തട്ടിപ്പുകാർ ഇവിടെയും, എവിടെയുമുണ്ട്

ഒരിടത്തും കെണിയിൽ വീഴരുത്!

#BankingDhyaanSe 2.0

AXIS BANK

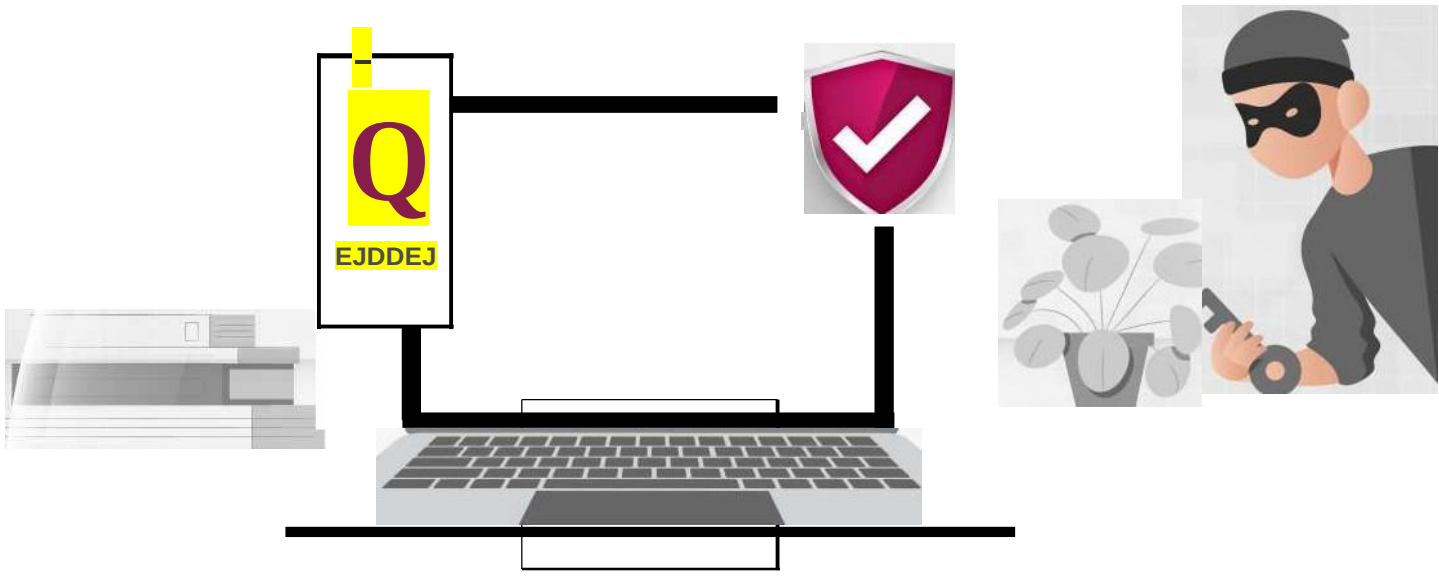
നിങ്ങൾ സമ്പാദിക്കാനായി കഠിനാദ്ധ്വാനം ചെയ്യുന്നു,
എങ്കിൽ പിന്നെ നിങ്ങളുടെ വരുമാനം എന്തുകൊണ്ട് സുരക്ഷിതമായി സൂക്ഷിച്ചുകൂടാ?

ആക്സിസ് ബാങ്ക് തട്ടിപ്പ് ബോധവൽക്കരണ ബുക്ക്ലെറ്റ് #BankingDhyaanSe 2.0-ലേക്ക് സ്വാഗതം **.**

സാമ്പത്തിക തട്ടിപ്പുകൾ മനസിലാക്കുന്നതിനും തടയുന്നതിനുമുള്ള നിങ്ങളുടെ താക്കോൽ. അതിവേഗം പരിണമിച്ചുകൊണ്ടിരിക്കുന്ന ഡിജിറ്റൽ യുഗത്തിൽ, അറിവാണ് തട്ടിപ്പുകാർക്കെതിരായ നിങ്ങളുടെ സംരക്ഷണം. നിങ്ങൾ കഠിനാധ്വാനം ചെയ്ത് സമ്പാദിച്ച പണം സംരക്ഷിക്കുന്നതിനുള്ള ഉൾക്കാഴ്ചകൾ, യഥാർത്ഥ ജീവിതത്തിലെ ഉദാഹരണങ്ങൾ, പ്രായോഗിക നുറുങ്ങുകൾ എന്നിവ ഈ ഗൈഡ്ബുക്ക് നിങ്ങൾക്ക് നൽകുന്നു.

