Ministry of Electronics and Information Technology
Government of India

सत्यमेव जयते

certin
Enhancing Cyber Security in India

സൈബർസ്മാർട്ട് ക്ലാസ്റൂം

അധ്യാപകർക്കും വിദ്യാർത്ഥികൾക്കുമു ള്ള സാഹചര്യാധിഷ്ഠിത സൈബർ സുരക്ഷാ മാർഗ്ഗദർശിക



ഇതിന്റെ ഭാഗമായി

ദേശീയ സൈബർ സുരക്ഷാ ബോധവത്കരണ മാസം
(ഒക്ടോബർ 2026)

“സൈബർ ശുചിത്വത്തിന്റെ സംസ്കാരം വളർത്താം”

#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

ഉള്ളടക്കപ്പട്ടിക

	ആമുഖം	3
1	സോഷ്യൽ എഞ്ചിനീയറിംഗ്: “വിശ്വാസമോ വഞ്ചനയോ?”	4
2	ഫിഷിംഗ്: “അപകടസൂചനകൾ തിരിച്ചറിയാം”	5
3	AI സുരക്ഷ: “ഇത് നിങ്ങൾ AI-യോട് ചോദിക്കുമോ?”	6
4	മാൽവെയർ: “ഇത് എങ്ങനെ അകത്തേക്ക് കടക്കുന്നു?”	7
5	സൈബർ സുരക്ഷാ എസ്കേപ് റൂം	8
	ഞങ്ങളെ ബന്ധപ്പെടുക	9



ആമുഖം

വിദ്യാർത്ഥികൾ ഓൺലൈനിൽ പഠിക്കാനും ആശയവിനിമയം നടത്താനും സഹകരിക്കാനും സൃഷ്ടിക്കാനും കൂടുതൽ സമയം ചെലവഴിക്കുന്നതിനാൽ, സൈബർ സുരക്ഷയെക്കുറിച്ചുള്ള ധാരണ അനിവാര്യമായ ഒരു ജീവിത നൈപുണ്യമായി മാറിയിരിക്കുന്നു. ദൈനംദിന ഡിജിറ്റൽ അനുഭവങ്ങളിൽ സൈബർ ഭീഷണികൾ കൂടുതൽ ഉൾക്കൊള്ളപ്പെടുകയും സംശയാസ്പദമായ ഒരു സന്ദേശം, പ്രതീക്ഷിക്കാത്ത ലോഗിൻ അഭ്യർത്ഥന, തെറ്റിദ്ധരിപ്പിക്കുന്ന വെബ്സൈറ്റ്, പരിചയമില്ലാത്ത ലിങ്ക്, വഞ്ചനാപരമായ ശബ്ദമോ വീഡിയോയോ, അല്ലെങ്കിൽ വ്യക്തിഗത വിവരങ്ങൾ ആവശ്യപ്പെടുന്ന അഭ്യർത്ഥനയോ ആയി പ്രത്യക്ഷപ്പെടുകയും ചെയ്യാം. ഇത്തരം സാഹചര്യങ്ങൾ തിരിച്ചറിയാനും, ഒരു നിമിഷം നിർത്തി പരിശോധിച്ചുറപ്പിക്കാനും, വിവരബോധമുള്ള തീരുമാനങ്ങൾ എടുക്കാനും വിദ്യാർത്ഥികളെ പ്രാപ്തരാക്കുന്നത് ചെറുപ്പം മുതലേ സുരക്ഷിതവും ഉത്തരവാദിത്തപരവുമായ ഡിജിറ്റൽ ശീലങ്ങൾ വളർത്താൻ സഹായിക്കും.

