

మాజీ సైనికులు మరియు వీర నారిలచే సైబర్ సెక్యూరిటీ మోసాల నిర్వహణ

కమాండర్ పి రాజగోపాల్ తంపి IN (R)

- AI మరియు పెద్ద భాషా నమూనాలు
- సాఫ్ట్‌వేర్ మరియు AI మధ్య తేడా ఏమిటి?
- ఏజెంట్ అంటే ఏమిటి?
- ఏజెంట్ LLM నుండి ఎలా భిన్నంగా ఉంటాడు?
- AI వల్ల కలిగే కొన్ని ముఖ్యమైన ప్రయోజనాలు ఏమిటి?
    - శాస్త్రీయ ఆవిష్కరణలలో వేగవంతమైన పురోగతి
    - కొత్త పదార్థాలు, కొత్త అణువులు, ఉత్పాదకత ప్రయోజనాలు
    - వాతావరణ అంచనాలు
    - సాఫ్ట్‌వేర్ కోడింగ్
    - రోబోట్లు మరియు ఆటోమేషన్
- ఏఐ వల్ల కలిగే ప్రధాన ప్రమాదాలు ఏమిటి?
    - మోసం, అధికారం కోసం ఆరాటం మరియు ఆత్మరక్షణ
    - డీప్‌ఫేక్‌లు
    - నియంత్రణ కోల్పోవడం
    - పునరావృత స్వీయ-అభివృద్ధి (RSI)
    - స్వీయ ప్రతిరూపణ

- హగ్గింగ్‌ఫేస్ సంఘటన, ఆంత్రోపిక్ ఐఓటి అంచనా
- ఫ్రాన్స్‌లో రిఫ్రిజిరేషన్ ప్లాంట్‌లను హ్యాకింగ్ చేయడం – అక్టోబర్ 2026 మధ్యలో
- ప్రభుత్వ వెబ్‌సైట్‌లు పనిచేయడం లేదు (PHP బగ్స్) – 21సెయింట్ అక్టోబర్ 2026
- సహజంగానే ద్వంద్వ ప్రయోజన సాంకేతికత – స్వయంప్రతిపత్తి గల ఆయుధాలు, CBRN మరియు యుద్ధకాల వినియోగంలో గొప్ప ప్రమాదాలు ఉన్నాయి.
- AI అనేది సైబర్ సెక్యూరిటీకి ఒక సాధకం మరియు రక్షకుడు.
- మన మెదడుల కన్నా శక్తివంతమైన కంప్యూటింగ్ ఇంజిన్ (వేగవంతమైనది మరియు అపరిమితమైన వనరులు).వారిని అందుకోలేరు లేదా అర్థం చేసుకోలేరు
- ఏజెంట్లు 24x7 పనిచేస్తాయి మరియు వందల సంఖ్యలో ఎన్‌క్రిప్షన్‌ను బ్రూట్ ఫోర్స్ చేయగలవు, సాఫ్ట్‌వేర్‌లోని బగ్‌లను కనుగొనగలవు. • AI వ్యవస్థలు శిక్షణ తర్వాత పవర్ ఆన్ చేయగానే పూర్తి పరిజ్ఞానంతో పనిచేయడం ప్రారంభిస్తాయి, ఎక్కడికైనా తరలి వెళ్లగలవు మరియు చాలా ఆలస్యం అయ్యే వరకు మనం వాటిని గుర్తించలేకపోవచ్చు.
- AI ఇంటర్నెట్‌ను స్వాధీనం చేసుకోవడం మరియు మౌలిక సదుపాయాలను హ్యాక్ చేయడం వల్ల

సమీప భవిష్యత్తులో నష్టం వాటిల్లవచ్చువ్యవస్థలు మరియు వినియోగాలు.

