

അന്താരാഷ്ട്ര വനിതാ ദിനം

എഴുതിയത്

8 മാർച്ച്, 2026

ഇന്ത്യൻ കമ്പ്യൂട്ടർ എമർജൻസി
റെസ്പോൺസ് ടീം

സ്ത്രീ സംരക്ഷണം



താൽക്കാലികമായി നിർത്തുക.
ചിന്തിക്കുക. ക്ലിക്ക് ചെയ്യുക.

സംരക്ഷിക്കാനും സുരക്ഷിതമാക്കാനും

ഉപകരണം. ഐഡന്റിറ്റി. ഡാറ്റ.
ഇൻ്റർനെറ്റിൽ

ഞങ്ങളെ
പിന്തുടരുക :

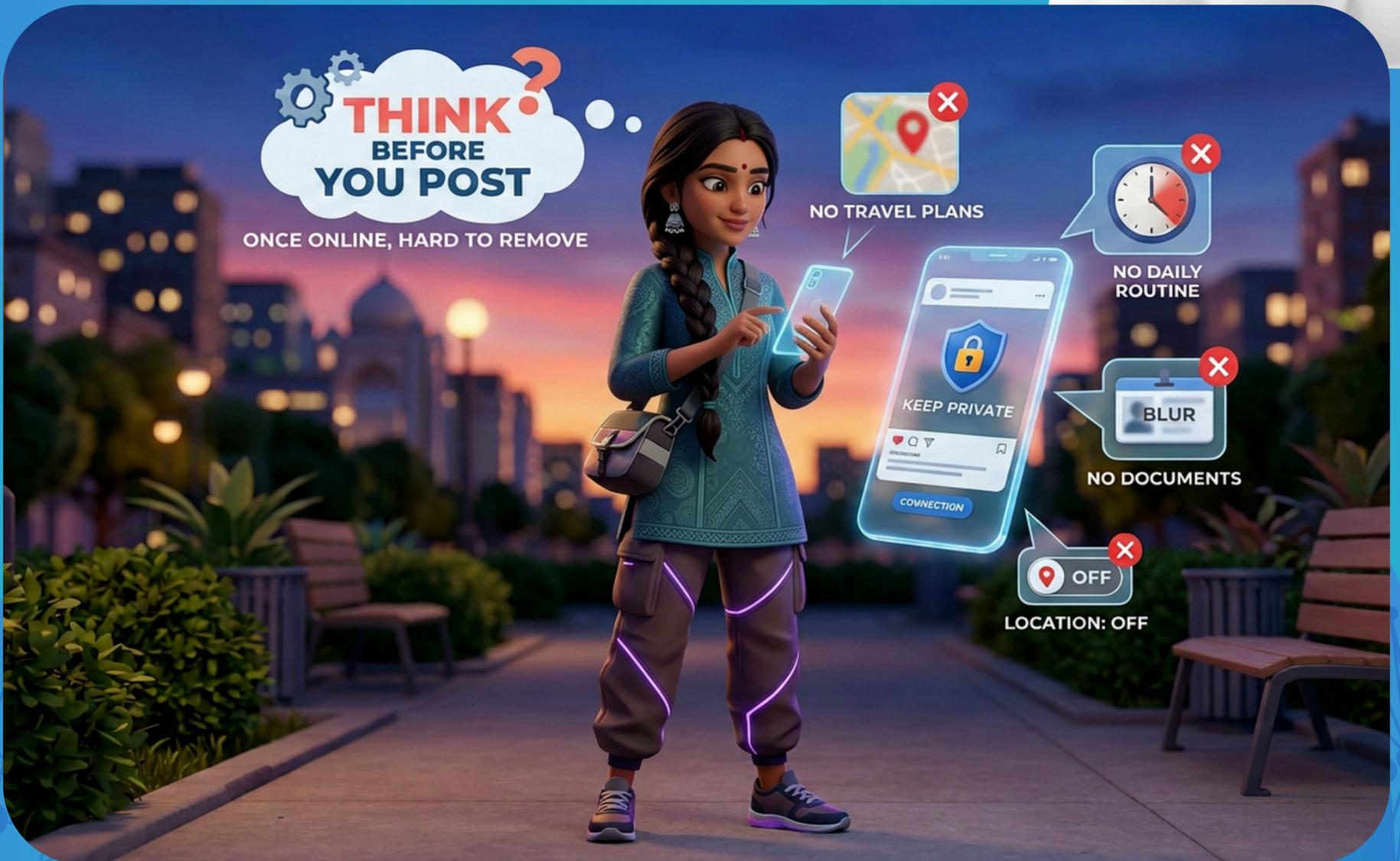


@IndianCERT



@cert_india

നിങ്ങളുടെ ഡിജിറ്റൽ കാൽപ്പാടുകൾ സൂക്ഷിക്കുക



സുരക്ഷാ നുറുങ്ങുകൾ

- പോസ്റ്റ് ചെയ്യുന്നതിന് മുമ്പ് ചിന്തിക്കുക. എന്തെങ്കിലും ഓൺലൈനായിക്കഴിഞ്ഞാൽ, അത് നീക്കം ചെയ്യാൻ പ്രയാസമാണ്.
- വ്യക്തിഗത വിവരങ്ങൾ, യാത്രാ പദ്ധതികൾ, ദൈനംദിന കാര്യങ്ങൾ എന്നിവ ഓൺലൈനിൽ പങ്കിടരുത്.
- വിശ്വസ്തരായ ആളുകൾക്ക് മാത്രം നിങ്ങളുടെ പോസ്റ്റുകൾ കാണാൻ കഴിയുന്ന തരത്തിൽ നിങ്ങളുടെ സോഷ്യൽ മീഡിയ അക്കൗണ്ടുകൾ സ്വകാര്യമായി സൂക്ഷിക്കുക.
- ആവശ്യമില്ലാത്തപ്പോൾ ലൊക്കേഷൻ പങ്കിടൽ ഓഫാക്കുക.
- പ്രധാനപ്പെട്ട രേഖകളുടെ ഫോട്ടോകൾ പോസ്റ്റ് ചെയ്യുന്നത് ഒഴിവാക്കുക.

ഞങ്ങളെ പിന്തുടരുക :



