इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

certin
Enhancing Cyber Security in India

ISEA
Information Security Education & Awareness

Digital India
Power To Empower

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

AI അവബോധ ഗൈഡ്

സൈബർ ശുചിത്വ സംസ്കാരം വളർത്തിയെടുക്കുക

#സൈബർ ശുചിത്വംനമ്മുടെ സംസ്കാരം



ദേശീയ സൈബർ സുരക്ഷാ ബോധവൽക്കരണ മാസം (ഒക്ടോബർ 2026)

പ്രസാധകർ

ഇന്ത്യൻ കമ്പ്യൂട്ടർ അടിയന്തര പ്രതികരണ സംഘം

ഞങ്ങളെ പിന്തുടരുക:

@IndianCERT

@cert_india

ഉള്ളടക്ക പട്ടിക

ആമുഖം 3

AI- മെച്ചപ്പെടുത്തിയ ഫിഷിംഗും സോഷ്യൽ എഞ്ചിനീയറിംഗും 4

വോയ്സ് & വീഡിയോ ഡീപ്ഫേക്കുകൾ (വിഷിംഗ്) 5

AI- സഹായത്തോടെയുള്ള മാൽവെയറും ഓട്ടോമേറ്റഡ് ആക്രമണങ്ങളും 6

വ്യാജ വെബ്സൈറ്റുകളും ഐഡന്റിറ്റി മോഷണവും 7

റെഡ് ഫ്ലാഗുകൾ ചെക്ക്ലിസ്റ്റ് 8

ഓൺലൈൻ സുരക്ഷ 9

ഉപകരണ സുരക്ഷ 10

ഉത്തരവാദിത്തത്തോടെ AI ഉപയോഗിക്കുക 11

വിശ്വസനീയ ആപ്പുകൾ തിരഞ്ഞെടുക്കുക 12

സൈബർ സുരക്ഷാ സംഭവങ്ങൾ CERT-In-ൽ റിപ്പോർട്ട് ചെയ്യുക. 13

ആമുഖം

നമ്മുടെ ജീവിതരീതി, ജോലി രീതി, ആശയവിനിമയം എന്നിവയെ കൃത്രിമബുദ്ധി (AI) പരിവർത്തനം ചെയ്യുകയാണ്. ഇത് നവീകരണം സാധ്യമാക്കുകയും ഉൽപ്പാദനക്ഷമത മെച്ചപ്പെടുത്തുകയും വ്യത്യസ്ത മേഖലകളിലെ സങ്കീർണ്ണമായ പ്രശ്നങ്ങൾ പരിഹരിക്കാൻ സഹായിക്കുകയും ചെയ്യുന്നു. എന്നിരുന്നാലും, കൂടുതൽ നൂതനവും ബോധ്യപ്പെടുത്തുന്നതുമായ സൈബർ ഭീഷണികൾ സൃഷ്ടിക്കുന്നതിന് ഭീഷണി ഘടകങ്ങൾ ഇതേ സാങ്കേതികവിദ്യ ദുരുപയോഗം ചെയ്യുന്നു.

ഡിജിറ്റൽ ഭീഷണികളെ തിരിച്ചറിയുന്നത് AI കൂടുതൽ ബുദ്ധിമുട്ടാക്കുന്നു, കാരണം ആക്രമണകാരികൾക്ക് ഇപ്പോൾ വളരെ യാഥാർത്ഥ്യബോധമുള്ള ഇമെയിലുകൾ, സന്ദേശങ്ങൾ, ഓഡിയോ, വീഡിയോകൾ, വെബ്സൈറ്റുകൾ എന്നിവ സൃഷ്ടിക്കാൻ കഴിയും. വ്യാകരണ വൈകല്യം, അസാധാരണമായ ഫോർമാറ്റിംഗ് അല്ലെങ്കിൽ വ്യക്തമായ തെറ്റുകൾ പോലുള്ള പരമ്പരാഗത മുന്നറിയിപ്പ് അടയാളങ്ങൾ ഇനി വിശ്വസനീയമായ സൂചകങ്ങളായിരിക്കില്ല. സ്ഥിരീകരണവും ഉത്തരവാദിത്തമുള്ള ഡിജിറ്റൽ രീതികളും എന്നത്തേക്കാളും പ്രധാനമാണ്.

നമ്മൾ ദിവസവും ഉപയോഗിക്കുന്ന AI ഉപകരണങ്ങളും സ്മാർട്ട് ഉപകരണങ്ങളും ശ്രദ്ധാപൂർവ്വം ഉപയോഗിച്ചില്ലെങ്കിൽ പുതിയ സ്വകാര്യത, സുരക്ഷാ അപകടസാധ്യതകൾ സൃഷ്ടിച്ചേക്കാം. വിശ്വസനീയമല്ലാത്ത AI ആപ്ലിക്കേഷനുകളുമായി വ്യക്തിഗതമോ രഹസ്യാത്മകമോ ആയ വിവരങ്ങൾ പങ്കിടുന്നത്, അനാവശ്യമായ അനുമതികൾ നൽകുന്നത്, അല്ലെങ്കിൽ സ്ഥിരീകരണമില്ലാതെ AI സൃഷ്ടിച്ച വിവരങ്ങളെ ആശ്രയിക്കുന്നത് എന്നിവ വ്യക്തികളെയും സ്ഥാപനങ്ങളെയും സുരക്ഷാ അപകടസാധ്യതകളിലേക്ക് നയിച്ചേക്കാം.

