SAFER INTERNET INDIA

ഉപയോക്തൃ സുരക്ഷാ കൈപ്പുസ്തകം

ഉപയോക്തൃ സുരക്ഷാ കൈപ്പുസ്തകം

ഫെബ്രുവരി 2025

അംഗീകാരങ്ങൾ

ആതീഷ് നന്ദി, ലളന്തിക അരവിന്ദ്, മേഘ്ന ബാൽ, സമൃദ്ധി കുമാർ, ശിവ ഭാർഗവി നോറി, സൃഷ്ടി ജോഷി എന്നിവരും, സേഫർ ഇന്റർനെറ്റ് ഇന്ത്യ കോയലിഷൻ അംഗങ്ങളും

CC BY

ഉള്ളിൽ എന്താണ് ഉള്ളത്?

സാധാരണ സ്കാമുകളും ഫ്രോഡുകളും

നിങ്ങൾ ജാഗ്രതയോടെയും ബോധത്തോടെയും നിലനിർത്താൻ സഹായിക്കുന്നതിന് സ്കാമുകാർ ഉപയോഗിക്കുന്ന വിവിധ തന്ത്രങ്ങൾ ഞങ്ങൾ വിശദീകരിക്കുന്നു

സേഫ് സർഫിങ് നുറുങ്ങുകൾ

ഇന്നത്തെ തിരക്കേറിയ ഇന്റർനെറ്റിൽ സുരക്ഷിതരായിരിക്കാൻ ചെയ്യേണ്ടതും ചെയ്യരുതാത്തതുമായ കാര്യങ്ങളുടെ ഒരു പട്ടിക ഞങ്ങൾ തയ്യാറാക്കുന്നു

വിശ്വാസത്തിനും സുരക്ഷയ്ക്കുമുള്ള അടിസ്ഥാന തൂണുകൾ

ഓൺലൈനിൽ വിശ്വാസവും സുരക്ഷിതത്വവും വളർത്തുന്നതിനുള്ള നാല് അടിസ്ഥാന തൂണുകളെക്കുറിച്ചു ഞങ്ങൾ ചർച്ച ചെയ്യുന്നു

വ്യവസായത്തിലെ മികച്ച രീതികൾ

നമുക്കെല്ലാവർക്കും ഇന്റർനെറ്റ് കുറച്ചുകൂടി സുരക്ഷിത മാക്കുന്ന മുൻനിര സാങ്കേതിക സ്ഥാപനങ്ങളിൽ നിന്നുള്ള മികച്ച രീതികളെക്കുറിച്ച് ഞങ്ങൾ ചർച്ച ചെയ്യുന്നു

ഉള്ളടക്ക പട്ടിക

ആമുഖം 06

അടിസ്ഥാനകാര്യങ്ങൾ 07

സാധാരണ അഴിമതികളും സ്കാമുകളും 11

എ ഐ വോയ്സ് സ്കാം 11
ഡേറ്റിംഗ് ആപ്പ് സ്കാം 13
ഡിജിറ്റൽ അറസ്റ്റ് സ്കാം 15
വ്യാജ നിക്ഷേപ / ട്രേഡിംഗ് ആപ്പ്സ്കാം 17
വ്യാജ ജോലി വാഗ്ദാന സ്കാം 19
വ്യാജ ലിങ്ക് / ക്യു ആർ കോഡ് സ്കാം 22
വ്യാജ ലോൺ ആപ്പ് സ്കാം 24
വ്യാജ മൊബൈൽ റീചാർജ് സ്കാം 26
പാഴ്സൽ ഡെലിവറി സ്കാം 28
കൃത്രിമ മാൽവെയർ സ്കാം 30
ടെക് സപ്പോർട്ട് സ്കാം 32
ഒ ടി പി സ്കാം 34
റിവാർഡ് സ്കാം 36
സിം സ്വാപ്പിംഗ് / സിം ക്ലോണിംഗ് സ്കാം 38
ആൾമാറാട്ട സ്കാം 40
സ്കിമ്മിംഗ് മെഷീൻ സ്കാം 42
വ്യാജ ക്ഷേമ പദ്ധതി സ്കാം 43

ചെയ്യേണ്ടതും ചെയ്യരുതാത്തതുമായ കാര്യങ്ങൾ 44

പ്രൊഫഷണൽ ടിപ്പുകൾ 45

ഉപയോക്തൃ സുരക്ഷയ്ക്കുള്ള വ്യവസായത്തിലെ മികച്ച രീതികൾ 47

SAFER INTERNET INDIA

പ്രിയ വായനക്കാരേ

ഇന്ത്യയുടെ വളർന്നുവരുന്ന ഡിജിറ്റൽ സമ്പദ്വ്യവസ്ഥയുടെ വിവിധ വിഭാഗങ്ങളിലായി വ്യാപിച്ചുകിടക്കുന്ന സമാന ചിന്താഗതിക്കാരായ കമ്പനികളുടെ ഒരു കൂട്ടായ്മയാണ് സേഫർ ഇന്റർനെറ്റ് ഇന്ത്യ (SII).

ഓൺലൈൻ സ്കാമുകൾ, സൈബർ ഭീഷണികൾ, ഡാറ്റാ ലംഘനങ്ങൾ എന്നിവയുടെ വർദ്ധിച്ചുവരുന്ന സംഭവങ്ങൾ കൈകാര്യം ചെയ്യേണ്ട അടിയന്തിര സാമൂഹിക ആവശ്യത്തോട് SII പ്രതികരിക്കുന്നു. ഉപയോക്തൃ വിശ്വാസവും ഓൺലൈനിൽ സുരക്ഷയും ശക്തിപ്പെടുത്തുന്നതിന് ഞങ്ങൾ ബഹുമുഖ ശബ്ദങ്ങളെ ഒരുമിച്ച് കൊണ്ടുവരുന്നു.

നിങ്ങളെപ്പോലുള്ള ഇന്റർനെറ്റ് ഉപയോക്താക്കൾക്ക് ഓൺലൈൻ ഫ്രോഡുകളിൽ നിന്നും സ്കാമുകളിൽ നിന്നും നിങ്ങളെത്തന്നെ സംരക്ഷിക്കാൻ വേണ്ടിയാണ് ഞങ്ങൾ ഈ കൈപ്പുസ്തകം എഴുതിയത്.

സാധാരണ സ്കാമുകളുടെയും ഫ്രോഡ്കളുടെയും ഘടനയെക്കുറിച്ച് ഈ കൈപ്പുസ്തകം വിശദമായി പ്രതിപാദിക്കുന്നു, കൂടാതെ ഇന്റർനെറ്റ് ഉപയോക്താക്കൾ ഇന്റർനെറ്റ് ഉപയോഗിക്കുന്നതിനും ഡിജിറ്റൽ ബിസിനസുകളുമായി സുരക്ഷിതമായ രീതിയിൽ ഇടപഴകുന്നതിനും ചെയ്യേണ്ടതും ചെയ്യരുതാത്തതുമായ കാര്യങ്ങൾ ശുപാർശ ചെയ്യുന്നു. ഓൺലൈൻ ഇടങ്ങൾ കൂടുതൽ സുരക്ഷിതമാക്കുന്നതിന്ബി സിനസുകളും നയരൂപീകരണക്കാരും സ്വീകരിച്ച നടപടികളും ഇത്അം ഗീകരിക്കുന്നു.

വായിച്ചതിന് നന്ദി.

സേഫർ ഇന്റർനെറ്റ് ഇന്ത്യ

ആമുഖം

ഡിജിറ്റൽ ഇടങ്ങൾ നമ്മുടെ ജീവിതത്തിന്റെ എല്ലാ മേഖലകളെയും സ്പർശിക്കുന്നു. ഇന്ത്യയിലെ 90 കോടിയിലധികം ഇന്റർനെറ്റ് ഉപയോക്താക്കൾ ജോലി ചെയ്യുന്നതിനും പഠിക്കുന്നതിനും വീട്ടുപകരണങ്ങൾ മുതൽ ആഡംബര വസ്തുക്കൾ, വിനോദ സബ്സ്ക്രിപ്ഷനുകൾ, സാമ്പത്തിക സേവനങ്ങൾ എന്നിവ വരെ എല്ലാം വാങ്ങുന്നതിനും പതിവായി ഓൺലൈനിൽ പോകുന്നു.

എന്നിരുന്നാലും, ഉപയോക്താക്കൾ ആരുമായി ഇടപഴകുന്നു, ഓൺലൈനിൽ എന്ത് വാങ്ങുന്നു എന്നതിനെക്കുറിച്ച് ശ്രദ്ധാലുവായിരിക്കണം. ഓൺലൈൻ ലോകം വളരെ നല്ലതായി തോന്നുന്ന ഓഫറുകളും ഡീലുകളും കൊണ്ട് നിറഞ്ഞിരിക്കുന്നു, മിക്കപ്പോഴും അങ്ങനെയാണ്. 2024-ലെ ആദ്യ ഒമ്പത് മാസങ്ങളിൽ ഓൺലൈൻ സ്കാമുകളിലൂടെഇന്ത്യക്കാർക്ക് ഏകദേശം 11,333 കോടി രൂപ നഷ്ടപ്പെട്ടതായി റിപ്പോർട്ട് ചെയ്യപ്പെട്ടിട്ടുണ്ട്!

സ്കാമുകാരും ഫ്രോഡ്കാരും വളരെ വിരുദ്ധരും അവസരവാദികളും വഴക്കമുള്ളവരുമാണ്. നിർഭാഗ്യവശാൽ, അവർ കൂടുതൽ പരിഷ്കൃതരായിക്കൊണ്ടിരിക്കുകയാണ്, അതേസമയം പല പൗരന്മാർക്കും അടിസ്ഥാന ഡിജിറ്റൽ നൈപുണ്യം ഇല്ല. ഇന്ത്യാ ഗവൺമെന്റ് (GoI) നടത്തിയ 2022-23 സർവേസൂചിപ്പിക്കുന്നത് ഇന്ത്യയിലെ ഇന്റർനെറ്റ് ഉപയോക്താക്കളിൽ പകുതിയോളം പേർക്കും ഇമെയിൽ എങ്ങനെ അയയ്ക്കണമെന്ന് അറിയില്ലായിരുന്നുവെന്നും 38 ശതമാനം ആളുകൾക്ക് മാത്രമേ ഓൺലൈൻ ബാങ്കിംഗ് ഇടപാട് നടത്താൻ കഴിയൂ എന്നുമാണ്. ഡിജിറ്റൽ നൈപുണ്യത്തിന്റെ കാര്യത്തിൽ ഗ്രാമീണ ഇന്ത്യ നഗരത്തിലുള്ള ആളുകളുമായുള്ള അന്തരം വലുതാണ്, കൂടാതെ വ്യത്യസ്ത ലിംഗഭേദങ്ങൾക്കിടയിൽ കാര്യമായ വ്യത്യാസങ്ങളുമുണ്ട്. ഫ്രോഡ്കൾ സമൂഹത്തിന്റെ മുഴുവൻ വെല്ലുവിളിയാണ് എന്നതാണ് സാരം. പല ഇന്ത്യക്കാരും വഞ്ചിക്കപ്പെടാനുള്ള സാധ്യതയിൽ തുടരുന്നു, കൂടാതെ ഓൺലൈനിൽ സ്വയം പരിരക്ഷിക്കുന്നതിന് നൈപുണ്യംവും അവബോധവും നൽകി അവരെ ശാക്തീകരിക്കണം.

ഓൺലൈൻ ഫ്രോഡ്കളുടെ ഭീഷണിയിൽ നിന്ന് ഇന്ത്യൻ ഇന്റർനെറ്റ് ഉപയോക്താക്കളെ സംരക്ഷിക്കേണ്ടതിന്റെ ആവശ്യകത GoI തിരിച്ചറിയുന്നു. ഇന്ത്യൻ സൈബർ ക്രൈം കോർഡിനേഷൻ സെന്റർ (I4C), ഇന്ത്യൻ കമ്പ്യൂട്ടർ എമർജൻസി റെസ്പോൺസ് ടീം (CERT-in) തുടങ്ങിയ പ്രത്യേക സ്ഥാപനങ്ങൾക്കൊപ്പം ആഭ്യന്തര മന്ത്രാലയവും (MHA) ഇലക്ട്രോണിക്സ് ആൻഡ് ഇൻഫർമേഷൻ ടെക്നോളജി മന്ത്രാലയവും സ്കാമുകളും അന്വേഷിക്കുന്നതിനും തടയുന്നതിനും അനുബന്ധ ഓൺലൈൻ സുരക്ഷാ പ്രശ്നങ്ങൾ പരിഹരിക്കുന്നതിനും 24 മണിക്കൂറും പ്രവർത്തിക്കുന്നു. റിസർവ് ബാങ്ക് ഓഫ് ഇന്ത്യ (RBI), ടെലികോം റെഗുലേറ്ററി അതോറിറ്റി ഓഫ് ഇന്ത്യ (TRAI) തുടങ്ങിയ റെഗുലേറ്റർമാർ ഇന്ത്യക്കാരെ സംരക്ഷിക്കുന്നതിനായി സാങ്കേതികവിദ്യ പ്രയോജനപ്പെടുത്തുന്നു, അത് കള്ളപ്പണം വെളുപ്പിക്കലിന് ഉപയോഗിക്കുന്ന മ്യൂൾ അക്കൗണ്ടുകൾ കണ്ടെത്തുന്നതിനുള്ള AI (ആർട്ടിഫിഷ്യൽ ഇന്റലിജൻസ്) സംവിധാനങ്ങളോ സ്പാം/ശല്യപ്പെടുത്തുന്ന കോളുകൾ പരിമിതപ്പെടുത്തുന്നതിന് ടെലിമാർക്കറ്റർമാരുടെ ഡിസ്ട്രിബ്യൂട്ടഡ് ലെഡ്ജർ ടെക്നോളജി (DLT) അടിസ്ഥാനമാക്കിയുള്ള രജിസ്ട്രേഷനോ ആകട്ടെ, അവരുടെ ഡൊമെയ്നുകളിൽ പുതിയ നിയന്ത്രണങ്ങൾ അവതരിപ്പിക്കുന്നു. എന്നാൽ ഓൺലൈൻ സുരക്ഷയുടെ പ്രശ്നത്തിന്റെ വ്യാപ്തി കണക്കിലെടുക്കുമ്പോൾ, എല്ലാവരും ഒറ്റക്കെട്ടായി പ്രവർത്തിക്കേണ്ടതുണ്ട് - ഉപയോക്താക്കളെ ഓൺലൈനിൽ സുരക്ഷിതമായി നിലനിർത്താൻ എല്ലാവരും ഒരുമിച്ച് പ്രവർത്തിക്കണം.

അടിസ്ഥാനകാര്യങ്ങൾ

ഓൺലൈനിൽ സുരക്ഷിതരായിരിക്കുക എന്നത് എക്കാലത്തേക്കാളും പ്രധാനമാണ്. ഈ വിഭാഗത്തിൽ, നിങ്ങൾക്ക് ഡിജിറ്റൽ ഇടങ്ങളിൽ മികച്ച രീതിയിൽ സഞ്ചരിക്കാൻ കഴിയുന്ന തരത്തിൽ ചില അടിസ്ഥാന പദങ്ങളും ആശയങ്ങളും ഞങ്ങൾ നിങ്ങൾക്ക് പരിചയപ്പെടുത്തുന്നു.

വ്യക്തിഗത വിവരങ്ങൾ

നിങ്ങളെക്കുറിച്ചുള്ള, നിങ്ങൾ ആരാണെന്ന് തിരിച്ചറിയാൻ കഴിയുന്ന ഏതൊരു വിവരവും വ്യക്തിഗത വിവരങ്ങളാണ്. ഇതിൽ നിങ്ങളുടെ പേര്, വിലാസം, ഫോൺ നമ്പർ, ഇമെയിൽ, ജനനത്തീയതി അല്ലെങ്കിൽ ബാങ്ക് വിശദാംശങ്ങൾ എന്നിവ ഉൾപ്പെടുന്നു. നിങ്ങളാണെന്ന് നടിക്കുന്നതിനോ നിങ്ങളുടെ അക്കൗണ്ടുകൾ ആക്സസ് ചെയ്യുന്നതിനോ വേണ്ടി സ്കാമുകാർ പലപ്പോഴും ഈ വിവരങ്ങൾ മോഷ്ടിക്കാൻ ശ്രമിക്കാറുണ്ട്.

തന്ത്രപ്രധാനമായ വ്യക്തിഗത വിവരങ്ങൾ

സെൻസിറ്റീവ് ആയ വ്യക്തിഗത വിവരങ്ങൾ എന്നാൽ നിങ്ങളെക്കുറിച്ചുള്ള സ്വകാര്യ വിവരങ്ങൾ ആണ്, അവയ്ക്ക് അധിക സംരക്ഷണം ആവശ്യമാണ്, കാരണം അവ തെറ്റായ കൈകളിൽ എത്തിയാൽ ദുരുപയോഗം ചെയ്യപ്പെടാം. ഇതിൽ നിങ്ങളുടെ പാസ്‌വേഡുകൾ, ബാങ്ക് അക്കൗണ്ട് നമ്പറുകൾ, ക്രെഡിറ്റ് കാർഡ് വിശദാംശങ്ങൾ, മെഡിക്കൽ രേഖകൾ, അല്ലെങ്കിൽ സർക്കാർ ഐഡി നമ്പറുകൾ (ആധാർ അല്ലെങ്കിൽ പാൻ പോലുള്ളവ) ഉൾപ്പെടുന്നു. നിങ്ങളുടെ ഐഡന്റിറ്റിയും സാമ്പത്തികവും സുരക്ഷിതമായി സൂക്ഷിക്കുന്നതിന് ഈ വിവരങ്ങൾ സംരക്ഷിക്കേണ്ടത് വളരെ പ്രധാനമാണ്. അത്തരം വിവരങ്ങൾ നിങ്ങൾ ആരുമായി പങ്കിടുന്നു എന്നതിനെക്കുറിച്ച് വളരെ ശ്രദ്ധാലുവായിരിക്കുക.

ഫ്രോഡ്

നുണയോ വഞ്ചനയോ ഉപയോഗിച്ച് ആരെങ്കിലും ഇന്റർനെറ്റ് വഴി നിയമ വിരുദ്ധമായി പണമോ സെൻസിറ്റീവ് വിവരങ്ങളോ കൈക്കലാക്കുന്നതിനെയാണ് ഓൺലൈൻ ഫ്രോഡ്എ ന്ന് പറയുന്നത്. അക്കൗണ്ടുകൾ ഹാക്ക് ചെയ്യുക, പേയ്മെന്റ് വിശദാംശങ്ങൾ മോഷ്ടിക്കുക, അല്ലെങ്കിൽ ആളുകളെ കബളിപ്പിക്കാൻ വ്യാജ വെബ്സൈറ്റുകൾ സൃഷ്ടിക്കുക തുടങ്ങിയ കാര്യങ്ങൾ ഇതിൽ ഉൾപ്പെടുന്നു.

സ്കാം

ഇന്റർനെറ്റിലൂടെ ആരെങ്കിലും നിങ്ങളെ കബളിപ്പിച്ച് നിങ്ങളുടെ പണമോ വ്യക്തിഗത വിവരങ്ങളോ സെൻസിറ്റീവ് ഡാറ്റയോ മോഷ്ടിക്കുന്നതിനെയാണ് ഓൺലൈൻ സ്കാം എന്ന് പറയുന്നത്. സ്കാമുകാർ പലപ്പോഴും വിശ്വസനീയരാണെന്ന് നടിക്കുകയും വ്യാജ ഡീലുകൾ വാഗ്ദാനം ചെയ്യുകയും ഉദ്യോഗസ്ഥരായി നടിക്കുകയും നിങ്ങളെ കബളിപ്പിക്കാൻ യഥാർത്ഥമെന്ന് തോന്നുന്ന സന്ദേശങ്ങൾ അയയ്ക്കുകയും ചെയ്യുന്നു.

ഓൺലൈൻ സ്കാം എന്നത് ഒരു തരം ഓൺലൈൻ ഫ്രോഡാണ്, എന്നാൽ എല്ലാ ഫ്രോഡുകളും സ്കാമുകളല്ല. പലപ്പോഴും ആളുകളെ പണമോ വിവരങ്ങളോ സ്വമേധയാ നൽകാൻ പ്രേരിപ്പിക്കുന്നതാണ് ഒരു സ്കാം (ഉദാ. വ്യാജ സമ്മാനങ്ങളോ ജോലി വാഗ്ദാനങ്ങളോ). മറുവശത്ത്, ഓൺലൈൻ സ്കാമിൽ ഐഡന്റിറ്റി മോഷണം അല്ലെങ്കിൽ ഹാക്കിംഗ് പോലുള്ള പ്രവർത്തനങ്ങൾ ഉൾപ്പെടാം, അവിടെ ഇരയ്ക്ക് തങ്ങൾ ഉടൻ തന്നെ ലക്ഷ്യം വച്ചിട്ടുണ്ടെന്ന് തിരിച്ചറിയാൻ പോലും കഴിയില്ല.

ചുരുക്കത്തിൽ, സ്കാമുകൾ ആളുകളെ കബളിപ്പിക്കുന്നതിനെ ആശ്രയിച്ചിരിക്കുന്നു, അതേസമയം സ്കാമിൽ വിവരങ്ങൾ മോഷ്ടിക്കുകയോ ദുരുപയോഗം ചെയ്യുകയോ പോലുള്ള വിശാലമായ രീതികൾ ഉൾപ്പെടുന്നു. അതുകൊണ്ടാണ് ഉപയോക്താക്കൾ ഓൺലൈനിൽ ആളുകളുമായി ഇടപഴകുമ്പോൾ മാത്രമല്ല, വെബ്സൈറ്റുകൾ സന്ദർശിക്കുമ്പോഴോ ആപ്പുകൾ ഡൗൺലോഡ് ചെയ്യാൻ നോക്കുമ്പോഴോ ജാഗ്രത പാലിക്കേണ്ടത്.

ഹാക്ക്

വിവരങ്ങൾ മോഷ്ടിക്കാനോ കേടുപാടുകൾ വരുത്താനോ നിയന്ത്രണം ഏറ്റെടുക്കാനോ അനുമതിയില്ലാതെ കംപ്യൂട്ടറിലേക്കോ അക്കൗണ്ടിലേക്കോ നെറ്റ്‌വർക്കിലേക്കോ ആരെങ്കിലും കടന്നുകയറുന്നതിനെയാണ് ഹാക്ക് എന്നു പറയുന്നത്. ബലഹീനതകൾ കണ്ടെത്തുന്നതിനും ആക്സസ് നേടുന്നതിനും ഹാക്കർമാർ പലപ്പോഴും പ്രത്യേക ഉപകരണങ്ങളോ തന്ത്രങ്ങളോ ഉപയോഗിക്കുന്നു.

ഫിഷിംഗ്

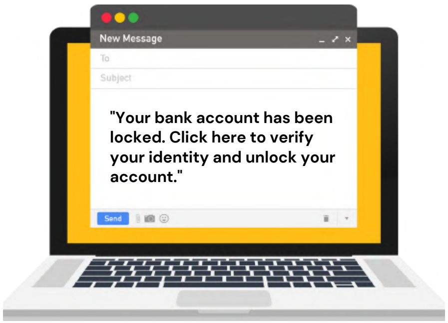
പാസ്‌വേഡുകൾ, ബാങ്ക് വിശദാംശങ്ങൾ, ക്രെഡിറ്റ് കാർഡ് നമ്പറുകൾ എന്നിവ പോലുള്ള നിങ്ങളുടെ സ്വകാര്യ വിവരങ്ങൾ മോഷ്ടിക്കാൻ സ്കാമർമാർ ഉപയോഗിക്കുന്ന ഒരു തന്ത്രമാണ് ഫിഷിംഗ്. വ്യാജ ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യുന്നതിനോ സെൻസിറ്റീവ് വിവരങ്ങൾ പങ്കിടുന്നതിനോ നിങ്ങളെ പ്രേരിപ്പിക്കുന്നതിനായി, നിങ്ങളുടെ ബാങ്ക്, കമ്പനി അല്ലെങ്കിൽ സർക്കാർ ഏജൻസി പോലുള്ള നിങ്ങൾ വിശ്വസിക്കുന്ന ഒരാളായി അവർ സാധാരണയായി നടിക്കുന്നു.

ഫിഷിംഗ് ആക്രമണങ്ങൾ ഒന്നിലധികം മോഡുകളിലൂടെ നടക്കാം. എസ്എംഎസ് / മെസേജിംഗ് ആപ്പുകൾ വഴി നടത്തുന്ന ആക്രമണങ്ങളെ സ്മിഷിംഗ് ആക്രമണങ്ങൾ എന്നും, ഫോൺ കോളുകൾ വഴി നടത്തുന്നവയെ വിഷിംഗ് (വോയ്സ്-ഫിഷിംഗ്) ആക്രമണങ്ങൾ എന്നും വിളിക്കുന്നു.

ഉദാഹരണം:

നിങ്ങൾക്ക് ഒരു ഇമെയിൽ ലഭിക്കും, അതിൽ പറയുന്നത്:

"**നിങ്ങളുടെ ബാങ്ക് അക്കൗണ്ട് ലോക്ക് ചെയ്തിരിക്കുന്നു. നിങ്ങളുടെ ഐഡന്റിറ്റി പരിശോധിച്ചുറപ്പിക്കാനും അക്കൗണ്ട് അൺലോക്ക് ചെയ്യാനും ഇവിടെ ക്ലിക്ക് ചെയ്യുക.**"



നിങ്ങളുടെ ബാങ്കിന്റെ സൈറ്റ് പോലെ തോന്നിക്കുന്ന ഒരു വ്യാജ വെബ്സൈറ്റിലേക്കാണ് ലിങ്ക് നിങ്ങളെ കൊണ്ടുപോകുന്നത്, എന്നാൽ നിങ്ങൾ നൽകുന്ന എല്ലാ വിശദാംശങ്ങളും സ്കാമർ ആക്സസ് ചെയ്യുന്നു.