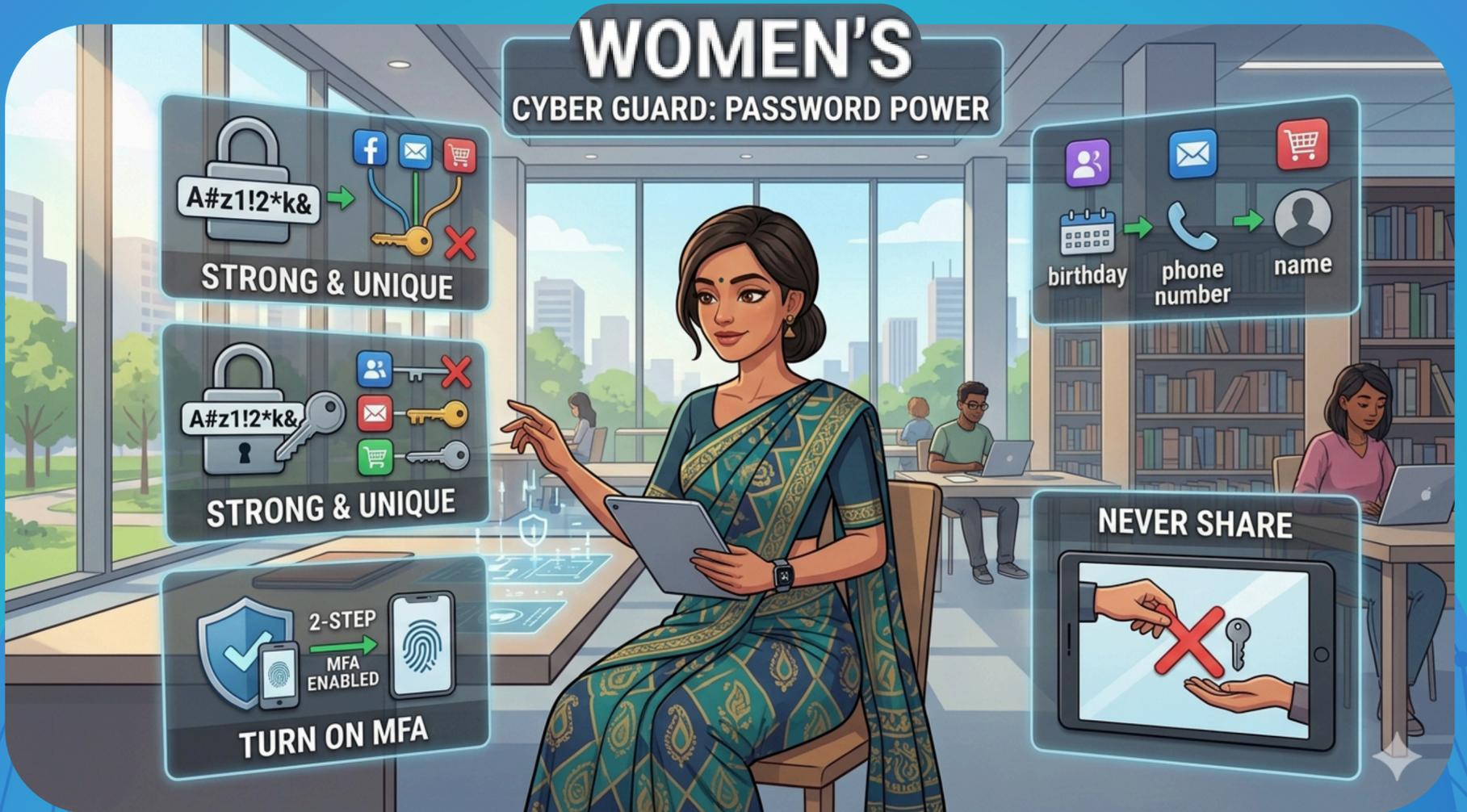
@IndianCERT



@cert_india



നിങ്ങളുടെ പാസ്‌വേഡ് കോട്ട നിർമ്മിക്കുക



സുരക്ഷാ നുറുങ്ങുകൾ

- വലിയക്ഷരങ്ങളും ചെറിയക്ഷരങ്ങളും, അക്കങ്ങളും, ചിഹ്നങ്ങളും ചേർത്ത് ഒരു നീണ്ട പാസ്‌വേഡും ശക്തമായ പാസ്‌വേഡും ഉപയോഗിക്കുക.
- നിങ്ങളുടെ പേര്, ജന്മദിനം, ഫോൺ നമ്പർ അല്ലെങ്കിൽ എളുപ്പത്തിൽ ഊഹിക്കാൻ കഴിയുന്ന പാസ്‌വേഡുകൾ ഉപയോഗിക്കരുത്.
- വ്യത്യസ്ത അക്കൗണ്ടുകൾക്ക് വ്യത്യസ്ത പാസ്‌വേഡുകൾ ഉപയോഗിക്കുക.
- സാധ്യമാകുമ്പോഴെല്ലാം മൾട്ടി ഫാക്ടർ ഓതന്റിക്കേഷൻ ഓണാക്കുക.
- നിങ്ങളുടെ പാസ്‌വേഡോ OTPയോ ഒരിക്കലും ആരുമായും പങ്കിടരുത്.

ഞങ്ങളെ പിന്തുടരുക :

