Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

certin
Enhancing Cyber Security in India

CyberSmart Classroom

शिक्षकाणां छात्राणां च कृते\परिस्थितिनिष्ठा साइबर-सुरक्षा-मार्गदर्शिका



उपलक्ष्ये

राष्ट्रीय-साइबर-सुरक्षा-जागरूकता-मासः

(October 2026)

“साइबर-स्वच्छतायाः संस्कृतिं निर्मामः”

#CyberHygieneOurCulture

ISEA 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

विषयसूची

	प्रस्तावना	3
1	सामाजिक-अभियांत्रिकी: “विश्वासो वा छलः?”	4
2	फ़िशिङ्ग्: “सन्देहास्पद-संकेतान् चिनुत”	5
3	कृत्रिम-बुद्धिमत्ता-सुरक्षा: “किं त्वम् एतत् कृत्रिमबुद्धिमत्तायै पृच्छेः?”	6
4	दुष्ट-सॉफ्टवेयरः: “अयं कथम् अन्तः प्रविशति?”	7
5	साइबर-सुरक्षा-रहस्य-कक्षः	8
	अस्माभिः सम्पर्कं कुरुत	9



प्रस्तावना

यदा छात्राः अध्ययनं, संवादं, सहकार्यं तथा अन्तर्जाल-माध्यमेन सृजनं च कुर्वन्तः अधिकं समयं यापयन्ति, तदा साइबर-सुरक्षायाः ज्ञानं जीवनस्य अत्यावश्यकं कौशलं जातम्। साइबर-धमक्यः नित्यजीवनस्य डिजिटल-अनुभवेषु अधिकाधिकं अन्तर्निहिताः भवन्ति। ताः सन्देहास्पद-सन्देशरूपेण, अप्रत्याशित-प्रवेश-अनुरोधरूपेण, भ्रामक-जालपुटरूपेण, अज्ञात-सम्बन्धसूत्ररूपेण, कपटपूर्ण-स्वरस्य वा दृश्यस्य रूपेण, अथवा वैयक्तिक-सूचनायाः अनुरोधरूपेण प्रकटितुं शक्नुवन्ति। एतादृशीनां परिस्थितीनां परिचयं कर्तुं, क्षणं विरम्य सत्यापनं कर्तुं तथा सूचितनिर्णयान् स्वीकर्तुं छात्रान् समर्थयितुं, बाल्यादेव सुरक्षितान् उत्तरदायित्वपूर्णांश्च डिजिटल-अभ्यासान् विकसितुं साहाय्यं भवति।

इत्यस्य Indian Computer Emergency Response Team (CERT-In) इत्यस्य CyberSmart Classroom: Scenario Based Cybersecurity Guide for Teachers & Students इति मार्गदर्शिका अध्यापकेभ्यः व्यावहारिकान् छात्रजीवनस्य समीपस्थान् च प्रसङ्गान् प्रददाति, येषां माध्यमेन कक्षाचर्चाः, क्रियाकलापाः तथा परस्पर-सहभागितापूर्णम् अधिगमं च आयोजयितुं शक्यते। प्रत्येकः प्रसङ्गः छात्रान् सम्भावित-जोखिमान् चिन्तयितुं, आलोचनात्मकतया विचारयितुं, सम्भावित-प्रतिक्रियानां विषये चर्चां कर्तुं तथा सरलान् साइबर-सुरक्षा-सदाचारान् अवगन्तुं प्रेरयति। छात्राः स्वदैनन्दिनजीवने अनुभवेयुः इत्यादृशैः परिस्थितिभिः सह साइबर-सुरक्षायाः अवधारणानां सम्बन्धं स्थापयित्वा, एषा मार्गदर्शिका साइबर-जागरूकतां रोचकां, प्रासङ्गिकां, व्यवहारोपयोगिनीं च कर्तुं प्रयतते। साथमेव सा उत्तरदायित्वपूर्ण-डिजिटल-नागरिकत्वस्य संस्कृतिं वर्धयति।

इदं पुस्तिकं CERT-In National Cyber Security Awareness Month activities (October 2026) इत्यस्य भागरूपेण प्रकाशितम् अस्ति। अस्य उद्देशः छात्रेषु शिक्षकेषु च साइबर-सुरक्षा-जागरूकतां सुदृढीकर्तुम् अस्ति। अन्तर्जाल-सुरक्षायाः विषये सार्थक-सम्भाषणानि सृजितुं तथा डिजिटल-जगति सूचितान्, सुरक्षितान्, उत्तरदायित्वपूर्णान् च विकल्पान् स्वीकर्तुं छात्रान् समर्थयितुं एतत् पुस्तिकं अध्यापकानां साहाय्यार्थं निर्मितम् अस्ति।

1. सामाजिक-अभियांत्रिकी: "विश्वासो वा छलः?"



