

വെറ്ററൻസും വീർ നാരിസും നടത്തുന്ന സൈബർ സുരക്ഷാ തട്ടിപ്പുകൾ കൈകാര്യം ചെയ്യൽ

കമാൻഡർ പി രാജഗോപാൽ തമ്പി IN (R)

- AI, വലിയ ഭാഷാ മോഡലുകൾ
- സോഫ്റ്റ്വെയറും AI-യും തമ്മിലുള്ള വ്യത്യാസം എന്താണ്?
- ഒരു ഏജന്റ് എന്താണ്?
- ഒരു എൽഎൽഎമ്മിൽ നിന്ന് ഒരു ഏജന്റ് എങ്ങനെ വ്യത്യാസപ്പെട്ടിരിക്കുന്നു?
- ചില പ്രധാന AI നേട്ടങ്ങൾ എന്തൊക്കെയാണ്?
    - ശാസ്ത്രീയ കണ്ടുപിടുത്തങ്ങളിൽ ദ്രുതഗതിയിലുള്ള പുരോഗതി
    - പുതിയ വസ്തുക്കൾ, പുതിയ തന്മാത്രകൾ, ഉൽപ്പാദനക്ഷമതാ നേട്ടങ്ങൾ
    - കാലാവസ്ഥാ പ്രവചനങ്ങൾ
    - സോഫ്റ്റ്വെയർ കോഡിംഗ്
    - റോബോട്ടുകളും ഓട്ടോമേഷനും
- AI യുടെ പ്രധാന അപകടസാധ്യതകൾ എന്തൊക്കെയാണ്?
    - വഞ്ചന, അധികാര മോഹം, ആത്മരക്ഷ
    - ഡീപ്ഫേക്കുകൾ
    - നിയന്ത്രണം നഷ്ടപ്പെടൽ
    - ആവർത്തന സ്വയം മെച്ചപ്പെടുത്തൽ (RSI)
    - സ്വയം പകർപ്പെടുക്കൽ

- ഹഗ്ഗിംഗ്ഫേസ് സംഭവം, ആന്ത്രോപിക് ഐഒടി പ്രവചനം
- ഫ്രാൻസിലെ റഫ്രിജറേഷൻ പ്ലാന്റുകൾ ഹാക്ക് ചെയ്യുന്നു - 2026 ഒക്ടോബർ മധ്യത്തിൽ
- സർക്കാർ വെബ്സൈറ്റുകൾ പ്രവർത്തനരഹിതം (PHP ബഗുകൾ) – 21 സെന്റ് 2026 ഒക്ടോബർ
- സ്വതസിദ്ധമായി ഒരു ഇരട്ട-ഉപയോഗ സാങ്കേതികവിദ്യ - സ്വയംഭരണ ആയുധം, CBRN, യുദ്ധകാല ഉപയോഗം എന്നിവയിൽ വലിയ അപകടങ്ങൾ.
- സൈബർ സുരക്ഷയെ പ്രാപ്തമാക്കുന്നതും സംരക്ഷിക്കുന്നതുമാണ് AI.
- നമ്മുടെ തലച്ചോറിനേക്കാൾ ശക്തമായ കമ്പ്യൂട്ടിംഗ് എഞ്ചിൻ (വേഗതയേറിയതും പരിധിയില്ലാത്തതുമായ വിഭവങ്ങൾ). നമ്മൾഅവരെ മനസ്സിലാക്കാനോ മനസ്സിലാക്കാനോ കഴിയില്ല.
- ഏജന്റുമാർക്ക് 24x7 പ്രവർത്തിക്കുന്നു, ആറുകണക്കിന് ബ്രൂട്ട് ഫോഴ്സ് എൻക്രിപ്ഷൻ ചെയ്യാനും സോഫ്റ്റ്വെയറിലെ ബഗുകൾ കണ്ടെത്താനും കഴിയും. • പവർ ഓൺ പരിശീലനത്തിന് ശേഷം AI സിസ്റ്റങ്ങൾക്ക് പൂർണ്ണ അറിവോടെ പ്രവർത്തിക്കാൻ കഴിയും, എവിടെയും മൈഗ്രേറ്റ് ചെയ്യാൻ കഴിയും, വളരെ വൈകുന്നതുവരെ നമുക്ക് അവ കണ്ടെത്താനായേക്കില്ല.

