इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

www.isea.gov.in

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

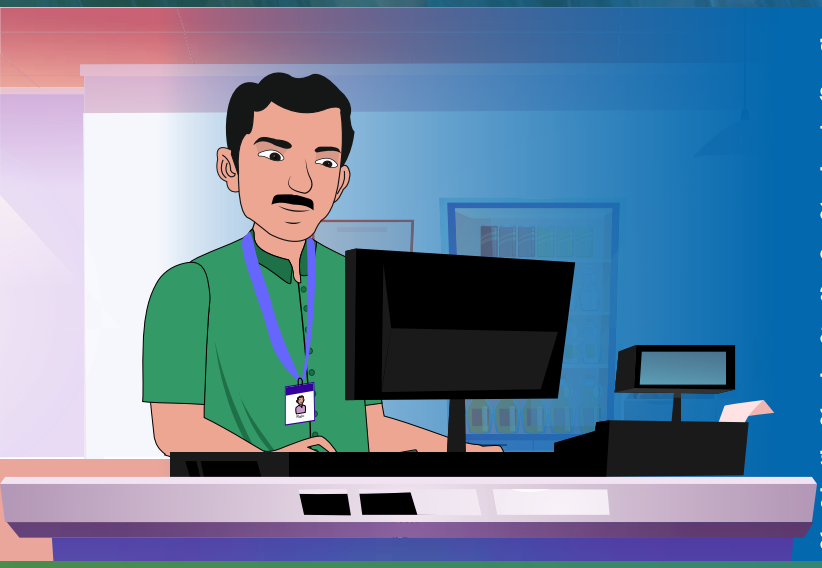
एन आई सी National Informatics Centre

सी डैक CDAC

సైబర్ అవేర్‌నెస్ కథ:

ఒక సాధారణ మనిషి సైబర్ యాత్ర - సేఫర్ ఇంటర్నెట్ డే

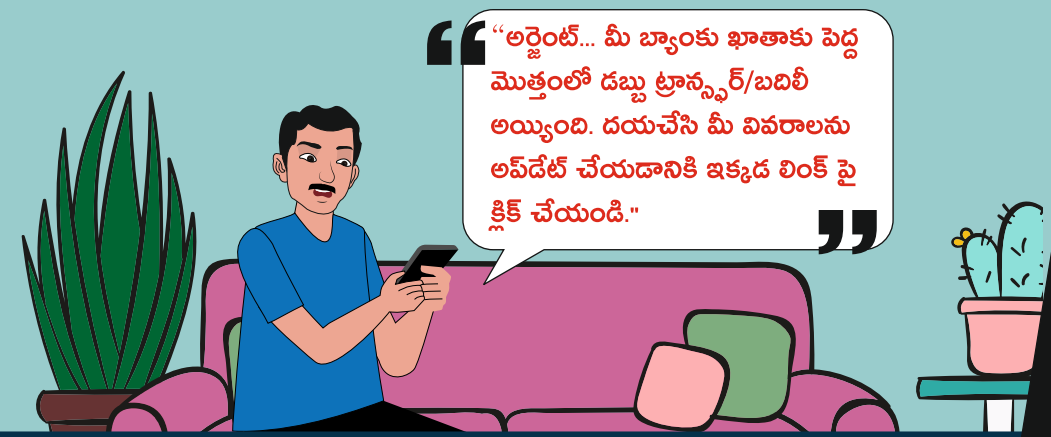
డిజిటల్ యుగంలో ఒక్క క్లిక్ ఏవిధమైన అవకాశాలకూ, ప్రమాదాలకూ తలుపులు తెరుస్తుందో చూడండి. రాజు సాధారణ వినియోగదారుడి స్థాయి నుండి సైబర్ రక్షకుడిగా మారడాన్ని గమనించండి. ఈ సేఫర్ ఇంటర్నెట్ డే... సురక్షిత అంతర్జాల దినాన్ని ఆరంభించండి.మీరు మీ ఆన్‌లైన్ ప్రపంచాన్ని ఎలా సురక్షితంగా ఉంచుకోవచ్చో ఈ కథ తెలియజేస్తుంది.



