15 -ാം കേരള നിയമസഭ

12 -ാം സമ്മേളനം

നക്ഷത്ര ചിഹ്നം ഇല്ലാത്ത ചോദ്യം നം. 161 **07-10-2024 - ൽ മറുപടിയ്ക്ക്**

സൈബർ തട്ടിപ്പ്

ചോദ്യം	ഉത്തരം
ശ്രീ. കെ. ജെ. മാക്സി	ശ്രീ. പിണറായി വിജയൻ (മുഖ്യമന്ത്രി)

(എ) സംസ്ഥാനത്ത് പുതിയ രീതിയിലുള്ള സൈബർ തട്ടിപ്പുകൾ വർദ്ധിച്ച് വരുന്നത് ശ്രദ്ധയിൽപ്പെട്ടിട്ടുണ്ടോ; ഉണ്ടെങ്കിൽ കഴിഞ്ഞ മൂന്ന് വർഷക്കാലയളവിൽ ഓരോ വർഷവും എത്ര പരാതികൾ ലഭ്യമായി; എത്ര കേസ്സുകൾ രജിസ്റ്റർ ചെയ്തു; എത്ര കേസുകളിൽ പ്രതികളെ കണ്ടെത്തി; വിശദാംശം ലഭ്യമാക്കുമോ;

(എ) അനുദിനം വികസിച്ചുവരുന്ന വിവര സാങ്കേതികവിദ്യയ്ക്കൊപ്പം, അവ ദുരുപയോഗം ചെയ്തുള്ള സാമ്പത്തിക തട്ടിപ്പുകളും സൈബർ കുറ്റകൃത്യങ്ങളും രാജ്യത്ത് ക്രമാതീതമായി വർദ്ധിക്കുന്നുണ്ട്. സംസ്ഥാനത്തും ഈ വർദ്ധനവ് ശ്രദ്ധയിൽപ്പെട്ടിട്ടുണ്ട്. National Cyber Crime Reporting Portal (NCRP) - ൽ ലഭ്യമായ വിവരം അനുസരിച്ച് കഴിഞ്ഞ 3 വർഷക്കാലയളവിലെ വിശദാംശങ്ങൾ ചുവടെ പട്ടികയിൽ ഉൾപ്പെടുത്തുന്നു:

Sl.No.	Year	Petitions Reported In NCRP Portal	FIR Registered	Accused found Case
1	2022	9619	116	43
2	2023	23748	2230	160
3	2024 (up to 30.09.2024)	31019	2207	309

(ബി) സൈബർ ചതികളിൽ നിന്നും പൊതുജനങ്ങളെ സംരക്ഷിക്കുന്നതിന് സ്വീകരിച്ചുവരുന്ന നടപടികളുടെ വിശദാംശം വ്യക്തമാക്കുമോ?

(ബി) ഇത്തരം 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 സ്വീകരിച്ചുവരുന്നു. 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 ഓൺ ലൈൻ സാമ്പത്തിക തട്ടിപ്പിനിരയായ പരാതികൾ രജിസ്റ്റർ ചെയ്യുന്നതിന് 24 മണിക്കൂറും പ്രവർത്തിക്കുന്ന

National Cyber Crime Reporting Portal (NCRP) - ന്റെ ടോൾ ഫ്രീ നമ്പർ 1930 (Call Center) നിലവിലുണ്ട്. ഇതിലൂടെ ലഭിക്കുന്ന വിവരങ്ങളിൻമേൽ തട്ടിപ്പുകാരുടെ ബാങ്ക് അക്കൗണ്ടുകൾ ബ്ലോക്ക് ചെയ്ത് തട്ടിയെടുത്ത തുകകൾ തിരിച്ചു പിടിയ്ക്കുന്നതിനുള്ള തുടർനടപടികൾ ബന്ധപ്പെട്ട ബാങ്ക് അധികാരികളുമായി ചേർന്ന് പബ്ലിക് ഔട്ട്റീച്ച് 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.