- ഇന്റർനെറ്റ് കൈയടക്കുന്നതിനും അടിസ്ഥാന സൗകര്യങ്ങൾ ഹാക്ക് ചെയ്യുന്നതിനും AI-യിൽ നിന്ന് ദീർഘകാല ദോഷം ഉണ്ടായേക്കാം.സിസ്റ്റങ്ങളും യൂട്ടിലിറ്റികളും.

- സംശയത്തോടെയും കുറഞ്ഞ വിശ്വാസ്യതയോടെയും AI സിസ്റ്റങ്ങളെ സമീപിക്കുക:
- സോഷ്യൽ മീഡിയയിൽ നിന്ന് ലഭിക്കുന്നത് വിശ്വസിക്കരുത്.
- സിരി അല്ലെങ്കിൽ തത്തുല്യമായ സംഭാഷണ നിരീക്ഷണ ആപ്പുകൾ പ്രവർത്തനരഹിതമാക്കി നിലനിർത്തുക.
- നിങ്ങൾ ചാറ്റ് ജിപിടി അല്ലെങ്കിൽ ക്ലോഡ് പോലുള്ള AI ഉപകരണങ്ങൾ ഉപയോഗിക്കുകയാണെങ്കിൽ “എല്ലാവർക്കും മോഡൽ മെച്ചപ്പെടുത്തുക” ഓപ്ഷനും ലൊക്കേഷൻ ഓപ്ഷനും ഓഫ് ചെയ്യുക.
- നിങ്ങളുടെ സ്വകാര്യ ഡാറ്റ എങ്ങനെ കൈകാര്യം ചെയ്യുന്നുവെന്ന് വിശ്വസനീയമായി പരിശോധിക്കാൻ കഴിയുമെങ്കിൽ ഒഴികെ, വാണിജ്യപരമായി ലഭ്യമായ AI ഏജന്റുകൾ ഉപയോഗിക്കുന്നത് ഒഴിവാക്കുക. നിങ്ങൾക്ക് അത്യാവശ്യമാണെങ്കിൽ മാത്രം കുറഞ്ഞ അപകടസാധ്യതയുള്ള ആപ്ലിക്കേഷനുകൾക്ക് ഇത് ഉപയോഗിക്കുക.
- നിങ്ങളുടെ ചിന്തകളും ഉദ്ദേശ്യങ്ങളും ഒരു AI ഏജന്റിനും, പ്രത്യേകിച്ച് നിങ്ങളുടെ ഡയറിയേക്കോ സ്വകാര്യ ജേണലേക്കോ കൈമാറരുത്. • നിങ്ങളുടെ ബാങ്ക് അക്കൗണ്ടുകൾ, ബില്ലുകൾ, പേയ്മെന്റുകൾ, മറ്റ് സാമ്പത്തിക കാര്യങ്ങൾ, ഇടപാടുകൾ എന്നിവയിലെ ഇടപാടുകൾ ഓട്ടോമേറ്റ് ചെയ്യുന്നതിന് AI ഏജന്റുമാർക്ക് ആക്സസ് നൽകരുത്.
- നിങ്ങളുടെ ഫോൾഡറുകളിലേക്കും ഇമെയിൽ സേവനങ്ങളിലേക്കും കാർഡ് വിവരങ്ങളിലേക്കും ആക്സസ് നൽകരുത്.
- എപ്പോഴും "സ്വയം ചിന്തിക്കുക", നിങ്ങൾക്കായി ചിന്തിക്കാൻ AI യോട് ആവശ്യപ്പെടരുത്.

• AI സിസ്റ്റങ്ങളെ ആശ്രയിക്കാതെ, വിശ്വസ്തനായ ഒരു സുഹൃത്തിനെ ഉപയോഗിച്ച് നിങ്ങളുടെ ചിന്താ പ്രക്രിയ പരിശോധിക്കുക.

