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

certin
Enhancing Cyber Security in India

ISEA Information Security Education & Awareness

Digital India
Power To Empower

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

# AI అవగాహన గైడ్

## సైబర్ పరిశుభ్రత సంస్కృతిని నిర్మించండి

#సైబర్ పరిశుభ్రత మన సంస్కృతి



## జాతీయ సైబర్ భద్రతా అవగాహన మాసం
## (అక్టోబర్ 2026)

నిర్వహించిన వారు

**భారత కంప్యూటర్ అత్యవసర ప్రతిస్పందన బృందం**

మమ్మల్ని అనుసరించండి :
@IndianCERT
@cert_india

# విషయ సూచిక

ముందుమాట 3

AI-ఆధారిత ఫిషింగ్ & సోషల్ ఇంజనీరింగ్ 4

వాయిస్ & వీడియో డీప్‌ఫేక్‌లు (విషింగ్) 5

AI-సహాయక మాల్వేర్ మరియు స్వయంచాలక దాడులు 6

నకిలీ వెబ్‌సైట్‌లు మరియు గుర్తింపు దొంగతనం 7

ప్రమాద సంకేతాల జాబితా 8

ఆన్‌లైన్ భద్రత 9

పరికర భద్రత 10

AIని బాధ్యతాయుతంగా ఉపయోగించండి 11

విశ్వసనీయమైన యాప్‌లను ఎంచుకోండి 12

సైబర్ భద్రతా సంఘటనలను CERT-Inకు నివేదించండి 13

# ముందుమాట

కృత్రిమ మేధస్సు (AI) మనం జీవించే, పనిచేసే మరియు సంభాషించే విధానాన్ని మారుస్తోంది. ఇది ఆవిష్కరణలను సాధ్యం చేస్తుంది, ఉత్పాదకతను మెరుగుపరుస్తుంది మరియు వివిధ రంగాలలో సంక్లిష్ట సమస్యలను పరిష్కరించడంలో సహాయపడుతుంది. అయితే, ఇదే సాంకేతికతను ముప్పు కలిగించే శక్తులు మరింత అధునాతనమైన మరియు నమ్మశక్యమైన సైబర్ బెదిరింపులను సృష్టించడానికి దుర్వినియోగం చేస్తున్నాయి.

AI డిజిటల్ ముప్పులను గుర్తించడాన్ని మరింత కష్టతరం చేస్తోంది, ఎందుకంటే దాడి చేసేవారు ఇప్పుడు అత్యంత వాస్తవికమైన ఇమెయిళ్ళు, సందేశాలు, ఆడియో, వీడియోలు మరియు వెబ్‌సైట్‌లను సృష్టించగలరు. తప్పుల వ్యాకరణం, అసాధారణ ఫార్మాటింగ్ లేదా స్పష్టమైన తప్పులు వంటి సాంప్రదాయ హెచ్చరిక సంకేతాలు ఇకపై నమ్మదగిన సూచికలు కాకపోవచ్చు. ధృవీకరణ మరియు బాధ్యతాయుతమైన డిజిటల్ పద్ధతులు గతంలో కంటే ఇప్పుడు మరింత ముఖ్యమైనవిగా మారాయి.

మనం ప్రతిరోజూ ఉపయోగించే AI సాధనాలు మరియు స్మార్ట్ పరికరాలను జాగ్రత్తగా ఉపయోగించకపోతే, అవి కొత్త గోప్యత మరియు భద్రతా ప్రమాదాలను తీసుకురాగలవు. నమ్మకం లేని AI అప్లికేషన్‌లతో వ్యక్తిగత లేదా గోప్యమైన సమాచారాన్ని పంచుకోవడం, అనవసరమైన అనుమతులు ఇవ్వడం, లేదా ధృవీకరణ లేకుండా AI ద్వారా రూపొందించబడిన సమాచారంపై ఆధారపడటం వంటివి వ్యక్తులను మరియు సంస్థలను భద్రతా ప్రమాదాలకు గురిచేయవచ్చు.

ఇండియన్ కంప్యూటర్ ఎమర్జెన్సీ రెస్పాన్స్ టీమ్ (CERT-In) వారి “AI సైబర్ అవేర్‌నెస్” పై రూపొందించిన ఈ పుస్తకం, కేవలం సైబర్‌సెక్యూరిటీ నిపుణులకే కాకుండా, సాధారణ పౌరులు, ఉద్యోగులు మరియు డిజిటల్ వినియోగదారుల కోసం ఉద్దేశించబడింది. AI డిజిటల్ ముప్పుల స్వరూపాన్ని ఎలా మారుస్తుందో ఇది వివరిస్తుంది మరియు వ్యక్తిగత సమాచారం, పరికరాలు మరియు ఆన్‌లైన్ గుర్తింపును రక్షించుకోవడానికి ప్రతి ఒక్కరూ అనుసరించగల సులభమైన, ఆచరణాత్మక దశలను అందిస్తుంది.

