15 -ാം കേരള നിയമസഭ

12 -ാം സമ്മേളനം

നക്ഷത്രചിഹ്നമിട്ട ചോദ്യം നം. 179 **14-10-2024 - ൽ മറുപടിയ്ക്ക്**

സൈബർ കുറ്റകൃത്യങ്ങൾക്കെതിരെയുള്ള നടപടി

ചോദ്യം		ഉത്തരം	
ശ്രീ പി എസ് സുപാൽ, ശ്രീ. വി. ആർ. സുനിൽകുമാർ, ശ്രീമതി സി. കെ. ആശ, ശ്രീ. പി. ബാലചന്ദ്രൻ		**ശ്രീ. പിണറായി വിജയൻ (മുഖ്യമന്ത്രി)**	
(എ)	ഡിജിറ്റൽ സൗകര്യങ്ങൾ വർദ്ധിക്കുകയും ഡിജിറ്റൽ ഇടപാടുകൾ കൂടുതലായി ജനങ്ങളിലേക്ക് വ്യാപിക്കുകയും ചെയ്യുന്ന സാഹചര്യത്തിൽ പ്രസ്തുത ഇടപാടുകളുടെ ഉപയോഗത്തിൽ സൈബർ സുരക്ഷ ഉറപ്പുവരുത്തേണ്ടതിന്റെ ആവശ്യകത ശ്രദ്ധയിൽപ്പെട്ടിട്ടുണ്ടോ; വ്യക്തമാക്കുമോ;	(എ)	ഉണ്ട്. അനുദിനം വികസിച്ചുവരുന്ന വിവര സാങ്കേതിക വിദ്യയ്ക്കൊപ്പം, അവ ദുരുപയോഗം ചെയ്യുള്ള സാമ്പത്തിക തട്ടിപ്പുകളും സൈബർ കുറ്റകൃത്യങ്ങളും രാജ്യത്ത് ക്രമാതീതമായി വർദ്ധിക്കുന്നുണ്ട്. അത്തരം കുറ്റകൃത്യങ്ങൾക്കെതിരെ ശക്തമായ നടപടികൾ സ്വീകരിക്കുന്നതിന് 05.01.2024-ലെ സ.ഉ(കൈ) നം. 04/2024/ആഭ്യന്തരം നമ്പർ ഉത്തരവ് പ്രകാരം സംസ്ഥാനത്ത് സൈബർ പോലീസ് ഡിവിഷൻ ആരംഭിച്ചു. **സൈബർ പോലീസ് ഡിവിഷൻ:** സൈബർ കുറ്റകൃത്യങ്ങളെ നേരിടുന്നതിനും അവ വിശകലനം ചെയ്ത് കുറ്റകൃത്യങ്ങൾക്ക് ഇടയാക്കുന്ന വസ്തുതകൾ കണ്ടെത്തി ഇല്ലായ്മ ചെയ്യുന്നതിനും, സൈബർ സംബന്ധമായ കേസുകളിൽ പോലീസ് സ്റ്റേഷനുകൾക്കും, സൈബർ സെല്ലുകൾക്കും ആവശ്യമായ പിന്തുണ നൽകുന്നതിനുമുള്ള നടപടികൾ സൈബർ ഡിവിഷൻ സ്വീകരിച്ചു വരുന്നു. പ്രസ്തുത ഡിവിഷന്റെ കീഴിൽ പബ്ലിക്ക് ഔട്ട് റീച്ച് ഗ്രൂപ്പ്, സൈബർ ഫ്രോഡ് ആന്റ് സോഷ്യൽ മീഡിയ ഗ്രൂപ്പ്, സൈബർ സെക്യൂരിറ്റി ആന്റ് അഡ്വാൻസ്ഡ് ക്രൈം ഗ്രൂപ്പ്, തിരുവനന്തപുരം, കൊച്ചി, കോഴിക്കോട് സൈബർ ഡോമുകൾ, അനാലിസിസ് വിംഗ്, ട്രെയിനിങ് ആൻഡ് കപ്പാസിറ്റി ബിൽഡിംഗ് എന്നീ വിഭാഗങ്ങളെ ഏകോപിപ്പിച്ച് കൊണ്ടുള്ള പ്രവർത്തനങ്ങൾ നടന്നു വരുന്നു. **പബ്ലിക് ഔട്ട് റീച്ച് ഗ്രൂപ്പ്:** പൊതുജനങ്ങൾക്ക് ഓൺലൈൻ സാമ്പത്തിക തട്ടിപ്പിനിരയായ പരാതികൾ രജിസ്റ്റർ ചെയ്യുന്നതിന് 24 മണിക്കൂറും പ്രവർത്തിക്കുന്ന National Cyber