• സ്വകാര്യതാ നിയന്ത്രണങ്ങൾ ഫലപ്രദമായി ഉപയോഗിക്കുക, ഒഴിവാക്കാനാവാത്ത ആവശ്യത്തിന് മാത്രം മെഡിക്കൽ,

സാമ്പത്തിക രേഖകൾ അപ്‌ലോഡ് ചെയ്യുക.28/10/2026 പി രാജഗോപാൽ തമ്പി 4

• കുടുംബാംഗത്തിന്റെ ശബ്ദം പോലെ തോന്നുന്നു എന്നതുകൊണ്ട് മാത്രം വിളിക്കുന്നയാളെ ഒരിക്കലും വിശ്വസിക്കരുത്. • അടിയന്തര സാഹചര്യത്തിൽ ബന്ധുവാണെന്ന് അവകാശപ്പെട്ട് ആരെങ്കിലും പണം ആവശ്യപ്പെട്ടാൽ, കോൾ വിച്ഛേദിച്ച് മുമ്പ് സേവ് ചെയ്ത നമ്പറിൽ നിന്ന് ആ വ്യക്തിയുടെ കോൾ തിരികെ വിളിക്കുക.

• അടിയന്തര സാഹചര്യങ്ങൾക്കുള്ള ഒരു സ്വകാര്യ കുടുംബ സ്ഥിരീകരണ വാക്യത്തിൽ യോജിക്കുന്നു. അത് സോഷ്യൽ മീഡിയയിൽ പങ്കിടരുത്.മാധ്യമങ്ങൾ.

• വ്യക്തിയുടെ മുഖം തിരിച്ചറിയാൻ കഴിയും എന്നതുകൊണ്ട് മാത്രം ഒരു വീഡിയോ കോൾ

യഥാർത്ഥമാണെന്ന് കരുതരുത്. • പണം, രഹസ്യ സ്വഭാവം അല്ലെങ്കിൽ ഉടനടി നടപടി എന്നിവയ്ക്കുള്ള അടിയന്തര അഭ്യർത്ഥനകളെ മുന്നറിയിപ്പ് അടയാളങ്ങളായി കണക്കാക്കുക. • പോലീസ്, സിബിഐ, കസ്റ്റംസ്, കോടതികൾ അല്ലെങ്കിൽ മറ്റ് അധികാരികൾ തിരിച്ചറിയുന്നുണ്ടെന്ന് അവകാശപ്പെടുന്ന സന്ദേശങ്ങൾ വിശ്വസിക്കരുത്.നിങ്ങളെ ഡിജിറ്റൽ അറസ്റ്റിൽ ആക്കി.

• തിരിച്ചറിയൽ തെളിവായി കോളർ ഐഡി, വാട്ട്സ്ആപ്പ് പ്രൊഫൈൽ ഫോട്ടോഗ്രാഫുകൾ അല്ലെങ്കിൽ പ്രദർശിപ്പിച്ചിരിക്കുന്ന സ്ഥാപനത്തിന്റെ പേരുകൾ എന്നിവ വിശ്വസിക്കരുത്.

• നിങ്ങളുടെ ഓൺലൈൻ ഡാറ്റ പ്രൊഫൈലും കാൽപ്പാടുകളും പരമാവധി കുറയ്ക്കുക • ആൾമാറാട്ട ഉദാഹരണം (വ്യാജ വീഡിയോ കോൾ അംഗീകാരം കാരണം $25 മില്യൺ കൈമാറി).

• നിയമപരമായ ഉദ്ദേശ്യമില്ലാതെ തിരിച്ചറിയൽ രേഖകൾ പങ്കിടുന്നത് ഒഴിവാക്കുക.