"AI സൈബർ അവബോധത്തെ"ക്കുറിച്ചുള്ള ഇന്ത്യൻ കമ്പ്യൂട്ടർ എമർജൻസി റെസ്പോൺസ് ടീം (CERT-In) തയ്യാറാക്കിയ ഈ ലഘുലേഖ, സൈബർ സുരക്ഷാ പ്രൊഫഷണലുകൾക്ക് മാത്രമല്ല, ദൈനംദിന പൗരന്മാർക്കും, ജീവനക്കാർക്കും, ഡിജിറ്റൽ ഉപയോക്താക്കൾക്കും വേണ്ടി രൂപകൽപ്പന ചെയ്തിരിക്കുന്നു. AI ഡിജിറ്റൽ ഭീഷണിയുടെ ഭൂപ്രകൃതിയെ എങ്ങനെ മാറ്റുന്നുവെന്ന് ഇത് വിശദീകരിക്കുകയും വ്യക്തിഗത വിവരങ്ങൾ, ഉപകരണങ്ങൾ, ഓൺലൈൻ ഐഡന്റിറ്റി എന്നിവ സംരക്ഷിക്കുന്നതിന് എല്ലാവർക്കും പിന്തുടരാവുന്ന ലളിതവും പ്രായോഗികവുമായ നടപടികൾ നൽകുകയും ചെയ്യുന്നു.

AI- മെച്ചപ്പെടുത്തിയ ഫിഷിംഗും സോഷ്യൽ എഞ്ചിനീയറിംഗും



ഇത് എങ്ങനെ പ്രവർത്തിക്കുന്നു ?

ഭീഷണി മുഴക്കുന്നവർ ഇപ്പോൾ യഥാർത്ഥവും പിശകുകളില്ലാത്തതുമായ ഇമെയിലുകളും ടെക്സ്റ്റുകളും അയയ്ക്കുന്നു. സന്ദേശങ്ങൾ വ്യക്തിപരമാക്കാൻ അവർ നിങ്ങളുടെ ജോലി, നിങ്ങൾ ഉപയോഗിക്കുന്ന സേവനങ്ങൾ അല്ലെങ്കിൽ സമീപകാല പ്രവർത്തനങ്ങൾ പോലുള്ള നിങ്ങളെക്കുറിച്ചുള്ള വിശദാംശങ്ങൾ ഉപയോഗിക്കുന്നു. ഈ സന്ദേശങ്ങൾ നന്നായി എഴുതിയിരിക്കുന്നതിനാൽ, സൈബർ ഭീഷണികൾ കണ്ടെത്താൻ വളരെ ബുദ്ധിമുട്ടായിരിക്കും.

എങ്ങനെ തിരിച്ചറിയാം?

- സന്ദേശം നിങ്ങൾക്ക് വളരെ പ്രത്യേകമായി തോന്നുന്നു, പക്ഷേ അപ്രതീക്ഷിതമായി എത്തിച്ചേരുന്നു.
- അത് ഒരു അടിയന്തര അല്ലെങ്കിൽ ഭീഷണി സ്വരത്തിൽ സംസാരിക്കുകയും ഉടനടി നടപടി ആവശ്യപ്പെടുകയും ചെയ്യുന്നു.
- ഒരു ലിങ്കിൽ ക്ലിക്ക് ചെയ്യാനോ, ഒരു അക്കൗണ്ട് പരിശോധിക്കാനോ, ഒരു പാസ്‌വേഡ് പുനഃസജ്ജമാക്കാനോ, അല്ലെങ്കിൽ ഒരു പേയ്മെന്റ് നടത്താനോ അത് നിങ്ങളോട് ആവശ്യപ്പെടുന്നു.
- അയച്ചയാളുടെ വിലാസം ഏതാണ്ട് ശരിയാണെന്ന് തോന്നുന്നു, പക്ഷേ പൂർണ്ണമായും ശരിയല്ല.

എങ്ങനെ സുരക്ഷിതരായിരിക്കാം?

- ആവശ്യപ്പെടാത്ത സന്ദേശങ്ങളിലെ ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യരുത്. പകരം നേരിട്ട് ഔദ്യോഗിക വെബ്സൈറ്റിലേക്കോ ആപ്പിലേക്കോ പോകുക.
- ഔദ്യോഗിക ഫോൺ നമ്പർ അല്ലെങ്കിൽ ആപ്പ് പോലുള്ള ഒരു പ്രത്യേക, വിശ്വസനീയ കോൺടാക്റ്റ് ചാനൽ വഴി അഭ്യർത്ഥനകൾ പരിശോധിച്ചുറപ്പിക്കുക.
- ഒരു സന്ദേശ ലിങ്ക് വഴി എത്തുന്ന പേജിൽ ഒരിക്കലും ക്രെഡൻഷ്യലുകളോ OTP-കളോ നൽകരുത്.
- സംശയാസ്പദമായ സന്ദേശങ്ങൾ റിപ്പോർട്ട് ചെയ്ത് അവ നിർത്തുക, തുടർന്ന് അയച്ചയാളെ തടയുക.

ഞങ്ങളെ പിന്തുടരുക: @IndianCERT @cert_india

വോയ്സ് & വീഡിയോ ഡീപ്ഫേക്കുകൾ [വിഷിംഗ്]



ഇത് എങ്ങനെ പ്രവർത്തിക്കുന്നു ?

ഭീഷണിപ്പെടുത്തുന്നവർക്ക് ശബ്ദങ്ങൾ ക്ലോൺ ചെയ്യാനോ യഥാർത്ഥമായി തോന്നിക്കുന്ന വ്യാജ വീഡിയോകൾ സൃഷ്ടിക്കാനോ കഴിയും. അവർ കുടുംബാംഗങ്ങളായോ സഹപ്രവർത്തകരായോ ഉദ്യോഗസ്ഥരായോ വേഷമിട്ട് തന്ത്രപ്രധാനമായ വിവരങ്ങൾ പങ്കിടാനോ പണം അയയ്ക്കാനോ വേഗത്തിൽ നടപടിയെടുക്കാനോ നിങ്ങളെ സമ്മർദ്ദത്തിലാക്കിയേക്കാം.

എങ്ങനെ തിരിച്ചറിയാം?

