Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

certin
Enhancing Cyber Security in India

CyberSmart

ક્લાસરૂમ

શિક્ષકો અને વિદ્યાર્થીઓ માટે સિનેરિયો આધારિત સાયબરસેફ્ટિ ગાઇડ



અવસરે

રાષ્ટ્રીય સાયબરસેફ્ટિ અવગતિ મહિનો

(ઓક્ટોબર ૨૦૨૬)

“સાયબર હાઇજિનની સંસ્કૃતિ બનાવો”

#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

વિષયસૂચિ

	પ્રસ્તાવના	3
1	સોશિયલ એન્જિનિયરિંગ: “વિશ્વાસ કે છેતરપિંડી?”	4
2	ફિશિંગ: “ચેતવણીના સંકેતો ઓળખો”	5
3	AI સલામતી: “શું તમે AI ને આ પૂછશો?”	6
4	માલવેર: “તે અંદર કેવી રીતે પ્રવેશે છે?”	7
5	સાયબરસિક્યુરિટી એસ્કેપ રૂમ	8
	અમારો સંપર્ક કરો	9



પ્રસ્તાવના

વિદ્યાર્થીઓ ઑનલાઇન શીખવામાં, સંવાદ કરવામાં, સહયોગ કરવામાં અને સર્જન કરવામાં વધુ સમય વિતાવે છે, તેથી સાયબર સુરક્ષાને સમજવી જીવન માટેની એક આવશ્યક કુશળતા બની ગઈ છે. સાયબર જોખમો રોજિંદા ડિજિટલ અનુભવોમાં વધુને વધુ સામેલ થઈ રહ્યાં છે અને તે શંકાસ્પદ સંદેશ, અણધારી લૉગિન વિનંતી, ભ્રામક વેબસાઇટ, અજાણી લિંક, છેતરામણો અવાજ અથવા વીડિયો, કે વ્યક્તિગત માહિતીની વિનંતી તરીકે દેખાઈ શકે છે. આવી પરિસ્થિતિઓને ઓળખવા, થોભવા, ચકાસવા અને માહિતીસભર નિર્ણયો લેવા માટે વિદ્યાર્થીઓને જ્ઞાનથી સજ્જ કરવાથી નાની ઉંમરથી જ સુરક્ષિત અને જવાબદાર ડિજિટલ આદતો વિકસાવવામાં મદદ મળી શકે છે.

ભારતીય કમ્પ્યુટર ઇમર્જન્સી રિસ્પોન્સ ટીમ (CERT-In)નું CyberSmart Classroom: શિક્ષકો અને વિદ્યાર્થીઓ માટે સિનેરિયો આધારિત સાયબરસિક્યુરિટી માર્ગદર્શિકા શિક્ષકોને વ્યવહારુ અને સરળતાથી સમજી શકાય તેવા સિનેરિયો પ્રદાન કરે છે, જેનો ઉપયોગ વર્ગખંડમાં ચર્ચાઓ, પ્રવૃત્તિઓ અને પરસ્પર સંવાદાત્મક શિક્ષણને સરળ બનાવવા માટે થઈ શકે છે. દરેક સિનેરિયો વિદ્યાર્થીઓને સંભવિત જોખમોને ઓળખવા, વિવેચનાત્મક રીતે વિચારવા, સંભવિત પ્રતિસાદોની ચર્ચા કરવા અને સાયબર સુરક્ષાની સરળ શ્રેષ્ઠ પદ્ધતિઓ સમજવા માટે પ્રોત્સાહિત કરે છે. વિદ્યાર્થીઓ તેમના દૈનિક જીવનમાં જે પરિસ્થિતિઓનો સામનો કરી શકે છે તેની સાથે સાયબર સુરક્ષાના ખ્યાલોને જોડીને, આ માર્ગદર્શિકા જવાબદાર ડિજિટલ નાગરિકતાની સંસ્કૃતિ વિકસાવવાની સાથે સાયબર જાગૃતિને રસપ્રદ, સંબંધિત અને અમલમાં મૂકી શકાય તેવી બનાવવાનો પ્રયાસ કરે છે.

