15 -ാം കേരള നിയമസഭ

11 -ാം സമ്മേളനം

നക്ഷത്ര ചിഹ്നം ഇല്ലാത്ത ചോദ്യം നം. 138 **10-06-2024 - ൽ മറുപടിയ്ക്ക്**

സൈബർ കുറ്റകൃത്യങ്ങൾ തടയാൻ നടപടി

ചോദ്യം		ഉത്തരം	
ശ്രീ. മോൻസ് ജോസഫ്		**ശ്രീ. പിണറായി വിജയൻ (മുഖ്യമന്ത്രി)**	
(എ)	സംസ്ഥാനത്ത് സൈബർ കുറ്റകൃത്യങ്ങൾ പെരുകുന്നത് സർക്കാരിന്റെ ശ്രദ്ധയിൽപെട്ടിട്ടുണ്ടോ; ആയത് തടയുന്നതിന് എന്തെല്ലാം നടപടികൾ സ്വീകരിച്ചു എന്ന് വ്യക്തമാക്കാമോ; കഴിഞ്ഞ ആറു മാസ കാലയളവിൽ എത്ര സൈബർ കേസ്സുകൾ തിരുവനന്തപുരം ജില്ലയിൽ റിപ്പോർട്ട് ചെയ്യപ്പെട്ടിട്ടുണ്ട്; ഇവയിൽ എത്രയെണ്ണത്തിന് എഫ്.ഐ.ആർ. രജിസ്റ്റർ ചെയ്തു; ആയതിന്റെ വിശദാംശം വെളിപ്പെടുത്താമോ;	(എ)	വിവിധ സർക്കാർ സേവനങ്ങളും ബാങ്കിംഗ് സേവനങ്ങളും ഇന്റർനെറ്റ് സഹായത്തോടെ സാധാരണക്കാരിലേക്ക് എത്തുകയും ഉപഭോഗം വർദ്ധിക്കുകയും ചെയ്തതനുസരിച്ച് കുറ്റകൃത്യങ്ങളും വർധിച്ചുവരുന്നതായി കണ്ടെത്തിയിട്ടുണ്ട്. സൈബർ കുറ്റകൃത്യങ്ങൾ തടയുന്നതിനായി താഴെപറയുന്ന നടപടികൾ സ്വീകരിച്ചിട്ടുണ്ട്. 05.01.2024-ലെ സർക്കാർ ഉത്തരവ് (കൈ)നം.04/2024/ആഭ്യ. പ്രകാരം സംസ്ഥാനത്ത് സൈബർ പോലീസ് ഡിവിഷൻ ആരംഭിക്കുന്നതിന് അനുമതി നൽകിയിരുന്നു. പ്രസ്തുത സൈബർ ഡിവിഷനിൽ താഴെപ്പറയുന്ന തസ്തികകൾ അനുവദിച്ചിട്ടുണ്ട്. തസ്തിക – എണ്ണം എസ്.പി. – 2 ഡി.വൈ.എസ്.പി. – 4 ഐ.ഒ.പി – 13 എസ്.ഐ – 39 എസ്.സി.പി.ഒ – 84 സി.പി.ഒ – 63 കൂടാതെ എല്ലാ പോലീസ് ജില്ലകളിലും സൈബർ പോലീസ് സ്റ്റേഷനുകളും പ്രവർത്തിച്ചു വരുന്നു. • ഓൺലൈൻ ലോൺ തട്ടിപ്പുകളെ കുറിച്ച് വിവരം നൽകുന്നതിനായി കേരള പോലീസിന്റെ 9497980900 എന്ന വാട്സ്ആപ്പ് നമ്പറും 1930 എന്ന ടോൾ ഫ്രീ നമ്പറും 24 മണിക്കൂറും ലഭ്യമാണ്. • റിസർവ് ബാങ്ക് ഓഫ് ഇന്ത്യ അംഗീകരിച്ച നോൺ ബാങ്കിംഗ് ഫിനാൻഷ്യൽ കോർപ്പറേഷൻ ലിസ്റ്റിൽ ഉൾപ്പെട്ട ലോൺ

