Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

certin
Enhancing Cyber Security in India

CyberSmart
वर्गखोली

शिक्षक आणि विद्यार्थ्यांसाठी परिस्थिती-आधारित सायबर सुरक्षा मार्गदर्शक



निमित्ताने

राष्ट्रीय सायबर सुरक्षा जागरूकता महिना

(ऑक्टोबर २०२६)

"सायबर स्वच्छतेची संस्कृती निर्माण करूया"

#CyberHygieneOurCulture

ISEA Information Security Education & Awareness

Digital India Power To Empower

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

certin
Enhancing Cyber Security in India

अनुक्रमणिका

	प्रस्तावना	3
1	सामाजिक अभियांत्रिकी: "विश्वास की फसवणूक?"	4
2	फिशिंग: "धोक्याची चिन्हे ओळखा"	5
3	एआय सुरक्षितता: "तुम्ही हे एआयला विचाराल का?"	6
4	मालवेअर: "ते आत कसे शिरते?"	7
5	सायबर सुरक्षा एस्केप रूम	8
	संपर्क करा	9



प्रस्तावना

विद्यार्थी ऑनलाइन शिकण्यात, संवाद साधण्यात, सहकार्य करण्यात आणि निर्मिती करण्यात अधिक वेळ घालवत असल्याने, सायबर सुरक्षा समजून घेणे हे जीवनातील एक आवश्यक कौशल्य बनले आहे. सायबर धोके दैनंदिन डिजिटल अनुभवांमध्ये वाढत्या प्रमाणात आढळतात आणि ते संशयास्पद संदेश, अनपेक्षित लॉगिन विनंती, दिशाभूल करणारी वेबसाइट, अपरिचित दुवा, फसवा आवाज किंवा व्हिडिओ किंवा वैयक्तिक माहितीची मागणी अशा स्वरूपात दिसू शकतात. या परिस्थिती ओळखणे, थांबणे, पडताळणी करणे आणि माहितीपूर्ण निर्णय घेणे यासाठी विद्यार्थ्यांना ज्ञान देणे, लहान वयापासून सुरक्षित आणि जबाबदार डिजिटल सवयी विकसित करण्यास मदत करू शकते.

भारतीय संगणक आपत्कालीन प्रतिसाद संघटनेचा (CERT-In) CyberSmart वर्गखोली: शिक्षक आणि विद्यार्थ्यांसाठी परिस्थिती-आधारित सायबर सुरक्षा मार्गदर्शक, वर्गातील चर्चा, उपक्रम आणि परस्परसंवादी शिक्षणासाठी वापरता येतील अशा व्यावहारिक आणि विद्यार्थ्यांना परिचित वाटणाऱ्या परिस्थिती शिक्षकांना उपलब्ध करून देतो. प्रत्येक परिस्थिती विद्यार्थ्यांना संभाव्य धोके ओळखण्यास, चिकित्सक विचार करण्यास, संभाव्य प्रतिसादांवर चर्चा करण्यास आणि सायबर सुरक्षेच्या सोप्या सर्वोत्तम पद्धती समजून घेण्यास प्रोत्साहित करते. विद्यार्थ्यांना त्यांच्या दैनंदिन जीवनात येऊ शकणाऱ्या परिस्थितींशी सायबर सुरक्षा संकल्पना जोडून, जबाबदार डिजिटल नागरिकत्वाची संस्कृती वाढवताना सायबर जागरूकता मनोरंजक, उपयुक्त आणि कृतीयोग्य बनवणे हा या मार्गदर्शकाचा उद्देश आहे.

ही पुस्तिका CERT-In राष्ट्रीय सायबर सुरक्षा जागरूकता महिना उपक्रमांचा (ऑक्टोबर २०२६) एक भाग म्हणून प्रकाशित करण्यात आली आहे. विद्यार्थ्यांमध्ये आणि शिक्षकांमध्ये सायबर सुरक्षा जागरूकता बळकट करणे हा यामागील उद्देश आहे. ऑनलाइन सुरक्षिततेभोवती अर्थपूर्ण संवाद निर्माण करण्यास आणि डिजिटल जगात माहितीपूर्ण, सुरक्षित व जबाबदार निवडी करण्यासाठी विद्यार्थ्यांना सक्षम करण्यास शिक्षकांना मदत करणे हा या पुस्तिकेचा हेतू आहे.

1. सामाजिक अभियांत्रिकी: "विश्वास की फसवणूक?"



- **A** — **अधिकार**: मी आयटी विभागातून बोलत आहे.
- **U** — **तातडी**: ताबडतोब कृती करा.
- **R** — **बक्षीस**: मोफत डाउनलोड.
- **F** — **ओळखीचा असल्याचा आव**: तो/ती तुमचा मित्र/मैत्रीण आहे.