ബാങ്കിംഗിലെ നിങ്ങളുടെ വിശ്വസ്തനായ പങ്കാളി എന്ന നിലയിൽ, ഡിജിറ്റൽ മേഖലയിൽ ആത്മവിശ്വാസത്തോടെ മുന്നേറാൻ നിങ്ങളെ സഹായിക്കുന്നതിന് ആക്സിസ് ബാങ്ക് പ്രതിജ്ഞാബദ്ധമാണ്. വഞ്ചനയിൽ നിന്ന് സുരക്ഷ നേടുകയും, നമുക്കൊരുമിച്ച് ശോഭനമായ സാമ്പത്തിക ഭാവി സുരക്ഷിതമാക്കുകയും ചെയ്യാം.

OTP തട്ടിപ്പുകൾ



നിങ്ങളുടെ പ്രവേശനസാധ്യമല്ലാത്ത ഡിജിറ്റൽ സാമ്രാജ്യത്തിലേക്ക് പ്രവേശനം നേടാനുള്ള ഒരു സ്വർണ്ണ താക്കോലാണ് ആണ് ഒറ്റത്തവണ പാസ്‌വേഡ്.

നിങ്ങളുടെ വിലയേറിയ താക്കോൽ മോഷ്ടിക്കുന്നതിൽ നിന്ന് കൗശലക്കാരായ വഞ്ചകരെ തടയാൻ, നിങ്ങൾ നിങ്ങളുടെ കോട്ടയുടെ കാവൽക്കാരനായിരിക്കണം!

OTP-കൾ രഹസ്യമായി സൂക്ഷിക്കുക: ഫോൺ കോളുകൾ, ഇമെയിലുകൾ, ടെക്സ്റ്റ് മെസേജുകൾ അല്ലെങ്കിൽ സോഷ്യൽ മീഡിയ എന്നിവയിലൂടെ ഒരിക്കലും ആരുമായും OTP-കൾ പങ്കിടരുത്, ഒരു കാവൽക്കാരനെപ്പോലെ ജാഗ്രത പാലിക്കുക.

അഭ്യർത്ഥനകൾ പരിശോധിച്ചുറപ്പാക്കുക: വിശ്വസിക്കുക, പക്ഷേ പരിശോധിച്ചുറപ്പാക്കണം. ഒരു OTP അഭ്യർത്ഥന നീലനിറത്തിൽ നിന്ന് പോപ്പ് അപ്പ് ചെയ്യുകയോ ഫിഷിംഗ് ആയി തോന്നുകയോ ചെയ്താൽ, തിരക്കുകൂട്ടരുത്. പ്രതികരിക്കുന്നതിന് മുമ്പ് അതിന്റെ ആധികാരികത രണ്ടുവട്ടം പരിശോധിക്കുക.

ഔദ്യോഗിക വെബ്സൈറ്റുകൾ അല്ലെങ്കിൽ ആപ്പുകൾ ഉപയോഗിക്കുക: OTP-കൾ പങ്കിടുമ്പോൾ സുരക്ഷിതരായിരിക്കുക. എല്ലായ്പ്പോഴും ഔദ്യോഗിക സൈറ്റ് അല്ലെങ്കിൽ ആപ്പ് നേരിട്ട് സന്ദർശിക്കുക - കുറുക്കുവഴികൾ ഉപയോഗിക്കരുത്. ഏത് ദിവസവും ടൈപ്പ് ചെയ്യുന്നത് വഴി ലിങ്ക് ക്ലിക്ക് ചെയ്യുന്നത് ഒഴിവാക്കുക.