f X YouTube in @IndianCERT

@cert_india



സ്മാർട്ട് ട്രാപ്പിനെ മറികടക്കൂ

WOMEN'S
CYBER GUARD: BE SECURE.



സുരക്ഷാ നുറുങ്ങുകൾ

- പണമോ ഒടിപിയോ ആവശ്യപ്പെടുന്ന അടിയന്തര സന്ദേശങ്ങളെ വിശ്വസിക്കരുത്.
- ഏതെങ്കിലും ലിങ്കിൽ ക്ലിക്ക് ചെയ്യുന്നതിന് മുമ്പ് അയച്ചയാളെ ശ്രദ്ധാപൂർവ്വം പരിശോധിക്കുക.
- എസ്എംഎസ് അല്ലെങ്കിൽ ഇമെയിൽ വഴി അയയ്ക്കുന്ന അജ്ഞാത ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യരുത്.
- ഷോർട്ട് URL-കൾ വികസിപ്പിച്ച് പരിശോധിക്കാതെ അവയിൽ ക്ലിക്ക് ചെയ്യരുത്.
- ഫോണിലൂടെയോ ഓൺലൈനിലൂടെയോ ഒരിക്കലും ബാങ്കിംഗ് വിവരങ്ങളോ സെൻസിറ്റീവ് വ്യക്തിഗത വിവരങ്ങളോ പങ്കിടരുത്.