			ആപ്പുകളെ കുറിച്ചും ഓൺലൈൻ ലോൺ തട്ടിപ്പുകളെ കുറിച്ചും ജനങ്ങളിൽ അവബോധം ഉണ്ടാക്കുന്നതിനും മുഖ്യ ധാരാ മാധ്യമങ്ങളിലൂടെയും സാമൂഹ്യ മാധ്യമങ്ങളിലൂടെയും പ്രചരണ നടപടികൾ സ്വീകരിച്ചിട്ടുണ്ട്. • സൈബർ ഓപ്പറേഷൻസ് വിഭാഗവും സൈബർ ഡോം തിരുവനന്തപുരം, കൊച്ചി, കോഴിക്കോട് യൂണിറ്റുകളും സൈബർ പട്രോളിംഗ് നടത്തി സൈബർ തട്ടിപ്പ് സംഘങ്ങളെ കണ്ടെത്തി സൈബർ സ്പേസിൽ നിന്നും നീക്കം ചെയ്യുന്നത്തിനുള്ള നടപടികൾ തുടർന്നുവരുന്നു. • സൈബർ കുറ്റകൃത്യങ്ങൾ തടയുന്നതിനായി നാഷണൽ സൈബർ ക്രൈം പോർട്ടൽ രൂപീകരിച്ചിട്ടുണ്ട്. 1930 എന്ന നമ്പരിൽ നിന്നും പോർട്ടൽ മുഖേന (www.cybercrime.gov.in) ഓൺലൈനായും പൊതുജനങ്ങൾക്ക് പരാതി അറിയിക്കാവുന്നതാണ്. സാമ്പത്തിക തട്ടിപ്പുകളുമായി ബന്ധപ്പെട്ട് അന്വേഷണ ഏജൻസികളും ബാങ്കുകൾ, RBI, സാമ്പത്തിക ഇടനിലക്കാർ, പേയ്മെന്റ് വാലറ്റുകൾ, NPCI മുതലായവ ഒരുമിച്ച് പ്രവർത്തിക്കുന്ന ഒരു പൊതു സംയോജിത പ്ലാറ്റ്ഫോമാണ് നാഷണൽ സൈബർക്രൈം പോർട്ടൽ. തട്ടിപ്പുകാരിലേക്ക് പോകുന്ന പണത്തിന്റെ ഒഴുക്ക് തടയുന്നതിന് ദ്രുതഗതിയിലുള്ള നടപടി സ്വീകരിക്കാൻ ഇതു വഴി കഴിയുന്നു. • കൂടാതെ സൈബർ കുറ്റകൃത്യങ്ങൾ അന്വേഷിക്കുന്നതിന് പോലീസ് ഉദ്യോഗസ്ഥരെ സജ്ജരാക്കുന്നതിനായി പോലീസ് ട്രെയിനിംഗ് കോളേജിലും, സൈബർ ക്രൈമുമായി ബന്ധപ്പെട്ട കോഴ്സുകൾ നിരന്തരം നടത്തി വരുന്നു. സൈബർ ഇടപാടുകളിലെ ചതിക്കുഴികളെ സംബന്ധിച്ച് ജനങ്ങളെ ബോധവൽക്കരണം നടത്തുന്നതിലേയ്ക്കായി പത്ര - ദൃശ്യമാധ്യമങ്ങൾ വഴി അറിയിപ്പുകൾ നൽകുകയും, വിവിധ സാമൂഹ്യ സംഘടനകൾ, ക്ലബ്ബുകൾ, സ്കൂളുകൾ, കോളേജുകൾ, റസിഡൻസ് അസോസിയേഷനുകൾ മുതലായവയുടെ സഹകരണത്തോടെ ബോധവൽക്കരണ പരിപാടികളും ക്ലാസുകളും നടത്തി വരികയും ചെയ്യുന്നു. കഴിഞ്ഞ 6 മാസക്കാലയളവിൽ തിരുവനന്തപുരം ജില്ലയിൽ 251 സൈബർ കേസുകൾ രജിസ്റ്റർ ചെയ്തിട്ടുണ്ട്.

