Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

certin
Enhancing Cyber Security in India

সাইবারস্মার্ট শ্রেণীকক্ষ

শিক্ষক ও শিক্ষার্থীদের জন্য পরিস্থিতিভিত্তিক সাইবার নিরাপত্তা নির্দেশিকা



জাতীয় সাইবার নিরাপত্তা সচেতনতা মাস
(অক্টোবর ২০২৬)
উপলক্ষে
"সাইবার হাইজিনের সংস্কৃতি গড়ে তুলুন"
#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

সূচিপত্র

	ভূমিকা	3
1	সামাজিক প্রকৌশল: “বিশ্বাস নাকি প্রতারণা?”	4
2	ফিশিং: “বিপদের সংকেত চিহ্নিত করুন”	5
3	এআই নিরাপত্তা: “আপনি কি এআইকে এটি জিজ্ঞেস করবেন?”	6
4	ম্যালওয়্যার: “এটি কীভাবে প্রবেশ করে?”	7
5	সাইবার নিরাপত্তা এসকেপ রুম	8
	যোগাযোগ করুন	9



ভূমিকা

শিক্ষার্থীরা অনলাইনে শেখা, যোগাযোগ, সহযোগিতা ও সৃজনশীল কাজে ক্রমশ বেশি সময় ব্যয় করছে। তাই সাইবার নিরাপত্তা বোঝা এখন একটি অপরিহার্য জীবনদক্ষতা হয়ে উঠেছে। প্রতিদিনের ডিজিটাল অভিজ্ঞতার মধ্যে সাইবার হুমকি ক্রমেই মিশে যাচ্ছে এবং এগুলো সন্দেহজনক বার্তা, অপ্রত্যাশিত লগইন অনুরোধ, বিভ্রান্তিকর ওয়েবসাইট, অজানা লিংক, প্রতারণামূলক কণ্ঠস্বর বা ভিডিও, কিংবা ব্যক্তিগত তথ্যের অনুরোধের মতো রূপে দেখা দিতে পারে। এসব পরিস্থিতি চিনতে, থামাতে, যাচাই করতে ও তথ্যভিত্তিক সিদ্ধান্ত নিতে শিক্ষার্থীদের জ্ঞান দিয়ে সক্ষম করা হলে ছোটবেলা থেকেই নিরাপদ ও দায়িত্বশীল ডিজিটাল অভ্যাস গড়ে তুলতে সাহায্য করবে।

ইন্ডিয়ান কম্পিউটার ইমার্জেন্সি রেসপন্স টিম (CERT-In)-এর 'সাইবারস্মার্ট শ্রেণীকক্ষ: শিক্ষক ও শিক্ষার্থীদের জন্য পরিস্থিতিভিত্তিক সাইবার নিরাপত্তা নির্দেশিকা' শিক্ষকদের জন্য বাস্তবধর্মী ও সহজবোধ্য পরিস্থিতি তুলে ধরে, যা শ্রেণীকক্ষের আলোচনা, কার্যক্রম এবং ইন্টার‍্যাক্টিভ শিক্ষণ পরিচালনায় ব্যবহার করা যায়। প্রতিটি পরিস্থিতি শিক্ষার্থীদের সম্ভাব্য ঝুঁকি শনাক্ত করতে, সমালোচনামূলকভাবে ভাবতে, সম্ভাব্য প্রতিক্রিয়া নিয়ে আলোচনা করতে এবং সাইবার নিরাপত্তার সহজ ও উত্তম অনুশীলনগুলো বুঝতে উৎসাহিত করে। শিক্ষার্থীরা দৈনন্দিন জীবনে যেসব পরিস্থিতির মুখোমুখি হতে পারে, সেগুলোর সঙ্গে সাইবার নিরাপত্তার ধারণাগুলো যুক্ত করে এই নির্দেশিকা সাইবার সচেতনতা শেখাকে আকর্ষণীয়, প্রাসঙ্গিক ও কার্যকর করে তুলতে চায় এবং দায়িত্বশীল ডিজিটাল নাগরিকত্বের সংস্কৃতি গড়ে তোলে।

এই পুস্তিকাটি CERT-In-এর জাতীয় সাইবার নিরাপত্তা সচেতনতা মাসের (অক্টোবর ২০২৬) কার্যক্রমের অংশ হিসেবে প্রকাশিত হয়েছে। এর উদ্দেশ্য শিক্ষার্থী ও শিক্ষকদের মধ্যে সাইবার নিরাপত্তা সচেতনতা আরও জোরদার করা। অনলাইন নিরাপত্তা নিয়ে অর্থবহ আলোচনা তৈরি করতে এবং ডিজিটাল জগতে তথ্যভিত্তিক, নিরাপদ ও দায়িত্বশীল সিদ্ধান্ত নিতে শিক্ষার্থীদের সক্ষম করে তুলতে এটি শিক্ষকদের সহায়তা করবে।

1. সামাজিক প্রকৌশল: “বিশ্বাস নাকি প্রতারণা?”