రాజు ఒక సాధారణ మనిషి, ఢిల్లీ లోని ఒక చిన్న పారుగు ప్రాంతంలో తన కుటుంబంతో నివసిస్తుండేవాడు. అతడు ఒక చిన్న అంగడిలో/దుకాణంలో పనిచేస్తుంటాడు. అతడి జీవితం చాలా సింపుల్ గా ఉండేది. ప్రతిరోజూ, అతను త్వరగా లేచి, పని మీద వెళ్ళి, దుకాణంలో పని చేసేవాడు. ఆ తర్వాత ఇంటికి తిరిగి వచ్చి కుటుంబంతో సమయం గడిపేవాడు. అతడు పెద్దగా ఇంటర్నెట్ వాడేవాడుకాదు. నీ కొన్నిసార్లు ఫోన్ లో సోషల్ మీడియా చూసేవాడు. ఆన్‌లైన్ బ్యాంకింగ్ లావాదేవీలు చేసేవాడు. అతడికి అవసరమైనంత ఇంటర్నెట్ వాడడం మాత్రమే తెలుసు కానీ అతను టెక్నాలజీలో పెద్దగా నిపుణుడేం కాదు. రాజు ఇంటర్నెట్ వినియోగం ప్రమాదకరం కూడా అని పెద్దగా ఆలోచించలేదు - ఓ రోజు, అతడి జీవితంలో అన్ని మారిపోయాయి.

రాజు సైబర్ యాత్ర – ఒక మిత్రుని తక్షణ హెచ్చరిక

ఒక రోజు, రాజు ఇంటి వద్ద కూర్చొని ఉన్నాడు. అతడికి గుర్తు తెలియని ఒక నెంబర్ నుండి వాట్సాప్ సందేశం/మెసేజ్ వచ్చింది. సందేశంలో ఒక లింక్ కూడా ఉంది...అది ఇలా ఉంది :



ఈ సందేశం అతని బ్యాంకు నుంచి వచ్చినట్టు అనిపించింది. ఈ సందేశంలోని అత్యవసరత రాజును ఆలోచనలో పడేసింది. ఇది అనుమానాస్పదంగా ఉన్నప్పటికీ, రాజు ఇటీవల కొంత పెద్ద లావాదేవీలు చేయడంతో, ఇది నిజమైన సందేశమే ఉండవచ్చు అనిపించింది.

రాజు మొదట అనుమానపడినా, చూద్దాం ఇంక అనిపించడంతో లింక్‌పై క్లిక్ చేయాలనుకునే సమయంలో అతడికి సమీపంలో ఉండే మిత్రుడు సురేష్ నుండి ఒక కాల్ వచ్చింది.

రాజు లింక్ గురించి సురేష్ కు వివరించాడు.

ఓ... రాజు! ఈ రోజు ఖాతా అప్‌డేట్ గురించి ఇదే తరహా మెసేజ్ చూసాను. ఆ లింక్‌పై క్లిక్ చేయవద్దు ! అది ఒక స్కామ్, సైబర్ మోసం. నాకూ ఇదే సందేశం వచ్చింది ,అది సైబర్ మోసాన్ని ఫిషింగ్ అంటారు.

ఇది విన్న రాజు గందరగోళంలో...

ఫిషింగ్? అది ఏంటి ?

ఫిషింగ్ అంటే సైబర్ మోసగాళ్లు నమ్మకమైన వ్యక్తులు గా నమ్మబలుకుతూ, నటిస్తూ, మీ వ్యక్తిగత సమాచారాన్ని, బ్యాంకు ఖాతా వివరాలు లేదా పాస్‌వర్డ్స్ వంటి వాటిని పంపించండి అని అభ్యర్థిస్తారు. విలువైన సమాచారం సేకరించి మోసగించడమే అది. వాళ్ళు ఫేక్ లింక్స్ లేదా మెసేజెస్ పంపుతూ నిజమైన అధికారుల్లా కనిపిస్తారు. మీరు వాటిపై క్లిక్ చేస్తే, వాళ్లు మీ విలువైన సమాచారాన్ని దొంగిలించి, మీ బ్యాంకు ఖాతాను ఖాళీ చేయగలరు.