Crime Reporting Portal (NCRP) ന്റെ Toll Free Number 1930 (Call Center) നിലവിലുണ്ട്. ഇതിലൂടെ ലഭിക്കുന്ന വിവരങ്ങളിന്മേൽ തട്ടിപ്പുകാരുടെ ബാങ്ക് അക്കൗണ്ടുകൾ ബ്ലോക്ക് ചെയ്ത് തട്ടിയെടുത്ത തുകകൾ തിരിച്ചുപിടിയ്ക്കുന്നതിനുള്ള തുടർനടപടികൾ ബന്ധപ്പെട്ട ബാങ്ക് അധികാരികളുമായി ചേർന്ന് പബ്ലിക് ഔട്ട് റീച്ച് ഗ്രൂപ്പ് മുഖേന സ്വീകരിച്ചുവരുന്നു.

തട്ടിപ്പുകാർ ഉപയോഗിച്ചുവന്ന 12,658 മൊബൈൽ സിം കാർഡുകളും 14,293 ഡിവൈസുകളും (IMEI നമ്പർ പ്രകാരം) ബ്ലോക്ക് ചെയ്ത് പ്രവർത്തന രഹിതമാക്കിയിട്ടുണ്ട്. തട്ടിപ്പുകാർ സ്ഥിരമായി ഉപയോഗിച്ചു വന്നിരുന്ന 29,020 അക്കൗണ്ടുകൾ (Mule Accounts) നിർജ്ജീവമാക്കിയിട്ടുണ്ട്.

<u>സൈബർ ഫ്രോഡ് ആന്റ് സോഷ്യൽ മീഡിയഗ്രൂപ്പ്:</u>

സൈബർ കുറ്റകൃത്യങ്ങളെ നേരിടുന്നതിനും, അവയെ വിശകലനം ചെയ്ത് കുറ്റകൃത്യങ്ങൾക്ക് ഇടയാക്കുന്ന വസ്തുതകൾ കണ്ടെത്തി ഇല്ലായ്മ ചെയ്യുന്നതിനും അത്തരം വെബ് സൈറ്റുകൾ, അനധികൃത ഓൺലൈൻ ലോൺ ആപ്പുകൾ, സോഷ്യൽ മീഡിയ അക്കൗണ്ട് / പോസ്റ്റ് / പേജ് മുതലായവ സൈബർ പട്രോളിങ്ങിലൂടെ കണ്ടെത്തി സൈബർ സ്പേസിൽ നിന്നും നീക്കം ചെയ്യുന്നതിനുമുള്ള നടപടികൾ സൈബർ ഫ്രോഡ് ആന്റ് സോഷ്യൽ മീഡിയ ഗ്രൂപ്പ് വഴി സ്വീകരിച്ച് വരുന്നു.

ഓൺലൈൻ സാമ്പത്തിക തട്ടിപ്പുമായി ബന്ധപ്പെട്ട് രജിസ്റ്റർ ചെയ്ത കേസുകളിലും, പട്രോളിങ്ങിലൂടെ തട്ടിപ്പിനുപയോഗിച്ചു എന്ന് കണ്ടെത്തിയതുമായ 18,200 വെബ് സൈറ്റുകളും 537 അനധികൃത ഓൺലൈൻ ലോൺ ആപ്പുകളും, 9,067 സോഷ്യൽ മീഡിയ അക്കൗണ്ട് /പോസ്റ്റ്/പേജ് എന്നിവയും നിർജീവമാക്കിയിട്ടുണ്ട്.

<u>സൈബർ സെക്യൂരിറ്റി ആന്റ് അഡ്വാൻസ്ഡ് ക്രൈം വിഭാഗം:</u>

സൈബർ സെക്യൂരിറ്റി ആക്രമണങ്ങൾ പ്രതിരോധിക്കുന്നതിനായി INDIAN COMPUTER EMERGENCY RESPONSE TEAM (CERT-IN) -മായി ചേർന്ന് സൈബർ സെക്യൂരിറ്റി ആന്റ് അഡ്വാൻസ്ഡ് ക്രൈം വിഭാഗം പ്രവർത്തിച്ചുവരുന്നു.

