Ministry of Electronics and Information Technology
Government of India

certin
Enhancing Cyber Security in India

సైబర్‌స్మార్ట్ తరగతి గది

ఉపాధ్యాయులు మరియు విద్యార్థుల కోసం పరిస్థితి ఆధారిత సైబర్ భద్రతా మార్గదర్శిని

జాతీయ సైబర్ భద్రత అవగాహన నెల
(అక్టోబర్ 2026)
సందర్భంగా
"సైబర్ పరిశుభ్రత సంస్కృతిని నిర్మిద్దాం"
#CyberHygieneOurCulture

Information Security Education & Awareness

Digital India
Power To Empower

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

certin
Enhancing Cyber Security in India

విషయ సూచిక

	ముందుమాట	3
1	సోషల్ ఇంజినీరింగ్: “నమ్మకమా లేదా మోసమా?”	4
2	ఫిషింగ్: “ప్రమాద సంకేతాలను గుర్తించండి”	5
3	AI భద్రత: “మీరు AIని ఇది అడుగుతారా?”	6
4	మాల్వేర్: “ఇది ఎలా ప్రవేశిస్తుంది?”	7
5	సైబర్ భద్రత ఎస్కేప్ రూమ్	8
	మమ్మల్ని సంప్రదించండి	9

ముందుమాట

విద్యార్థులు ఆన్‌లైన్‌లో నేర్చుకోవడం, సంభాషించడం, కలిసి పనిచేయడం మరియు సృజనాత్మకంగా పనిచేయడం కోసం ఎక్కువ సమయం కేటాయిస్తున్నందున, సైబర్ భద్రతను అర్థం చేసుకోవడం ఒక ముఖ్యమైన జీవన నైపుణ్యంగా మారింది. సైబర్ ముప్పులు రోజువారీ డిజిటల్ అనుభవాల్లో మరింతగా భాగమవుతున్నాయి. అవి అనుమానాస్పద సందేశం, ఊహించని లాగిన్ అభ్యర్థన, తప్పుదారి పట్టించే వెబ్‌సైట్, తెలియని లింక్, మోసపూరిత వాయిస్ లేదా వీడియో, లేదా వ్యక్తిగత సమాచారాన్ని కోరే అభ్యర్థన రూపంలో కనిపించవచ్చు. ఈ పరిస్థితులను గుర్తించడం, ఆగి ఆలోచించడం, ధృవీకరించడం మరియు సమాచారంతో కూడిన నిర్ణయాలు తీసుకోవడం వంటి జ్ఞానాన్ని విద్యార్థులకు అందించడం ద్వారా చిన్న వయస్సు నుంచే సురక్షితమైన మరియు బాధ్యతాయుతమైన డిజిటల్ అలవాట్లను పెంపొందించవచ్చు.

ఇండియన్ కంప్యూటర్ ఎమర్జెన్సీ రెస్పాన్స్ టీమ్ (CERT-In) యొక్క 'సైబర్‌స్మార్ట్ తరగతి గది: ఉపాధ్యాయులు మరియు విద్యార్థుల కోసం పరిస్థితి ఆధారిత సైబర్ భద్రతా మార్గదర్శిని' ఉపాధ్యాయులకు తరగతి చర్చలు, కార్యకలాపాలు మరియు పరస్పర అభ్యాసాన్ని సులభతరం చేయడానికి ఉపయోగించగల ఆచరణాత్మకమైన, సులభంగా అర్థమయ్యే పరిస్థితులను అందిస్తుంది. ప్రతి పరిస్థితి విద్యార్థులను సంభావ్య ప్రమాదాలను గుర్తించడానికి, విమర్శనాత్మకంగా ఆలోచించడానికి, సాధ్యమైన ప్రతిస్పందనలను చర్చించడానికి మరియు సులభమైన సైబర్ భద్రత ఉత్తమ పద్ధతులను అర్థం చేసుకోవడానికి ప్రోత్సహిస్తుంది. విద్యార్థులు తమ రోజువారీ జీవితంలో ఎదుర్కొనే పరిస్థితులతో సైబర్ భద్రత భావనలను అనుసంధానించడం ద్వారా, బాధ్యతాయుతమైన డిజిటల్ పౌరసత్వ సంస్కృతిని పెంపొందిస్తూ సైబర్ అవగాహనను ఆసక్తికరంగా, సంబంధితంగా మరియు ఆచరణాత్మకంగా మార్చడానికి ఈ మార్గదర్శిని ప్రయత్నిస్తుంది.