• ഉചിതമായിടത്ത്, തിരിച്ചറിയൽ രേഖകളുടെ പകർപ്പുകളിൽ ഒരു പ്രത്യേക ഉദ്ദേശ്യ വാട്ടർമാർക്ക്

ചേർക്കുക.• വാട്ട്സ്ആപ്പ്, ഫേസ്ബുക്ക്, ഇൻസ്റ്റാഗ്രാം, മറ്റ് സോഷ്യൽ പ്ലാറ്റ്ഫോമുകൾ എന്നിവയിലെ സ്വകാര്യതാ ക്രമീകരണങ്ങൾ അവലോകനം ചെയ്യുക.• മെസ്സേജിംഗ് ഗ്രൂപ്പുകളിലേക്ക് ആർക്കൊക്കെ നിങ്ങളെ ചേർക്കാൻ കഴിയുമെന്ന് നിയന്ത്രിക്കുക, ഗ്രൂപ്പ് അംഗത്വങ്ങൾ കുറയ്ക്കാൻ ശ്രമിക്കുക. • പ്രായോഗികമാകുന്നിടത്തെല്ലാം പൊതുവായി ലഭ്യമായ വോയ്സ് റെക്കോർഡിംഗുകളും വ്യക്തിഗത വീഡിയോകളും പരിമിതപ്പെടുത്തുക. • വിശദമായ കുടുംബ ബന്ധങ്ങൾ, ദിനചര്യകൾ, സാമ്പത്തിക സാഹചര്യങ്ങൾ എന്നിവ പ്രസിദ്ധീകരിക്കുന്നത് ഒഴിവാക്കുക. • പൊതു ഓൺലൈൻ പ്രൊഫൈലുകളിൽ നിന്ന് അനാവശ്യമായ വ്യക്തിഗത വിവരങ്ങൾ നീക്കം ചെയ്യുക.• UIDAI യുടെ ഔദ്യോഗിക ആധാർ പ്രാമാണീകരണ-ചരിത്രവും ബയോമെട്രിക്-ലോക്കിംഗ് സൗകര്യങ്ങളും ഉപയോഗിക്കുക, അവിടെഅനുയോജ്യം.

- ലഭ്യമെങ്കിൽ, ഔദ്യോഗിക സർക്കാർ ടെലികോം സേവനങ്ങൾ വഴി നിങ്ങളുടെ മൊബൈൽ കണക്ഷനുകൾ പരിശോധിക്കുക.
- വിശ്വാസ്യത കുറഞ്ഞ സബ്സ്ക്രിപ്ഷനുകൾക്കും രജിസ്ട്രേഷനുകൾക്കും ഒരു പ്രത്യേക ഇമെയിൽ വിലാസം ഉപയോഗിക്കുക.• ക്ലൗഡ്-ഷെയറിംഗ് ലിങ്കുകൾ അവലോകനം ചെയ്യുക, ആവശ്യമില്ലാത്തപ്പോൾ പൊതു ആക്സസ് നീക്കം ചെയ്യുക.

• നിങ്ങളുടെ ബാങ്കിംഗ് പിൻ, UPI പിൻ, ATM പിൻ, CVV, പാസ്‌വേഡ്, ജനനത്തീയതി അല്ലെങ്കിൽ OTP എന്നിവ ഒരിക്കലും വെളിപ്പെടുത്തരുത്.• ഓർമ്മിക്കുക: പണം സ്വീകരിക്കാൻ നിങ്ങൾ ഒരു UPI പിൻ നൽകേണ്ടതില്ല. അത് നൽകുന്നത് സാധാരണയായി ഒരു പേയ്‌മെന്റിന് അംഗീകാരം നൽകുന്നു.• പണം സ്വീകരിക്കാൻ അപരിചിതർ അയച്ച QR കോഡ് ഒരിക്കലും സ്കാൻ ചെയ്യരുത്.

• അപ്രതീക്ഷിതമായ UPI കളക്ഷൻ അഭ്യർത്ഥന ഒരിക്കലും അംഗീകരിക്കരുത്.

• AI ഉപയോഗിച്ച് ഉറപ്പായ ഉയർന്ന വരുമാനമോ അസാധാരണമായ ലാഭമോ വാഗ്ദാനം ചെയ്യുന്ന നിക്ഷേപ പദ്ധതികളെ വിശ്വസിക്കരുത്.• നിങ്ങളുടെ ബാങ്കിംഗ് ആപ്ലിക്കേഷൻ വിദൂരമായി പ്രവർത്തിപ്പിക്കാൻ ഏജന്റുമാരെയും അപരിചിതരെയും ഒരിക്കലും അനുവദിക്കരുത്.