ഫിഷിംഗ് ഇമെയിലിന്റെ മറ്റൊരു ഉദാഹരണം, ഒരു സ്കാമുകാരൻ ഒരു വ്യക്തിയുടെ സ്ഥാപനത്തിലെ സഹപ്രവർത്തകനായി നടിച്ച് പണം ആവശ്യപ്പെട്ട് ഇമെയിൽ അയയ്ക്കുന്നതാണ്. അത്തരം സന്ദർഭങ്ങളിൽ, ദയവായി പണം കൈമാറരുത്, നിങ്ങളുടെ സഹപ്രവർത്തകനെ (അത് നിങ്ങളുടെ ബോസാണെങ്കിൽ പോലും) വിളിച്ച് അവരുടെ ഐഡന്റിറ്റി പരിശോധിക്കണം. മറ്റൊരു ടിപ്പ് ഇമെയിൽ സ്ഥിരീകരിക്കുക എന്നതാണ്. സാധാരണഗതിയിൽ, ഇമെയിൽ നിങ്ങളുടെ സ്ഥാപനത്തിന്റെ പേരുമായോ സഹപ്രവർത്തകന്റെ യഥാർത്ഥ വർക്ക് ഇമെയിലുമായോ പൊരുത്തപ്പെടില്ല.

മാൽവെയർ

നിങ്ങളുടെ അനുമതിയില്ലാതെ നിങ്ങളുടെ കമ്പ്യൂട്ടർ, ഫോൺ അല്ലെങ്കിൽ മറ്റ് ഉപകരണങ്ങൾ കേടുവരുത്താനോ മോഷ്ടിക്കാനോ നിയന്ത്രണം ഏറ്റെടുക്കാനോ രൂപകൽപ്പന ചെയ്തിരിക്കുന്ന ദോഷകരമായ സോഫ്റ്റ്വെയറാണ് മാൽവെയർ. ഇത് വ്യാജ ആപ്പുകളിലോ ഇമെയിൽ അറ്റാച്ചുമെന്റുകളിലോ (ഇമെയിലുകൾക്കൊപ്പമുള്ള ഫയലുകൾ) വെബ്സൈറ്റുകളിലോ മറഞ്ഞിരിക്കാനും നിങ്ങളുടെ വിവരങ്ങൾ മോഷ്ടിക്കുകയോ നിങ്ങളുടെ ഉപകരണം മന്ദഗതിയിലാക്കുകയോ പോലുള്ള പ്രശ്നങ്ങൾക്ക് കാരണമാകാനും കഴിയും.

ആർട്ടിഫിഷ്യൽ ഇന്റലിജൻസ് (എ.ഐ.)

ഡാറ്റ വിശകലനം ചെയ്യാനും, മനുഷ്യരുടെ പെരുമാറ്റത്തെ അനുകരിക്കാനും, സന്ദേശങ്ങളോ ശബ്ദങ്ങളോ പോലുള്ള യഥാർത്ഥ ഉള്ളടക്കം സൃഷ്ടിക്കാനും കഴിയുന്ന ഒരു സാങ്കേതികവിദ്യയാണ് എ.ഐ. യഥാർത്ഥമെന്ന് തോന്നുന്ന വ്യാജ സന്ദേശങ്ങൾ സൃഷ്ടിക്കുക, ആരുടെയെങ്കിലും ശബ്ദം അനുകരിക്കുക, അല്ലെങ്കിൽ പണമോ വ്യക്തിഗത വിവരങ്ങളോ പങ്കിടാൻ ആളുകളെ കബളിപ്പിക്കാൻ വ്യക്തിഗതമാക്കിയ ഇമെയിലുകൾ അയയ്ക്കുക തുടങ്ങിയ തന്ത്രങ്ങൾ കൂടുതൽ ബോധ്യപ്പെടുത്താൻ സ്കാമുകാർക്ക് എ.ഐ. ഉപയോഗിക്കാം. സ്കാമുകാരെ ഇരകളെ കൂടുതൽ ഫലപ്രദമായി ലക്ഷ്യം വയ്ക്കാൻ എ.ഐ. സഹായിക്കുന്നു, കൂടാതെ അവരുടെ സ്കാമുകൾ കണ്ടെത്തുന്നത് കൂടുതൽ ബുദ്ധിമുട്ടാക്കുന്നു.

സ്പാം

സ്പാം എന്നത് അനാവശ്യമായ അല്ലെങ്കിൽ ജങ്ക് കമ്മ്യൂണിക്കേഷൻ ആണ്, സാധാരണയായി ഫോൺ കോളുകൾ, ഇമെയിൽ, ടെക്സ്റ്റ്, സോഷ്യൽ മീഡിയ എന്നിവയിലൂടെയാണ് ഇത് നിർമ്മിക്കുന്നത്. ഇത് പലപ്പോഴും കാര്യങ്ങൾ പരസ്യപ്പെടുത്താൻ ഉപയോഗിക്കുന്നു, പക്ഷേ ചിലപ്പോൾ ഇത് നിങ്ങളുടെ വിവരങ്ങളോ പണമോ മോഷ്ടിക്കാനുള്ള ശ്രമത്തിന്റെ ഭാഗവുമാണ്.

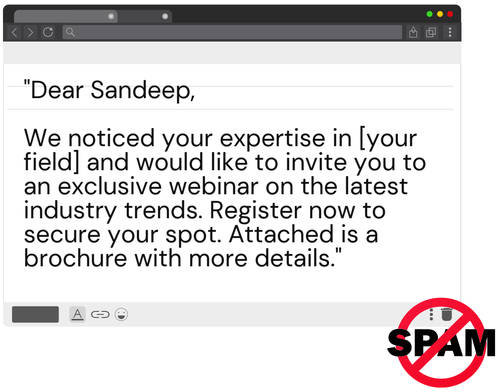
ഉദാഹരണം:

"അഭിനന്ദനങ്ങൾ! നിങ്ങൾ $1,000 സമ്മാന കാർഡ് നേടി! ഇപ്പോൾ തന്നെ നിങ്ങളുടെ സമ്മാനം ക്ലെയിം ചെയ്യാൻ ഇവിടെ ക്ലിക്ക് ചെയ്യുക.."

ഈ ഇമെയിൽ സാധാരണയായി വ്യാജമായിരിക്കും, ലിങ്കിൽ ക്ലിക്ക് ചെയ്യുന്നത് ഒരു സ്കാമിലേക്ക് നയിച്ചേക്കാം അല്ലെങ്കിൽ നിങ്ങളുടെ ഉപകരണത്തിൽ ദോഷകരമായ സോഫ്റ്റ്‌വെയർ ബാധിച്ചേക്കാം.

സ്പാം കൂടുതൽ സങ്കീർണ്ണമാവുകയാണ്, നിങ്ങളുടെ ബിസിനസ്സ്, പ്രൊഫഷൻ, എന്നിവയുമായി ബന്ധപ്പെട്ട ആശയവിനിമയവുമായി സാമ്യപ്പെടുത്താൻ കഴിയും.

നിങ്ങളുടെ തൊഴിലിന് അനുയോജ്യമായ സങ്കീർണ്ണമായ സ്പാമിന്റെ ഒരു ഉദാഹരണം ഇതായിരിക്കാം:



ഇമെയിൽ പ്രൊഫഷണലും നിങ്ങളുടെ ജോലിക്ക് പ്രസക്തവുമായി തോന്നുന്നു, പക്ഷേ ലിങ്ക് ഒരു ഫിഷിംഗ് സൈറ്റിലേക്ക് നയിച്ചേക്കാം, കൂടാതെ അറ്റാച്ചുമെന്റിൽ മാൽവെയർ അടങ്ങിയിരിക്കാം. നിയമാനുസൃതവും വ്യക്തിപരവുമാണെന്ന് കാണിച്ചുകൊണ്ട് പ്രൊഫഷണലുകളെ കബളിപ്പിക്കുന്നതിനാണ് ഇത്തരത്തിലുള്ള സ്പാം രൂപകൽപ്പന ചെയ്തിരിക്കുന്നത്.

സാധാരണ ഫ്രോഡുകളും സ്കാമു കളും

സ്കാം # 1 എഐ വോയ്സ് സ്കാം

അത് എന്താണ്

ഒരു എ.ഐ. വോയ്സ് സ്കാം എന്നത്, കുടുംബാംഗത്തിന്റെയോ മേലധികാരിയുടെയോ പോലുള്ള ഒരാളുടെ ശബ്ദം പകർത്തി നിങ്ങളെ കബളിപ്പിക്കാൻ സ്കാമർമാർ എ.ഐ. ഉപയോഗിക്കുന്നതാണ്. അടിയന്തര സാഹചര്യമാണെന്ന് നടിച്ച് അവർ നിങ്ങളെ വിളിച്ച് പണം ആവശ്യപ്പെട്ടേക്കാം, അല്ലെങ്കിൽ വിവരങ്ങൾ മോഷ്ടിക്കാൻ വ്യാജ നിർദ്ദേശങ്ങൾ നൽകിയേക്കാം. ശബ്ദം യഥാർത്ഥമായി തോന്നുന്നതിനാൽ, അത് വളരെ ബോധ്യപ്പെടുത്തുന്നതും കണ്ടെത്താൻ പ്രയാസകരവുമാണ്.

അത് എങ്ങനെ പ്രവർത്തിക്കുന്നു

സോഷ്യൽ മീഡിയയിൽ നിന്നോ വീഡിയോകളിൽ നിന്നോ വോയ്സ്മെയിലുകളിൽ നിന്നോ ആരുടെയെങ്കിലും ശബ്ദത്തിന്റെ റെക്കോർഡിംഗുകൾ സ്കാമുകാർ കണ്ടെത്തുന്നു. എ.ഐ. ഉപകരണങ്ങൾ ഉപയോഗിച്ച്, അവർ ആ വ്യക്തിയുടെ ശബ്ദം യഥാർത്ഥവും സ്വാഭാവികവുമാക്കാൻ പകർത്തുന്നു.

വ്യാജ ശബ്ദം ഉപയോഗിച്ച് നിങ്ങളെ വിളിക്കുന്ന സ്കാമുകാരൻ, സുഹൃത്ത്, കുടുംബാംഗം അല്ലെങ്കിൽ ബോസ് പോലുള്ള നിങ്ങൾക്ക് പരിചയമുള്ള ഒരാളായി നടിക്കുന്നു. അടിയന്തര സാഹചര്യമുണ്ടെന്ന് അവകാശപ്പെടുന്നതുപോലുള്ള അടിയന്തര സാഹചര്യങ്ങൾ സൃഷ്ടിക്കുകയും പണമോ സമ്മാന കാർഡുകളോ സെൻസിറ്റീവ് വിവരങ്ങളോ ആവശ്യപ്പെടുകയും ചെയ്യുന്നു.

നിങ്ങൾ അതിൽ വീണുപോയാൽ, നിങ്ങൾ അവർക്ക് നൽകുന്നത് ഉപയോഗിച്ച് നിങ്ങളുടെ പണമോ വ്യക്തിഗത വിവരങ്ങളോ അവർ മോഷ്ടിക്കും.

- **അടിയന്തര സാഹചര്യങ്ങളെക്കുറിച്ച് ജാഗ്രത പാലിക്കുക**: സ്കാമുകാർ പലപ്പോഴും വേഗത്തിൽ പ്രവർത്തിക്കാൻ നിങ്ങളെ സമ്മർദ്ദത്തിലാക്കുന്നു. എന്തെങ്കിലും ചെയ്യുന്നതിന് മുമ്പ് ചിന്തിക്കാനും പരിശോധിക്കാനും സമയമെടുക്കുക.
- **വിളിക്കുന്നയാളെ സ്ഥിരീകരിക്കുക**: ആരെങ്കിലും പണമോ സെൻസിറ്റീവ് വ്യക്തിഗത വിവരങ്ങളോ ആവശ്യപ്പെട്ടാൽ, അത് അവർ തന്നെയാണെന്ന് സ്ഥിരീകരിക്കാൻ അവരുടെ പതിവ് നമ്പറിൽ തിരികെ വിളിക്കുക.

- **വ്യക്തിപരമായ ചോദ്യങ്ങൾ ചോദിക്കുക**: സ്കാമുകാരനെ പെട്ടെന്ന് പിടികൂടാൻ, യഥാർത്ഥ വ്യക്തിക്ക് മാത്രം അറിയാവുന്ന എന്തെങ്കിലും ചോദിക്കുക.

- **സുരക്ഷിതമായ ഒരു വാക്ക് ഉപയോഗിക്കുക**: കുടുംബത്തിലോ ജോലിസ്ഥലത്തോ വിശ്വസനീയരായ ആളുകൾക്ക് മാത്രം അറിയാവുന്ന ഒരു "സുരക്ഷിതമായ വാക്ക്" സജ്ജമാക്കുക, ഉദാഹരണത്തിന് "ദ്രാവിഡ്ദവാൾ" അല്ലെങ്കിൽ "റവ ദോശ". ബന്ധുവാണെന്നോ ബോസ് ആണെന്നോ അവകാശപ്പെട്ട് ആരെങ്കിലും പണം ആവശ്യപ്പെട്ടാൽ, മുന്നോട്ട് പോകുന്നതിന് മുമ്പ് സുരക്ഷിതമായ വാക്ക് ചോദിക്കുക. ഒരു സ്കാമുകാരന് അത് അറിയില്ല, അത് അവരുടെ ഐഡന്റിറ്റി പരിശോധിക്കാൻ നിങ്ങളെ സഹായിക്കും.

സ്കാം # 2 ഡേറ്റിംഗ് ആപ്പ് സ്കാം

അത് എന്താണ്

ഒരു ഡേറ്റിംഗ് ആപ്പിൽ ഒരാളുമായി ആരെങ്കിലും പരിചയപ്പെടുകയും സ്കാമിന്റെ ഭാഗമായ ഒരു റസ്റ്റോറന്റിലോ കഫേയിലോ കാണാൻ ക്ഷണിക്കുകയും ചെയ്യുമ്പോഴാണ് ഈ സ്കാം നടക്കുന്നത്. സ്കാമുകാരൻ വിലകൂടിയ സാധനങ്ങൾ, ചിലപ്പോൾ മെനുവിൽ പോലും ഇല്ലാത്ത സാധനങ്ങൾ പോലും ഓർഡർ ചെയ്യുന്നു, തുടർന്ന് പോകാൻ ഒരു ഒഴികഴിവ് കണ്ടെത്തുന്നു. ഇരയ്ക്ക് വലിയൊരു ബിൽ ബാക്കിയാകുകയും ജീവനക്കാരോ ബൗൺസർമാരോ പണം നൽകാൻ നിർബന്ധിതനാകുകയും ചെയ്യുന്നു.

അത് എങ്ങനെ പ്രവർത്തിക്കുന്നു

ഡേറ്റ് ആസൂത്രണം ചെയ്യുന്നു: സ്കാമുകാരൻ തീയതി ആസൂത്രണം ചെയ്യുകയും ഇരയോട് ഒരു പ്രത്യേക കഫേയിൽ കാണാൻ ആവശ്യപ്പെടുകയും ചെയ്യുന്നു. ചിലപ്പോൾ സ്കാമുകാരൻ ഒരു സ്ഥലം നിർദ്ദേശിച്ചേക്കാം, കൂടാതെ അടുത്തുള്ള ഒരു കഫേ തിരഞ്ഞെടുക്കാമെന്ന് പറഞ്ഞ് ഒരു മെട്രോ സ്റ്റേഷനിൽ കാണാൻ ഇരയോട് ആവശ്യപ്പെട്ടേക്കാം.

കഫേയിൽ: അകത്തു കടന്നാൽ, സ്കാമുകാരൻ ഭക്ഷണമോ പാനീയങ്ങളോ ഓർഡർ ചെയ്യും, ചിലപ്പോൾ മെനുവിൽ ഇല്ലാത്ത സാധനങ്ങൾ പോലും. അടിയന്തരാവസ്ഥ വ്യാജമായി നിർമ്മിച്ച് അവർ പെട്ടെന്ന് സ്ഥലം വിട്ടേക്കാം.

ഒരു അപ്രതീക്ഷിത ബിൽ: ബിൽ വരുമ്പോൾ, അത് പ്രതീക്ഷിച്ചതിലും വളരെ കൂടുതലാണ് - പലപ്പോഴും സാധാരണ വിലയുടെ പലമടങ്ങ്. ഇര പ്രതിഷേധിച്ചാൽ, കഫേ ജീവനക്കാരോ ബൗൺസർമാരോ അവരെ ഭീഷണിപ്പെടുത്തി പണം നൽകാൻ നിർബന്ധിക്കുന്നു.

സ്കാം പ്രവർത്തനം: കഫേ ഉടമ, മാനേജർമാരോ ബൗൺസർമാരോ ഉൾപ്പെടെയുള്ള ജീവനക്കാർ, ഡേറ്റിംഗ് ആപ്പിൽ ഇരയുമായി പൊരുത്തപ്പെടുന്ന വ്യക്തി എന്നിവരടങ്ങുന്ന ഒരു ഗ്രൂപ്പാണ് സ്കാം നടത്തുന്നത്. ഊതിപ്പെരുപ്പിച്ച ബില്ലുകളിൽ നിന്ന് ശേഖരിക്കുന്ന പണത്തിന്റെ ഒരു പങ്ക് ഓരോ വ്യക്തിക്കും ലഭിക്കും.

മിക്ക ഇരകളും സ്കാം റിപ്പോർട്ട് ചെയ്യാത്തത്, അവർക്ക് നാണക്കേട് ഭയന്നോ അല്ലെങ്കിൽ അവർ ഒരു ഡേറ്റിംഗ് ആപ്പ് ഉപയോഗിക്കുന്നുണ്ടെന്ന് അവരുടെ കുടുംബത്തോട് വെളിപ്പെടുത്തുമെന്നോ ഉള്ള ഭയം മൂലമാണ്.
ഇത് നിങ്ങൾക്ക് സംഭവിച്ചാൽ, ദയവായി നിങ്ങളുടെ പ്രാദേശിക പോലീസ് സ്റ്റേഷനിലോ www.cybercrime.gov.in എന്ന വെബ്സൈറ്റിലോ റിപ്പോർട്ട് ചെയ്യുക.

- **മീറ്റിംഗ് സ്ഥലത്തെക്കുറിച്ച് ജാഗ്രത പാലിക്കുക**: നിങ്ങൾക്ക് ആ പ്രദേശത്തെക്കുറിച്ച് പരിചയമില്ലെങ്കിൽ മറ്റേയാൾ തിരഞ്ഞെടുത്ത സ്ഥലങ്ങളിൽ മീറ്റിംഗ് നടത്തുന്നത് ഒഴിവാക്കുക.

- **മറ്റൊരാൾ നിർദ്ദേശിക്കുന്ന കഫേയെക്കുറിച്ച് അന്വേഷിക്കുക**: അത് നിയമാനുസൃതമായ സ്ഥലമാണെന്ന് ഉറപ്പാക്കാൻ ഓൺലൈനിൽ കഫേ നോക്കി അവലോകനങ്ങൾ പരിശോധിക്കുക. അവലോകനങ്ങളുടെ ഒന്നിലധികം ഉറവിടങ്ങളിൽ നിന്ന് ക്രോസ്-വെരിഫൈ ചെയ്യുന്നുണ്ടെന്ന് ഉറപ്പാക്കുക.ഒരു സ്ഥലം നിയമാനുസൃതമാണെന്ന് വരുത്തിത്തീർക്കാൻ സ്കാമുകാർ ചിലപ്പോൾ വ്യാജ അവലോകനങ്ങൾ ചേർക്കുന്നു.

- **നിങ്ങളുടെ സഹജവാസനകളെ വിശ്വസിക്കുക**: എന്തെങ്കിലും അസ്വസ്ഥത തോന്നിയാൽ - ആ വ്യക്തി ഒരു സ്ഥലത്ത് അമിതമായി നിർബന്ധം പിടിക്കുകയോ, നിങ്ങൾ റസ്റ്റോറന്റിൽ ഇരുന്നുകഴിഞ്ഞാൽ പെട്ടെന്ന് തണുത്തുറഞ്ഞ് അകന്നു നിൽക്കുകയോ ചെയ്താൽ - ജാഗ്രത പാലിക്കുക.

- **സംശയാസ്പദമായ പെരുമാറ്റം റിപ്പോർട്ട് ചെയ്യുക**: വ്യാജപ്രചാരണം നടക്കുന്നതായി നിങ്ങൾ സംശയിക്കുന്നുവെങ്കിൽ, മറ്റുള്ളവരെ വഞ്ചിക്കുന്നത് തടയാൻ പോലീസിനെയും ഡേറ്റിംഗ് ആപ്പിനെയും അറിയിക്കു

സ്കാം # 3 ഡിജിറ്റൽ അറസ്റ്റ് സ്കാം

അത് എന്താണ്

കസ്റ്റംസ് ഉദ്യോഗസ്ഥരെപ്പോലെ ഓൺലൈനായോ ഫോണിലൂടെയോ പോലീസോ സർക്കാർ ഉദ്യോഗസ്ഥരോ ആയി അഭിനയിക്കുന്ന സ്കാമു കാരെയാണ് ഡിജിറ്റൽ അറസ്റ്റ് സ്കാം എന്ന് വിളിക്കുന്നത്. നിങ്ങൾ നിയമപരമായ പ്രശ്നത്തിലാണെന്ന് അവർ അവകാശപ്പെടുകയും "അറസ്റ്റ് ഒഴിവാക്കാൻ" ഉടനടി പണം നൽകണമെന്ന് ആവശ്യപ്പെടുകയും ചെയ്യുന്നു. ഇരകളെ വേഗത്തിൽ പണം നൽകാൻ സമ്മർദ്ദത്തിലാക്കാൻ അവർ പലപ്പോഴും ഭയവും അടിയന്തിരാവസ്ഥയും ഉപയോഗിക്കുന്നു.

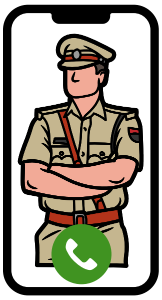
അത് എങ്ങനെ പ്രവർത്തിക്കുന്നു

വ്യാജ കോൾ അല്ലെങ്കിൽ സന്ദേശം: നിയമം ലംഘിച്ചുവെന്നും പിഴ അടയ്ക്കണമെന്നും അല്ലെങ്കിൽ അറസ്റ്റ് നേരിടേണ്ടിവരുമെന്നും അവകാശപ്പെടുന്ന ഒരു കോൾ, ഇമെയിൽ അല്ലെങ്കിൽ ടെക്സ്റ്റ് നിങ്ങൾക്ക് ലഭിക്കും. ഉദാഹരണത്തിന്, ഒരു പാഴ്സലിന്റെ ഷെഡ്യൂൾ ചെയ്ത ഡെലിവറി റദ്ദാക്കിയതായി അവകാശപ്പെടുന്ന ഒരു അന്താരാഷ്ട്ര നമ്പറിൽ നിന്ന് ഒരു ഇരയ്ക്ക് ഒരു കോൾ ലഭിക്കുന്നു.

ഭീഷണികളും സമ്മർദ്ദവും: ഉടനടി പണം നൽകിയില്ലെങ്കിൽ ജയിൽ ശിക്ഷ പോലുള്ള ഗുരുതരമായ പ്രത്യാഘാതങ്ങൾ നേരിടേണ്ടിവരുമെന്ന് സ്കാമുകാരൻ പറയുന്നു. മുകളിൽ സൂചിപ്പിച്ച സാഹചര്യത്തിൽ, വിളിച്ചയാൾ ഇരയോട് പിന്തുണയ്ക്കായി "0" അമർത്താൻ ആവശ്യപ്പെട്ടു. അവർ ഇത് ചെയ്തയുടനെ, കസ്റ്റമർ സപ്പോർട്ട് പ്രതിനിധിയായി വേഷംമാറിയ ഒരാൾ കോളിൽ എത്തി, അവരുടെ പേരിലുള്ള ഒരു പാക്കേജിൽ നിയമവിരുദ്ധ വസ്തുക്കൾ അടങ്ങിയിട്ടുണ്ടെന്നും അത് ചൈനയിലേക്ക് അയച്ചിട്ടുണ്ടെന്നും അവകാശപ്പെട്ടു. തനിക്കെതിരെ അറസ്റ്റ് വാറണ്ട് പുറപ്പെടുവിച്ചിട്ടുണ്ടെന്നും പ്രതിനിധി അവകാശപ്പെട്ടു. തുടർന്ന് വ്യാജ പോലീസ് ഉദ്യോഗസ്ഥരും അന്വേഷകരും വീഡിയോ കോളിൽ ചേർന്നു. സ്കാമുകാർ യഥാർത്ഥ പോലീസുകാരാണെന്ന് നിങ്ങളെ ബോധ്യപ്പെടുത്താൻ ഏതറ്റം വരെയും പോകും. വ്യാജ ലെറ്റർഹെഡുകളും ഐഡി കാർഡുകളും അവർ നിങ്ങൾക്ക് കാണിച്ചുതരും. വ്യാജ പോലീസ് സ്റ്റേഷനുകൾ പോലും അവർ സൃഷ്ടിക്കുകയും വീഡിയോ കോളിംഗ് സമയത്ത് പോലീസുകാരെപ്പോലെ വേഷം ധരിക്കുകയും ചെയ്യും.

ഐസൊലേഷനും അടിയന്തരാവസ്ഥയും: സ്കാമുകാരൻ നിങ്ങളെ ഒറ്റപ്പെടുത്താൻ പ്രേരിപ്പിക്കാൻ ശ്രമിക്കും. ഒരു വിദൂര സ്ഥലത്തേക്ക് യാത്ര ചെയ്യാൻ അല്ലെങ്കിൽ ഒരു മുറിയിൽ പൂട്ടിയിട്ട് കർട്ടനുകൾ വലിക്കാൻ അവർ നിങ്ങളോട് പറയും. മറ്റ് കോളുകൾ എടുക്കുന്നത് ഒഴിവാക്കാനും അവർ നിങ്ങളോട് പറയും.

നിരന്തരമായ പേയ്മെന്റ് ആവശ്യങ്ങൾ: അവർ പണത്തിനായി നിരന്തരമായ ആവശ്യങ്ങൾ ഉന്നയിക്കുന്നു, സാധാരണയായി ഒന്നിലധികം അക്കൗണ്ടുകളിലേക്ക് പണം തട്ടുന്നതിനാൽ അത് കണ്ടെത്താൻ കഴിയില്ല.