- അസാധാരണമായ അടിയന്തിരാവസ്ഥ, പരിഭ്രാന്തി, അല്ലെങ്കിൽ ആരോടും പറയരുത് പോലുള്ള രഹസ്യ അഭ്യർത്ഥനകൾ.
- അല്പം വ്യത്യസ്തമായ ടോൺ, വേഗത, പശ്ചാത്തല ശബ്ദം അല്ലെങ്കിൽ ഓഡിയോ നിലവാരം.
- സാധാരണ സ്ഥിരീകരണ അല്ലെങ്കിൽ അംഗീകാര പ്രക്രിയകൾ മറികടക്കാനുള്ള അഭ്യർത്ഥനകൾ.
- ഗിഫ്റ്റ് കാർഡുകൾ, ക്രിപ്റ്റോകറൻസി അല്ലെങ്കിൽ ബാങ്ക് മുഖേനയുള്ള വഴിയുള്ള പേയ്മെന്റിനുള്ള അഭ്യർത്ഥനകൾ.

എങ്ങനെ സുരക്ഷിതരായിരിക്കാം?

- ഫോൺ കട്ട് ചെയ്ത്, ആ വ്യക്തിയുടെ അറിയപ്പെടുന്ന, സേവ് ചെയ്ത നമ്പർ ഉപയോഗിച്ച് തിരികെ വിളിക്കുക.
- അടിയന്തര ഘട്ടങ്ങളിൽ ഐഡന്റിറ്റി പരിശോധിക്കാൻ കുടുംബത്തിലോ ജോലിസ്ഥലത്തോ സുരക്ഷിതമായ ഒരു വാക്ക് സജ്ജമാക്കുക.
- ഒരു കോളിന്റെയോ വീഡിയോയുടെയോ അടിസ്ഥാനത്തിൽ മാത്രം ഒരിക്കലും പേയ്മെന്റുകൾക്ക് അംഗീകാരം നൽകരുത്. പ്രത്യേക ചാനൽ വഴി രേഖാമൂലം സ്ഥിരീകരിക്കുക.
- പ്രതികരിക്കുന്നതിന് മുമ്പ് താൽക്കാലികമായി നിർത്തുക. നിങ്ങളുടെ വിധിന്യായത്തെ മങ്ങിക്കാൻ ഭീഷണി നടത്തുന്നവർ പരിഭ്രാന്തിയെ ആശ്രയിക്കുന്നു.

ഞങ്ങളെ പിന്തുടരുക: @IndianCERT @cert_india

AI- സഹായത്തോടെയുള്ള മാൽവെയറും ഓട്ടോമേറ്റഡ് ആക്രമണങ്ങളും



ഇത് എങ്ങനെ പ്രവർത്തിക്കുന്നു ?

ഭീഷണി നടത്തുന്നവർ ക്ഷുദ്ര കോഡ് സൃഷ്ടിക്കുന്നതിനോ മറയ്ക്കുന്നതിനോ, ഒന്നിലധികം സൈറ്റുകളിൽ മോഷ്ടിച്ച പാസ്‌വേഡുകൾ പരിശോധിക്കുന്നതിനോ, അപ്‌ഡേറ്റുകൾ ആവശ്യമുള്ള സിസ്റ്റങ്ങളെ തിരിച്ചറിയുന്നതിനോ AI ഉപകരണങ്ങൾ ഉപയോഗിക്കുന്നു. ഇത് ആക്രമണങ്ങളെ വേഗത്തിലാക്കാനും കൂടുതൽ വ്യാപകമാക്കാനും സഹായിക്കുന്നു.

എങ്ങനെ തിരിച്ചറിയാം?

- അപ്രതീക്ഷിത ലോഗിൻ അലേർട്ടുകൾ, പാസ്‌വേഡ് റീസെറ്റ് ഇമെയിലുകൾ, അല്ലെങ്കിൽ നിങ്ങൾ അഭ്യർത്ഥിക്കാത്ത MFA നിർദ്ദേശങ്ങൾ
- നിങ്ങളുടെ അക്കൗണ്ട് പ്രവർത്തനത്തിൽ ലിസ്റ്റ് ചെയ്തിട്ടുള്ള അപരിചിതമായ ഉപകരണങ്ങളോ സെഷനുകളോ
- ആന്റിവൈറസ് മുന്നറിയിപ്പുകൾ, പോപ്പ്-അപ്പുകൾ, അല്ലെങ്കിൽ അസാധാരണമായി ഉപകരണ പ്രകടനം മന്ദഗതിയിലാക്കൽ
- നിങ്ങൾക്ക് തിരിച്ചറിയാൻ കഴിയാത്ത ഫയലുകൾ, ക്രമീകരണങ്ങൾ അല്ലെങ്കിൽ ബ്രൗസർ വിപുലീകരണങ്ങൾ

എങ്ങനെ സുരക്ഷിതരായിരിക്കാം?

- ഓരോ അക്കൗണ്ടിനും ഒരു സവിശേഷവും ശക്തവുമായ പാസ്‌വേഡ് ഉപയോഗിക്കുക.
- എല്ലാ പ്രധാനപ്പെട്ട അക്കൗണ്ടുകളിലും മൾട്ടി ഫാക്ടർ ഓതന്റിക്കേഷൻ (എംഎഫ്എ) പ്രാപ്തമാക്കുക.
- ആന്റിവൈറസ് സോഫ്റ്റ്‌വെയർ, സിസ്റ്റങ്ങൾ, ആപ്പുകൾ എന്നിവ കാലികമായി നിലനിർത്തുക.
- അപ്രതീക്ഷിത ലോഗിൻ അല്ലെങ്കിൽ എംഎഫ്എ അലേർട്ടുകളിൽ ഉടനടി നടപടിയെടുക്കുക.

വ്യാജ വെബ്സൈറ്റുകളും ഐഡന്റിറ്റി മോഷണവും



ഇത് എങ്ങനെ പ്രവർത്തിക്കുന്നു ?