• ബാങ്ക് കാർഡുകൾ, ചെക്കുകൾ അല്ലെങ്കിൽ സാമ്പത്തിക രേഖകൾ എന്നിവയുടെ ഫോട്ടോഗ്രാഫുകൾ അജ്ഞാതരായ ആളുകളുമായി പങ്കിടരുത്. • എല്ലാ പ്രധാനപ്പെട്ട അക്കൗണ്ടുകളിലും ഇടപാട് അലേർട്ടുകൾ പ്രാപ്തമാക്കുക.

• നിങ്ങളുടെ ബാങ്ക് അനുവദിക്കുന്നിടത്ത്, നിങ്ങളുടെ ആവശ്യങ്ങൾക്ക് അനുയോജ്യമായ ദൈനംദിന ട്രാൻസ്ഫർ പരിധികൾ സജ്ജമാക്കുക.

• കാർഡുകളുടെ പരിചരണം: നിങ്ങൾക്ക് അത് ഓൺലൈനിൽ ഒഴിവാക്കാൻ കഴിയുമെങ്കിൽ കാർഡ് വിശദാംശങ്ങൾ സൂക്ഷിക്കരുത്. കാർഡ് വിശദാംശങ്ങൾ സ്വയമേവ പൂരിപ്പിക്കുന്ന നടപടിക്രമം ഒഴിവാക്കുക. • ഉയർന്ന പരിധികൾ ഇനി ആവശ്യമില്ലാത്തപ്പോൾ ക്രെഡിറ്റ്-കാർഡ് ഓൺലൈൻ ഇടപാട് പരിധികൾ കുറയ്ക്കുക. • ആവശ്യമില്ലാത്തപ്പോൾ അന്താരാഷ്ട്ര കാർഡ് ഇടപാടുകൾ പ്രവർത്തനരഹിതമാക്കുക.

• വിദേശ യാത്ര ചെയ്യുമ്പോൾ കോൺടാക്റ്റ്‌ലെസ് ഇടപാടുകൾ അപ്രാപ്തമാക്കുക, പ്രത്യേകിച്ച് ആംസ്റ്റർഡാം സംഭവം • പതിവ്

ഓൺലൈൻ/യുപിഐ പേയ്മെന്റുകൾക്കായി ഉപയോഗിക്കുന്ന അക്കൗണ്ടുകളിൽ നിന്ന് ഗണ്യമായ സമ്പാദ്യം വേറിട്ട് സൂക്ഷിക്കുക.28/10/2026 പി രാജഗോപാൽ തമ്പി 7

• ബാങ്കിംഗ്, ഇമെയിൽ, പ്രധാനപ്പെട്ട അക്കൗണ്ടുകൾ എന്നിവയ്ക്ക് വ്യത്യസ്ത പാസ്വേഡുകൾ ഉപയോഗിക്കുക. • ഊഹിക്കാൻ പ്രയാസമുള്ള നീളമുള്ള പാസ്വേഡുകളോ പാസ്ഫ്രെയ്സുകളോ ഉപയോഗിക്കുക.

• ലഭ്യമായിടത്തെല്ലാം ടു-ഫാക്ടർ ഓതന്റിക്കേഷൻ അല്ലെങ്കിൽ FIDO2 ഓതന്റിക്കേഷൻ പ്രാപ്തമാക്കുക.• പിൻ, ഫിംഗർപ്രിന്റ് അല്ലെങ്കിൽ മുഖം പ്രാമാണീകരണം ഉപയോഗിച്ച് നിങ്ങളുടെ ഫോൺ ലോക്ക് ചെയ്യുക.

• ഏറ്റവും പുതിയ പതിപ്പുകൾക്കൊപ്പം നിങ്ങളുടെ ഫോണും ആപ്ലിക്കേഷനുകളും അപ്ഡേറ്റ് ചെയ്യുക. • ഔദ്യോഗിക ആപ്പ് സ്റ്റോറുകളിൽ നിന്ന് മാത്രം ആപ്ലിക്കേഷനുകൾ ഡൗൺലോഡ് ചെയ്യുക.