(ബി)	വ്യാജരേഖ നൽകിയതിന്റെ പേരിൽ കഴിഞ്ഞ ആറുമാസത്തിനുള്ളിൽ സംസ്ഥാനത്ത് എത്ര സിം കാർഡുകളാണ് ബ്ലോക്ക് ചെയ്തതെന്ന് വ്യക്തമാക്കാമോ; സൈബർ തട്ടിപ്പിൽ ഉൾപ്പെട്ട എത്ര മൊബൈൽ ഫോണുകളാണ് കഴിഞ്ഞ 6 മാസത്തിനുള്ളിൽ ബ്ലോക്ക് ചെയ്തതെന്ന് വ്യക്തമാക്കാമോ;	(ബി)	01/12/2023 മുതൽ 31/05/2024 വരെ നാഷണൽ ക്രൈം റിപ്പോർട്ട് പോർട്ടലിൽ റിപ്പോർട്ടായ പരാതികളുടെ അടിസ്ഥാനത്തിൽ 5055 സിം കാർഡുകളും 4766 മൊബൈൽ ഫോണുകളും ബ്ലോക്ക് ചെയ്തിട്ടുണ്ട്.
(സി)	സൈബർ സംഘങ്ങൾക്കായി അനധികൃതമായി സിം കാർഡുകൾ സംഘടിപ്പിച്ച് കൈമാറുന്ന സംഘങ്ങൾ പ്രവർത്തിക്കുന്നതായി ആഭ്യന്തര വകുപ്പിന് കണ്ടെത്താൻ കഴിഞ്ഞിട്ടുണ്ടോ; വിശദാംശം അറിയിക്കാമോ;	(സി)	മലപ്പുറം ജില്ലയിലെ വേങ്ങര പോലീസ് സ്റ്റേഷനിലെ ക്രൈം നമ്പർ 214/2024 കേസിൽ വ്യാജ മൊബൈൽ സിം കാർഡുകളുടെ wholesale dealer ആയ അബ്ദുൾ റോഷൻ എന്ന പ്രതി കർണ്ണാടകയിൽ വച്ച് അറസ്റ്റിലായിട്ടുണ്ട്. ടിയാളിൽ നിന്നും 40000 സിം കാർഡുകളും നൂറ് കണക്കിന് മൊബൈൽ ഡിവൈയ്സും പിടികൂടിയിട്ടുണ്ട്. തൃശ്ശൂർ റൂറൽ സൈബർ ക്രൈം പോലീസ് സ്റ്റേഷൻ ക്രൈം നമ്പർ.14/2024 ആയി റജിസ്റ്റർ ചെയ്ത കേസിൽ തട്ടിപ്പ് സംഘങ്ങൾക്ക് സിം കാർഡ് ആക്ടിവേറ്റ് ചെയ്ത് നൽകിയ വിഷ്ണു എന്ന പ്രതിയെയും ടി സിം കാർഡുകൾ ഉപയോഗപ്പെടുത്തി തട്ടിപ്പ് നടത്തിയ കംബോഡിയൻ സംഘത്തിലെ പ്രധാനി മുഫ്ലിക് എന്ന പ്രതിയെയും അറസ്റ്റ് ചെയ്തിട്ടുണ്ട്.
(ഡി)	രാജ്യത്തെ വിവിധ ഭാഗങ്ങളിൽ നിന്ന് തട്ടിപ്പ് കോളുകൾ വരുന്നത് തടയുന്നതിനും ആയത് നിയന്ത്രിക്കുന്നതിനും സംസ്ഥാന സർക്കാർ എന്തെല്ലാം നടപടി സ്വീകരിച്ചു എന്ന് വ്യക്തമാക്കാമോ; ഇത്തരത്തിലുള്ള എത്ര കേസുകൾ രജിസ്റ്റർ ചെയ്തുവെന്നും