നിങ്ങളുടെ ലോഗിൻ ക്രെഡൻഷ്യലുകൾ, OTP-കൾ അല്ലെങ്കിൽ പേയ്മെന്റ് വിശദാംശങ്ങൾ മോഷ്ടിക്കുന്നതിന്, ബാങ്കിംഗ് അല്ലെങ്കിൽ ഷോപ്പിംഗ് പോർട്ടലുകൾ പോലുള്ള, സമാനമായ വെബ്സൈറ്റുകളും ചാറ്റ്ബോട്ടുകളും സൃഷ്ടിച്ച് ഭീഷണിപ്പെടുത്തുന്നവർക്ക് കഴിയും. തെറ്റായ ഐഡന്റിറ്റികൾ സൃഷ്ടിക്കാൻ അവർ വ്യാജ ഫോട്ടോകളോ രേഖകളോ ഉപയോഗിച്ചേക്കാം.

എങ്ങനെ തിരിച്ചറിയാം?

- അധിക അക്ഷരങ്ങൾ, ഹൈഫനുകൾ, അല്ലെങ്കിൽ മറ്റൊരു ഡൊമെയ്ൻ അവസാനം എന്നിവ പോലുള്ള ചെറുതായി മാറ്റം വരുത്തിയ വെബ്സൈറ്റ് URL-കൾ.
- OTP-കൾ, PIN-കൾ അല്ലെങ്കിൽ പൂർണ്ണ കാർഡ് നമ്പറുകൾ ആവശ്യപ്പെടുന്ന ചാറ്റ്ബോട്ടുകൾ അല്ലെങ്കിൽ ഏജന്റുമാർ.
- പരിചിതമായ ഒരു സൈറ്റിൽ HTTPS കാണുന്നില്ല അഥവാ അസാധാരണമായ ഡിസൈൻ പൊരുത്തക്കേടുകൾ.

എങ്ങനെ സുരക്ഷിതരായിരിക്കാം?

- ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യുന്നതിനുപകരം എപ്പോഴും ഔദ്യോഗിക URL-കൾ നേരിട്ട് ടൈപ്പ് ചെയ്യുകയോ പരിശോധിച്ചുറപ്പിച്ച ബുക്ക്മാർക്കുകൾ ഉപയോഗിക്കുകയോ ചെയ്യുക.
- ഒരു ചാറ്റ്ബോട്ടുമായോ "സപ്പോർട്ട് ഏജന്റുമായോ" ഒരിക്കലും OTP-കൾ, PIN-കൾ അല്ലെങ്കിൽ പൂർണ്ണ കാർഡ് വിശദാംശങ്ങൾ പങ്കിടരുത്.
- എവിടെയെങ്കിലും ലോഗിൻ ചെയ്യുന്നതിന് മുമ്പ് HTTPS പരിശോധിക്കുകയും ഡൊമെയ്ൻ നാമം സൂക്ഷ്മമായി പരിശോധിക്കുകയും ചെയ്യുക.
- അപരിചിതമായ പ്രവർത്തനങ്ങൾക്കായി നിങ്ങളുടെ ബാങ്ക് സ്റ്റേറ്റ്മെന്റുകളും ക്രെഡിറ്റ് കാർഡ് റിപ്പോർട്ടും പതിവായി നിരീക്ഷിക്കുക.

ഞങ്ങളെ പിന്തുടരുക: @IndianCERT @cert_india

ചുവന്ന പതാകകൾക്കുള്ള ചെക്ക്‌ലിസ്റ്റ്

AI- പ്രാപ്തമാക്കിയ ആക്രമണത്തിന്റെ ഈ ലക്ഷണങ്ങൾക്കായി ശ്രദ്ധിക്കുക:

- പണത്തിനോ, യോഗ്യതാപത്രങ്ങൾക്കോ, അംഗീകാരത്തിനോ വേണ്ടിയുള്ള അടിയന്തര, സമ്മർദ്ദപരമായ അഭ്യർത്ഥന.
- "അറിയപ്പെടുന്ന" വ്യക്തിയിൽ നിന്നുള്ള കോളിലോ വീഡിയോയിലോ നേരിയ ഓഡിയോ/വീഡിയോ പൊരുത്തക്കേടുകൾ
- സാധാരണ പരിശോധന/അംഗീകാര നടപടിക്രമങ്ങൾ മറികടക്കാനുള്ള അഭ്യർത്ഥന.
- പരിചിതമല്ലാത്ത സെൻഡർ ഡൊമെയ്ൻ അല്ലെങ്കിൽ ചെറുതായി മാറ്റം വരുത്തിയ URL
- നിങ്ങൾ അഭ്യർത്ഥിക്കാത്ത അപ്രതീക്ഷിത MFA പ്രോംപ്റ്റുകൾ അല്ലെങ്കിൽ OTP-കൾ
- സുരക്ഷാ സോഫ്റ്റ്‌വെയർ പ്രവർത്തനരഹിതമാക്കാനോ അനൗദ്യോഗിക ലിങ്കുകൾ വഴി "പരിശോധിക്കാനോ" അഭ്യർത്ഥനകൾ.
- മുൻകൂർ പണമടയ്ക്കൽ അല്ലെങ്കിൽ വ്യക്തിഗത സാമ്പത്തിക വിവരങ്ങൾ ആവശ്യമുള്ള ജോലി/നിക്ഷേപ ഓഫറുകൾ.

സംശയമുണ്ടെങ്കിൽ — താൽക്കാലികമായി ശാന്തമായി ചിന്തിക്കുക, സ്വതന്ത്രമായി പരിശോധിക്കുക, സമ്മർദ്ദത്തിന് വഴങ്ങി പ്രവർത്തിക്കരുത്.

