പതിനാറാം കേരളനിയമസഭ

രണ്ടാം സമ്മേളനം

നക്ഷത്രചിഹ്നമിട്ട ചോദ്യം നമ്പർ: 191 27-10-2026-ൽ മറുപടിയ്ക്ക്

ഓൺലൈൻ സൈബർ പരാതി പോർട്ടൽ

ചോദ്യം ഉന്നയിച്ച അംഗങ്ങൾ

ശ്രീ. ടോണി ചമ്മണി

ശ്രീ. എം. വിൻസെന്റ്

ശ്രീ. വി. എസ്. ജോയി

ശ്രീ. കെ. നീലകണ്ഠൻ

മറുപടി നൽകിയ മന്ത്രി

ശ്രീ. രമേശ് ചെന്നിത്തല

(ആഭ്യന്തര- വിജിലൻസ്, കയർ വകുപ്പ് മന്ത്രി)

(എ) സൈബർ കുറ്റകൃത്യങ്ങൾ റിപ്പോർട്ട് ചെയ്യുന്നതിനുള്ള ടോൾ ഫ്രീ ഹെൽപ്ലൈൻ നമ്പരായ 1930-നെക്കുറിച്ചും ഓൺലൈൻ സൈബർ പരാതി പോർട്ടലിനെക്കുറിച്ചും പൊതുജനങ്ങളിൽ അവബോധം സൃഷ്ടിക്കുന്നതിനും പരാതികളിൽ സമയബന്ധിതമായ നടപടി ഉറപ്പാക്കുന്നതിനും സ്വീകരിച്ചുവരുന്ന നടപടികൾ വിശദമാക്കാമോ;

മറുപടി: കേരള പോലീസിന്റെ സൈബർ ഓപ്പറേഷൻസ് വിഭാഗത്തിന്റെ നേതൃത്വത്തിൽ സൈബർ സാമ്പത്തിക തട്ടിപ്പുകൾ റിപ്പോർട്ട് ചെയ്യുന്നതിനും തട്ടിപ്പിലൂടെ നഷ്ടപ്പെട്ട തുകയുടെ തുടർ കൈമാറ്റം തടയുന്നതിനും അടിയന്തര നടപടികൾ സ്വീകരിച്ചു വരുന്നു. സൈബർ സാമ്പത്തിക തട്ടിപ്പിനിരയാകുന്നവർക്ക് 1930 എന്ന ടോൾ ഫ്രീ ഹെൽപ്പ് ലൈൻ നമ്പർ മുഖേനയോ നാഷണൽ സൈബർ ക്രൈം റിപ്പോർട്ടിംഗ് പോർട്ടലായ www.cybercrime.gov.in മുഖേനയോ പരാതി രജിസ്റ്റർ ചെയ്യാവുന്നതാണ്. പരാതി ലഭിക്കുന്ന മുറയ്ക്ക് ബന്ധപ്പെട്ട ബാങ്കുകളുമായി ഏകോപനം നടത്തി ഇടപാട് വിവരങ്ങൾ ശേഖരിക്കുകയും തട്ടിപ്പിലൂടെ നഷ്ടപ്പെട്ട തുകയുടെ തുടർ കൈമാറ്റം തടയുന്നതിനും ലഭ്യമായ സാഹചര്യങ്ങളിൽ തുക തടഞ്ഞു വയ്ക്കുന്നതിനും ആവശ്യമായ നടപടി സ്വീകരിക്കുകയും ചെയ്യുന്നു. തട്ടിപ്പുമായി ബന്ധപ്പെട്ട ബാങ്ക് അക്കൗണ്ട് വിവരങ്ങളും സാമ്പത്തിക ഇടപാടുകളുടെ വിശദാംശങ്ങളും ശേഖരിച്ച് തുടർ അന്വേഷണത്തിനായി ബന്ധപ്പെട്ട അന്വേഷണ ഉദ്യോഗസ്ഥർക്ക് കൈമാറുകയും ചെയ്യുന്നു.

