Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

certin
Enhancing Cyber Security in India

साइबर स्मार्ट कक्षा

शिक्षक तथा विद्यार्थीहरूका लागि परिस्थिति-आधारित साइबर सुरक्षा मार्गदर्शिका



अवसरमा

राष्ट्रिय साइबर सुरक्षा सचेतना महिना

(अक्टोबर २०२६)

"साइबर स्वच्छताको संस्कृति निर्माण गरौं"

#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 इन्जिनियरिङः “विश्वास कि छल?”	4
2	फिसिङः “खतराका संकेतहरू पहिचान गर्नुहोस्”	5
3	एआई सुरक्षा: “के तपाईं एआईलाई यस्तो सोध्नुहुन्छ?”	6
4	मालवेयर: “यो भित्र कसरी पस्छ?”	7
5	साइबर सुरक्षा एस्केप रुम	8
	सम्पर्क गर्नुहोस्	9



प्रस्तावना

विद्यार्थीहरूले अनलाइन सिकाइ, सञ्चार, सहकार्य र सिर्जनामा बढी समय बिताउँदै जाँदा साइबर सुरक्षाको बुझाइ जीवनको अनिवार्य सीप बनेको छ। साइबर खतरा दैनिक डिजिटल अनुभवहरूमा झन् बढ्दै मिसिएका छन् र शंकास्पद सन्देश, अनपेक्षित लगइन अनुरोध, भ्रामक वेबसाइट, अपरिचित लिङ्क, छलपूर्ण आवाज वा भिडियो, अथवा व्यक्तिगत जानकारी माग्ने अनुरोधका रूपमा देखा पर्न सक्छन्। यस्ता परिस्थितिहरू पहिचान गर्न, रोकिएर जाँच गर्न, प्रमाणित गर्न र सूचित निर्णय लिन सक्ने ज्ञानले विद्यार्थीहरूमा सानै उमेरदेखि सुरक्षित र जिम्मेवार डिजिटल बानी विकास गर्न मद्दत गर्छ।

भारतीय कम्प्युटर आपत्कालीन प्रतिक्रिया टोली (CERT-In) को CyberSmart Classroom: शिक्षक तथा विद्यार्थीहरूका लागि परिस्थिति-आधारित साइबर सुरक्षा मार्गदर्शिकाले शिक्षकहरूलाई कक्षागत छलफल, गतिविधि र अन्तरक्रियात्मक सिकाइ सञ्चालन गर्न प्रयोग गर्न सकिने व्यावहारिक तथा सहज परिस्थितिहरू प्रदान गर्छ। प्रत्येक परिस्थितिले विद्यार्थीहरूलाई सम्भावित जोखिम पहिचान गर्न, आलोचनात्मक रूपमा सोच्न, सम्भावित प्रतिक्रियाबारे छलफल गर्न र साइबर सुरक्षाका सरल उत्तम अभ्यासहरू बुझ्न प्रोत्साहित गर्छ। विद्यार्थीहरूले दैनिक जीवनमा सामना गर्न सक्ने परिस्थितिसँग साइबर सुरक्षा अवधारणाहरू जोडेर यस मार्गदर्शिकाले साइबर सचेतनालाई रोचक, सान्दर्भिक र व्यवहारमा लागू गर्न सकिने बनाउने तथा जिम्मेवार डिजिटल नागरिकताको संस्कृति विकास गर्ने उद्देश्य राख्छ।

यो पुस्तिका CERT-In राष्ट्रिय साइबर सुरक्षा सचेतना महिना (अक्टोबर २०२६) का गतिविधिहरूअन्तर्गत विद्यार्थी र शिक्षकमाझ साइबर सुरक्षा सचेतना सुदृढ गर्ने उद्देश्यले प्रकाशित गरिएको हो। यसले शिक्षकहरूलाई अनलाइन सुरक्षाबारे अर्थपूर्ण संवाद सिर्जना गर्न र विद्यार्थीहरूलाई डिजिटल संसारमा सूचित, सुरक्षित तथा जिम्मेवार छनोट गर्न सक्षम बनाउन सहयोग गर्ने उद्देश्य राख्छ।

1. सामाजिक इन्जिनियरिङः "विश्वास कि छल?"