പോലീസിനെ സൈബർ അറ്റാക്കുകൾ നേരിടാൻ സുസജ്ജമാക്കുന്നതിന്റെ ഭാഗമായി ഒരു വിദഗ്ധ സേന സംസ്ഥാന തലത്തിലും ജില്ലാതലത്തിലും രൂപീകരിക്കുന്നതിനായി BSNL, കൊച്ചിൻ

യൂണിവേഴ്സിറ്റി ഓഫ് സയൻസ് ആന്റ് ടെക്നോളജി (CUSAT), ഇന്ത്യൻ ഇൻസ്റ്റിഡ്യൂട്ട് ഓഫ് ഇൻഫർമേഷൻ ടെക്നോളജി (IIT) നാഷണൽ ഫോറൻസിക് സയൻസ് യൂണിവേഴ്സിറ്റി (NFSU), NIT Calicut എന്നീ സ്ഥാപനങ്ങളുമായി ചേർന്ന് സമഗ്രമായ പരിശീലന പരിപാടികൾ നടത്തുകയും, ഇപ്രകാരം ട്രെയിനിംഗ് ലഭിച്ച പോലീസ് ഉദ്യോഗസ്ഥരെ ഉൾപ്പെടുത്തി എല്ലാ ജില്ലകളിലും ഇൻസിഡന്റ് റെസ്പോൺസ് ടീമുകൾ രൂപീകരിക്കുകയും ചെയ്തിട്ടുണ്ട്. സംസ്ഥാനത്തെ വിവിധ സർക്കാർ വകുപ്പുകളിൽ വിദേശ രാജ്യങ്ങളിൽ നിന്നുൾപ്പെടെ ഉണ്ടായ സൈബർ ആക്രമണങ്ങൾ പ്രസ്തുത ടീമുകളെ ഉപയോഗപ്പെടുത്തി പരിഹരിക്കാൻ സാധിച്ചിട്ടുണ്ട്. കേന്ദ്ര-സംസ്ഥാന സർക്കാരുകളുടെ വിവിധ വകുപ്പുകളിലുണ്ടായ 31 ഡാറ്റാ ബ്രീച്ചുകൾ ഡാർക്ക് വെബ് ഇൻവെസ്റ്റിഗേഷൻ വഴി കണ്ടെത്തി പ്രസ്തുത വകുപ്പുകളെ അറിയിക്കുകയും, അവ ഒഴിവാക്കാൻ സൈബർ ഹൈജീൻ പാലിക്കുന്നതിനുള്ള നിർദ്ദേശങ്ങൾ, സൈബർ സെക്യൂരിറ്റി ആന്റ് അഡ്വാൻസ്ഡ് ക്രൈം വിഭാഗം മുഖേന നൽകുകയും ചെയ്തിട്ടുണ്ട്.

<u>സെക്യൂരിറ്റി ഓപ്പറേഷൻ സെന്റർ :</u>

പോലീസ് വകുപ്പിലെ കമ്പ്യൂട്ടറുകളും നെറ്റ് വർക്കുകളും 24 മണിക്കൂറും നിരീക്ഷിക്കുന്നതിനും സൈബർ വെല്ലുവിളികൾ നേരിടുന്നതിനും തിരുവനന്തപുരം സൈബർ ഡോമിൽ സെക്യൂരിറ്റി ഓപ്പറേഷൻ സെന്ററിന്റെ ഒന്നാംഘട്ട പ്രവർത്തനം ആരംഭിച്ചിട്ടുണ്ട്. പോലീസ് സൈബർ നെറ്റ് വർക്ക് സുരക്ഷ ഉറപ്പാക്കുന്നതിന് സെക്യൂരിറ്റി ഓപ്പറേഷൻ സെന്റർ മുഖേന കേരള പോലീസിലെ 1000 സിസ്റ്റം ഓൺ ബോർഡ് ചെയ്തുകൊണ്ടാണ് ഒന്നാംഘട്ട പ്രവർത്തനം ആരംഭിച്ചിട്ടുള്ളത്. ഇന്ത്യയിൽ തന്നെ സ്വന്തമായി സെക്യൂരിറ്റി ഓപ്പറേഷൻ സെന്റർ പ്രവർത്തിപ്പിക്കുന്ന ഏക പോലീസ് സേന കേരള പോലീസ് ആണ്.

