Ministry of Electronics and
Information Technology
Government of India
सत्यमेव जयते

certin
Enhancing Cyber Security in India

साइबरस्मार्ट कक्षा

शिक्षकों एवं विद्यार्थियों के लिए परिदृश्य-आधारित साइबर सुरक्षा मार्गदर्शिका

राष्ट्रीय साइबर सुरक्षा जागरूकता माह
(अक्टूबर 2026)
के अवसर पर
"साइबर स्वच्छता की संस्कृति बनाएं"
#CyberHygieneOurCulture

ISEA
Information Security
Education & Awareness

Digital India
Power To Empower

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

विषय-सूची

प्रस्तावना 3
1 सोशल इंजीनियरिंग: “भरोसा या चाल?” 4
2 फ़िशिंग: "चेतावनी संकेतों को पहचानें 5
3 एआई सुरक्षा: “क्या आप एआई से यह पूछेंगे?” 6
4 मैलवेयर: “यह अंदर कैसे आता है?” 7
5 साइबर सुरक्षा चुनौती कक्ष 8
हमसे संपर्क करें 9

भूमिका

जैसे-जैसे विद्यार्थी ऑनलाइन सीखने, संवाद करने, सहयोग करने और रचनात्मक कार्य करने में अधिक समय बिताते हैं, साइबर सुरक्षा को समझना जीवन का एक आवश्यक कौशल बन गया है। साइबर खतरे रोज़मर्रा के डिजिटल अनुभवों में तेजी से शामिल हो रहे हैं और संदिग्ध संदेश, अनपेक्षित लॉगिन अनुरोध, भ्रामक वेबसाइट, अनजान लिंक, धोखाधड़ी वाली आवाज़ या वीडियो, अथवा व्यक्तिगत जानकारी के अनुरोध के रूप में सामने आ सकते हैं। विद्यार्थियों को इन स्थितियों को पहचानने, रुककर सत्यापन करने और सोच-समझकर निर्णय लेने का ज्ञान देने से कम उम्र से ही सुरक्षित और जिम्मेदार डिजिटल आदतें विकसित करने में सहायता मिल सकती है।

भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (CERT-In) की साइबरस्मार्ट कक्षा: शिक्षकों और विद्यार्थियों के लिए परिदृश्य-आधारित साइबर सुरक्षा मार्गदर्शिका शिक्षकों को ऐसे व्यावहारिक और सरल परिदृश्य प्रदान करती है, जिनका उपयोग कक्षा में चर्चा, गतिविधियों और संवादात्मक सिखाने के लिए किया जा सकता है। प्रत्येक परिदृश्य विद्यार्थियों को संभावित जोखिम पहचानने, आलोचनात्मक ढंग से सोचने, संभावित प्रतिक्रियाओं पर चर्चा करने और साइबर सुरक्षा की सरल सर्वोत्तम पद्धतियों को समझने के लिए प्रेरित करता है। साइबर सुरक्षा की अवधारणाओं को उन परिस्थितियों से जोड़कर, जिनका सामना विद्यार्थी अपने दैनिक जीवन में कर सकते हैं, यह मार्गदर्शिका साइबर जागरूकता को रोचक, प्रासंगिक और उपयोगी बनाने के साथ जिम्मेदार डिजिटल नागरिकता की संस्कृति विकसित करने का प्रयास करती है।

यह पुस्तिका CERT-In के राष्ट्रीय साइबर सुरक्षा जागरूकता माह (अक्टूबर 2026) की गतिविधियों के अंतर्गत प्रकाशित की गई है। इसका उद्देश्य विद्यार्थियों और शिक्षकों के बीच साइबर सुरक्षा जागरूकता को मजबूत करना है। यह शिक्षकों को ऑनलाइन सुरक्षा पर सार्थक संवाद शुरू करने और विद्यार्थियों को डिजिटल दुनिया में सोच-समझकर, सुरक्षित तथा जिम्मेदारीपूर्ण विकल्प चुनने के लिए सशक्त बनाने में सहायता देने के लिए तैयार की गई है।

1. सोशल इंजीनियरिंग: “भरोसा या चाल?”