# AI-ఆధారిత ఫిషింగ్ & సోషల్ ఇంజనీరింగ్




## ఇది ఎలా పనిచేస్తుంది?

ఇప్పుడు హాని కలిగించే వ్యక్తులు నిజమైనవిగా, దోషరహితమైనవిగా కనిపించే ఈమెయిళ్ళు మరియు టెక్స్ట్ సందేశాలను పంపుతున్నారు. ఆ సందేశాలు వ్యక్తిగతమైనవిగా అనిపించేలా చేయడానికి, వారు మీ ఉద్యోగం, మీరు ఉపయోగించే సేవలు లేదా ఇటీవలి కార్యకలాపాల వంటి మీ గురించిన వివరాలను ఉపయోగిస్తారు. ఈ సందేశాలు చక్కగా వ్రాయబడి ఉంటాయి కాబట్టి, వాటిని గుర్తించడం చాలా కష్టంగా ఉంటుంది.

## ఎలా గుర్తించాలి?

- ఆ సందేశం మీకు చాలా ప్రత్యేకమైనదిగా అనిపిస్తుంది, కానీ అది అనుకోకుండా వస్తుంది.
- ఇది ఆత్రుతతో కూడిన లేదా బెదిరించే ధోరణిని ఉపయోగిస్తుంది మరియు తక్షణ చర్యను కోరుతుంది.
- ఇది మిమ్మల్ని ఒక లింక్‌పై క్లిక్ చేయమని, ఖాతాను ధృవీకరించమని, పాస్‌వర్డ్‌ను రీసెట్ చేయమని లేదా చెల్లింపు చేయమని అడుగుతుంది.
- పంపినవారి చిరునామా దాదాపు సరిగ్గానే ఉంది, కానీ పూర్తిగా కాదు.

## సురక్షితంగా ఉండటం ఎలా?

- అభ్యర్థించని సందేశాలలోని లింక్‌లను క్లిక్ చేయవద్దు. బదులుగా నేరుగా అధికారిక వెబ్‌సైట్ లేదా యాప్‌కి వెళ్లండి.
- అధికారిక ఫోన్ నంబర్ లేదా యాప్ వంటి ప్రత్యేకమైన, విశ్వసనీయమైన సంప్రదింపు మార్గం ద్వారా అభ్యర్థనలను ధృవీకరించండి.
- సందేశ లింక్ ద్వారా చేరుకున్న పేజీలో ఎప్పుడూ ఆధారాలను లేదా OTPలను నమోదు చేయవద్దు.
- అనుమానాస్పద సందేశాలను రిపోర్ట్ చేసి, తొలగించండి, ఆపై పంపినవారిని బ్లాక్ చేయండి.

# వాయిస్ & వీడియో డీప్‌ఫేక్‌లు [విషింగ్]




## ఇది ఎలా పనిచేస్తుంది?

హాని కలిగించే వ్యక్తులు స్వరాలను క్లోన్ చేయగలరు లేదా నిజమైనవిగా కనిపించే మరియు వినిపించే నకిలీ వీడియోలను సృష్టించగలరు. వారు సున్నితమైన సమాచారాన్ని పంచుకోవడానికి, డబ్బు పంపడానికి లేదా త్వరగా చర్య తీసుకోవడానికి మీపై ఒత్తిడి తెచ్చేందుకు కుటుంబ సభ్యులుగా, సహోద్యోగులుగా లేదా అధికారులుగా నటిస్తారు.

## ఎలా గుర్తించాలి?

- అసాధారణమైన ఆత్రుత, భయాందోళన, లేదా ఎవరికీ చెప్పవద్దు వంటి గోప్యత కోరడాలు.
- స్వరంలో స్వల్ప తేడా, వేగం, నేపథ్య శబ్దం, లేదా ఆడియో నాణ్యత.
- సాధారణ ధృవీకరణ లేదా ఆమోద ప్రక్రియలను దాటవేయడానికి చేసే అభ్యర్థనలు.
- గిఫ్ట్ కార్డ్‌లు, క్రిప్టోకరెన్సీ లేదా వైర్ ట్రాన్స్‌ఫర్ ద్వారా చెల్లింపు కోసం అభ్యర్థనలు.