<u>Counter Child Sexual Exploitation Center:</u>

ഈ വിഭാഗം മുഖേന കുട്ടികൾക്ക് നേരെയുള്ള ലൈംഗിക കുറ്റകൃത്യങ്ങൾക്കെതിരെ ശക്തമായ പ്രവർത്തനം നടത്തി വരുന്നു. ഓപ്പറേഷൻ പി - ഹണ്ട് എന്ന പേരിൽ നടത്തുന്ന ഓപ്പറേഷനുകളിലൂടെ ഇതുവരെ 351 പേരെ അറസ്റ്റ് ചെയ്യുകയും, 1758 കേസുകൾ രജിസ്റ്റർ ചെയ്യുകയും 3305 ഉപകരണങ്ങൾ പിടിച്ചെടുക്കുകയും ചെയ്തിട്ടുണ്ട്.

			നൂതന സാങ്കേതിക വിദ്യ ഉപയോഗിച്ച്, തട്ടിപ്പുകൾ ഫലപ്രദമായി അന്വേഷിക്കുന്നതിന് 355 ഉദ്യോഗസ്ഥർ അടങ്ങുന്ന ഒരു പ്രത്യേക അന്വേഷണ സംഘം രൂപീകരിക്കുന്നതിനും, Artificial Intelligence -ന്റെ സഹായത്തോടു കൂടി സൈബർ കുറ്റകൃത്യങ്ങളെ പ്രതിരോധിക്കുന്നതിന് ജനങ്ങൾക്ക് ഉപയോഗ പ്രദമായ സൈബർവാൾ പ്രോജക്ടുകൾ വികസിപ്പിക്കുന്നതിനും, Crypto currency വഴി തട്ടിപ്പ് തുക കൈമാറ്റം ചെയ്യുന്നത് അന്വേഷിക്കുന്നതിനും ഫലപ്രദമായി ഇടപെടുന്നതിനും ഒരു ക്രിപ്റ്റോ കറൻസി ഇൻവെസ്റ്റിഗേഷൻ സെന്റർ കൊച്ചി സൈബർ ഡോമിൽ ആരംഭിക്കുന്നതിനുമുള്ള നടപടികൾ സ്വീകരിച്ചു വരുന്നു. സൈബർ സാങ്കേതിക മേഖലയിലെ പുതിയ അറിവുകൾ പകർന്നു നൽകുന്നതിനായി പ്രവർത്തിയ്ക്കുന്ന ട്രെയിനിങ് ആൻഡ് കപ്പാസിറ്റി ബിൽഡിംഗ് വിഭാഗത്തിന് കീഴിൽ വിവിധ റാങ്കുകളിൽ നിന്നുള്ള 4697 പോലീസ് ഉദ്യോഗസ്ഥർക്ക് വിവിധ വിഷയങ്ങളിൽ പരിശീലനം നൽകിയിട്ടുണ്ട്. സൈബർ തട്ടിപ്പുകളെക്കുറിച്ച് പൗരൻമാരെ ബോധവൽക്കരിക്കുന്നതിനും സാമ്പത്തിക തട്ടിപ്പുകളിൽ നിന്നും ഭീഷണികളിൽ നിന്നും സുരക്ഷിതരാക്കുന്നതിനുള്ള പ്രായോഗിക അറിവ് നേടുന്നതിനുമായി ഓൺലൈൻ മുഖേനയുള്ള വിവിധ ബോധവൽക്കരണ പ്രോഗ്രാമുകളും നടത്തി വരുന്നുണ്ട്. സൈബർ കുറ്റകൃത്യങ്ങളെക്കുറിച്ചു ജനങ്ങളിൽ അവബോധം വളർത്തുന്നതിന് വേണ്ടി 7708 സൈബർ വോളന്റിയർമാർ രജിസ്റ്റർ ചെയ്യുകയും അവർക്ക് ജില്ലാതലത്തിൽ ട്രെയിനിങ് നൽകുകയും ചെയ്തിട്ടുണ്ട്. സൈബർ കുറ്റാന്വേഷണങ്ങൾ ഏകോപിപ്പിക്കുന്നതിനും വിവരശേഖരണത്തിനുമായി സൈബർ പട്രോൾ വിഭാഗവും പ്രവർത്തിച്ചുവരുന്നുണ്ട്.
(ബി)	ടെലിഗ്രാം ആപ്പിലൂടെ നടത്തുന്ന ഓൺലൈൻ ട്രേഡിംഗിലൂടെ വീട്ടിലിരുന്നു പണമുണ്ടാക്കാമെന്ന് വാഗ്ദാനം ചെയ്ത് സംസ്ഥാനത്തു ഒട്ടേറെപ്പേരുടെ പണം തട്ടിയെടുത്തതായി പൊലീസ് കണ്ടെത്തിയിട്ടുണ്ടോ; ഇത്തരം തട്ടിപ്പുകൾ അവസാനിപ്പിക്കുന്നതിന് സംസ്ഥാന പൊലീസിന്റെ നേതൃത്വത്തിൽ നടപടി സ്വീകരിച്ചിട്ടുണ്ടോ; വിശദമാക്കുമോ;	(ബി)	ഉണ്ട്. ടെലിഗ്രാം തട്ടിപ്പ്, ഡിജിറ്റൽ അറസ്റ്റ് എന്നീ തട്ടിപ്പുകൾക്ക് ഇരയായി ജനങ്ങളിൽ നിന്നും പണം നഷ്ടപ്പെടുന്നതായി ശ്രദ്ധയിൽപ്പെട്ടതിനെ തുടർന്ന് ഇത്തരം കുറ്റകൃത്യങ്ങളെ കുറിച്ച് വിവരം ശേഖരിക്കുകയും കുറ്റവാളികളെ തിരിച്ചറിയുകയും തുടർനടപടികൾ സ്വീകരിക്കുകയും ചെയ്യുന്നുണ്ട്. പൊതുജനങ്ങൾക്ക് ഓൺലൈൻ സാമ്പത്തിക തട്ടിപ്പിനിരയായ പരാതികൾ രജിസ്റ്റർ ചെയ്യുന്നതിനായി NCRP (National Cyber Crime Reporting Portal) - യുടെ www.cybercrime.gov.in

