవలపర్ని సరి చూసుకోండి

- డెవలపర్ రెప్యూటేషన్ పరిశోధించండి.
- పారి వెబ్‌సైట్, రిప్యూట్ మరియు రెటీంగ్లను తనిటి చేయండి.



యాప్ అనుమతులను తనిటి చేయండి

- అధిక లేదా అనవసరమైన అనుమతుల పట్ల జార్చుతూ ఉండండి.
- సంబంధిత అనుమతులను మాత్రమే మంజూరు చేయండి.



REVIEW US!

- బద్రతా సమస్యలు లేదా అనుమతాన్ని ప్రవర్తన కోసం చూడండి.
- పనిశీలు సమిత్కులైపై శ్రద్ధ వేసించండి.



యాప్ వివరణ మరియు స్ట్రోట్లను విశ్లేషించండి

- వివరణలు మరియు స్ట్రోట్లల కోసం తనిటి చేయండి.
- వ్యాకరణ లోపాలు లేదా తక్కువ రిజల్యూషన్ చిత్రాల పట్ల జార్చుత వేంచండి.



యాప్ స్టోర్ ప్రామాణికతను తనిటి చేయండి



- Google Play లేదా Apple App Store వంటి అధికారిక యాప్ స్టోర్లను ఉపయోగించండి.
- థర్డ్ పార్ట్ యాప్ స్టోర్ల పట్ల జార్చుతూ ఉండండి.



అధికారిక వెబ్‌సైట్లను క్రాన్-చెక్ చేయండి



- యాప్ అధికారిక వెబ్‌సైట్ ను సందర్శించండి.
- ప్రింట్ మరియు ప్రైఫెచ్చన్ల డిజైన్ ను నిర్మాణించుకోండి.

అసాధారణ డౌన్‌లోడ్సును నివారించండి



- విశ్లేషించ మూలాధారాలకు కళ్చుబడి ఉండండి మరియు యాచ్చచ్చిక లింక్లను నివారించండి.
- అసఫికారిక స్టోర్మార్మల నుండి ఇన్స్టాల్ చేయడం ప్రమాదకరం.



SSL సర్టిఫికెట్ల కోసం చూడండి



- సురక్షిత కనెక్షన్ (https://) మరియు ప్యాడ్మిల్ చివ్వు కోసం తనిటి చేయండి.
- వ్యక్తిగత సమాచారాన్ని నమోదు చేయడానికి ముందు డేటా రిఫ్జణ్ ను నిర్మాణించుకోండి.



గుర్తుంచుకోండి: నివారణ కీలకం!
అప్పుమత్తంగా ఉండండి మరియు మీ
ఆన్‌లైన్ భద్రతకు ప్రాధాన్యత ఇవ్వండి.



డెస్క్‌టాప్ సెక్యూరిటీ



సాఫ్ట్‌వేర్ అప్డేట్ చేసుకోండి



బలమైన మరియు ప్రత్యేకమైన పాస్‌వర్డ్లు

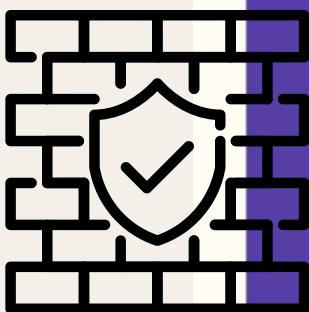
- మీ ఆపరేటింగ్ సిస్టమ్, యాంటివైరస్ సాఫ్ట్‌వేర్ మరియు అప్పిటెషనలను క్రమం త్వరించడా అప్పేది చెయ్యండి.
- అప్డేట్లలో తరచుగా సెక్యూరిటీ ప్యాచ్‌లు ఉంటాయి.

టు పాక్టర్ అఱేంటీకేషన్ (2FA)



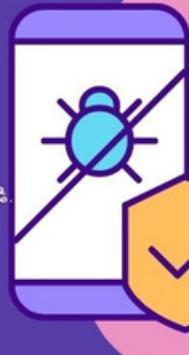
- అదనపు భద్రత కోసం 2FAని ప్రారంభించండి.
- మీ మొబైల్ పరికరానికి పంపబడిన కోడ్ వంటి రెండవ ధృవీకరణ దశ అవసరం.