## సురక్షితంగా ఉండటం ఎలా?

- ఫోన్ పెట్టేసి, వారికి తెలిసిన, సేవ్ చేసుకున్న నంబర్‌తో తిరిగి కాల్ చేయండి.
- అత్యవసర పరిస్థితుల్లో గుర్తింపును ధృవీకరించుకోవడానికి కుటుంబం లేదా కార్యాలయంలో ఒక సురక్షిత పదాన్ని (సేఫ్ వర్డ్) ఏర్పాటు చేసుకోండి.
- కేవలం కాల్ లేదా వీడియో ఆధారంగా చెల్లింపులను ఎప్పుడూ ఆమోదించవద్దు. వేరొక మార్గం ద్వారా వ్రాతపూర్వకంగా నిర్ధారించుకోండి.
- ప్రతిస్పందించే ముందు ఒక క్షణం ఆగండి. ముప్పు కలిగించే వ్యక్తులు మీ నిర్ణయ శక్తిని దెబ్బతీయడానికి భయాందోళనలను ఆసరాగా చేసుకుంటారు.

# AI-సహాయక మాల్వేర్ & స్వయంచాలక దాడులు




## ఇది ఎలా పనిచేస్తుంది?

హాని కలిగించేవారు హానికరమైన కోడ్‌ను సృష్టించడానికి లేదా దాచడానికి, దొంగిలించిన పాస్‌వర్డ్‌లను పలు సైట్‌లలో పరీక్షించడానికి, మరియు అప్‌డేట్‌లు అవసరమైన సిస్టమ్‌లను గుర్తించడానికి AI సాధనాలను ఉపయోగిస్తారు. దీనివల్ల దాడులు మరింత వేగంగా, విస్తృతంగా జరుగుతాయి.

## ఎలా గుర్తించాలి?

- అనుకోని లాగిన్ హెచ్చరికలు, పాస్‌వర్డ్ రీసెట్ ఇమెయిల్‌లు లేదా మీరు అభ్యర్థించని MFA ప్రాంప్ట్‌లు
- మీ ఖాతా కార్యకలాపంలో జాబితా చేయబడిన అపరిచిత పరికరాలు లేదా సెషన్‌లు
- యాంటీవైరస్ హెచ్చరికలు, పాప్-అప్‌లు లేదా పరికరం పనితీరు అసాధారణంగా నెమ్మదిగా ఉండటం
- మీకు తెలియని ఫైల్‌లు, సెట్టింగ్‌లు లేదా బ్రౌజర్ ఎక్స్‌టెన్షన్‌లు

## సురక్షితంగా ఉండటం ఎలా?

- ప్రతి ఖాతాకు ప్రత్యేకమైన, బలమైన పాస్‌వర్డ్‌ను ఉపయోగించండి.
- అన్ని ముఖ్యమైన ఖాతాలపై మల్టీ ఫ్యాక్టర్ అథెంటికేషన్ (MFA)ను ఎనేబుల్ చేయండి.
- యాంటీవైరస్ సాఫ్ట్‌వేర్, సిస్టమ్‌లు మరియు యాప్‌లను ఎప్పటికప్పుడు అప్‌డేట్‌గా ఉంచండి.
- అనుకోని లాగిన్ లేదా MFA హెచ్చరికలపై తక్షణమే చర్య తీసుకోండి.

# నకిలీ వెబ్‌సైట్‌లు మరియు గుర్తింపు దొంగతనం




## ఇది ఎలా పనిచేస్తుంది?

హాని కలిగించే వ్యక్తులు మీ లాగిన్ ఆధారాలు, OTPలు లేదా చెల్లింపు వివరాలను దొంగిలించడానికి, బ్యాంకింగ్ లేదా షాపింగ్ పోర్టల్స్ వంటి నిజమైనవిగా కనిపించే నకిలీ వెబ్‌సైట్‌లు మరియు చాట్‌బాట్‌లను సృష్టించగలరు. వారు తప్పుడు గుర్తింపులను సృష్టించడానికి నకిలీ ఫోటోలు లేదా పత్రాలను కూడా ఉపయోగించవచ్చు.

## ఎలా గుర్తించాలి?

- అదనపు అక్షరాలు, హైఫన్‌లు లేదా భిన్నమైన డొమైన్ ఎండింగ్ వంటి వాటితో కొద్దిగా మార్చబడిన వెబ్‌సైట్ URLలు.
- OTPలు, PINలు లేదా పూర్తి కార్డ్ నంబర్‌లను అడిగే చాట్‌బాట్‌లు లేదా ఏజెంట్లు.
- సుపరిచితమైన సైట్‌లో HTTPS లేకపోవడం లేదా అసాధారణమైన డిజైన్ వ్యత్యాసాలు.

