പതിനാറാം കേരളനിയമസഭ

രണ്ടാം സമ്മേളനം

നക്ഷത്രചിഹ്നമിടാത്ത ചോദ്യം നമ്പർ: 2223 **27-10-2026-ൽ മറുപടിയ്ക്ക്**

സൈബർ തട്ടിപ്പുകളും ഓൺലൈൻ സാമ്പത്തിക കുറ്റകൃത്യങ്ങളും

ചോദ്യം ഉന്നയിച്ച അംഗങ്ങൾ **മറുപടി നൽകിയ മന്ത്രി**

ശ്രീ. ടി. എം. ശശി ശ്രീ. രമേശ് ചെന്നിത്തല
(ആഭ്യന്തര- വിജിലൻസ്, കയർ വകുപ്പ് മന്ത്രി)

(എ) സൈബർ തട്ടിപ്പുകളും ഓൺലൈൻ സാമ്പത്തിക കുറ്റകൃത്യങ്ങളും വർധിച്ചുവരുന്ന നിലവിലെ സാമൂഹിക സാഹചര്യത്തിൽ അവ തടയുന്നതിനും നഷ്ടപ്പെട്ട പണം പരാതിക്കാർക്ക് തിരിച്ച് നൽകുന്നതിനും കേരള പോലീസിന്റെ സൈബർ വിഭാഗത്തിൽ എന്തൊക്കെ സംവിധാനങ്ങളാണ് ഏർപ്പെടുത്തിയിട്ടുള്ളതെന്ന് വിശദമാക്കാമോ;

മറുപടി: സൈബർ സാമ്പത്തിക തട്ടിപ്പുകൾ തടയുന്നതിനും നഷ്ടപ്പെട്ട തുകയുടെ തുടർ കൈമാറ്റം നിയന്ത്രിക്കുന്നതിനും കേരള പോലീസ് സൈബർ ഓപ്പറേഷൻസ് വിഭാഗത്തിന്റെ നേതൃത്വത്തിൽ വിവിധ നടപടികൾ സ്വീകരിച്ചുവരുന്നു. ഇരകൾക്ക് 1930 ടോൾഫ്രീ ഹെൽപ്ലൈൻ മുഖേനയോ www.cybercrime.gov.in എന്ന നാഷണൽ സൈബർ ക്രൈം റിപ്പോർട്ടിംഗ് പോർട്ടൽ (NCRP) മുഖേനയോ പരാതി നൽകാവുന്നതാണ്. പരാതികൾ ലഭിക്കുന്ന മുറയ്ക്ക് ബന്ധപ്പെട്ട ബാങ്കുകളുമായും ടെലികോം സേവനദാതാക്കളുമായും ഏകോപനം നടത്തി തുക തടഞ്ഞുവയ്ക്കുന്നതിനും തിരികെ ലഭ്യമാക്കുന്നതിനും നടപടി സ്വീകരിക്കുന്നു.

കൂടാതെ, പോലീസ് ആസ്ഥാനത്തെ സൈബർ ഓപ്പറേഷൻസ് വിഭാഗത്തിനു കീഴിൽ പ്രവർത്തിക്കുന്ന ജോയിന്റ് സൈബർ ക്രൈം കോർഡിനേഷൻ ടീം (JCCT) മുഖേന ബാങ്ക് ഉദ്യോഗസ്ഥരുമായി നേരിട്ട് ഏകോപനം നടത്തി സംശയാസ്പദമായ ഇടപാടുകൾ പരിശോധിക്കുകയും തട്ടിപ്പിലൂടെ കൈമാറ്റം ചെയ്യപ്പെട്ട തുക തടഞ്ഞുവയ്ക്കുന്നതിനുള്ള നടപടികൾ ത്വരിതപ്പെടുത്തുകയും ചെയ്യുന്നു.

അഞ്ചു ലക്ഷം രൂപയ്ക്ക് മുകളിലുള്ള സൈബർ സാമ്പത്തിക തട്ടിപ്പ് പരാതികളിൽ എഫ്.ഐ.ആർ. രജിസ്റ്റർ ചെയ്യുന്നത് വേഗത്തിലാക്കുന്നതിനായി NCRP-യെയും കേരള പോലീസിന്റെ ICOPS സംവിധാനത്തെയും സംയോജിപ്പിച്ച് ഇ-സീറോ എഫ്.ഐ.ആർ. (e-Zero FIR) സംവിധാനവും നടപ്പിലാക്കിയിട്ടുണ്ട്.