ഞങ്ങളെ പിന്തുടരുക: @IndianCERT @cert_india

ഓൺലൈൻ സുരക്ഷ



നിങ്ങളുടെ അക്കൗണ്ടുകൾ പരിരക്ഷിക്കുക

- ഓരോ അക്കൗണ്ടിനും ശക്തവും അതുല്യവുമായ പാസ്‌വേഡുകൾ ഉപയോഗിക്കുക; അവ സുരക്ഷിതമായി സൂക്ഷിക്കാൻ ഒരു പാസ്‌വേഡ് മാനേജർ ഉപയോഗിക്കുക.
- ലഭ്യമാകുന്നിടത്തെല്ലാം മൾട്ടി-ഫാക്ടർ ഓതന്റിക്കേഷൻ (എംഎഫ്എ) പ്രാപ്തമാക്കുക.
- ഒരിക്കലും OTP-കൾ, PIN-കൾ, പാസ്‌വേഡുകൾ അല്ലെങ്കിൽ സുരക്ഷാ കോഡുകൾ ആരുമായും പങ്കിടരുത്.
- ഒരു അധിക സുരക്ഷാ പാളിയായി ബയോമെട്രിക് പ്രാമാണീകരണം (വിരലടയാളം/മുഖം തിരിച്ചറിയൽ) ഉപയോഗിക്കുക.

ഇമെയിലും ഇന്റർനെറ്റും ഉപയോഗിക്കുമ്പോൾ സുരക്ഷിതരായിരിക്കുക

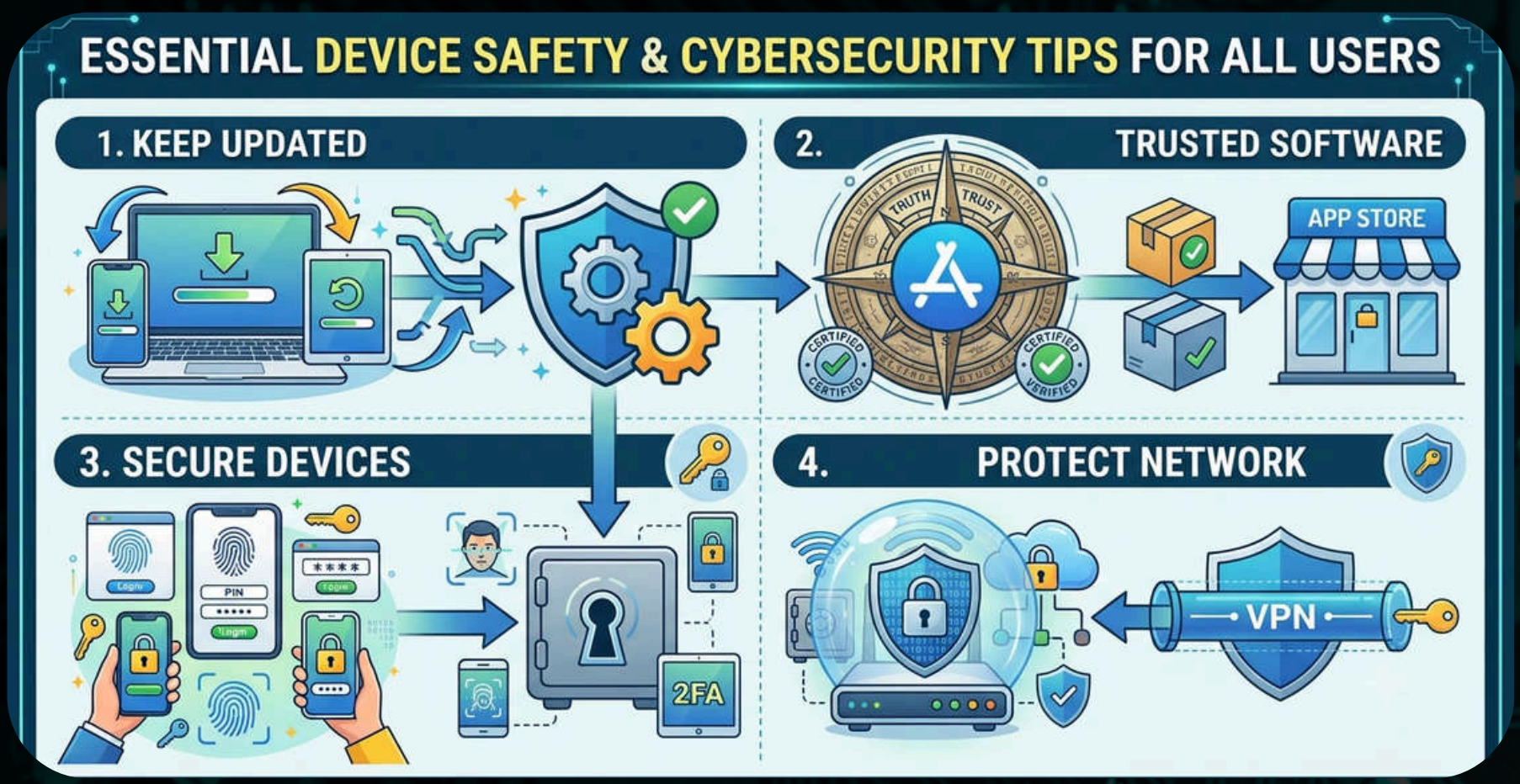
- സംശയാസ്പദമായതോ സമാനമായതോ ആയ ഇമെയിൽ വിലാസങ്ങൾക്കായി അയച്ചയാളുടെ വിശദാംശങ്ങൾ ശ്രദ്ധാപൂർവ്വം പരിശോധിക്കുക.
- ക്ലിക്ക് ചെയ്യുന്നതിനു മുമ്പ് ലിങ്കുകൾ പരിശോധിച്ചുറപ്പിക്കുക, അപ്രതീക്ഷിത അറ്റാച്ചുമെന്റുകൾ തുറക്കുന്നത് ഒഴിവാക്കുക.
- ലോഗിൻ അല്ലെങ്കിൽ സാമ്പത്തിക വിശദാംശങ്ങൾ നൽകുന്നതിനുമുമ്പ് വെബ്സൈറ്റ് ആധികാരികത സ്ഥിരീകരിക്കുക.
- സംശയമുണ്ടെങ്കിൽ, നടപടിയെടുക്കുന്നതിന് മുമ്പ് സാവധാനം പരിശോധിക്കുക.