## సురక్షితంగా ఉండటం ఎలా?

- లింక్‌లను క్లిక్ చేయడానికి బదులుగా, ఎల్లప్పుడూ అధికారిక URLలను నేరుగా టైప్ చేయండి లేదా ధృవీకరించబడిన బుక్‌మార్క్‌లను ఉపయోగించండి.
- ఏ చాట్‌బాట్ లేదా "సపోర్ట్ ఏజెంట్"తోనూ OTPలు, PINలు లేదా పూర్తి కార్డ్ వివరాలను ఎప్పుడూ పంచుకోవద్దు.
- ఎక్కడైనా లాగిన్ చేసే ముందు HTTPS ఉందో లేదో తనిఖీ చేయండి మరియు డొమైన్ పేరును జాగ్రత్తగా పరిశీలించండి.
- మీ బ్యాంక్ స్టేట్‌మెంట్‌లను మరియు క్రెడిట్ రిపోర్ట్‌ను అనుమానాస్పద కార్యకలాపాల కోసం క్రమం తప్పకుండా పర్యవేక్షించండి.

# ప్రమాద సంకేతాల జాబితా

AI ఆధారిత దాడికి సంబంధించిన ఈ సంకేతాల పట్ల జాగ్రత్త వహించండి:

- డబ్బు, గుర్తింపు పత్రాలు లేదా ఆమోదం కోసం అత్యవసరమైన, ఒత్తిడితో కూడిన అభ్యర్థన
- తెలిసిన వ్యక్తి నుండి వచ్చిన కాల్ లేదా వీడియోలో స్వల్ప ఆడియో/వీడియో వ్యత్యాసాలు
- సాధారణ ధృవీకరణ/ఆమోద ప్రక్రియలను దాటవేయడానికి అభ్యర్థన
- అపరిచిత పంపినవారి డొమైన్ లేదా కొద్దిగా మార్చబడిన URL
- ఊహించని MFA ప్రాంప్ట్‌లు లేదా మీరు అభ్యర్థించని OTPలు
- భద్రతా సాఫ్ట్‌వేర్‌ను నిలిపివేయమని లేదా అనధికారిక లింక్‌ల ద్వారా "ధృవీకరించమని" అభ్యర్థనలు
- ముందస్తు చెల్లింపు లేదా వ్యక్తిగత ఆర్థిక వివరాలు అవసరమయ్యే ఉద్యోగ/పెట్టుబడి ఆఫర్లు

**సందేహం ఉన్నప్పుడు — ఆగండి, స్వయంగా సరిచూసుకోండి, ఒత్తిడికి లోనై చర్యలు తీసుకోవద్దు.**

# ఆన్‌లైన్ భద్రత



## మీ ఖాతాలను రక్షించుకోండి

- ప్రతి ఖాతాకు బలమైన మరియు ప్రత్యేకమైన పాస్‌వర్డ్‌లను ఉపయోగించండి; వాటిని సురక్షితంగా నిల్వ చేయడానికి పాస్‌వర్డ్ మేనేజర్‌ను వాడండి.
- అందుబాటులో ఉన్న చోటల్లా మల్టీ-ఫ్యాక్టర్ అథెంటికేషన్ (MFA) ను ఎనేబుల్ చేయండి.
- OTPలు, PINలు, పాస్‌వర్డ్‌లు లేదా సెక్యూరిటీ కోడ్‌లను ఎవరితోనూ పంచుకోవద్దు.
- అదనపు భద్రతా పొరగా బయోమెట్రిక్ ప్రమాణీకరణను (వేలిముద్ర/ముఖ గుర్తింపు) ఉపయోగించండి.