ఫైర్‌వాల్ రక్షణ



- విశ్వసనియ ఫైర్‌వాల్ ను ఆప్టిమిజ్ చేయండి మరియు నిర్వహించండి.
- నెట్‌వర్క్ ట్రాఫిక్ ను పర్యవేక్షించుట మరియు నియమించుట.
- అసిక్రిట యూక్స్‌ను మరియు హాక్‌రెస్ట్‌ను కార్బోన్‌లాపాలను జ్ఞాక్ చేస్తుంది.

సురక్షిత Wi-Fi కనెక్షన్



- ఎన్పిఫ్స్ ఇన్స్ సురక్షిత Wi-Fi నెట్‌వర్క్‌ని ఉపయోగించండి.
- డిప్ప్‌రూటర్ పాస్‌వర్డ్లు మార్చండి.
- WPA2 లేదా WPA3 ఎన్కెఫ్ట్‌ప్రోటోకాల్‌లను ఉపయోగించండి.

రెగ్యులర్ డేటా బ్యాక్‌ప్యాప్

- ముఖ్యమైన పైల్లు మరియు ప్లాలను తరచుగా బ్యాక్‌ప్ప చేయండి.
- హార్డ్ డ్రైవ్లు, క్లౌడ్ లేదా బ్యాక్‌ప్ సాఫ్ట్‌వేర్ ను ఉపయోగించండి.

యాంట్ మాల్వేర్ సాఫ్ట్‌వేర్



- ప్రసిద్ధ యాంట్-మాల్వేర్ సాఫ్ట్‌వేర్ ను ఇంప్లెంట్ చేయండి.
- దీన్ని అప్డేట్ కావండి.
- మాల్వేర్ ను గుర్తించి, తిసివేయడానికి సాధారణ స్క్రూలను అమలు చేయండి.

సురక్షిత బ్రోజంగ్ పద్ధతులు



- లింక్‌లపై క్లిక్ చేసేటప్పుడు లేదా పైల్లును డౌన్‌లోడ్ చేసేటప్పుడు జార్జుత్తగా ఉండండి.
- పిషింగ్ ఇమెయిల్లు, అనుమానస్వర వెబ్‌సైట్లు మరియు పాష్-అప్ ప్రకలనల కోసం చూడండి.

యూసర్ అకౌంట్ నిర్వహణ



- ప్రతి వ్యక్తికి ప్రత్యేక వినియోగదారు భాతాలను స్థాపించండి.
- నష్టాలను తగ్గించడానికి అడ్జెన్ అధికారాలను పరిమితం చేయండి.

రెగ్యులర్ సిస్టమ్ నిర్వహణ

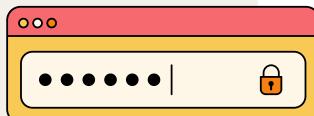


- సాధారణ సిస్టమ్ నిర్వహణ పనులను నిర్వహించండి.
 - డిస్క్ క్లీనిప్ (Disk cleanUp) మరియు డిష్ట్రోగ్రౌంట్ (defragmentation).
- పనితీరును అనుమతించడానికి అధికారాలను పైల్లును తిసివేయండి.



ధరింపదగిన గాడ్జెట్లపై భద్రతా అవగాహన

ధరింపదగిన గాడ్జెట్ అనేది ఎలక్ట్రోనిక్ సాంకేతికత పరికరాల కోపు చెందినది, విటిని ఉపకరణాలుగా ధరింపవచ్చు, యస్టులలో పొందుపరచవచ్చు, వినియోగదారు శరీరంలో అమర్ఖవచ్చు లేదా చర్చంపై పచ్చబోట్లు కూడా వేయవచ్చు.