A **কর্তৃত্ব**
আমি আইটি বিভাগ থেকে বলছি।

U **জরুরি তাগিদ**
অবিলম্বে কাজ করুন।

R **পুরস্কার**
বিনামূল্যে ডাউনলোড।

F **পরিচিতি**
এটি আপনার বন্ধু।

সংকেত

1. কেউ স্কুলের আইটি বিভাগের সদস্য পরিচয় দিয়ে ফোন করে আপনার পাসওয়ার্ড চায়।
2. কেউ নিজেকে আপনার বন্ধু বলে, কিন্তু নতুন অ্যাকাউন্ট ব্যবহার করে এবং জরুরি ভিত্তিতে টাকা পাঠাতে বলে।
3. কেউ আপনার লগইন তথ্যের বিনিময়ে বিনামূল্যে একটি গেম ডাউনলোডের প্রস্তাব দেয়।
4. একজন শিক্ষার্থী একটি বার্তা পায়, যেখানে বলা হয় যে অবিলম্বে ব্যবস্থা না নিলে তার অ্যাকাউন্ট মুছে ফেলা হবে।

সিদ্ধান্তের পথ

🟢 সম্ভবত নিরাপদ | 🟡 যাচাই করা প্রয়োজন | 🔴 সম্ভাব্য প্ররোচনা

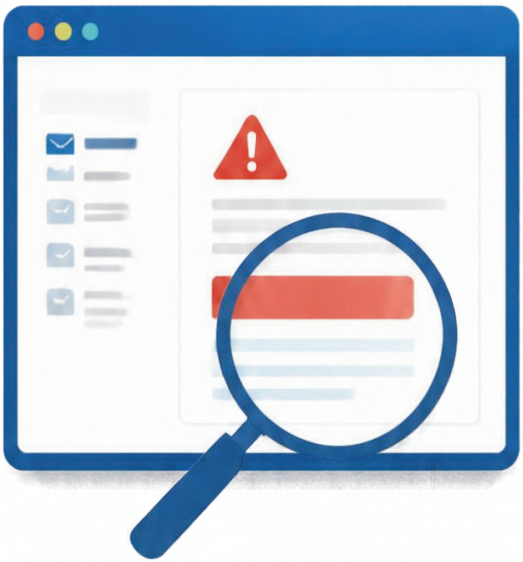
মূল শিক্ষা:

আক্রমণকারীরা মানুষকে প্রভাবিত করতে জরুরি তাগিদ, কর্তৃত্ব, ভয়, কৌতূহল, পুরস্কার বা পরিচিতির মতো কৌশল ব্যবহার করতে পারে।

2. ফিশিং: “বিপদের সংকেত চিহ্নিত করুন”

শিক্ষার্থীদের মনে রাখা উচিত:

থামুন → পরীক্ষা করুন → যাচাই করুন → রিপোর্ট করুন



- সন্দেহজনক প্রেরকের ঠিকানা
- জরুরি বা হুমকিমূলক ভাষা
- অপ্রত্যাশিত সংযুক্তি
- পাসওয়ার্ড বা ব্যক্তিগত তথ্যের অনুরোধ
- সন্দেহজনক লিংক
- বানান বা ব্যাকরণের অসঙ্গতি
- অস্বাভাবিক পেমেন্টের অনুরোধ
- অমিল ওয়েবসাইটের ঠিকানা



3. এআই নিরাপত্তা: “এআইকে কি এটি জিজ্ঞেস করবেন?”

শিক্ষার্থীদের শেখান:



1. ব্যক্তিগত তথ্য সুরক্ষিত রাখুন
2. গুরুত্বপূর্ণ তথ্য যাচাই করুন
3. পরিণতি বিবেচনা করুন
4. দায়িত্বশীল ব্যবহার

মূল শিক্ষা

এআই উপকারী হতে পারে, তবে শিক্ষার্থীদের ব্যক্তিগত তথ্য সুরক্ষিত রাখতে হবে, গুরুত্বপূর্ণ তথ্য যাচাই করতে হবে এবং তারা যা তৈরি ও শেয়ার করে তার পরিণতি বিবেচনা করতে হবে।

4. ম্যালওয়্যার: “এটি কীভাবে প্রবেশ করে?”



5. সাইবার নিরাপত্তা এসকেপ রুম



যোগাযোগ করুন

CERT-In-এ সাইবার নিরাপত্তা সংক্রান্ত ঘটনা রিপোর্ট করতে:

- **ওয়েবসাইট দেখুন:** https://www.cert-in.org.in/
- **ইমেইল:** incident@cert-in.org.in
- **টোল-ফ্রি ফোন:** +91-1800-11-4949
- **টোল-ফ্রি ফ্যাক্স:** +91-1800-11-6969

তথ্য ডেস্ক

- **ফোন:** +91-11-22902657

প্রশিক্ষণ ও সচেতনতা সেশনে অংশগ্রহণ করতে ইমেইল করুন:
training@cert-in.org.in

আমাদের অনুসরণ করুন

@IndianCERT

@cert_india

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

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

SCAN ME!