• AI వ్యవస్థలను సందేహంతో మరియు తక్కువ స్థాయి నమ్మకంతో సమీపించండి:
• సోషల్ మీడియా నుండి పొందిన సమాచారాన్ని నమ్మవద్దు.
• సిరి లేదా దానికి సమానమైన సంభాషణ పర్యవేక్షణ యాప్‌లను నిలిపివేసి ఉంచండి.
• మీరు Chat GPT లేదా Claude వంటి AI సాధనాలను ఉపయోగిస్తుంటే, “అందరి కోసం మోడల్‌ను మెరుగుపరచండి” అనే ఎంపికను మరియు లొకేషన్ ఎంపికను నిలిపివేయండి.
• వాణిజ్యపరంగా లభించే AI ఏజెంట్లు మీ వ్యక్తిగత డేటాను ఎలా నిర్వహిస్తాయో మీరు విశ్వసనీయంగా ధృవీకరించగలిగితే తప్ప వాటిని ఉపయోగించవద్దు. మీకు ఖచ్చితంగా అవసరమైతేనే, తక్కువ ప్రమాదం ఉన్న అప్లికేషన్‌ల కోసం దీనిని ఉపయోగించండి.
• మీ ఆలోచనలను మరియు ఉద్దేశాలను, ముఖ్యంగా మీ డైరీని లేదా వ్యక్తిగత జర్నల్‌ను ఏ AI ఏజెంట్‌కు అప్పగించవద్దు. • మీ బ్యాంక్ ఖాతాలు, బిల్లులు, చెల్లింపులు, ఇతర ఆర్థిక విషయాలు మరియు లావాదేవీలను ఆటోమేట్ చేయడానికి AI ఏజెంట్లకు యాక్సెస్ ఇవ్వవద్దు.
• మీ ఫోల్డర్‌లకు, ఇమెయిల్ సేవలకు మరియు కార్డ్ సమాచారానికి యాక్సెస్ ఇవ్వవద్దు.
• ఎల్లప్పుడూ మీ అంతట మీరే ఆలోచించండి, మీ తరపున ఆలోచించమని ఏఐని అడగవద్దు.
• మీ ఆలోచనా విధానాన్ని AI సిస్టమ్‌లతో కాకుండా, నమ్మకమైన స్నేహితునితో సరిచూసుకోండి.

• గోప్యతా నియంత్రణలను సమర్థవంతంగా ఉపయోగించండి, తప్పనిసరి అయితేనే వైద్య మరియు ఆర్థిక రికార్డులను అప్‌లోడ్

చేయండి.28/10/2026 పి రాజగోపాల్ తంపి 4

• కేవలం గొంతు కుటుంబ సభ్యునిలాగే వినిపిస్తుందన్న కారణంతో కాల్ చేసే వారిని ఎప్పుడూ నమ్మవద్దు. • ఎవరైనా అత్యవసర పరిస్థితిలో ఉన్న బంధువునని చెప్పుకుని డబ్బు అడిగితే, కాల్ కట్ చేసి, వారు ముందుగా సేవ్ చేసుకున్న నంబర్‌కు తిరిగి కాల్ చేయండి.

• అత్యవసర పరిస్థితుల కోసం కుటుంబ సభ్యులందరూ వ్యక్తిగతంగా ధృవీకరించుకోవడానికి ఒక వాక్యాన్ని నిర్ణయించుకోండి. దానిని సోషల్ మీడియాలో పంచుకోవద్దు.మీడియా.

• అవతలి వ్యక్తి ముఖాన్ని మీరు గుర్తుపట్టినంత మాత్రాన వీడియో కాల్ నిజమైనదని భావించవద్దు. • డబ్బు, గోప్యత లేదా తక్షణ చర్య కోసం చేసే అత్యవసర అభ్యర్థనలను హెచ్చరిక సంకేతాలుగా పరిగణించండి. • పోలీసులు, సీబీఐ, కస్టమ్స్, కోర్టులు లేదా ఇతర అధికారులు ఉన్నారని పేర్కొనే సందేశాలను నమ్మవద్దు.మిమ్మల్ని డిజిటల్ అరెస్టుకు గురిచేశారు.