ഞങ്ങളെ പിന്തുടരുക :



@IndianCERT



@cert_india



സ്മാർട്ട് ടാപ്പുകൾ. സുരക്ഷിതമായ ആപ്പുകൾ.



സുരക്ഷാ നുറുങ്ങുകൾ

- നിങ്ങളുടെ ഫോൺ എപ്പോഴും പിൻ, പാസ്‌വേഡ് അല്ലെങ്കിൽ വിരലടയാളം ഉപയോഗിച്ച് ലോക്ക് ചെയ്യുക.
- ഔദ്യോഗിക ആപ്പ് സ്റ്റോറുകളിൽ നിന്ന് മാത്രം ആപ്പുകൾ ഡൗൺലോഡ് ചെയ്യുക.
- അപ്ഡേറ്റുകൾ ലഭ്യമാകുമ്പോൾ നിങ്ങളുടെ ഫോൺ പതിവായി അപ്ഡേറ്റ് ചെയ്യുക.
- ആപ്പ് അനുമതികൾ പരിശോധിക്കുക, ക്യാമറയിലേക്കോ കോൺടാക്റ്റുകളിലേക്കോ അനാവശ്യ ആക്സസ് അനുവദിക്കരുത്.
- നിങ്ങൾ ഉപയോഗിക്കാത്ത ആപ്പുകൾ നീക്കം ചെയ്യുക.
- സൈബർ സ്വച്ഛതാ കേന്ദ്ര വെബ്സൈറ്റിൽ നിന്ന് സൗജന്യ ബോട്ട്നെറ്റ് നീക്കംചെയ്യൽ ഉപകരണങ്ങൾ ഡൗൺലോഡ് ചെയ്യുക:
<https://www.csk.gov.in/security-tools.html>.



സുരക്ഷിത ഡെസ്ക്, അപകടസാധ്യത ഒഴിവാക്കുക



സുരക്ഷാ നുറുങ്ങുകൾ

- നിങ്ങളുടെ മേശയിൽ നിന്ന് ഇറങ്ങുമ്പോൾ കമ്പ്യൂട്ടർ ലോക്ക് ചെയ്യുക.
- ഓഫീസ് കമ്പ്യൂട്ടറുകളിൽ അജ്ഞാത യൂഎസ്ബി ഡ്രൈവുകൾ പ്ലഗ് ചെയ്യരുത്.
- ഓഫീസ് സിസ്റ്റങ്ങളിൽ അംഗീകൃത സോഫ്റ്റ്‌വെയർ മാത്രം ഉപയോഗിക്കുക.
- ഓഫീസ് ലോഗിൻ വിവരങ്ങൾ ആരുമായും പങ്കിടരുത്.
- ജോലിസ്ഥലത്ത് ഇമെയിൽ അറ്റാച്ചുമെന്റുകൾ തുറക്കുന്നതിന് മുമ്പ് ശ്രദ്ധിക്കുക.
- സംശയാസ്പദമായ ഇമെയിലുകളോ പ്രവർത്തനങ്ങളോ ഉടൻ തന്നെ നിങ്ങളുടെ ഐടി ടീമിനെ അറിയിക്കുക.

ഞങ്ങളെ പിന്തുടരുക :

f X YouTube in @IndianCERT

Instagram @cert_india



സൈബർ സുരക്ഷാ സംഭവങ്ങൾ CERT-IN-നെ അറിയിക്കുക

സൈബർ സുരക്ഷാ സംഭവങ്ങൾ CERT-In-ൽ റിപ്പോർട്ട് ചെയ്യുന്നതിന്:

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

ഇമെയിൽ: incident@cert-in.org.in

ടോൾ ഫ്രീ ഫോൺ: +91-1800-11-4949

ടോൾ ഫ്രീ ഫാക്സ്: +91-1800-11-6969

ഇൻഫർമേഷൻ ഡെസ്ക്

ഫോൺ: +91-11-22902657

ഞങ്ങളെ
പിന്തുടരുക :



@IndianCERT



@cert_india



<https://cert-in.org.in/>

साइबर स्वच्छता केन्द्र

CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre



ബോധവൽക്കരണ ലഘുലേഖ
<https://cert-in.org.in/AwarenessBooklets.jsp>



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