• അജ്ഞാത വ്യക്തി വാട്ട്സ്ആപ്പ്, എസ്എംഎസ് അല്ലെങ്കിൽ ഇമെയിൽ വഴി അയച്ച APK അല്ലെങ്കിൽ ആപ്ലിക്കേഷൻ ഇൻസ്റ്റാൾ ചെയ്യരുത്.

• അപരിചിതരുടെ അഭ്യർത്ഥന പ്രകാരം സ്ക്രീൻ-ഷെയറിംഗ് അല്ലെങ്കിൽ റിമോട്ട്-ആക്സസ് ആപ്ലിക്കേഷനുകൾ ഇൻസ്റ്റാൾ ചെയ്യരുത്. • നിങ്ങളുടെ KYC, PAN, ആധാർ, ബാങ്ക്

അക്കൗണ്ട്, വൈദ്യുതി വിതരണം അല്ലെങ്കിൽ ഡെലിവറി എന്നിവ ബ്ലോക്ക് ചെയ്യപ്പെടുമെന്ന് അവകാശപ്പെടുന്ന അപ്രതീക്ഷിത ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യരുത്.

• സന്ദേശങ്ങളിലെ ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യുന്നതിന് പകരം ഔദ്യോഗിക ബാങ്കിംഗ് അല്ലെങ്കിൽ സേവന ആപ്ലിക്കേഷൻ സ്വയം തുറക്കുക.

• സാധ്യമെങ്കിൽ അക്കൗണ്ടുകൾക്കായി ഒരു ബാക്കപ്പ് സുരക്ഷാ കീ രജിസ്റ്റർ ചെയ്ത് സുരക്ഷിതമായി സൂക്ഷിക്കുക.

• വ്യക്തിപരം, കുടുംബം, ബന്ധ വിവരങ്ങൾ, ഫോട്ടോഗ്രാഫുകൾ എന്നിവ ഉൾപ്പെടുത്തുന്നത് ഒഴിവാക്കുക.സോഷ്യൽ മീഡിയയിൽ.

• നിങ്ങളുടെ യാത്രാ പരിപാടിയോ ദിനചര്യയോ സോഷ്യൽ മീഡിയയിൽ പ്രസിദ്ധീകരിക്കരുത്. • നിങ്ങളുടെ ഇഷ്ടങ്ങളും, അനിഷ്ടങ്ങളും, രാഷ്ട്രീയ ചായ്വുകളും, സാമ്പത്തിക വാങ്ങലുകളും, സ്വകാര്യ പ്രവർത്തനങ്ങളും സോഷ്യൽ മീഡിയയിൽ വെളിപ്പെടുത്തരുത്.

- വീട്ടിലെ വൈഫൈയ്ക്ക് ശക്തമായ പാസ്‌വേഡുകൾ ഉപയോഗിച്ച് WPA2 AES അല്ലെങ്കിൽ WPA 3 എൻക്രിപ്ഷൻ ഉപയോഗിക്കുക.
- നിങ്ങൾ ഹോം ക്യാമറകളും IoT ഉപകരണങ്ങളും ഉപയോഗിക്കുകയാണെങ്കിൽ ഡാറ്റ നിങ്ങളുടെ ഡാറ്റ കാർഡിൽ തന്നെ തുടരുന്നുവെന്ന് ഉറപ്പാക്കുക. അത് ക്ലൗഡിലേക്ക് മാറ്റരുത്.
- സോഷ്യൽ മീഡിയയിലെ ആൾമാറാട്ട അക്കൗണ്ടുകൾ ബ്ലോക്ക് ചെയ്ത് റിപ്പോർട്ട്

ചെയ്യുക.28/10/2026 പി രാജഗോപാൽ തമ്പി 9

എ.ടിതട്ടിപ്പ് നടന്നിട്ടുണ്ടെങ്കിൽ എന്താണ് ചെയ്യേണ്ടത്?

1. ഉടൻ തന്നെ 1930 എന്ന നമ്പറിൽ വിളിക്കുക - ഇന്ത്യയുടെ ദേശീയ സൈബർ സാമ്പത്തിക തട്ടിപ്പ് ഹെൽപ്പ്‌ലൈൻ.