അടിയന്തര അഭ്യർത്ഥനകളിൽ ജാഗ്രത പാലിക്കുക: നിങ്ങളുടെ OTP പങ്കിടുന്നതിന് നിങ്ങളെ സമ്മർദ്ദത്തിലാക്കാനായി സ്കാമർമാർ പലപ്പോഴും അടിയന്തിര സാഹചര്യങ്ങൾ സൃഷ്ടിക്കുന്നു. ഒരു ചുവട് പിന്നോട്ട് പോകുക, വിമർശനാത്മകമായി ചിന്തിക്കുക, നടപടിയെടുക്കും മുമ്പ് അഭ്യർത്ഥന സ്വതന്ത്രമായി പരിശോധിക്കുക.

ടു-ഫാക്ടർ ഓതന്റിക്കേഷൻ പ്രവർത്തനക്ഷമമാക്കുക: 2FA (ടു-ഫാക്ടർ ആധികാരികത) ഉപയോഗിച്ച് സുരക്ഷ ഇരട്ടിയാക്കുക. ആപ്പ് അധിഷ്ഠിതമോ അല്ലെങ്കിൽ ഹാർഡ്‌വെയർ ടോക്കണുകളോ പോലുള്ള നല്ല ഉറപ്പുള്ള ഓപ്ഷനുകൾ തിരഞ്ഞെടുക്കുക. എല്ലാ ദിവസവും MS OTP-കളെ മറികടക്കും.

ബാങ്ക് നിങ്ങളുടെ CVV, OTP, PIN, കാർഡ് നമ്പർ, പാസ്‌വേഡുകൾ തുടങ്ങിയ ചോദിക്കില്ലെന്ന കാര്യം ഓർമ്മിക്കുക. ഈ വിവരങ്ങൾ ആരുമായും പങ്കിടരുത്.

ക്രെഡിറ്റ് കാർഡ് തട്ടിപ്പുകൾ

ക്രെഡിറ്റ് കാർഡ് തട്ടിപ്പുകൾ ഒളിച്ച് കളിക്കുന്ന ഒരു ഗെയിമായി നമുക്ക് സങ്കൽപ്പിക്കാം. എങ്ങനെ ഒരു സ്കാമർ എങ്ങനെയാണോ അവരുടെ യഥാർത്ഥ ഉദ്ദേശ്യങ്ങൾ മറച്ചുവയ്ക്കുന്നത് അത് പോലെ തന്നെ, നിങ്ങളുടെ ക്രെഡിറ്റ് കാർഡ് വിവരങ്ങൾ വെളിപ്പെടുത്താൻ അവർ നിങ്ങളെ കബളിപ്പിച്ചേക്കാം.

അവരുടെ കെണിയിൽ വീഴാതിരിക്കാൻ, ചുവടെ പറയുന്ന നുറുങ്ങുകൾ ശ്രദ്ധിക്കുക:

ഫിഷർമാരെ ശ്രദ്ധിക്കുക: സ്കാമർമാർ നിങ്ങളുടെ ബാങ്കിൽ നിന്നോ പരിചയമുള്ള കമ്പനിയിൽ നിന്നോ ആണെന്ന് ഭാവിച്ചേക്കാം. അവരുടെ തന്ത്രങ്ങളിൽ വീഴരുത്.; അവരുടെ ഐഡന്റിറ്റി പരിശോധിച്ചുറപ്പാക്കുക.

നിങ്ങളുടെ സ്റ്റേറ്റ്മെന്റുകൾ പരിശോധിക്കുക: നിങ്ങളുടെ ക്രെഡിറ്റ് കാർഡ് സ്റ്റേറ്റ്മെന്റുകൾ പതിവായി പരിശോധിക്കുക. നിങ്ങൾക്ക് അറിയാത്ത ചെലവുകൾ അല്ലെങ്കിൽ നിരക്കുകൾ കണ്ടെത്തിയാൽ, അത്ഗെയിമിൽ മറഞ്ഞിരിക്കുന്ന കളിക്കാരെ കണ്ടെത്തുന്നത് പോലെയാണ് - അവരെ ഉടൻ പുറത്തു കൊണ്ടുവരുക.