എത്രയെണ്ണത്തിൽ നടപടി സ്വീകരിച്ചുവെന്നും വ്യക്തമാക്കാമോ;	(ഡി)	രാജ്യത്തെ വിവിധ ഭാഗങ്ങളിൽ നിന്ന് തട്ടിപ്പ് കോളുകൾ വരുന്നത് തടയുന്നതിനും ആയത് നിയന്ത്രിക്കുന്നതിനും ബോധവൽക്കണ പരിപാടികളും മറ്റും സംഘടിപ്പിച്ചും ഓൺലൈൻ മീഡിയ വഴി അലർട്ട് മെസേജുകൾ നൽകിയും നടപടികൾ സ്വീകരിച്ച് വരുന്നുണ്ട്. കൂടാതെ രാജ്യത്തെ വിവിധ ഭാഗങ്ങളിൽ നിന്നും തട്ടിപ്പ് കോൾ തടയുന്നതിനും ആയത് നിയന്ത്രിക്കുന്നതിനുമായി സിം കാർഡുകളും ഡിവൈസുകളും ബ്ലോക്ക് ചെയ്യുന്നതിനുള്ള നടപടി സ്വീകരിച്ചിട്ടുണ്ട്. 01/12/2023 മുതൽ 31/05/2024 വരെ NCR Portal- ൽ ആകെ 21159 പരാതികൾ റിപ്പോർട്ട് ചെയ്തിട്ടുള്ളതിൽ 1312 കേസുകൾ കേരളത്തിലെ വിവിധ പോലീസ് സ്റ്റേഷനുകളിൽ രജിസ്റ്റർ ചെയ്തിട്ടുള്ളതാണ്.
(ഇ)	മൊബൈലിലെ സന്ദേശങ്ങളുടെയും ലിങ്കുകളുടെയും സമൂഹമാധ്യമ പ്രൊഫൈലുകളുടെയും ആധികാരികത പരിശോധിച്ച് ഉറപ്പുവരുന്ന സൈബർ സേഫ് മൊബൈൽ ആപ്പ് തയ്യാറാക്കുന്നതിന് സംസ്ഥാന പോലീസ് സ്വീകരിച്ച നടപടികൾ വിശദീകരിക്കാമോ; ഫോണുകളിലും വാട്സാപ്പിലും വരുന്ന തട്ടിപ്പ് കോളുകളും മെസ്സേജുകളും പൊതുജനങ്ങൾക്ക് റിപ്പോർട്ട് ചെയ്യാനായി കേന്ദ്ര സർക്കാർ ആരംഭിച്ച ചക്ഷു എന്ന പോർട്ടലിൽ	(ഇ)	സൈബർ ഡിവിഷന്റെ കീഴിൽ നിർമ്മിത ബുദ്ധിയിൽ അധിഷ്ഠിതമായ സൈബർ വാൾ പ്രൊജക്റ്റ് ആരംഭിക്കുന്നതിനുള്ള നടപടികൾ സ്വീകരിച്ച് വരുന്നു. ഈ പ്രൊജക്റ്റിൽ പൊതുജനങ്ങൾക്ക് ഫോൺ നമ്പറുകൾ, സോഷ്യൽ മീഡിയ പ്രൊഫൈലുകൾ, URL- കൾ എന്നിവ വ്യാജമാണോ എന്ന് പരിശോധിക്കാൻ സാധിക്കും. ഈ പ്രൊജക്റ്റ് PoL- App പോലുള്ള പോലീസ് ആപ്ലിക്കേഷനുകളുമായി സംയോജിച്ച് പ്രവർത്തിപ്പിക്കുവാൻ ഉദ്ദേശിക്കുന്നു. ചക്ഷു എന്ന പോർട്ടൽ കേന്ദ്ര സർക്കാർ