• గుర్తింపు రుజువుగా కాలర్ ఐడి, వాట్సాప్ ప్రొఫైల్ ఫోటోలు లేదా ప్రదర్శించబడే సంస్థ పేర్లను నమ్మవద్దు.

• మీ ఆన్‌లైన్ డేటా ప్రొఫైల్ మరియు ఫుట్‌ప్రింట్‌ను సాధ్యమైనంత కనిష్ట స్థాయికి తగ్గించండి • నకిలీ గుర్తింపు ఉదాహరణ (నకిలీ వీడియో కాల్ ఆమోదం కారణంగా $25 మిలియన్లు బదిలీ చేయబడ్డాయి).

• సరైన కారణం లేకుండా గుర్తింపు పత్రాలను పంచుకోవడం మానుకోండి.
• అవసరమైన చోట, గుర్తింపు పత్రాల కాపీలకు నిర్దిష్ట ప్రయోజనానికి సంబంధించిన వాటర్‌మార్క్‌ను జోడించండి.• వాట్సాప్, ఫేస్‌బుక్, ఇన్‌స్టాగ్రామ్ మరియు ఇతర సోషల్ ప్లాట్‌ఫామ్‌లలోని గోప్యతా సెట్టింగ్‌లను సమీక్షించండి.• మిమ్మల్ని మెసేజింగ్ గ్రూపులలో ఎవరు చేర్చగలరో పరిమితం చేయండి, గ్రూపు సభ్యత్వాలను తగ్గించడానికి ప్రయత్నించండి. • ఆచరణ సాధ్యమైన చోట, బహిరంగంగా అందుబాటులో ఉండే వాయిస్ రికార్డింగ్‌లు మరియు వ్యక్తిగత వీడియోలను పరిమితం చేయండి. • వివరణాత్మక కుటుంబ సంబంధాలు, దినచర్యలు మరియు ఆర్థిక పరిస్థితులను ప్రచురించడం మానుకోండి. • బహిరంగ ఆన్‌లైన్ ప్రొఫైల్‌ల నుండి అనవసరమైన వ్యక్తిగత సమాచారాన్ని తొలగించండి.• UIDAI యొక్క అధికారిక ఆధార్ ధృవీకరణ-చరిత్ర మరియు బయోమెట్రిక్-లాకింగ్ సౌకర్యాలను ఉపయోగించండితగినది.
• అందుబాటులో ఉన్నచోట, అధికారిక ప్రభుత్వ టెలికాం సేవల ద్వారా మీ మొబైల్ కనెక్షన్‌లను

సరిచూసుకోండి.

• విశ్వసనీయత తక్కువగా ఉన్న సబ్‌స్క్రిప్షన్‌లు మరియు రిజిస్ట్రేషన్‌ల కోసం ప్రత్యేక ఇమెయిల్ చిరునామాను ఉపయోగించండి.• క్లౌడ్-షేరింగ్ లింక్‌లను సమీక్షించండి మరియు ఇకపై అవసరం లేనప్పుడు పబ్లిక్ యాక్సెస్‌ను తొలగించండి.

• మీ బ్యాంకింగ్ పిన్, యూపీఐ పిన్, ఏటీఎం పిన్, సీవీవీ, పాస్‌వర్డ్, పుట్టిన తేదీ లేదా ఓటీపీని ఎప్పుడూ వెల్లడించవద్దు.• గుర్తుంచుకోండి: డబ్బు స్వీకరించడానికి మీరు UPI PINను నమోదు చేయనవసరం లేదు. దానిని నమోదు చేయడం సాధారణంగా చెల్లింపును ఆమోదిస్తుంది.• డబ్బు స్వీకరించడానికి అపరిచితులు పంపిన క్యూఆర్ కోడ్‌ను ఎప్పుడూ స్కాన్ చేయవద్దు.

• అనుకోని UPI సేకరణ అభ్యర్థనను ఎప్పుడూ ఆమోదించవద్దు.

