



इलेक्ट्रॉनिकी एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY

सत्यमेव जयते

സുരക്ഷിത ഇന്റർനെറ്റ് ദിനം



സുരക്ഷിത
ബ്രൈറ്റുകൾ

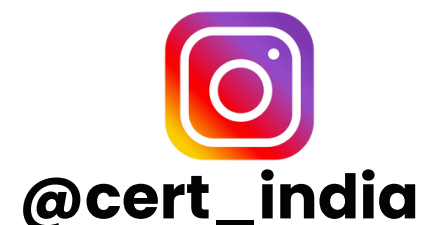
എഴുതിയത്

ഇന്ത്യൻ കമ്പ്യൂട്ടർ എമർജൻസി
റെസ്പോൺസ് ടീം



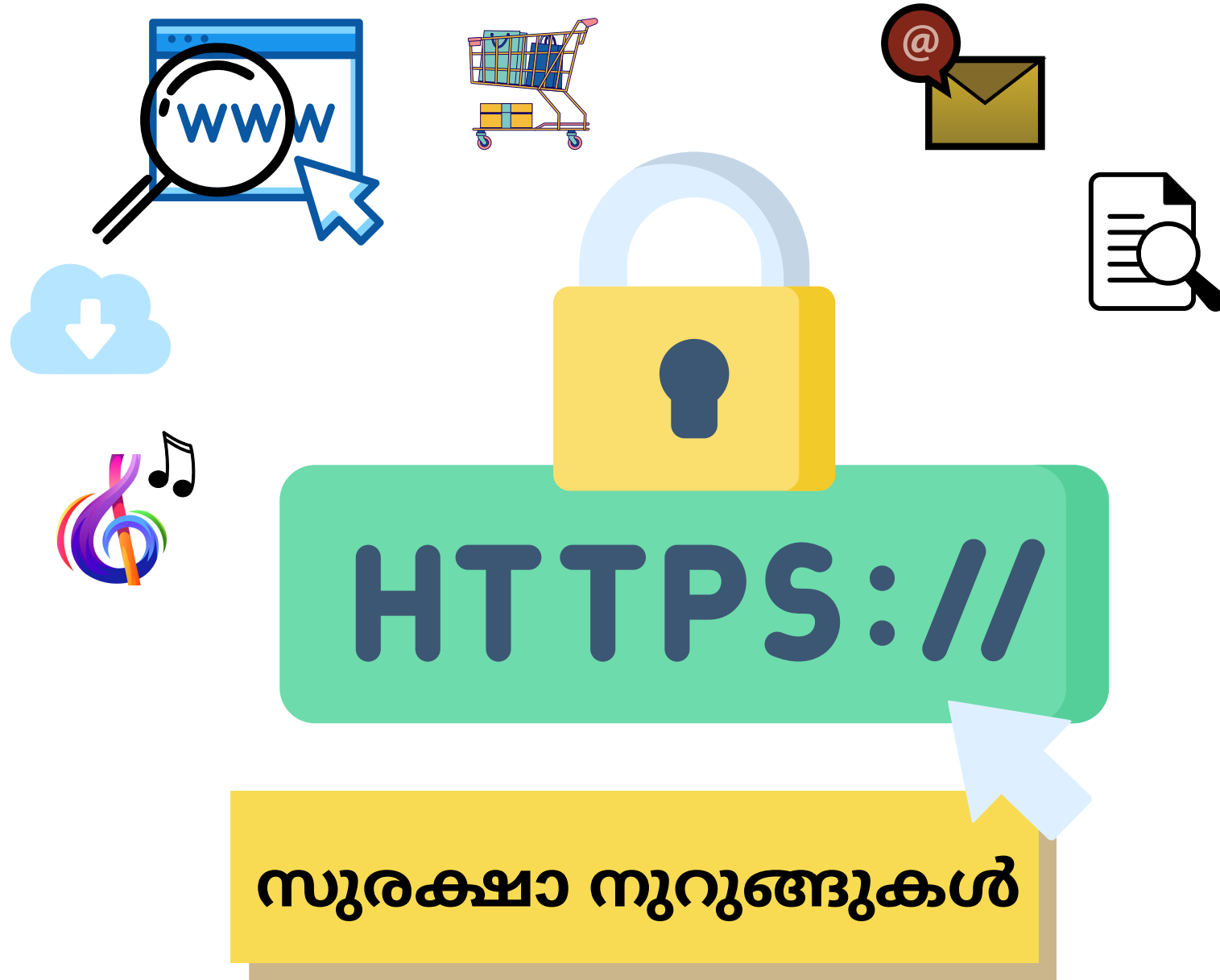
താൽക്കാലികമായി നിർത്തുക.
ചിന്തിക്കുക. ക്ലിക്ക് ചെയ്യുക.
സംരക്ഷിക്കാനും സുരക്ഷിതമാക്കാനും
ഉപകരണം. ഐഡന്റിറ്റി. ഡാറ്റ.
ഇന്റർനെറ്റിൽ