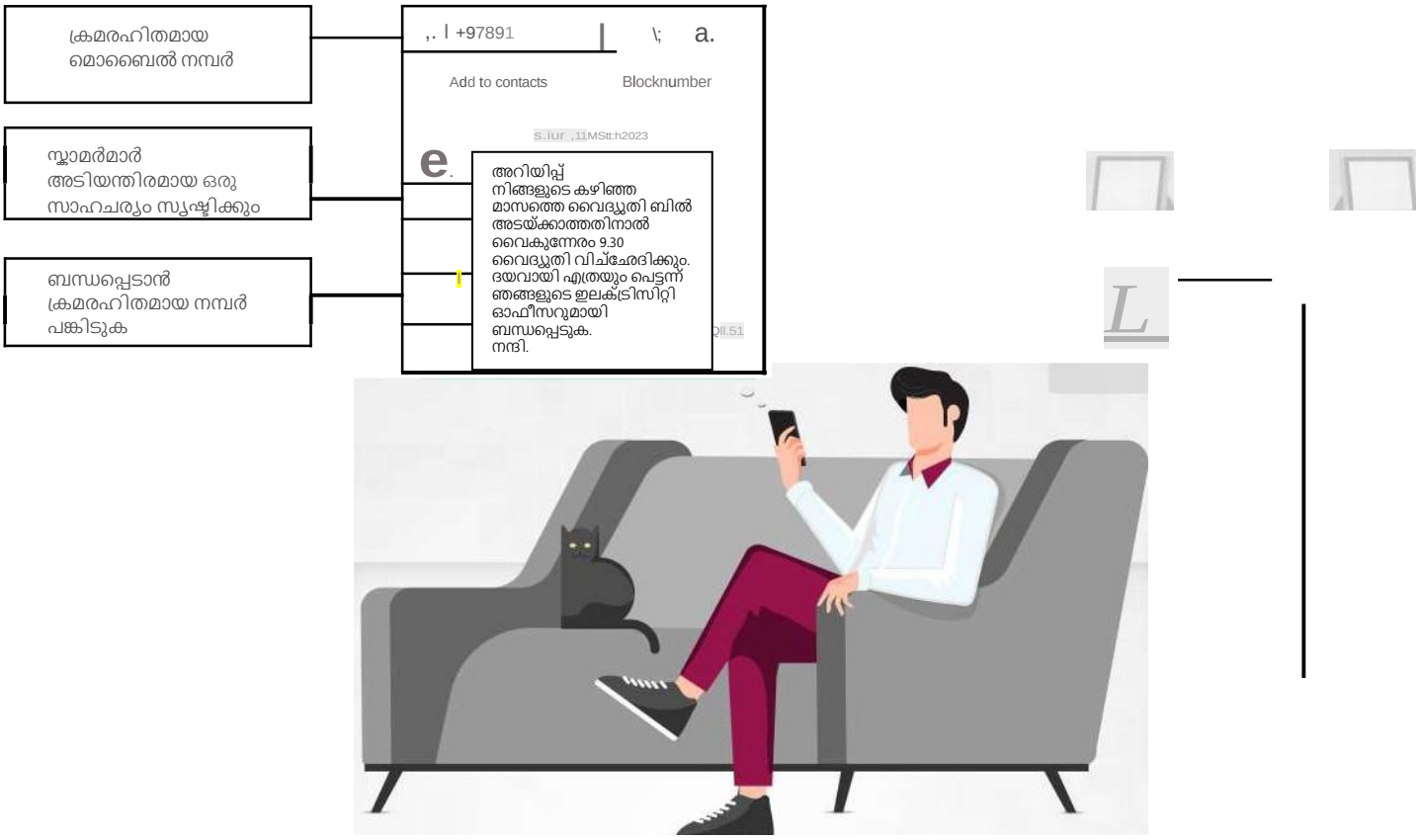
ഇടപാട് പരിധി സജ്ജമാക്കുക: നിങ്ങളുടെ എല്ലാ പേയ്മെന്റ് ചാനലുകളിലും ഇടപാട് പരിധി സജ്ജമാക്കുക, നിങ്ങളുടെ ആവശ്യാനുസരണം 'ഉപയോഗം മാനേജ് ചെയ്യുക' വിഭാഗം ഇഷ്ടാനുസൃതമാക്കുക.