A **अधिकारिता**
अहं IT-विभागात् अस्मि।

U **तात्कालिकता**
तत्क्षणं कार्यं कुरु।

R **पुरस्कारः**
निःशुल्क-अवतरणम्।

F **परिचितता**
एषः तव मित्रम् अस्ति।

संकेताः

1 १. कश्चित् विद्यालयस्य IT-विभागात् आगतः इति कथयित्वा दूरभाषं करोति तथा तव कूटशब्दं पृच्छति।

2 २. कश्चित् त्वदीयः मित्रः इति कथयति, किन्तु नूतनं खातं प्रयुङ्क्ते तथा शीघ्रं धन-हस्तान्तरणं याचते।

3 ३. कश्चित् तव प्रवेश-विवरणानां विनिमये निःशुल्क-क्रीडायाः अवतरणं प्रस्तावयति।

4 ४. एकः छात्रः सन्देशं प्राप्नोति यत् यदि सः तत्क्षणं कार्यं न करिष्यति तर्हि तस्य खातं विलोपयिष्यते।

निर्णय-मार्गः

🟢 सम्भवतः सुरक्षितम्

🟡 सत्यापनम् आवश्यकम्

🔴 सम्भावित-प्रपञ्चनम्

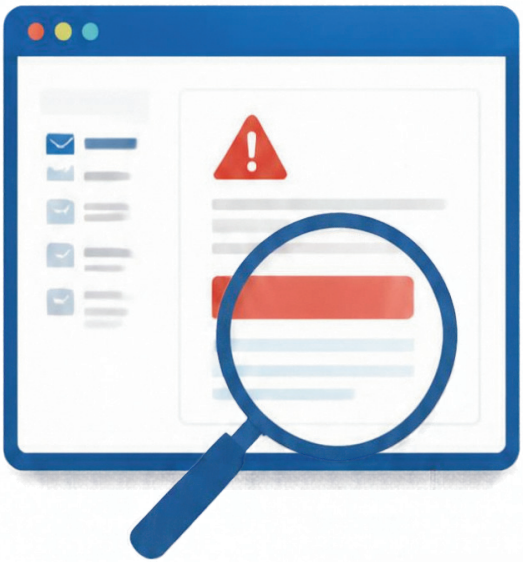
मुख्यं शिक्षणम्:

आक्रमणकर्तारः जनानां प्रभावनाय तात्कालिकतायाः, अधिकारितायाः, भयस्य, जिज्ञासायाः, पुरस्कारस्य वा परिचिततायाः उपयोगं कर्तुं शक्नुवन्ति।

2. फ़िशिङ्ग्: “सन्देहास्पद-संकेतान् चिनुत”

छात्रैः स्मर्तव्यः नियमः:

विरमतु → परीक्षताम् → सत्यापयतु → निवेदयतु



- सन्देहास्पद-प्रेषक-पत्तनानि
- तात्कालिकं वा धमकीपूर्णं वा भाषणम्
- अप्रत्याशित-संलग्नकानि
- कूटशब्दानां वा वैयक्तिक-सूचनायाः वा अनुरोधाः
- सन्देहास्पदानि सम्बन्धसूत्राणि
- वर्तनी-व्याकरणयोः असङ्गतयः
- असामान्य-भुगतान-अनुरोधाः
- असङ्गत-जालपुट-पत्तनानि



सुरक्षितम्



फ़िशिङ्ग्

3. कृत्रिम-बुद्धिमत्ता-सुरक्षा: “किं त्वम् एतत् कृत्रिम-बुद्धिमत्तायै पृच्छे:?”