	സംസ്ഥാനത്ത് നിന്നും എത്ര കേസുകളാണ് റിപ്പോർട്ട് ചെയ്തതെന്നും എത്രയെണ്ണത്തിൽ നടപടി സ്വീകരിച്ചുവെന്നും വ്യക്തമാക്കാമോ;		നിയന്ത്രണത്തിലായതിനാൽ ഇത് സംബന്ധിച്ച് വിവരങ്ങൾ ലഭ്യമല്ല.
(എഫ്)	തിരുവനന്തപുരം ജില്ലയിൽ ശ്രീകാര്യം പോലീസ് സ്റ്റേഷനിൽ എത്ര സൈബർ കേസ് രജിസ്റ്റർ ചെയ്തു; ഇവയിൽ എത്രയെണ്ണത്തിൽ എഫ്.ഐ.ആർ. ഇട്ടു; പെറ്റീഷൻ നൽകി രസീതു നൽകിയിട്ടും എഫ്.ഐ. ആർ. ഇടാത്തതിനു കാരണം വ്യക്തമാക്കാമോ;	(എഫ്)	തിരുവനന്തപുരം ജില്ലയിൽ ശ്രീകാര്യം പോലീസ് സ്റ്റേഷനിൽ 20.05.2021 - മുതൽ 02.06.2024 വരെ മൂന്ന് കേസ്സുകൾ രജിസ്റ്റർ ചെയ്തിട്ടുണ്ട്. കൂടാതെ 08 പരാതികളും ലഭിച്ചിട്ടുണ്ട്. ആയതിൽ 02 പരാതിയിന്മേൽ കേസ്സ് രജിസ്റ്റർ ചെയ്ത് അന്വേഷണം നടത്തിയിട്ടുള്ളതാണ്. പരാതിയിൽ പറഞ്ഞിട്ടുള്ള കുറ്റകൃത്യത്തെ സംബന്ധിച്ച് വ്യക്തതയില്ലാത്ത സന്ദർഭങ്ങളിലും, പരാതിക്കാരന് തുടർ നടപടികൾ ആവശ്യമില്ലായെന്ന് പറഞ്ഞിട്ടുള്ള പരാതികളിലും ഒഴികെ FIR രജിസ്റ്റർ ചെയ്തിട്ടുള്ളതാണ്.
(ജി)	സൈബർ കേസ് രജിസ്റ്റർ ചെയ്യുന്നതിനുള്ള നമ്പരായ 1930-യിൽ രജിസ്റ്റർ ചെയ്ത പെറ്റിഷൻ അവിടെ നിന്നും തിരികെ ശ്രീകാര്യം സ്റേറഷനിൽ എത്തിയതിൽ എഫ്.ഐ.ആർ. ഇടാത്തതിന് കാരണം വ്യക്തമാക്കാമോ; ഇവ അടിയന്തരമായി എഫ്.ഐ. ആർ. ഇടുന്നതിന് നടപടി സ്വീകരിക്കുമോ?	(ജി)	എൻ സി ആർ പി പോർട്ടൽ നമ്പരായ 1930 ൽ രജിസ്റ്റർ ചെയ്യുന്ന പരാതികളിൽ നഷ്ടപ്പെട്ട രൂപ ഹോൾഡ് ചെയ്യപ്പെടുന്ന സാഹചര്യത്തിൽ ആയത് വീണ്ടെടുക്കുവാൻ കേസ് രജിസ്റ്റർ ചെയ്തു വരുന്നു. 1930- ലേക്ക് വരുന്ന മറ്റു പരാതികളിലെല്ലാം സ്വീകരിക്കേണ്ട ആവശ്യമായ നടപടികൾ വിശദീകരിച്ച് 15.11.2023-ൽ സംസ്ഥാന പോലീസ് മേധാവി No.D7-188683/2023/PHQ Dtd പ്രകാരം നിർദ്ദേശങ്ങൾ പുറപ്പെടുവിച്ചിട്ടുള്ളതും അത് പ്രകാരമുള്ള നടപടികൾ ശ്രീകാര്യം പോലീസ് സ്റ്റേഷനിൽ സ്വീകരിച്ചുവരുന്നതുമാണ്. പകർപ്പ് അനുബന്ധമായി ചേർക്കുന്നു.