സുരക്ഷിതമായ സൈറ്റുകൾ മാത്രം: ഓൺലൈനിൽ ഷോപ്പിംഗ് നടത്തുമ്പോൾ, വെബ്സൈറ്റ് സുരക്ഷിതമാണെന്ന് ഉറപ്പാക്കുക (URL-ൽ "https" ഉണ്ടോയെന്ന് നോക്കുക). കളിക്കായി ഒരു സുരക്ഷിതമായ കളിസ്ഥലം തിരഞ്ഞെടുക്കുന്നത് പോലെയാണ് ഇത്.

അപ്ഡേറ്റായിരിക്കുക: നിങ്ങൾ ഗെയിമിൽ പുതിയ തന്ത്രങ്ങൾ പഠിക്കുന്നതുപോലെ ഏറ്റവും പുതിയ തട്ടിപ്പ് തന്ത്രങ്ങൾ ശ്രദ്ധിച്ചുകൊണ്ടിരിക്കുക. ഇത്തരത്തിൽ, നിങ്ങൾ സ്കാമർമാരെ മറികടക്കാൻ തയ്യാറാകും.

ഇലക്ട്രിസിറ്റി തട്ടിപ്പുകൾ

ഒരു വ്യാജ SMS എങ്ങനെ തിരിച്ചറിയാം?



ഇങ്ങനെ സങ്കൽപ്പിക്കുക: നിങ്ങൾ സായാഹ്നം ആസ്വദിച്ച് വീട്ടിൽ വിശ്രമിക്കുകയും, ടിവിയിൽ പ്രിയപ്പെട്ട ഷോ കാണുകയുമാണ്, അപ്പോൾ നിങ്ങളുടെ ഫോണിൽ ഇൻകമിംഗ് സന്ദേശം വന്നതിന്റെ ശബ്ദം കേൾക്കുന്നു. അത് നിങ്ങളുടെ വൈദ്യുതി ദാതാവാണ്, നിങ്ങളുടെ ഏറ്റവും പുതിയ ബില്ലിൽ നിങ്ങൾ വലിയ ഒരു അടയ്ക്കേണ്ടതുണ്ടെന്ന് അവർ പറയുന്നു.

നിങ്ങൾ പരിഭ്രാന്തരാകുന്നതിന് മുമ്പ്, ഇനി പറയുന്നത് ശ്രദ്ധിക്കുക: വൈദ്യുതി ബിൽ തട്ടിപ്പ്, ഒരു ഗൂഢാലോചന പോലെ, ഒരു മുന്നറിയിപ്പുമില്ലാതെ നിങ്ങളുടെ ജീവിതത്തിലേക്ക് കടന്നുവന്നേക്കാം.

F) LW നിങ്ങളുടെ രഹസ്യാത്മകമായ വിശദാംശങ്ങൾ ഒരിക്കലും ആരുമായും പങ്കിടരുത്, അല്ലെങ്കിൽ ആവശ്യപ്പെടാത്ത ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യരുത്.

[!...- •! ബില്ലുകൾ അടയ്ക്കുന്നതിന് ഔദ്യോഗികവും സുരക്ഷിതവുമായ വെബ്സൈറ്റുകൾ മാത്രം ഉപയോഗിക്കുക.

ക്രമരഹിതമായ/രജിസ്റ്റർ ചെയ്യാത്ത നമ്പറുകളിലൂടെ വൈദ്യുതി വകുപ്പ് ഒരിക്കലും വ്യക്തിഗത വിവരങ്ങളോ പേയ്മെന്റുകളോ ആവശ്യപ്പെടില്ല.