സൈബർ ഫ്രോഡ് ആന്റ് സോഷ്യൽ മീഡിയ ഗ്രൂപ്പ് : സൈബർ കുറ്റകൃത്യങ്ങളെ നേരിടുന്നതിനും, അവയെ വിശകലനം ചെയ്ത് കുറ്റകൃത്യങ്ങൾക്ക് ഇടയാക്കുന്ന വസ്തുതകൾ കണ്ടെത്തി ഇല്ലായ്മ ചെയ്യുന്നതിനും അത്തരം വെബ്സൈറ്റുകൾ, 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, സൈബർ പട്രോളിങ്ങിലൂടെ തട്ടിപ്പിനുപയോഗിച്ചു എന്ന് കണ്ടെത്തിയതുമായ 18,200 വെബ് സൈറ്റുകളും 537 അനധികൃത ഓൺലൈൻ ലോൺ ആപ്പുകളും, 9,067 സോഷ്യൽ മീഡിയ അക്കൗണ്ട് /പോസ്റ്റ്/ പേജ് എന്നിവയും നിർജീവമാക്കിയിട്ടുണ്ട്.

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

പോലീസ് സേനയെ സൈബർ അറ്റാക്കുകൾ നേരിടാൻ സുസജ്ജമാക്കുന്നതിന്റെ ഭാഗമായി ഒരു വിദഗ്ധ സേനയെ സംസ്ഥാന തലത്തിലും ജില്ലാതലത്തിലും രൂപീകരിക്കുന്നതിനായി BSNL, കൊച്ചിൻ യൂണിവേഴ്സിറ്റി ഓഫ് സയൻസ് ആൻഡ് ടെക്നോളജി (CUSAT), ഇന്ത്യൻ ഇൻസ്റ്റിട്യൂട്ട് 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.

സെക്യൂരിറ്റി ഓപ്പറേഷൻ സെന്റർ : 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.

Counter Child Sexual Exploitation Center: ഈ വിഭാഗം മുഖേന കുട്ടികൾക്ക് നേരെയുള്ള ലൈംഗിക കുറ്റകൃത്യങ്ങൾക്കെതിരെ ശക്തമായ പ്രവർത്തനം നടത്തിവരുന്നു. 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 സഹായത്തോടുകൂടി സൈബർ കുറ്റകൃത്യങ്ങളെ പ്രതിരോധിക്കുന്നതിന് ജനങ്ങൾക്ക് ഉപയോഗപ്രദമായ സൈബർവാൾ പ്രോജക്റ്റുകൾ വികസിപ്പിക്കുന്നതിനും, Crypto currency വഴി തട്ടിപ്പ് തുക കൈമാറ്റം ചെയ്യുന്നത് അന്വേഷിക്കുന്നതിനും ഫലപ്രദമായി ഇടപെടുന്നതിനും ഒരു ക്രിപ്റ്റോ കറൻസി ഇൻവെസ്റ്റിഗേഷൻ സെന്റർ കൊച്ചി സൈബർ ഡോമിൽ ആരംഭിക്കുന്നതിനുമുള്ള നടപടികൾ സ്വീകരിച്ചുവരുന്നു.

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 പൗരന്മാരെ ബോധവൽക്കരിക്കുന്നതിനും സാമ്പത്തിക തട്ടിപ്പുകളിൽ നിന്നും ഭീഷണികളിൽ നിന്നും സുരക്ഷിതരാക്കുന്നതിനുള്ള പ്രായോഗിക അറിവ് നേടുന്നതിനുമായി ഓൺലൈൻ മുഖേനയുള്ള വിവിധ ബോധവൽക്കരണ പ്രോഗ്രാമുകളും നടത്തി വരുന്നുണ്ട്.സൈബർ കുറ്റകൃത്യങ്ങളെക്കുറിച്ച് ജനങ്ങളിൽ അവബോധം വളർത്തുന്നതിന് വേണ്ടി 7703 സൈബർ വോളന്റിയർമാരെ രജിസ്റ്റർ ചെയ്യുകയും അവർക്ക് ജില്ലാതലത്തിൽ ട്രെയിനിങ് നൽകുകയും ചെയ്തിട്ടുണ്ട്.

