STATE POLICE MEDIA CENTRE
KERALA POLICE
Police Headquarters
Vazhuthacaud
Thiruvananthapuram - 695010
0471 2318188
info.pol@kerala.gov.in
statepolicemediacentre

No.189/PR/SPMC/PHQ/2026 Date: 20.04.2026

വിവോ , iQoo ഉപയോക്താക്കളെ ലക്ഷ്യമിട്ട് സൈബർ തട്ടിപ്പ്

വിവോ (Vivo), iQoo സ്മാർട്ട് ഫോണുകൾ ഉപയോഗിക്കുന്നവരെ ലക്ഷ്യമിട്ട് 'ഒറിജിൻ ഒ എസ് അപ്ഡേറ്റ്' (OriginOS Update) എന്ന വ്യാജേന അയക്കുന്ന സന്ദേശങ്ങൾ വഴി മൊബൈൽ ഫോണുകളിൽ മാൽവെയറുകൾ ഇൻസ്റ്റാൾ ചെയ്യിപ്പിച്ച് ഉപയോക്താക്കളുടെ ബാങ്കിംഗ് വിവരങ്ങൾ ചോർത്തുന്നതാണ് തട്ടിപ്പിന്റെ രീതി.

മൊബൈൽ ഫോൺ ഉപയോഗിക്കുന്നതിനിടെ 'അടിയന്തരമായി സിസ്റ്റം അപ്ഡേറ്റ് ചെയ്യുക' (Urgent System Update Required) എന്ന തരത്തിലുള്ള പോപ്പ്അപ്പ് സന്ദേശങ്ങൾ സ്ക്രീനിൽ പ്രത്യക്ഷപ്പെടും. ഇതിൽ നൽകിയിരിക്കുന്ന ലിങ്കിൽ ക്ലിക്ക് ചെയ്താൽ ഔദ്യോഗിക അപ്ഡേറ്റിന് പകരം മാൽവെയർ അടങ്ങിയ എ.പി.കെ (APK) ഫയലുകൾ ഡൗൺലോഡ് ആകുന്നു.

ആപ്പുകൾ ഇൻസ്റ്റാൾ ചെയ്യുന്നതോടെ ഫോണിന്റെ നിയന്ത്രണം തട്ടിപ്പുകാർക്ക് ലഭിക്കുകയും ക്യാമറ, മൈക്രോഫോൺ, എസ്എംഎസ്, കോൺടാക്ട് വിവരങ്ങൾ എന്നിവ ചോർത്തുകയും ചെയ്യുന്നു. ഇതിലൂടെ ബാങ്ക് അക്കൗണ്ടുകളിൽ നിന്ന് പണം തട്ടാനാണ് സംഘം ലക്ഷ്യമിടുന്നത്.

Settings മെനുവിലെ 'System Update' വഴി അല്ലാതെ ബ്രൗസർ വഴിയോ മെസേജുകൾ വഴിയോ വരുന്ന അപ്ഡേറ്റ് ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യരുത്.

'ഫോൺ ബ്ലോക്ക് ചെയ്യും' എന്ന രീതിയിൽ ഭീഷണിപ്പെടുത്തുന്ന സന്ദേശങ്ങൾ കണ്ടാൽ അവ പൂർണ്ണമായും അവഗണിക്കുക.

ഫോണിലെ 'Install from Unknown Sources' എന്ന ഓപ്ഷൻ എപ്പോഴും ഓഫ് ചെയ്തു വെക്കുക.

വിശ്വസനീയമായ ആന്റിവൈറസ് സോഫ്റ്റ്‌വെയറുകൾ മാത്രം ഫോണിൽ ഉപയോഗിക്കുക.

അബദ്ധവശാൽ ലിങ്കിൽ ക്ലിക്ക് ചെയ്താൽ ഉടൻ തന്നെ ഇന്റർനെറ്റ് ബന്ധം വിച്ഛേദിക്കുക. ഫോൺ സുരക്ഷാ ആപ്പുകൾ ഉപയോഗിച്ച് സ്കാൻ ചെയ്ത് അജ്ഞാതമായ ആപ്പുകൾ നീക്കം ചെയ്യുക. ബാങ്കിംഗ്, സോഷ്യൽ മീഡിയ പാസ്‌വേഡുകൾ മറ്റൊരു സുരക്ഷിത ഉപകരണം ഉപയോഗിച്ച് ഉടൻ മാറ്റുക.

സാമ്പത്തിക തട്ടിപ്പിനിരയായാൽ ഉടൻ തന്നെ 1930 എന്ന സൈബർ ഹെൽപ്പ്‌ലൈൻ നമ്പറിലോ, https://cybercrime.gov.in എന്ന ദേശീയ സൈബർ ക്രൈം പോർട്ടലിലോ പരാതി നൽകുക.

****