2. സംഭവം ഓൺലൈനായി റിപ്പോർട്ട് ചെയ്യുകദേശീയ സൈബർ കുറ്റകൃത്യ റിപ്പോർട്ടിംഗ് പോർട്ടൽ
3. ഉടൻ തന്നെ നിങ്ങളുടെ ബാങ്കുമായി ബന്ധപ്പെടുക
4. ഉചിതമായി, ബാധിച്ച കാർഡുകൾ, അക്കൗണ്ടുകൾ അല്ലെങ്കിൽ പേയ്മെന്റ് ആക്സസ് എന്നിവ ബ്ലോക്ക് ചെയ്യാൻ അഭ്യർത്ഥിക്കുക.5. നേരത്തെയുള്ള റിപ്പോർട്ട് കൂടുതൽ കൈമാറ്റങ്ങൾ നിർത്താനുള്ള അവസരം മെച്ചപ്പെടുത്തുന്നു, എന്നിരുന്നാലും വീണ്ടെടുക്കൽ ഉറപ്പില്ല.കൂടാതെ ഈ ഘട്ടങ്ങൾ സ്വീകരിക്കുക:
1. സംശയിക്കപ്പെടുന്ന തട്ടിപ്പുകാരനുമായി ആശയവിനിമയം നടത്തുന്നത് നിർത്തുക.
2. റിമോട്ട്-ആക്സസ് സെഷനുകൾ വിച്ഛേദിച്ച് അനധികൃത സോഫ്റ്റ്വെയർ നീക്കം ചെയ്യാൻ സഹായം തേടുക. 3. വിശ്വസനീയമായ ഒരു ഉപകരണം ഉപയോഗിച്ച് അപഹരിക്കപ്പെട്ട പാസ്വേഡുകൾ മാറ്റുക.
4. സംശയാസ്പദമായ ലോഗിൻ സെഷനുകൾ പിൻവലിക്കുകയും ആവശ്യമുള്ളിടത്ത് പ്രാമാണീകരണ രീതികൾ പുനഃസജ്ജമാക്കുകയും ചെയ്യുക.5. സന്ദേശങ്ങൾ, സ്ക്രീൻഷോട്ടുകൾ, ഫോൺ നമ്പറുകൾ, ഇടപാട് റഫറൻസുകൾ, മറ്റ് തെളിവുകൾ എന്നിവ സൂക്ഷിക്കുക. 6. വ്യാജ പ്രൊഫൈലുകൾ, ഡീപ്ഫേക്കുകൾ, ആൾമാറാട്ട ഉള്ളടക്കം എന്നിവ ബന്ധപ്പെട്ട പ്ലാറ്റ്ഫോമുകളിലും അധികാരികളിലും റിപ്പോർട്ട് ചെയ്യുക. 7. നിങ്ങളുടെ അക്കൗണ്ട് ഉപയോഗിച്ച് വ്യാജ സന്ദേശങ്ങൾ അയച്ചിട്ടുണ്ടെങ്കിൽ, ബാധിച്ച കോൺടാക്റ്റുകൾക്ക് മുന്നറിയിപ്പ് നൽകുക.

1. സ്വതന്ത്രമായ പരിശോധന കൂടാതെ പരിചിതമായ ശബ്ദത്തെയോ മുഖത്തെയോ ഒരിക്കലും വിശ്വസിക്കരുത്. 2. ഒരു OTP, PIN, പാസ്‌വേഡ് അല്ലെങ്കിൽ ബാങ്കിംഗ് ക്രെഡൻഷ്യൽ ഒരിക്കലും വെളിപ്പെടുത്തരുത്.

3. ഭീഷണികൾ, അടിയന്തരാവസ്ഥ അല്ലെങ്കിൽ രഹസ്യം കാരണം ഒരിക്കലും പണം കൈമാറ്റം ചെയ്യരുത്.

4. ഡിജിറ്റൽ അറസ്റ്റ് അല്ലെങ്കിൽ പോലീസ് സേഫ് അക്കൗണ്ടുകൾ സംബന്ധിച്ച അവകാശവാദങ്ങൾ ഒരിക്കലും വിശ്വസിക്കരുത്.