આ પુસ્તિકા CERT-In રાષ્ટ્રીય સાયબર સુરક્ષા જાગૃતિ મહિનો (ઑક્ટોબર ૨૦૨૬)ની પ્રવૃત્તિઓના ભાગરૂપે પ્રકાશિત કરવામાં આવી છે, જેનો ઉદ્દેશ વિદ્યાર્થીઓ અને શિક્ષકોમાં સાયબર સુરક્ષા અંગેની જાગૃતિને મજબૂત બનાવવાનો છે. તેનો હેતુ શિક્ષકોને ઑનલાઇન સલામતી વિશે અર્થપૂર્ણ સંવાદો ઊભા કરવામાં સહાય કરવો અને વિદ્યાર્થીઓને ડિજિટલ વિશ્વમાં માહિતીસભર, સુરક્ષિત અને જવાબદાર પસંદગીઓ કરવા સશક્ત બનાવવાનો છે.

1. સોશિયલ એન્જિનિયરિંગ



A **અધિકાર**
હું IT વિભાગમાંથી છું.

U **તાત્કાલિકતા**
તરત જ કાર્યવાહી કરો.

R **ઇનામ**
મફત ડાઉનલોડ.

F **પરિચિતતા**
આ તમારો મિત્ર છે.

સંકેતો

1. કોઈ વ્યક્તિ શાળાના IT વિભાગમાંથી હોવાનો દાવો કરીને ફોન કરે છે અને તમારો પાસવર્ડ માંગે છે.
2. કોઈ વ્યક્તિ પોતાને તમારો મિત્ર ગણાવે છે, પરંતુ નવા એકાઉન્ટનો ઉપયોગ કરીને તાત્કાલિક નાણાં ટ્રાન્સફર કરવા કહે છે.
3. કોઈ વ્યક્તિ તમારી લૉગિન વિગતોના બદલામાં મફત ગેમ ડાઉનલોડ કરવાની ઑફર આપે છે.
4. એક વિદ્યાર્થીને સંદેશ મળે છે કે જો તે તરત જ કાર્યવાહી નહીં કરે તો તેનું એકાઉન્ટ કાઢી નાખવામાં આવશે.

નિર્ણય માર્ગ

🟢 મોટાભાગે સુરક્ષિત | 🟡 ચકાસણી જરૂરી | 🔴 સંભવિત છેતરપિંડી

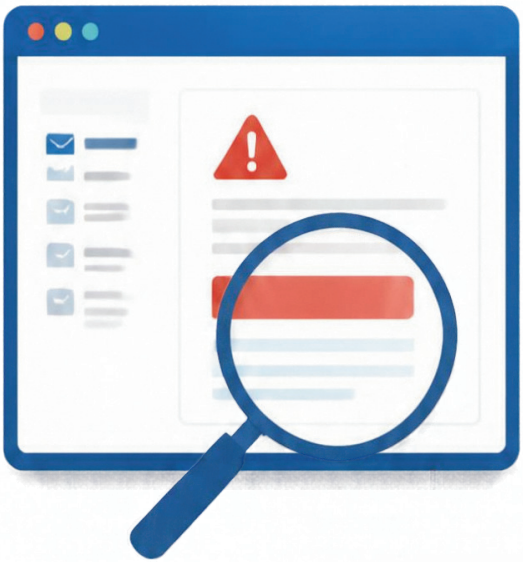
મુખ્ય શીખ:

હુમલાખોરો લોકોને પ્રભાવિત કરવા માટે તાત્કાલિકતા, અધિકાર, ભય, જિજ્ઞાસા, ઇનામ અથવા પરિચિતતાનો ઉપયોગ કરી શકે છે.

2. ફિશિંગ: “ચેતવણીના સંકેતો ઓળખો”

વિદ્યાર્થીઓએ યાદ રાખવાનો નિયમ:

થોભો → તપાસો → ચકાસો → જાણ કરો



- શંકાસ્પદ મોકલનારના સરનામાં
- તાત્કાલિક અથવા ધમકીભરી ભાષા
- અનપેક્ષિત જોડાણો
- પાસવર્ડ અથવા વ્યક્તિગત માહિતી માટેની વિનંતીઓ
- શંકાસ્પદ લિંક્સ
- જોડણી/વ્યાકરણની અસંગતતાઓ
- અસામાન્ય ચુકવણી વિનંતીઓ
- મેળ ન ખાતાં વેબસાઇટ સરનામાં



સુરક્ષિત

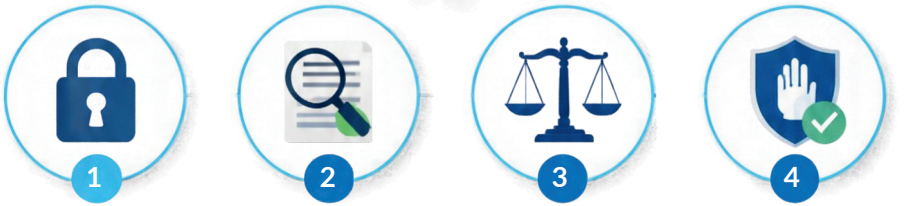


ફિશિંગ

3. AI સલામતી: “શું તમે AI ને આ પૂછશો?”

વિદ્યાર્થીઓને આ વિશે શીખવો:



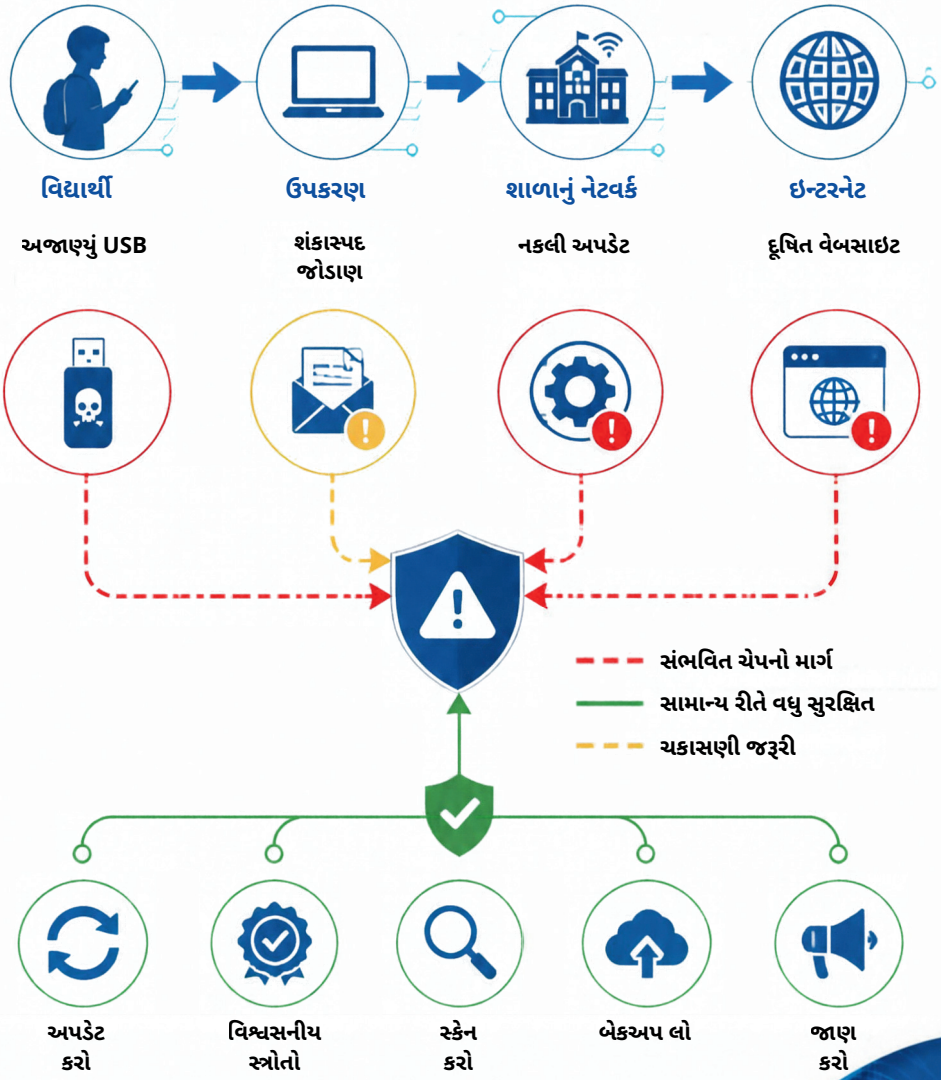


1. વ્યક્તિગત માહિતીનું રક્ષણ કરો
2. મહત્વપૂર્ણ માહિતીની ચકાસણી કરો
3. પરિણામોનો વિચાર કરો
4. જવાબદાર ઉપયોગ