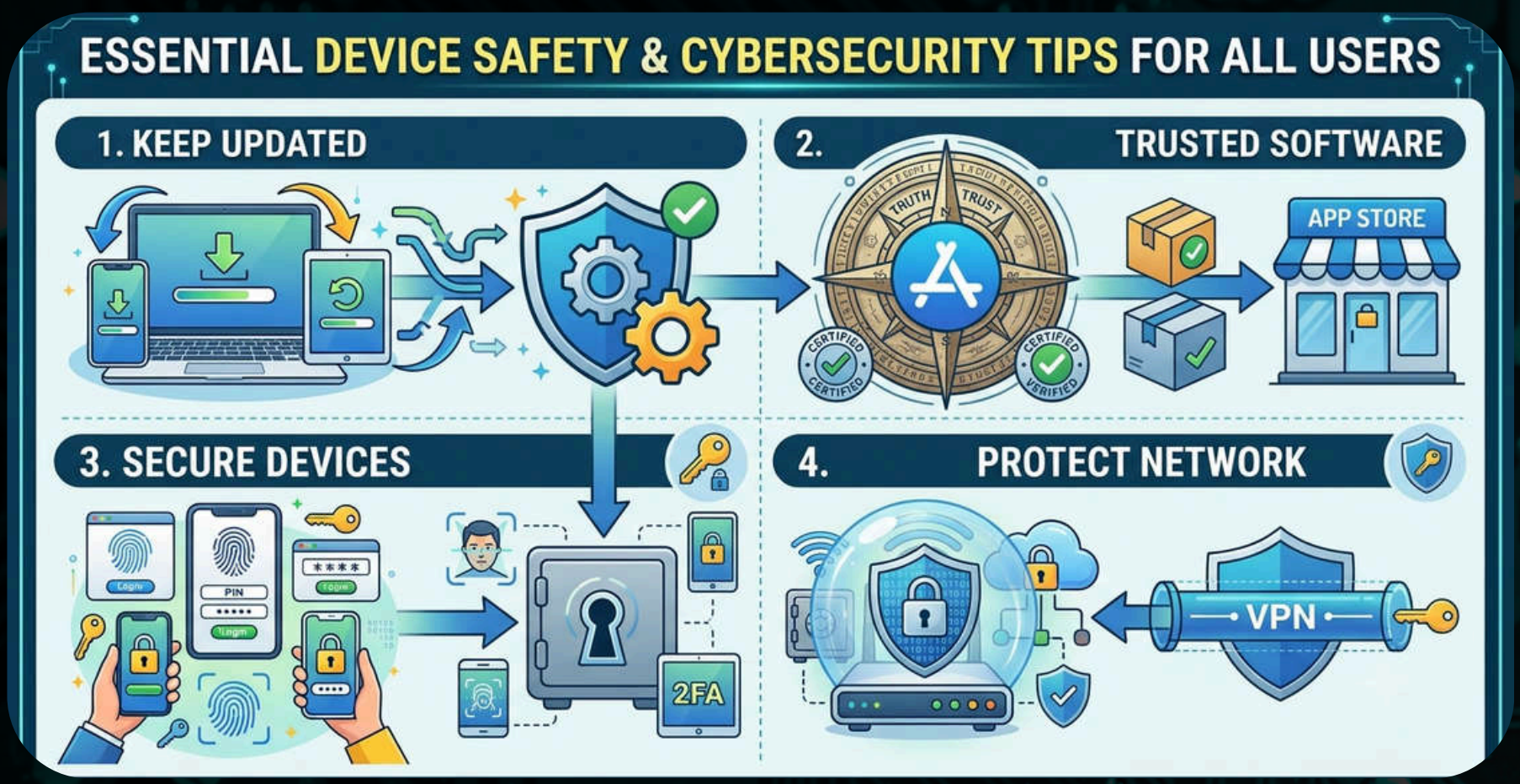
## ఇమెయిల్ మరియు ఇంటర్నెట్ ఉపయోగిస్తున్నప్పుడు సురక్షితంగా ఉండండి

- అనుమానాస్పదమైన లేదా ఒకేలా కనిపించే ఇమెయిల్ చిరునామాల కోసం పంపినవారి వివరాలను జాగ్రత్తగా తనిఖీ చేయండి.
- లింక్‌లను క్లిక్ చేసే ముందు సరిచూసుకోండి మరియు అనుకోని అటాచ్‌మెంట్‌లను తెరవకుండా ఉండండి.
- లాగిన్ లేదా ఆర్థిక వివరాలను నమోదు చేసే ముందు వెబ్‌సైట్ ప్రామాణికతను నిర్ధారించుకోండి.
- సందేహం ఉన్నప్పుడు, చర్య తీసుకునే ముందు ఆగి, సరిచూసుకోండి.

## ఏదైనా తప్పు జరగక ముందే సిద్ధపడండి

- ముఖ్యమైన ఫైళ్లను ఆఫ్‌లైన్‌లో లేదా సురక్షితమైన క్లౌడ్ సేవలో క్రమం తప్పకుండా బ్యాకప్ చేసుకోండి.
- ఖాతా పునరుద్ధరణ సమాచారాన్ని (ఈమెయిల్/ఫోన్) అప్‌డేట్‌గా మరియు సురక్షితంగా ఉంచండి.

# పరికర భద్రత




## పరికరాలను అప్‌డేట్‌గా ఉంచండి

- తెలిసిన లోపాలను సరిచేయడానికి ఆపరేటింగ్ సిస్టమ్‌లు, అప్లికేషన్‌లు, బ్రౌజర్‌లు మరియు భద్రతా సాఫ్ట్‌వేర్‌లను క్రమం తప్పకుండా అప్‌డేట్ చేయండి.
- సాధ్యమైన చోటల్లా ఆటోమేటిక్ అప్‌డేట్‌లను ఎనేబుల్ చేయండి.

## విశ్వసనీయమైన సాఫ్ట్‌వేర్‌ను మాత్రమే ఇన్‌స్టాల్ చేయండి

- అసలైన సాఫ్ట్‌వేర్‌ను ఉపయోగించండి మరియు అధికారిక యాప్ స్టోర్‌లు లేదా విశ్వసనీయ మూలాల నుండి మాత్రమే అప్లికేషన్‌లను ఇన్‌స్టాల్ చేయండి.
- విశ్వసనీయమైన యాంటీవైరస్ లేదా భద్రతా పరిష్కారాలను ఉపయోగించండి మరియు వాటిని ఎప్పటికప్పుడు అప్‌డేట్ చేస్తూ ఉండండి.

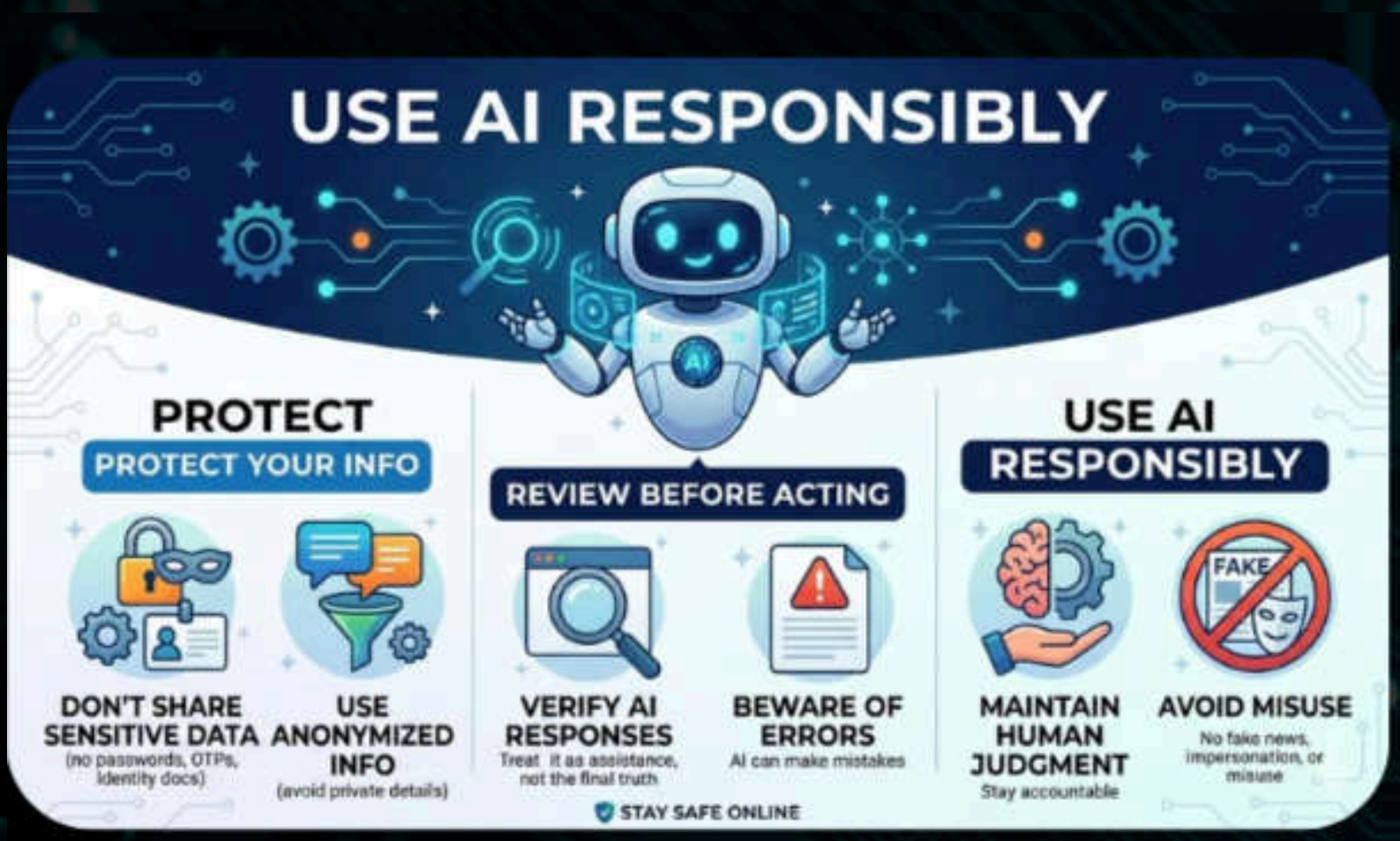
## మీ పరికరాలు మరియు ఖాతాలను సురక్షితం చేసుకోండి

- అన్ని పరికరాలలో బలమైన పాస్‌వర్డ్‌లను లేదా స్క్రీన్ లాక్‌లను ఉపయోగించండి.
- అందుబాటులో ఉన్నప్పుడల్లా పరికర ఎన్క్రిప్షన్ మరియు భద్రతా ఫీచర్లను ప్రారంభించండి.
- అనవసరమైన అప్లికేషన్‌లు మరియు అనుమతులను సమీక్షించి, తొలగించండి.