• ఏఐని ఉపయోగించి గ్యారెంటీతో కూడిన అధిక రాబడులు లేదా అసాధారణ లాభాలను వాగ్దానం చేసే పెట్టుబడి పథకాలను నమ్మవద్దు.• మీ బ్యాంకింగ్ అప్లికేషన్‌ను రిమోట్‌గా ఆపరేట్ చేయడానికి ఏజెంట్లను మరియు అపరిచితులను ఎప్పుడూ అనుమతించవద్దు.

• బ్యాంకు కార్డులు, చెక్కులు లేదా ఆర్థిక పత్రాల ఫోటోలను తెలియని వ్యక్తులతో పంచుకోవద్దు. • అన్ని ముఖ్యమైన ఖాతాలపై లావాదేవీల హెచ్చరికలను ఎనేబుల్ చేయండి.

• మీ బ్యాంకు అనుమతించిన చోట, మీ అవసరాలకు తగినట్లుగా రోజువారీ బదిలీ పరిమితులను నిర్ణయించుకోండి.

• కార్డుల సంరక్షణ: ఆన్‌లైన్‌లో వీలైనంత వరకు కార్డు వివరాలను నిల్వ చేయవద్దు. కార్డు వివరాలు ఆటోమేటిక్‌గా నింపే ప్రక్రియను నివారించండి. • అధిక పరిమితులు ఇకపై అవసరం లేనప్పుడు క్రెడిట్-కార్డ్ ఆన్‌లైన్ లావాదేవీల పరిమితులను తగ్గించండి. • అవసరం లేనప్పుడు అంతర్జాతీయ కార్డు లావాదేవీలను నిలిపివేయండి.

• విదేశాలకు ప్రయాణించేటప్పుడు, ముఖ్యంగా కాంటాక్ట్‌లెస్ లావాదేవీలను నిలిపివేయండి – ఆమ్‌స్టర్‌డామ్ సంఘటన • తరచుగా ఆన్‌లైన్/UPI చెల్లింపుల కోసం ఉపయోగించే ఖాతాల నుండి గణనీయమైన పొదుపును వేరుగా ఉంచండి.28/10/2026 పి రాజగోపాల్ తంపి 7

• బ్యాంకింగ్, ఇమెయిల్ మరియు ముఖ్యమైన ఖాతాలకు వేర్వేరు పాస్‌వర్డ్‌లను ఉపయోగించండి. • ఊహించడం కష్టంగా ఉండే పొడవైన పాస్‌వర్డ్‌లను లేదా పాస్‌ఫ్రేజ్‌లను ఉపయోగించండి.

• అందుబాటులో ఉన్న చోట టూ-ఫ్యాక్టర్ అథెంటికేషన్ లేదా FIDO2 అథెంటికేషన్‌ను ఎనేబుల్ చేయండి.• మీ ఫోన్‌ను పిన్, వేలిముద్ర లేదా ముఖ ప్రమాణీకరణతో లాక్ చేయండి.

• మీ ఫోన్ మరియు అప్లికేషన్‌లను తాజా విడుదలలతో అప్‌డేట్‌గా ఉంచుకోండి. • అప్లికేషన్‌లను అధికారిక యాప్ స్టోర్‌ల నుండి మాత్రమే డౌన్‌లోడ్ చేసుకోండి.

• అపరిచిత వ్యక్తి వాట్సాప్, SMS లేదా ఇమెయిల్ ద్వారా పంపిన APK లేదా అప్లికేషన్‌ను ఇన్‌స్టాల్ చేయవద్దు.

• అపరిచితుల అభ్యర్థన మేరకు స్క్రీన్-షేరింగ్ లేదా రిమోట్-యాక్సెస్ అప్లికేషన్‌లను ఇన్‌స్టాల్ చేయవద్దు. • మీ KYC, PAN, ఆధార్, బ్యాంక్ ఖాతా, విద్యుత్ సరఫరా లేదా డెలివరీ నిలిపివేయబడుతుందని పేర్కొంటూ వచ్చే ఊహించని లింక్‌లను క్లిక్ చేయవద్దు.
• సందేశాలలోని లింక్‌లను క్లిక్ చేయడానికి బదులుగా, అధికారిక బ్యాంకింగ్ లేదా సేవా అప్లికేషన్‌ను మీరే తెరవండి.