వినియోగదారుల కోసం ధరింపదగిన గాడ్జెట్ల వల్ల కలిగే భద్రతా సమస్యలు

డేటాకు భౌతికంగా ప్రవేశించడం చాల సులభం

PIN లేదా పాస్‌వర్డ్ రక్షణ ఉండదు, బయోమెట్రిక్ భద్రత ఉండదు మరియు డేటాను యాక్స్‌సెచ్యూరిటీ చేయడానికి వినియోగదారుడు అవసరం లేదు. ఇది తప్పుడు చేతుల్లోకి పడితే, డేటాను దాలా సులభంగా యాక్స్‌సెచ్యూరిటీ చేసే ప్రమాదం ఉంది.

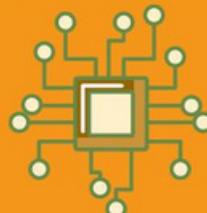


ఫోటోలు, విడియోలు మరియు ఆడియోను రికార్డ్ చేయగల సామర్థ్యం స్వార్థాపన లేదా స్వార్థాపన వంటి ఉపయోగించి ఎవరైనా ఫోటోగ్రాఫీలు తీయడం లేదా విడియో లేదా ఆడియో ఫైల్లను రికార్డ్ చేయడం సులభం. ముఖ్యమైన సమాచారం మరియు విడియోలు మరియు సున్నితమైన డేటా యొక్క చిత్రాలను రహస్యంగా తీసే అవకాశం ఉంది.



అసురక్షిత వైరల్స్ కనెక్టివిటీ

ధరింపదగిన సాంకేతిక పరికరాలు ఉ.డ. భూటూత్, NFC మరియు Wi-Fi వంటి ప్రోటోకాల్లను ఉపయోగించి వైరల్స్ స్వార్థాపనలు లేదా టాష్టోవ్లలు కనెక్ట్ అపుతూయి అనేది వాస్తవం. ఈ వైరల్స్ కనుమ్మానికేషన్లలో దాలా పరకు బ్రూట్-ఫోర్స్(Brute force) దాడికి వ్యతిరేకంగా రక్షించడానికి తగినంత రక్షణలో లేవు.



ఎన్క్రిప్షన్ (Encryption) లేకపోవడం



కొన్ని భద్ర్-పార్టీ యాప్లు ప్రాథమిక భద్రతా ప్రమాణాలను నిర్దిష్టం చేస్తాయి మరియు ఎన్క్రిప్షన్ లేని సమాచారాన్ని పంపుతాయి లేదా పొందుపరుస్తాయి. ధరింపగలిగి వాటి ద్వారా ఆటోమేటిక్ గా సేకరించబడే డేటా, అవి కోరుకునే వ్యక్తులకు దాలా విలువైనది.

సెక్యూరిటీ వల్సేరబిలిటీస్ మరియు అటాక్స్



స్మాపింగ్ మరియు స్పృహక

QR ఫోటోబాంబింగ్ మాల్వేర్

Wi-Fi-ప్రోజాక్టింగ్

ఫిఫింగ్

బ్రూట్ ఫోర్స్ దాడి



వినియోగదారు ఐడెంపటీ మరియు డేటా ప్రైవెసీ

తరచుగా వారి అనుమతి లేకుండా కెమెరాలు మరియు మైక్రోఫోన్ల వంటి ఎంబెడెడ్ సెన్సర్లు, వ్యక్తికి సంబంధించిన డేటాను క్యాప్చర్ చేస్తాయి మరియు పరిసరాలను కూడా. ఈ డేటా వ్యక్తిగతమైనది, గోప్యమైనది మరియు సున్నితమైనది, ఇది వినియోగదారుల పైప్సీపై దాడి చేస్తుంది.

ట్రైం అండ్ లోకేషన్-బెస్ట్ పైప్సీ

ఒక నిర్దిష్ట సమయంలో ఒక వ్యక్తి స్థానాన్ని ట్రౌన్ చేయగల GPS ధరింపగలిగి గాడ్జెట్ లోపల పొందుపరచబడింది. నావిగేషన్ చేయడం వల్ల ప్రజలకు ఎక్కువ ప్రయోజనాలు లభిస్తాయి, అయితే ఇది ఎక్కువ సష్టాలను కూడా కలిగిస్తుంది. ఇంకి వ్యక్తుల స్థానాన్ని ట్రౌన్ చేయగలిగితే వినియోగదారు పైప్సీపై సమస్యలు పెరుగుతాయి.