			എന്ന വെബ് സൈറ്റും ടോൾ ഫ്രീ നമ്പറായ 1930-(Call Center) ഉം 24 മണിക്കൂറും പ്രവർത്തിച്ചു വരുന്നു. ഫിനാൻഷ്യൽ ഫ്രോഡിലേക്ക് നയിച്ചേക്കാവുന്ന സോഷ്യൽമീഡിയ അക്കൗണ്ടുകളും, പോസ്റ്റുകളും, പരസ്യങ്ങളും, വെബ് സൈറ്റുകളും, അനധികൃത ഓൺലൈൻ ആപ്പുകളും പ്രവർത്തനരഹിതമാക്കിയിട്ടുണ്ട്. സൈബർ കുറ്റാന്വേഷണ മികവ് വർദ്ധിപ്പിക്കുന്നതിന്റെ ഭാഗമായി 3636 പോലീസ് ഉദ്യോഗസ്ഥർക്ക് സൈബർ ഡിവിഷൻ പരിശീലനം നൽകിയിട്ടുണ്ട്. ഇത് കൂടാതെ ഇൻസ്പെക്ടർ, സബ് ഇൻസ്പെക്ടർ റാങ്കിൽപ്പെട്ട 360 പോലീസ് ഉദ്യോഗസ്ഥർക്കും 3 ഘട്ടങ്ങളിലായി പ്രത്യേക പരിശീലനം നൽകിയിട്ടുണ്ട്. കൗണ്ടർ ചൈൽഡ് സെക്ഷൽ എക്സ്പ്ലോയിറ്റേഷൻ സെന്റർ (CCSE) മുഖേനയുള്ള ഓപ്പറേഷനിലൂടെ കുറ്റക്കാരെ കേന്ദ്രീകരിച്ച് സെർച്ച് ഓപ്പറേഷൻ നടത്തി അവർ കൃത്യത്തിന് ഉപയോഗിച്ച ഉപകരണങ്ങൾ, ദൃശ്യങ്ങൾ എന്നിവ കണ്ടെടുക്കുകയും ആവശ്യമായ നിയമനടപടികൾ സ്വീകരിച്ചു വരികയും ചെയ്യുന്നുണ്ട്. സ്ത്രീകൾക്കും കുട്ടികൾക്കും എതിരായ ഓൺലൈൻ കുറ്റകൃത്യങ്ങൾ തടയുന്നതിന് നടത്തിയ മാതൃകാപരമായ പ്രവർത്തനത്തിന് കേരളത്തിന് കേന്ദ്ര ആഭ്യന്തരമന്ത്രാലയത്തിന്റെ പുരസ്കാരം ലഭിച്ചിട്ടുണ്ട്.
(സി)	സ്ത്രീകളും കുട്ടികളുമാണ് സൈബർ തട്ടിപ്പുകളിൽ കൂടുതലായി ഇരയാക്കപ്പെടുന്നതെന്നത് പരിഗണിച്ച് അവരുടെ സുരക്ഷ ഉറപ്പാക്കാൻ മുൻഗണന നൽകിക്കൊണ്ടുള്ള സൈബർ സുരക്ഷാ നടപടികൾ സ്വീകരിച്ചിട്ടുണ്ടോ; 'വെർച്വൽ അറസ്റ്റ്' ഉൾപ്പെടെ സൈബർ കുറ്റകൃത്യങ്ങൾ തടയുന്നതിനായി ആവശ്യമായ ഇടപെടലുകൾ നടത്തുന്ന തരത്തിൽ പോലീസ് സേനയുടെ പ്രവർത്തനം വിപുലമാക്കിയിട്ടുണ്ടോയെന്ന വിലയിരുത്തിയിട്ടുണ്ടോ; വ്യക്തമാക്കുമോ;	(സി)	ഉണ്ട്. ടെലിഗ്രാം തട്ടിപ്പ്, ഡിജിറ്റൽ അറസ്റ്റ് എന്നീ തട്ടിപ്പുകൾക്ക് ഇരയായി ജനങ്ങളിൽ നിന്നും പണം നഷ്ടപ്പെടുന്നതായി ശ്രദ്ധയിൽപ്പെട്ടതിനെ തുടർന്ന് ഇത്തരം കുറ്റകൃത്യങ്ങളെ കുറിച്ച് വിവരം ശേഖരിക്കുകയും കുറ്റവാളികളെ തിരിച്ചറിയുകയും തുടർനടപടികൾ സ്വീകരിക്കുകയും ചെയ്യുന്നുണ്ട്. പൊതുജനങ്ങൾക്ക് ഓൺലൈൻ സാമ്പത്തിക തട്ടിപ്പിനിരയായ പരാതികൾ രജിസ്റ്റർ ചെയ്യുന്നതിനായി NCRP (National Cyber Crime Reporting Portal) - യുടെ www.cybercrime.gov.in എന്ന വെബ് സൈറ്റും ടോൾ ഫ്രീ നമ്പറായ 1930-(Call Center) ഉം 24 മണിക്കൂറും പ്രവർത്തിച്ചു വരുന്നു. ഫിനാൻഷ്യൽ ഫ്രോഡിലേക്ക് നയിച്ചേക്കാവുന്ന സോഷ്യൽമീഡിയ അക്കൗണ്ടുകളും, പോസ്റ്റുകളും, പരസ്യങ്ങളും, വെബ് സൈറ്റുകളും, അനധികൃത ഓൺലൈൻ ആപ്പുകളും പ്രവർത്തനരഹിതമാക്കിയിട്ടുണ്ട്.