Dear Customer your Credit Card PIN has been redet to 9999. Click here to activate

దీంతో రాజు కొంత ఊరట పొందాడు, అపరాధ భావన కూడా కలిగింది .

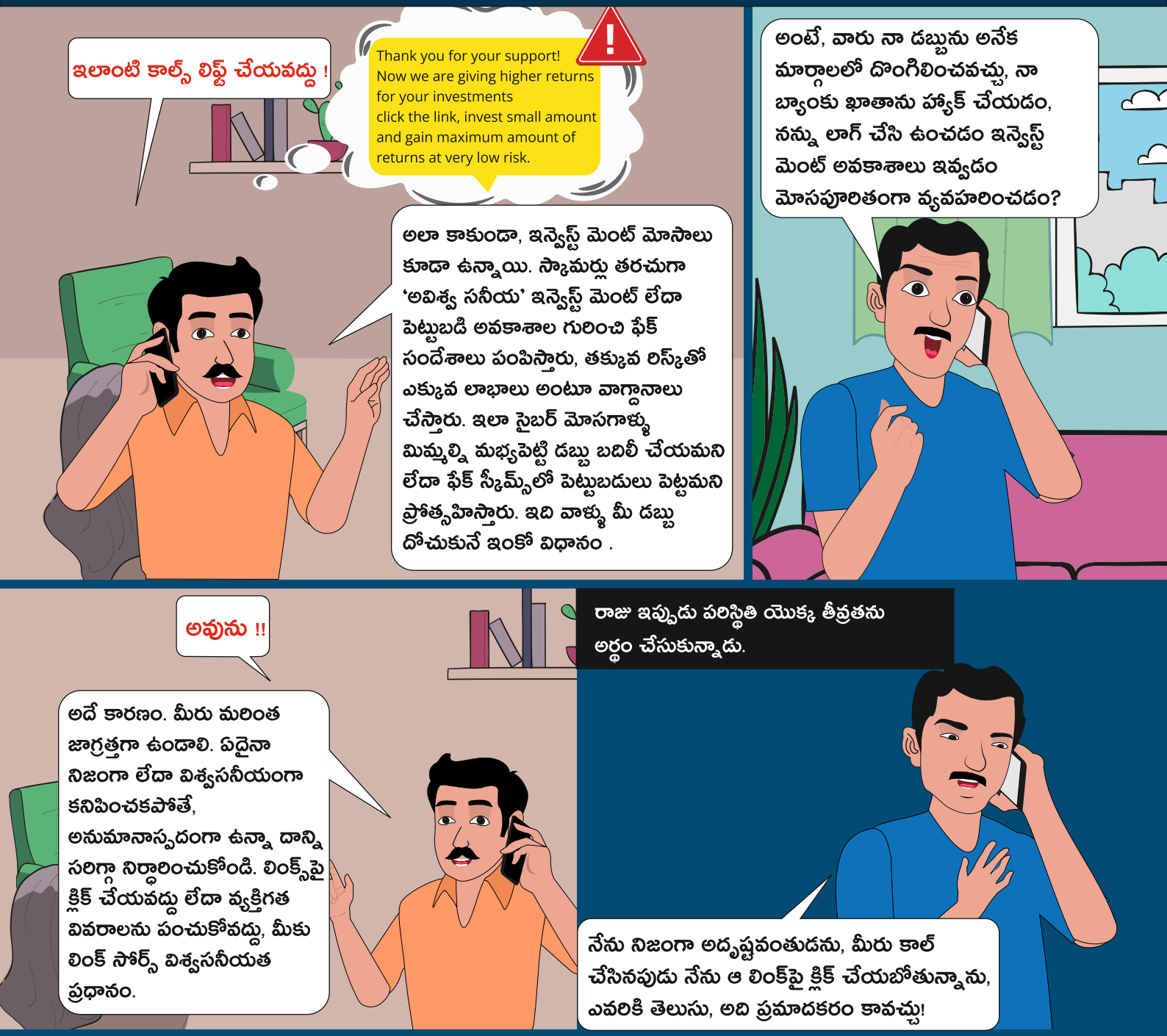
నన్ను రక్షించినందుకు ధన్యవాదాలు, సురేష్. నాకు ఫిషింగ్ గురించి ఏమీ తెలీదు.