ఎలక్టోనిక్ గాడ్జెట్లపై పని చేస్తున్నప్పుడు కంటి ఒత్తిడిని ఎలా నివారించాలి

కారణాలు, లక్షణాలు మరియు
పరిష్కారాలు



మీ స్మిగ్స్ కి ద్వారా ఉండచానికి మీ వెనుకభాగం గుండ్రంగా, గెర్మం ముందుకు వంచి, తల వెనుకకు వంచి కూర్చుకుండి. మీరు మంచి భంగమతో మీ స్మిగ్స్ న్యూమా దూరాలకొరిక, కంటి వైద్యుతిని సందర్శించండి.

కారణాలు

మితిమీరిన వెలుతురు వల్ల కంటి జబ్బుది కలుగుతాయి. ఓవర్ హెచ్ లెటీగ్ మీ స్మిగ్స్ కంటి ప్రాపంతంగా ఉండకూడదు.

మీ వీపులు సహా ఉండాలి కాబట్టి మీరు నిటారుగా మరియు మీ స్మిగ్స్ నుండి సాక్ష్యవంతున్న వీపులు దూరంలో కూర్చుపుచుండి.



పాత ర్స్ట్స్ లీఫ్స్ ల ఉన్న అప్పాలు దరించిపుట్టి, గెర్మి సాకర్మం కేసిం, యాంటీ రిస్ట్స్ కంప్యూటింగ్ కళ్లుల కేసిం మీ కంటి వైద్యుతిని సంపూర్ణంగా ఉండకూడదు.



లక్షణాలు



పొడి కళ్లు
కళ్లు చిరాకుగా ఉండటం
మనక దృష్టి
అలసిపోయిన కళ్లు
మెడ & వెన్నునొప్పి
తలనొప్పులు



మీరు చెయ్యాల్సినివి

- UV కాంతి వల్ల కలిగే కంటి ఒత్తిడిని నిరోధించడానికి రూపొందించబడిన రక్షణ కళ్లద్దాలు మరియు అధ్యాలు ధరించండి.
- 20-20-20 నియమాన్ని గుర్తుంచుకోండి: ప్రతి 20 నిమిషాలకు, విరామం తీసుకోండి మరియు 20 సెకన్డు పాటు 20 అడుగుల దూరంలో ఉన్నదాన్ని చూడండి.
- కంటి ఒత్తిడిని మరింత తీవ్రతరం చేసి స్మిగ్స్ గీర్ను తొలగించడానికి ఓవర్ హెచ్ లైటింగ్ తగ్గించండి.
- మీరు కూర్చున్న వోటు నుండి మీ స్మిగ్స్ "ప్రా-ప్లేవ్" దూరంలో ఉండని నిర్ధారించుకోండి.
- కంటి వ్యాయామం



మానసిక ఆరోగ్యం



ముందస్తు హాచ్చరికలు

వీకార్గత లేకపోవడం

దృష్టి పెట్టడంలో సమస్య, ప్రేలవమైన పనితీరు మరియు అధిక చురుకు తసను.



మానసిక స్థితి మార్పులు

విచారం లేదా ఉపసంహరణ భావాలు, కొనసాగుతను కోపం లేదా చిరాకు, తీవ్రమైన మానసిక కల్లోలం, బంటరితనం, గతంలో ఆనందించిన కార్బోకలాపాలను నివారించడం.



బత్తిడి మరియు అందోళన

గాడ్జెట్ల వ్యసనాన్ని సూచించే హాచ్చరిక సంకేతాలు

- ఎవరితోపోనా మాట్లాడుతున్నప్పుడు కూడా మీరు మీ ఫోన్‌ను అఫ్‌లో ఉంచలేరు.
- మీరు ఏకార్గతతో ఇఖ్యంది పడుతారు మరియు ఇతర పనులను పూర్తి చేయలేరు. మీరు మీ ఫోన్‌ని వెక్ష చేయాలనుకుంటున్నందున మీరు ఎప్పటికే పరధ్యానంలో ఉంటారు.
- మీరు నిద్ర సమస్యలను అనుభవించడం పూరంభిస్తారు.
- మీరు మీ ఫోన్‌లో ఉండాలి లేదా మీరు ఆత్మతగా మరియు చిరాకుగా అనిపించడం పూరంభం అవుతుంది.
- మీ ఫోన్‌లో లేనప్పుడు మీరు ఎదో కోల్పోయారని అనుకుంటారు.