സൈബർ സാമ്പത്തിക തട്ടിപ്പുകളുടെ വിവിധ രീതികൾ, തട്ടിപ്പുകാർ അവലംബിക്കുന്ന തന്ത്രങ്ങൾ, സ്വീകരിക്കേണ്ട മുൻകരുതലുകൾ എന്നിവ സംബന്ധിച്ച് പൊതുജനങ്ങളിൽ അവബോധം സൃഷ്ടിക്കുന്നതിനായി ബോധവൽക്കരണ വീഡിയോകളും പോസ്റ്ററുകളും തയ്യാറാക്കി പ്രചരിപ്പിച്ചുവരുന്നു. സിനിമാ രംഗത്തെ പ്രമുഖരുടെ പങ്കാളിത്തത്തോടെ തയ്യാറാക്കുന്ന ബോധവൽക്കരണ വീഡിയോകൾ കേരള പോലീസിന്റെ ഔദ്യോഗിക സാമൂഹിക മാധ്യമ പേജുകൾ ഉൾപ്പെടെയുള്ള നവമാധ്യമങ്ങളിലൂടെ പ്രചരിപ്പിക്കുന്നു. കൂടാതെ, റസിഡന്റ്സ് അസോസിയേഷനുകൾ ഉൾപ്പെടെയുള്ള വിവിധ സംഘടനകളുടെ സഹകരണത്തോടെ ബോധവൽക്കരണ ക്ലാസുകളും പൊതുജന സമ്പർക്ക പരിപാടികളും സംഘടിപ്പിക്കുകയും കേരള പോലീസ് മീഡിയ സെന്റർ മുഖേന ഓൺലൈൻ മുന്നറിയിപ്പുകളും ബോധവൽക്കരണ സന്ദേശങ്ങളും നൽകുകയും ചെയ്യുന്നു.

സൈബർ സാമ്പത്തിക തട്ടിപ്പുകളുടെ സ്വഭാവവും പ്രവണതകളും വിശകലനം ചെയ്ത് കുറ്റകൃത്യങ്ങൾ തടയുന്നതിനും കുറ്റവാളികളെ കണ്ടെത്തുന്നതിനും ആവശ്യമായ നടപടികൾ സ്വീകരിച്ചുവരുന്നു. ഇതിന്റെ ഭാഗമായി, 'ഓപ്പറേഷൻ സൈ-ഹണ്ട്' ഉൾപ്പെടെയുള്ള പ്രത്യേക പരിശോധനാ പ്രവർത്തനങ്ങളിലൂടെ സൈബർ തട്ടിപ്പുകൾക്കായി ഉപയോഗിക്കുന്ന മ്യൂൾ ബാങ്ക് അക്കൗണ്ടുകൾ കണ്ടെത്തുകയും അവയുടെ ദുരുപയോഗവുമായി ബന്ധപ്പെട്ട അക്കൗണ്ട് ഉടമകളെയും മറ്റ് പ്രതികളെയും തിരിച്ചറിഞ്ഞ് നിയമാനുസൃതമായ നടപടികൾ സ്വീകരിക്കുകയും ചെയ്യുന്നു. തട്ടിപ്പുമായി ബന്ധപ്പെട്ട ബാങ്ക് അക്കൗണ്ടുകൾ, മൊബൈൽ ഫോൺ നമ്പറുകൾ, മൊബൈൽ ഉപകരണങ്ങൾ എന്നിവ സംബന്ധിച്ച വിവരങ്ങൾ വിശദമായി പരിശോധിച്ച്, ആവശ്യമായ സാഹചര്യങ്ങളിൽ ബന്ധപ്പെട്ട ബാങ്കുകളുമായും ടെലികോം സേവനദാതാക്കളുമായും ഏകോപനം നടത്തി അക്കൗണ്ടുകൾ മരവിപ്പിക്കുന്നതിനും മൊബൈൽ നമ്പറുകളും ഉപകരണങ്ങളും ബ്ലോക്ക് ചെയ്യുന്നതിനും നടപടികൾ സ്വീകരിക്കുന്നു. ഇത്തരം നടപടികളിലൂടെ സൈബർ സാമ്പത്തിക തട്ടിപ്പുകൾക്കായി ഉപയോഗിക്കുന്ന സാമ്പത്തിക-സാങ്കേതിക സംവിധാനങ്ങൾ തടസ്സപ്പെടുത്തുന്നതിനും കുറ്റകൃത്യങ്ങളുടെ ആവർത്തനം കുറയ്ക്കുന്നതിനും കുറ്റവാളികളെ കണ്ടെത്തുന്നതിനും ലക്ഷ്യമിടുന്നു.