ഉദാഹരണം:

നിങ്ങൾക്ക് ഒരു കോൾ ലഭിക്കുന്നു: **"ഇത് സൈബർ ക്രൈം യൂണിറ്റിലെ ഓഫീസർ X ആണ്. നിങ്ങളുടെ അക്കൗണ്ടുമായി ബന്ധിപ്പിച്ചിരിക്കുന്ന നിയമവിരുദ്ധ പ്രവർത്തനം ഞങ്ങൾ കണ്ടെത്തി. നിങ്ങൾ പണം നൽകണം. അറസ്റ്റ് ഒഴിവാക്കാൻ ഇപ്പോൾ ₹10,000. ഇത് പാലിക്കുന്നതിൽ പരാജയപ്പെട്ടാൽ അറസ്റ്റിൽ കലാശിക്കും."**

- **ശാന്തത പാലിക്കുക**: ഇന്ത്യയിൽ ഒരു ഫോൺ കോളിലൂടെയോ വീഡിയോ കോളിലൂടെയോ പോലീസിന് അറസ്റ്റ് ചെയ്യാൻ കഴിയില്ല, അറസ്റ്റ് ചെയ്യുകയുമില്ല. നിങ്ങളുടെ വിലാസം, പേര് തുടങ്ങിയ വ്യക്തിഗത വിവരങ്ങൾ അറിയാമെന്ന് സ്കാമുകാരൻ അവകാശപ്പെട്ടാലും പരിഭ്രാന്തരാകരുത്. ഉടൻ തന്നെ കോൾ വിച്ഛേദിച്ച് ഇടപെടുന്നത് നിർത്തുക.

- **ക്ലെയിം സ്ഥിരീകരിക്കുക:** ഫോൺ കട്ട് ചെയ്ത് ഔദ്യോഗിക സ്ഥാപനത്തെ അവരുടെ ഔദ്യോഗിക ഫോൺ നമ്പറോ വെബ്സൈറ്റോ ഉപയോഗിച്ച് നേരിട്ട് ബന്ധപ്പെടുക, അത് പോലീസോ മറ്റ് സർക്കാർ ഉദ്യോഗസ്ഥരോ അല്ലെങ്കിൽ നിങ്ങളെ വിളിച്ച ഉപഭോക്തൃ സേവന പ്രതിനിധിയുടെ സ്ഥാപനമോ ആകട്ടെ.

- **ഒറ്റപ്പെടൽ നിരസിക്കുക**: നിങ്ങളെ ഒറ്റപ്പെടുത്താനോ സുഹൃത്തുക്കളിൽ നിന്നോ കുടുംബാംഗങ്ങളിൽ നിന്നോ കോളുകൾ എടുക്കുന്നത് ഒഴിവാക്കാനോ ആരും നിങ്ങളെ നിർബന്ധിക്കാൻ ഒരിക്കലും അനുവദിക്കരുത്. നിങ്ങൾ വിശ്വസിക്കുന്ന ഒരാളുമായി ഉടൻ തന്നെ ഫോൺ കട്ട് ചെയ്ത് സംസാരിക്കുക.

- **പണമടയ്ക്കരുത്**: യഥാർത്ഥ നിയമപാലകർ ഒരിക്കലും ഫോണിലൂടെ പണം ആവശ്യപ്പെടില്ല. അത്തരം എല്ലാ ആവശ്യങ്ങളും നിരസിക്കുക.

- **റെഡ് ഫ്ലാഗുകൾക്കായി ശ്രദ്ധിക്കുക**: നിങ്ങൾക്ക് തിരിച്ചറിയാൻ കഴിയാത്ത അന്താരാഷ്ട്ര അല്ലെങ്കിൽ ആഭ്യന്തര നമ്പറുകളിൽ നിന്നുള്ള കോളുകൾ. നിങ്ങളുടെ പേര്, ബാങ്ക് അക്കൗണ്ട് അല്ലെങ്കിൽ ഐഡി പോലുള്ള വ്യക്തിഗത വിവരങ്ങൾ "പരിശോധിക്കുന്നതിനുള്ള" അഭ്യർത്ഥനകൾ.

- **ശ്രദ്ധിക്കുക**: വിദേശ രാജ്യങ്ങളിൽ നിന്നുള്ള കോളുകൾ പോലെ അജ്ഞാതമായതോ സംശയാസ്പദമായതോ ആയ നമ്പറുകളിൽ നിന്നുള്ള ഫോൺ കോളുകൾക്ക് മറുപടി നൽകുമ്പോൾ ജാഗ്രത പാലിക്കുക.

സ്കാം # 4 വ്യാജ നിക്ഷേപ / ട്രേഡിംഗ് ആപ്പ് സ്കാം

അത് എന്താണ്

നിക്ഷേപകരെ കബളിപ്പിക്കാൻ രൂപകൽപ്പന ചെയ്തിരിക്കുന്ന ഫ്രോഡായിട്ടുള്ള ട്രേഡിംഗ് ആപ്ലിക്കേഷനുകളുടെ സൃഷ്ടിയും പ്രചാരണവും വ്യാജ ട്രേഡിംഗ് ആപ്പ് സ്കാമിൽ ഉൾപ്പെടുന്നു. ഈ ആപ്പുകൾ പലപ്പോഴും ഉയർന്ന വരുമാനവും കുറഞ്ഞ അപകടസാധ്യതകളും വാഗ്ദാനം ചെയ്യുന്നു, ഇത് നിങ്ങളുടെ പണം നിക്ഷേപിക്കാൻ നിങ്ങളെ വശീകരിക്കുന്നു. എന്നിരുന്നാലും, നിങ്ങൾ ഈ വ്യാജ ആപ്പുകളിൽ ഫണ്ട് നിക്ഷേപിച്ചുകഴിഞ്ഞാൽ, നിങ്ങൾക്ക് നിരവധി ഫ്രോഡായിട്ടുള്ള രീതികൾ നേരിടേണ്ടി വന്നേക്കാം.

അത് എങ്ങനെ പ്രവർത്തിക്കുന്നു

വ്യാജ നിക്ഷേപ ആപ്പുകൾക്കായുള്ള പരസ്യങ്ങളും പ്രമോഷനും: അസാധാരണമായി ഉയർന്ന സാമ്പത്തിക വരുമാനം വാഗ്ദാനം ചെയ്ത് ഇരകളെ ആകർഷിക്കാൻ സ്കാമു കാർ ഫ്രോഡായിട്ടുള്ള പരസ്യങ്ങൾ ഉപയോഗിക്കുന്നു. പലപ്പോഴും, "ഐസിഐസിഐ ഐആർ ടീം" പോലുള്ള നിയമാനുസൃതമായ പേരുകളുള്ള സ്കാമു കാർ ഇരകളെ വാട്ട്സ്ആപ്പ് ഗ്രൂപ്പുകളിലേക്ക് ചേർക്കുന്നു, ഇത് ഇരകളെ ലൈസൻസുള്ള ധനകാര്യ സ്ഥാപനങ്ങളുമായി ബന്ധമുള്ളവരാണെന്ന് ചിന്തിപ്പിക്കുന്നു. ഇരയുടെ വിശ്വാസം നേടുന്നതിനായി വ്യാജ വിജയഗാഥകൾ പങ്കിടാൻ സ്കാമു കാർ സാധാരണയായി ഈ ഗ്രൂപ്പുകളെ ഉപയോഗിക്കുന്നു.

വ്യാജ ആപ്പുകൾ ഡൗൺലോഡ് ചെയ്യാനും നിക്ഷേപിക്കാനുമുള്ള നിർദ്ദേശങ്ങൾ: യഥാർത്ഥ നിക്ഷേപ അവസരങ്ങൾ വാഗ്ദാനം ചെയ്യുന്നതായി തോന്നുന്ന വ്യാജ ആപ്പുകൾ ഡൗൺലോഡ് ചെയ്യാൻ ഇരകളോട് നിർദ്ദേശിക്കുന്നു.
'IC ORGAN MAX', 'Techstars.shop' പോലുള്ള ഈ ആപ്പുകൾ, അറിയപ്പെടുന്ന സ്റ്റോക്കുകളുടെയും സാമ്പത്തിക ഉപകരണങ്ങളുടെയും പേരുകൾ പ്രദർശിപ്പിക്കുകയും ഉപയോക്താക്കളെ അവ നിയമാനുസൃതമാണെന്ന് വിശ്വസിപ്പിക്കുകയും ചെയ്യുന്നു. വ്യാജ ചാർട്ടുകൾ, അക്കൗണ്ട് ബാലൻസുകൾ, ലാഭ പ്രസ്താവനകൾ എന്നിവ ഉപയോഗിച്ച് നിങ്ങളുടെ നിക്ഷേപങ്ങൾ വളരുന്നതായി തോന്നിപ്പിക്കുന്ന തരത്തിൽ യഥാർത്ഥമായി കാണപ്പെടുന്ന തരത്തിലാണ് ആപ്പ് രൂപകൽപ്പന ചെയ്തിരിക്കുന്നത്.

ഉയർന്ന റിട്ടേണുകളുടെ കൃത്രിമ പ്രദർശനം: ഇരകൾ വ്യാജ ആപ്പുകൾ ഇൻസ്റ്റാൾ ചെയ്ത് പണം നിക്ഷേപിച്ചുകഴിഞ്ഞാൽ, ഡാഷ്ബോർഡിൽ നല്ല റിട്ടേണുകൾ പ്രദർശിപ്പിക്കുന്നത് അവർ കാണും, ഇത് കൂടുതൽ നിക്ഷേപിക്കാൻ അവരെ പ്രോത്സാഹിപ്പിക്കുന്നു. എന്നിരുന്നാലും, ഈ റിട്ടേണുകൾ കെട്ടിച്ചമച്ച സംഖ്യകളാണ്. ഇരകൾ പണം പിൻവലിക്കാൻ ശ്രമിക്കുമ്പോൾ, നിയമാനുസൃത നികുതികൾ അല്ലെങ്കിൽ ബ്രോക്കറേജ് ഫീസ് പോലുള്ള അധിക ചാർജുകൾ അടയ്ക്കാൻ അവരോട് ആവശ്യപ്പെടുന്നു, അതുവഴി സ്കാമു കാർക്ക് അവരിൽ നിന്ന് കൂടുതൽ പണം കൈക്കലാക്കാൻ കഴിയും.

ഫ്രോഡായ പ്രവൃത്തികൾ

ലോക്ക് ചെയ്ത ഫണ്ടുകൾ: നിങ്ങളുടെ പണം പിൻവലിക്കാൻ കഴിയില്ലെന്ന് നിങ്ങൾ കണ്ടെത്തിയേക്കാം.

ഫീസ് ആവശ്യങ്ങൾ: നിങ്ങളുടെ ഫണ്ടുകൾ ആക്സസ് ചെയ്യുന്നതിന് മുമ്പ് ആപ്പ് അധിക "ഫീസ്" അല്ലെങ്കിൽ "നികുതി" ആവശ്യപ്പെട്ടേക്കാം.
അപ്രത്യക്ഷമാകുന്ന നിയമം: സ്കാമു കാർ ആപ്പ് പൂർണ്ണമായും അടച്ചുപൂട്ടി നിങ്ങളുടെ പണം അവർക്കൊപ്പം കൊണ്ടുപോയിരിക്കാം.

വ്യാജ പിന്തുണ: നിങ്ങൾ സഹായത്തിനായി സമീപിച്ചാൽ, കൂടുതൽ ഫണ്ട് നിക്ഷേപിക്കാൻ നിങ്ങളെ തടയുകയോ സമ്മർദ്ദം ചെലുത്തുകയോ ചെയ്യുന്ന വ്യാജ ഉപഭോക്തൃ പിന്തുണ നിങ്ങൾക്ക് നേരിടേണ്ടി വന്നേക്കാം.

അപ്രത്യക്ഷമാകുന്ന സ്കാമുകാർ: സ്കാം തുറന്നുകാട്ടിയാൽ, ആപ്പ് നീക്കം ചെയ്യപ്പെടുകയും സ്കാമുകാർ അപ്രത്യക്ഷമാവുകയും ചെയ്യുന്നു, ഇത് ഇരകൾക്ക് അവരുടെ പണം വീണ്ടെടുക്കാൻ ഒരു മാർഗവുമില്ലാതെയാക്കുന്നു.

- ഓൺലൈൻ നിക്ഷേപങ്ങളിലൂടെ വേഗത്തിലുള്ള പണം വാഗ്ദാനം ചെയ്യാൻ നിങ്ങൾ ആവശ്യപ്പെട്ടിട്ടില്ലാത്ത അനാവശ്യ/അപ്രതീക്ഷിതമായ സന്ദേശങ്ങളെക്കുറിച്ച് ജാഗ്രത പാലിക്കുക.
- അസാധ്യമായ വരുമാനം വാഗ്ദാനം ചെയ്യുന്ന നിക്ഷേപ അവസരങ്ങൾ ഒഴിവാക്കുക.
- ഔദ്യോഗിക വെബ്സൈറ്റുകളിലൂടെയോ ആപ്പുകളിലൂടെയോ നിക്ഷേപ പ്ലാറ്റ്ഫോമുകളുടെ നിയമസാധുത പരിശോധിക്കുക. ഉദാഹരണത്തിന്, അവർ ഐ.സി.ഐ.സി.ഐ. പോലുള്ള ഒരു പ്രത്യേക ബാങ്കുമായി അഫിലിയേറ്റ് ചെയ്തിട്ടുണ്ടെന്ന് നിർദ്ദേശിക്കുകയാണെങ്കിൽ, ഇത് ശരിയാണോ എന്ന് കാണാൻ ഐ.സി.ഐ.സി.ഐ.-യുടെ കസ്റ്റമർ സപ്പോർട്ടിനെ വിളിക്കുകയോ അവരുടെ ഔദ്യോഗിക വെബ്സൈറ്റ് പരിശോധിക്കുകയോ ചെയ്യുക..
- പ്രത്യേകിച്ച് മെസേജിംഗ് ആപ്പുകളിൽ, ലോഗിൻ ക്രെഡൻഷ്യലുകൾ, വ്യക്തിഗത അല്ലെങ്കിൽ സാമ്പത്തിക വിവരങ്ങൾ അപരിചിതരുമായി പങ്കിടരുത്.
- പരിചയമില്ലാത്ത കോൺടാക്റ്റുകൾ ആവശ്യപ്പെട്ടാൽ അജ്ഞാത ആപ്പുകളോ ഫയലുകളോ ഡൗൺലോഡ് ചെയ്യുന്നത് ഒഴിവാക്കുക.

സ്കാം # 5 വ്യാജ ജോലി ഓഫർ സ്കാം

അത് എന്താണ്

ജോലി വാഗ്ദാനം ചെയ്യുന്നതായി നടിച്ച് പണമോ വ്യക്തിഗത വിവരങ്ങളോ നൽകുന്നതിനായി സ്കാമുകാർ നിങ്ങളെ കബളിപ്പിക്കുന്നതാണ് വ്യാജ ജോലി ഓഫർ സ്കാം. ഉയർന്ന ശമ്പളം, എളുപ്പമുള്ള ജോലി അല്ലെങ്കിൽ ആനുകൂല്യങ്ങൾ വാഗ്ദാനം ചെയ്ത് ജോലി അന്വേഷിക്കുന്ന ആളുകളെയാണ് ഈ സ്കാമുകൾ പലപ്പോഴും ലക്ഷ്യമിടുന്നത്.

ഇത് എങ്ങനെ പ്രവർത്തിക്കുന്നു

ആകർഷകമായ ജോലി പോസ്റ്റ്: സ്കാമുകാർ വെബ്സൈറ്റുകളിലും സോഷ്യൽ മീഡിയയിലും വ്യാജ തൊഴിൽ പരസ്യങ്ങൾ സൃഷ്ടിക്കുകയോ ഇമെയിലുകളിലൂടെയോ സന്ദേശങ്ങളിലൂടെയോ അയയ്ക്കുകയോ ചെയ്യുന്നു. ചിലപ്പോൾ, ഒരു പ്രശസ്ത കമ്പനിയിൽ നിങ്ങൾക്ക് പ്ലേസ്മെന്റ് ഉറപ്പുനൽകുന്ന കൺസൾട്ടൻസികളായി സ്കാമർമാർ നടിച്ചേക്കാം.

ദ്രുത തിരഞ്ഞെടുപ്പ് പ്രക്രിയ: ജോലിക്ക് നിങ്ങളെ "തിരഞ്ഞെടുത്തിരിക്കുന്നു" എന്ന് അവർ നിങ്ങളോട് പറയും, പലപ്പോഴും ഒരു അഭിമുഖമോ ശരിയായ സ്ക്രീനിംഗോ ഇല്ലാതെ.

പേയ്മെന്റ് അല്ലെങ്കിൽ വ്യക്തിഗത വിവരങ്ങൾക്കായുള്ള അഭ്യർത്ഥനകൾ: പരിശീലനം, രജിസ്ട്രേഷൻ, ജോലി സാമഗ്രികൾ അല്ലെങ്കിൽ വിസ പ്രോസസ്സിംഗ് (അത് ഒരു അന്താരാഷ്ട്ര ജോലിയാണെങ്കിൽ) പോലുള്ള കാര്യങ്ങൾക്ക് ഫീസ് അടയ്ക്കാൻ നിങ്ങളോട് ആവശ്യപ്പെടും.

വ്യാജ രേഖകൾ അല്ലെങ്കിൽ ലിങ്കുകൾ: അവർ വ്യാജ ഓഫർ ലെറ്ററുകൾ, കരാറുകൾ അല്ലെങ്കിൽ നിയമാനുസൃതമാണെന്ന് കാണിക്കാൻ നിങ്ങളെ ഫ്രോഡായിട്ടുള്ള വെബ്സൈറ്റുകളിലേക്ക് നയിച്ചേക്കാം.

വാനിഷിംഗ് ആക്റ്റ്: പണമോ നിങ്ങളുടെ സ്വകാര്യ വിവരങ്ങളോ അവർ ശേഖരിച്ചുകഴിഞ്ഞാൽ, സ്കാമുകാർ അപ്രത്യക്ഷമാകും, ജോലി നിലവിലില്ല.

വ്യാജ ജോലി സ്കാമുകളുടെ ഉദാഹരണങ്ങൾ

ഇതാ പലതരം വ്യാജ തൊഴിൽ സ്കാമുകൾ.

- **വീട്ടിലിരുന്ന് ജോലി ചെയ്യൽ സ്കാം**
- **ജോലി പ്ലെയ്സ്മെന്റ് സേവന സ്കാമുകൾ**
- **നാനി, കെയർഗിവർ, വെർച്വൽ പേഴ്സണൽ അസിസ്റ്റന്റ് ജോലി സ്കാമുകൾ**

വീട്ടിലിരുന്ന് ജോലി ചെയ്യുന്നതിനുള്ള സ്കാം

കുറഞ്ഞ സമയവും പരിശ്രമവും ഉപയോഗിച്ച് വീട്ടിൽ നിന്ന് ജോലി ചെയ്ത് പ്രതിമാസം ലക്ഷക്കണക്കിന് രൂപ സമ്പാദിക്കാൻ കഴിയുന്ന ജോലികൾ വാഗ്ദാനം ചെയ്യുന്നുവെന്ന് സ്കാമുകാർ അവകാശപ്പെടുന്നു.

വീട്ടിൽ നിന്ന് ജോലി ചെയ്യുന്ന സാധാരണ സ്കാമുകളിൽ റീഷിപ്പിംഗ് സ്കാമുകളും ചരക്ക് റീസെല്ലിംഗ് സ്കാമുകളും ഉൾപ്പെടുന്നു.

റീഷിപ്പിംഗ് സ്കാമുകൾ: ഗുണനിലവാര നിയന്ത്രണ മാനേജർമാർ അല്ലെങ്കിൽ വെർച്വൽ അസിസ്റ്റന്റുകൾ പോലുള്ള വ്യാജ ജോലികൾ സ്കാമുകാർ പരസ്യപ്പെടുത്തുന്നു. "നിയമിക്കപ്പെട്ടുകഴിഞ്ഞാൽ", നിങ്ങളുടെ ചുമതല വിലയേറിയ ഇനങ്ങൾ സ്വീകരിക്കുക, വീണ്ടും പായ്ക്ക് ചെയ്യുക, വീണ്ടും ഷിപ്പ് ചെയ്യുക എന്നിവയാണ്, പലപ്പോഴും മോഷ്ടിച്ച ക്രെഡിറ്റ് കാർഡുകൾ ഉപയോഗിച്ച് വാങ്ങുന്നു. ശമ്പളം ഒരിക്കലും ലഭിക്കില്ല, കമ്പനി അപ്രത്യക്ഷമാകും, ഇത് നിങ്ങളെ ഒരു കുറ്റകൃത്യത്തിൽ ഉൾപ്പെടുത്തും. "പേറോളിന്" നിങ്ങൾ വ്യക്തിഗത വിവരങ്ങൾ നൽകിയാൽ, നിങ്ങൾക്ക് ഐഡന്റിറ്റി മോഷണവും നേരിടേണ്ടിവരും.

മെർച്ചൻഡൈസ് റീസെല്ലിംഗ് സ്കാമുകൾ: ലാഭത്തിൽ ആഡംബര ഉൽപ്പന്നങ്ങൾ വീണ്ടും വിൽക്കുന്ന ജോലി സ്കാമുകാർ വാഗ്ദാനം ചെയ്യുന്നു. നിങ്ങൾ ഇനങ്ങൾക്ക് പണം നൽകിയ ശേഷം, പാക്കേജ് ഒരിക്കലും എത്തുകയോ വിലകെട്ട മാലിന്യങ്ങൾ അടങ്ങിയിരിക്കുകയോ ചെയ്യില്ല.

നാനി, കെയർഗിവർ, വെർച്വൽ പേഴ്സണൽ അസിസ്റ്റന്റ് ജോബ് സ്കാം

നാനിമാർ, പരിചരണം നൽകുന്നവർ, വെർച്വൽ അസിസ്റ്റന്റുമാർ എന്നിവർക്കായി സ്കാമർമാർ ജോബ് സൈറ്റുകളിൽ വ്യാജ ജോലി പരസ്യങ്ങൾ പോസ്റ്റ് ചെയ്യുന്നു. അല്ലെങ്കിൽ നിങ്ങളുടെ കമ്മ്യൂണിറ്റിയിലെ ഒരാളിൽ നിന്നാണെന്ന് തോന്നിപ്പിക്കുന്ന ഇമെയിലുകൾ അവർ അയച്ചേക്കാം. നിങ്ങളുടെ കോളേജ് അല്ലെങ്കിൽ യൂണിവേഴ്സിറ്റി പോലുള്ള നിങ്ങൾക്ക് അറിയാവുന്ന ഒരു സ്ഥാപനത്തിന്റെ ഭാഗമായ ഒരാളിൽ നിന്നും സന്ദേശം വരുന്നതായി തോന്നിയേക്കാം.

നിങ്ങൾ അപേക്ഷിക്കുകയാണെങ്കിൽ, നിങ്ങളെ നിയമിക്കുന്ന വ്യക്തി നിങ്ങൾക്ക് ഒരു ചെക്ക് അയച്ചേക്കാം. ചെക്ക് നിക്ഷേപിക്കാനും, നിങ്ങളുടെ സേവനങ്ങൾക്കായി പണത്തിന്റെ ഒരു ഭാഗം സൂക്ഷിക്കാനും, ബാക്കി മറ്റൊരാൾക്ക് അയയ്ക്കാനും അവർ നിങ്ങളോട് പറയും.

ഇതൊരു സ്കാമാണ്. ഒരു നിയമാനുസൃത തൊഴിലുടമ ഒരിക്കലും നിങ്ങളോട് അങ്ങനെ ചെയ്യാൻ ആവശ്യപ്പെടില്ല. ചെക്ക് വ്യാജമാണ്, അത് ബൗൺസ് ചെയ്യും, വ്യാജ ചെക്കിന്റെ മുഴുവൻ തുകയും നിങ്ങൾ തിരികെ നൽകണമെന്ന് ബാങ്ക് ആവശ്യപ്പെടും, അതേസമയം സ്കാമുകാരൻ നിങ്ങൾ അയച്ച യഥാർത്ഥ പണം സൂക്ഷിക്കും.

ജോബ് പ്ലേസ്മെന്റ് സർവീസ് സ്കാമുകൾ

ഒരു മികച്ച കമ്പനിയിൽ നിങ്ങളെ നിയമിക്കാൻ സഹായിക്കുന്ന ഒരു കൺസൾട്ടൻസി എന്ന വ്യാജേനയാണ് സ്കാമുകാരൻ നിങ്ങളെ സമീപിക്കുന്നത്. അവർ നിങ്ങളെ ഒരു അഭിമുഖത്തിനായി വിളിക്കും. നിങ്ങൾ എത്തുമ്പോൾ, പ്രവേശന കവാടത്തിൽ വലിയ ആളുകൾ നിൽക്കുന്നുണ്ടാകാം. സ്കാമുകാരൻ ഒരു കൺസൾട്ടന്റായി വേഷമിട്ട് നിങ്ങളുടെ യോഗ്യതകളെക്കുറിച്ച് ചില പൊതുവായ ചോദ്യങ്ങൾ ചോദിക്കും. മുമ്പ് പ്രധാന മൾട്ടി-നാഷണൽ കമ്പനികളിൽ ജോലി ചെയ്തിട്ടുണ്ടെന്ന് ആരോപിക്കപ്പെടുന്ന ആളുകളുടെ വ്യാജ ചിത്രങ്ങൾ പോലും അവർ നിങ്ങളെ കാണിച്ചേക്കാം. ഇതിനുശേഷം, അവർ നിങ്ങളോട് പണം ചോദിക്കും, വലിയ ആളുകൾ പണം നൽകാൻ നിർബന്ധിച്ചേക്കാം.