ജോലി തട്ടിപ്പുകൾ

നിങ്ങൾ ജോലികളുടെ ലിസ്റ്റിലൂടെ സ്ക്രോൾ ചെയ്യുകയാണെന്ന് സങ്കൽപ്പിക്കുക, പെട്ടെന്ന് വളരെ സത്യസന്ധമാണെന്ന് തോന്നുന്ന നിങ്ങൾ ഒരു ജോലി ഓഫർ ശ്രദ്ധയിൽപ്പെടുന്നു. പരിധിയില്ലാത്ത അവധി ദിവസങ്ങൾ, നിങ്ങളുടെ ഇഷ്ട വേഷത്തിലുള്ള ജോലി, ഡാറ്റാ എൻട്രിക്ക് ആറക്ക ശമ്പളം? സൈൻ അപ്പ് ചെയ്യൂ!

നിങ്ങൾ "ഇപ്പോൾ അപേക്ഷിക്കുക" ബട്ടൺ അമർത്തുന്നതിന് മുമ്പ് ഒന്നു നിൽക്കൂ!

കമ്പനിയെ കുറിച്ച് അന്വേഷിക്കുക: കമ്പനിയെ ഓൺലൈനിൽ തിരയുക, അത് സൽപ്പേരുള്ളതാണെന്ന് ഉറപ്പാക്കുക. സ്കാമർമാർ പലപ്പോഴും വിശ്വാസ്യത തോന്നിപ്പിക്കുന്ന വെബ്സൈറ്റുകൾ സഹിതം വ്യാജ കമ്പനികൾ സൃഷ്ടിക്കുന്നു.

മുൻകൂറായി പണം നൽകരുത്: നിയമപരമായ തൊഴിലുടമകൾ നിങ്ങൾ ജോലി ആരംഭിക്കുന്നതിന് മുമ്പ് പരിശീലനം, മെറ്റീരിയലുകൾ അല്ലെങ്കിൽ പശ്ചാത്തല പരിശോധനകൾ എന്നിവയ്ക്ക് പണം നൽകാൻ ആവശ്യപ്പെടില്ല.

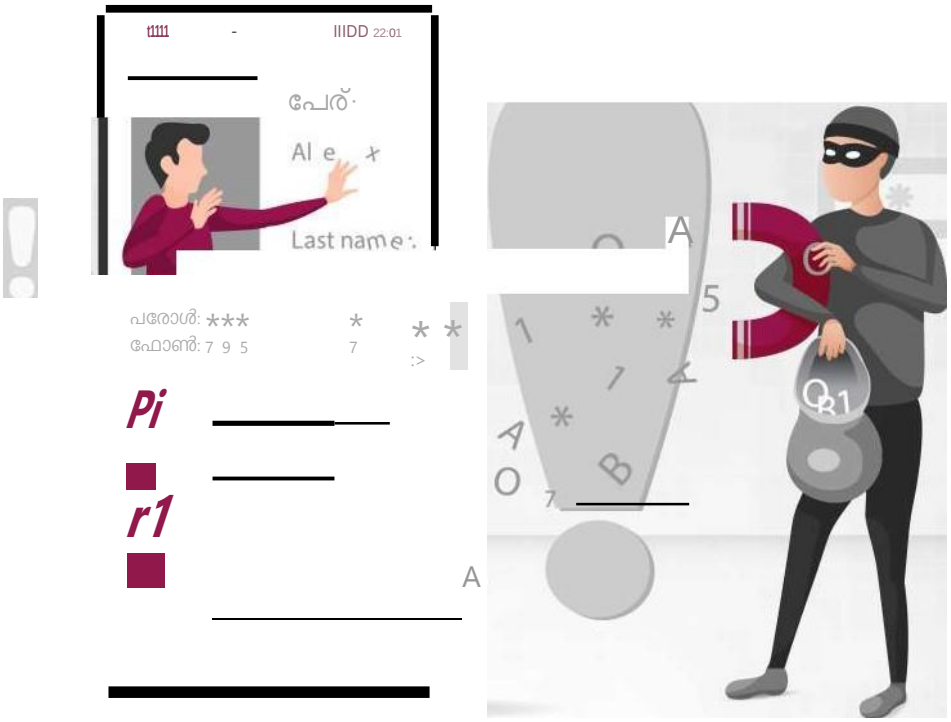
അപകട സൂചനകൾക്കായി നോക്കുക: നിങ്ങളുടെ സോഷ്യൽ സെക്യൂരിറ്റി നമ്പർ അല്ലെങ്കിൽ സാമ്പത്തിക വിവരങ്ങൾ പോലുള്ള സെൻസിറ്റീവായ വിവരങ്ങൾ ഉടൻ നൽകണമെങ്കിൽ ജാഗ്രത പാലിക്കുക.