എന്തെങ്കിലും തെറ്റ് സംഭവിക്കുന്നതിന് മുമ്പ് തയ്യാറാകൂ

- പ്രധാനപ്പെട്ട ഫയലുകളുടെ പതിവ് ബാക്കപ്പുകൾ സൂക്ഷിക്കുക, അവ ഓഫ്‌ലൈനിലോ സുരക്ഷിതമായ ക്ലൗഡ് സേവനത്തിലോ സൂക്ഷിക്കുക.
- അക്കൗണ്ട് വീണ്ടെടുക്കൽ വിവരങ്ങൾ (ഇമെയിൽ/ഫോൺ) അപ്ഡേറ്റ് ചെയ്ത് സുരക്ഷിതമായി സൂക്ഷിക്കുക.

ഞങ്ങളെ പിന്തുടരുക:
@IndianCERT
@cert_india

ഉപകരണ സുരക്ഷ



ഉപകരണങ്ങൾ അപ്ഡേറ്റ് ആയി നിലനിർത്തുക

- അറിയപ്പെടുന്ന അപകടസാധ്യതകൾ പരിഹരിക്കുന്നതിന് ഓപ്പറേറ്റിംഗ് സിസ്റ്റങ്ങൾ, ആപ്ലിക്കേഷനുകൾ, ബ്രൗസറുകൾ, സുരക്ഷാ സോഫ്റ്റ്വെയർ എന്നിവ പതിവായി അപ്ഡേറ്റ് ചെയ്യുക.
- സാധ്യമാകുന്നിടത്തെല്ലാം ഓട്ടോമാറ്റിക് അപ്ഡേറ്റുകൾ പ്രാപ്തമാക്കുക.

വിശ്വസനീയ സോഫ്റ്റ്വെയർ മാത്രം ഇൻസ്റ്റാൾ ചെയ്യുക

- യഥാർത്ഥ സോഫ്റ്റ്വെയർ ഉപയോഗിക്കുക, ഔദ്യോഗിക ആപ്പ് സ്റ്റോറുകളിൽ നിന്നോ വിശ്വസനീയമായ ഉറവിടങ്ങളിൽ നിന്നോ മാത്രം ആപ്ലിക്കേഷനുകൾ ഇൻസ്റ്റാൾ ചെയ്യുക.
- വിശ്വസനീയമായ ആന്റിവൈറസോ സുരക്ഷാ പരിഹാരങ്ങളോ ഉപയോഗിക്കുക, അവ അപ്ഡേറ്റ് ചെയ്ത് നിലനിർത്തുക.

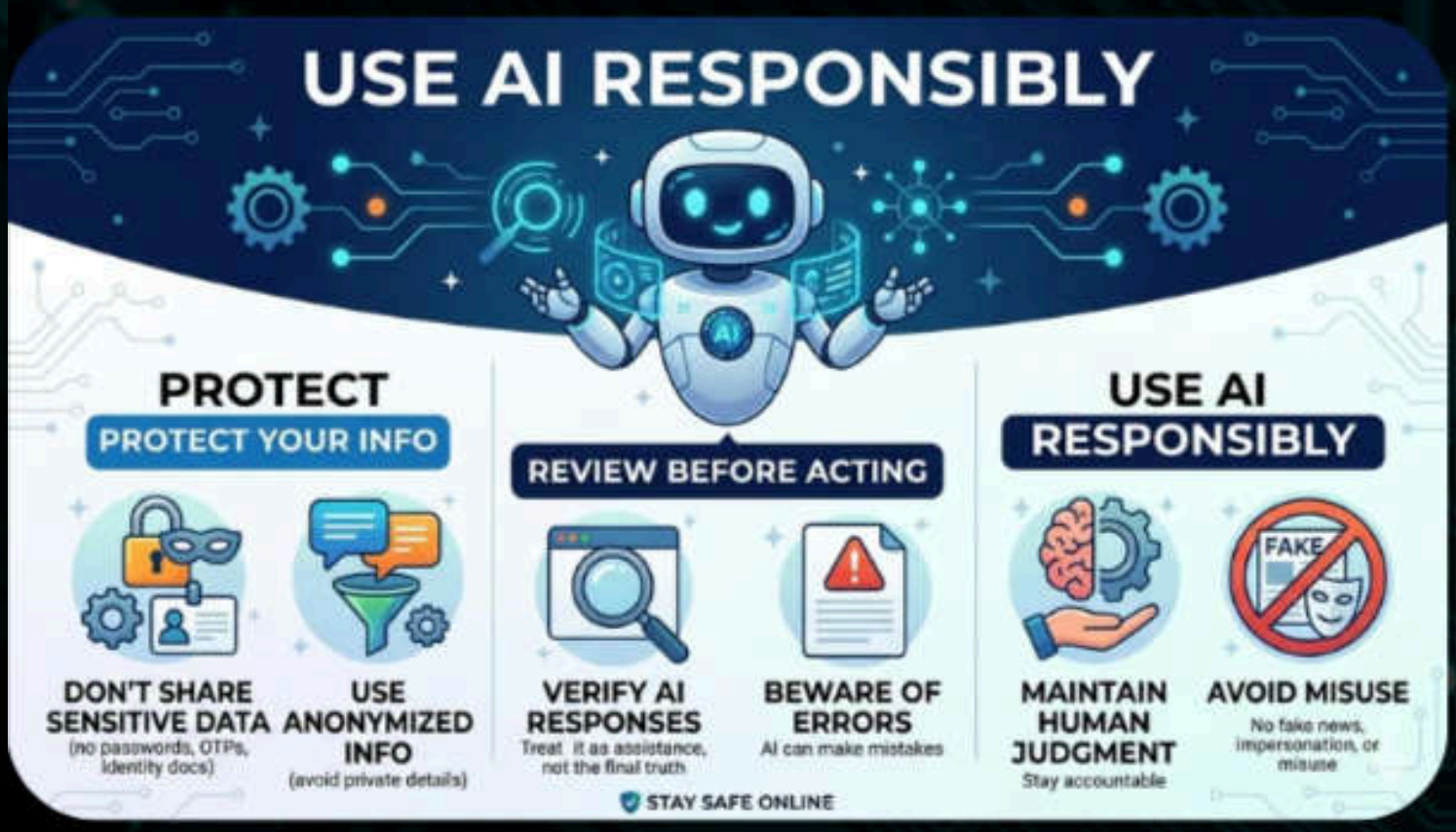
നിങ്ങളുടെ ഉപകരണങ്ങളും അക്കൗണ്ടുകളും സുരക്ഷിതമാക്കുക