- ഒരു സ്ഥാപനമോ/കമ്പനിയോ ഒരിക്കലും അവർക്കുവേണ്ടി പ്രവർത്തിക്കാൻ പണം ആവശ്യപ്പെടില്ല. സ്പാം / ജങ്ക് ഇമെയിലുകൾ അല്ലെങ്കിൽ സന്ദേശങ്ങൾ വഴി അയയ്ക്കുന്ന ജോലി ഓഫറുകൾ അവഗണിക്കുക.
- ഒരു ചെക്ക് നിക്ഷേപിക്കുകയും പിന്നീട് ഏതെങ്കിലും കാരണത്താൽ കുറച്ച് പണം ഉപയോഗിക്കുകയും ചെയ്യുന്ന ഒരു ഓഫർ നിങ്ങൾക്ക്ല ഭിക്കുകയാണെങ്കിൽ, അത് ഒരു സ്കാമാ ണ്. അകന്നു പോകുക.
- പ്ലേസ്മെന്റ് സ്ഥാപനങ്ങൾ ഉദ്യോഗാർത്ഥികൾക്ക് ഫീസ് ആവശ്യപ്പെടുന്നില്ല. ജോലികൾക്കായി ഉദ്യോഗാർത്ഥികളെ കണ്ടെത്താൻ കമ്പനികൾ അവർക്ക് ഫീസ് നൽകുന്നു. ഒരു പ്ലെയ്സ്മെന്റ് സ്ഥാപനം നിങ്ങളോട് ഒരു ഫീസ് ചോദിച്ചാൽ - പ്രത്യേകിച്ച് നിങ്ങൾ മുൻകൂട്ടി അടയ്ക്കേണ്ട ഒന്ന് - ഒഴിഞ്ഞുമാറുക. നിങ്ങൾ ഒരു സ്കാം നേരിടുകയായിരിക്കാം.
- ആരെങ്കിലും നിങ്ങൾക്ക് ഒരു ജോലി വാഗ്ദാനം ചെയ്യുകയും കുറഞ്ഞ സമയത്തിനുള്ളിൽ നിങ്ങൾക്ക് ധാരാളം പണം സമ്പാദിക്കാൻ കഴിയുമെന്ന് അവകാശപ്പെടുകയും ചെയ്താൽ, അത് തീർച്ചയായും ഒരു സ്കാമാ ണ്.
- കമ്പനിയുടെ വെബ്സൈറ്റ്, അവലോകനങ്ങൾ, ഔദ്യോഗിക കോൺടാക്റ്റ് വിശദാംശങ്ങൾ എന്നിവ പരിശോധിക്കുക.
- ഓൺലൈൻ സാന്നിധ്യമില്ലാത്തതോ അവ്യക്തമായ വിശദാംശങ്ങളോ ഇല്ലാത്ത കമ്പനികളിൽ നിന്നുള്ള ഓഫറുകൾ ഒഴിവാക്കുക.
- നിങ്ങളുടെ ബാങ്ക് അക്കൗണ്ട്, ആധാർ അല്ലെങ്കിൽ പാൻ പോലുള്ള സെൻസിറ്റീവ് വിശദാംശങ്ങൾ കമ്പനി പരിശോധിക്കാതെ പങ്കിടരുത്.

സ്കാം # 6 വ്യാജ ലിങ്ക് / ക്യുആർ കോഡ് സ്കാം

അത് എന്താണ്

വ്യാജ ലിങ്ക്/ക്യുആർ കോഡ് സ്കാം വഴി നിങ്ങളെ ഒരു ക്ഷുദ്ര ലിങ്കിൽ ക്ലിക്ക് ചെയ്യുന്നതിനോ ഫ്രോഡായിട്ടുള്ള ക്യുആർ കോഡ് സ്കാൻ ചെയ്യുന്നതിനോ കഴിയും. വ്യക്തിഗത വിവരങ്ങൾ, പേയ്മെന്റ് വിശദാംശങ്ങൾ എന്നിവ മോഷ്ടിക്കുന്നതിനോ നിങ്ങളുടെ ഉപകരണത്തിൽ ദോഷകരമായ സോഫ്റ്റ്‌വെയർ ഇൻസ്റ്റാൾ ചെയ്യുന്നതിനോ വേണ്ടിയാണ് ഈ സ്കാമുകൾ രൂപകൽപ്പന ചെയ്തിരിക്കുന്നത്.

ഇത് എങ്ങനെ പ്രവർത്തിക്കുന്നു

വ്യാജ ലിങ്കുകൾ: ആകർഷകമായ എന്തെങ്കിലും വാഗ്ദാനം ചെയ്യുമെന്ന് അവകാശപ്പെട്ട് സ്കാമുകാർ ഇമെയിലുകൾ, ടെക്സ്റ്റുകൾ അല്ലെങ്കിൽ സോഷ്യൽ മീഡിയ വഴി ലിങ്കുകൾ അയയ്ക്കുന്നു (ഉദാ. കിഴിവുകൾ, റിവാർഡുകൾ, അടിയന്തര അപ്ഡേറ്റുകൾ). ലിങ്കിൽ ക്ലിക്ക് ചെയ്യുന്നത് നിങ്ങളെ നിയമാനുസൃതമെന്ന് തോന്നുമെങ്കിലും നിങ്ങളുടെ വിവരങ്ങൾ മോഷ്ടിക്കാൻ രൂപകൽപ്പന ചെയ്തിരിക്കുന്ന ഒരു വ്യാജ വെബ്സൈറ്റിലേക്ക് നയിക്കും.

ഫ്രോഡായിട്ടുള്ള ക്യുആർ കോഡുകൾ: സ്കാമുകാർ ഫിഷിംഗ് വെബ്സൈറ്റുകളിലേക്ക് നയിക്കുന്നതോ ദോഷകരമായ പ്രവർത്തനങ്ങൾക്ക് കാരണമാകുന്നതോ ആയ ക്യുആർ കോഡുകൾ സൃഷ്ടിക്കുന്നു (ഉദാ. മാൽവെയർ ഇൻസ്റ്റാൾ ചെയ്യുന്നത്). ഈ കോഡുകൾ ഡിജിറ്റലായി അയയ്ക്കുകയോ ഫിസിക്കൽ പോസ്റ്ററുകളിലോ പരസ്യങ്ങളിലോ സ്ഥാപിക്കുകയോ ചെയ്തേക്കാം.

ചിലപ്പോൾ സ്കാമുകാർ ഒരു നിയമാനുസൃത പരസ്യം എടുത്ത് ക്യുആർ കോഡിന് പകരം ഒരു വ്യാജ പരസ്യം ഉണ്ടാക്കി, അത് ആളുകളെ തങ്ങൾ നിയമാനുസൃതമാണെന്ന് തെറ്റിദ്ധരിപ്പിക്കും.

വ്യാജ ലിങ്ക് / ക്യുആർ കോഡ് സ്കാമിന്റെ ഉദാഹരണങ്ങൾ

- നിങ്ങളുടെ പാക്കേജ് ഡെലിവറി വൈകിയതായി ഒരു ടെക്സ്റ്റ് സന്ദേശം പറയുന്നു; ലിങ്ക് പേയ്മെന്റ് വിശദാംശങ്ങൾ ആവശ്യപ്പെടുന്നു.
- സ്കാമുകാർ ബാങ്കുകൾ പോലുള്ള നിയമാനുസൃത സ്ഥാപനങ്ങളുടെ സൈറ്റുകളെ അനുകരിക്കുകയും നിങ്ങളുടെ KYC വിശദാംശങ്ങൾ അപ്ഡേറ്റ് ചെയ്യാൻ ആവശ്യപ്പെടുകയും ചെയ്യുന്നു.
- നിങ്ങളുടെ ക്രെഡിറ്റ് കാർഡിലോ UPI പിൻകളിലോ പൂരിപ്പിക്കുന്നതിന് നിങ്ങളെ കബളിപ്പിക്കാൻ സ്കാമുകാർക്ക് വ്യാജ പേയ്മെന്റ് ലിങ്കുകളോ ക്യുആർ കോഡുകളോ പ്രചരിപ്പിക്കാൻ കഴിയും.
- ഒരു പോസ്റ്ററിലെ ഒരു ക്യൂആർ കോഡ് ഒരു കിഴിവ് വാഗ്ദാനം ചെയ്യുന്നു, പക്ഷേ അത് ഒരു ഫിഷിംഗ് സൈറ്റിലേക്ക് നയിക്കുന്നു

- അപ്രതീക്ഷിതമായ ഒരു സ്ഥലത്ത് നിങ്ങൾ ഒരു QR കോഡ് കണ്ടാൽ, അത് തുറക്കുന്നതിന് മുമ്പ് URL പരിശോധിക്കുക. നിങ്ങൾക്ക് തിരിച്ചറിയാൻ കഴിയുന്ന ഒരു URL പോലെ തോന്നുകയാണെങ്കിൽ, അത് വ്യാജമല്ലെന്ന് ഉറപ്പാക്കുക - അക്ഷരത്തെറ്റുകൾ ഉണ്ടോ അല്ലെങ്കിൽ മാറ്റിയ അക്ഷരമോ ഉണ്ടോ എന്ന് നോക്കുക.

- നിങ്ങൾ പ്രതീക്ഷിക്കാത്ത ഒരു ഇമെയിലിലോ ടെക്സ്റ്റ് സന്ദേശത്തിലോ ഉള്ള QR കോഡ് സ്കാൻ ചെയ്യരുത് - പ്രത്യേകിച്ച് അത് ഉടനടി നടപടിയെടുക്കാൻ നിങ്ങളെ പ്രേരിപ്പിക്കുന്നുണ്ടെങ്കിൽ. സന്ദേശം നിയമാനുസൃതമാണെന്ന് നിങ്ങൾ കരുതുന്നുവെങ്കിൽ, കമ്പനിയുമായി ബന്ധപ്പെടാൻ നിങ്ങൾക്ക് യഥാർത്ഥമാണെന്ന് അറിയാവുന്ന ഒരു ഫോൺ നമ്പറോ വെബ്സൈറ്റോ ഉപയോഗിക്കുക.

- അജ്ഞാത ഉറവിടങ്ങളിൽ നിന്നുള്ള പേയ്മെന്റ് ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യരുത്.

- QR കോഡ് പേയ്മെന്റുകൾ നടത്തുമ്പോൾ എല്ലായ്പ്പോഴും ഉദ്ദേശിക്കുന്ന സ്വീകർത്താവിന്റെ പേര് പരിശോധിക്കുക.

- നിങ്ങളുടെ KYC ആവശ്യപ്പെടുമ്പോൾ, KYC യുടെ ഉദ്ദേശ്യവും അത്തരം വിവരങ്ങൾ അഭ്യർത്ഥിക്കുന്ന വ്യക്തിയുടെ ഐഡന്റിറ്റിയും പരിശോധിക്കുക

സ്കാം # 7 വ്യാജ വായ്പാ ആപ്പ് സ്കാം

അത് എന്താണ്

കുറഞ്ഞ രേഖകൾ ഉപയോഗിച്ച് വേഗത്തിലും എളുപ്പത്തിലും വായ്പകൾ വാഗ്ദാനം ചെയ്യുന്ന ഫ്രോഡായിട്ടുള്ള ആപ്പുകൾ സൃഷ്ടിക്കുന്നതാണ് വ്യാജ ലോൺ ആപ്പ് സ്കാം. പണം അത്യാവശ്യമുള്ള വ്യക്തികളെ ഈ ആപ്പുകൾ പലപ്പോഴും ലക്ഷ്യം വയ്ക്കുന്നു, അവരെ കബളിപ്പിച്ച് ഫീസ് അടയ്ക്കുകയോ വ്യക്തിഗത വിവരങ്ങൾ പങ്കിടുകയോ ചെയ്യുന്നു. പലപ്പോഴും അവയ്ക്ക് മറഞ്ഞിരിക്കുന്ന നിരക്കുകളും വളരെ ഉയർന്ന പലിശ നിരക്കുകളും ഉണ്ട്.

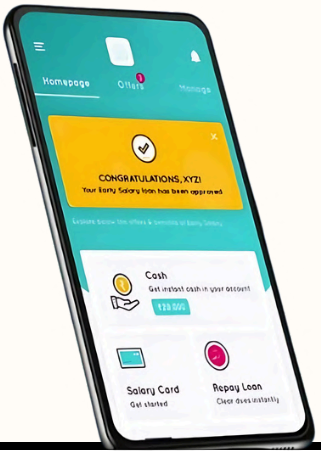
ഇത് എങ്ങനെ പ്രവർത്തിക്കുന്നു

ആകർഷകമായ ഓഫറുകൾ: ക്രെഡിറ്റ് പരിശോധനകളോ തൽക്ഷണ അംഗീകാരമോ വളരെ കുറഞ്ഞ പലിശ നിരക്കുകളോ ഇല്ലാതെ വായ്പകൾ പരസ്യപ്പെടുത്തുന്നതിലൂടെ, ആപ്പ് നിങ്ങളെ അവരുടെ സേവനങ്ങൾ ഉപയോഗിക്കാൻ പ്രേരിപ്പിക്കുന്നു. സ്കാമു കാർ പലപ്പോഴും ബാങ്കുകൾ പോലുള്ള പ്രശസ്ത ധനകാര്യ സ്ഥാപനങ്ങളുടെ പേരുകൾക്ക് സമാനമായ പേരുകൾ തിരഞ്ഞെടുക്കുന്നു, അവ നിയമാനുസൃതമാണെന്ന് നിങ്ങളെ കബളിപ്പിക്കാൻ.

മുൻകൂർ ഫീസ്: നിങ്ങൾ അപേക്ഷിച്ചുകഴിഞ്ഞാൽ, വായ്പ വിതരണം ചെയ്യുന്നതിന് മുമ്പ് ആപ്പ് പ്രോസസ്സിംഗ് ഫീസ്, സേവന നിരക്കുകൾ അല്ലെങ്കിൽ മറ്റ് പേയ്മെന്റുകൾ ആവശ്യപ്പെടുന്നു.

ഡാറ്റ മോഷണവും മാൽവെയർ ആക്രമണങ്ങളും: നിങ്ങളുടെ ബാങ്ക് അക്കൗണ്ട് നമ്പർ, ഐഡി പ്രൂഫ്, ഫോൺ കോൺടാക്റ്റുകൾ എന്നിവ പോലുള്ള സെൻസിറ്റീവ് വ്യക്തിഗത വിവരങ്ങൾ ആപ്പ് ശേഖരിക്കുന്നു. ചിലപ്പോൾ ഈ ആപ്പുകളിൽ മാൽവെയർ ഇൻസ്റ്റാൾ ചെയ്തിട്ടുണ്ടാകും, അത് നിങ്ങൾ ആപ്പ് ഡൗൺലോഡ് ചെയ്തതിന് ശേഷം നിങ്ങളുടെ ഫോണിലേക്ക് ലോഡ് ചെയ്യപ്പെടും.

ഉപദ്രവം: നിങ്ങൾ പണമടയ്ക്കുന്നതിൽ പരാജയപ്പെട്ടാൽ, സ്കാമുകാർ മോഷ്ടിച്ച ഡാറ്റ ഉപയോഗിച്ച് നിങ്ങളെയോ നിങ്ങളുടെ കുടുംബത്തെയോ കോൺടാക്റ്റുകളെയോ ഭീഷണിപ്പെടുത്തുകയോ പൊതു അപമാനം വരുത്തുകയോ ചെയ്യും. ഉദാഹരണത്തിന്, വീഡിയോ-കെവൈസി നടത്തുക എന്ന വ്യാജേന അവർ നിങ്ങളുടെ ഫോട്ടോകൾ ആക്സസ് ചെയ്യുകയും അവർ കണ്ടെത്തുന്നതിന്റെ അടിസ്ഥാനത്തിൽ നിങ്ങളെ ബ്ലാക്ക്മെയിൽ ചെയ്യുകയും ചെയ്തേക്കാം.



വായ്പ വിതരണം ചെയ്തിട്ടില്ല: പലപ്പോഴും, ഫീസ്അടച്ചതിനുശേഷവും വായ്പ നൽകില്ല, ആപ്പ്അപ്രത്യക്ഷമാകുകയോ പ്രതികരിക്കുന്നത് നിർത്തുകയോ ചെയ്യും.

- **ഉറവിടം പരിശോധിക്കുക**: ലോൺ ആപ്പുകൾ ഒരിക്കലും സ്വയം വായ്പകൾ നൽകില്ല; പകരം അവർ ആർ.ബി.ഐ. നിയന്ത്രിത ബാങ്കുകളുമായോ ബാങ്ക് ഇതര ധനകാര്യ കമ്പനികളുമായോ (NBFC) പങ്കാളിത്തം വഹിക്കുന്നു.

  അത്തരമൊരു പങ്കാളിത്തം അവകാശപ്പെടുന്ന ലോൺ ആപ്പുമായി അവർ യഥാർത്ഥത്തിൽ പങ്കാളിത്തം വഹിച്ചിട്ടുണ്ടോ എന്ന് കാണാൻ ബാങ്കുകളുടെയും എൻ.ബി.എഫ്.സി.-കളുടെയും വെബ്സൈറ്റുകൾ പരിശോധിക്കുക. വെബ്സൈറ്റിൽ നിങ്ങൾക്ക് ഒന്നും കണ്ടെത്താൻ കഴിയുന്നില്ലെങ്കിൽ, കൂടുതൽ പരിശോധിക്കാൻ ബാങ്കിന്റെ/ എൻ.ബി.എഫ്.സി.-യുടെ ഉപഭോക്തൃ സേവന നമ്പറിൽ വിളിക്കുക.

- **അനുമതികളിൽ ജാഗ്രത പാലിക്കുക**: കോൺടാക്റ്റുകളിലേക്കോ ഫോട്ടോകളിലേക്കോ സന്ദേശങ്ങളിലേക്കോ അനാവശ്യമായ ആക്സസ് ആവശ്യപ്പെടുന്ന ആപ്പുകൾ ഒഴിവാക്കുക.

- **വിശ്വസനീയ ഉറവിടങ്ങൾ ഉപയോഗിക്കുക**: ആപ്പ് ഉപയോഗിക്കുന്നതിന് മുമ്പ് അതിന്റെ നിയമസാധുതയും അവലോകനങ്ങളും പരിശോധിക്കുക. ഒന്നിലധികം ഉറവിടങ്ങളിൽ നിന്നുള്ള അവലോകനങ്ങൾ പരിശോധിക്കുന്നത് ഉറപ്പാക്കുക. നേരത്തെ സൂചിപ്പിച്ചതുപോലെ, സ്കാമുകാർ പലപ്പോഴും നിയമാനുസൃതമാണെന്ന് തോന്നിപ്പിക്കാൻ വ്യാജ അവലോകനങ്ങൾ പുറപ്പെടുവിക്കുന്നു.

- **മുൻകൂർ ഫീസ്**: നിയമാനുസൃത വായ്പാദാതാക്കൾ സാധാരണയായി മുൻകൂർ ഫീസ് ആവശ്യപ്പെടാറില്ല. വായ്പ നൽകുന്നതിന് മുമ്പ് പേയ്മെന്റ് ആവശ്യപ്പെടുന്ന വായ്പാദാതാക്കളെ ഒഴിവാക്കുക.

- **റെഡ് ഫ്ലാഗ്സ്**: തൽക്ഷണ വായ്പാ ഓഫറുകളെക്കുറിച്ച് ജാഗ്രത പാലിക്കുക, പ്രത്യേകിച്ച് ക്രെഡിറ്റ് പരിശോധനകളില്ലാതെ ഉറപ്പുള്ള അംഗീകാരം വാഗ്ദാനം ചെയ്യുന്നവർ.

- **പലിശ നിരക്കുകൾ**: പലിശ നിരക്കുകളും നിബന്ധനകളും ശ്രദ്ധാപൂർവ്വം പരിശോധിക്കുക. അവ വളരെ നല്ലതായി തോന്നുന്നുണ്ടെങ്കിൽ, അവ ഒരുപക്ഷേ അങ്ങനെയായിരിക്കാം.

- **ബന്ധപ്പെടാനുള്ള വിവരങ്ങൾ**: വായ്പ നൽകുന്നയാളുടെ ബന്ധപ്പെടാനുള്ള വിവരങ്ങളും ഭൗതിക വിലാസവും സ്ഥിരീകരിക്കുക. സ്കാമുകാർ പലപ്പോഴും വ്യാജ വിവരങ്ങൾ ഉപയോഗിക്കുന്നു.

- **സംശയിക്കപ്പെടുന്ന സ്കാം റിപ്പോർട്ട് ചെയ്യുക**: നിങ്ങൾ ഒരു സൈബർ വായ്പാ ദാതാവിനെ കണ്ടുമുട്ടുകയോ നിങ്ങൾ വഞ്ചിക്കപ്പെട്ടുവെന്ന് വിശ്വസിക്കുകയോ ചെയ്താൽ, ഉചിതമായ അധികാരികളെ ഉടൻ അറിയിക്കുക.

സ്കാം # 8 വ്യാജ മൊബൈൽ റീചാർജ് സ്കാം

അത് എന്താണ്

വ്യാജ മൊബൈൽ റീചാർജ് സ്കാമിലൂടെ നിങ്ങളെ വ്യാജ ഫോൺ റീചാർജുകൾക്കോ ഓഫറുകൾക്കോ പണം നൽകേണ്ടിവരുന്നു. ഡിസ്കൗണ്ടുകൾ, ക്യാഷ്ബാക്ക് അല്ലെങ്കിൽ സൗജന്യ റീചാർജുകൾ എന്നിവ നൽകുമെന്ന് അവകാശപ്പെടുന്ന വ്യാജ വെബ്സൈറ്റുകൾ, ആപ്പുകൾ അല്ലെങ്കിൽ സന്ദേശങ്ങൾ ഉപയോഗിച്ചാണ് സ്കാമുകാർ സ്കാം നടത്തുന്നത്..

ഇത് എങ്ങനെ പ്രവർത്തിക്കുന്നു

വ്യാജ ഓഫറുകൾ: സന്ദേശങ്ങൾ, സോഷ്യൽ മീഡിയ, അല്ലെങ്കിൽ വ്യാജ ആപ്പുകൾ എന്നിവയിലൂടെ വമ്പൻ കിഴിവുകൾ അല്ലെങ്കിൽ "സൗജന്യ റീചാർജുകൾ" പോലുള്ള അയഥാർത്ഥ ഡീലുകൾ സ്കാമുകാർ പരസ്യപ്പെടുത്തുന്നു. ചിലപ്പോൾ സ്കാമുകാർ **ട്രായ്**-യിൽ നിന്നുള്ള ഉദ്യോഗസ്ഥരായി നടിക്കുകയും നിങ്ങളെ വിശ്വസിപ്പിക്കുകയും ചെയ്യുന്നു..

റീചാർജിനായി പണമടയ്ക്കൽ: വ്യാജ പ്ലാറ്റ്ഫോം വഴിയാണ് ഇര റീചാർജിനായി പണം നൽകുന്നത്, പക്ഷേ യഥാർത്ഥത്തിൽ ഒരു റീചാർജും നടക്കുന്നില്ല..

വിവരങ്ങൾ മോഷ്ടിക്കൽ: വ്യാജ റീചാർജ് പ്ലാറ്റ്ഫോമുകൾ പലപ്പോഴും വ്യക്തിഗത വിശദാംശങ്ങൾ, പേയ്മെന്റ് വിവരങ്ങൾ, അല്ലെങ്കിൽ ബാങ്ക് വിശദാംശങ്ങൾ/ക്രെഡിറ്റ് കാർഡ് വിവരങ്ങൾ എന്നിവ പ്രോസസ്സിനിടെ ശേഖരിക്കുന്നു.

ഫിഷിംഗ് ലിങ്കുകൾ: സ്കാമുകാർ എസ്എംഎസ് അല്ലെങ്കിൽ ഇമെയിൽ വഴി ലിങ്കുകൾ അയയ്ക്കുന്നു, നിയമാനുസൃതമായ ടെലികോം റീചാർജ് സേവനങ്ങളെ അനുകരിക്കുന്ന വ്യാജ വെബ്സൈറ്റുകളിലേക്ക് നിങ്ങളെ റീഡയറക്ട് ചെയ്യുന്നു

- **വിശ്വസനീയ പ്ലാറ്റ്ഫോമുകൾ ഉപയോഗിക്കുക**: നിങ്ങളുടെ മൊബൈൽ ദാതാവിന്റെ ആപ്പ് വഴിയോ അല്ലെങ്കിൽ നിങ്ങളുടെ യു.പി.ഐ.-യുമായി ലിങ്ക് ചെയ്തിരിക്കുന്ന ആപ്പ് വഴിയോ മാത്രം റീചാർജ് ചെയ്യുക..
- **അപ്രായോഗികമായ ഓഫറുകൾ സൂക്ഷിക്കുക**: വമ്പിച്ച കിഴിവുകൾ അല്ലെങ്കിൽ സൗജന്യ റീചാർജുകൾ പോലുള്ള സത്യമാണെന്ന് തോന്നുന്ന ഡീലുകൾ അവഗണിക്കുക..
- **വെബ്സൈറ്റുകളും ആപ്പുകളും പരിശോധിക്കുക**: വ്യാജമായതോ അക്ഷരത്തെറ്റുള്ളതോ ആയ പേരുകൾക്കായി യു.ആർ.എൽ. പരിശോധിക്കുക, ഔദ്യോഗിക ആപ്പ് സ്റ്റോറുകളിൽ നിന്ന് മാത്രം ആപ്പുകൾ ഡൗൺലോഡ് ചെയ്യുക.
- **സ്ഥിരീകരിക്കാത്ത ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യരുത്**: അജ്ഞാത ഉറവിടങ്ങളിൽ നിന്ന് എസ്.എം.എസ്., വാട്ട്സ്ആപ്പ് അല്ലെങ്കിൽ ഇമെയിൽ വഴി അയയ്ക്കുന്ന റീചാർജ് ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യുന്നത് ഒഴിവാക്കുക.

- **സുരക്ഷിത പേയ്മെന്റ് വിശദാംശങ്ങൾ**: പരിശോധിച്ചുറപ്പിക്കാത്ത തേർഡ് പാർട്ടി പ്ലാറ്റ്ഫോമുകളുമായി നിങ്ങളുടെ പേയ്മെന്റ് വിവരങ്ങൾ ഒരിക്കലും പങ്കിടരുത്..

- **സംശയാസ്പദമായ പ്രവർത്തനം റിപ്പോർട്ട് ചെയ്യുക**: ഒരു സ്കാം നേരിടുകയാണെങ്കിൽ നിങ്ങളുടെ ടെലികോം ദാതാവിനെയോ പ്രാദേശിക സൈബർ ക്രൈം ഹെൽപ്പ്ലൈനിനെയോ അറിയിക്കുക..

സ്കാം # 9 പാഴ്സൽ ഡെലിവറി സ്കാം

അത് എന്താണ്

ഒരു പാഴ്സൽ ഡെലിവറി സ്കാം നിങ്ങളെ ഒരു പാക്കേജ് ഡെലിവറിക്കായി കാത്തിരിക്കുന്നുണ്ടെന്ന് തെറ്റിദ്ധരിപ്പിക്കുന്നു. പാക്കേജ് പുറത്തിറക്കുന്നതിന് പണമടയ്ക്കൽ അല്ലെങ്കിൽ വ്യക്തിഗത വിവരങ്ങൾ ആവശ്യപ്പെട്ട് സ്കാമു കാർ വ്യാജ സന്ദേശങ്ങളോ ഇമെയിലുകളോ അയയ്ക്കുന്നു..

