



Ministry of Electronics and
Information Technology
Government of India

certin 
Enhancing Cyber Security in India

சைபர் ஸ்மார்ட் வகுப்பறை

ஆசிரியர்களும்
மாணவர்களும்
கொண்ட சூழ்நிலை
அடிப்படையிலான
இணைய பாதுகாப்பு
வழிகாட்டி



முன்னிட்டு

தேசிய இணைய பாதுகாப்பு விழிப்புணர்வு மாதம்
(அக்டோபர் 2026)

"இணைய சுகாதார பண்பாட்டை உருவாக்குவோம்"
#CyberHygieneOurCulture



Information Security
Education & Awareness



Digital India
Power To Empower

साइबर स्वच्छता केंद्र

CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

உள்ளடக்க அட்டவணை

	முன்னுரை	3
1	சமூகப் பொறியியல்: “நம்பிக்கையா அல்லது ஏமாற்றமா?”	4
2	ஃபிஷிங்: “எச்சரிக்கை அறிகுறிகளை கண்டறியுங்கள்”	5
3	AI பாதுகாப்பு: “இதைக் குறித்து AI-யிடம் கேட்பீர்களா?”	6
4	மால்வேர்: “இது எவ்வாறு உள்ளே நுழைகிறது?”	7
5	இணையப் பாதுகாப்பு எஸ்கேப் ரூம்	8
	எங்களைத் தொடர்புகொள்ளுங்கள்	9



முன்னுரை

மாணவர்கள் ஆன்லைனில் கற்றல், தொடர்புகொள்வது, ஒத்துழைப்பது மற்றும் படைப்புகளை உருவாக்குவது போன்றவற்றில் அதிக நேரம் செலவிடுவதால், இணையப் பாதுகாப்பைப் புரிந்துகொள்வது அத்தியாவசியமான வாழ்க்கைத் திறனாக மாறியுள்ளது. அன்றாட டிஜிட்டல் அனுபவங்களில் இணைய அச்சுறுத்தல்கள் அதிகமாக உட்பொதிந்துள்ளன. அவை சந்தேகத்திற்கிடமான செய்தி, எதிர்பாராத உள்நுழைவு கோரிக்கை, தவறாக வழிநடத்தும் இணையதளம், தெரியாத இணைப்பு, ஏமாற்றும் குரல் அல்லது காணொளி, அல்லது தனிப்பட்ட தகவலுக்கான கோரிக்கை போன்ற வடிவங்களில் தோன்றலாம். இத்தகைய சூழ்நிலைகளை அடையாளம் காணவும், சற்று நின்று சிந்திக்கவும், சரிபார்க்கவும், தகவலறிந்த முடிவுகளை எடுக்கவும் மாணவர்களுக்கு அறிவை வழங்குவது, சிறு வயதிலிருந்தே பாதுகாப்பான மற்றும் பொறுப்பான டிஜிட்டல் பழக்கங்களை உருவாக்க உதவும்.

இந்திய கணினி அவசரநிலைப் பதிலளிப்பு குழுவின் (CERT-In) சைபர் ஸ்மார்ட் வகுப்பறை: ஆசிரியர்கள் மற்றும் மாணவர்களுக்கான சூழ்நிலை அடிப்படையிலான இணையப் பாதுகாப்பு வழிகாட்டி. வகுப்பறை விவாதங்கள், செயல்பாடுகள் மற்றும் ஊடாடும் கற்றலை நடத்துவதற்கு ஆசிரியர்கள் பயன்படுத்தக்கூடிய நடைமுறை மற்றும் எளிதில் தொடர்புபடுத்திக்கொள்ளக்கூடிய சூழ்நிலைகளை வழங்குகிறது. ஒவ்வொரு சூழ்நிலையும் சாத்தியமான அபாயங்களை அடையாளம் காணவும், விமர்சனமாக சிந்திக்கவும், சாத்தியமான பதில்களைப் பற்றி விவாதிக்கவும், எளிய இணையப் பாதுகாப்பு சிறந்த நடைமுறைகளைப் புரிந்துகொள்ளவும் மாணவர்களை ஊக்குவிக்கிறது. மாணவர்கள் தங்கள் அன்றாட வாழ்க்கையில் சந்திக்கக்கூடிய சூழ்நிலைகளுடன் இணையப் பாதுகாப்புக் கருத்துகளை இணைப்பதன் மூலம், இணைய விழிப்புணர்வை ஈர்க்கக்கூடியதாகவும், தொடர்புடையதாகவும், செயல்படுத்தக்கூடியதாகவும் மாற்றுவதுடன், பொறுப்பான டிஜிட்டல் குடியுரிமைப் பண்பாட்டையும் வளர்ப்பதே இந்த வழிகாட்டியின் நோக்கமாகும்.