• వీలైతే ఖాతాల కోసం బ్యాకప్ సెక్యూరిటీ కీని నమోదు చేసి, దానిని సురక్షితంగా భద్రపరచండి.
• వ్యక్తిగత, కుటుంబ, సంబంధాల వివరాలు మరియు ఫోటోలను పెట్టడం మానుకోండిసోషల్ మీడియాలో.
• మీ ప్రయాణ ప్రణాళికను లేదా దినచర్యను సోషల్ మీడియాలో ప్రచురించవద్దు. • మీ ఇష్టాలు, అయిష్టాలు, రాజకీయ అభిప్రాయాలు, ఆర్థిక కొనుగోళ్లు మరియు వ్యక్తిగత కార్యకలాపాలను సోషల్ మీడియాలో బహిర్గతం చేయవద్దు.

• ఇంటి వైఫై కోసం బలమైన పాస్‌వర్డ్‌లతో WPA2 AES లేదా WPA 3 ఎన్‌క్రిప్షన్‌ను ఉపయోగించండి.

• మీరు ఇంటి కెమెరాలు మరియు ఐఓటీ పరికరాలను ఉపయోగిస్తే, డేటా మీ డేటా కార్డ్‌లోనే ఉండేలా చూసుకోండి. దానిని క్లౌడ్‌కు బదిలీ చేయవద్దు.

• సోషల్ మీడియాలో నకిలీ ఖాతాలను బ్లాక్ చేసి, రిపోర్ట్ చేయండి.

లో మోసం జరిగితే ఏం చేయాలి?

1. భారతదేశపు జాతీయ సైబర్ ఆర్థిక మోసాల హెల్ప్‌లైన్ అయిన 1930కు వెంటనే కాల్ చేయండి.
2. ఈ సంఘటన గురించి ఆన్‌లైన్‌లో ఇక్కడ నివేదించండిజాతీయ సైబర్ క్రైమ్ రిపోర్టింగ్ పోర్టల్
3. వెంటనే మీ బ్యాంకును సంప్రదించండి
4. ప్రభావితమైన కార్డ్‌లు, ఖాతాలు లేదా చెల్లింపు యాక్సెస్‌ను తగిన విధంగా నిరోధించమని అభ్యర్థించండి.5. రికవరీకి హామీ లేనప్పటికీ, ముందుగా రిపోర్ట్ చేయడం వల్ల తదుపరి బదిలీలను నిలిపివేసే అవకాశం మెరుగుపడుతుంది.ఈ చర్యలను కూడా తీసుకోండి:
1. మోసగాడిగా అనుమానిస్తున్న వ్యక్తితో సంభాషణను ఆపివేయండి.

2. రిమోట్-యాక్సెస్ సెషన్‌లను డిస్‌కనెక్ట్ చేసి, అనధికార సాఫ్ట్‌వేర్‌ను తీసివేయడానికి సహాయం తీసుకోండి. 3. విశ్వసనీయమైన పరికరాన్ని ఉపయోగించి రాజీపడిన పాస్‌వర్డ్‌లను మార్చండి. 4. అనుమానాస్పద లాగిన్ సెషన్‌లను రద్దు చేయండి మరియు అవసరమైన చోట ప్రమాణీకరణ పద్ధతులను రీసెట్ చేయండి.5. సందేశాలు, స్క్రీన్‌షాట్‌లు, ఫోన్ నంబర్లు, లావాదేవీల వివరాలు మరియు ఇతర సాక్ష్యాలను భద్రపరచండి. 6. నకిలీ ప్రొఫైల్‌లు, డీప్‌ఫేక్‌లు మరియు నకిలీ గుర్తింపును ప్రదర్శించే కంటెంట్‌ను సంబంధిత ప్లాట్‌ఫారమ్‌లకు మరియు అధికారులకు నివేదించండి. 7. మోసపూరిత సందేశాలు పంపడానికి మీ ఖాతాను ఉపయోగించినట్లయితే, ప్రభావితమైన పరిచయస్తులను హెచ్చరించండి.