संकेत

1. कोणीतरी शाळेच्या आयटी विभागातून बोलत असल्याचे सांगून तुमचा संकेतशब्द विचारतो.
2. एक व्यक्ती स्वतःला तुमचा मित्र/मैत्रीण सांगते, परंतु नवीन खाते वापरते आणि तातडीने पैसे पाठवण्यास सांगते.
3. कोणीतरी तुमच्या लॉगिन तपशीलांच्या बदल्यात मोफत गेम डाउनलोड देऊ करतो.
4. एका विद्यार्थ्याला ताबडतोब कृती न केल्यास त्याचे खाते हटवले जाईल असा संदेश मिळतो.

निर्णयाचा मार्ग

🟢 बहुधा सुरक्षित | 🟡 पडताळणी आवश्यक | 🔴 संभाव्य फसवणूक

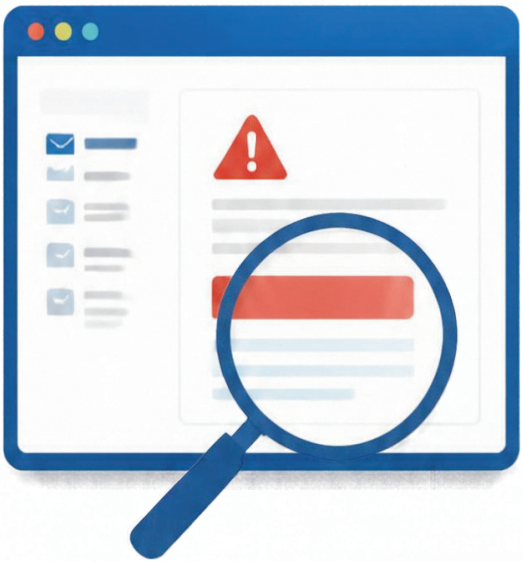
मुख्य धडा:

हल्लेखोर लोकांवर प्रभाव टाकण्यासाठी तातडी, अधिकार, भीती, कुतूहल, बक्षिसे किंवा ओळखीचा वापर करू शकतात.

2. फिशिंग: "धोक्याची चिन्हे ओळखा"

विद्यार्थ्यांनी लक्षात ठेवण्याचा नियम:

थांबा → तपासा → पडताळा → अहवाल द्या



- संशयास्पद पाठवणाऱ्याचे पत्ते
- तातडीची किंवा धमकीची भाषा
- अनपेक्षित संलग्नके
- संकेतशब्द किंवा वैयक्तिक माहितीची मागणी
- संशयास्पद दुवे
- शब्दलेखन/व्याकरणातील विसंगती
- असामान्य देयकाच्या मागण्या
- जुळत नसलेले वेबसाइट पत्ते



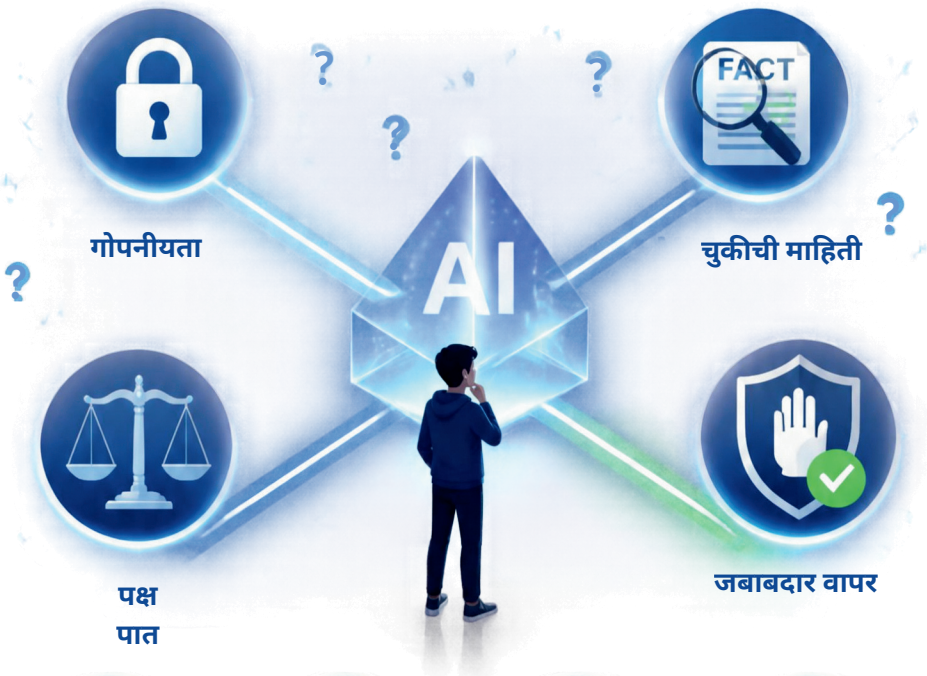
सुरक्षित



फिशिंग

3. एआय सुरक्षितता: "तुम्ही हे एआयला विचाराल का?"