ഞങ്ങളെ
പിന്തുടരുക:



സുരക്ഷിത ഇന്റർനെറ്റ് ദിനം

പൊതു ഉപയോക്താക്കൾക്കുള്ള മികച്ച രീതികൾ



- പൊതു വെബ്സൈറ്റുകളിലോ സോഷ്യൽ മീഡിയയിലോ വ്യക്തിഗത വിവരങ്ങൾ പങ്കിടരുത്.
- വ്യത്യസ്ത അക്കൗണ്ടുകൾക്ക് വ്യത്യസ്ത പാസ്‌വേഡുകൾ ഉപയോഗിക്കുക.
- ക്ലിക്ക് ചെയ്യുന്നതിനു മുമ്പ് ചുരുക്കിയ URL-കൾ വികസിപ്പിച്ച് പരിശോധിക്കുക.
- സൈബർ സ്വച്ഛതാ കേന്ദ്രത്തിൽ നിന്ന് സൗജന്യ ബോട്ട് നീക്കംചെയ്യൽ ഉപകരണങ്ങൾ ഡൗൺലോഡ് ചെയ്യുക <https://www.csk.gov.in/security-tools.html>.
- പങ്കിട്ടതോ പൊതു ഉപകരണങ്ങളോ ഉപയോഗിച്ച ശേഷം ലോഗ് ഔട്ട് ചെയ്യുക.

ഞങ്ങളെ
പിന്തുടരുക:



സൈബർ സുരക്ഷാ സംഭവങ്ങൾ incident@cert-in.org.in എന്ന വിലാസത്തിൽ റിപ്പോർട്ട് ചെയ്യുക.

കൂടുതൽ സുരക്ഷാ നുറുങ്ങുകൾക്ക് സന്ദർശിക്കുക: <https://www.cert-in.org.in>, <https://www.csk.gov.in>

സുരക്ഷിത ഇന്റർനെറ്റ് ദിനം

ഓഫീസ് ഉപയോക്താക്കൾക്കുള്ള മികച്ച രീതികൾ



സുരക്ഷാ നുറുങ്ങുകൾ

- ശക്തമായ പാസ്‌വേഡുകൾ ഉപയോഗിക്കുക, അവ ആരുമായും പങ്കിടരുത്.
- നിങ്ങളുടെ മേശയിൽ നിന്ന് ഇറങ്ങുമ്പോൾ കമ്പ്യൂട്ടർ ലോക്ക് ചെയ്യുക.
- അജ്ഞാത ഇമെയിൽ ലിങ്കുകളിലോ അറ്റാച്ചുമെന്റുകളിലോ ക്ലിക്ക് ചെയ്യരുത്.
- ഓഫീസ് അംഗീകൃത സോഫ്റ്റ്‌വെയറുകളും വെബ്സൈറ്റുകളും മാത്രം ഉപയോഗിക്കുക.
- സംശയാസ്പദമായ ഇമെയിലുകളോ സന്ദേശങ്ങളോ നിങ്ങളുടെ ഐടി സുരക്ഷാ ടീമിനെ ഉടൻ റിപ്പോർട്ട് ചെയ്യുക.

ഞങ്ങളെ
പിന്തുടരുക:



@IndianCERT



@cert_india

സൈബർ സുരക്ഷാ സംഭവങ്ങൾ incident@cert-in.org.in എന്ന വിലാസത്തിൽ റിപ്പോർട്ട് ചെയ്യുക.