- എല്ലാ ഉപകരണങ്ങളിലും ശക്തമായ പാസ്വേഡുകളോ സ്ക്രീൻ ലോക്കുകളോ ഉപയോഗിക്കുക.
- ലഭ്യമാകുമ്പോഴെല്ലാം ഉപകരണ എൻക്രിപ്ഷനും സുരക്ഷാ സവിശേഷതകളും പ്രാപ്തമാക്കുക.
- അനാവശ്യ ആപ്ലിക്കേഷനുകളും അനുമതികളും അവലോകനം ചെയ്ത് നീക്കം ചെയ്യുക.

നിങ്ങളുടെ നെറ്റ്വർക്ക് കണക്ഷൻ പരിരക്ഷിക്കുക

- ശക്തമായ ഒരു പാസ്വേഡ് ഉപയോഗിച്ച് നിങ്ങളുടെ വൈഫൈ സുരക്ഷിതമാക്കുക, ഡിഫോൾട്ട് റൂട്ടർ ക്രെഡൻഷ്യലുകൾ മാറ്റുക.
- അപ്ഡേറ്റ് ചെയ്ത റൂട്ടർ ഫേംവെയറും സുരക്ഷിത നെറ്റ്വർക്ക് ക്രമീകരണങ്ങളും ഉപയോഗിക്കുക.
- സെൻസിറ്റീവ് അക്കൗണ്ടുകൾ ആക്സസ് ചെയ്യുന്നതോ സുരക്ഷിതമല്ലാത്ത നെറ്റ്വർക്കുകൾ വഴി രഹസ്യ വിവരങ്ങൾ പങ്കിടുന്നതോ ഒഴിവാക്കുക.

AI ഉത്തരവാദിത്തത്തോടെ ഉപയോഗിക്കുക



നിങ്ങളുടെ സ്വകാര്യ വിവരങ്ങൾ പരിരക്ഷിക്കുക

- പൊതു AI ഉപകരണങ്ങളിലോ അജ്ഞാത ഓൺലൈൻ സേവനങ്ങളിലോ വ്യക്തിഗത, സാമ്പത്തിക, ആരോഗ്യ, ഔദ്യോഗിക അല്ലെങ്കിൽ രഹസ്യ വിവരങ്ങൾ നൽകരുത്.
- പാസ്‌വേഡുകൾ, OTP-കൾ, അക്കൗണ്ട് നമ്പറുകൾ, തിരിച്ചറിയൽ രേഖകൾ, ഉപഭോക്തൃ ഡാറ്റ, അല്ലെങ്കിൽ സ്വകാര്യ സംഭാഷണങ്ങൾ എന്നിവ പോലുള്ള സെൻസിറ്റീവ് വിശദാംശങ്ങൾ പങ്കിടുന്നത് ഒഴിവാക്കുക.
- AI ഉപകരണങ്ങളോട് സഹായം ആവശ്യപ്പെടുമ്പോൾ അജ്ഞാതമാക്കിയതോ പൊതുവായതോ ആയ വിവരങ്ങൾ ഉപയോഗിക്കുക.

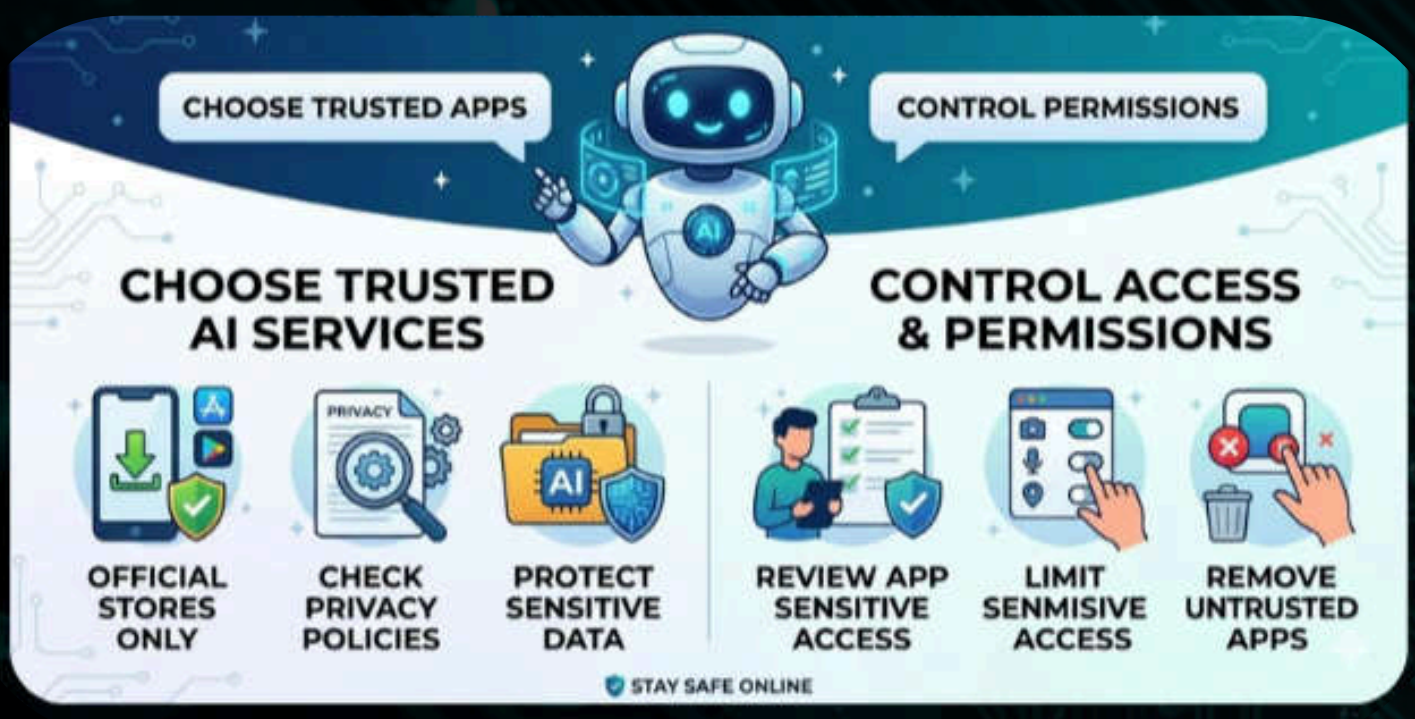
പങ്കിടുന്നതിനോ പ്രവർത്തിക്കുന്നതിനോ മുമ്പ് അവലോകനം ചെയ്യുക