ഇത് എങ്ങനെ പ്രവർത്തിക്കുന്നു

വ്യാജ അറിയിപ്പുകൾ: വിലാസ വിവരങ്ങൾ അപൂർണ്ണമായതിനാലോ കുടിശ്ശിക അടച്ചതിനാലോ നിങ്ങൾക്ക് ഒരു പാക്കേജ് എത്തിച്ചേർന്നിട്ടുണ്ടെങ്കിലും അത് ഡെലിവറി ചെയ്യാൻ കഴിയുന്നില്ലെന്ന് അവകാശപ്പെടുന്ന ഒരു ടെക്സ്റ്റ്, ഇമെയിൽ അല്ലെങ്കിൽ കോൾ നിങ്ങൾക്ക് ലഭിക്കും. ഇത് ഫെഡെക്സ്, ഡി.എച്.എൽ, ഇന്ത്യ പോസ്റ്റ് പോലുള്ള ഒരു വിശ്വസനീയ കൊറിയർ കമ്പനിയിൽ നിന്നുള്ളതാണെന്ന് തോന്നാം.

ഫിഷിംഗ് ലിങ്കുകൾ: നിങ്ങളുടെ വിലാസം അപ്ഡേറ്റ് ചെയ്യുന്നതിനുള്ള ഒരു ലിങ്ക് സന്ദേശത്തിൽ ഉൾപ്പെടുന്നു, സാധാരണയായി സമയബന്ധിതമായി, 12 മണിക്കൂറിനുള്ളിൽ. സന്ദേശത്തിൽ "ഡെലിവറി സ്ഥിരീകരിക്കുക" അല്ലെങ്കിൽ ഫീസ് അടയ്ക്കുന്നതിനുള്ള ഒരു ലിങ്കും ഉൾപ്പെടുത്താം. ലിങ്കിൽ ക്ലിക്കുചെയ്യുന്നത് നിങ്ങളെ ഒരു വ്യാജ വെബ്സൈറ്റിലേക്ക് കൊണ്ടുപോകുന്നു, അവിടെ സ്കാമുകാർ നിങ്ങളുടെ പേയ്മെന്റോ വ്യക്തിഗത വിശദാംശങ്ങളോ മോഷ്ടിക്കുന്നു.

ഫോളോ അപ്പ് കോൾ: സാധാരണയായി, കൊറിയർ കമ്പനിയുടെ പ്രതിനിധിയായി വേഷമിടുന്ന ഒരാളിൽ നിന്നുള്ള ഒരു ഫോൺ കോളിനൊപ്പം ഒരു എസ്.എം.എസ്. അല്ലെങ്കിൽ ഇമെയിൽ ലഭിക്കും. നിങ്ങളുടെ വിലാസം അപൂർണ്ണമായതിനാലോ എന്തെങ്കിലും പണമടയ്ക്കൽ അവസാനിച്ചതിനാലോ നിങ്ങളുടെ പാഴ്സൽ ഡെലിവറി ചെയ്യാൻ കഴിയില്ലെന്ന് അവർ ആവർത്തിക്കുകയും നൽകിയിരിക്കുന്ന ലിങ്കിലെ ഔപചാരികതകൾ പൂർത്തിയാക്കാൻ നിങ്ങളെ പ്രേരിപ്പിക്കുകയും ചെയ്യും.

അടിയന്തരാവസ്ഥയും സമ്മർദ്ദവും: വിലാസം അപ്ഡേറ്റ് ചെയ്തില്ലെങ്കിലോ പണമടച്ചില്ലെങ്കിലോ ഓർഡർ റദ്ദാക്കുകയോ പാഴ്സൽ നശിപ്പിക്കുകയോ ചെയ്യുമെന്ന് ഭീഷണിപ്പെടുത്തി വിളിക്കുന്നയാൾ ഇരയുടെ മേൽ സമ്മർദ്ദം ചെലുത്തുന്നു.

പേയ്മെന്റ് ട്രാപ്പ്: റീ-ഡെലിവറിക്ക് നിങ്ങളോട് ഒരു ചെറിയ ഫീസ് അടയ്ക്കാൻ ആവശ്യപ്പെടുന്നു. പേജ് ഡെബിറ്റ് അല്ലെങ്കിൽ ക്രെഡിറ്റ് കാർഡ് പേയ്മെന്റുകൾ മാത്രമേ സ്വീകരിക്കുന്നുള്ളൂ, യു.പി.ഐ. അല്ലെങ്കിൽ ക്യാഷ് ഓൺ ഡെലിവറി എന്നിവയ്ക്കുള്ള ഓപ്ഷനുകളൊന്നുമില്ല.

ഡെലിവറി ഇല്ല: നിങ്ങൾ പണമടച്ചുകഴിഞ്ഞാൽ അല്ലെങ്കിൽ വിശദാംശങ്ങൾ നൽകിക്കഴിഞ്ഞാൽ, സ്കാമർമാർക്ക് അപ്രത്യക്ഷമാകും, നിങ്ങൾക്ക് പാക്കേജും മോഷ്ടിക്കപ്പെട്ട വിവരങ്ങളും ലഭിക്കില്ല.

- **നിങ്ങൾ ഒരു ഓർഡർ നൽകിയിട്ടുണ്ടോ എന്ന് ഓർക്കുക**: നിങ്ങളുടെ കൈവശം ഒരു പാക്കേജ് വന്നിട്ടുണ്ടോ അതോ നിങ്ങൾ ഓർഡർ ചെയ്തിട്ട് അത് ഇതുവരെ ഡെലിവറി ചെയ്തിട്ടില്ലേ എന്ന് ഓർമ്മിക്കാൻ ശ്രമിക്കുക.

- **സന്ദേശം പരിശോധിക്കുക**: ഡെലിവറി സ്ഥിരീകരിക്കുന്നതിന് കൊറിയർ കമ്പനിയെ അവരുടെ ഔദ്യോഗിക വെബ്സൈറ്റ് അല്ലെങ്കിൽ ഫോൺ നമ്പർ വഴി നേരിട്ട് ബന്ധപ്പെടുക.

- **അജ്ഞാത ലിങ്കുകളിൽ ക്ലിക്കുചെയ്യുന്നത് ഒഴിവാക്കുക**: ഒരു പാഴ്സലിനെക്കുറിച്ചാണെന്ന് അവകാശപ്പെടുന്ന സന്ദേശങ്ങളിലെ ലിങ്കുകളിൽ ക്ലിക്കുചെയ്യരുത്, പ്രത്യേകിച്ച് അജ്ഞാതരായ അയച്ചവരിൽ നിന്ന്.

- **റെഡ് ഫ്ലാഗ്കൾക്കായി തിരയുക**: മോശം വ്യാകരണം, പൊതുവായ ആശംസകൾ അല്ലെങ്കിൽ സംശയാസ്പദമായ ഇമെയിൽ വിലാസങ്ങൾ എന്നിവയെക്കുറിച്ച് ജാഗ്രത പാലിക്കുക.

- **നിങ്ങളുടെ വിവരങ്ങൾ സുരക്ഷിതമാക്കുക**: ഉറവിടം നിയമാനുസൃതമാണെന്ന് നിങ്ങൾക്ക് ഉറപ്പില്ലെങ്കിൽ വ്യക്തിഗത അല്ലെങ്കിൽ പേയ്മെന്റ് വിവരങ്ങൾ ഒരിക്കലും പങ്കിടരുത്.

സ്കാം # 10 കൃത്രിമ മാൽവെയർ സ്കാം

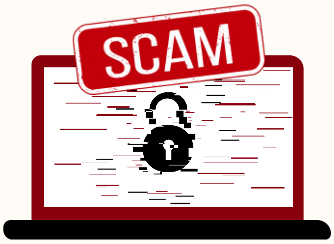
അത് എന്താണ്

മാൽവെയർ പ്രചരിപ്പിക്കുന്നതിനോ വ്യക്തിഗത വിവരങ്ങൾ മോഷ്ടിക്കുന്നതിനോ രൂപകൽപ്പന ചെയ്തിരിക്കുന്ന ഒരു ദോഷകരമായ ലിങ്കിൽ ക്ലിക്കുചെയ്യാൻ ഒരു കൃത്രിമ മാൽവെയർ സ്കാം നിങ്ങളെ പ്രേരിപ്പിക്കുന്നു. ഈ ലിങ്കുകൾ പലപ്പോഴും നിയമാനുസൃതമായി കാണപ്പെടും, പക്ഷേ അവയിൽ ക്ലിക്കുചെയ്യുന്നത് നിങ്ങളുടെ ഉപകരണത്തെ ബാധിക്കുകയോ ദോഷകരമായ സൈറ്റുകളിലേക്ക് നിങ്ങളെ നയിക്കുകയോ ചെയ്യും.

ഇത് എങ്ങനെ പ്രവർത്തിക്കുന്നു

വെബ്സൈറ്റുകളിലെ പ്ലേസ്മെന്റ്: വെബ്സൈറ്റുകളിലെ പരസ്യങ്ങൾ പോലുള്ള വിവിധ മാർഗങ്ങളിലൂടെയാണ് സ്കാമുകാർ ഈ ലിങ്കുകൾ സ്ഥാപിക്കുന്നത്.

ക്ലിക്ക് ചെയ്ത് മാൽവെയർ വരുത്തുക: ലിങ്കിൽ ക്ലിക്ക് ചെയ്യുമ്പോൾ, ഇത് സംഭവിക്കാം:
നിങ്ങളുടെ ഉപകരണത്തിൽ മാൽവെയർ ഇൻസ്റ്റാൾ ചെയ്യുക,
ഫിഷിംഗ് വെബ്സൈറ്റുകളിലേക്ക് നിങ്ങളെ
റീഡയറക്ട് ചെയ്യുക, അല്ലെങ്കിൽ
വ്യാജ സോഫ്റ്റ്വെയറോ അപ്ഡേറ്റുകളോ ഡൗൺലോഡ് ചെയ്യാൻ നിങ്ങളെ കബളിപ്പിക്കുക.



ഇടപെടൽ ആവശ്യമില്ല: ചില ദോഷകരമായ ലിങ്കുകൾക്ക് ഒരു ക്ലിക്ക് പോലും ആവശ്യമില്ല - ചില വെബ്സൈറ്റുകളിൽ (ക്ഷുദ്ര കോഡ് വഴി) പ്രദർശിപ്പിക്കുന്നതിലൂടെ അവ നിങ്ങളുടെ ഉപകരണത്തെ ബാധിച്ചേക്കാം.

- **സംശയാസ്പദമായ ലിങ്കുകൾ ഒഴിവാക്കുക**: അവിശ്വസനീയമായ ഡീലുകൾ, സൗജന്യ സോഫ്റ്റ്വെയർ അല്ലെങ്കിൽ അടിയന്തര മുന്നറിയിപ്പുകൾ എന്നിവ വാഗ്ദാനം ചെയ്യുന്ന ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യരുത്.
- **സോഫ്റ്റ്വെയർ അപ്ഡേറ്റ് ചെയ്ത് സൂക്ഷിക്കുക**: ക്ഷുദ്രകരമായ പരസ്യങ്ങൾ തടയുന്നതിന് നിങ്ങളുടെ ബ്രൗസറും സുരക്ഷാ സോഫ്റ്റ്വെയറും കാലികമാണെന്ന് ഉറപ്പാക്കുക.
- **സുരക്ഷാ സവിശേഷതകൾ പ്രവർത്തനക്ഷമമാക്കുക**: ഭീഷണികൾ കണ്ടെത്തി തടയുന്നതിന് ആന്റിവൈറസ് സോഫ്റ്റ്വെയറും ബ്രൗസർ സുരക്ഷാ ക്രമീകരണങ്ങളും ഉപയോഗിക്കുക. ചില ആന്റിവൈറസ് സോഫ്റ്റ്വെയറുകൾ മാൽവെയർ പരിരക്ഷയോടെയാണ് വരുന്നത്, നിങ്ങൾ അശ്രദ്ധമായി ഒരു റോഗ് വെബ്സൈറ്റിലേക്ക് പോയാൽ ഭീഷണികളെ തടയുന്നു. അത്തരം സവിശേഷതകളുള്ള ഒരു ആന്റിവൈറസ് സോഫ്റ്റ്വെയർ നിങ്ങൾക്ക് ലഭിക്കുന്നുണ്ടെന്ന് ഉറപ്പാക്കുക. കൂടാതെ, നിങ്ങളുടെ ബ്രൗസറിലെ റിസ്ക് മോണിറ്ററിംഗ് ക്രമീകരണങ്ങൾ ഓണാക്കിയിട്ടുണ്ടെന്ന് ഉറപ്പാക്കുക.

സംശയാസ്പദമായ കോളുകളോ സ്കാമുകളോ **സൈബർ ക്രൈം ഹെൽപ്പ്ലൈൻ നമ്പറായ 1930** യിൽ അറിയിക്കുക. അല്ലെങ്കിൽ www.cybercrime.gov.in എന്ന വെബ്സൈറ്റിൽ അറിയിക്കുക.

വിശ്വസനീയ വെബ്സൈറ്റുകളിൽ ഉറച്ചുനിൽക്കുക: സംശയാസ്പദമായതോ സ്ഥിരീകരിക്കാത്തതോ ആയ വെബ്സൈറ്റുകൾ സന്ദർശിക്കുന്നതോ അവയുമായി ഇടപഴകുന്നതോ ഒഴിവാക്കുക. ദോഷകരമായ ഉള്ളടക്കം, മാൽവെയർ അല്ലെങ്കിൽ സുരക്ഷാ സർട്ടിഫിക്കറ്റുകൾ ഇല്ലാത്ത വെബ്സൈറ്റുകൾ തുറക്കുന്നതിന് മുമ്പ് നിങ്ങൾക്ക് മുന്നറിയിപ്പ് നൽകുന്ന വിശ്വസനീയവും അറിയപ്പെടുന്നതുമായ വെബ് ബ്രൗസറുകൾ ഉപയോഗിക്കുക.

സ്കാം # 11 ടെക് സപ്പോർട്ട് സ്കാം

അത് എന്താണ്

നിങ്ങളുടെ കമ്പ്യൂട്ടറിലോ ഉപകരണത്തിലോ ഒരു പ്രശ്നമുണ്ടെന്ന് വിശ്വസിപ്പിക്കാൻ ഒരു ടെക് സപ്പോർട്ട് സ്കാം നിങ്ങളെ കബളിപ്പിക്കുന്നു. സ്കാമർമാർ മൈക്രോസോഫ്റ്റ്, ആപ്പിൾ പോലുള്ള നിയമാനുസൃത കമ്പനികളിൽ നിന്നുള്ളവരായി നടിച്ച്, നിലവിലില്ലാത്ത പ്രശ്നങ്ങൾ പരിഹരിക്കുന്നതിന് വ്യാജ "പിന്തുണ" വാഗ്ദാനം ചെയ്യുന്നു, പലപ്പോഴും പണമോ വ്യക്തിഗത വിവരങ്ങളോ മോഷ്ടിക്കുന്നു.

ഇത് എങ്ങനെ പ്രവർത്തിക്കുന്നു

വ്യാജ മുന്നറിയിപ്പ് സന്ദേശങ്ങൾ: നിങ്ങളുടെ കമ്പ്യൂട്ടറിലോ ഫോണിലോ വൈറസ് ബാധിച്ചിട്ടുണ്ടെന്നോ ഗുരുതരമായ പിശകുണ്ടെന്നോ അവകാശപ്പെടുന്ന ഒരു പോപ്പ്-അപ്പ് നിങ്ങൾ കാണുന്നു. അതിൽ പലപ്പോഴും ഒരു വ്യാജ ഉപഭോക്തൃ പിന്തുണ നമ്പർ ഉൾപ്പെടുന്നു.

സ്പാം കോളുകൾ: നിങ്ങളുടെ ഉപകരണത്തിൽ പ്രശ്നങ്ങൾ കണ്ടെത്തിയെന്ന് അവകാശപ്പെട്ട്, സാങ്കേതിക പിന്തുണയായി നടിച്ച് സ്കാമുകാർ വിളിക്കുന്നു.

സ്ക്രീൻ മിററിംഗ് സോഫ്റ്റ്‌വെയർ: നിങ്ങളുടെ കമ്പ്യൂട്ടറിലെ ഒരു പിശക് പരിഹരിക്കാനെന്ന വ്യാജേന റിമോട്ട് ഡെസ്ക്ടോപ്പ് സോഫ്റ്റ്‌വെയറോ സ്ക്രീൻ-ഷെയറിംഗ് ആപ്പുകളോ ഡൗൺലോഡ് ചെയ്യാൻ സ്കാമുകാർ നിങ്ങളോട് ആവശ്യപ്പെടുന്നു. ഏത് സ്ഥലത്തുനിന്നും നിങ്ങളുടെ ഉപകരണം ആക്സസ് ചെയ്യാൻ അവരെ പ്രാപ്തരാക്കുന്ന ഒരു പിൻ പങ്കിടാൻ അവർ നിങ്ങളോട് ആവശ്യപ്പെടും. തുടർന്ന് സ്കാമുകാർക്ക് നിങ്ങളുടെ ഫയലുകൾ കാണാനും അതിൽ മാറ്റങ്ങൾ വരുത്താനും, ഡാറ്റ കൈമാറാനും, വൈറസുകൾ ഇൻസ്റ്റാൾ ചെയ്യാനും, നിങ്ങളുടെ ഉപകരണത്തിന്റെ നിയന്ത്രണം ഏറ്റെടുക്കാനും കഴിയും.

പേയ്മെന്റ് ആവശ്യങ്ങൾ: പ്രശ്നം പരിഹരിക്കുമെന്ന് അവർ അവകാശപ്പെടുകയും വ്യാജ സേവനങ്ങൾക്ക് പണം ആവശ്യപ്പെടുകയും ചെയ്യുന്നു, പലപ്പോഴും ക്രെഡിറ്റ് കാർഡുകൾ അല്ലെങ്കിൽ ഗിഫ്റ്റ് കാർഡുകൾ വഴി.

ഡാറ്റ മോഷണം: നിങ്ങളുടെ ഉപകരണം ആക്സസ് ചെയ്യുമ്പോൾ, പാസ്‌വേഡുകൾ അല്ലെങ്കിൽ ബാങ്കിംഗ് വിശദാംശങ്ങൾ പോലുള്ള സെൻസിറ്റീവ് വിവരങ്ങൾ അവർ മോഷ്ടിച്ചേക്കാം.

- **അനാവശ്യ കോളുകളെ വിശ്വസിക്കരുത്**: നിങ്ങൾ റിപ്പോർട്ട് ചെയ്യാത്ത പ്രശ്നങ്ങളെക്കുറിച്ച് നിയമാനുസൃത കമ്പനികൾ നിങ്ങളെ വിളിക്കില്ല.

- **പോപ്പ്-അപ്പുകൾ അവഗണിക്കുക**: സംശയാസ്പദമായ പോപ്പ്-അപ്പുകൾ അടയ്ക്കുക, പ്രദർശിപ്പിച്ചിരിക്കുന്ന നമ്പറുകളിലേക്ക് വിളിക്കരുത്. പകരം നിങ്ങളുടെ ഉപകരണം സ്കാൻ ചെയ്യാൻ ആന്റിവൈറസ് സോഫ്റ്റ്‌വെയർ ഉപയോഗിക്കുക.

- **ഒരിക്കലും റിമോട്ട് ആക്സസ് നൽകരുത്**: വിശ്വസനീയവും സ്ഥിരീകരിച്ചതുമായ ഒരു പിന്തുണാ സേവനവുമായി ബന്ധപ്പെടുന്നില്ലെങ്കിൽ ആരെയും നിങ്ങളുടെ ഉപകരണം റിമോട്ട് ആയി നിയന്ത്രിക്കാൻ അനുവദിക്കരുത്.

- **പിന്തുണ ക്ലെയിമുകൾ പരിശോധിക്കുക**: സ്കാമർമാർ നൽകുന്നവയല്ല, മറിച്ച് അവരുടെ വെബ്സൈറ്റിൽ നിന്നുള്ള ഔദ്യോഗിക കോൺടാക്റ്റ് വിശദാംശങ്ങൾ ഉപയോഗിച്ച് കമ്പനിയെ നേരിട്ട് ബന്ധപ്പെടുക.

- **ആന്റിവൈറസ് സോഫ്റ്റ്‌വെയർ ഉപയോഗിക്കുക**: വിശ്വസനീയമായ ആന്റിവൈറസ് സോഫ്റ്റ്‌വെയർ ഉപയോഗിച്ച് നിങ്ങളുടെ ഉപകരണങ്ങൾ അപ്ഡേറ്റ് ചെയ്യുകയും പരിരക്ഷിക്കുകയും ചെയ്യുക.

- **സ്കാം റിപ്പോർട്ട് ചെയ്യുക**: നിങ്ങൾ ഒരു ടെക് സപ്പോർട്ട് സ്കാം നേരിടുന്നുണ്ടെങ്കിൽ, അത് പ്രാദേശിക അധികാരികളോ ആൾമാറാട്ടം നടത്തുന്ന കമ്പനിയോടോ റിപ്പോർട്ട് ചെയ്യുക.

സ്കാം # 12 OTP സ്കാം

അത് എന്താണ്

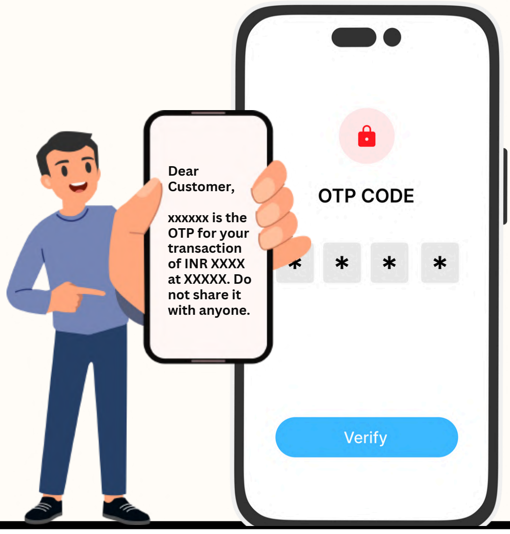
വൺ ടൈം പാസ്‌വേഡ് (ഓ.ടി.പി) സ്കാമി ലൂടെ നിങ്ങളുടെ ഓ.ടി.പി -കൾ സ്കാമുകാർക്ക് വെളിപ്പെടുത്താൻ കഴിയും. ഓൺലൈൻ ഇടപാടുകൾക്കോ വെബ്സൈറ്റുകളിൽ ലോഗിൻ ചെയ്യുന്നതിനോ നിങ്ങളുടെ ഐഡന്റിറ്റി അല്ലെങ്കിൽ അംഗീകാരം പരിശോധിക്കുന്നതിനാണ് ഓ.ടി.പി -കൾ സാധാരണയായി ഉപയോഗിക്കുന്നത്. ഈ കോഡുകൾ സാധാരണയായി എസ്.എം.എസ്. അല്ലെങ്കിൽ ഇമെയിൽ വഴി അയയ്ക്കുന്നു, ഒരിക്കൽ മാത്രം ഉപയോഗിക്കാൻ ഉദ്ദേശിച്ചുള്ളതാണ്.

ഇത് എങ്ങനെ പ്രവർത്തിക്കുന്നു

ആൾമാറാട്ടം: കോളുകൾ അല്ലെങ്കിൽ ഇമെയിലുകൾ വഴി ബാങ്കുകൾ, ഇ-കൊമേഴ്സ് വെബ്സൈറ്റുകൾ, പാഴ്സൽ ഡെലിവറി സേവനങ്ങൾ അല്ലെങ്കിൽ മറ്റ് സേവന ദാതാക്കൾ പോലുള്ള നിയമാനുസൃത സേവനങ്ങളായി സ്കാമുകാർ ആൾമാറാട്ടം നടത്തുന്നു.

തെറ്റായ അടിയന്തരബോധം: സ്കാമുകാർ ഒരു തെറ്റായ അടിയന്തരബോധം സൃഷ്ടിക്കുകയും, നിങ്ങളുടെ വിധിന്യായത്തിൽ മങ്ങലേൽപ്പിക്കുകയും, സ്വീകർത്താവ് ആരാണെന്ന് പരിശോധിക്കാതെ ഓ.ടി.പി പങ്കിടാൻ നിങ്ങളെ സമ്മർദ്ദത്തിലാക്കുകയും ചെയ്യുന്നു.

പണമോ വ്യക്തിഗത വിവരങ്ങളോ മോഷ്ടിക്കൽ: ബാങ്കിംഗ് വിശദാംശങ്ങൾ അല്ലെങ്കിൽ വ്യക്തിഗത വിവരങ്ങൾ പോലുള്ള സെൻസിറ്റീവ് വിവരങ്ങൾ ആക്സസ് ചെയ്യുന്നതിന് സ്കാമുകാർ ഓ.ടി.പി-കൾ ഉപയോഗിക്കുന്നു, അതുവഴി ഐഡന്റിറ്റി മോഷണം സാധ്യമാകുന്നു..



- **ശാന്തത പാലിക്കുക**: സൃഷ്ടിക്കപ്പെടുന്ന അടിയന്തിരാവസ്ഥയിൽ മുഴുകരുത്, ശാന്തത പാലിക്കുക, നിങ്ങളുടെ ഇടപാട് ചരിത്രം ട്രാക്ക് ചെയ്യുക, അയച്ചയാളുടെ ഐഡന്റിറ്റി പരിശോധിക്കുക, ഉചിതമായ ജാഗ്രത പാലിക്കുക.

- **അജ്ഞാത കോളുകളെയും ഇമെയിലുകളെയും കുറിച്ച് ജാഗ്രത പാലിക്കുക**: അപ്രതീക്ഷിതമായി നിങ്ങളെ ബന്ധപ്പെടുന്ന ഒരാളുമായി വ്യക്തിഗത വിവരങ്ങളോ ഓ.ടി.പി-കളോ ഒരിക്കലും പങ്കിടരുത്. സാധാരണയായി, സെൻസിറ്റീവ് വിവരങ്ങൾ ആവശ്യമായി വന്നേക്കാവുന്ന ബാങ്കുകളെയോ മറ്റ് സേവനങ്ങളെയോ ബന്ധപ്പെടുമ്പോൾ മാത്രമേ അവർ സി.വി.വി -കളും മറ്റ് സെൻസിറ്റീവ് വ്യക്തിഗത അല്ലെങ്കിൽ സാമ്പത്തിക വിവരങ്ങളും ആവശ്യപ്പെടുകയുള്ളൂ.

- **അയച്ചയാളുടെ ഐഡന്റിറ്റി പരിശോധിക്കുക**: ഇമെയിലുകളിലോ ലിങ്കുകളിലോ ക്ലിക്കുചെയ്യുന്നതിന് മുമ്പ്, അയച്ചയാളുടെ ഐഡന്റിറ്റി പരിശോധിക്കുക.