A **अधिकार**
म आईटी विभागबाट हुँ।

U **अत्यावश्यकता**
तुरुन्तै कार्य गर्नुहोस्।

R **पुरस्कार**
निःशुल्क डाउनलोड।

F **परिचितपन**
यो तपाईंको साथी हो।

संकेतहरू

1. कसैले विद्यालयको आईटी विभागबाट भएको दाबी गर्दै फोन गर्छ र तपाईंको पासवर्ड माग्छ।
2. एक व्यक्तिले आफू तपाईंको साथी भएको बताउँछ, तर नयाँ खाता प्रयोग गरिरहेको हुन्छ र तुरुन्तै पैसा पठाउन भन्छ।
3. कसैले तपाईंको लगइन विवरणको बदलामा निःशुल्क गेम डाउनलोड दिने प्रस्ताव गर्छ।
4. एक विद्यार्थीले तुरुन्तै कार्य नगरे आफ्नो खाता मेटिनेछ भन्ने सन्देश प्राप्त गर्छ।

निर्णय मार्ग

🟢 सम्भवतः सुरक्षित | 🟡 प्रमाणीकरण आवश्यक | 🔴 सम्भावित हेरफेर

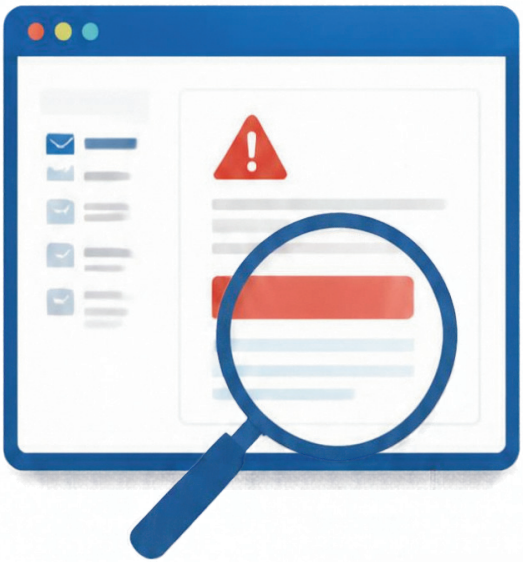
मुख्य सिकाइः

आक्रमणकारीहरूले मानिसहरूलाई प्रभावित पार्न अत्यावश्यकता, अधिकार, डर, जिज्ञासा, पुरस्कार वा परिचितपनको प्रयोग गर्न सक्छन्।

2. फिसिङः "खतराका संकेतहरू पहिचान गर्नुहोस्"

विद्यार्थीहरूले सम्झनुपर्ने नियमः

रोक्नुहोस् → जाँच्नुहोस् → प्रमाणित गर्नुहोस् → रिपोर्ट गर्नुहोस्



- शंकास्पद प्रेषक ठेगानाहरू
- अत्यावश्यक वा धम्कीपूर्ण भाषा
- अनपेक्षित संलग्न फाइलहरू
- पासवर्ड वा व्यक्तिगत जानकारीका अनुरोधहरू
- शंकास्पद लिङ्कहरू
- हिज्जे/व्याकरणका असंगतिहरू
- असामान्य भुक्तानीका अनुरोधहरू
- नमिल्दा वेबसाइट ठेगानाहरू



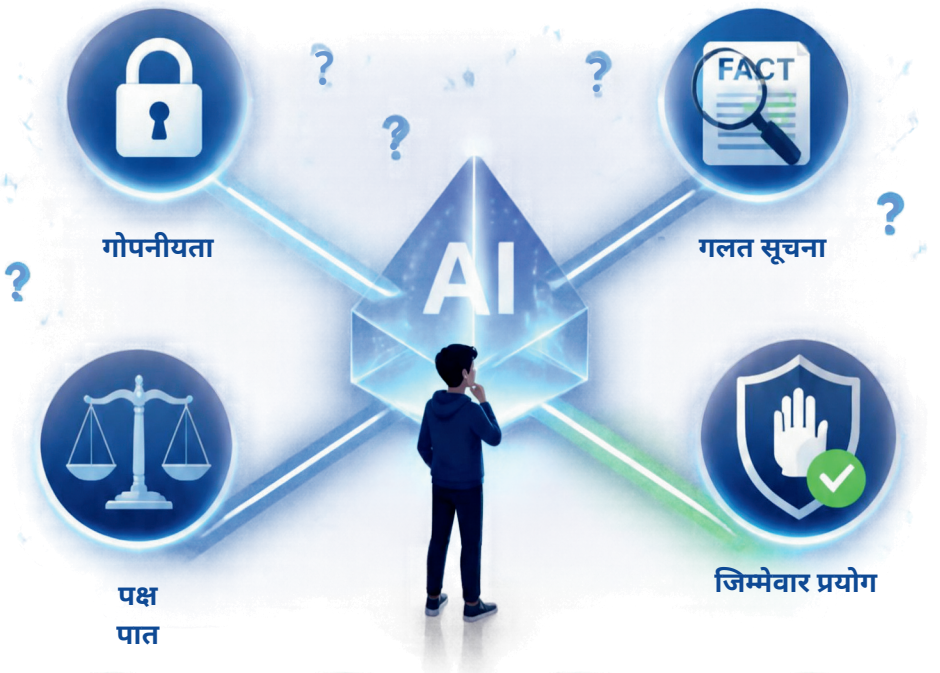
सुरक्षित



फिसिङ

3. एआई सुरक्षा: “के तपाईं एआईलाई यस्तो सोध्नुहुन्छ?”