ഇന്ത്യൻ കമ്പ്യൂട്ടർ എമർജൻസി റെസ്പോൺസ് ടീം (CERT-In) -ന്റെ സൈബർസ്മാർട്ട് ക്ലാസ്റൂം: അധ്യാപകർക്കും വിദ്യാർത്ഥികൾക്കുമുള്ള സാഹചര്യാധിഷ്ഠിത സൈബർ സുരക്ഷാ മാർഗ്ഗദർശിക, ക്ലാസ് മുറിയിലെ ചർച്ചകൾ, പ്രവർത്തനങ്ങൾ, സംവേദനാത്മക പഠനം എന്നിവ സുഗമമാക്കാൻ അധ്യാപകർക്ക് ഉപയോഗിക്കാവുന്ന പ്രായോഗികവും എളുപ്പം മനസ്സിലാക്കാവുന്നതുമായ സാഹചര്യങ്ങൾ നൽകുന്നു. ഓരോ സാഹചര്യവും സാധ്യതയുള്ള അപകടസാധ്യതകൾ തിരിച്ചറിയാനും വിമർശനാത്മകമായി ചിന്തിക്കാനും സാധ്യമായ പ്രതികരണങ്ങൾ ചർച്ച ചെയ്യാനും ലളിതമായ സൈബർ സുരക്ഷാ മികച്ച രീതികൾ മനസ്സിലാക്കാനും വിദ്യാർത്ഥികളെ പ്രോത്സാഹിപ്പിക്കുന്നു. വിദ്യാർത്ഥികൾ ദൈനംദിന ജീവിതത്തിൽ നേരിടാനിടയുള്ള സാഹചര്യങ്ങളുമായി സൈബർ സുരക്ഷാ ആശയങ്ങളെ ബന്ധിപ്പിക്കുന്നതിലൂടെ, ഉത്തരവാദിത്തമുള്ള ഡിജിറ്റൽ പൗരത്വത്തിന്റെ സംസ്കാരം വളർത്തിക്കൊണ്ട് സൈബർ ബോധവത്കരണം ആകർഷകവും പ്രസക്തവും പ്രായോഗികവുമാക്കുകയാണ് ഈ മാർഗ്ഗദർശികയുടെ ലക്ഷ്യം.

വിദ്യാർത്ഥികൾക്കും അധ്യാപകർക്കും ഇടയിലെ സൈബർ സുരക്ഷാ ബോധവത്കരണം ശക്തിപ്പെടുത്തുക എന്ന ലക്ഷ്യത്തോടെ, CERT-In ദേശീയ സൈബർ സുരക്ഷാ ബോധവത്കരണ മാസം (ഒക്ടോബർ 2026) പ്രവർത്തനങ്ങളുടെ ഭാഗമായി ഈ ബുക്ക്ലെറ്റ് പ്രസിദ്ധീകരിച്ചിരിക്കുന്നു. ഓൺലൈൻ സുരക്ഷയെക്കുറിച്ചുള്ള അർത്ഥവത്തായ സംഭാഷണങ്ങൾ സൃഷ്ടിക്കാനും ഡിജിറ്റൽ ലോകത്ത് വിവരബോധമുള്ളതും സുരക്ഷിതവും ഉത്തരവാദിത്തപരവുമായ തിരഞ്ഞെടുപ്പുകൾ നടത്താൻ വിദ്യാർത്ഥികളെ പ്രാപ്തരാക്കാനും അധ്യാപകരെ പിന്തുണയ്ക്കുന്നതിനാണ് ഇത് ഉദ്ദേശിക്കുന്നത്.

1. സോഷ്യൽ എഞ്ചിനീയറിംഗ്: "വിശ്വാസമോ വഞ്ചനയോ?"



A **അധികാരം**
ഞാൻ IT വിഭാഗത്തിൽ നിന്നാണ്.

U **അടിയന്തരത**
ഉടൻ പ്രവർത്തിക്കുക.

R **പ്രതിഫലം**
സൗജന്യ ഡൗൺലോഡ്.

F **പരിചയം**
ഇത് നിങ്ങളുടെ സുഹൃത്താണ്.

സൂചനകൾ

1. ഒരാൾ സ്കൂളിലെ IT വിഭാഗത്തിൽ നിന്നാണെന്ന് അവകാശപ്പെട്ട് വിളിക്കുകയും നിങ്ങളുടെ പാസ്‌വേഡ് ചോദിക്കുകയും ചെയ്യുന്നു.

2. ഒരാൾ താൻ നിങ്ങളുടെ സുഹൃത്താണെന്ന് പറയുന്നു, എന്നാൽ പുതിയ അക്കൗണ്ടാണ് ഉപയോഗിക്കുന്നത്, അടിയന്തരമായി പണം കൈമാറാൻ ആവശ്യപ്പെടുന്നു.

3. നിങ്ങളുടെ ലോഗിൻ വിവരങ്ങൾക്ക് പകരം ഒരാൾ സൗജന്യ ഗെയിം ഡൗൺലോഡ് വാഗ്ദാനം ചെയ്യുന്നു.

4. ഉടൻ പ്രവർത്തിച്ചില്ലെങ്കിൽ തന്റെ അക്കൗണ്ട് ഇല്ലാതാക്കുമെന്ന് ഒരു വിദ്യാർത്ഥിക്ക് സന്ദേശം ലഭിക്കുന്നു.