			സൈബർ കുറ്റാന്വേഷണ മികവ് വർദ്ധിപ്പിക്കുന്നതിന്റെ ഭാഗമായി 3636 പോലീസ് ഉദ്യോഗസ്ഥർക്ക് സൈബർ ഡിവിഷൻ പരിശീലനം നൽകിയിട്ടുണ്ട്. ഇത് കൂടാതെ ഇൻസ്പെക്ടർ, സബ് ഇൻസ്പെക്ടർ റാങ്കിൽപ്പെട്ട 360 പോലീസ് ഉദ്യോഗസ്ഥർക്കും 3 ഘട്ടങ്ങളിലായി പ്രത്യേക പരിശീലനം നൽകിയിട്ടുണ്ട്. കൗണ്ടർ ചൈൽഡ് സെക്ഷൽ എക്സ്പ്ലോയിറ്റേഷൻ സെന്റർ (CCSE) മുഖേനയുള്ള ഓപ്പറേഷനിലൂടെ കുറ്റക്കാരെ കേന്ദ്രീകരിച്ച് സെർച്ച് ഓപ്പറേഷൻ നടത്തി അവർ കൃത്യത്തിന് ഉപയോഗിച്ച ഉപകരണങ്ങൾ, ദൃശ്യങ്ങൾ എന്നിവ കണ്ടെടുക്കുകയും ആവശ്യമായ നിയമനടപടികൾ സ്വീകരിച്ചു വരികയും ചെയ്യുന്നുണ്ട്. സ്ത്രീകൾക്കും കുട്ടികൾക്കും എതിരായ ഓൺലൈൻ കുറ്റകൃത്യങ്ങൾ തടയുന്നതിന് നടത്തിയ മാതൃകാപരമായ പ്രവർത്തനത്തിന് കേരളത്തിന് കേന്ദ്ര ആഭ്യന്തരമന്ത്രാലയത്തിന്റെ പുരസ്കാരം ലഭിച്ചിട്ടുണ്ട്.
(ഡി)	സൈബർ കുറ്റകൃത്യങ്ങളുടെ ഉറവിടങ്ങളുടെ വലിയൊരു ശതമാനവും മറ്റു സംസ്ഥാനങ്ങളിലാണെന്നത് പരിഗണിച്ച് കേന്ദ്രസർക്കാരുമായി സഹകരിച്ച് സൈബർ കുറ്റാന്വേഷണം ത്വരിതപ്പെടുത്തുന്നതിന് സംസ്ഥാന പൊലീസ് നടപടി സ്വീകരിച്ചിട്ടുണ്ടോ; വിശദമാക്കുമോ?	(ഡി)	ഉണ്ട്. സാമ്പത്തിക തട്ടിപ്പുമായി ബന്ധപ്പെട്ട കേസുകളിൽ അന്യസംസ്ഥാനത്തിൽപ്പെട്ട പ്രതികളെ Indian Cyber Crime Coordination Center (I4C) - മായി ബന്ധപ്പെട്ട് സഹായങ്ങൾ ലഭ്യമാക്കി പ്രതികൾ രക്ഷപ്പെടാൻ അനുവദിക്കാതെ അറസ്റ്റ് ചെയ്യുവാൻ ആവശ്യമായ നടപടികൾ സ്വീകരിച്ചുവരുന്നു. ഇതിനായി I4C-യുടെ നിയന്ത്രണത്തിലുള്ള സമൻവയ (SAMANVAYA) പോർട്ടൽ സംവിധാനം കൂടാതെ, സൈബർ കുറ്റകൃത്യങ്ങളിൽ ഉൾപ്പെട്ടിട്ടുള്ള മൊബൈൽ ഫോണുകളും മറ്റും തെരഞ്ഞു കണ്ടുപിടിക്കുന്നതിനും പ്രവർത്തനരഹിതമാക്കുന്നതിനുമായി കേന്ദ്ര സർക്കാരിന്റെ മേൽനോട്ടത്തിലുള്ള CEIR (Central Equipment Identity Register) പോർട്ടൽ സംവിധാനവും ഉപയോഗിച്ചു വരുന്നു. തട്ടിപ്പുകൾ മുൻകൂട്ടി കണ്ടെത്തി ഉപഭോക്താക്കൾക്ക് മുൻകൂർ മുന്നറിയിപ്പുകൾ നൽകുന്ന സംവിധാനങ്ങൾ ബാങ്കിങ് മേഖലയിൽ ഏർപ്പെടുത്തിയാൽ മാത്രമേ ഉപഭോക്താക്കളുടെ സമഗ്രമായ പ്രതിരോധം ഉറപ്പുവരുത്താൻ സാധിക്കുകയുള്ളൂ. ഇതോടൊപ്പം തന്നെ ഡിവൈസ് വൈറ്റ് ലിസ്റ്റിംഗ് മുതലായ സാങ്കേതിക സംവിധാനങ്ങളും ബാങ്കിംഗ് സെക്ടറിൽ ഏർപ്പെടുത്തേണ്ടതുണ്ട്.സമഗ്രമായ സൈബർ സുരക്ഷിത ഫിൻ ഇക്കോ സിസ്റ്റം കെട്ടിപ്പടുക്കുന്നതിന് ആർ.ബി.ഐയുടെയും കേന്ദ്ര സർക്കാരിന്റെയും സംയുക്തമായ ഇടപെടൽ ആവശ്യമാണ്.

സെക്ഷൻ ഓഫീസർ