(ബി) ഓൺലൈൻ സൈബർ പരാതി പോർട്ടൽ വഴി ലഭിക്കുന്ന പരാതികളിൽ വേഗത്തിൽ നടപടി സ്വീകരിക്കുന്നതിന് നിലവിൽ എന്തെല്ലാം സംവിധാനങ്ങളാണുള്ളത്; വിശദമാക്കാമോ;

<u>മറുപടി:</u> സൈബർ സാമ്പത്തിക തട്ടിപ്പുകളുമായി ബന്ധപ്പെട്ട പരാതികളിൽ സമയബന്ധിതമായി നടപടി സ്വീകരിക്കുന്നതിനും തട്ടിപ്പിലൂടെ നഷ്ടപ്പെട്ട തുകയുടെ തുടർ കൈമാറ്റം തടയുന്നതിനുമായി വിവിധ സാങ്കേതിക സംവിധാനങ്ങളും ഏകോപന സംവിധാനങ്ങളും നടപ്പിലാക്കിയിട്ടുണ്ട്. നാഷണൽ സൈബർ ക്രൈം റിപ്പോർട്ടിംഗ് പോർട്ടലും (NCRP) ബാങ്കുകളുടെയും ടെലികോം സേവനദാതാക്കളുടെയും (TSP) സംവിധാനങ്ങളും സംയോജിപ്പിച്ചിട്ടുള്ളതിനാൽ പരാതികൾ ലഭിക്കുന്ന മുറയ്ക്ക് ബന്ധപ്പെട്ട ഇടപാട് വിവരങ്ങൾ ശേഖരിക്കുന്നതിനും തട്ടിപ്പിലൂടെ കൈമാറ്റം ചെയ്യപ്പെട്ട തുക തടഞ്ഞുവയ്ക്കുന്നതിനുള്ള നടപടികൾ സ്വീകരിക്കുന്നതിനും സാധിക്കുന്നു.

കേരള പോലീസ് ആസ്ഥാനത്തെ സൈബർ ഓപ്പറേഷൻസ് വിഭാഗത്തിന്റെ നേതൃത്വത്തിൽ പ്രവർത്തിക്കുന്ന ജോയിന്റ് സൈബർ ക്രൈം കോർഡിനേഷൻ ടീം (JCCT) മുഖേന ബാങ്ക് ഉദ്യോഗസ്ഥരുമായി നേരിട്ട് ഏകോപനം നടത്തി ഇടപാട് വിവരങ്ങൾ വേഗത്തിൽ ശേഖരിക്കുകയും തട്ടിപ്പിലൂടെ നഷ്ടപ്പെട്ട തുക കണ്ടെത്തി തടഞ്ഞുവയ്ക്കുന്നതിനുള്ള നടപടികൾ സ്വീകരിക്കുകയും ചെയ്യുന്നു.

കൂടാതെ, NCRP പോർട്ടലിൽ ലഭിക്കുന്ന അഞ്ച് ലക്ഷം രൂപയ്ക്ക് മുകളിലുള്ള സൈബർ സാമ്പത്തിക തട്ടിപ്പ് പരാതികളിൽ എഫ്.ഐ.ആർ രജിസ്ട്രേഷൻ വേഗത്തിലാക്കുന്നതിനായി ഇ-സീറോ എഫ്.ഐ.ആർ (e-Zero FIR) സംവിധാനം നടപ്പിലാക്കിയിട്ടുണ്ട്. കേരള പോലീസിന്റെ iCOPS (Integrated Core Policing System) സംവിധാനവുമായി സംയോജിപ്പിച്ചിട്ടുള്ള ഈ സംവിധാനം മുഖേന നിശ്ചിത മാനദണ്ഡങ്ങൾ പാലിക്കുന്ന പരാതികളിൽ എഫ്.ഐ.ആർ രജിസ്ട്രേഷൻ നടപടികൾ വേഗത്തിലാക്കാനും അന്വേഷണം സമയബന്ധിതമായി ആരംഭിക്കാനും സാധിക്കുന്നു.