തട്ടിപ്പിലൂടെ നഷ്ടപ്പെട്ട തുക തിരികെ ലഭ്യമാക്കുന്നതിനായി CFCFRMS (Citizen Financial Cyber Fraud Reporting and Management System), മണി റീസ്റ്റോറേഷൻ മോഡ്യൂൾ (MRM) എന്നിവ പ്രയോജനപ്പെടുത്തിവരുന്നു.

സൈബർ സാമ്പത്തിക തട്ടിപ്പുകളുടെ രീതികൾ വിശകലനം ചെയ്ത് കുറ്റവാളികളെയും തട്ടിപ്പിന് സഹായിക്കുന്ന ബാങ്ക് അക്കൗണ്ട് ഉടമകളെയും കണ്ടെത്തുന്നതിനും നിയമനടപടികൾ സ്വീകരിക്കുന്നതിനും 'ഓപ്പറേഷൻ സൈ-ഹണ്ട്' ഉൾപ്പെടെയുള്ള നടപടികൾ നടപ്പിലാക്കിവരുന്നു.

തട്ടിപ്പിന് ഉപയോഗിക്കുന്ന ബാങ്ക് അക്കൗണ്ടുകൾ, മൊബൈൽ നമ്പറുകൾ, ഇലക്ട്രോണിക് ഉപകരണങ്ങൾ എന്നിവ പരിശോധിച്ച് ആവശ്യമായ സാഹചര്യങ്ങളിൽ അവ മരവിപ്പിക്കുന്നതിനും തടയുന്നതിനും ബന്ധപ്പെട്ട സ്ഥാപനങ്ങളുമായി ചേർന്ന് നടപടികൾ സ്വീകരിക്കുന്നു.

ഇതിനുപുറമേ, വീഡിയോകൾ, പോസ്റ്ററുകൾ, സാമൂഹിക മാധ്യമ സന്ദേശങ്ങൾ, ഓൺലൈൻ ക്ലാസുകൾ എന്നിവയിലൂടെ മുതിർന്ന പൗരന്മാർ ഉൾപ്പെടെയുള്ള പൊതുജനങ്ങൾക്ക് സൈബർ സുരക്ഷാ ബോധവൽക്കരണം നൽകിവരുന്നു.

(ബി) സൈബർ പോലീസിന്റെ പ്രവർത്തന മികവ് വർധിപ്പിക്കുന്നതിനായി ഭാവിയിൽ എന്തൊക്കെ പദ്ധതികളാണ് നടപ്പിലാക്കുവാൻ ഉദ്ദേശിക്കുന്നതെന്ന് വ്യക്തമാക്കുമോ?

<u>മറുപടി:</u> കേരള പോലീസിന്റെ സൈബർ വിഭാഗത്തിന്റെ പ്രവർത്തനക്ഷമതയും സൈബർ സുരക്ഷാ ശേഷിയും വർധിപ്പിക്കുന്നതിനായി താഴെപ്പറയുന്ന പദ്ധതികൾ ആവിഷ്കരിച്ച് നടപ്പിലാക്കിവരുന്നു.

<u>1. സൈബർ റെസിലിയൻസ് സെന്ററുകൾ</u>

വർധിച്ചുവരുന്ന സൈബർ കുറ്റകൃത്യങ്ങൾ, ഓൺലൈൻ സാമ്പത്തിക തട്ടിപ്പുകൾ, സാമൂഹിക മാധ്യമങ്ങളുടെ ദുരുപയോഗം, കുട്ടികൾക്കെതിരായ ഓൺലൈൻ കുറ്റകൃത്യങ്ങൾ എന്നിവ തടയുന്നതിനും സൈബർ സുരക്ഷാ അവബോധം വർധിപ്പിക്കുന്നതിനുമായി കേരള പോലീസ് 'സൈബർ സേഫ് കേരളം' പദ്ധതി നടപ്പിലാക്കിവരുന്നു. പോലീസും അക്കാദമിക് സ്ഥാപനങ്ങളും ഐ.ടി. മേഖലയുമായി സഹകരിച്ച് ജില്ലകളിൽ സൈബർ റെസിലിയൻസ് സെന്ററുകൾ സ്ഥാപിച്ച് വിദ്യാർത്ഥികളുടെ സാങ്കേതിക വൈദഗ്ധ്യം സൈബർ സുരക്ഷാ പ്രവർത്തനങ്ങൾക്കായി പ്രയോജനപ്പെടുത്തുകയാണ് പദ്ധതിയുടെ ലക്ഷ്യം.