ఈ బుక్‌లెట్ CERT-In జాతీయ సైబర్ భద్రత అవగాహన నెల కార్యకలాపాల్లో (అక్టోబర్ 2026) భాగంగా ప్రచురించబడింది. విద్యార్థులు మరియు విద్యాబోధకులలో సైబర్ భద్రత అవగాహనను బలోపేతం చేయడం దీని లక్ష్యం. ఆన్‌లైన్ భద్రతపై అర్థవంతమైన చర్చలను ప్రారంభించడంలో ఉపాధ్యాయులకు సహాయపడటం మరియు డిజిటల్ ప్రపంచంలో సమాచారంతో కూడిన, సురక్షితమైన మరియు బాధ్యతాయుతమైన ఎంపికలు చేసుకునేలా విద్యార్థులను ప్రోత్సహించడం దీని ఉద్దేశ్యం.

1. సోషల్ ఇంజినీరింగ్: 'నమ్మకమా లేదా మోసమా?'

A — అధికార ప్రతిష్ఠ
నేను IT విభాగం నుంచి మాట్లాడుతున్నాను.

U — తక్షణత
వెంటనే చర్య తీసుకోండి.

R — బహుమతి
ఉచిత డౌన్‌లోడ్.

F — పరిచయం
ఇది మీ స్నేహితుడే.

సంకేతాలు

1. ఎవరో పాఠశాల IT విభాగం నుంచి మాట్లాడుతున్నామని చెప్పి మీ పాస్‌వర్డ్‌ను అడుగుతారు.
2. ఒక వ్యక్తి తాను మీ స్నేహితుడినని చెబుతూ, కొత్త ఖాతాను ఉపయోగించి అత్యవసరంగా డబ్బు పంపమని అడుగుతారు.
3. ఎవరో మీ లాగిన్ వివరాలకు బదులుగా ఉచిత గేమ్ డౌన్‌లోడ్‌ను అందిస్తారు.
4. వెంటనే చర్య తీసుకోకపోతే తమ ఖాతా తొలగించబడుతుందని ఒక విద్యార్థికి సందేశం వస్తుంది.

నిర్ణయ మార్గం

🟢 బహుశా సురక్షితం | 🟡 ధృవీకరణ అవసరం | 🔴 మోసపూరిత ప్రభావం ఉండవచ్చు

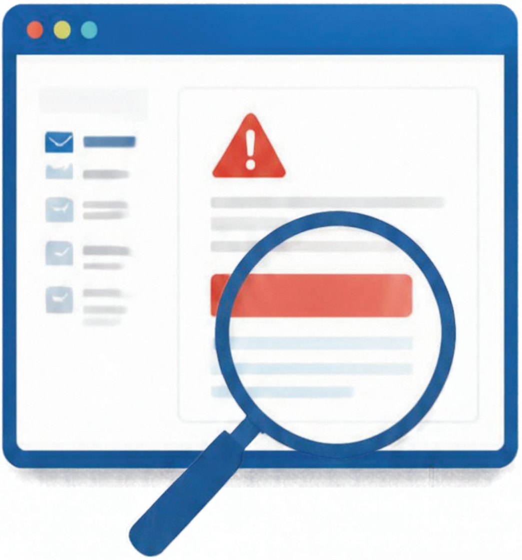
ముఖ్య పాఠం:

వ్యక్తులను ప్రభావితం చేయడానికి దాడి చేసేవారు తక్షణత, అధికారం, భయం, ఆసక్తి, బహుమతులు లేదా పరిచయాన్ని ఉపయోగించవచ్చు.