## మీ నెట్‌వర్క్ కనెక్షన్‌ను రక్షించుకోండి

- బలమైన పాస్‌వర్డ్‌తో మీ Wi-Fi ని సురక్షితం చేసుకోండి మరియు డిఫాల్ట్ రూటర్ ఆధారాలను మార్చండి.
- నవీకరించిన రౌటర్ ఫర్మ్‌వేర్ మరియు సురక్షిత నెట్‌వర్క్ సెట్టింగ్‌లను ఉపయోగించండి.
- సున్నితమైన ఖాతాలను యాక్సెస్ చేయడం లేదా అసురక్షిత నెట్‌వర్క్‌ల ద్వారా గోప్యమైన సమాచారాన్ని పంచుకోవడం వంటివి చేయవద్దు.

# AIని బాధ్యతాయుతంగా ఉపయోగించండి




## మీ వ్యక్తిగత సమాచారాన్ని రక్షించుకోండి

- వ్యక్తిగత, ఆర్థిక, ఆరోగ్య, అధికారిక లేదా గోప్యమైన సమాచారాన్ని పబ్లిక్ AI సాధనాలలో లేదా తెలియని ఆన్‌లైన్ సేవల్లో నమోదు చేయవద్దు.
- పాస్‌వర్డ్‌లు, OTPలు, ఖాతా నంబర్‌లు, గుర్తింపు పత్రాలు, కస్టమర్ డేటా లేదా ప్రైవేట్ సంభాషణల వంటి సున్నితమైన వివరాలను పంచుకోవడం మానుకోండి.
- AI సాధనాల నుండి సహాయం కోరేటప్పుడు, అనామక లేదా సాధారణ సమాచారాన్ని ఉపయోగించండి.

## పంచుకోవడానికి లేదా చర్య తీసుకోవడానికి ముందు సమీక్షించండి

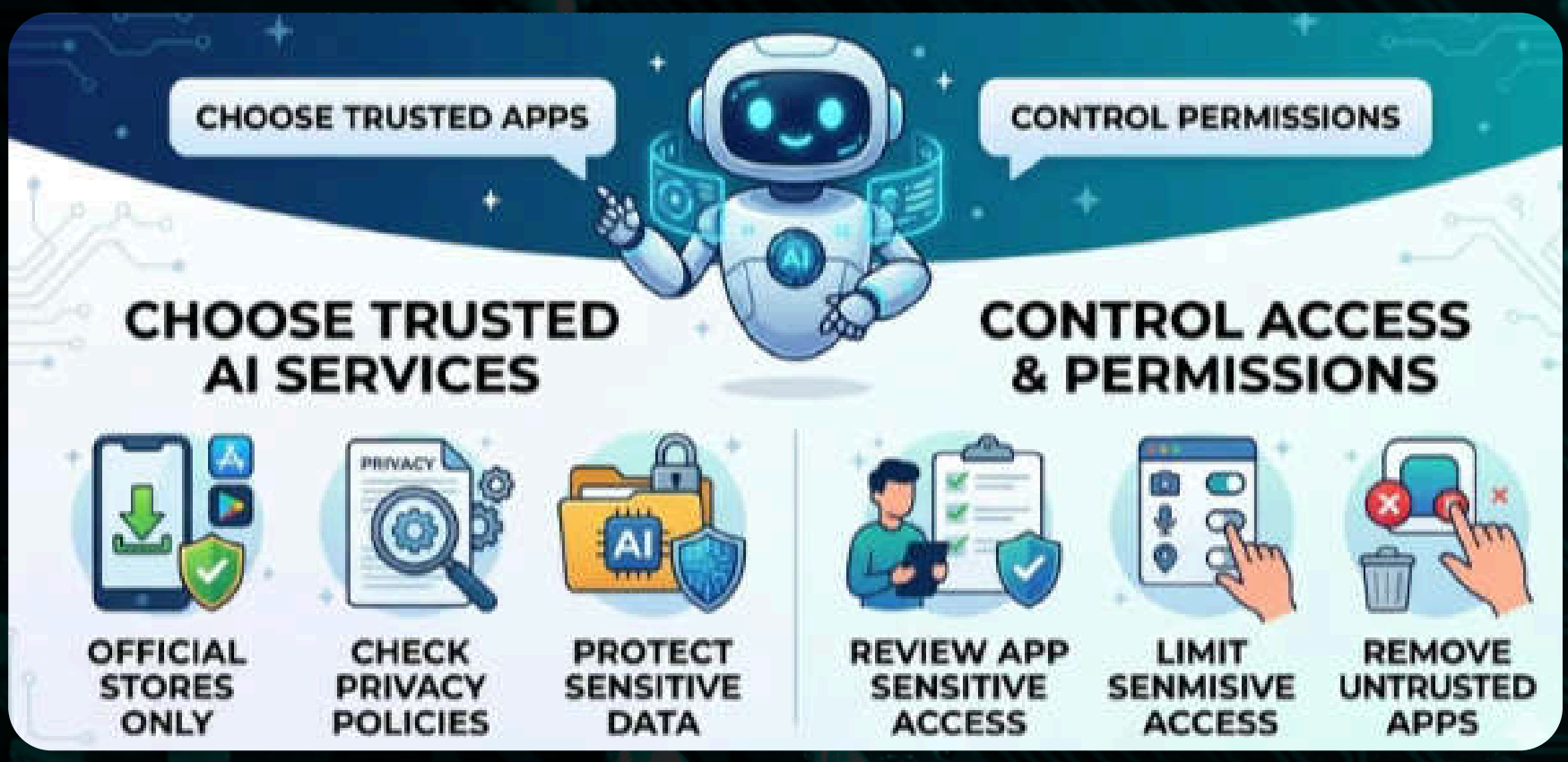
- AI రూపొందించిన ప్రతిస్పందనలను సహాయంగా పరిగణించండి, అంతిమ సత్యంగా కాదు.
- ఆర్థిక, చట్టపరమైన, వృత్తిపరమైన లేదా వ్యక్తిగత నిర్ణయాల కోసం ముఖ్యమైన సమాచారాన్ని ఉపయోగించే ముందు దాన్ని సరిచూసుకోండి.
- AI సాధనాలు తప్పుడు, అసంపూర్ణమైన లేదా తప్పుదారి పట్టించే సమాచారాన్ని అందించవచ్చని గమనించండి.