- **ജാഗ്രത പാലിക്കുക:** നിങ്ങൾ ഓ.ടി.പി യുടെ കൃത്യമായ ഉദ്ദേശ്യത്തെക്കുറിച്ചുള്ള വിവരങ്ങൾ വിളിക്കുന്നയാളിൽ നിന്ന് ആവശ്യപ്പെടുക, നിങ്ങൾ അത്തരം എന്തെങ്കിലും ഇടപാടുകൾ നടത്തിയിട്ടുണ്ടെങ്കിൽ, ഫോണിലൂടെയോ ലിങ്കിലൂടെയോ ഓ.ടി.പി പങ്കിടാൻ അവർ നിങ്ങളോട് ആവശ്യപ്പെടുന്നുണ്ടോ എന്നും നിങ്ങളുടെ സ്വകാര്യ രേഖകൾ ഉപയോഗിച്ച് ക്രോസ്-ചെക്ക് ചെയ്യുക.

സ്കാം # 13 റിവാർഡ് സ്കാം

അത് എന്താണ്

റിവാർഡ് സ്കാമുകൾ നിങ്ങളെ കബളിപ്പിച്ച് ഒരു റിവാർഡിന്റെ മറവിൽ തന്ത്രപ്രധാനമായ വിവരങ്ങൾ പങ്കിടാൻ പ്രേരിപ്പിക്കുന്നു.

ഇത് എങ്ങനെ പ്രവർത്തിക്കുന്നു

റിവാർഡ് ആശയവിനിമയം പങ്കിടൽ: വൻ തുകകൾ നേടിയതിന് അഭിനന്ദനങ്ങൾ അറിയിച്ചുകൊണ്ട് സ്കാമു കാർ ഇമെയിലുകളോ എസ്എംഎസുകളോ അയയ്ക്കും. ഒരു വെബ്സൈറ്റിലേക്കോ ഫ്രോഡായിട്ടുള്ള ആപ്പിലോ ഉള്ള ലിങ്കിൽ ക്ലിക്ക് ചെയ്യാൻ ഇത് നിങ്ങളെ നിർദ്ദേശിക്കും.

ഇത് ഇതുപോലെ തോന്നാം: "പ്രിയ മൂല്യമുള്ള ഉപഭോക്താക്കളേ, നിങ്ങളുടെ എസ്ബിഐ നെറ്റ്ബാങ്കിംഗ് റിവാർഡ് പോയിന്റുകൾ (9980 രൂപ) ഇന്ന് കാലഹരണപ്പെടും! ഇപ്പോൾ എസ്ബിഐ റിവാർഡ് ആപ്പ് വഴി റിഡീം ചെയ്യുക നിങ്ങളുടെ അക്കൗണ്ടിൽ പണം നിക്ഷേപിച്ച് നിങ്ങളുടെ റിവാർഡ് ഇൻസ്റ്റാൾ ചെയ്ത് ക്ലെയിം ചെയ്യുക".

വ്യാജ വെബ്സൈറ്റുകൾ: വെബ്സൈറ്റ് നിയമാനുസൃതമായി തോന്നുകയും നിങ്ങളുടെ സ്വകാര്യ അല്ലെങ്കിൽ ബാങ്കിംഗ് വിവരങ്ങൾ നൽകാൻ ആവശ്യപ്പെടുകയും ചെയ്തേക്കാം. എന്നിരുന്നാലും, ഡാറ്റ സ്കാമർമാർ ആക്സസ് ചെയ്യുന്നു.

വ്യാജ ആപ്പുകൾ: സമ്മാനങ്ങൾ ആക്സസ് ചെയ്യുന്നതിന് 'എസ്ബിഐ റിവാർഡ്സ്' പോലുള്ള നിയമാനുസൃതമെന്ന് തോന്നുന്ന ആപ്പുകൾ ഡൗൺലോഡ് ചെയ്യാൻ സ്കാമർമാർ നിങ്ങളെ നിർദ്ദേശിക്കും. എന്നിരുന്നാലും, ഇത് ഒരു ക്ഷുദ്രകരമായ ആപ്പാണ്, കൂടാതെ ക്യാമറ, മൈക്രോഫോൺ, കോൺടാക്റ്റ് ലിസ്റ്റ്, ഫോട്ടോകൾ, സന്ദേശങ്ങൾ എന്നിവയും അതിലേറെയും പോലുള്ള സെൻസിറ്റീവ് ആപ്പുകളിലേക്ക് ആക്സസ് ചെയ്യാൻ കഴിയും.

ക്ഷുദ്രകരമായ റിവാർഡുകൾ: പകരമായി, നിങ്ങൾ ഒരു പുതിയ ഫോൺ, ടാബ്ലെറ്റ് അല്ലെങ്കിൽ ലാപ്ടോപ്പ് നേടിയെന്ന് സ്കാമർമാർക്ക് പ്രസ്താവിക്കാനും കഴിയും. എന്നിരുന്നാലും, ബാങ്കിംഗ് ഡാറ്റ ഉൾപ്പെടെയുള്ള നിങ്ങളുടെ സെൻസിറ്റീവ് വ്യക്തിഗത വിവരങ്ങൾ മോഷ്ടിക്കാൻ കഴിയുന്ന ക്ഷുദ്രകരമായ ആപ്പുകളോ വൈറസുകളോ ഈ ഉപകരണങ്ങളിൽ മുൻകൂട്ടി ഇൻസ്റ്റാൾ ചെയ്തിട്ടുണ്ട്.

- **ജാഗ്രത പാലിക്കുക**: റിവാർഡുകളും സമ്മാനങ്ങളും ക്ലെയിം ചെയ്യുന്നതിന് ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യുന്നതിന് മുമ്പ് സന്ദേശത്തിന്റെ ഉള്ളടക്കം ശ്രദ്ധാപൂർവ്വം വായിക്കുക.

- **പരിശോധിക്കുക**: അത്തരമൊരു റിവാർഡ് പ്രോഗ്രാം തത്സമയമാണോ എന്ന് ബാങ്കുകളുമായോ മറ്റ് സേവനങ്ങളുമായോ പരിശോധിക്കുക. ഉദാഹരണത്തിന്, റിവാർഡ് പ്രോഗ്രാമുകൾ നടത്തുന്ന വലിയ കമ്പനികൾ അവരുടെ ഔദ്യോഗിക വെബ്സൈറ്റുകളിൽ അത് പരസ്യപ്പെടുത്തും.

- **ഫാക്ടറി റീസെറ്റ്**: വ്യക്തിഗത വിവരങ്ങൾ നൽകുന്നതിന് മുമ്പ് നിങ്ങൾക്ക് സമ്മാനമായോ റിവാർഡായോ ലഭിക്കുന്ന ഏതൊരു ഉപകരണവും ഫാക്ടറി റീസെറ്റ് ചെയ്യുക. നിങ്ങൾ വാങ്ങുന്ന ഏതൊരു റീ-സെയിൽ ഉപകരണങ്ങൾക്കും ഇത് ഒരു നല്ല രീതിയാണ്.

സ്കാം # 14 സിം സ്വാപ്പിംഗ് / സിം ക്ലോണിംഗ് സ്കാം

അത് എന്താണ്

സിം സ്വാപ്പിംഗ്, സിം ക്ലോണിംഗ് എന്നും അറിയപ്പെടുന്നു, സ്കാമു കാർ നിങ്ങളുടെ ഫോൺ നമ്പർ നിയന്ത്രിക്കാൻ നിങ്ങളുടെ സിം കാർഡ് ഡ്യൂപ്ലിക്കേറ്റ് ചെയ്യുന്നതിനെയാണ് ഇത് സൂചിപ്പിക്കുന്നത്. അവർക്ക് ആക്സസ് ലഭിച്ചുകഴിഞ്ഞാൽ, അവർക്ക് OTP അടിസ്ഥാനമാക്കിയുള്ള സുരക്ഷാ പരിശോധനകൾ മറികടന്ന് നിങ്ങളുടെ ബാങ്ക് അക്കൗണ്ടിൽ നിന്ന് പണം മോഷ്ടിക്കാൻ കഴിയും.

ഇത് എങ്ങനെ പ്രവർത്തിക്കുന്നു

ടെലികോം ദാതാവിനെ പോർട്ട് നമ്പറിലേക്ക് ബോധ്യപ്പെടുത്തൽ: ഫിഷിംഗ് ഇമെയിലുകൾ, മാൽവെയർ ആക്രമണങ്ങൾ അല്ലെങ്കിൽ ഡാറ്റ ചോർച്ചകൾ എന്നിവ ഉപയോഗിച്ച് സ്കാമുകാർ വ്യക്തിഗത വിവരങ്ങൾ ശേഖരിക്കുന്നു. തുടർന്ന് അവർ നിങ്ങളാണെന്ന് നടിച്ച് നിങ്ങളുടെ മൊബൈൽ നെറ്റ്‌വർക്ക് ദാതാവിനെ ബന്ധപ്പെടുകയും വ്യാജ ഐഡി പ്രൂഫ് നൽകുകയും പഴയത് നഷ്ടപ്പെട്ടുവെന്നോ കേടായതായെന്നോ അവകാശപ്പെട്ട് പുതിയ സിം കാർഡ് അഭ്യർത്ഥിക്കുകയും ചെയ്യുന്നു.

സിം സ്വാപ്പിനായി നിങ്ങളെ ബോധ്യപ്പെടുത്തുന്നു: ചിലപ്പോൾ സ്കാമർമാർ നിങ്ങളെ ഒരു സിം സ്വാപ്പ് സജീവമാക്കാൻ നിർബന്ധിക്കാൻ ശ്രമിക്കുന്നു. ഈ സമീപനത്തിൽ, നിങ്ങളുടെ ടെലികോം ദാതാവിന്റെ എക്സിക്യൂട്ടീവാണെന്ന് നടിച്ച് സ്കാമർ നിങ്ങൾക്ക് ഒരു വ്യാജ കോൾ ചെയ്യുന്നു. സ്കാമർ മികച്ച മൊബൈൽ സബ്സ്ക്രിപ്ഷൻ പാക്കേജ് വാഗ്ദാനം ചെയ്യുകയും നിങ്ങളുടെ 20 അക്ക സിം നമ്പർ പങ്കിടാനും ഓഫർ സജീവമാക്കാൻ "1" അമർത്താനും നിങ്ങളെ ബോധ്യപ്പെടുത്തുകയും ചെയ്യുന്നു. എന്നിരുന്നാലും, നിങ്ങൾ "1" അമർത്തുമ്പോൾ, നിങ്ങളുടെ നമ്പറിലെ സിം സ്വാപ്പ് പ്രാമാണീകരിക്കുകയും സ്കാമർമാർക്ക് നിയന്ത്രണം നൽകുകയും ചെയ്യുന്നു.

നിയന്ത്രണം നേടുന്നു: ദാതാവ് ഒരു പുതിയ സിം നൽകിക്കഴിഞ്ഞാൽ അല്ലെങ്കിൽ സിം സ്വാപ്പ് പൂർത്തിയാക്കിയാൽ, നിങ്ങളുടെ യഥാർത്ഥ സിം നിർജ്ജീവമാക്കപ്പെടും. നിങ്ങളുടെ കോളുകൾ, സന്ദേശങ്ങൾ, ഒടിപികൾ എന്നിവയിലേക്ക് സ്കാമർ ആക്സസ് നേടുന്നു.

സാമ്പത്തിക സ്കാമും ഐഡന്റിറ്റി മോഷണവും: ഫണ്ട് ട്രാൻസ്ഫർ ചെയ്യാനും പാസ്‌വേഡുകൾ പുനഃസജ്ജമാക്കാനും നിങ്ങളുടെ സാമ്പത്തിക, സോഷ്യൽ മീഡിയ അക്കൗണ്ടുകൾ കൈയടക്കാനും സ്കാമുകാർ ഓ.ടി.പി-കൾ ഉപയോഗിക്കുന്നു.

- **സിം ലോക്ക് പ്രവർത്തനക്ഷമമാക്കുക**: നിങ്ങളുടെ ഉപകരണത്തിലെ ക്രമീകരണങ്ങളിലേക്ക് പോയി സിം ലോക്ക് ചെയ്യുന്നതിന് ഒരു സിം പിൻ സജ്ജമാക്കുക. സിം പിൻ ഇല്ലാതെ സ്കാമുകാർക്ക് നിങ്ങളുടെ സിം സ്വാപ്പ് ചെയ്യാനോ നിർജ്ജീവമാക്കാനോ കഴിയില്ല.

- **നെറ്റ്‌വർക്ക് പ്രശ്നങ്ങളെക്കുറിച്ച് ജാഗ്രത പാലിക്കുക**: മറ്റുള്ളവയ്ക്ക് സിഗ്നൽ ഉള്ളപ്പോൾ നിങ്ങളുടെ ഫോണിൽ പെട്ടെന്ന് നെറ്റ്‌വർക്ക് നഷ്ടപ്പെട്ടാൽ, ഉടൻ തന്നെ നിങ്ങളുടെ ദാതാവിനെ ബന്ധപ്പെടുക.

- **നിങ്ങളുടെ ഡിജിറ്റൽ ഫൂട്ട്പ്രിന്റിനെ കുറിച്ച് ജാഗ്രത പാലിക്കുക**: ഗൂഗിൾ, മെറ്റ പോലുള്ള ജനപ്രിയ സേവനങ്ങളിലെ നിങ്ങളുടെ സ്വകാര്യതാ ക്രമീകരണങ്ങൾ അവലോകനം ചെയ്യാൻ സമയം ചെലവഴിക്കുക. നിങ്ങളുടെ സ്വകാര്യ ഡാറ്റ എത്രത്തോളം മൂന്നാം കക്ഷികളുമായി പങ്കിടുന്നുണ്ടെന്ന് നിങ്ങൾക്ക് അറിയാൻ കഴിയും..

സ്കാം # 15 ആൾമാറാട്ട സ്കാം

അത് എന്താണ്

നിങ്ങളുടെ സുഹൃത്ത്, ബന്ധു അല്ലെങ്കിൽ സഹപ്രവർത്തകൻ എന്ന് ആൾമാറാട്ടം നടത്തുന്നതിന് ഹാക്കിംഗ്, മോഷ്ടിച്ച പാസ്‌വേഡുകൾ, ഫിഷിംഗ് ടെക്‌നിക്കുകൾ എന്നിവ ഉപയോഗിച്ച് സ്കാമുകാർ പണം അയയ്ക്കുന്നു. അറിയപ്പെടുന്ന ഒരാളിൽ നിന്നാണ് സന്ദേശങ്ങൾ വരുന്നതെന്ന് തോന്നുന്നതിനാൽ, ഇരകൾ പലപ്പോഴും സ്കാമിന് ഇരയാകുന്നു.

ഇത് എങ്ങനെ പ്രവർത്തിക്കുന്നു

സ്കാമു കാർ ഒരാളുടെ സോഷ്യൽ മീഡിയ അക്കൗണ്ടിൽ കയറി അടിയന്തര സാഹചര്യം അവകാശപ്പെട്ട് അവരുടെ കോൺടാക്റ്റുകൾക്ക് സന്ദേശം അയയ്ക്കുന്നു.

സന്ദേശങ്ങൾ ഇങ്ങനെയായിരിക്കാം: “ഹായ്, ഞാൻ ഡൽഹിയിൽ കുടുങ്ങിക്കിടക്കുകയാണ്, അവിടെ ഞാൻ അവധിക്കാലത്തായിരുന്നു, കൊള്ളയടിക്കപ്പെട്ടു. എനിക്ക് അടിയന്തിരമായി 5000 രൂപ ആവശ്യമാണ്, പക്ഷേ നിങ്ങൾ എനിക്ക് നൽകുന്ന ഏത് സഹായവും വളരെ നന്ദിയുള്ളതായിരിക്കും, ഞാൻ തിരിച്ചെത്തിയാലുടൻ ഞാൻ നിങ്ങൾക്ക് പണം തിരികെ നൽകും. ദയവായി സഹായിക്കുക”.

ചിലപ്പോൾ സ്കാമു കാർ നിങ്ങളുടെ സഹപ്രവർത്തകന്റെയോ ബോസിന്റെയോ ഇമെയിൽ ഐഡിയോട് സാമ്യമുള്ള ഒരു ഇമെയിൽ സൃഷ്ടിക്കുന്നു. ഒരു പ്രധാന ജോലി പൂർത്തിയാക്കാൻ അടിയന്തിരമായി പണം അയയ്ക്കാൻ ആവശ്യപ്പെട്ട് അവർ ഔദ്യോഗിക സ്വരത്തിൽ നിങ്ങൾക്ക് എഴുതുന്നു.

ഹാക്ക് ചെയ്യപ്പെട്ട അക്കൗണ്ടിലെ / വ്യാജ ഇമെയിലിലെ സ്കാമു കാരന് നിങ്ങൾ മറുപടി നൽകിക്കഴിഞ്ഞാൽ, ഒരു പ്രത്യേക അക്കൗണ്ടിലേക്കോ യുപിഐ ഹാൻഡിലിലേക്കോ ഫണ്ട് ട്രാൻസ്ഫർ ചെയ്യാൻ അവർ നിങ്ങളോട് ആവശ്യപ്പെടുന്നു. പണം അയച്ചതിനുശേഷം സ്കാമു കാർ അപ്രത്യക്ഷമാവുകയും ഇരയെ ബ്ലോക്ക് ചെയ്യുകയും ചെയ്യും.

അടിയന്തര സന്ദേശങ്ങൾ സൂക്ഷിക്കുക: വേഗത്തിൽ പ്രവർത്തിക്കാൻ വേണ്ടി സ്കാമുകാർ പരിഭ്രാന്തി സൃഷ്ടിക്കുന്നു. മെസേജിംഗ് ആപ്പുകൾ, സോഷ്യൽ മീഡിയ അല്ലെങ്കിൽ ഇമെയിൽ വഴി ലഭിക്കുന്ന പണത്തിനായുള്ള പെട്ടെന്നുള്ള അടിയന്തര അഭ്യർത്ഥനകൾ അടങ്ങിയ സന്ദേശങ്ങളെക്കുറിച്ച് ജാഗ്രത പാലിക്കുക.

അഭ്യർത്ഥനകൾ പരിശോധിക്കുക: പണത്തിനായുള്ള അടിയന്തര അഭ്യർത്ഥനകളിൽ നടപടിയെടുക്കുന്നതിന് മുമ്പ് ആ വ്യക്തിയെ നേരിട്ട് വിളിക്കുകയോ ഒരു പൊതു സുഹൃത്തിനോടോ ബന്ധുവിനോടോ സംസാരിക്കുകയോ ചെയ്യുക.

റെഡ് ഫ്ലാഗുകൾക്കായി പരിശോധിക്കുക: അയയ്ക്കുന്നയാൾ സാധാരണയായി ആശയവിനിമയം നടത്തുന്ന രീതിയിലാണോ സന്ദേശം വായിക്കുന്നത്? അസാധാരണമായ അഭ്യർത്ഥനകൾ, വിചിത്രമായ വ്യാകരണം, ഫോർമാറ്റിംഗ്, പുതിയ/അജ്ഞാത ബാങ്ക് അക്കൗണ്ടുകളിലേക്ക് പണം കൈമാറാനുള്ള അഭ്യർത്ഥനകൾ എന്നിവയ്ക്കായി ശ്രദ്ധിക്കുക.

സ്കാം # 16 സ്കിമ്മിംഗ് മെഷീൻ സ്കാം

അത് എന്താണ്

നിങ്ങളുടെ കാർഡ് നമ്പർ, കാലാവധി തീയതി, പിൻവശത്തുള്ള മൂന്നക്ക കാർഡ് വെരിഫിക്കേഷൻ വാല്യൂ (സി.വി.വി) തുടങ്ങിയ പ്രധാനപ്പെട്ട കാർഡ് വിശദാംശങ്ങൾ മോഷ്ടിക്കുന്നതിനായി സ്കാമർമാർ എടിഎമ്മുകളിലോ ഹാൻഡ്ഹെൽഡ് കാർഡ് പേയ്മെന്റ് മെഷീനുകളിലോ ഒരു മറഞ്ഞിരിക്കുന്ന ഉപകരണം ഇൻസ്റ്റാൾ ചെയ്യുമ്പോൾ സ്കിമ്മിംഗ് സംഭവിക്കുന്നു.

ഈ ഉപകരണങ്ങൾ പലപ്പോഴും മെഷീനിന്റെ ഒരു സാധാരണ ഭാഗം പോലെ തോന്നിപ്പിക്കാൻ വേഷംമാറി ഉപയോഗിക്കപ്പെടുന്നു. കാർഡ് വിശദാംശങ്ങൾ പിടിച്ചെടുത്തുകഴിഞ്ഞാൽ, സ്കാമർമാർ ഡ്യൂപ്ലിക്കേറ്റ് കാർഡുകൾ സൃഷ്ടിച്ച് നിങ്ങളുടെ അക്കൗണ്ടിൽ നിന്ന് ഇടപാടുകൾ നടത്തുന്നു.

ഇത് എങ്ങനെ പ്രവർത്തിക്കുന്നു

ഒരു സ്കിമ്മർ സ്ഥാപിക്കൽ: സ്കാമു കാർ എടിഎമ്മിന്റെയോ സ്വൈപ്പ് മെഷീനിന്റെയോ കാർഡ് റീഡറിന് മുകളിൽ ഒരു ഉപകരണം ഘടിപ്പിക്കുന്നു.

കാർഡ് ഡാറ്റ പിടിച്ചെടുക്കൽ: നിങ്ങൾ നിങ്ങളുടെ കാർഡ് ചേർക്കുമ്പോൾ, സ്കിമ്മർ നിങ്ങളുടെ കാർഡ് വിശദാംശങ്ങൾ വായിക്കുന്നു.

പിൻ നമ്പറുകൾ റെക്കോർഡുചെയ്യൽ: ഒരു ചെറിയ ക്യാമറ അല്ലെങ്കിൽ വ്യാജ കീപാഡ് എടിഎമ്മിൽ നിങ്ങളുടെ പിൻ നമ്പർ രേഖപ്പെടുത്തുന്നു.

ക്ലോണിംഗും ഫ്രോഡായിട്ടുള്ള ഇടപാടുകളും: സ്കാമു കാർ മോഷ്ടിച്ച വിശദാംശങ്ങൾ ഉപയോഗിച്ച് ഡ്യൂപ്ലിക്കേറ്റ് കാർഡുകൾ സൃഷ്ടിച്ച് പണം പിൻവലിക്കുന്നു.

- **എടിഎം പരിശോധിക്കുക**: എടിഎമ്മുകളിൽ അയഞ്ഞ കാർഡ് സ്ലോട്ടുകൾ, ഇളകുന്ന കീപാഡുകൾ അല്ലെങ്കിൽ അധിക ക്യാമറകൾ എന്നിവ പരിശോധിക്കുക.
- **ശ്രദ്ധിക്കുക:** എപ്പോഴും നിങ്ങളുടെ മുന്നിൽ കാർഡ് സ്വൈപ്പ് മെഷീൻ ഉപയോഗിക്കാൻ ആവശ്യപ്പെടുക, സംശയാസ്പദമായ സ്ഥലങ്ങളിലോ മെഷീനുകളിലോ കാർഡ് സ്വൈപ്പ് ചെയ്യുന്നതിൽ ശ്രദ്ധാലുവായിരിക്കുക..
- **ബാങ്ക് സ്റ്റേറ്റ്മെന്റുകൾ നിരീക്ഷിക്കുക**: അനധികൃത ഡെബിറ്റ് ഇടപാടുകൾക്കായി നിങ്ങളുടെ ബാങ്ക് സ്റ്റേറ്റ്മെന്റുകളും എസ്എംഎസും പതിവായി പരിശോധിക്കുക..
- **അനധികൃത ഇടപാടുകൾ ഉടൻ ബാങ്കിൽ റിപ്പോർട്ട് ചെയ്യുക**. എത്രയും വേഗം നിങ്ങളുടെ ബാങ്കിനെ അറിയിച്ചാൽ നഷ്ടം പരിമിതപ്പെടുത്താൻ നിങ്ങൾക്ക് കഴിഞ്ഞേക്കും..

സ്കാം # 17 വ്യാജ ക്ഷേമ പദ്ധതി സ്കാം

അത് എന്താണ്

പിഎം കിസാൻ യോജന, പിഎം ആവാസ് യോജന തുടങ്ങിയ സാധാരണ പദ്ധതികളുടെ വെബ്സൈറ്റുകൾ പോലെ തോന്നിക്കുന്ന വ്യാജ പോർട്ടലുകൾ സ്കാമുകാർ സൃഷ്ടിക്കുന്നു. ബാങ്ക് അക്കൗണ്ട്, മൊബൈൽ നമ്പർ, ആധാർ വിവരങ്ങൾ എന്നിവ സ്കാമുകാർക്ക് വെളിപ്പെടുത്താൻ ഇരകളെ പ്രലോഭിപ്പിക്കുന്നു.

ഇത് എങ്ങനെ പ്രവർത്തിക്കുന്നു

ഒരു സാമൂഹിക ക്ഷേമ പദ്ധതി പ്രകാരം ഫണ്ട് ലഭിക്കാൻ നിങ്ങൾക്ക് അർഹതയുണ്ടെന്ന് പറഞ്ഞ് സ്കാമുകാർ നിങ്ങളെ വിളിക്കുന്നു, എന്നാൽ തുക നിങ്ങൾക്ക് അയയ്ക്കുന്നതിന് മുമ്പ് നിങ്ങൾ ആദ്യം നിങ്ങളുടെ ബാങ്ക് വിശദാംശങ്ങൾ 'പരിശോധിക്കുക' അല്ലെങ്കിൽ 'അപ്ഡേറ്റ്' ചെയ്യേണ്ടതുണ്ട്.

'പരിശോധിച്ചുറപ്പിക്കൽ' പ്രക്രിയ പൂർത്തിയാക്കാൻ നിങ്ങളുടെ ബാങ്ക് അക്കൗണ്ടിന്റെയും ഡെബിറ്റ് കാർഡ് വിശദാംശങ്ങളുടെയും വിശദാംശങ്ങൾ പങ്കിടാൻ സ്കാമുകാർ നിങ്ങളോട് ആവശ്യപ്പെടുന്നു. സ്ഥിരീകരണം പൂർത്തിയാക്കാൻ അവർ ഒടുവിൽ നിങ്ങളോട് ഒരു OTP ആവശ്യപ്പെടുന്നു.