2. ఫిషింగ్: ‘ప్రమాద సంకేతాలను గుర్తించండి’

విద్యార్థులు గుర్తుంచుకోవాల్సిన నియమం:

ఆగండి → తనిఖీ చేయండి → ధృవీకరించండి → నివేదించండి



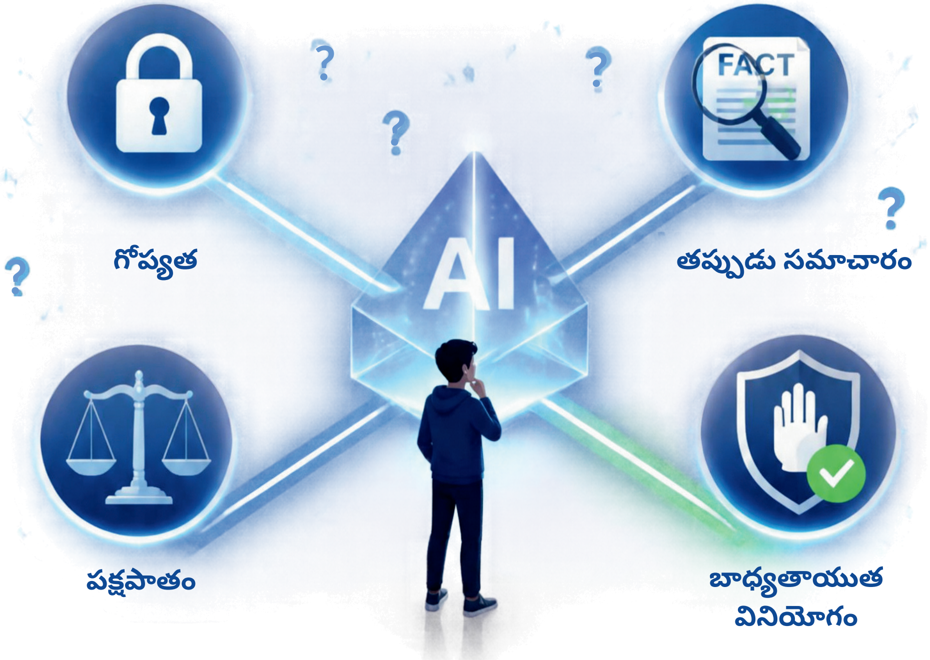
- అనుమానాస్పద పంపినవారి చిరునామాలు
- అత్యవసర లేదా బెదిరింపు భాష
- ఊహించని జోడింపులు
- పాస్‌వర్డ్‌లు లేదా వ్యక్తిగత సమాచారాన్ని కోరే అభ్యర్థనలు
- అనుమానాస్పద లింకులు
- అక్షరదోషాలు లేదా వ్యాకరణ అసంగతతలు
- అసాధారణ చెల్లింపు అభ్యర్థనలు
- సరిపోలని వెబ్‌సైట్ చిరునామాలు

సురక్షితం

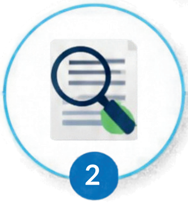
ఫిషింగ్

3. AI భద్రత: “మీరు AIని ఇది అడుగుతారా?”

విద్యార్థులకు బోధించాల్సిన అంశాలు:



వ్యక్తిగత సమాచారాన్ని రక్షించండి



ముఖ్యమైన సమాచారాన్ని ధృవీకరించండి

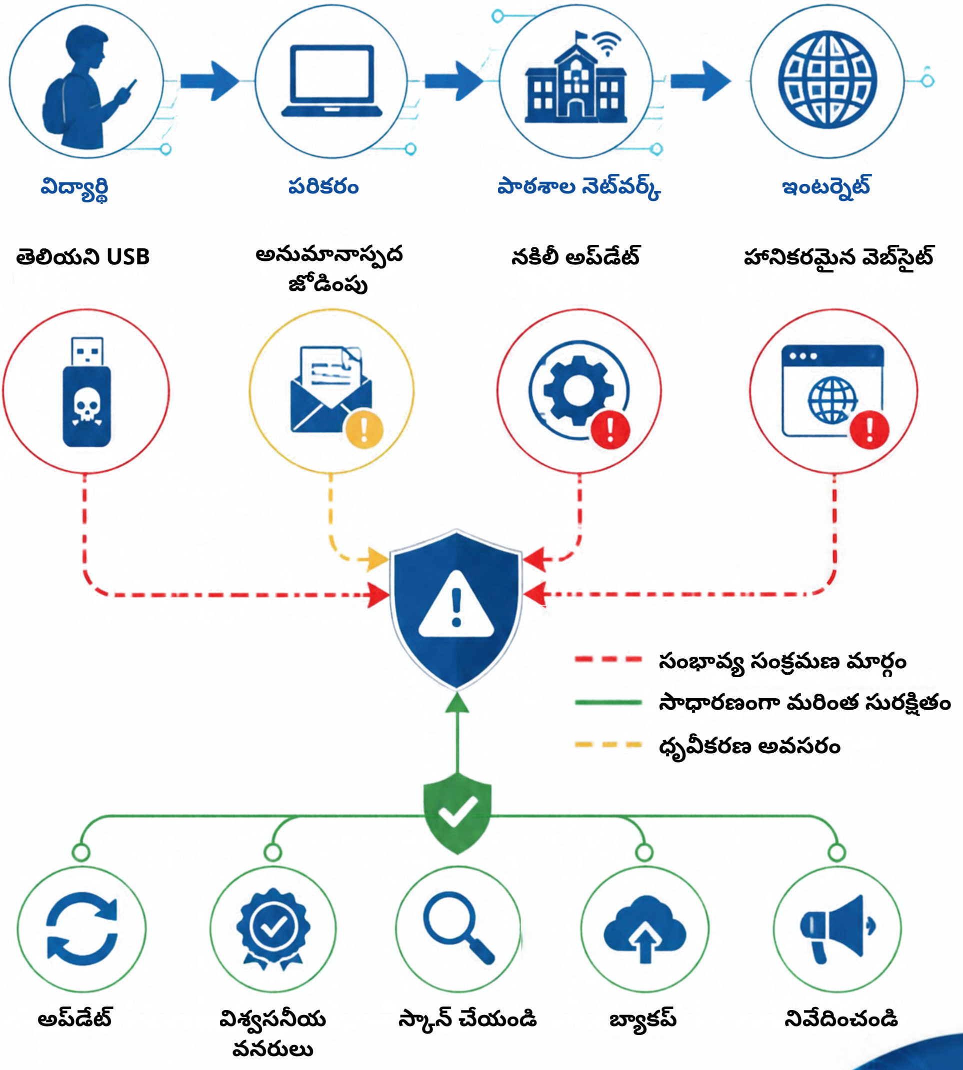
పరిణామాలను పరిగణించండి

బాధ్యతాయుత వినియోగం

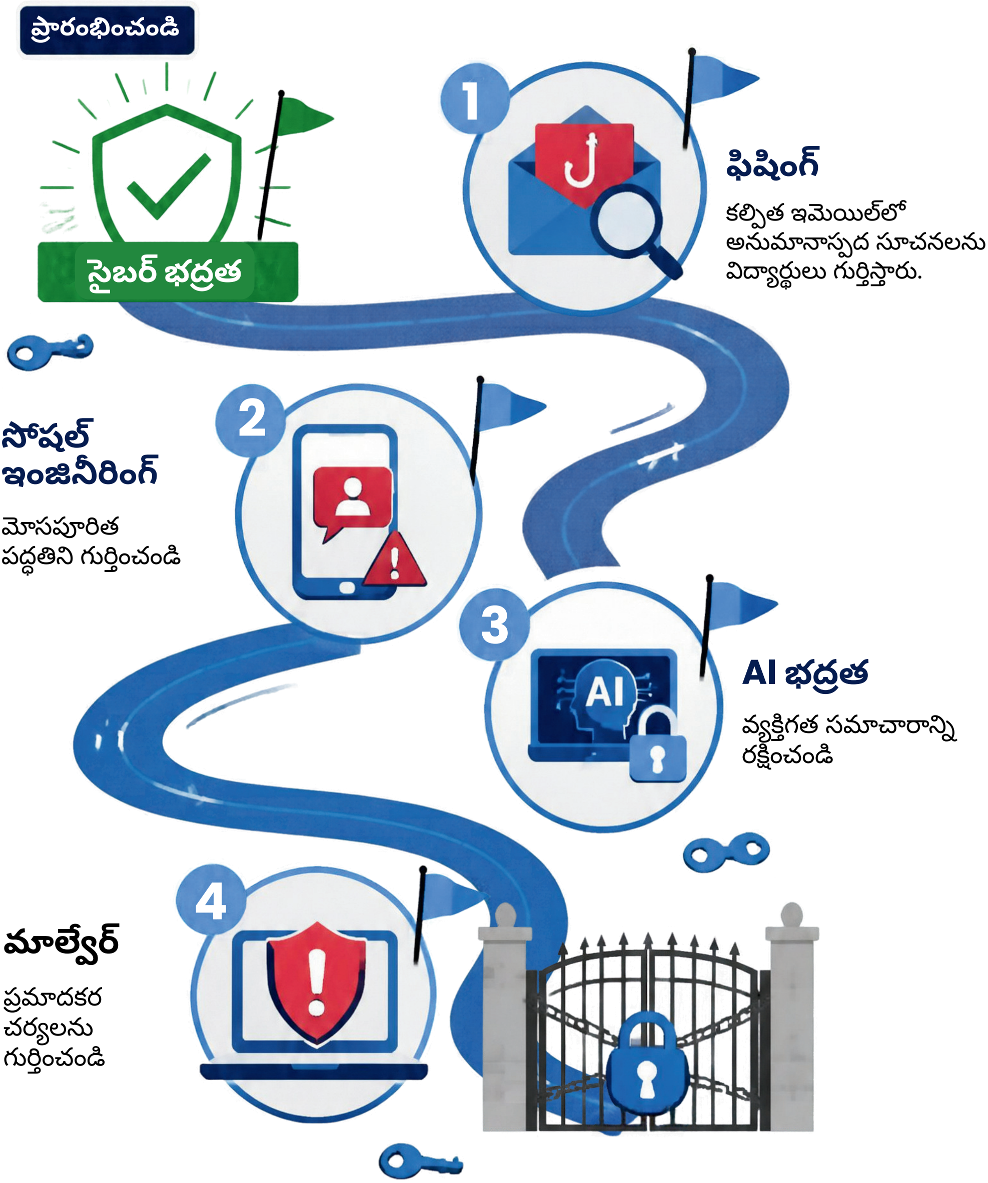
ముఖ్యమైన పాఠం

AI ఉపయోగకరంగా ఉండవచ్చు, కానీ విద్యార్థులు వ్యక్తిగత సమాచారాన్ని రక్షించాలి, ముఖ్యమైన సమాచారాన్ని ధృవీకరించాలి మరియు తాము రూపొందించి, పంచుకునే విషయాల పరిణామాలను పరిగణించాలి.

4. మాల్వేర్: “ఇది ఎలా ప్రవేశిస్తుంది?”



5. సైబర్ భద్రత ఎస్కేప్ రూమ్



certin Enhancing Cyber Security in India

మమ్మల్ని సంప్రదించండి

CERT-Inకు సైబర్ భద్రతా సంఘటనలను నివేదించడానికి:

- వెబ్‌సైట్‌ను సందర్శించండి: https://www.cert-in.org.in/
- ఇమెయిల్: incident@cert-in.org.in
- టోల్ ఫ్రీ ఫోన్: +91-1800-11-4949
- టోల్ ఫ్రీ ఫ్యాక్స్: +91-1800-11-6969

సమాచార విభాగం

- ఫోన్: +91-11-22902657

శిక్షణ మరియు అవగాహన కార్యక్రమాల్లో పాల్గొనడానికి, ఇమెయిల్ చేయండి:

training@cert-in.org.in

మమ్మల్ని అనుసరించండి

@IndianCERT

@cert_india

అవగాహన పుస్తికలు

https://www.cert-in.org.in/AwarenessBooklets.jsp

భద్రతా సాధనాలు

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

SCAN ME!