സെക്ഷൻ ഓഫീസർ

POLICE **DEPARTMENT**

KERALA

No. D7-188683/2023/PHQ
Police Headquarters,
Thiruvananthapuram
✉phq.pol@kerala.gov.in
✆04712721547
Dated. 15-11-2023

STANDARD OPERATING PROCEDURE (SOP) TO BE FOLLOWED FOR THE EFFECTIVE RELEASE OF DEFRAUDED AMOUNTS IDENTIFIED IN VARIOUS BANK ACCOUNTS TO THE ELIGIBLE VICTIMS

CONFIDENTIAL

A large amount of defrauded money has been frozen through the active intervention of Cyber Operations team of Kerala Police in the NCRP portal. However the release of frozen amounts to eligible victims has not gained much momentum. The major reason for the same is the lack of clarity among the field officers on the procedure to be followed in the release of frozen amounts. It has become imperative to issue comprehensive guidelines in this regard. A Standard Operating Procedure (SOP) to be followed for the seizure and release of defrauded amounts located in various bank accounts is issued herewith.

Guidelines for release of defrauded money held in various bank accounts

1. The retrieval of key information on the recovered amounts from NCRP Portal is the first step to be followed. The SHOs can access the, Portal to elicit information on the details of defrauded amounts recovered and held in various bank accounts in respect of any complient registered on the portal.

2. Subsequently the KYC details of the account in which the amount has been located may be obtained on a notice under 91 CrPC issued to the competent bank official.

3. The defrauded amounts which are located in various bank accounts through the portal needs to be seized under 102 CrPC and placed under the interim custody of the competent Bank Official subject to further orders of the Court concerned. A Seizure Mahazar needs to be prepared in this regard and a report in this regard shall be sent to the Court having jurisdiction.

4. Module and format for digital seizure and entrustment of defrauded amounts located in bank accounts has been introduced in iCoPS (CCTNS). It is accessible through the path below which has been registered

Investigation > Mahazar > Account Seizure Mahazar

The standardized format is made available in the above path which

D7-188683/2023/PHQ

may be duly filled and digitally signed.

5. The procedure described above will apply only in cases where an FIR already exists in respect of which a seizure under 102 CrPC is contemplated. If the FIR does not exist and a seizure report under 102 CrPC is to be prepared, it can be done in the iCoPs through the path below:

Utilities > Digital Signature

Any document (in pdf) can be digitally signed in the above module. The digital seizure cum entrustment mahazar may be prepared in the format enclosed and uploaded to the above module for digital signature.

6. Digital signature of the investigating officer can be affixed on the Seizure Mahazar through either of the modules in para 4 or 5 above for the seizure of defrauded amount. After signature, it can be electronically transmitted to the competent bank official for endorsing his digital signature indicating the acceptance or third party custody subject to further orders of the Court concerned.

7. The Seizure and entrustment (Kacheet) Mahazar prepared as detailed above can be submitted to the Court concerned through email immediately and through the ICJS platform at the time of charge sheet.

8. Once the seizure and entrustment Mahazar is produced before the Court the victim may be intimated.

9. The Victim may approach the Court concerned and file a petition seeking release of the seized amount to his bank account from the custodian bank authorities under chapter XXXIV of CrPC.

10. The release orders, if any, issued by the Court concerned, may be sent to the Bank Authority holding interim custody of the amount for the release of defrauded money.

11. When defrauded amount from a compliant has been located in different bank accounts, separate Seizure Mahazar need to be prepared for the respective amounts seized from each account.

SHAIK DARVESH SAHEB IPS
State Police Chief

To : All Unit Heads for information and necessary action.
Copy To : CAs to SPC/ADGP [illegible] HQ/ all Staff Officers in PHQ
The D Space

D7-188683/2023/PHQ

a4c516