STATE POLICE MEDIA CENTRE
KERALA POLICE

Police Headquarters
Vazhuthacaud
Thiruvananthapuram - 695010
0471 2318188
info.pol@kerala.gov.in
statepolicemediacentre

No.125/PR/SPMC/PHQ/2026 Date: 06.03.2026

ഓപ്പറേഷൻ "സൈഹണ്ട് 2.0": 165 പേർ അറസ്റ്റിൽ 455 കേസുകൾ രജിസ്റ്റർ ചെയ്തു

സൈബർ സാമ്പത്തിക കുറ്റകൃത്യങ്ങൾ തടയുന്നതിൻറെ ഭാഗമായി സംസ്ഥാനവ്യാപകമായി നടത്തിയ സ്പെഷ്യൽ ഡ്രൈവിൽ 165 പേരെ അറസ്റ് ചെയ്യുകയും 455 കേസുകൾ രജിസ്റ്റർ ചെയ്യുകയും ചെയ്തു.

"ഓപ്പറേഷൻ സൈഹണ്ട് 2.0" എന്ന പേരിൽ നടത്തിയ സ്പെഷ്യൽ ഡ്രൈവിൽ 1168 റെയ്ഡുകൾ നടത്തുകയും 216 പേർക്ക് നോട്ടീസ് നൽകുകയും 306 ഓളം ഉപകരണങ്ങൾ പിടിച്ചെടുക്കുകയും ചെയ്തു.

ഡിജിറ്റൽ പ്ലാറ്റ്ഫോമുകളും ബാങ്കിംഗ് സംവിധാനങ്ങളും ദുരുപയോഗം ചെയ്ത് രാജ്യത്തുടനീളം നടക്കുന്ന സൈബർ തട്ടിപ്പുകൾക്ക് പിന്തുണ നൽകുന്ന ശൃംഖലകളെ കണ്ടെത്തുകയും തടയുകയും ചെയ്യുക എന്ന ലക്ഷ്യത്തോടെയാണ് സ്പെഷ്യൽ ഡ്രൈവ് നടത്തിയത്.

സംസ്ഥാന പോലീസ് മേധാവിയുടെ നിർദ്ദേശപ്രകാരം 2026 മാർച്ച് 5ന് രാവിലെ 07:00 മണി മുതൽ സംസ്ഥാനത്തെ എല്ലാ പോലീസ് സ്റ്റേഷൻ പരിധികളിലും ഒരേസമയം പരിശോധനകളും റെയ്ഡുകളും തുടർനടപടികളും ആരംഭിച്ചു.

സൈബർ ഓപ്പറേഷൻസ് വിംഗിന്റെ കേന്ദ്രീകൃത മേൽനോട്ടത്തിലും റേഞ്ച് ഡി.ഐ.ജിമാരുടെയും ജില്ലാ പോലീസ് മേധാവികളുടെയും നേതൃത്വത്തിലുമാണ് പ്രവർത്തനങ്ങൾ ഏകോപിതമായി നടപ്പിലാക്കിയത്.

സാധാരണ കേസ്അടിസ്ഥാനത്തിലുള്ള അന്വേഷണ രീതിയിൽ നിന്ന് വ്യത്യസ്തമായി, സൈബർ തട്ടിപ്പുകളുടെ സാമ്പത്തിക അടിസ്ഥാന ഘടകങ്ങളെ ലക്ഷ്യമിട്ടുള്ള ഇന്റലിജൻസ് അധിഷ്ഠിത സമീപനമാണ് ഈ ഓപ്പറേഷനിൽ

സ്വീകരിച്ചത്. മ്യൂൾ ബാങ്ക് അക്കൗണ്ടുകൾ, തട്ടിപ്പിലൂടെ ലഭിക്കുന്ന പണം പിൻവലിക്കുന്ന സൗകര്യങ്ങൾ ഒരുക്കുന്നവർ, സാമ്പത്തിക ഇടനിലക്കാർ എന്നിവരുമായി ബന്ധപ്പെട്ട വിവരങ്ങൾ കേന്ദ്രീകരിച്ചാണ് പരിശോധനകളും നടപടികളും നടത്തിയത്.