- AI- സൃഷ്ടിച്ച പ്രതികരണങ്ങളെ സത്യത്തിന്റെ അന്തിമ പക്ഷഒരു, സഹായമായി കണക്കാക്കുക.
- സാമ്പത്തിക, നിയമപരമായ, പ്രൊഫഷണൽ അല്ലെങ്കിൽ വ്യക്തിപരമായ തീരുമാനങ്ങൾക്കായി ഉപയോഗിക്കുന്നതിന് മുമ്പ് പ്രധാനപ്പെട്ട വിവരങ്ങൾ പരിശോധിച്ചുറപ്പിക്കുക.
- AI ഉപകരണങ്ങൾ തെറ്റായ, അപൂർണ്ണമായ അല്ലെങ്കിൽ തെറ്റിദ്ധരിപ്പിക്കുന്ന വിവരങ്ങൾ സൃഷ്ടിച്ചേക്കാം എന്ന കാര്യം അറിഞ്ഞിരിക്കുക.

AI ഉപകരണങ്ങൾ ഉത്തരവാദിത്തത്തോടെ ഉപയോഗിക്കുക

- നിങ്ങളുടെ ജോലിയെയും പഠനത്തെയും പിന്തുണയ്ക്കാൻ AI ഉപയോഗിക്കുക, എന്നാൽ മനുഷ്യന്റെ വിധിന്യായവും ഉത്തരവാദിത്തവും നിലനിർത്തുക.
- തെറ്റായ വിവരങ്ങൾ സൃഷ്ടിക്കുന്നതിനോ പ്രചരിപ്പിക്കുന്നതിനോ, മറ്റുള്ളവരെ അനുകരിക്കുന്നതിനോ, ആരുടെയെങ്കിലും സ്വകാര്യ ഡാറ്റ ദുരുപയോഗം ചെയ്യുന്നതിനോ AI ഉപയോഗിക്കരുത്.

വിശ്വസനീയ ആപ്പുകൾ തിരഞ്ഞെടുക്കുക



ആപ്പ് ആക്സസും അനുമതികളും നിയന്ത്രിക്കുക

- AI ആപ്ലിക്കേഷനുകൾക്കും ഡിജിറ്റൽ അസിസ്റ്റന്റുകൾക്കും നൽകിയിട്ടുള്ള അനുമതികൾ പുനഃപരിശോധിക്കുക.
- ക്യാമറ, മൈക്രോഫോൺ, കോൺടാക്റ്റുകൾ അല്ലെങ്കിൽ ലൊക്കേഷൻ പോലുള്ള സവിശേഷതകളിലേക്ക് ആവശ്യമുള്ളപ്പോൾ മാത്രം ആക്സസ് അനുവദിക്കുക.
- വിശ്വസനീയമല്ലാത്ത ഉറവിടങ്ങളിൽ നിന്ന് അനാവശ്യ അനുമതികൾ നീക്കം ചെയ്യുകയും ആപ്പുകൾ അൺഇൻസ്റ്റാൾ ചെയ്യുകയും ചെയ്യുക.

വിശ്വസനീയമായ AI സേവനങ്ങൾ തിരഞ്ഞെടുക്കുക

- പ്രശസ്ത ദാതാക്കളിൽ നിന്നുള്ള AI ആപ്ലിക്കേഷനുകൾ ഉപയോഗിക്കുക, ഔദ്യോഗിക ആപ്പ് സ്റ്റോറുകളിൽ നിന്ന് മാത്രം ഡൗൺലോഡ് ചെയ്യുക.
- AI സേവനങ്ങൾ ഉപയോഗിക്കുന്നതിന് മുമ്പ് സ്വകാര്യതാ ക്രമീകരണങ്ങൾ, ഉപയോഗ നിബന്ധനകൾ, ഡാറ്റ കൈകാര്യം ചെയ്യൽ രീതികൾ എന്നിവ അവലോകനം ചെയ്യുക.
- സുരക്ഷാ നിയന്ത്രണങ്ങൾ പരിശോധിച്ചുറപ്പിച്ചിട്ടില്ലെങ്കിൽ, സെൻസിറ്റീവ് അക്കൗണ്ടുകളിലേക്കോ ഫയലുകളിലേക്കോ AI ഉപകരണങ്ങൾ ബന്ധിപ്പിക്കുന്നത് ഒഴിവാക്കുക.

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

certin Enhancing Cyber Security in India

ISEA Information Security Education & Awareness

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

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***

Toll Free Fax: ***+91-1800-11-6969***

Information Desk

Phone: ***+91-11-22902657***

Follow us :

@IndianCERT

@cert_india

WEBSITE
https://www.cert-in.org.in/

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

Awareness Booklet
https://cert-in.org.in/AwarenessBooklets.jsp

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