കൂടുതൽ സുരക്ഷാ നുറുങ്ങുകൾക്ക് സന്ദർശിക്കുക: <https://www.cert-in.org.in>, <https://www.csk.gov.in>

സുരക്ഷിത ഇന്റർനെറ്റ് ദിനം

സ്ത്രീകൾക്കുള്ള മികച്ച രീതികൾ



സുരക്ഷാ നുറുങ്ങുകൾ

- സോഷ്യൽ മീഡിയ പ്രൊഫൈലുകൾ സ്വകാര്യമായി സൂക്ഷിക്കുക.
- അപരിചിതരിൽ നിന്നുള്ള സൗഹൃദ അഭ്യർത്ഥനകൾ സ്വീകരിക്കരുത്.
- ഒരിക്കലും OTP-കൾ, PIN-കൾ, പാസ്‌വേഡുകൾ എന്നിവ ആരുമായും പങ്കിടരുത്.
- ഓൺലൈൻ പീഡനം ഉടൻ റിപ്പോർട്ട് ചെയ്ത് റിപ്പോർട്ട് ചെയ്യുക.
- ഓൺലൈനിൽ ഫോട്ടോകളോ ലൊക്കേഷനോ പങ്കിടുമ്പോൾ ശ്രദ്ധിക്കുക.

ഞങ്ങളെ
പിന്തുടരുക:



@IndianCERT



@cert_india

സൈബർ സുരക്ഷാ സംഭവങ്ങൾ incident@cert-in.org.in എന്ന വിലാസത്തിൽ റിപ്പോർട്ട് ചെയ്യുക.

കൂടുതൽ സുരക്ഷാ നുറുങ്ങുകൾക്ക് സന്ദർശിക്കുക: <https://www.cert-in.org.in>, <https://www.csk.gov.in>

സുരക്ഷിത ഇന്റർനെറ്റ് ദിനം

മുതിർന്ന പൗരന്മാർക്കുള്ള മികച്ച രീതികൾ



സുരക്ഷാ നുറുങ്ങുകൾ

- ബാങ്കിംഗ് വിവരങ്ങൾ ചോദിച്ച് വരുന്ന കോളുകളെയോ സന്ദേശങ്ങളെയോ വിശ്വസിക്കരുത്.
- സോഷ്യൽ മീഡിയ ചാറ്റുകൾ വഴി ലഭിക്കുന്ന ഒരു ആപ്പും ഡൗൺലോഡ് ചെയ്യരുത്.
- ശക്തമായ പാസ്‌വേഡുകൾ ഉപയോഗിക്കുക, ആരുമായും പങ്കിടരുത്.
- "സത്യമാകാൻ വളരെ നല്ലതാണെന്ന്" തോന്നുന്ന ഓൺലൈൻ ഓഫറുകൾ ഒഴിവാക്കുക.
- ആന്റിവൈറസ് സോഫ്റ്റ്‌വെയർ ഉപയോഗിക്കുക, ഉപകരണങ്ങൾ അപ്ഡേറ്റ് ചെയ്യുക.

ഞങ്ങളെ
പിന്തുടരുക:



@IndianCERT



@cert_india

സൈബർ സുരക്ഷാ സംഭവങ്ങൾ incident@cert-in.org.in എന്ന വിലാസത്തിൽ റിപ്പോർട്ട് ചെയ്യുക.

കൂടുതൽ സുരക്ഷാ നുറുങ്ങുകൾക്ക് സന്ദർശിക്കുക: <https://www.cert-in.org.in>, <https://www.csk.gov.in>

സുരക്ഷിത ഇന്റർനെറ്റ് ദിനം

കുട്ടികൾക്കുള്ള മികച്ച രീതികൾ



സുരക്ഷാ നുറുങ്ങുകൾ

- ഓൺലൈനിൽ അപരിചിതരുമായി ഇടപഴകരുത്.
- നിങ്ങളുടെ പേര്, സ്കൂൾ, വിലാസം, ഫോട്ടോകൾ എന്നിവ ഓൺലൈനിൽ അപരിചിതരുമായി ഒരിക്കലും പങ്കിടരുത്.
- ഓൺലൈനിൽ എന്തെങ്കിലും നിങ്ങൾക്ക് അസുസ്ഥത ഉണ്ടാക്കുന്നുവെങ്കിൽ മാതാപിതാക്കളോട് പറയുക.
- കുട്ടികൾക്ക് സുരക്ഷിതമായ ആപ്ലികളും വെബ്സൈറ്റുകളും മാത്രം ഉപയോഗിക്കുക.
- അനുവാദമില്ലാതെ ഗെയിമുകളോ ആപ്ലികളോ ഡൗൺലോഡ് ചെയ്യരുത്.