(സി) സൈബർ സാമ്പത്തിക തട്ടിപ്പുകൾക്ക് ഇരയാകുന്നവരുടെ പണം നഷ്ടപ്പെടുന്നത് തടയുന്നതിനും നഷ്ടപ്പെട്ട തുക വീണ്ടെടുക്കുന്നതിനും അടിയന്തര ഇടപെടൽ ഉറപ്പാക്കുന്നുണ്ടോ; ഹെൽപ്‌ലൈൻ നമ്പർ 1930 വഴിയും ഓൺലൈൻ പോർട്ടൽ വഴിയും ലഭിക്കുന്ന പരാതികളുടെ തുടർനടപടികൾ പരാതിക്കാർക്ക് അറിയുന്നതിനുള്ള സംവിധാനം നിലവിലുണ്ടോ;

മറുപടി: സൈബർ സാമ്പത്തിക തട്ടിപ്പുകളിലൂടെ നഷ്ടപ്പെടുന്ന തുകയുടെ തുടർ കൈമാറ്റം തടയുന്നതിനും തട്ടിപ്പിനിരയായവർക്ക് തുക തിരികെ ലഭ്യമാക്കുന്നതിനുമായി നാഷണൽ സൈബർ ക്രൈം റിപ്പോർട്ടിംഗ് പോർട്ടലിൽ (NCRP) ബാങ്കിംഗ് സംവിധാനങ്ങളുമായി സാങ്കേതിക സംയോജനം നടപ്പിലാക്കിയിട്ടുണ്ട്. ഇതിന്റെ ഭാഗമായി, CFCFRMS (Citizen Financial Cyber Fraud Reporting and Management System) മൊഡ്യൂൾ മുഖേന പരാതികളിലെ വിവരങ്ങൾ ബന്ധപ്പെട്ട ബാങ്കുകൾക്ക് കൈമാറുകയും തടഞ്ഞുവയ്ക്കാൻ സാധിക്കുന്ന തുക ഹോൾഡ് ചെയ്യുന്നതിനുള്ള നടപടികൾ സ്വീകരിക്കുകയും ചെയ്യുന്നു. തുടർന്ന്, മണി റീസ്റ്റോറേഷൻ മോഡ്യൂൾ (MRM) മുഖേന നിലവിലുള്ള നടപടിക്രമങ്ങൾക്കനുസൃതമായി തുക പരാതിക്കാർക്ക് തിരികെ ലഭ്യമാക്കുന്നതിനുള്ള നടപടികൾ സ്വീകരിക്കുന്നു.

പരാതികളുടെ നിലവിലെ സ്ഥിതിയും സ്വീകരിച്ച തുടർനടപടികളും അറിയുന്നതിനായി NCRP പോർട്ടലിൽ *Track Your Complaint* സൗകര്യം ലഭ്യമാണ്. കൂടാതെ, തുക തിരികെ ലഭ്യമാക്കുന്നതിനുള്ള നടപടികളുമായി ബന്ധപ്പെട്ട വിവരങ്ങൾ ലഭിക്കുന്നതിനും മാർഗനിർദേശങ്ങൾക്കുമായി പരാതിക്കാർക്ക് 1930 എന്ന ടോൾ ഫ്രീ ഹെൽപ്‌ലൈൻ നമ്പറിലോ 0471-2300042 എന്ന നമ്പറിലോ ബന്ധപ്പെടാവുന്നതാണ്. ഈ സംവിധാനങ്ങളിലൂടെ പരാതികളുടെ തുടർനടപടികളിൽ സുതാര്യത ഉറപ്പാക്കുന്നതിനും പരാതിക്കാർക്ക് സമയബന്ധിതമായി വിവരങ്ങൾ ലഭ്യമാക്കുന്നതിനും നടപടി സ്വീകരിച്ചുവരുന്നു.