సురేష్ కొనసాగించాడు

Unknown...

డిజిటల్ అరెస్టు? నాకు తెలియదు. నాకు తెలియని నెంబర్ల నుంచి కాల్స్ వస్తున్నాయి, నేను వాటిని లిఫ్ట్ చేద్దామని అనుకున్నా

కానీ అదే కాదు. 'డిజిటల్ అరెస్టు' అనే సైబర్ మోసం కూడా ఉంది. ఇది స్కామర్లు, కాల్ ద్వారా పోలీసు అధికారుల్లా లేదా చట్ట అధికారుల్లాగా వ్యవహరిస్తూ, మీ పేరుతో పార్సెల్‌లో డ్రగ్స్ ఉన్నట్లు చెబుతారు, మీరు డిజిటల్ అరెస్టులో ఉన్నారని చెప్పి భయ పెడ తారు. ఆ స్కామర్లు పెద్ద మొత్తంలో డబ్బు చెల్లించమని అడుగుతారు.



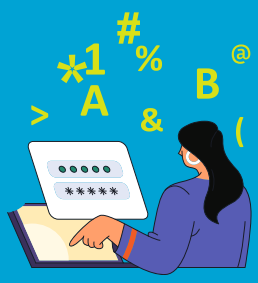
రాజు తన మిత్రుడి సమయోచిత సలహా వల్ల కృతజ్ఞతలు తెలపడంతో పాటు, డిజిటల్ ప్రపంచంలో పెరుగుతున్న సైబర్ మోసాలు, ప్రమాదాలపై మరింత అవగాహన పొందాలని ఆయన నిర్ణయించుకున్నాడు ఆయన ఇకపై ఈ -మెయిల్స్, సందేశాలు లేదా అనుమానాస్పదమైన లేదా అసంభవమైన ఆఫర్లతో వ్యవహరించే సమయంలో మరింత జాగ్రత్తగా ఉండాలని నిర్ణయం తీసుకున్నాడు.

సేఫర్ ఇంటర్నెట్ డే గురించి

సురేష్ రాజుకు "సేఫర్ ఇంటర్నెట్ డే" గురించి కూడా సమాచారాన్ని అందించాడు, ఇది త్వరలోనే రాబోతోంది. "సేఫర్ ఇంటర్నెట్ డే ఒక వార్షిక కార్యక్రమం, ఇది ఆన్‌లైన్ భద్రత, డిజిటల్ సంరక్షణ ప్రాధాన్యతను ప్రచారం చేయడానికి ప్రపంచవ్యాప్తంగా నిర్వహిస్తున్నారు.

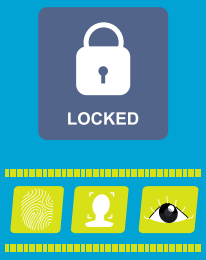
సైబర్ హైజీన్ అనేది వ్యక్తులు తమ ఫోన్, కంప్యూటర్ తదితర పరికరాలలో వ్యక్తిగత సమాచారాన్ని భద్రంగా ఉంచడానికి పాటించాల్సిన కొన్నివిధానాలు. మీరు క్రిములను తొలగించడానికి చేతులు కడిగేలా, సైబర్ హైజీన్ అనేది మీ ఆన్‌లైన్ అలవాట్లను శుభ్రం చేసి, మీ డిజిటల్ జీవితాన్ని రక్షించడం కోసమే. మంచి సైబర్ హైజీన్ తో ఫిషింగ్, హ్యాకింగ్ మరియు మాల్వేర్ వంటి వాటిని మీ వ్యక్తిగత ఖాతాలు, పరికరాలపై ప్రభావం చూపకుండా నివారించవచ్చు.