తీవ్రమైన బరువు మార్పులు

మానసిక అనారోగ్యం యొక్క చిహ్నాలు: అతిగా తినడం, ఆకలి లేకపోవడాన్ని ప్రదర్శించడం, వాంతులు లేదా జీడ్ర్ కోసానికి సంబంధించిన వ్యాధులు.



శారీరక లక్షణాలు

కొండరు వ్యక్తులు అనుభవించే మానసిక అనారోగ్యం యొక్క శారీరక లక్షణాలు: దీర్ఘకాలిక తలనొప్పి, కడుపునొప్పి, ఇతర రకాల నొప్పులు మరియు నిద్ర లేమి.



డిప్రెషన్ మరియు ఒంటరితనం



మీ మానసిక ఆరోగ్యానికి బాధ్యత వహించడం

మర్మిపోకూడనివి



- కుటుంబం మరియు స్నేహితులతో కలవండి.
- మీరు ఇష్టపడేదాన్ని చేయడం కొనసాగించండి: చదువడం, కీడులు, రాయిడం, ప్రకృతి సడకలు మరియు కళలను స్ఫూర్చించడం.
- షెడ్యూల్స్ నీ స్ఫూర్చించండి & మీ దినచర్యకు కట్టుబడి ఉండండి.



బత్తిడి మరియు అందోళనతో ఎలా వ్యవహరించాలి



శరీరం

- బాగా సమతుల్య భోజనం తినండి.
- తగినంత నిద్ర పొందండి.
- రోజుా వ్యాయామం చేయండి.



మనసు

- మీరు ప్రతిది నియంత్రించలేరని అంగీకరించండి.
- మీ వంతు కృషి చేయండి.
- సానుకూల వైభాగికిని కొనసాగించండి.



చర్యలు



- శ్యాసన తీసుకోండి - నెమ్ముదిగా **10** లేక్కించండి.
- యోగా కోసం సమయం కేటాయించండి, సంగీతం వినండి మరియు ధ్యానం చేయండి.
- స్నేహితులు** & కుటుంబ సభ్యులతో మాట్లాడండి మరియు మీరు ఎలా భావిస్తున్నారో వారికి చెప్పండి.

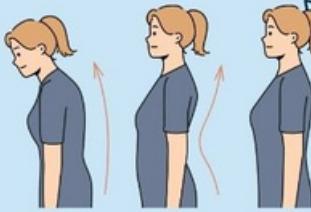
అధిక గాడ్జెట్ వాడకం వల్ల శారీరక ఆరోగ్యంపై ప్రభావం

లక్షణాలు



1. భంగిమ సమస్యలు:

- గుండ్రని భుజాలు
- వేళలో నొప్పి
- వెన్నెముకలో నొప్పి



3. నిద్ర ఆటంకాలు:

- నిద్రపోవడంలో కష్టం
- నిద్రలో నాణ్యత లేకపోవడం
- నిద్రలేచి

2. నిశ్చల జీవనసైలి:

- శారీరక శ్రుతి లేకపోవడం
- బయలు పెరుగుట
- హృదయ ఆనారోగ్యం



ఉపయోగకరమైన చిట్టాలు:

1. మంచి భంగిమను సాధన చేయండి:

- మీ వెనుకకు మద్దతుగా నిటారుగా కూర్చోండి
- మీ పాదాలను నెల్పు చదునుగా ఉంచండి
- మీ స్థిరాన్ని కంటి స్థాయికి సర్దుబాటు చేయండి