എന്നാൽ നിങ്ങളുടെ അക്കൗണ്ടിൽ ഒരു പേയ്മെന്റ് സജ്ജീകരിക്കാൻ സ്കാമർമാർ യഥാർത്ഥത്തിൽ നിങ്ങളുടെ ബാങ്ക്, ഡെബിറ്റ് കാർഡ് വിശദാംശങ്ങൾ ഉപയോഗിക്കുന്നു, കൂടാതെ ഡെബിറ്റ് ഇടപാടിന് അംഗീകാരം നൽകാൻ OTP ഉപയോഗിക്കുന്നു. ഇരകൾ OTP പങ്കിട്ടുകഴിഞ്ഞാൽ, സ്കാമുകാർ അവരുടെ അക്കൗണ്ടുകളിൽ നിന്ന് പണം പിൻവലിച്ചതായി അവർ മനസ്സിലാക്കുന്നു.

- **സൗജന്യങ്ങളെക്കുറിച്ച് ജാഗ്രത പാലിക്കുക**: നിങ്ങളുടെ വ്യക്തിപരവും സാമ്പത്തികവുമായ വിവരങ്ങൾ പങ്കിടാൻ നിങ്ങളെ വശീകരിക്കാൻ സ്കാമുകാർ പലപ്പോഴും സൗജന്യങ്ങൾ, നികുതി ഇളവുകൾ അല്ലെങ്കിൽ മറ്റ് ആനുകൂല്യങ്ങൾ വാഗ്ദാനം ചെയ്യുന്നു.
- **സർക്കാർ വെബ്സൈറ്റുകൾ പരിശോധിക്കുക**: ക്ഷേമ പദ്ധതികൾക്കായി ഔദ്യോഗിക പോർട്ടലുകൾ ഉപയോഗിക്കുക. സർക്കാർ വെബ്സൈറ്റുകളുടെ അവസാനം സാധാരണയായി “.gov.in” അല്ലെങ്കിൽ “.nic.in” എന്ന എക്സ്റ്റൻഷൻ ഉണ്ടാകും.
- **സ്കീം വിശദാംശങ്ങൾ പരിശോധിക്കുക**: നിങ്ങളുടെ ഗ്രാമപഞ്ചായത്തിൽ നിന്നോ നിങ്ങളുടെ ജില്ലയിലെ തഹസിൽദാർ ഓഫീസിൽ നിന്നോ ഏതെങ്കിലും സർക്കാർ പദ്ധതികളുടെ വിശദാംശങ്ങൾ പരിശോധിക്കുക.
- **ജാഗ്രത പാലിക്കുക**: OTP അടങ്ങിയ സന്ദേശം വായിക്കുക. അത് നിയമാനുസൃതമാണോ അതോ മറ്റെന്തെങ്കിലും ആവശ്യത്തിനാണോ എന്ന് പരിശോധിക്കുക. പേജ് 38-ലെ ഞങ്ങളുടെ പ്രോ-ടിപ്പുകൾ കാണുക..

ചെയ്യേണ്ടതും ചെയ്യരുതാത്തതുമായ കാര്യങ്ങൾ

സുരക്ഷിത സർഫിംഗ് നുറുങ്ങുകൾ

- നിങ്ങളെക്കുറിച്ച് ഓൺലൈനിൽ പങ്കിടുന്ന വിവരങ്ങൾ പരിമിതപ്പെടുത്തുന്നതിന്, നിങ്ങളുടെ ബ്രൗസറിലെയും ആപ്പുകളിലെയും സന്ദേശമയയ്ക്കൽ, സോഷ്യൽ മീഡിയ, മാപ്പുകൾ എന്നിവയ്ക്കായുള്ള സ്വകാര്യതാ ക്രമീകരണങ്ങൾ ഇടയ്ക്കിടെ അവലോകനം ചെയ്യുക.
- ഫോട്ടോകൾ, ഫയലുകൾ, ഉപകരണ ലൊക്കേഷൻ എന്നിവ പോലുള്ള നിങ്ങളുടെ ഉപകരണത്തിലെ ഡാറ്റയിലേക്ക് മൂന്നാം കക്ഷി, സോഷ്യൽ മീഡിയ ആപ്പുകൾക്ക് പരിമിതമായ ആക്സസ് ഉണ്ടെന്ന് ഉറപ്പാക്കുക.
- പാസ്‌വേഡുകൾ ഓർമ്മിക്കുക അല്ലെങ്കിൽ അവയുടെ ഒരു ഭൗതിക റെക്കോർഡ് എവിടെയെങ്കിലും സുരക്ഷിതമായി സൂക്ഷിക്കുക. നിങ്ങളുടെ പാസ്‌വേഡുകൾ പതിവായി മാറ്റുന്നതും വ്യത്യസ്ത വെബ്സൈറ്റുകളിലും ആപ്പുകളിലും പാസ്‌വേഡുകൾ ആവർത്തിക്കുന്നത് ഒഴിവാക്കുന്നതും ഉറപ്പാക്കുക.
- നിങ്ങളുടെ ബാങ്ക് അല്ലെങ്കിൽ കാർഡ് വിശദാംശങ്ങൾ അപഹരിക്കപ്പെട്ട ഒരു ഫിഷിംഗ് സ്കാമി ന് നിങ്ങൾ ഇരയായാൽ, നിങ്ങളുടെ ബാങ്കുമായി ബന്ധപ്പെടുകയും അത് ഉടൻ റിപ്പോർട്ട് ചെയ്യുകയും ചെയ്യുക.
- ആവശ്യമില്ലെങ്കിൽ നിങ്ങളുടെ ഉപകരണത്തിൽ ലൊക്കേഷൻ സേവനങ്ങൾ ഓഫാക്കി വയ്ക്കുക.
- നിക്ഷേപ പദ്ധതി/ജോലി ആണെങ്കിൽ ഓഫർ ശരിയാകാൻ വളരെ നല്ലതായി തോന്നുന്നു - അത് അങ്ങനെയാകാൻ സാധ്യതയുണ്ട്

പൂർണ്ണമായി വേണ്ടേ -വേണ്ട

- എസ്എംഎസ് / ഇമെയിൽ അല്ലെങ്കിൽ മെസേജിംഗ് ആപ്പുകളിലെ അജ്ഞാത ഉറവിടങ്ങളിൽ നിന്നുള്ള ലിങ്കുകളിൽ ശ്രദ്ധാപൂർവ്വം വായിക്കാതെ ക്ലിക്ക് ചെയ്യരുത്.
- കോളുകൾ, എസ്എംഎസ്, ഓൺലൈൻ ഫോമുകൾ, ഇമെയിലുകൾ എന്നിവയിൽ ഒടിപി, എടിഎം അല്ലെങ്കിൽ യുപിഐ പിൻ, പാസ്‌വേഡുകൾ എന്നിവ പങ്കിടരുത്.
- അജ്ഞാത നമ്പറുകളിൽ നിന്നുള്ള ഫയലുകൾ (വിവാഹ ക്ഷണക്കത്തുകൾ പോലുള്ളവ) മെസേജിംഗ് ആപ്പുകളിൽ ഡൗൺലോഡ് ചെയ്യരുത്.
- സോഷ്യൽ മീഡിയയിൽ അപരിചിതരിൽ നിന്നുള്ള സൗഹൃദ അഭ്യർത്ഥനകളും സന്ദേശ അഭ്യർത്ഥനകളും സ്വീകരിക്കരുത്.
- സോഫ്റ്റ്‌വെയറിന്റെയും മീഡിയയുടെയും വ്യാജ പകർപ്പുകൾ ഡൗൺലോഡ് ചെയ്ത് ഇൻസ്റ്റാൾ ചെയ്യരുത്; അവയിൽ മാൽവെയർ അടങ്ങിയിരിക്കാം.
- സുരക്ഷിതമല്ലാത്ത വെബ്സൈറ്റുകളിൽ ഇടപാട് നടത്തുന്നതിൽ ശ്രദ്ധിക്കുക (വെബ് വിലാസം “https://” ൽ ആരംഭിക്കുന്നുവെന്നും “http://” ൽ ആരംഭിക്കുന്നില്ലെന്നും സ്ഥിരീകരിക്കുക).
- ഓൺലൈൻ ഇടപാടുകൾക്കായി സിവിവികൾ നൽകുന്നതിൽ ശ്രദ്ധിക്കുക.s.

സംശയാസ്പദമായ കോളുകളോ സ്കാമുകളോ **സൈബർ ക്രൈം ഹെൽപ്പ്ലൈൻ നമ്പറായ 1930** യിൽ അറിയിക്കുക. അല്ലെങ്കിൽ **www.cybercrime.gov.in** എന്ന വെബ്സൈറ്റിൽ അറിയിക്കുക.

അനുകൂല നുറുങ്ങുകൾ

1 പാസ്‌വേഡ് ശുചിത്വം

- വലിയക്ഷരം, ചെറിയക്ഷരം, അക്കങ്ങൾ, ചിഹ്നങ്ങൾ എന്നിവയുടെ മിശ്രിതമുള്ള കുറഞ്ഞത് 16അക്ഷരങ്ങൾ ഉപയോഗിക്കുക.
- പ്രവചിക്കാവുന്ന പാറ്റേണുകൾ, വ്യക്തിഗത വിവരങ്ങൾ അല്ലെങ്കിൽ തുടർച്ചയായ പ്രതീകങ്ങൾ എന്നിവ ഒഴിവാക്കുക.
- സാധ്യമാകുന്നിടത്തെല്ലാം പാസ്കീകൾ പ്രവർത്തനക്ഷമമാക്കുക.
- പരമ്പരാഗത പാസ്‌വേഡുകൾക്ക് പകരം വിരലടയാളം, മുഖം തിരിച്ചറിയൽ അല്ലെങ്കിൽ വോയ്സ് തിരിച്ചറിയൽ പോലുള്ള ബയോമെട്രിക്സാണ് പാസ്കീകൾ ഉപയോഗിക്കുന്നത്.
- അധികസുരക്ഷയ്ക്കായി ലഭ്യമാകുമ്പോഴെല്ലാം മൾട്ടി ഫാക്ടർ പ്രാമാണീകരണം സജ്ജമാക്കുക.

Weak passwords

Simple: Aditi1995 (name + birth year)
Sequential: abcdxyz123 **Predictable**: SalmanBhaiFan

Strong passwords

Personal: Maachbhaat&Dal92

Random words & multiple characters: C@rr0tcake&MnMs!

2 SMS കോഡുകൾ മനസ്സിലാക്കൽ

യഥാർത്ഥ എസ്എംഎസ് സന്ദേശങ്ങൾ അനുകരിക്കുന്നതിനാണ് വ്യാജ എസ്എംഎസ് സന്ദേശങ്ങൾ രൂപകൽപ്പന ചെയ്തിരിക്കുന്നത്, പലപ്പോഴും പെട്ടെന്ന് നടപടിയെടുക്കാൻ പ്രേരിപ്പിക്കുന്നു. ഇത്തരം സ്കാമുകളിൽ നിന്ന് സ്വയം തിരിച്ചറിയാനും സംരക്ഷിക്കാനും എങ്ങനെയെന്ന് ഇതാ:

- വ്യക്തിഗത മൊബൈൽ നമ്പറുകളിൽ നിന്നോ 567678 അല്ലെങ്കിൽ 909090 പോലുള്ള പൊതുവായ സംഖ്യാ ഐഡികളിൽ നിന്നോ പലപ്പോഴും വ്യാജ സന്ദേശങ്ങൾ അയയ്ക്കാറുണ്ട്.
- യഥാർത്ഥ എസ്എംഎസുകൾക്ക് [XY-ABCDEF] എന്ന ഫോർമാറ്റ് ഉണ്ട് X എന്നത് അയയ്ക്കുന്നയാളുടെ ടെലികോം സേവന ദാതാവിന്റെ പേരാണ് (ഉദാ. J എന്നത് ജിയോയ്ക്കും, A എന്നത് എയർടെല്ലിനും, V എന്നത് വോഡഫോണിനും). Y എന്നത് സേവന മേഖലയുടെ പേരാണ് (ഉദാ. D എന്നത് ഡൽഹിക്കും, M എന്നത് മുംബൈയ്ക്കും, X എന്നത് കർണാടകയ്ക്കും). ABCDEF എന്നത് അയച്ചയാൾക്ക് നൽകിയിട്ടുള്ള കോഡിനെ സൂചിപ്പിക്കുന്നു (ഉദാ. SPICEJ എന്നത് സ്പൈസ് ജെറ്റിനെ സൂചിപ്പിക്കുന്നു).

.. തുടരുന്നു

- **ചിത്രീകരണങ്ങൾ:**
  - **‘AD-SHPRKT’ എന്ന എസ്എംഎസ് കോഡ് അയച്ചയാൾ ഷിപ്പ് റോക്കറ്റ് എന്നും അയച്ചയാളുടെ കാരിയർ എയർടെൽ എന്നും സന്ദേശം ഡൽഹിയിൽ നിന്ന് അയച്ചതാണെന്നും അർത്ഥമാക്കുന്നു..**
  - **'VM-SBIUPI' എന്ന എസ്എംഎസ് കോഡ് അയയ്ക്കുന്നയാൾ സ്റ്റേറ്റ് ബാങ്ക് ഓഫ് ഇന്ത്യയാണെന്നും അയയ്ക്കുന്നയാളുടെ കാരിയർ വോഡഫോണാണെന്നും സന്ദേശം മുംബൈയിൽ നിന്നാണ് അയച്ചിരിക്കുന്നതെന്നും അർത്ഥമാക്കുന്നു..**
- സേവന ദാതാവിന്റെ കോഡുകളുടെ വിശദമായ പട്ടിക TRAI സൂക്ഷിക്കുന്നു, ടെലികോം സേവന ഏരിയ കോഡുകളും ബിസിനസുകൾക്കുള്ള നിയുക്ത തലക്കെട്ടുകളും. പേയ്മെന്റിനായി ഏതെങ്കിലും ലിങ്കിൽ ക്ലിക്കുചെയ്യുന്നതിന് മുമ്പ്, പ്രത്യേകിച്ച് SMS-ന്റെ ആധികാരികത പരിശോധിക്കുന്നത് ഉറപ്പാക്കുക..

#3 സ്കാമുകാരോടും ഫ്രോഡുകളോടും പ്രതികരിക്കുന്നു

- **കോൾ കട്ട് ചെയ്ത് നമ്പർ ബ്ലോക്ക് ചെയ്യുക**: അജ്ഞാത കോളർമാർ സ്വീകരിക്കുന്ന അടിയന്തര സാഹചര്യങ്ങളോ ഭയപ്പെടുത്തൽ തന്ത്രങ്ങളോ സ്വീകരിക്കരുത്, അവർ ബാങ്ക് പ്രതിനിധികളോ സർക്കാർ പ്രതിനിധികളോ ആണെന്ന് നിങ്ങളോട് പറഞ്ഞാലും.
- **റിപ്പോർട്ട്**: ‘സഞ്ചാർ സാത്തി’ പോർട്ടലിൽ (www.sancharsaathi.gov.in) ‘ചക്ഷു’ എന്ന വിലാസത്തിൽ റിപ്പോർട്ട് ചെയ്തുകൊണ്ട് സ്കാമുകാരന്റെ നമ്പർ പ്രവർത്തനരഹിതമാക്കുക.
- **നിങ്ങളുടെ പണം ഇതിനകം നഷ്ടപ്പെട്ടിട്ടുണ്ടെങ്കിൽ**: ഉടൻ തന്നെ നിങ്ങളുടെ ബാങ്കിൽ വിളിച്ച് ഇടപാട് റിപ്പോർട്ട് ചെയ്യുക. ദേശീയ സൈബർ കുറ്റകൃത്യ റിപ്പോർട്ടിംഗ് പോർട്ടലിലും സംഭവം റിപ്പോർട്ട് ചെയ്യുക (1930 എന്ന നമ്പറിൽ ഡയൽ ചെയ്യുക അല്ലെങ്കിൽ www.cybercrime.gov.in സന്ദർശിക്കുക).
- **സ്പാം ഫിൽട്ടർ ചെയ്യുക**: 1909 ഡയൽ ചെയ്ത് TRAI നിർദ്ദേശപ്രകാരം നിങ്ങളുടെ ടെലികോം ദാതാവ് വാഗ്ദാനം ചെയ്യുന്ന സ്പാം ബ്ലോക്കിംഗ് സൗകര്യത്തിനായി രജിസ്റ്റർ ചെയ്യുക.
- **നിരന്തരമായ ജാഗ്രത**: ഏറ്റവും പുതിയ വിവരങ്ങൾ അറിയാൻ സോഷ്യൽ മീഡിയയിൽ I4C പിന്തുടരുക: (Twitter-ൽ @CyberDost; Facebook-ൽ CyberDostI4C അല്ലെങ്കിൽ Instagram-ൽ @cyberdosti4c എന്നിവ കാണുക)..
- **നിങ്ങളുടെ കാൽപ്പാടുകൾ പരിശോധിക്കുക**: നിങ്ങളുടെ ഡിജിറ്റൽ കാൽപ്പാടുകളുടെ വലുപ്പത്തെക്കുറിച്ച് ശ്രദ്ധാലുവായിരിക്കുക. നിങ്ങളുടെ ഡാറ്റ എത്ര കമ്പനികൾക്ക് നൽകിയിട്ടുണ്ടെന്ന് അവലോകനം ചെയ്യുക. ആവശ്യമെങ്കിൽ നിങ്ങളുടെ ഡാറ്റ ഇല്ലാതാക്കാൻ അവരോട് ആവശ്യപ്പെടുക. കൂടാതെ, നിങ്ങളുടെ ഡാറ്റ ഏതെങ്കിലും ഡാറ്റാ ലംഘനത്തിന്റെ ഭാഗമാണോ എന്ന് കണ്ടെത്താൻ ‘www.haveibeenpwned.com’ പോലുള്ള സൗജന്യ **ഉപകരണങ്ങൾ ഉപയോഗിക്കുക..**

ഉപയോക്തൃ സുരക്ഷയ്ക്കുള്ള വ്യവസായത്തിലെ മികച്ച രീതികൾ

ഉപയോക്തൃ സുരക്ഷ ഉറപ്പാക്കുന്നത് തുടർച്ചയായ ഒരു പ്രവർത്തനമാണ്. ഡിജിറ്റൽ ഇടങ്ങൾ കൂടുതൽ കൂടുതൽ ആഴത്തിലുള്ളതായിത്തീരുമ്പോൾ, ഉപയോക്താക്കളെ അറിയിക്കുന്നതിനും ശാക്തീകരിക്കുന്നതിനും സംരക്ഷിക്കുന്നതിനുമുള്ള രീതികൾ ബിസിനസുകൾ വികസിപ്പിക്കേണ്ടതുണ്ട്.

ഉപയോക്തൃ സുരക്ഷയ്ക്കുള്ള നാല് അടിസ്ഥാന തത്വങ്ങൾ ഇവയാണ്:

🤖 **ഉപയോക്താക്കളെ സംരക്ഷിക്കുന്നതിനും ശാക്തീകരിക്കുന്നതിനും AI ഉപകരണങ്ങൾ ഉപയോഗിക്കുന്നു**

🔐 **രൂപകൽപ്പന പ്രകാരം സുരക്ഷിതമായ ഉൽപ്പന്നങ്ങൾ നിർമ്മിക്കുന്നു**

🤝 **വേഗത്തിലുള്ളതും ഫലപ്രദവുമായ പരാതി പരിഹാരം ഉറപ്പാക്കൽ**

💪 **ഓൺലൈൻ ഇടപെടലുകൾ നിയന്ത്രിക്കാൻ ഇന്റർനെറ്റ് ഉപയോക്താക്കളെ പ്രാപ്തരാക്കൽ.**

🤖 ഉപയോക്താക്കളെ സംരക്ഷിക്കുന്നതിനും ശാക്തീകരിക്കുന്നതിനും AI യുടെ ഉപയോഗം.

AI (ആർട്ടിഫിഷ്യൽ ഇന്റലിജൻസ്) എന്നത് ഒരു അൽഗോരിതം അടിസ്ഥാനമാക്കിയുള്ള തീരുമാനമെടുക്കൽ സംവിധാനത്തെയാണ് സൂചിപ്പിക്കുന്നത്, ഇത് സാധാരണയായി മനുഷ്യബുദ്ധി ആവശ്യമുള്ള ജോലികൾ ചെയ്യാൻ കഴിയും. ഉദാഹരണത്തിന്, സ്വാഭാവിക ഭാഷാധിഷ്ഠിത പ്രോസസ്സിംഗ് അൽഗോരിതങ്ങൾ ടെക്സ്റ്റ്, ഇമേജ്, വീഡിയോ ഉള്ളടക്കം എന്നിവ വിശകലനം ചെയ്ത് കൃത്രിമം കാണിച്ച ഉള്ളടക്കം കണ്ടെത്തുകയും അസാധാരണമായ പ്രവർത്തനങ്ങളോ ഇടപാടുകളോ ഫ്ലാഗ് ചെയ്യുകയും ചെയ്യുന്നു.

ഇന്ത്യൻ അധികാരികൾ പറയുന്നത്

- **സ്പാം ഫിൽട്ടറിംഗ്: എല്ലാ ടെലികോം ദാതാക്കളും (എയർടെൽ, വോഡഫോൺ പോലുള്ളവ) സ്പാം/അലോസരപ്പെടുത്തുന്ന കോളുകൾ ഫിൽട്ടർ ചെയ്യുന്നതിന് AI ഉപയോഗിക്കണമെന്ന് TRAI ആവശ്യപ്പെടുന്നു.**
- **മ്യൂൾ അക്കൗണ്ട് നിരീക്ഷണം**: സ്കാമുകാരും കള്ളപ്പണം വെളുപ്പിക്കുന്നവരും ഉപയോഗിക്കുന്ന മ്യൂൾ അക്കൗണ്ടുകൾ കണ്ടെത്താൻ ബാങ്കുകളെയും ധനകാര്യ സ്ഥാപനങ്ങളെയും സഹായിക്കുന്ന, അനുബന്ധ സ്ഥാപനമായ ആർബിഐ ഇന്നൊവേഷൻ ഹബ് (ആർബിഐഎച്ച്) നിർമ്മിച്ച ഒരു എഐ മോഡലുമായി സഹകരിക്കാൻ ആർബിഐ ബാങ്കുകളോട് ആവശ്യപ്പെടുന്നു..

.. തുടരുന്നു

അന്താരാഷ്ട്ര ഇൻകമിംഗ് സ്പൂഫ്ഡ് കോളുകൾ തടയൽ സംവിധാനം: ഇന്ത്യയിൽ നിന്ന് വരുന്നതായി തോന്നുന്ന അന്താരാഷ്ട്ര സ്പാം കോളുകൾ കണ്ടെത്തി തടയുന്നതിനുള്ള ഒരു സംവിധാനം ഡിഒടി നടപ്പിലാക്കി. തൽഫലമായി, **"(+91 XXXXX XXXXX)"** എന്ന ഇന്ത്യൻ നമ്പറുകൾ പ്രദർശിപ്പിക്കുന്നതിനായി കോളർ വിശദാംശങ്ങൾ കൃത്രിമം കാണിക്കുന്ന അന്താരാഷ്ട്ര സ്കാമർമാർ യാന്ത്രികമായി തിരിച്ചറിയപ്പെടുകയും തടയപ്പെടുകയും ചെയ്യുന്നു.

🤖 AI പരിഹാരങ്ങൾ പ്രവർത്തനത്തിൽ

എയർടെൽ

സ്പാം ഫിൽട്ടറിംഗ്
ഉപയോഗ രീതികൾ, എസ്എംഎസ് ഫ്രീക്വൻസി, കോൾ ദൈർഘ്യം തുടങ്ങിയ വിവരങ്ങൾ പ്രോസസ്സ് ചെയ്ത് സ്പാം കോളുകളും സന്ദേശങ്ങളും തത്സമയം തിരിച്ചറിയാൻ എയർടെല്ലിന്റെ AI പവർഡ് സ്പാം ഡിറ്റക്ഷൻ ടൂൾ സഹായിക്കുന്നു.

ദോഷകരമായ സന്ദേശങ്ങൾ ഫ്ലാഗ് ചെയ്യുക
സന്ദേശം സംശയാസ്പദമാണെങ്കിൽ വിളിക്കുന്നതിനായി, പങ്കിട്ട ലിങ്ക് ബ്ലാക്ക്‌ലിസ്റ്റ് ചെയ്തിട്ടുണ്ടോ ഇല്ലയോ എന്നതുപോലുള്ള വിവിധ വശങ്ങൾ എയർടെല്ലിന്റെ AI ഉപകരണങ്ങൾ പരിശോധിക്കുന്നു.

ട്രൂകോളർ

AI അസിസ്റ്റന്റ്
ട്രൂകോളർ AI അസിസ്റ്റന്റ് വോയ്സ്-ടു-ടെക്സ്റ്റ് സാങ്കേതികവിദ്യ ഉപയോഗിച്ച് കോളുകൾ സ്ക്രീൻ ചെയ്യുന്നു, വിളിക്കുന്നയാളുടെ ഉദ്ദേശ്യത്തെക്കുറിച്ച് അന്വേഷിക്കുന്നു, സ്പാം കോളുകൾ തിരിച്ചറിയാനും ഏതൊക്കെ കോളുകൾക്ക് മറുപടി നൽകണമെന്ന് തീരുമാനിക്കാനും നിങ്ങളെ സഹായിക്കുന്നു.

സന്ദർഭം തിരയുക
ഫോൺ നമ്പറുകളുടെ പതിവ് പേര് മാറ്റങ്ങൾ പോലുള്ള സംശയാസ്പദമായ പ്രവർത്തനങ്ങൾ തത്സമയം തിരയൽ സന്ദർഭം ഫ്ലാഗ് ചെയ്യുന്നു, ഇത് ഫ്രോഡായ കോളർമാരെ തിരിച്ചറിയാൻ നിങ്ങളെ പ്രാപ്തമാക്കുന്നു..

🔐 രൂപകൽപ്പന അനുസരിച്ചുള്ള സുരക്ഷ

'നിങ്ങളുടെ ഉപകരണം, ഡാറ്റ, നെറ്റ്‌വർക്ക് അടിസ്ഥാന സൗകര്യങ്ങൾ എന്നിവ സുരക്ഷിതമാക്കാൻ അധിക നടപടികൾ സ്വീകരിക്കേണ്ടതില്ലെന്ന് ഉറപ്പാക്കുന്ന തരത്തിൽ സാങ്കേതിക ഉൽപ്പന്നങ്ങൾ നിർമ്മിക്കുന്നത് 'ഡിസൈൻ ബൈ സെക്യൂരിറ്റി' എന്നതിൽ ഉൾപ്പെടുന്നു. ഉൽപ്പന്നങ്ങൾ ഡിസൈൻ വഴി സുരക്ഷിതമാക്കുന്നതിന് രഹസ്യാത്മകത, സമഗ്രത, ലഭ്യത എന്നിവയിൽ ശ്രദ്ധ കേന്ദ്രീകരിക്കേണ്ടതുണ്ട്..