സൈബർ കുറ്റാന്വേഷണങ്ങൾ ഏകോപിപ്പിക്കുന്നതിനും വിവരശേഖരണത്തിനുമായി സൈബർ പട്രോൾ വിഭാഗം പ്രവർത്തിച്ച് വരുന്നു. പൊതുജനങ്ങൾക്ക് ലഭിക്കുന്ന മെസേജുകൾ, യുആർഎൽ, ഇ - മെയിൽ, സോഷ്യൽ മീഡിയ വിവരങ്ങൾ എന്നിവ വ്യാജമാണോ എന്ന് പരിശോധിച്ച് സൈബർ തട്ടിപ്പുകളിൽ നിന്നും സംരക്ഷിക്കുന്നതിനായി AI അധിഷ്ഠിതമായി പ്രവർത്തിക്കുന്ന സൈബർ വാൾ പ്രോജക്റ്റ് വികസിപ്പിക്കുന്നതിനുള്ള പ്രാരംഭ നടപടികൾ പുരോഗമിച്ച് വരുന്നു.

പൊതുജനങ്ങളെ ബോധവൽക്കരിക്കുന്നതിനുള്ള ഓൺലൈൻ വെബിനാറുകൾ സൈബർ ഡിവിഷന്റെ കീഴിൽ നടത്തിവരുന്നുണ്ട്. പോലീസിന്റെ Social Media Centre വഴിയും വലിയ രീതിയിലുള്ള പ്രചാരണം നടത്തിവരുന്നു. സൈബർ ഓപ്പറേഷൻ വിഭാഗത്തിന്റെയും ലോക്കൽ പോലീസിന്റെയും സംയുക്ത

			പ്രവർത്തനങ്ങളിലൂടെ പ്രധാനപ്പെട്ട കേസുകളിലെ പ്രതികളെ അറസ്റ്റ് ചെയ്യുകയും തട്ടിയെടുത്ത തുക വീണ്ടെടുക്കുകയും ചെയ്തിട്ടുണ്ട്. Crypto currency വഴി തട്ടിപ്പ് തുക കൈമാറ്റം ചെയ്യുന്നത് അന്വേഷിക്കുന്നതിനും ഫലപ്രദമായി ഇടപെടുന്നതിനും ഒരു ക്രിപ്റ്റോ കറൻസി ഇൻവെസ്റ്റിഗേഷൻ സെന്റർ കൊച്ചി സൈബർ ഡോമിൽ ആരംഭിക്കുന്നതിനുള്ള നടപടികൾ സ്വീകരിച്ചു വരുന്നു. സൈബർ കുറ്റകൃത്യങ്ങൾ സമഗ്രമായി തടയുന്നതിന് Fin Tech മേഖലയിൽ സമഗ്രമായ മാറ്റങ്ങൾ വരുത്തേണ്ടതായിട്ടുണ്ട്. തട്ടിപ്പുകൾ മുൻകൂട്ടി കണ്ടെത്തി ഉപഭോക്താക്കൾക്ക് മുൻകൂർ മുന്നറിയിപ്പുകൾ നൽകുന്ന സംവിധാനങ്ങൾ ബാങ്കിങ്ങ് മേഖലയിൽ ഏർപ്പെടുത്തിയാൽ മാത്രമേ ഉപഭോക്താക്കളുടെ സമഗ്രമായ പ്രതിരോധം ഉറപ്പുവരുത്താൻ സാധിക്കുകയുള്ളൂ. ഇതോടൊപ്പം തന്നെ ഡിവൈസ് വൈറ്റ് ലിസ്റ്റിംഗ് മുതലായ സാങ്കേതിക സംവിധാനങ്ങൾ ബാങ്കിംഗ് സെക്ടറിൽ ഏർപ്പെടുത്തേണ്ടതുണ്ട്. സമഗ്രമായ സൈബർ സുരക്ഷിത ഫിൻ ഇക്കോ സിസ്റ്റം കെട്ടിപ്പടുക്കുന്നതിന് ആർബിഐയുടെയും കേന്ദ്രസർക്കാരിന്റെയും സംയുക്തമായ ഇടപെടൽ ആവശ്യമാണ്.

സെക്ഷൻ ഓഫീസർ