2. విరామం తీసుకోడి మరియు కదలండి

- ప్రతి గంటకు నిలబడి మరియు విరామం తీసుకోడానికి రిటైండ్ లను సట్ చేయండి
- నడక లేదా వ్యాయామం వంటి శారీరక కార్బూకలాపాలలో పాల్గొనండి

3. పరికర రహిత దినచర్యను స్థాపించండి:

- నిద్రవేళకు కనీసం ఒక గంట ముందు గాడ్జెట్ వాడకాన్ని నివారించండి
- ధ్యానం వంటి విక్రాంతి కార్బూకలాపాలలో పాల్గొనండి



4. స్థిర్ము సమయ పరిమితం చేయండి:

- స్థిర్ము సమయాన్ని ట్ర్యూచెయడానికి మరియు పరిమితం చేయడానికి యాప్లెల్ లేదా అంటర్స్ట్రీట ఫీచర్లను ఉపయోగించండి
- అఫ్లైన్ కార్బూకలాపాలు మరియు సామాజిక పరస్పర చర్యల కోసం సమయాన్ని కేటాయించండి



ముగింపు:

మితిమీరిన గాడ్జెట్ వినియోగం మన శారీరక ఆరోగ్యంపై పోకిరమైన ప్రభావాలను కలిగిస్తుంది. లక్షణాల గురించి తెలుసుకోవడం మరియు ఈ చిట్టాలను అమలు చేయడం ద్వారా, ప్రభావాన్ని తగ్గించవచ్చు మరియు ఆరోగ్యకరమైన జీవనసైలిని ప్రోత్సహించవచ్చు. గాడ్జెట్ వినియోగం మరియు శారీరకంగా చురుకైన దినచర్యను నిర్వహించడం మధ్య సమతల్యతను సాధించాలని గుర్తుంచుకోండి, ఇది పూర్తి శైయస్సును మెరుగుపరచడానికి అనుమతిస్తుంది.





మీ పనిని సేవ చేయుండి

- షట్ డోన్ చేయడానికి ముందు, అన్ని బిపెన్ డాక్యుమెంటులను సేవ చేయండి మరియు నడుష్టులైను మూసివేయండి.
- డేటా నష్టాన్ని నిరోధిస్తుంది మరియు మీరు తర్వాత పనిని పునర్పూరంఖించవచ్చని నిర్ణారిస్తుంది.



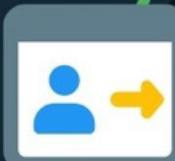
అప్లికేషన్లను మూసివేయండి

- అన్ని టిప్పణీ అప్లికేషన్లు మరియు బ్రౌజర్ టూల్స్ లను మూసివేయండి.
- బున్నామెన్ రమా ఫోలో చేస్తుంది మరియు పనితీరును మెరుగుపరుస్తుంది.



భాతాల నుండి లాగ్ అవుట్ చేయండి

- అన్ని వినియోగదారు భాతాలు మరియు అప్లికేషన్ నుండి లాగ్ అవుట్ చేయండి.
- అన్ని టిప్పణీ రమా ఫోలో నుండి సున్నితమైన సమాచారాన్ని రాశ్చుంది.



బాహ్య పరికరాలను తొలగించండి

- కనెక్ట్ చేయబడిన బాహ్య పరికరాలను (కడా., ప్రెస్టి, డెంప్స్, బాహ్య ప్రెస్టి డెంప్స్) సురక్షితంగా తొలగించండి.
- ఇది దేహకు మరియు పరికరాలకు నష్టం జరగకుండా నిరోధిస్తుంది.

కంప్యూటర్లను ఆపెయ్యండి

ఆపేట్ లను అమలు చేయండి

- సిస్టమ్ అప్టెట్ కోసం తనిటి చేయండి మరియు అందుబాటులో ఉంటే వాటిని ఇన్సెల్ చేయండి.
- అప్టెట్ తరచూ ముఖ్యమైన భద్రతా పాచెన మరియు బగ్ పరిష్కారాలను కలిగి ఉంచాయి.