ഞങ്ങളെ
പിന്തുടരുക:



സൈബർ സുരക്ഷാ സംഭവങ്ങൾ incident@cert-in.org.in എന്ന വിലാസത്തിൽ റിപ്പോർട്ട് ചെയ്യുക.

കൂടുതൽ സുരക്ഷാ നുറുങ്ങുകൾക്ക് സന്ദർശിക്കുക: <https://www.cert-in.org.in>, <https://www.csk.gov.in>

സുരക്ഷിത ഇന്റർനെറ്റ് ദിനം

പ്രത്യേക ആവശ്യങ്ങളുള്ള വ്യക്തികൾക്കുള്ള മികച്ച രീതികൾ



സുരക്ഷാ നുറുങ്ങുകൾ

- ഉപയോഗക്ഷമതയ്ക്ക് അനുയോജ്യമായ സുരക്ഷാ ഉപകരണങ്ങൾ (സ്ക്രീൻ റീഡറുകൾ, വോയ്സ് അലേർട്ടുകൾ) ഉപയോഗിക്കുക.
- വ്യക്തിഗത അല്ലെങ്കിൽ സാമ്പത്തിക വിവരങ്ങൾ ഓൺലൈനിൽ പങ്കിടരുത്.
- അജ്ഞാത സന്ദേശങ്ങൾക്ക് മറുപടി നൽകുന്നതിനുമുമ്പ് ഒരു വിശ്വസ്ത വ്യക്തിയോട് ചോദിക്കുക.
- സാധ്യമെങ്കിൽ ശക്തമായ പാസ്‌വേഡുകളും പാസ്‌വേഡ് മാനേജർ‌മാരും ഉപയോഗിക്കുക.
- സുരക്ഷാ പ്രശ്നങ്ങൾ ഒഴിവാക്കാൻ ഉപകരണങ്ങൾ അപ്ഡേറ്റ് ചെയ്ത് സൂക്ഷിക്കുക.

ഞങ്ങളെ
പിന്തുടരുക:



@IndianCERT



@cert_india

സൈബർ സുരക്ഷാ സംഭവങ്ങൾ incident@cert-in.org.in എന്ന വിലാസത്തിൽ റിപ്പോർട്ട് ചെയ്യുക.

കൂടുതൽ സുരക്ഷാ നുറുങ്ങുകൾക്ക് സന്ദർശിക്കുക: <https://www.cert-in.org.in>, <https://www.csk.gov.in>



इलेक्ट्रॉनिक्स एवं
सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF
ELECTRONICS AND
INFORMATION TECHNOLOGY



Enhancing Cyber Security in India



Information Security
Education & Awareness



ऑनलाइन सुरक्षा कचय



Digital India
Power To Empower

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

REPORT CYBER SECURITY INCIDENTS TO CERT-IN

For reporting Cyber Security Incidents to CERT-In:

Visit website: <https://www.cert-in.org.in>

Email: incident@cert-in.org.in

Toll Free Phone: [+91-1800-11-4949](tel:+91-1800-11-4949)

Toll Free Fax: [+91-1800-11-6969](tel:+91-1800-11-6969)

Information Desk

Phone: [+91-11-22902657](tel:+91-11-22902657)

For Collaboration with CERT-In in the area of Cyber Security:

Visit website: <https://www.cert-in.org.in>

Email: collaboration@cert-in.org.in

Phone: [+11-22902600](tel:+11-22902600) Ext: [1012, +91-11-24368572](tel:+91-11-24368572)

For Trainings/ Awareness programmes:

Email: training@cert-in.org.in

Official social media handles of @IndianCERT

 <https://www.facebook.com/IndianCERT/>

 <https://twitter.com/IndianCERT>

 https://www.instagram.com/cert_india/

 <https://www.linkedin.com/company/indiancert-cert-in/>

 <https://youtube.com/@indiancert>

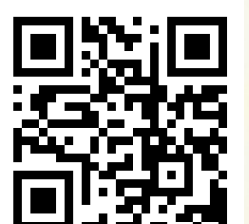


csk@cert-in.org.in

साइबर स्वच्छता केन्द्र

CYBER SWACHHTA KENDRA

Botnet Cleaning and Malware Analysis Centre



Announcements

<https://www.csk.gov.in/announcements/index.html>



Security Tools

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