రాజు సైబర్ హైజీన్‌లో ఈ క్రింది విధమైన ప్రాక్టీసులను కలిగి ఉన్నట్లు తెలుసుకున్నాడు:



శక్తివంతమైన, ప్రత్యేకమైన పాస్‌వర్డ్స్ సెట్ చేయడం: “123456” లేదా “password” వంటి సులభంగా అంచనా వేసే పాస్‌వర్డ్స్‌ని ఉపయోగించకండి. పాస్‌వర్డ్స్‌ను సృష్టించేటప్పుడు అక్షరాలు, సంఖ్యలు మరియు చిహ్నాల మిశ్రమాన్ని ఉపయోగించి శక్తివంతమైన పాస్‌వర్డ్స్‌ను సృష్టించండి.

రెండు-పదార్థ గుర్తింపు (2FA) సక్రియం చేయడం: 2FA అనేది అదనపు భద్రతా పొరను అందిస్తుంది, మీరు మీ ఐడెంటిటీని రెండవ అంశంతో ధృవీకరించాల్సి ఉంటుంది, ఉదాహరణకు, మీ ఫోన్‌కు పంపబడిన కోడ్.



శక్తివంతమైన స్క్రీన్ లాక్ మరియు బయోమెట్రిక్ గుర్తింపు సెట్ చేయడం: మీ పరికరాన్ని మరింత భద్రతగా చేయడానికి బయోమెట్రిక్‌లు (ఫింగర్‌ప్రింట్ లేదా ముఖ గుర్తింపు) లేదా శక్తివంతమైన PIN/పాస్‌వర్డ్‌ని ఉపయోగించండి.

అప్లికేషన్లను నమ్మదగిన మూలాల నుండి మాత్రమే డౌన్లోడ్ చేయడం: అధికారిక అప్లికేషన్ స్టోర్లలో మాత్రమే అప్లికేషన్లు డౌన్లోడ్ చేయండి. అనధికారిక మూలాల నుండి అప్లికేషన్లు మాల్వేర్‌ను కలిగి ఉండవచ్చు లేదా మీ డేటాను దొంగిలించడానికి రూపొందించబడవచ్చు.

భద్రతాత్మక కనెక్షన్లు ఉపయోగించడం: పబ్లిక్ Wi-Fi వాడే సమయంలో, ఆన్‌లైన్ బ్యాంకింగ్ వంటి సున్నితమైన ఖాతాలను ప్రవేశించడాన్ని నివారించండి.

అనుమానాస్పద లింక్స్‌ని నివారించడం: మీరు ఎటువంటి లింక్‌లపై క్లిక్ చేసే ముందు,లింక్ యొక్క మూలాన్ని ఎప్పుడూ ధృవీకరించండి .

సాఫ్ట్‌వేర్ మరియు అప్లికేషన్లను రెగ్యులర్‌గా అప్‌డేట్ చేయడం: రెగ్యులర్ అప్‌డేట్స్ భద్రతా సున్నితతలను పరిష్కరిస్తాయి, వాటిని చెడు వ్యక్తులు దుర్వినియోగం చేసేందుకు ప్రయత్నిస్తారు.

Report cyber frauds at 1930 www.cybercrime.gov.in

Supported by

certin Enhancing Cyber Security in India | साइबर स्वच्छता केन्द्र CYBER SWACHHTA KENDRA Botnet Cleaning and Malware Analysis Centre | Digital India Power To Empower | mygov मेरी सरकार | रा.इ.सू.प्रौ.सं NIELIT