विद्यार्थ्यांना याबद्दल शिकवा:

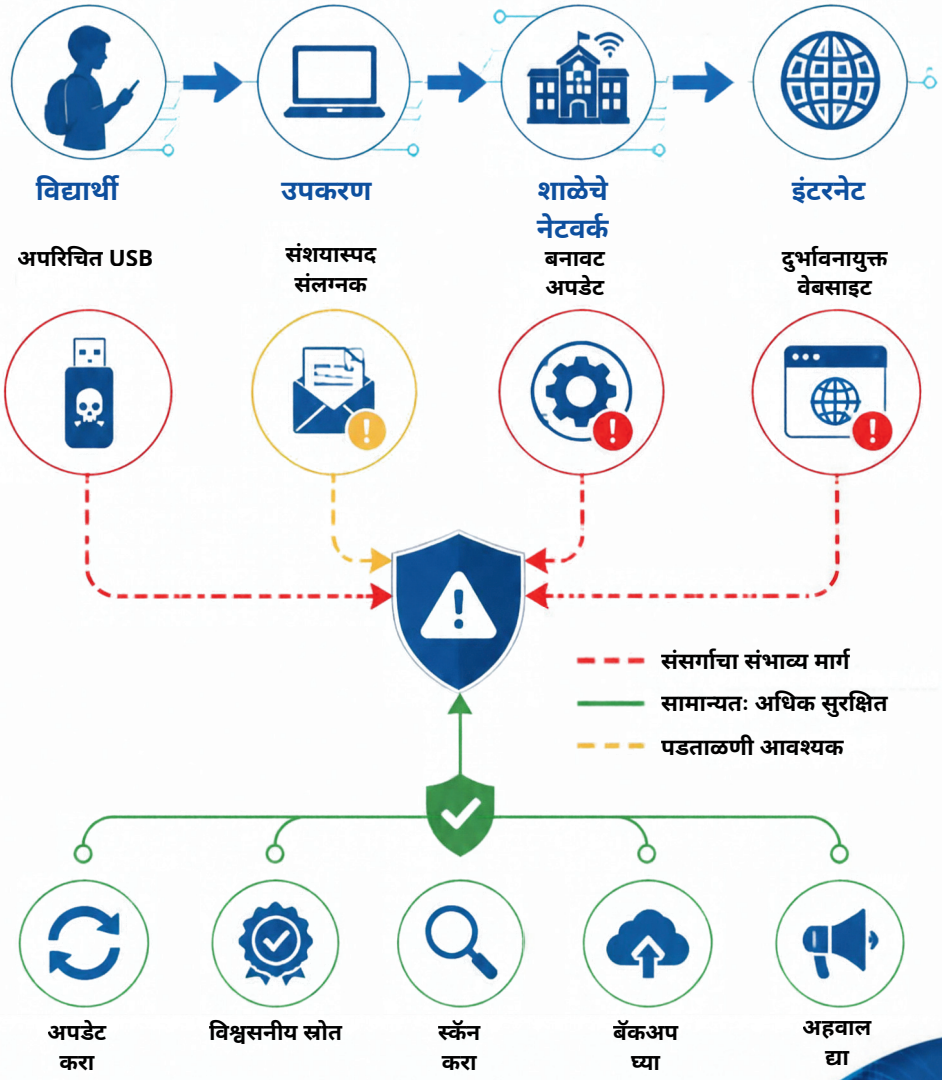


1. वैयक्तिक माहितीचे संरक्षण करा
2. महत्त्वाची माहिती पडताळा
3. परिणामांचा विचार करा
4. जबाबदार वापर

मुख्य धडा

एआय उपयुक्त ठरू शकते; परंतु विद्यार्थ्यांनी वैयक्तिक माहितीचे संरक्षण करावे, महत्त्वाची माहिती पडताळून पाहावी आणि त्यांनी तयार करून शेअर केलेल्या सामग्रीच्या परिणामांचा विचार करावा.

4. मालवेअर: "ते आत कसे शिरते?"



5. सायबर सुरक्षा एस्केप रूम



संपर्क करा

CERT-In कडे सायबर सुरक्षा घटनांची तक्रार नोंदवण्यासाठी:

- **वेबसाइटला भेट द्या:** https://www.cert-in.org.in/
- **ई-मेल:** incident@cert-in.org.in
- **टोल-फ्री फोन:** +91-1800-11-4949
- **टोल-फ्री फॅक्स:** +91-1800-11-6969

माहिती कक्ष

- **फोन:** +91-11-22902657

प्रशिक्षण आणि जागरूकता सत्रांमध्ये सहभागी होण्यासाठी ई-मेल करा:

training@cert-in.org.in

येथे आम्हाला फॉलो करा

@IndianCERT

@cert_india

जागरूकता पुस्तिका

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

सुरक्षा साधने

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

SCAN ME!