(ഡി) സൈബർ കുറ്റകൃത്യങ്ങൾ വർധിച്ചുവരുന്ന സാഹചര്യത്തിൽ വിദ്യാർഥികൾ ഉൾപ്പെടെയുള്ള പൊതുജനങ്ങൾക്കായി ബോധവത്കരണ പരിപാടികൾ കൂടുതൽ വ്യാപിപ്പിക്കാൻ നടപടി സ്വീകരിക്കുമോ?

മറുപടി: കുട്ടികളിൽ സൈബർ സുരക്ഷാ അവബോധം വളർത്തുന്നതിനും അവരെ സൈബർ കുറ്റകൃത്യങ്ങളിൽനിന്ന് സംരക്ഷിക്കുന്നതിനുമായി കേരള പോലീസ് 'KID GLOVE' എന്ന പേരിൽ ബോധവൽക്കരണ പരിപാടി നടപ്പിലാക്കിയിട്ടുണ്ട്. ഇതിന്റെ ഭാഗമായി, കുട്ടികൾക്ക് ഓൺലൈൻ സുരക്ഷ, സൈബർ ഭീഷണികൾ, സാമ്പത്തിക തട്ടിപ്പുകൾ, വ്യക്തിഗത വിവരങ്ങളുടെ സംരക്ഷണം എന്നിവ സംബന്ധിച്ച് അവബോധം നൽകിവരുന്നു. കൂടാതെ, സ്കൂളുകളിലും കോളേജുകളിലും വിദ്യാർത്ഥികൾക്കായി സൈബർ സുരക്ഷാ ബോധവൽക്കരണ ക്ലാസുകളും സംഘടിപ്പിക്കുന്നു.

പൊതുജനങ്ങളിൽ സൈബർ സുരക്ഷാ അവബോധം വ്യാപിപ്പിക്കുന്നതിനായി റസിഡന്റ്സ് അസോസിയേഷനുകളുടെ സഹകരണത്തോടെ ബോധവൽക്കരണ പരിപാടികൾ സംഘടിപ്പിക്കുകയും എഫ്.എം. റേഡിയോ, ആകാശവാണി തുടങ്ങിയ മാധ്യമങ്ങളിലൂടെ മുന്നറിയിപ്പുകളും സുരക്ഷാ സന്ദേശങ്ങളും പ്രചരിപ്പിക്കുകയും ചെയ്യുന്നു. സൈബർ സാമ്പത്തിക തട്ടിപ്പുകൾ തിരിച്ചറിയുന്നതിനും സുരക്ഷിതമായ ഓൺലൈൻ ഇടപാടുകൾ നടത്തുന്നതിനും തട്ടിപ്പിനിരയായാൽ ഉടൻ 1930 എന്ന ഹെൽപ്‌ലൈൻ നമ്പറിൽ പരാതി നൽകുന്നതിനും പൊതുജനങ്ങളെ പ്രാപ്തരാക്കുകയാണ് ഈ പ്രവർത്തനങ്ങളുടെ ലക്ഷ്യം.

സൈബർ സാമ്പത്തിക തട്ടിപ്പുകൾ തടയുന്നതിൽ ബാങ്ക് ഉദ്യോഗസ്ഥരുടെ പങ്ക് കണക്കിലെടുത്ത്, സംശയാസ്പദമായ ഇടപാടുകളും മ്യൂൾ അക്കൗണ്ടുകളും തിരിച്ചറിയൽ, പരാതികളിൽ അടിയന്തര നടപടി സ്വീകരിക്കൽ, തട്ടിപ്പിലൂടെ കൈമാറ്റം ചെയ്യപ്പെട്ട തുക തടഞ്ഞുവയ്ക്കുന്നതിനായി പോലീസുമായി ഏകോപനം നടത്തൽ തുടങ്ങിയ വിഷയങ്ങളിലും ബോധവൽക്കരണവും മാർഗനിർദേശങ്ങളും നൽകിവരുന്നു.

സെക്ഷൻ ഓഫീസർ