ഇന്റലിജൻസ് വിശകലനത്തിന്റെ അടിസ്ഥാനത്തിൽ 422 മ്യൂൾ ബാങ്ക് അക്കൗണ്ടുകൾ കണ്ടെത്തുകയും 670 പേർ ചെക്ക് വഴി പണം പിൻവലിക്കുന്ന കേസുകളിലും 263 പേർ എ.ടി.എം. വഴി പിൻവലിച്ച കേസുകളിലും ഉൾപെട്ടതായും കണ്ടെത്തി

ദേശീയ സൈബർ ക്രൈം റിപ്പോർട്ടിംഗ് പോർട്ടൽ (NCRP) വഴി ലഭ്യമായ പരാതികളും സാമ്പത്തിക ഇന്റലിജൻസും വിശകലനം ചെയ്താണ് പരിശോധനകൾ ആസൂത്രണം ചെയ്തത്. ചെക്ക് വഴിയും എ.ടി.എം. വഴിയും തട്ടിപ്പിലൂടെ ലഭിച്ച പണം പിൻവലിക്കുന്നവരെയും മ്യൂൾ ബാങ്ക് അക്കൗണ്ടുകൾ നൽകുന്നവരെയും ലക്ഷ്യമിട്ടാണ് റെയ്ഡുകളും തുടർനടപടികളും നടപ്പാക്കിയത്.

ഓപ്പറേഷന്റെ ഭാഗമായി ശേഖരിച്ച വിവരങ്ങളും തെളിവുകളും തുടർ അന്വേഷണങ്ങൾക്കും ഭാവിയിലെ പ്രതിരോധ നടപടികൾക്കും ഉപയോഗിക്കുന്നതിനായി വിശദമായി വിശകലനം ചെയ്യുകയും. മറ്റ് സംസ്ഥാനങ്ങളുമായി ബന്ധപ്പെട്ട കേസുകൾ കണ്ടെത്തുന്ന സാഹചര്യത്തിൽ ഇന്റർസ്റ്റേറ്റ് ലിങ്കേജിലൂടെ ബന്ധപ്പെട്ട സംസ്ഥാന പോലീസ് മേധാവികളുമായി ഏകോപനം നടത്തി ആവശ്യമായ നിയമനടപടികൾ സ്വീകരിക്കും.

സൈബർ സുരക്ഷ ഉറപ്പാക്കുന്നതിനായി പൊതുജനങ്ങൾ ചില പ്രധാന ജാഗ്രതകൾ പാലിക്കണം. OTP, PIN, CVV, പാസ്വേഡ് തുടങ്ങിയ ബാങ്ക് വിവരങ്ങൾ ഒരിക്കലും മറ്റാരുമായും പങ്കുവെക്കരുത്. സംശയകരമായ ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യരുത്, പരിചയമില്ലാത്ത "വർക്ക് ഫ്രം ഹോം" അല്ലെങ്കിൽ ടാസ്ക് അടിസ്ഥാനത്തിലുള്ള ഓഫറുകളിൽ ജാഗ്രത പാലിക്കുകയും വേണം. ഓരോ അക്കൗണ്ടിനും വ്യത്യസ്തവും ശക്തവുമായ പാസ്വേഡുകൾ ഉപയോഗിക്കുകയും TwoFactor Authentication (2FA) പോലുള്ള സുരക്ഷാ സംവിധാനം സജീവമാക്കുകയും ചെയ്യുന്നത് കൂടുതൽ സുരക്ഷ ഉറപ്പാക്കും. സംശയകരമായ സൈബർ സംഭവങ്ങൾ ശ്രദ്ധയിൽപ്പെട്ടാൽ ഉടൻ 1930 എന്ന ഹെൽപ്പ്ലൈൻ നമ്പറിൽ ബന്ധപ്പെടുകയോ https://cybercrime.gov.in എന്ന വെബ്സൈറ്റ് വഴി പരാതി നൽകുകയോ ചെയ്യാവുന്നതാണ്.

****