## AI సాధనాలను బాధ్యతాయుతంగా ఉపయోగించండి

- మీ పని మరియు అభ్యాసానికి మద్దతుగా ఏఐని ఉపయోగించుకోండి, కానీ మానవ విచక్షణ మరియు జవాబుదారీతనాన్ని పాటించండి.
- తప్పుడు సమాచారాన్ని సృష్టించడానికి లేదా వ్యాప్తి చేయడానికి, ఇతరుల వలె నటించడానికి, లేదా ఒకరి వ్యక్తిగత డేటాను దుర్వినియోగం చేయడానికి AIని ఉపయోగించవద్దు.

మమ్మల్ని అనుసరించండి : @IndianCERT @cert_india

# విశ్వసనీయమైన యాప్‌లను ఎంచుకోండి




## యాప్ యాక్సెస్ మరియు అనుమతులను నియంత్రించండి

- AI అప్లికేషన్‌లు మరియు డిజిటల్ అసిస్టెంట్‌లకు మంజూరు చేసిన అనుమతులను సమీక్షించండి.
- కెమెరా, మైక్రోఫోన్, కాంటాక్ట్స్ లేదా లొకేషన్ వంటి ఫీచర్లకు అవసరమైనప్పుడు మాత్రమే యాక్సెస్ ఇవ్వండి.
- అనవసరమైన అనుమతులను తొలగించి, నమ్మకం లేని మూలాల నుండి యాప్‌లను అన్‌ఇన్‌స్టాల్ చేయండి.

## విశ్వసనీయమైన AI సేవలను ఎంచుకోండి

- ప్రతిష్టాత్మకమైన సంస్థల AI అప్లికేషన్‌లను ఉపయోగించండి మరియు వాటిని అధికారిక యాప్ స్టోర్‌ల నుండి మాత్రమే డౌన్‌లోడ్ చేసుకోండి.
- AI సేవలను ఉపయోగించే ముందు గోప్యతా సెట్టింగ్‌లు, వినియోగ నిబంధనలు మరియు డేటా నిర్వహణ పద్ధతులను సమీక్షించండి.
- భద్రతా నియంత్రణలు ధృవీకరించబడే వరకు, AI సాధనాలను సున్నితమైన ఖాతాలకు లేదా ఫైళ్లకు అనుసంధానించవద్దు.

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

certin Enhancing Cyber Security in India

ISEA Information Security Education & Awareness

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

Digital India Power To Empower

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

# Report Cyber Security Incidents to CERT-In

## For reporting Cyber Security Incidents to CERT-In:

*Visit website:* ***https://www.cert-in.org.in***

*Email:* ***incident@cert-in.org.in***

*Toll Free Phone:* ***+91-1800-11-4949***

*Toll Free Fax:* ***+91-1800-11-6969***

### *Information Desk*

*Phone:* ***+91-11-22902657***

**Follow us :**

@IndianCERT

@cert_india

WEBSITE
https://www.cert-in.org.in/

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

**Awareness Booklet**
https://cert-in.org.in/AwarenessBooklets.jsp

**Security Tools**
https://www.csk.gov.in/security-tools.html