रुकें • जाँचें • सत्यापित करें

प्र **प्राधिकार**
मैं आईटी विभाग से हूँ।

ता **तात्कालिकता**
तुरंत कार्रवाई करें।

पु **पुरस्कार**
मुफ़्त डाउनलोड।

परि **परिचितता**
यह आपका मित्र है।

संकेत

1 कोई व्यक्ति स्कूल के आईटी विभाग से होने का दावा करके आपका पासवर्ड माँगता है।

2 एक व्यक्ति कहता है कि वह आपका मित्र है, लेकिन नए खाते का उपयोग कर रहा है और तुरंत पैसे भेजने को कहता है।

3 कोई व्यक्ति आपके लॉगिन विवरण के बदले मुफ़्त गेम डाउनलोड देने की पेशकश करता है।

4 एक विद्यार्थी को संदेश मिलता है कि तुरंत कार्रवाई न करने पर उसका खाता हटा दिया जाएगा।

निर्णय प्रक्रिया

🟢 संभवतः सुरक्षित

🟡 सत्यापन आवश्यक

🔴 संभावित हेरफेर

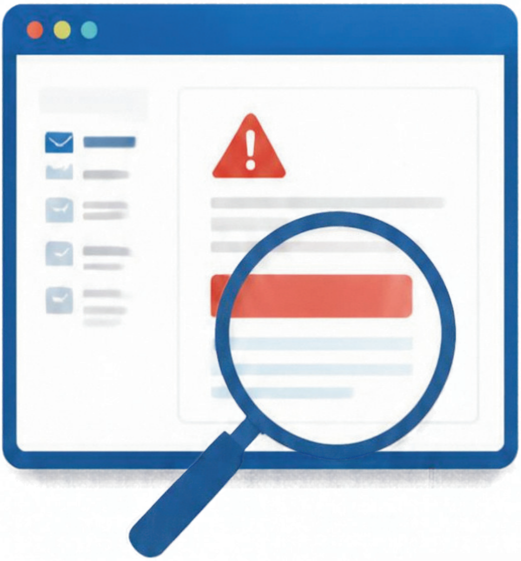
मुख्य सीख:

साइबर हमलावर लोगों को प्रभावित या भ्रमित करने के लिए जल्द कार्रवाई का दबाव, किसी प्राधिकरण का हवाला, डर, जिज्ञासा, इनाम का लालच या परिचित व्यक्ति/संगठन होने का विश्वास पैदा करने जैसी रणनीतियों का उपयोग कर सकते हैं।

2. फ़िशिंग: "चेतावनी संकेतों को पहचानें

विद्यार्थियों को याद रखने का नियम:

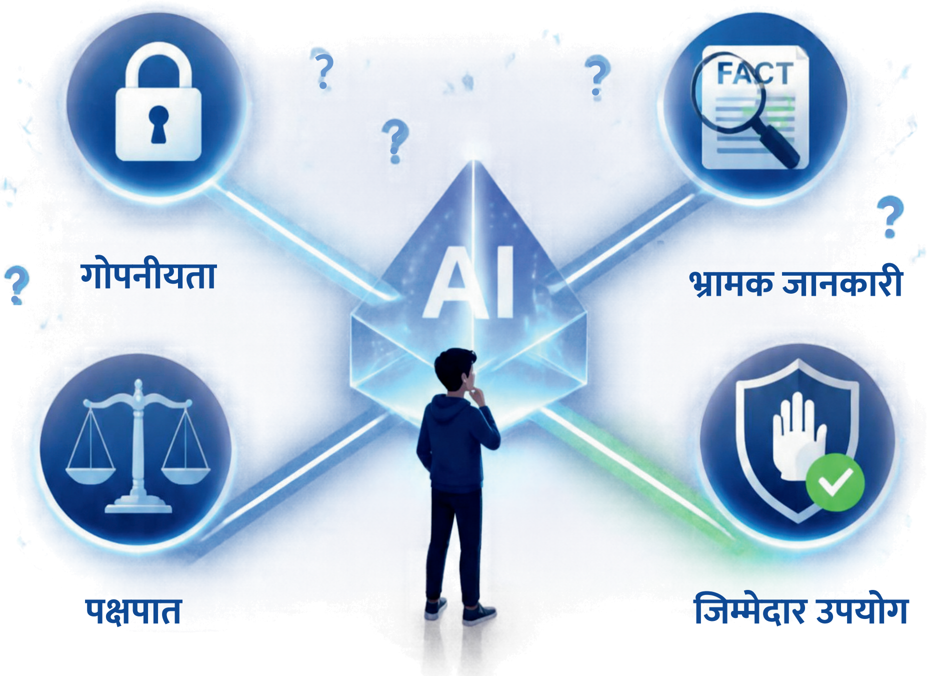
रुकें → जाँचें → सत्यापित करें → रिपोर्ट करें



- संदिग्ध प्रेषक के ईमेल पते
- तात्कालिक या धमकी भरी भाषा
- अप्रत्याशित संलग्न फ़ाइलें
- पासवर्ड या व्यक्तिगत जानकारी माँगना
- संदिग्ध लिंक
- वर्तनी या व्याकरण की असंगतियाँ
- असामान्य भुगतान अनुरोध
- मेल न खाने वाले वेबसाइट पते

3. एआई सुरक्षा: “क्या आप एआई से यह पूछेंगे?”