1. స్వయంగా ధృవీకరించుకోకుండా, తెలిసిన గొంతును గానీ, ముఖాన్ని గానీ ఎప్పుడూ నమ్మవద్దు. 2. OTP, PIN, పాస్‌వర్డ్ లేదా బ్యాంకింగ్ వివరాలను ఎప్పుడూ బయటపెట్టవద్దు.
3. బెదిరింపులు, అత్యవసరం లేదా గోప్యత కారణంగా ఎప్పుడూ డబ్బు బదిలీ చేయవద్దు.
4. డిజిటల్ అరెస్టు లేదా పోలీస్ సేఫ్ ఖాతాల గురించిన వాదనలను ఎప్పుడూ నమ్మవద్దు.
5. డబ్బు స్వీకరించడానికి క్యూఆర్ కోడ్‌ను స్కాన్ చేయడం లేదా యూపీఐ పిన్‌ను నమోదు చేయడం ఎప్పుడూ చేయవద్దు.
6. అపరిచితుల కోరిక మేరకు సాఫ్ట్‌వేర్‌ను ఇన్‌స్టాల్ చేయవద్దు లేదా మీ స్క్రీన్‌ను షేర్ చేయవద్దు.

7. అనుకోని లింకులు, పెట్టుబడి ఆఫర్లు లేదా పెన్షన్‌కు సంబంధించిన సందేశాలను ఎప్పుడూ నమ్మవద్దు. 8. ఫోన్‌లను అప్‌డేట్‌గా ఉంచుకోండి మరియు బలమైన ఖాతా ప్రామాణీకరణను ప్రారంభించండి.

9. అసాధారణమైన ఆర్థిక నిర్ణయాలు తీసుకునే ముందు నమ్మకమైన వ్యక్తిని సంప్రదించండి. 10. మోసం జరిగితే, మీ బ్యాంకును సంప్రదించి, వెంటనే 1930కి కాల్ చేయండి.

11. గుర్తుంచుకోవలసిన అత్యంత ప్రభావవంతమైన సూత్రం ఒక్కటే:

12. కేవలం నిజమైనదిగా కనిపిస్తున్నంత మాత్రాన ఒక స్వరం, ముఖం, సందేశం లేదా వీడియోను ఎప్పుడూ నమ్మవద్దు. చర్య తీసుకునే ముందు గుర్తింపును మరియు అభ్యర్థనను స్వతంత్రంగా ధృవీకరించుకోండి.

మొబైల్ ఫోన్ భద్రత	
సెట్టింగ్స్	సిఫార్సు చేయబడిన సె
స్థానం	యాప్‌ను ఉపయోగిస్తు
కెమెరా	యాప్‌ను ఉపయోగిస్తు

మైక్రోఫోన్	ప్రతిసారీ అడగండి
పరిచయాలు మరియు SMS	ప్రతిసారీ అడగండి
క్యాలెండర్	ప్రతిసారీ అడగండి
ఆరోగ్య డేటా	లేదు
ఫోటోలు మరియు వీడియోలు	లేదు
శారీరక కార్యకలాపాలు	లేదు

నోటిఫికేషన్లు	లేదు
బ్లూటూత్	ఉపయోగించినప్పుడు
AI యాప్‌లు	శిక్షణ కోసం డేటాను ఉ

అవకాశం మరియు సంసిద్ధత కలిసే చోటే అదృష్టం ఉంటుంది.

AIP రీసెర్చ్ వెబ్-సైట్ HTTPS:AIPATHFINDER.ORG

అనువర్తిత మానవ-కేంద్రీకృత AI –HTTPS://www.amazon.com/dp/B0CYXHYPHC

మీ తెలివితేటలను పెంపొందించుకోండి -https://www.amazon.in/dp/B0D3WZXY99

ధన్యవాదాలు!