രഹസ്യസ്വഭാവം

രഹസ്യവാക്കുകൾ പോലുള്ള സെൻസിറ്റീവ് വ്യക്തിഗത ഡാറ്റ സ്വകാര്യമായി സൂക്ഷിക്കാൻ എൻക്രിപ്ഷൻ ഉപകരണങ്ങളുടെ ഉപയോഗം.

സമഗ്രത

ഡാറ്റാ ലംഘനങ്ങളും അനധികൃത ആക്സസ്സും തടയുന്നതിനുള്ള സാങ്കേതിക നടപടികളുടെ ഉപയോഗം

ലഭ്യത

ഡാറ്റ ബാക്കപ്പുകളുടെ ലഭ്യതയും സമഗ്രമായ പോസ്റ്റ്-ബ്രീച്ച് ഡാറ്റ വീണ്ടെടുക്കൽ പ്ലാനും ഉറപ്പാക്കുന്നു.

സ്വകാര്യത മെച്ചപ്പെടുത്തുന്ന സാങ്കേതികവിദ്യകൾ (PET-കൾ) നിങ്ങളുടെ ഡാറ്റയെ അനധികൃത ആക്സസ്സിൽ നിന്ന് സംരക്ഷിക്കുന്ന പ്രധാന സുരക്ഷാ ഉപകരണങ്ങളാണ്. എൻക്രിപ്ഷൻ, അജ്ഞാതമാക്കൽ, സുരക്ഷിത കമ്പ്യൂട്ടേഷനുകൾ തുടങ്ങിയ സാങ്കേതിക വിദ്യകൾ സാധാരണയായി PET-യിൽ ഉപയോഗിക്കുന്നു.

ഡാറ്റ ഉപയോഗത്തിന്റെ ആവശ്യകതയും സ്വകാര്യതയുടെ ആവശ്യകതയും സന്തുലിതമാക്കാൻ ഇവ സഹായിക്കുന്നു.

ഇന്ത്യൻ അധികാരികൾ പറയുന്നത്

- **ക്ലൗഡ് സേവനങ്ങൾ**: ഡാറ്റയുടെ ഘടന (ക്രെഡിറ്റ് കാർഡ് നമ്പർ പോലുള്ളവ) നിലനിർത്തിക്കൊണ്ട് വിവരങ്ങൾ സംരക്ഷിക്കുന്നതിന് 'ഫുൾ ഡിസ്ക് എൻക്രിപ്ഷൻ', 'ഫോർമാറ്റ് പ്രിസർവിംഗ് എൻക്രിപ്ഷൻ' തുടങ്ങിയ സുരക്ഷാ നടപടികൾ നടപ്പിലാക്കാൻ MeitY ബിസിനസുകളെ ശുപാർശ ചെയ്യുന്നു.
- **സാമ്പത്തിക സേവനങ്ങൾ:** ബാങ്കുകളും ധനകാര്യ കമ്പനികളും ഇനിപ്പറയുന്നവ ചെയ്യണമെന്ന് ആർബിഐ ആവശ്യപ്പെടുന്നു:
  - മാസ്ക് ഡാറ്റ: ഒരു കാർഡിന്റെ അവസാന നാല് അക്കങ്ങൾ മാത്രം കാണിക്കുന്നത് പോലെ, വിവരങ്ങളുടെ സെൻസിറ്റീവ് ഭാഗങ്ങൾ മറയ്ക്കുക..
  - ഓൺലൈൻ കാർഡ് പേയ്മെന്റുകൾക്ക് CVV + OTP പോലുള്ള ഒരു അധിക സുരക്ഷാ പാളി ചേർക്കാൻ മൾട്ടി-ഫാക്ടർ ഓതന്റിക്കേഷൻ ഉപയോഗിക്കുക..
  - ശക്തമായ എൻക്രിപ്ഷൻ സ്വീകരിക്കുക: ഹാക്കർമാർക്ക് ഡാറ്റ വായിക്കുന്നത് വെല്ലുവിളിയാക്കുന്ന ഉപകരണങ്ങൾ ഉപയോഗിക്കുക..

🔐 പ്രവർത്തനത്തിലുള്ള ഡിസൈൻ പരിഹാരങ്ങൾ വഴിയുള്ള സുരക്ഷ

മൈക്രോസോഫ്റ്റ്

സീറോ-ട്രസ്റ്റ് മോഡൽ
മൈക്രോസോഫ്റ്റിന്റെ സീറോ ട്രസ്റ്റ് മോഡൽ ഓരോ ഡാറ്റ ആക്സസ് അഭ്യർത്ഥനയും സുരക്ഷിതമല്ലാത്ത ഒരു തുറന്ന നെറ്റ്‌വർക്കിൽ നിന്ന് ഉത്ഭവിക്കുന്നതായി പരിശോധിച്ചുറപ്പിക്കുകയും പ്രാമാണീകരിക്കുകയും എൻക്രിപ്റ്റ് ചെയ്യുകയും ചെയ്യുന്നു..

സെക്യുർ ഫ്യൂച്ചർ
ഇനിഷ്യേറ്റീവ്
മൈക്രോസോഫ്റ്റ് ഉൽപ്പന്നങ്ങളിലെ സുരക്ഷാ പരിരക്ഷകൾ സ്വതവേ പ്രാപ്തമാക്കുകയും നടപ്പിലാക്കുകയും ചെയ്യുന്നു, അധിക പരിശ്രമം ആവശ്യമില്ല, കൂടാതെ ഓപ്ഷണൽ അല്ല..

എയർടെൽ

ഫേസ് മാച്ച്
ഐഡന്റിറ്റി മോഷണം അല്ലെങ്കിൽ ഫ്രോഡിങ്ങിലൂടെ ഭീഷണി കണ്ടെത്തിയാൽ, സെൽഫി അടിസ്ഥാനമാക്കിയുള്ള മുഖം തിരിച്ചറിയൽ പരിശോധന സജീവമാക്കുന്ന സുരക്ഷാ അൽഗോരിതങ്ങൾ എയർടെൽ പേയ്മെന്റ്സ് ബാങ്ക് ഉപയോഗിക്കുന്നു.

രാജ്യത്തിന് പുറത്തുനിന്നുള്ള എല്ലാ കോളുകൾക്കും "ഇന്റർനാഷണൽ കോൾ" പ്രദർശിപ്പിക്കുന്ന ഒരു സാങ്കേതിക പരിഹാരം എയർടെൽ നടപ്പിലാക്കുന്നു.

ഇത് അന്താരാഷ്ട്ര കോളുകൾ എളുപ്പത്തിൽ തിരിച്ചറിയാൻ നിങ്ങളെ പ്രാപ്തമാക്കുകയും പ്രതീക്ഷിക്കുന്ന കോളുകളും സാധ്യതയുള്ള കോളുകളും തമ്മിൽ വേർതിരിച്ചറിയാൻ നിങ്ങളെ സഹായിക്കുകയും ചെയ്യുന്നു..

മെറ്റ

എൻഡ്-ടു-എൻഡ് എൻക്രിപ്ഷൻ
അയയ്ക്കുന്നയാൾക്കും സ്വീകർത്താവിനും മാത്രമേ സന്ദേശങ്ങൾ, കോളുകൾ, ഫോട്ടോകൾ, വീഡിയോകൾ എന്നിവ ആക്സസ് ചെയ്യാൻ കഴിയൂ എന്ന് **WhatsApp** ഉറപ്പാക്കുന്നു.

പരിമിതമായ ഡാറ്റ ശേഖരണം
ഫോൺ നമ്പറുകൾ പോലുള്ള അവശ്യ ഡാറ്റ മാത്രമേ **WhatsApp** സംഭരിക്കുന്നുള്ളൂ കൂടാതെ സന്ദേശ ഉള്ളടക്കമോ ലൊക്കേഷൻ ഡാറ്റയോ സ്ഥിരസ്ഥിതിയായി സംഭരിക്കുന്നത് ഒഴിവാക്കുന്നു.

🤝 ഉപയോക്താക്കൾക്കുള്ള പരാതി പരിഹാര ചാനലുകൾ

വ്യക്തവും ലളിതവുമായ പരാതി പരിഹാര സംവിധാനങ്ങൾ, ഡിജിറ്റൽ ബിസിനസുകളുമായി ഇടപഴകുമ്പോൾ നിങ്ങൾ അഭിമുഖീകരിച്ചേക്കാവുന്ന പ്രശ്നങ്ങൾക്ക് സമയബന്ധിതമായ പരിഹാരം ലഭിക്കാൻ നിങ്ങളെപ്പോലുള്ള ഡിജിറ്റൽ സേവനങ്ങളുടെ ഉപയോക്താക്കളെ അനുവദിക്കുന്നു. നിങ്ങളുടെ ഇ-കൊമേഴ്സ് വാങ്ങലിന്റെ ഡെലിവറിയിലെ കാലതാമസം, അല്ലെങ്കിൽ പരാതി പരിഹാര ചാനലുകൾ വഴി ഒരു ക്യാബ് യാത്രയ്ക്ക് പണം നൽകുന്നതിലെ പ്രശ്നങ്ങൾ എന്നിവ ബിസിനസുകൾ പരിഹരിക്കുന്നു.

പരാതി പരിഹാരത്തിനുള്ള സംവിധാനങ്ങൾ

- **സഞ്ചാർ സാഥി:** ടെലികമ്മ്യൂണിക്കേഷൻസ് വകുപ്പ് (DoT) ടെലികോം സ്കാമുകളെ ചെറുക്കാൻ നിങ്ങളെ സഹായിക്കുന്നതിന് വിവിധ സംരംഭങ്ങൾ വാഗ്ദാനം ചെയ്യുന്നു. സഞ്ചാര സാഥി സംരംഭം നിങ്ങളെ അനുവദിക്കുന്നു:
    - ചക്ഷുവിലെ സംശയാസ്പദമായ സ്കാം ആശയവിനിമയങ്ങൾ റിപ്പോർട്ട് ചെയ്യുക (www.sancharsaathi.gov.in/sfc/ സന്ദർശിക്കുക);
    - നിങ്ങളുടെ പേരിൽ നൽകിയിട്ടുള്ള എല്ലാ മൊബൈൽ കണക്ഷനുകളും തിരിച്ചറിയുകയും കൈകാര്യം ചെയ്യുകയും ചെയ്യുക;
    - നഷ്ടപ്പെട്ട/മോഷ്ടിക്കപ്പെട്ട മൊബൈൽ ഹാൻഡ്സെറ്റ് റിപ്പോർട്ട് ചെയ്യുക, അതുവഴി അവ ബ്ലോക്ക് ചെയ്യാനും കണ്ടെത്താനും വീണ്ടെടുക്കാനും കഴിയും..
- **ധനകാര്യ മേഖല നിരീക്ഷണ കേന്ദ്രം:** ആർബിഐയുടെ സംയോജിത ഓംബുഡ്സ്മാൻ പദ്ധതി ഒരു കേന്ദ്രീകൃത പരാതി പരിഹാര സംവിധാനം സൃഷ്ടിക്കുന്നു, ഇത് ബാങ്കുകൾ, പേയ്മെന്റ് സേവന ദാതാക്കൾ, ക്രെഡിറ്റ് ബ്യൂറോകൾ, മറ്റ് ധനകാര്യ സ്ഥാപനങ്ങൾ എന്നിവയ്ക്കെതിരെ ആർബിഐയിൽ പരാതിപ്പെടാൻ നിങ്ങളെ അനുവദിക്കുന്നു..

.. തുടരുന്നു

- **ഉപഭോക്തൃ ഹെൽപ്പ്ലൈൻ:** ബിസിനസുകൾക്കും സേവന ദാതാക്കൾക്കുമെതിരായ പരാതികൾ പരിഹരിക്കുന്നതിന് ഉപഭോക്തൃ കാര്യ വകുപ്പ് (DoCA) നിങ്ങൾക്ക് ഒന്നിലധികം ചാനലുകൾ വാഗ്ദാനം ചെയ്യുന്നു: വാട്ട്സ്ആപ്പ്-സംയോജിത ഹെൽപ്പ്ലൈൻ നമ്പർ (8800001915), നാഷണൽ കൺസ്യൂമർ ഹെൽപ്പ്ലൈൻ വെബ് പോർട്ടൽ (www.consumerhelpline.gov.in), UMANG ആപ്പ് എന്നിവ ഇതിൽ ഉൾപ്പെടുന്നു.
- **ഇടനില മാർഗ്ഗനിർദ്ദേശങ്ങൾ:** സോഷ്യൽ മീഡിയ, ഗെയിമിംഗ് കമ്പനികൾ പോലുള്ള ഡിജിറ്റൽ പ്ലാറ്റ്ഫോമുകൾ പരാതി പരിഹാര സംവിധാനങ്ങൾ സ്ഥാപിക്കുകയും ഉപഭോക്തൃ പരാതികൾ സമയബന്ധിതമായി പരിഹരിക്കുകയും ചെയ്യണമെന്ന് MeitY ആവശ്യപ്പെടുന്നു. കമ്പനിയുടെ പരാതി പരിഹാര പ്രക്രിയയിൽ നിങ്ങൾ തൃപ്തനല്ലെങ്കിൽ, സർക്കാർ നിയമിച്ച പരാതി അപ്പലേറ്റ് കമ്മിറ്റിക്ക് (GAC) നിങ്ങൾക്ക് ഒരു ഇ-പരാതി ഫയൽ ചെയ്യാം..

🤝 പരാതി പരിഹാര മാർഗങ്ങൾ പ്രവർത്തനത്തിലുള്ളത്

വോഡഫോൺ ഐഡിയ (VI)

സ്പെഷ്യലൈസ്ഡ് ഹെൽപ്പ്ലൈനുകൾ
മൊബൈൽ നമ്പർ പോർട്ടബിലിറ്റി, ഡാറ്റ ആക്ടിവേഷൻ തുടങ്ങിയ നിങ്ങളുടെ വ്യത്യസ്ത ആവശ്യകതകളെ അടിസ്ഥാനമാക്കി സ്പെഷ്യലൈസ്ഡ് ഹെൽപ്പ്ലൈനുകൾ Vi വാഗ്ദാനം ചെയ്യുന്നു.

മൈ VI ആപ്പ്
വിവിധ ഉൽപ്പന്ന, സുരക്ഷാ ഓപ്ഷനുകൾ ആക്സസ് ചെയ്യാൻ MyVi ആപ്പ് നിങ്ങളെ അനുവദിക്കുന്നു. നിങ്ങൾക്ക് ശല്യപ്പെടുത്തരുത് (DND) സൗകര്യം തിരഞ്ഞെടുക്കാനും ടെലിമാർക്കറ്റർമാർക്കെതിരെ പരാതിപ്പെടാനും കസ്റ്റമർ കെയർ എക്സിക്യൂട്ടീവുകൾക്ക് സേവന അഭ്യർത്ഥനകളും പരാതികളും നൽകാനും കഴിയും..

എയർടെൽ

എയർടെൽ താങ്ക്സ് ആപ്പ്
അനാവശ്യ നമ്പറുകൾ കൈകാര്യം ചെയ്യാനും / തടയാനും, ക്ഷുദ്രകരമായ പ്രവർത്തനങ്ങൾ റിപ്പോർട്ട് ചെയ്യാനും, മാർക്കറ്റിംഗ് സന്ദേശങ്ങൾ ഒഴിവാക്കാൻ ശല്യപ്പെടുത്തരുത് (DND) സേവനം തിരഞ്ഞെടുക്കാനും എയർടെൽ താങ്ക്സ് ആപ്പ് നിങ്ങളെ അനുവദിക്കുന്നു.

പരാതികൾക്കായുള്ള ദ്വിതല അപ്പലേറ്റ് അതോറിറ്റി
പരിഹാരത്തിൽ നിങ്ങൾ അതൃപ്തനാണെങ്കിൽ, 30 ദിവസത്തിനുള്ളിൽ സേവന മേഖല അടിസ്ഥാനമാക്കിയുള്ള അപ്പലേറ്റ് അതോറിറ്റിക്ക് മുമ്പാകെ അപ്പീൽ നൽകാം..

💪 ഇന്റർനെറ്റ് ഉപയോക്താക്കളെ ശാക്തീകരിക്കുന്നതിനുള്ള അലേർട്ടുകളും ഉപകരണങ്ങളും

ബിസിനസുകൾ അവരുടെ ആപ്പുകളിലും ഡിജിറ്റൽ സേവനങ്ങളിലും ഡിസൈൻ സവിശേഷതകൾ സംയോജിപ്പിക്കുന്നു, ഇത് നിങ്ങളുടെ ഡാറ്റയിൽ ശ്രദ്ധ പുലർത്താനും സ്വകാര്യത, സുരക്ഷാ ക്രമീകരണങ്ങൾ ക്രമീകരിക്കാനും മുൻകരുതലോടെ ഇരിക്കാനും നിങ്ങളെ സഹായിക്കുന്നു.

മൂന്നാം കക്ഷികളുമായി നിങ്ങളുടെ വിവരങ്ങൾ എങ്ങനെ പങ്കിടുന്നുവെന്ന് പരിശോധിക്കാനും നിയന്ത്രിക്കാനും, ഏതൊക്കെ വിവരങ്ങൾ പങ്കിടണമെന്നും എന്തൊക്കെ സ്വകാര്യമായി സൂക്ഷിക്കണമെന്നും തീരുമാനിക്കാനും, ആരെങ്കിലും നിങ്ങളുടെ അക്കൗണ്ട് ആക്സസ് ചെയ്യാൻ ശ്രമിക്കുന്നത് പോലുള്ള സംശയാസ്പദമായ പ്രവർത്തനങ്ങളെക്കുറിച്ച് അറിയിപ്പ് നേടാനും ഇത് നിങ്ങളെ സഹായിക്കുന്നു.

ഇന്ത്യൻ അധികാരികൾ പറയുന്നത്

- **ആവർത്തിച്ചുള്ള പേയ്മെന്റുകൾക്കുള്ള ഇടപാട് അറിയിപ്പുകൾ:** സബ്സ്ക്രിപ്ഷനുകൾ അല്ലെങ്കിൽ സിസ്റ്റമാറ്റിക് നിക്ഷേപ പദ്ധതികൾ പോലുള്ള ആവർത്തിച്ചുള്ള പേയ്മെന്റുകൾ പ്രോസസ്സ് ചെയ്യുന്നതിന് കുറഞ്ഞത് 24 മണിക്കൂർ മുമ്പെങ്കിലും അറിയിപ്പുകൾ നൽകാൻ ബാങ്കുകൾക്ക് RBI നിർദ്ദേശം നൽകുന്നു.
- **ഇനം തിരിച്ചുള്ള സ്വകാര്യതാ അറിയിപ്പുകൾ:** നിങ്ങളിൽ നിന്ന് അവർ ഏത് തരത്തിലുള്ള വ്യക്തിഗത ഡാറ്റയാണ് ശേഖരിക്കുന്നതെന്നും ശേഖരണത്തിന്റെ ഉദ്ദേശ്യത്തെക്കുറിച്ചും ബിസിനസുകൾ വ്യക്തവും വ്യക്തവുമായിരിക്കണമെന്ന് ഇലക്ട്രോണിക്സ് ആൻഡ് ഇൻഫർമേഷൻ ടെക്നോളജി മന്ത്രാലയം (MeitY) ആവശ്യപ്പെടുന്നു.
- **സ്പാം/ശല്യപ്പെടുത്തുന്ന കോളുകൾ തടയുന്നതിന് TRAI നിയമങ്ങൾ:** ആപ്പുകളിലേക്കും വെബ്സൈറ്റുകളിലേക്കും ലിങ്കുകൾ അടങ്ങിയ ബൾക്ക് ടെക്സ്റ്റുകൾ അയയ്ക്കുന്ന കമ്പനികൾ ടെലികോം ദാതാക്കളിൽ അവരുടെ ഉള്ളടക്കം രജിസ്റ്റർ ചെയ്യണമെന്ന് TRAI നിർദ്ദേശിക്കുന്നു. പരിശോധിച്ചുറപ്പിച്ചതും വൈറ്റ്ലിസ്റ്റ് ചെയ്തതുമായ ലിങ്കുകളും അറ്റാച്ച്മെന്റുകളും മാത്രമേ പ്രൊമോഷണൽ സന്ദേശങ്ങളിൽ പൊതുജനങ്ങൾക്ക് പ്രചരിപ്പിക്കുന്നുള്ളൂ എന്ന് ഇത് ഉറപ്പാക്കുന്നു.
- **ഇരുണ്ട പാറ്റേണുകളിൽ നിന്നുള്ള സംരക്ഷണം:** ബിസിനസുകൾ ഉപയോഗിക്കുന്ന ഫ്രോഡായ ഡിസൈൻ പാറ്റേണുകൾ അന്യായമായ വ്യാപാര രീതിയായി കാണാമെന്ന് ഉപഭോക്തൃ കാര്യ വകുപ്പ് (DoCA) പറയുന്നു.
  - ഫ്രോഡായ ഡിസൈനുകളുടെ ഉദാഹരണങ്ങളിൽ ആവർത്തിച്ചുള്ള ഇടപാട്റദ്ദാക്കുന്നത് ബുദ്ധിമുട്ടാക്കുന്ന സങ്കീർണ്ണമായ ഉപയോക്തൃ ഇന്റർഫേസുകൾ (UI) ഉള്ള ആപ്പുകൾ, ചെക്ക്ഔട്ടിന് തൊട്ടുമുമ്പ് മറഞ്ഞിരിക്കുന്ന ചാർജുകളും അധിക ഫീസുകളും ചേർക്കുന്ന ആപ്പുകൾ എന്നിവ ഉൾപ്പെടുന്നു.
  - അത്തരം ഫ്രോഡായ ഡിസൈനുകൾ പ്രവർത്തനത്തിൽ കാണുകയാണെങ്കിൽ, 1915 ഡയൽ ചെയ്യുകയോ INGRAM പോർട്ടൽ (www.consumerhelpline.gov.in/user/) സന്ദർശിക്കുകയോ ചെയ്തുകൊണ്ട് നിങ്ങൾക്ക് DoCA-യിൽ പരാതിപ്പെടാം.

💪 ഇന്റർനെറ്റ് ഉപയോക്താക്കളെ പ്രവർത്തനത്തിൽ ശാക്തീകരിക്കുന്നതിനുള്ള ഉപകരണങ്ങൾ

മൈക്രോസോഫ്റ്റ്

കോപൈലറ്റ് നിയന്ത്രണങ്ങൾ
കോപൈലറ്റിൽ നിങ്ങൾക്ക് മുൻഗണനകൾ സജ്ജമാക്കാനും ഡാറ്റ കാണാനും എഡിറ്റ് ചെയ്യാനും ഇല്ലാതാക്കാനും സംഭാഷണ ചരിത്രങ്ങൾ കൈകാര്യം ചെയ്യാനും കഴിയും.

സ്കൈപ്പിൽ സ്വകാര്യതയും റിപ്പോർട്ടിംഗും
നിങ്ങൾക്ക് സ്കൈപ്പിൽ ദോഷകരമായ സന്ദേശങ്ങൾ റിപ്പോർട്ട് ചെയ്യാനും സംശയാസ്പദമായ സന്ദേശങ്ങൾ തടയാനും റിപ്പോർട്ട് ചെയ്യാനും കഴിയും..

മെറ്റ

സ്വകാര്യതാ കേന്ദ്രം
ഫേസ്ബുക്ക്, ഇൻസ്റ്റാഗ്രാം, മെസഞ്ചർ, മറ്റ് മെറ്റാ ഉൽപ്പന്നങ്ങൾ എന്നിവയിൽ നിങ്ങളുടെ സ്വകാര്യത കൈകാര്യം ചെയ്യുന്നതിനും നിയന്ത്രിക്കുന്നതിനുമായി നിങ്ങൾക്ക് ക്രമീകരണങ്ങൾ ക്രമീകരിക്കാൻ കഴിയും.

വാട്ട്സ്ആപ്പ് സ്വകാര്യതാ നിയന്ത്രണങ്ങൾ
നിങ്ങളുടെ പ്രൊഫൈൽ ഫോട്ടോ, അവസാനം കണ്ട വിശദാംശങ്ങൾ എന്നിവ ആരൊക്കെ കാണണമെന്ന് നിങ്ങൾക്ക് ഇഷ്ടാനുസൃതമാക്കാനും വാട്ട്സ്ആപ്പിൽ ചാറ്റുകൾ ലോക്ക് ചെയ്യാനും കഴിയും.

ട്രൂകോളർ

കോളർ ഐഡി
ട്രൂകോളറിന്റെ കോളർ ഐഡി പേരുകൾ കാണിക്കുന്നതിനപ്പുറം പോകുന്നു—ഇത് വിളിക്കുന്നയാളുടെ സ്ഥാനം, കമ്മ്യൂണിറ്റി റേറ്റിംഗുകൾ, ഫ്രോഡ് അലേർട്ടുകൾ എന്നിവ നൽകുന്നു സംശയാസ്പദമായ കോളുകൾ “സ്പാം” അല്ലെങ്കിൽ” ഫ്രോഡ് അലേർട്ട്” പോലുള്ള ലേബലുകൾ ഉപയോഗിച്ച് ഫ്ലാഗ് ചെയ്യുന്നു, ഇത് നിങ്ങളെ വിവരമുള്ള തീരുമാനങ്ങൾ എടുക്കാൻ സഹായിക്കുന്നു.

പരിശോധിച്ചുറപ്പിച്ച ബിസിനസ് ഐഡികൾ
ട്രൂകോളർ ബിസിനസ് കോളുകളിൽ ഒരു കൃത്രിമം കാണിക്കാത്ത പേര്, പച്ച ബാഡ്ജ്, ലോഗോ എന്നിവ ചേർക്കുന്നു, ഇത് ആൾമാറാട്ട സ്കാമുകൾ തടയുകയും യഥാർത്ഥ കോളർമാരെ ഫ്രോഡായവരിൽ നിന്ന് വേർതിരിച്ചറിയാൻ നിങ്ങളെ സഹായിക്കുകയും ചെയ്യുന്നു.

SAFER INTERNET INDIA

സന്ദർശിക്കുക: www.saferinternetindia.com
ഞങ്ങൾക്ക് എഴുതുക secretariat@saferinternetindia.com

Safer Internet India
@saferinternetindia
SaferInternetIN
@SaferInternetIndia