5. പണം സ്വീകരിക്കാൻ ഒരിക്കലും QR കോഡ് സ്കാൻ ചെയ്യുകയോ UPI പിൻ നൽകുകയോ ചെയ്യരുത്.

6. അപരിചിതരുടെ അഭ്യർത്ഥനപ്രകാരം ഒരിക്കലും സോഫ്റ്റ്‌വെയർ ഇൻസ്റ്റാൾ ചെയ്യുകയോ സ്ക്രീൻ പങ്കിടുകയോ ചെയ്യരുത്.

7. അപ്രതീക്ഷിത ലിങ്കുകൾ, നിക്ഷേപ ഓഫറുകൾ അല്ലെങ്കിൽ പെൻഷൻ സംബന്ധമായ സന്ദേശങ്ങൾ എന്നിവ ഒരിക്കലും വിശ്വസിക്കരുത്. 8. ഫോണുകൾ അപ്‌ഡേറ്റ് ചെയ്ത് ശക്തമായ അക്കൗണ്ട് പ്രാമാണീകരണം പ്രാപ്തമാക്കുക.

9. അസാധാരണമായ സാമ്പത്തിക തീരുമാനങ്ങൾ എടുക്കുന്നതിന് മുമ്പ് ഒരു വിശ്വസ്ത വ്യക്തിയുമായി കൂടിയാലോചിക്കുക. 10. തട്ടിപ്പ് നടന്നാൽ, നിങ്ങളുടെ ബാങ്കുമായി ബന്ധപ്പെടുകയും ഉടൻ തന്നെ 1930 എന്ന നമ്പറിൽ വിളിക്കുകയും ചെയ്യുക.

11. ഓർമ്മിക്കേണ്ട ഏറ്റവും ഫലപ്രദമായ ഏക തത്വം ഇതാണ്:

12. ഒരു ശബ്ദത്തെയോ, മുഖത്തെയോ, സന്ദേശത്തെയോ, വീഡിയോയെയോ, അത് യഥാർത്ഥമാണെന്ന്

തോന്നുന്ന എന്നതുകൊണ്ട് മാത്രം ഒരിക്കലും വിശ്വസിക്കരുത്. നടപടിയെടുക്കുന്നതിന് മുമ്പ് ഐഡന്റിറ്റിയും അഭ്യർത്ഥനയും സ്വതന്ത്രമായി പരിശോധിക്കുക.

കലണ്ടർ	എപ്പോഴും ചോദിക്കുക
ആരോഗ്യ ഡാറ്റ	ഇല്ല
ഫോട്ടോകളും വീഡിയോകളും	ഇല്ല
ശാരീരിക പ്രവർത്തനങ്ങൾ	ഇല്ല
അറിയിപ്പുകൾ	ഇല്ല
ബ്ലൂടൂത്ത്	ഉപയോഗിക്കുമ്പോൾ മാ
AI ആപ്പുകൾ	പരിശീലനത്തിനായി ഡ

മൊബൈൽ ഫോൺ സു	
ക്രമീകരണങ്ങൾ	ശുപാർശ ചെയ്യുന്ന ക്ര
സ്ഥലം	ആപ്പ് ഉപയോഗിക്കുമ
ക്യാമറ	ആപ്പ് ഉപയോഗിക്കുമ
മൈക്രോഫോൺ	എപ്പോഴും ചോദിക്കുക
കോൺടാക്റ്റുകളും എസ്എംഎസും	എപ്പോഴും ചോദിക്കുക

അവസരവും തയ്യാറെടുപ്പും ഒത്തുചേരുന്നിടത്താണ് ഭാഗ്യം.

AIP റിസർച്ച് വെബ്സൈറ്റ് HTTPS:AIPATHFINDER.ORG

പ്രായോഗിക മനുഷ്യ കേന്ദ്രീകൃത AI –എച്ച്ടിടിപിഎസ്://www.amazon.com/dp/B0CYXHYPHC

നിങ്ങളുടെ ബുദ്ധിശക്തി വർദ്ധിപ്പിക്കുക -https://www.amazon.in/dp/B0D3WZXY99

നന്ദി!