विद्यार्थीहरूलाई यी विषयमा सिकाउनुहोस्:

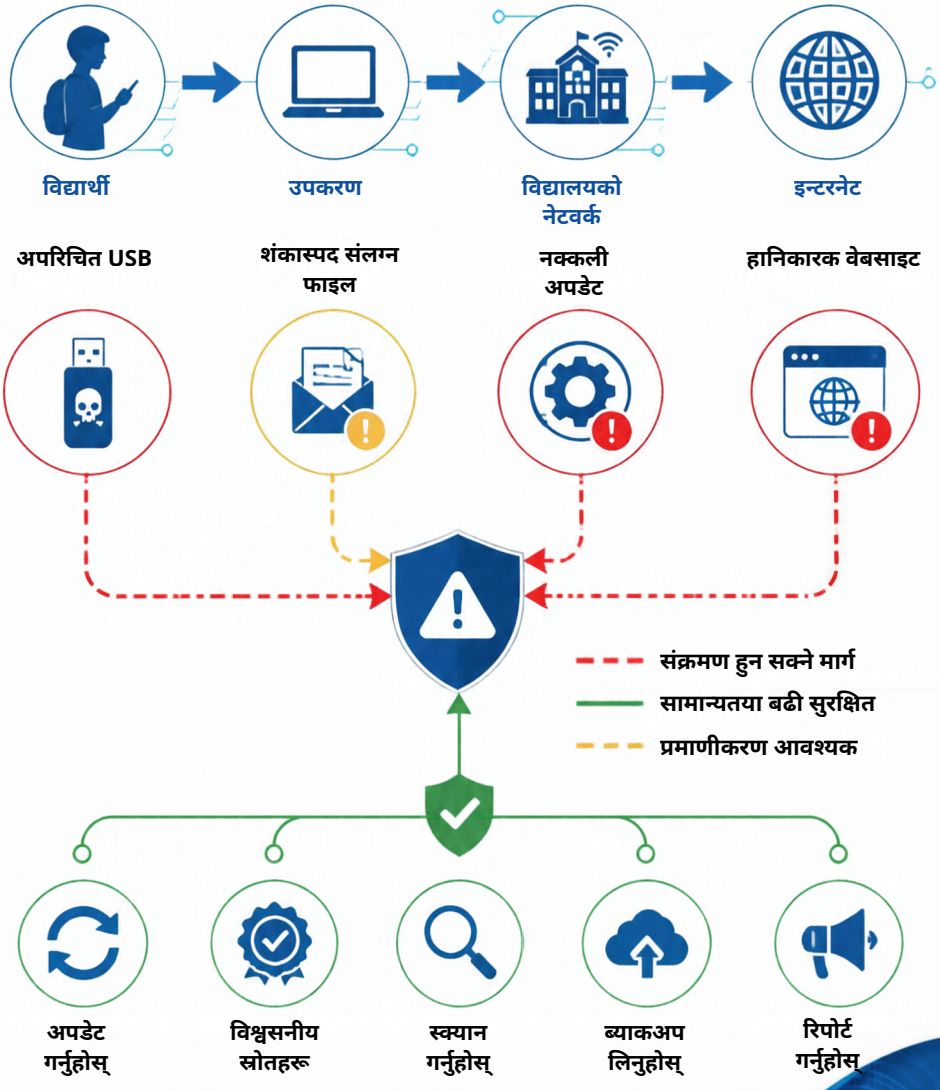


1. व्यक्तिगत जानकारी सुरक्षित राख्नुहोस्
2. महत्त्वपूर्ण जानकारी प्रमाणित गर्नुहोस्
3. परिणामहरूबारे विचार गर्नुहोस्
4. जिम्मेवार प्रयोग

मुख्य सिकाइ

एआई उपयोगी हुन सक्छ, तर विद्यार्थीहरूले व्यक्तिगत जानकारी सुरक्षित राख्नुपर्छ, महत्त्वपूर्ण जानकारी प्रमाणित गर्नुपर्छ, र आफूले सिर्जना तथा साझा गर्ने सामग्रीका परिणामहरूबारे विचार गर्नुपर्छ।

4. मालवेयर: “यो भित्र कसरी पस्छ?”



5. साइबर सुरक्षा एस्केप रुम



सम्पर्क

CERT-In मा साइबर सुरक्षा घटनाहरू रिपोर्ट गर्न:

- **वेबसाइटमा जानुहोस्:** https://www.cert-in.org.in/
- **इमेल:** incident@cert-in.org.in
- **टोल-फ्री फोन:** +91-1800-11-4949
- **टोल-फ्री फ्याक्स:** +91-1800-11-6969

सूचना डेस्क

- **फोन:** +91-11-22902657

प्रशिक्षण तथा सचेतना सत्रहरूमा सहभागी हुन इमेल गर्नुहोस्:
training@cert-in.org.in

हामीलाई यहाँ फलो गर्नुहोस्

@IndianCERT

@cert_india

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

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

SCAN ME!