विद्यार्थियों को सिखाएँ:

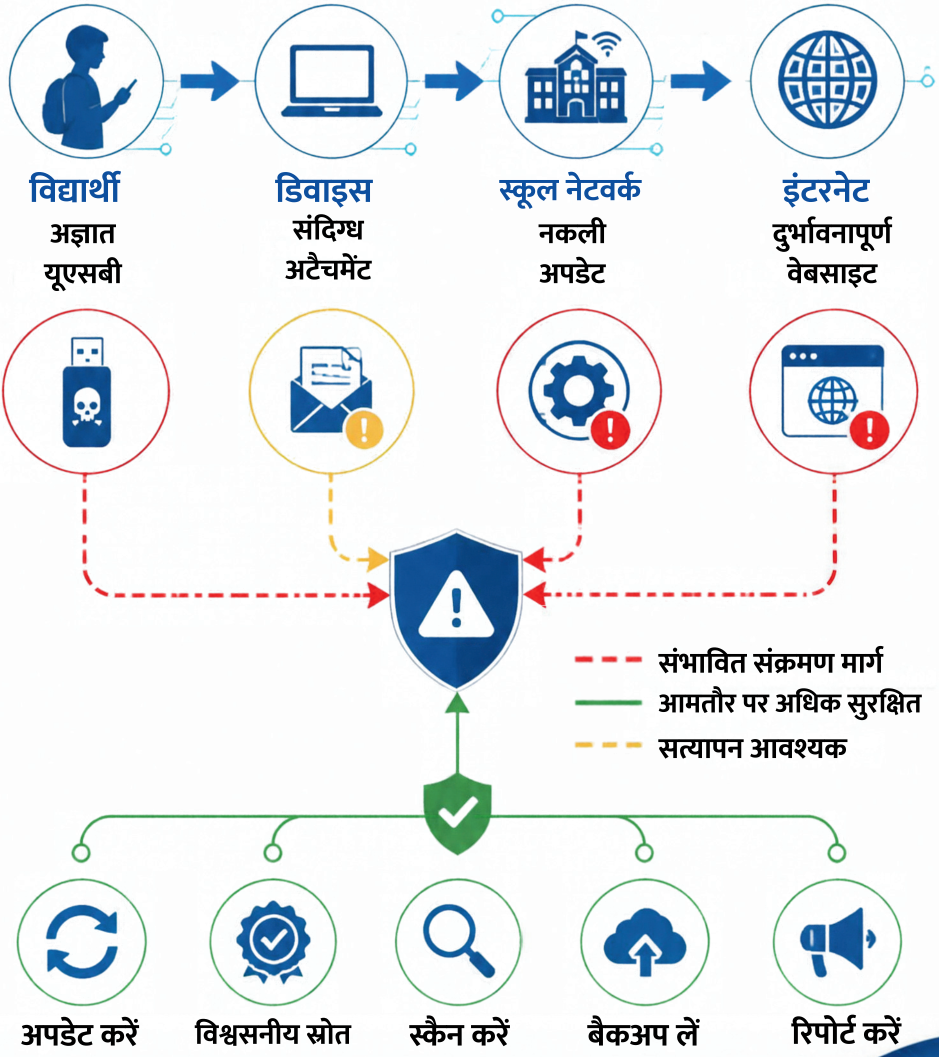

गोपनीयता
FACT
भ्रामक जानकारी
AI
पक्षपात
जिम्मेदार उपयोग

1. व्यक्तिगत जानकारी की सुरक्षा करें
2. महत्वपूर्ण जानकारी सत्यापित करें
3. परिणामों पर विचार करें
4. जिम्मेदार उपयोग

मुख्य सीख

एआई उपयोगी हो सकता है, लेकिन विद्यार्थियों को व्यक्तिगत जानकारी की सुरक्षा करनी चाहिए, महत्वपूर्ण जानकारी सत्यापित करनी चाहिए और वे जो सामग्री बनाते व साझा करते हैं, उसके परिणामों पर विचार करना चाहिए।

4. मैलवेयर: “यह अंदर कैसे आता है?”