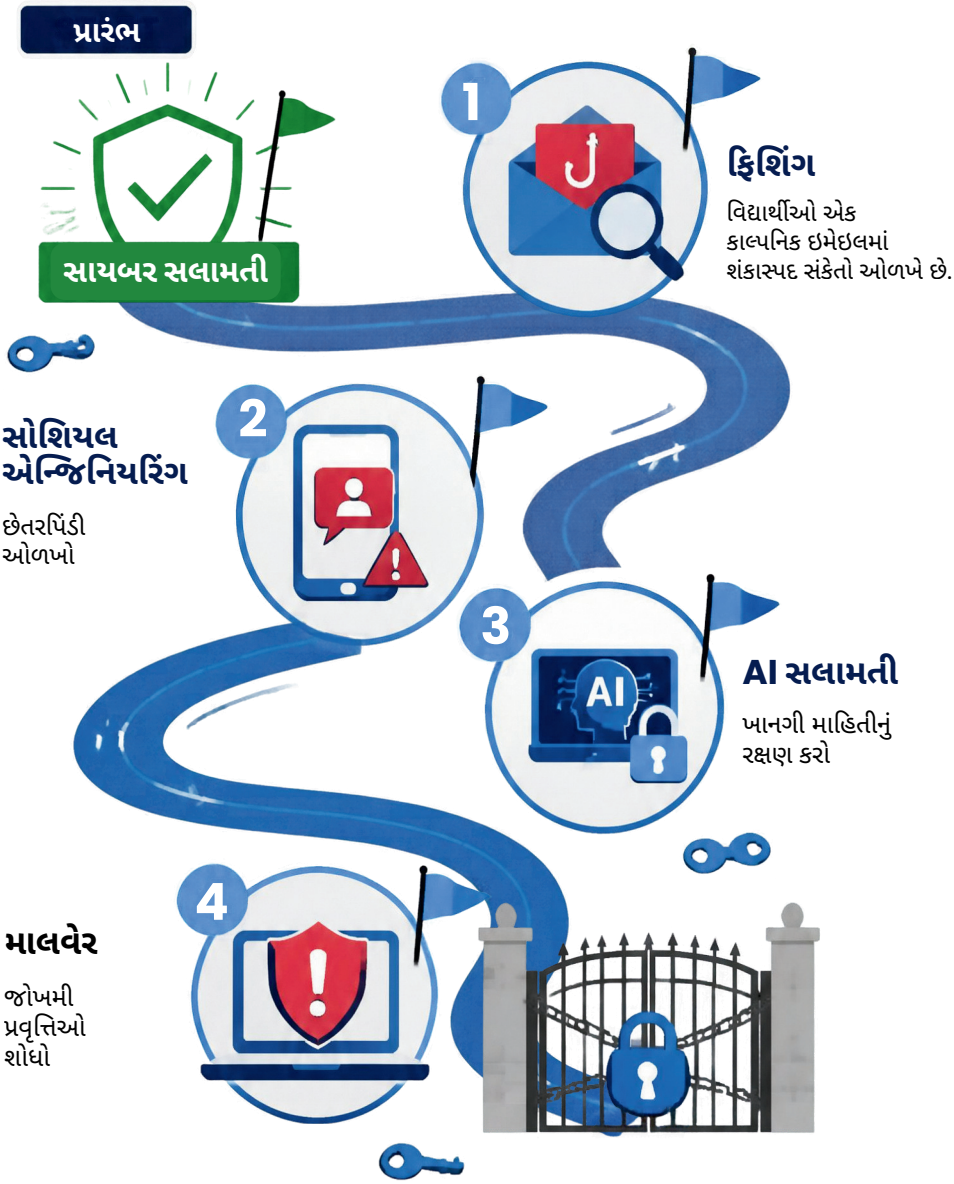
મુખ્ય શીખ

AI ઉપયોગી બની શકે છે, પરંતુ વિદ્યાર્થીઓએ વ્યક્તિગત માહિતીનું રક્ષણ કરવું, મહત્વપૂર્ણ માહિતીની ચકાસણી કરવી અને તેઓ જે બનાવે તથા શેર કરે તેના પરિણામોનો વિચાર કરવો જોઈએ.

4. માલવેર: “તે અંદર કેવી રીતે પ્રવેશે છે?”



5. સાયબર સુરક્ષા એસ્કેપ રૂમ



અમારો સંપર્ક કરો

CERT-In ને સાયબર સુરક્ષા ઘટનાઓની જાણ કરવા માટે:

- **વેબસાઇટની મુલાકાત લો:** https://www.cert-in.org.in/
- **ઇમેઇલ:** incident@cert-in.org.in
- **ટોલ-ફ્રી ફોન:** +91-1800-11-4949
- **ટોલ-ફ્રી ફેક્સ:** +91-1800-11-6969

માહિતી ડેસ્ક

- **ફોન:** +91-11-22902657

તાલીમ અને જાગૃતિ સત્રોમાં ભાગ લેવા માટે, ઇમેઇલ કરો:
training@cert-in.org.in

અમને અહીં અનુસરો

@IndianCERT

@cert_india

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

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

SCAN ME!