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

No.267/PR/SPMC/PHQ/2026 Date:04.07.2026

പത്രക്കുറിപ്പ്

വാട്സ്ആപ്പ് അക്കൗണ്ടുകൾ ഹാക്ക് ചെയ്ത് പുതിയ സൈബർ തട്ടിപ്പ്: ബിസിനസ് സ്ഥാപനങ്ങൾ ജാഗ്രത പാലിക്കണമെന്ന് കേരള പോലീസ്.

സംസ്ഥാനത്തെ ബിസിനസ് സ്ഥാപനങ്ങളെയും അവയുടെ സാമ്പത്തിക വിഭാഗങ്ങളെയും ലക്ഷ്യമിട്ട് വാട്സ്ആപ്പ് വഴി പുതിയ രീതിയിലുള്ള സൈബർ സാമ്പത്തിക തട്ടിപ്പ് വ്യാപിക്കുന്നു. സ്ഥാപനങ്ങളുമായി സ്ഥിരമായി സാമ്പത്തിക ഇടപാടുകൾ നടത്തുന്ന കസ്റ്റമർമാരുടെയോ സപ്ലയർമാരുടെയോ ഹാക്ക് ചെയ്യപ്പെട്ട വാട്സ്ആപ്പ് അക്കൗണ്ടുകൾ ഉപയോഗിച്ചാണ് തട്ടിപ്പുകാർ വലവിരിക്കുന്നത്. അക്കൗണ്ട്സ് വിഭാഗത്തിലേക്ക് 'അക്കൗണ്ട് സ്റ്റേറ്റ്മെന്റ്' എന്ന പേരിൽ .vbs പോലുള്ള അപകടകരമായ എക്സ്റ്റൻഷനുകളോടുകൂടിയ സ്ക്രിപ്റ്റ് ഫയലുകൾ വാട്സ്ആപ്പ് വഴി അയച്ചു നൽകുകയാണ് ഇവരുടെ രീതി.

ഈ ഫയലുകൾ തുറക്കുന്നതോടെ സ്ഥാപനത്തിലെ കമ്പ്യൂട്ടറുകളിൽ മാൽവെയറുകൾ ഇൻസ്റ്റാൾ ചെയ്യപ്പെടുകയും സിസ്റ്റത്തിന്റെ പൂർണ്ണ നിയന്ത്രണം തട്ടിപ്പുകാർ കൈക്കലാക്കുകയും ചെയ്യുന്നു. തുടർന്ന് ബ്രൗസറുകളിൽ സേവ് ചെയ്തിട്ടുള്ള പാസ്‌വേർഡുകളും സാമ്പത്തിക വിവരങ്ങളും ചോർത്തിയെടുത്ത ശേഷം, സ്ഥാപനത്തിലെ ഉന്നത ഉദ്യോഗസ്ഥരുടെ വാട്സ്ആപ്പ് അക്കൗണ്ടുകൾ ഹൈജാക്ക് ചെയ്ത് അവരുടെ പേരിൽ വ്യാജ ചാറ്റുകൾ നിർമ്മിച്ച് കീഴ്ജീവനക്കാരോട് അടിയന്തരമായി പണം ട്രാൻസ്ഫർ ചെയ്യാൻ ആവശ്യപ്പെടുകയാണ് ചെയ്യുന്നത്.

വിശ്വസ്തരായ വ്യക്തികളുടെ സന്ദേശമാണെന്ന് കരുതി സ്ഥാപനങ്ങൾ വൻ തുകകൾ ഇത്തരത്തിൽ കൈമാറി ചതിക്കപ്പെടാൻ സാധ്യതയേറെയാണ്.

കോംപ്രമൈസ് ചെയ്യപ്പെട്ട കമ്പ്യൂട്ടറുകളിൽ നിന്നും ലിസ്റ്റിലുള്ള മറ്റ് ബിസിനസ് ഗ്രൂപ്പുകളിലേക്ക് ഈ വ്യാജ ഫയലുകൾ തനിയെ അയക്കപ്പെടുകയും ചെയ്യുന്നുണ്ട്.

ഇത്തരം തട്ടിപ്പുകളിൽ പെടാതിരിക്കാൻ ബിസിനസ് സ്ഥാപനങ്ങളും പൊതുജനങ്ങളും കർശനമായ മുൻകരുതലുകൾ എടുക്കേണ്ടതാണ്. വാട്സ്ആപ്പ് വഴി വരുന്ന അക്കൗണ്ട് സ്റ്റേറ്റ്മെന്റുകളോ ഫയലുകളോ തുറക്കുന്നതിന് മുൻപ് അവരെ നേരിട്ട് ഫോണിൽ വിളിച്ച് ഉറപ്പുവരുത്തേണ്ടതാണ്.

അപരിചിതമായ ലിങ്കുകളോ സാധാരണ രീതിക്ക് വിപരീതമായ എക്സ്റ്റൻഷനുകളോഉള്ള ഡോക്യുമെന്റുകൾ യാതൊരു കാരണവശാലും ഡൗൺലോഡ് ചെയ്യുകയോ റൺ ചെയ്യുകയോ ചെയ്യരുത്. വാട്സ്ആപ്പ് സന്ദേശങ്ങൾ മാത്രം അടിസ്ഥാനമാക്കി ഔദ്യോഗികമായ ഇരട്ട സ്ഥിരീകരണമില്ലാതെ ഫണ്ട് ട്രാൻസാക്ഷനുകൾ നടത്താതിരിക്കുക.

അഥവാ കമ്പ്യൂട്ടറിൽ മാൽവെയർ ഇൻസ്റ്റാൾ ആയെന്ന് സംശയം തോന്നിയാൽ അടിയന്തരമായി വൈഫൈയോ ലാൻ കേബിളോ വേർപെടുത്തി ഇന്റർനെറ്റ് കണക്ഷൻ പൂർണ്ണമായും വിച്ഛേദിക്കുകയാണ് ആദ്യം ചെയ്യേണ്ടത്. ഈ ഫയലുകൾ പരിശോധിക്കാനെന്ന പേരിൽ മറ്റ് കമ്പ്യൂട്ടറുകളിലേക്കോ ഫോണുകളിലേക്കോ കൈമാറുകയും ചെയ്യരുത്. ഇൻഫെക്ട് ആയ ഡിവൈസുകൾ സുരക്ഷിതമാക്കാൻ അടിയന്തരമായി അടുത്തുള്ള സൈബർ പോലീസ് സ്റ്റേഷനിൽ ബന്ധപ്പെടുക.

ഇത്തരത്തിലുള്ള ഓൺലൈൻ സാമ്പത്തിക തട്ടിപ്പിനിരയായാൽ ഉടൻ തന്നെ 1930 എന്ന സൈബർ ഹെല്പ് ലൈൻ നമ്പറിലേക്കോ www.cybercrime.gov.in എന്ന സൈബർ ക്രൈം റിപ്പോർട്ടിങ് പോർട്ടലിലേക്കോ ബന്ധപ്പെടുക.

ഡോ. അഞ്ചൽ കൃഷ്ണകുമാർ,

ഡെപ്യൂട്ടി ഡയറക്ടർ,

സ്റ്റേറ്റ് പോലീസ്

മീഡിയ സെൻറർ

****