വളരെ വേഗത്തിലുള്ള നിയമനം: ഒരു അഭിമുഖം അല്ലെങ്കിൽ അധികം വിവരങ്ങൾ നൽകാതെ അപ്പോൾ തന്നെ ജോലി വാഗ്ദാനം ചെയ്യുകയാണെങ്കിൽ അത് ഒരു തട്ടിപ്പ് ആകാം.

നിങ്ങളുടെ നൈസർഗ്ഗികമായ തോന്നലുകളെ വിശ്വസിക്കുക: എന്തെങ്കിലും ശരിയല്ലായെന്ന് തോന്നുകയാണെങ്കിൽ, നിങ്ങളുടെ തോന്നലിൽ വിശ്വസിക്കുക, ജാഗ്രതയോടെ മുന്നോട്ട് പോകുകയോ ഒഴിവാക്കുകയോ ചെയ്യുക.

ഓർക്കുക, തൊഴിൽ അന്വേഷണം നിങ്ങളുടെ പ്രഥമ മുൻഗണന ആയിരിക്കുമ്പോൾ തന്നെ, നിങ്ങളുടെ വ്യക്തിപരവും സാമ്പത്തികവുമായ വിവരങ്ങൾ പരിരക്ഷിക്കുക.

കോൾ സ്പൂഫിംഗ് തട്ടിപ്പുകൾ



ഒരു മാന്ത്രികന് എങ്ങനെ കാര്യങ്ങൾ യഥാർത്ഥത്തിൽ ഉള്ളതിൽ നിന്ന് വ്യത്യസ്തമായി കാണിക്കാനാനാവുമെന്നത് പോലെ തന്നെ, സ്കാമർമാർക്ക് അവർ നിങ്ങൾക്കറിയാവുന്നതോ അല്ലെങ്കിൽ വിശ്വസിക്കാവുന്ന ഒരാളാണെന്ന് തോന്നിപ്പിക്കുന്ന വിധത്തിൽ നിങ്ങളുടെ കോളർ ഐഡിയിൽ കൃത്രിമം കാണിക്കാൻ കഴിയും - ഈ കേസിൽ അത് നിങ്ങളുടെ ബാങ്കാണ്. ഇത് അവരുടെ യഥാർത്ഥ ഐഡന്റിറ്റിക്ക് ഒരു ഡിജിറ്റൽ വേഷപ്പകർച്ച പോലെയാണ്.

ഈ മറഞ്ഞിരുന്നുള്ള തന്ത്രത്തിൽ നിന്ന് സ്വയം പരിരക്ഷിക്കാൻ, ഇനി പറയുന്ന നുറുങ്ങുകൾ ഓർക്കുക:

ജാഗ്രതയോടെ പരിശോധിച്ചുറപ്പാക്കുക: കോളർ ഐഡി പരിചിതമാണെന്ന് തോന്നിയാലും സംശയം പുലർത്തുക. ആരെങ്കിലും സെൻസിറ്റീവായ വിവരങ്ങൾ ആവശ്യപ്പെടുകയാണെങ്കിൽ, മറ്റ് മാർഗ്ഗങ്ങളിലൂടെ അവരുടെ ഐഡന്റിറ്റി രണ്ടുതവണ പരിശോധിക്കുക.