തീരുമാന പാത

🟢 സുരക്ഷിതമായിരിക്കാം

🟡 പരിശോധിച്ച് ഉറപ്പാക്കേണ്ടതാണ്

🔴 കൃത്രിമ സ്വാധീനത്തിനുള്ള സാധ്യതയുണ്ട്

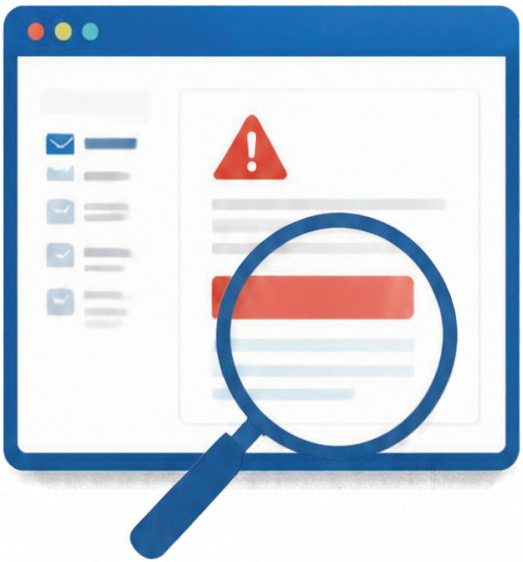
പ്രധാന പാഠം:

ആളുകളെ സ്വാധീനിക്കാൻ ആക്രമണകാരികൾ അടിയന്തരത, അധികാരം, ഭയം, കൗതുകം, പ്രതിഫലം, അല്ലെങ്കിൽ പരിചയം എന്നിവ ഉപയോഗിച്ചേക്കാം.

2. ഫിഷിംഗ്: അപകടസൂചനകൾ തിരിച്ചറിയാം

വിദ്യാർത്ഥികൾ ഓർക്കേണ്ട നിയമം

നിർത്തുക → പരിശോധിക്കുക → ഉറപ്പാക്കുക → റിപ്പോർട്ട് ചെയ്യുക





SAFE



PHISHING

- സംശയാസ്പദമായ അയച്ചയാളുടെ വിലാസങ്ങൾ
- അടിയന്തരമോ ഭീഷണിപ്പെടുത്തുന്നതോ ആയ ഭാഷ
- പ്രതീക്ഷിക്കാത്ത അറ്റാച്ച്മെന്റുകൾ
- പാസ്വേഡുകളോ വ്യക്തിഗത വിവരങ്ങളോ ആവശ്യപ്പെടൽ
- സംശയാസ്പദമായ ലിങ്കുകൾ
- അക്ഷരത്തെറ്റുകളോ വ്യാകരണത്തിലെ പൊരുത്തക്കേടുകളോ
- അസാധാരണമായ പണമടയ്ക്കൽ അഭ്യർത്ഥനകൾ
- പൊരുത്തപ്പെടാത്ത വെബ്സൈറ്റ് വിലാസങ്ങൾ

3. AI സുരക്ഷ: "ഇത് നിങ്ങൾ AI-യോട് ചോദിക്കുമോ?"

വിദ്യാർത്ഥികളെ പഠിപ്പിക്കേണ്ടത്:

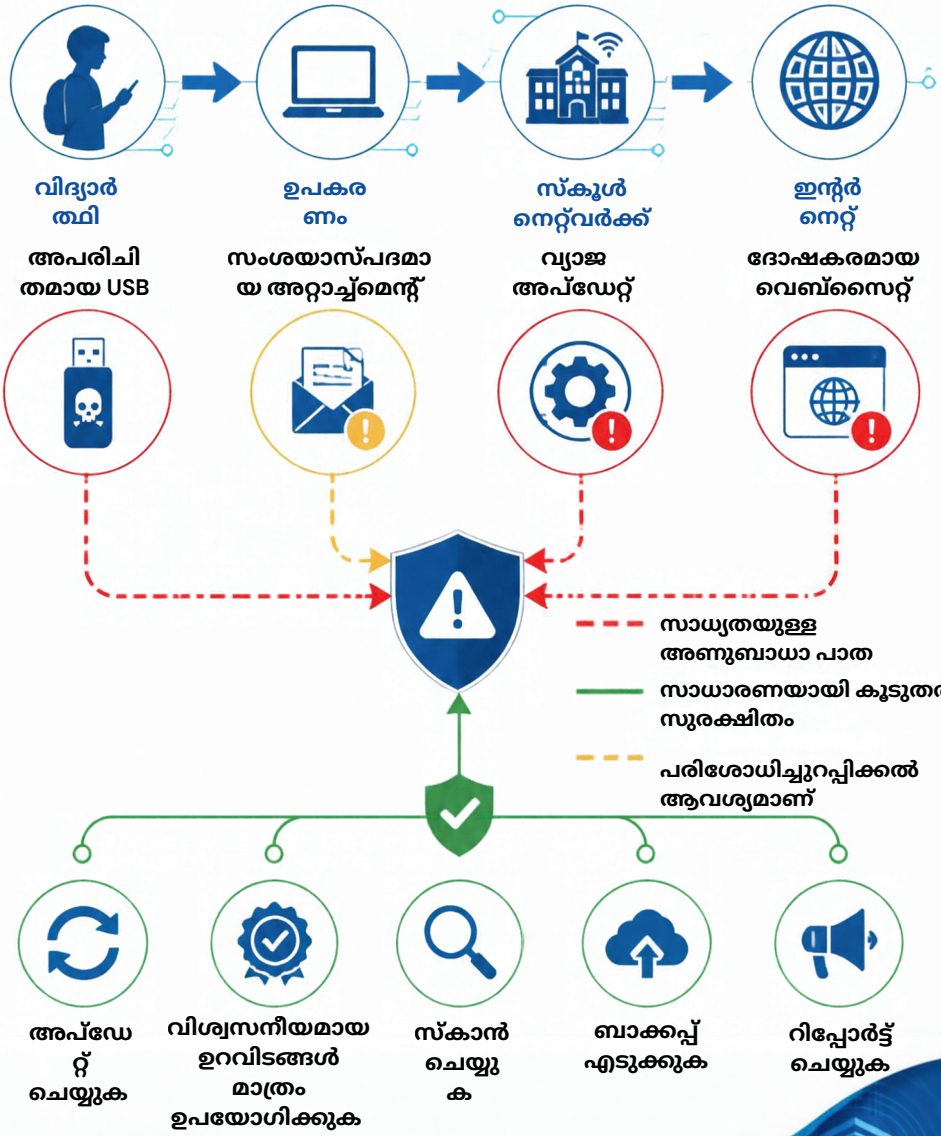


1. വ്യക്തിഗത വിവരങ്ങൾ സംരക്ഷിക്കുക
2. പ്രധാനപ്പെട്ട വിവരങ്ങൾ പരിശോധിച്ച് ഉറപ്പാക്കുക
3. പരിണതഫലങ്ങൾ പരിഗണിക്കുക
4. ഉത്തരവാദിത്തപരമായി ഉപയോഗിക്കുക

പ്രധാന പാഠം

AI ഉപകാരപ്രദമായ ഒരു ഉപകരണമായിരിക്കാം. എന്നാൽ വിദ്യാർത്ഥികൾ വ്യക്തിഗത വിവരങ്ങൾ സംരക്ഷിക്കുകയും, പ്രധാനപ്പെട്ട വിവരങ്ങൾ പരിശോധിച്ച് ഉറപ്പാക്കുകയും, തങ്ങൾ സൃഷ്ടിക്കുകയും പങ്കിടുകയും ചെയ്യുന്ന ഉള്ളടക്കങ്ങളുടെ സാധ്യതയുള്ള പ്രത്യാഘാതങ്ങൾ പരിഗണിക്കുകയും വേണം.

4. മാൽവെയർ: "ഇത് എങ്ങനെ അകത്തേക്ക് കടക്കുന്നു?"



5. സൈബർ സുരക്ഷാ എസ്കേപ്പ് റൂം



ഞങ്ങളെ ബന്ധപ്പെടുക

CERT-In-ലേക്ക് സൈബർ സുരക്ഷാ സംഭവങ്ങൾ റിപ്പോർട്ട് ചെയ്യാൻ:

വെബ്സൈറ്റ് സന്ദർശിക്കുക: https://www.cert-in.org.in/

ഇ-മെയിൽ: incident@cert-in.org.in

ടോൾ-ഫ്രീ ഫോൺ: +91-1800-11-4949

ടോൾ-ഫ്രീ ഫാക്സ്: +91-1800-11-6969

വിവര ഡെസ്ക്

ഫോൺ: +91-11-22902657

പരിശീലന, ബോധവത്കരണ സെഷനുകളിൽ പങ്കെടുക്കുന്നതിനായി ഇ-മെയിൽ ചെയ്യുക:

training@cert-in.org.in

ഞങ്ങളെ പിന്തുടരുക

@IndianCERT

@cert_india

ബോധവത്കരണ ലഘുപുസ്തകങ്ങൾ

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

സുരക്ഷാ ഉപകരണങ്ങൾ

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

SCAN ME!