विद्यार्थी
अज्ञात यूएसबी

डिवाइस
संदिग्ध अटैचमेंट

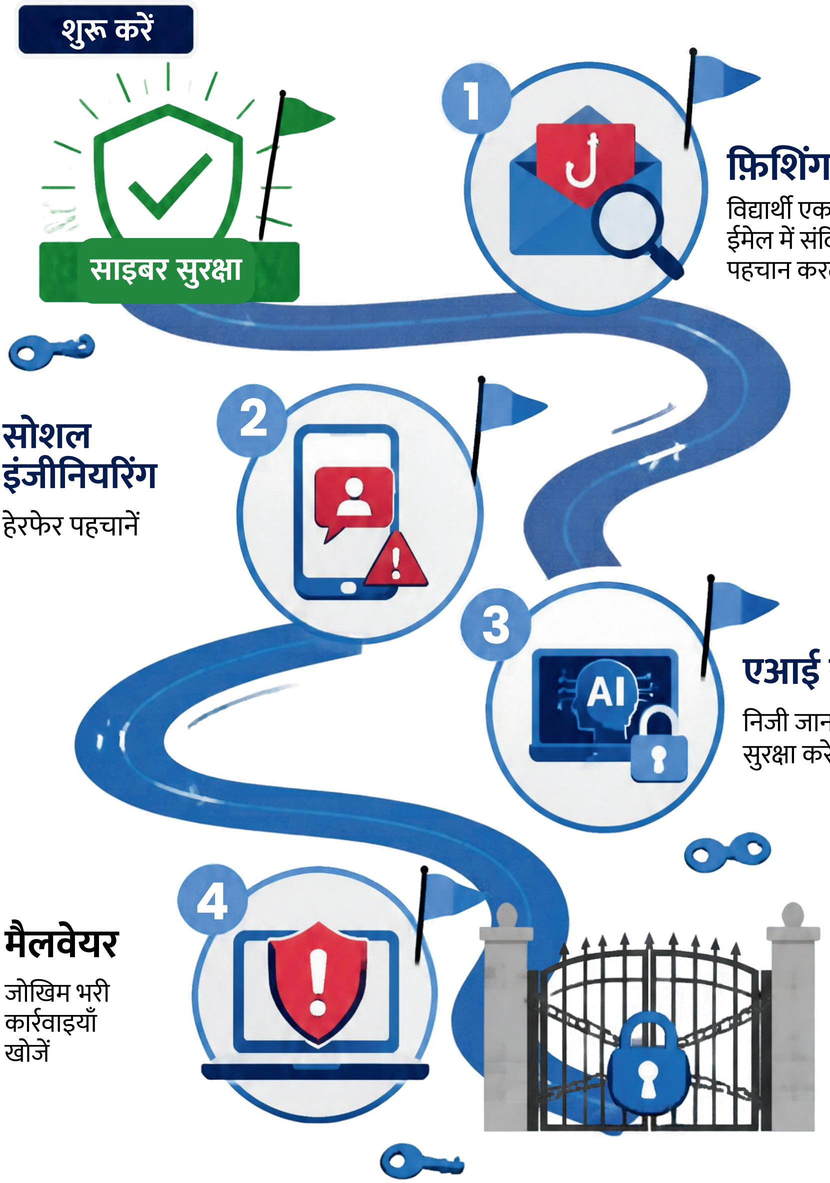
स्कूल नेटवर्क
नकली अपडेट

इंटरनेट
दुर्भावनापूर्ण वेबसाइट

🟥 - - - संभावित संक्रमण मार्ग
🟩 —— आमतौर पर अधिक सुरक्षित
🟨 - - - सत्यापन आवश्यक

अपडेट करें
विश्वसनीय स्रोत
स्कैन करें
बैकअप लें
रिपोर्ट करें

5. साइबर सुरक्षा चुनौती कक्ष


शुरू करें
साइबर सुरक्षा
1
2
3
AI
4

फ़िशिंग

विद्यार्थी एक काल्पनिक ईमेल में संदिग्ध संकेतों की पहचान करते हैं।

सोशल इंजीनियरिंग

हेरफेर पहचानें

एआई सुरक्षा

निजी जानकारी की सुरक्षा करें

मैलवेयर

जोखिम भरी कार्रवाइयाँ खोजें

हमसे संपर्क करें

CERT-In को साइबर सुरक्षा घटनाओं की रिपोर्ट करने के लिए:

वेबसाइट पर जाएँ: https://www.cert-in.org.in/

ईमेल: incident@cert-in.org.in

टोल-फ्री फ़ोन: +91-1800-11-4949

टोल-फ्री फ़ैक्स: +91-1800-11-6969

सूचना डेस्क

फ़ोन: +91-11-22902657

प्रशिक्षण और जागरूकता सत्रों में भाग लेने के लिए ईमेल करें:

training@cert-in.org.in

हमें यहाँ फ़ॉलो करें

@IndianCERT

@cert_india

जागरूकता पुस्तिकाएँ

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

सुरक्षा उपकरण

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

SCAN ME!