సరిగ్గా షట్ డాన్ చేయండి

- స్టార్ మెను లేదా ఆపెల్ మెనుపై క్లిక్ చేసి, "షట్ డాన్" లేదా "పవర్ ఆఫ్" ఎంచుకోండి.
- పవర్ ఆఫ్ చేయడానికి ముందు కంప్యూటర్ షట్ డాన్ ప్రక్రియను పూర్తి చేసిదాకా వేచి ఉండండి.



పెరిఫెరల్ పవర్ ఆఫ్ చేయండి

- కనెక్ట్ చేయబడిన పెరిఫెరల్ (కడా., మౌసిటర్, ప్రింటర్, సైకట్) ఆఫ్ చేయండి.
- విద్యుత్ శక్తిని ఆదా చేసుంది మరియు పరికర జీవితకాలాన్ని పొడిగిస్తుంది.



ఉపయోగంలో లేనప్పుడు అన్పస్గ్ చేయండి

- ఎక్స్ట్ కాలం ఉపయోగంలో లేకుంటే పవర్ సోట్ నుండి కంప్యూటర్ను అన్పస్గ్ చేయడాన్ని పరిగణించండి.
- విద్యుత్ శక్తి వినియోగాన్ని తగ్గిస్తుంది.





సైబర్ చట్టాలు -భారతదేశం



ఇన్విట్షన్ డిక్షూలజె చట్టం, 2000

1

- ఎలక్ట్రానిక్ రికార్డులు మరియు డిజిటల్ సంతకాలకు చట్టపరమైన గుర్తింపు.
- సైబర్ సోషల్ మరియు వాటి జరిమాలను నిర్వచిస్తుంది.

సైబర్ సోషల్

2

- హైకింగ్, గుర్తింపు దీంగతనం, ఆన్‌లైన్ మోసం మరియు డేటా ఉళ్లంఘనలు.
- సైబర్ నోర్మేల్ జరిమాలు.
- అందికార యాక్సెస్, కంప్యూటర్ సంబంధిత సోషల్, సైబర్ బీర్పరిజం.



డేటా రక్షణ మరియు గోప్యత

3

- సమాదార సాంకేతికత (సమాతుక్కున వద్దల పద్ధతులు మరియు విధానాలు మరియు సుఖ్యతక్కున వ్యక్తిగత డేటా లేకా సమాధారం) నియమాలు, 2011.
- వ్యక్తిగత డేటా రక్షణ.
- సుఖ్యతక్కున వ్యక్తిగత సమాధారాన్ని నిర్వసించే ఎంటిటీల కేసం వద్దల పద్ధతులు.
- డేటా ఉళ్లంఘనలు మరియు డేటా సక్రియిస్టిక్స్ సమూలి కేసం విధానాలు.

సైబర్ ఫోరెన్సిక్

4



సైబర్ అప్పులేట్ ట్రైబ్యునల్ (CAT)

5

- ఇన్విట్షన్ డిక్షూలజె చట్టం, 2000 ప్రకారం స్థాపించబడింది.
- న్యూయిర్ న్యూఐల అధికారుల నిర్ద్ధయాలకు వ్యక్తికంగా అవీలు (Appeal).
- సైబర్ చట్టాన్ని సమర్పించండి అమలు చేయడాన్ని నిర్మారిస్తుంది.

సైబర్ సోషల్ నివేదించడం

6



- సైబర్ సోషల్ నివేదించడాన్ని ప్రొత్తుపెస్తుంది.
- సురక్షితమైన ఆన్‌లైన్ వాతావరణాన్ని ప్రొత్తుపెస్తుంది.
- సమర్పించండి చట్ట అమలును సులభతరం చేస్తుంది.

సైబర్ లౌబ్ పోర్టల్ మరియు డోల్ర ట్రై సంబర్

7

- Portal: <https://cybercrime.gov.in/>
- సైబర్ క్రైమ్ పోల్ట్ లైన్ 1930



అత్యవసర పరిస్థితుల్లో, దయచేసి మమ్మల్ని సంప్రదించడి:



Women Safety Wing

www.womensafetywing.telangana.gov.in/



She Team Whatsapp

9441669988



Reception Number

9440700906

Child Helpline Number
1098

Cyber Crime Number
1930

Cyber crime website
Cybercrime.gov.in