<u>2. ആർട്ടിഫിഷ്യൽ ഇന്റലിജൻസ് (AI) ചാറ്റ്ബോട്ട്</u>

കേരള പോലീസിന്റെ വെബ്സൈറ്റിലൂടെ പൊതുജനങ്ങൾക്ക് ഔദ്യോഗിക വിവരങ്ങൾ വേഗത്തിലും കൃത്യതയോടെയും ലഭ്യമാക്കുന്നതിനായി AI ചാറ്റ്ബോട്ട് ഉൾപ്പെടുത്തിയിട്ടുണ്ട്. ഏകദേശം 10,000 വെബ്പേജുകളിലെ വിവരങ്ങൾ ഉൾപ്പെടുത്തിയ Knowledge Base ഉപയോഗിച്ച് ടെക്സ്റ്റ്, ശബ്ദം എന്നിവയിലൂടെ വിവരങ്ങൾ തിരയുന്നതിനുള്ള സൗകര്യം ലഭ്യമാക്കുന്ന സംവിധാനം പ്രവർത്തനസജ്ജമാക്കുന്നതിനുള്ള നടപടികൾ പുരോഗമിക്കുന്നു.

<u>3. സൈബർ വാൾ</u>

ഡിജിറ്റൽ ഇടപാടുകളുടെ സുരക്ഷ ഉറപ്പാക്കുന്നതിനും സൈബർ തട്ടിപ്പുകൾ തടയുന്നതിനുമായി കേരള പോലീസ് ആവിഷ്കരിച്ച പദ്ധതിയാണ് സൈബർ വാൾ. ഫോൺ നമ്പറുകൾ, ഇ-മെയിൽ വിലാസങ്ങൾ, ആപ്ലിക്കേഷനുകൾ, വെബ്സൈറ്റ് URL-കൾ, സന്ദേശങ്ങൾ, ബാങ്ക് അക്കൗണ്ടുകൾ, IP വിലാസങ്ങൾ തുടങ്ങിയവ വിശകലനം ചെയ്ത് Trust Score നിർണയിക്കുന്നതിലൂടെ സംശയാസ്പദമായ ഡിജിറ്റൽ ഇടപാടുകളും സൈബർ ഭീഷണികളും തിരിച്ചറിയുകയാണ് പദ്ധതിയുടെ ലക്ഷ്യം.

<u>4. സെക്യൂരിറ്റി ഓപ്പറേഷൻസ് സെന്റർ (SOC)</u>

കേരള പോലീസും C-DOT-ഉം സംയുക്തമായി സ്ഥാപിച്ച ആർട്ടിഫിഷ്യൽ ഇന്റലിജൻസ് അധിഷ്ഠിത സെക്യൂരിറ്റി ഓപ്പറേഷൻസ് സെന്റർ (SOC) 2025 മാർച്ച് 1-ന് ഉദ്ഘാടനം ചെയ്തു. C-DOT വികസിപ്പിച്ച ത്രിനേത്ര സോഫ്റ്റ്വെയർ ഉപയോഗിച്ച് പോലീസ് നെറ്റ്വർക്കുകൾ 24 മണിക്കൂറും നിരീക്ഷിക്കുകയും സുരക്ഷാ വീഴ്ചകളും സൈബർ ഭീഷണികളും കണ്ടെത്തി മുന്നറിയിപ്പുകൾ നൽകുകയും ചെയ്യുന്നു. നിലവിൽ പോലീസ് ആസ്ഥാനം, മേഖലാ-റേഞ്ച് ഓഫീസുകൾ, ജില്ലാ പോലീസ്

മേധാവിമാരുടെ ഓഫീസുകൾ എന്നിവിടങ്ങളിലെ കമ്പ്യൂട്ടറുകൾ SOC-യുമായി ബന്ധിപ്പിച്ചിട്ടുണ്ട്. പോലീസ് സ്റ്റേഷനുകൾ ഉൾപ്പെടെ വകുപ്പിലെ മുഴുവൻ കമ്പ്യൂട്ടറുകളെയും ഫയർവാളുകളെയും SOC-യുമായി സംയോജിപ്പിച്ച് സൈബർ സുരക്ഷ കൂടുതൽ ശക്തിപ്പെടുത്തുന്നതിനുള്ള നടപടികൾ സ്വീകരിച്ചുവരുന്നു.

സെക്ഷൻ ഓഫീസർ