இந்தக் கையேடு CERT-In தேசிய இணையப் பாதுகாப்பு விழிப்புணர்வு மாத நடவடிக்கைகளின் (அக்டோபர் 2026) ஒரு பகுதியாக வெளியிடப்பட்டுள்ளது. மாணவர்கள் மற்றும் கல்வியாளர்களிடையே இணையப் பாதுகாப்பு விழிப்புணர்வை வலுப்படுத்துவதே இதன் நோக்கமாகும். ஆன்லைன் பாதுகாப்பைப் பற்றிய அர்த்தமுள்ள உரையாடல்களை உருவாக்கவும், டிஜிட்டல் உலகில் தகவலறிந்த, பாதுகாப்பான மற்றும் பொறுப்பான தேர்வுகளைச் செய்ய மாணவர்களுக்கு அதிகாரமளிக்கவும் ஆசிரியர்களுக்கு ஆதரவளிப்பதே இதன் நோக்கம்.

1. சமூகப் பொறியியல்: “நம்பிக்கையா அல்லது ஏமாற்றமா?”



A

அதிகாரம்

நான் IT துறையிலிருந்து பேசுகிறேன்.

U

அவசரம்

உடனே செயல்படு.

R

வெகுமதி

இலவசப் பதிவிறக்கம்.

F

பரிச்சயம்

இவர் உங்கள் நண்பர்.

அறிகுறிகள்

1

பள்ளியின் IT துறையிலிருந்து அழைக்கிறேன் என்று கூறி, உங்கள் கடவுச்சொல்லைக் கேட்கும் ஒருவர்.

2

ஒருவர் உங்கள் நண்பர் என்று கூறுகிறார், ஆனால் புதிய கணக்கைப் பயன்படுத்தி அவசரமாகப் பணம் அனுப்புமாறு கேட்கிறார்.

3

உங்கள் உள்நுழைவு விவரங்களுக்கு மாற்றாக இலவச கேம் பதிவிறக்கத்தை வழங்கும் ஒருவர்.

4

ஒரு மாணவருக்கு, உடனடியாகச் செயல்படாவிட்டால் அவரது கணக்கு நீக்கப்படும் என்று கூறும் செய்தி வருகிறது.

முடிவு பாதை

● பெரும்பாலும் பாதுகாப்பானது

● சரிபார்ப்பு தேவை

● சாத்தியமான கையாளுதல்

முக்கியப் பாடம்:

தாக்குதலாளர்கள் மக்களைத் தங்கள் கட்டுப்பாட்டிற்குள் கொண்டு வர அவசரம், அதிகாரம், பயம், ஆர்வம், வெகுமதி அல்லது பரிச்சயம் ஆகியவற்றைப் பயன்படுத்தலாம்.

2.ஃபிஷிங்: “எச்சரிக்கை அறிகுறிகளை கண்டறியுங்கள்”

மாணவர்கள் நினைவில் கொள்ள வேண்டிய விதி:



நிறுத்து



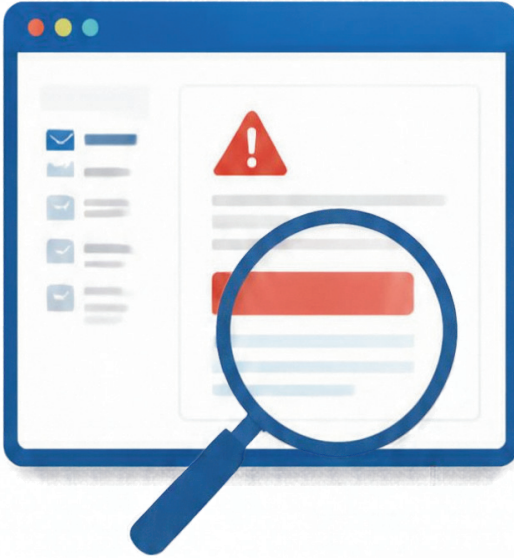
சரிபார்



உறுதிப்படுத்து



புகாரளி



பாதுகாப்
பானது



ஃபிஷிங்



சந்தேகத்திற்கிடமான
அனுப்புநர் முகவரிகள்



அவசரப்படுத்தும் அல்லது
மிரட்டும் மொழி



எதிர்பாராத இணைப்புக்
கோப்புகள்



கடவுச்சொற்கள் அல்லது
தனிப்பட்ட
தகவல்களுக்கான
கோரிக்கைகள்



சந்தேகத்திற்கிடமான
இணைப்புகள்



எழுத்துப்பிழைகள் /
இலக்கண
முரண்பாடுகள்



வழக்கத்திற்கு மாறான
பணம் செலுத்தும்
கோரிக்கைகள்



பொருந்தாத
இணையதள
முகவரிகள்

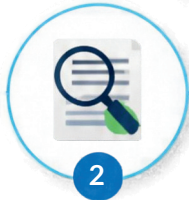


3. AI பாதுகாப்பு: “இதைப் பற்றி AI-யிடம் கேட்பீர்களா?”

மாணவர்களுக்கு கற்பிக்க வேண்டியவை:



தனிப்பட்ட தகவல்களைப் பாதுகாக்கவும்



முக்கியமான தகவல்களைச் சரிபார்க்கவும்



விளைவுகளைப் பரிசீலிக்கவும்



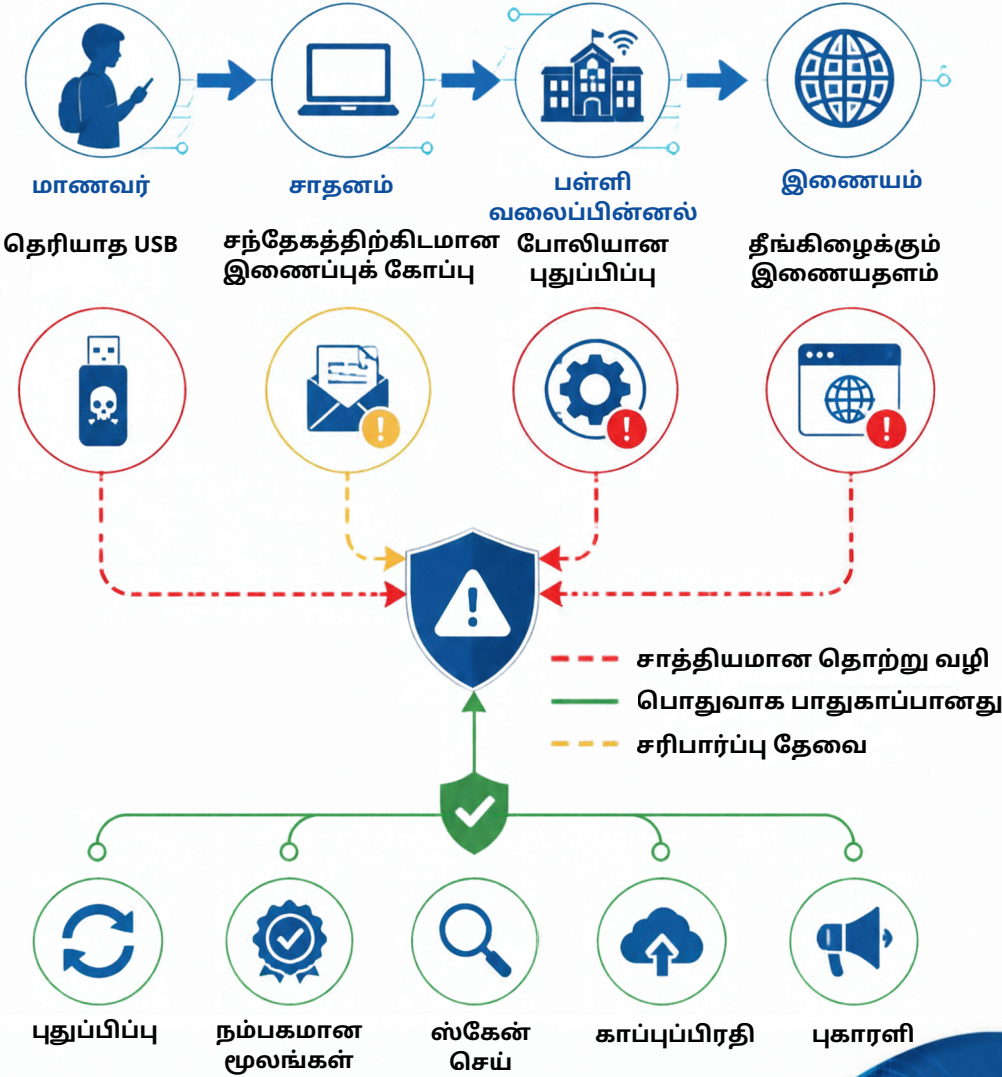
பொறுப்பான பயன்பாடு



முக்கியப் பாடம்

AI பயனுள்ளதாக இருக்கலாம்; ஆனால் மாணவர்கள் தனிப்பட்ட தகவல்களைப் பாதுகாக்கவும், முக்கியமான தகவல்களைச் சரிபார்க்கவும், தாங்கள் உருவாக்கிப் பகிரும் உள்ளடக்கத்தின் விளைவுகளைப் பரிசீலிக்கவும் வேண்டும்.

4. மால்வேர்: “இது எவ்வாறு உள்ளே நுழைகிறது?”



5. இணையப் பாதுகாப்பு எஸ்கேப் ரூம்

தொடங்கு

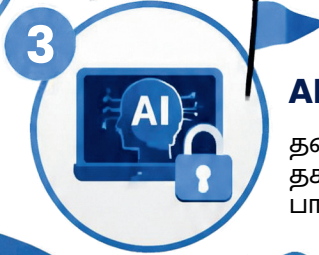


ஃபிஷிங்

கற்பனை
மின்னஞ்சலில் உள்ள
சந்தேகத்திற்கிடமான
குறிகளை
மாணவர்கள்
கண்டறிகின்றனர்.

சமூகப் பொறியியல்

கையாளுதலைக்
கண்டறியுங்கள்



AI பாதுகாப்பு

தனிப்பட்ட
தகவல்களைப்
பாதுகாக்கவும்

மால்வேர்

ஆபத்தான
செயல்களைக்
கண்டறியுங்கள்



எங்களைத் தொடர்புகொள்ளுங்கள்



**CERT-In-க்கு இணையப் பாதுகாப்பு
சம்பவங்களைப் புகாரளிக்க:**



தகவல் மையம்

இணையதளத்தைப் <https://www.cert-in.org.in/>
பார்வையிடவும்:
மின்னஞ்சல்: incident@cert-in.org.in

தொலை
பேசி: +91-11-22902657

கட்டணமில்லா தொலைபேசி: +91-1800-11-4949

கட்டணமில்லா தொலைநகல்: +91-1800-11-6969



**பயிற்சி மற்றும் விழிப்புணர்வு
அமர்வுகளில் பங்கேற்க, மின்னஞ்சல்
அனுப்பவும்:**

training@cert-in.org.in

**எங்களைப்
பின்தொடரவும்**



@IndianCERT



@cert_india

விழிப்புணர்வு கையேடுகள்

[https://www.cert-
in.org.in/AwarenessBooklets.jsp](https://www.cert-in.org.in/AwarenessBooklets.jsp)



பாதுகாப்புக் கருவிகள்

[https://www.csk.gov.in/security-
tools.html](https://www.csk.gov.in/security-tools.html)



**SCAN
ME!**