छात्रान् एतेषु विषये शिक्षयन्तु:

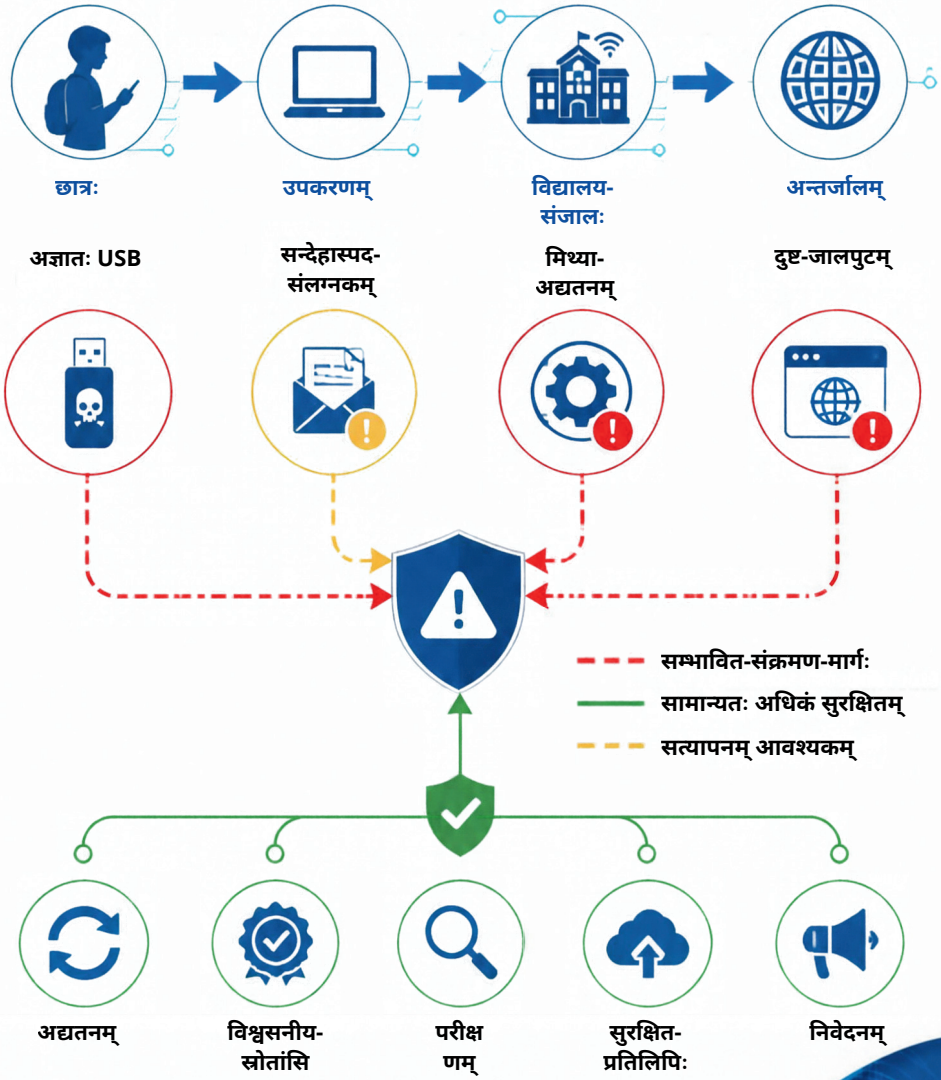


1. वैयक्तिक-सूचनां रक्षन्तु
2. महत्त्वपूर्ण-सूचनायाः सत्यापनं कुर्वन्तु
3. परिणामान् विचारयन्तु
4. उत्तरदायित्वपूर्णः उपयोगः

मुख्यं शिक्षणम्

कृत्रिम-बुद्धिमत्ता उपयोगिनी भवितुं शक्नोति, किन्तु छात्रैः वैयक्तिक-सूचना रक्षणीया, महत्त्वपूर्ण-सूचनायाः सत्यापनं करणीयम्, तथा च यत् ते जनयन्ति साझां कुर्वन्ति वा तस्य परिणामाः विचारणीयाः।

4. दुष्ट-सॉफ्टवेयरः: “अयं कथं अन्तः प्रविशति?”



5. साइबर-सुरक्षा-रहस्य-कक्षः



अस्माभिः

साइबर-सुरक्षा-घटनानां CERT-In प्रति निवेदनायः

- **जालपुटं पश्यन्तु:** https://www.cert-in.org.in/
- **ईमेल्:** incident@cert-in.org.in
- **शुल्करहित-दूरभाषः:** +91-1800-11-4949
- **शुल्करहित-फैक्स्:** +91-1800-11-6969

सूचना-कक्षः

- **दूरभाषः:** +91-11-22902657

प्रशिक्षण-जागरूकता-सत्रेषु भागं ग्रहीतुं ईमेल् प्रेषयन्तु:
training@cert-in.org.in

अस्मान् अनुसरन्तु

@IndianCERT

@cert_india

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

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

SCAN ME!