വ്യക്തിഗത വിവരങ്ങൾ പങ്കിടരുത്: വിളിക്കുന്നയാൾ നിയമാനുസൃതമാണെന്ന് തോന്നിയാലും വ്യക്തിപരമോ സാമ്പത്തികമോ ആയ വിവരങ്ങൾ ഒരിക്കലും ഫോൺ വഴി നൽകരുത്. കോൾ അവസാനിപ്പിച്ച് വിശ്വസനീയമായ നമ്പർ ഉപയോഗിച്ച് തിരികെ വിളിക്കുക.

സ്വകാര്യത നിലനിർത്തുക: നിങ്ങൾ ഓൺലൈനിലോ സോഷ്യൽ മീഡിയയിലോ പങ്കിടുന്ന വ്യക്തിഗത വിവരങ്ങളെക്കുറിച്ച് ജാഗ്രത പാലിക്കുക. സ്കാമർമാർ പലപ്പോഴും ഈ ഉറവിടങ്ങളിൽ നിന്നുള്ള വിവരങ്ങൾ ശേഖരിക്കുകയും അവരുടെ വ്യാജ കോളുകൾ കൂടുതൽ വിശ്വാസ്യതയുള്ളതാക്കുകയും ചെയ്യുന്നു..

കോൾ ബ്ലോക്കിംഗ് ഉപയോഗിക്കുക: നിങ്ങളുടെ ഫോൺ കാരിയർ നൽകുന്ന കോൾ-ബ്ലോക്കിംഗ് ആപ്പുകൾ അല്ലെങ്കിൽ ഫീച്ചറുകൾ അടുത്തറിയുക. സാധ്യതയുള്ള സ്കാം കോളുകൾ ഫിൽട്ടർ ചെയ്യാൻ അവ സഹായിക്കും.

ഗൂഗിളിലോ ഏതെങ്കിലും സെർച്ച് എഞ്ചിനിലോ ഫോൺ നമ്പറുകൾ തിരയരുത്. നിങ്ങൾ അങ്ങനെ ചെയ്യുകയാണെങ്കിൽ, സ്ഥാപനമോ വ്യാപാരിയോ നിങ്ങൾക്ക് അയച്ച ഏതെങ്കിലും ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യരുത്..

കൂടാതെ, അംഗീകൃത ആപ്ലിക്കേഷൻ സ്റ്റോറുകളിൽ നിന്ന് മാത്രം നിങ്ങളുടെ ഉപകരണങ്ങളിൽ ഡൗൺലോഡ് ചെയ്ത ബാങ്കിംഗ് ആപ്ലിക്കേഷനുകളുടെ ഏറ്റവും പുതിയ പതിപ്പുകൾ ഉണ്ടെന്ന് ദയവായി ഉറപ്പാക്കുക. ദയവായി ഇത് ഇടയ്ക്കിടെ പരിശോധിക്കുക.

ഓർക്കുക, യഥാർത്ഥ ജീവിതത്തിൽ ഒരു മുഖംമൂടിയുള്ള അപരിചിതനെ വിശ്വസിക്കാത്തത് പോലെ, ഫോണിലും ഒരു മുഖംമൂടിയുള്ള കോളറെ വിശ്വസിക്കരുത്. ജാഗ്രത പാലിക്കുക!

UPI റീഫണ്ട് തട്ടിപ്പുകൾ

നിങ്ങൾ ഒരു UPI റീഫണ്ട് അറിയിപ്പ് കണ്ടെത്തുമ്പോൾ ഫോണിൽ സ്ക്രോൾ ചെയ്യുകൊണ്ടിരിക്കുകയാണെന്ന് സങ്കൽപ്പിക്കുക, പെട്ടെന്ന്, നിങ്ങൾ ആശ്ചര്യപ്പെടുന്നു! എന്നാൽ കാത്തിരിക്കുക. ഇത് ഒരു UPI റീഫണ്ട് തട്ടിപ്പ് ആകാം!

UPI അല്ലെങ്കിൽ യൂണിഫൈഡ് പേയ്മെന്റ് ഇന്റർഫേസ് നമ്മുടെ ദൈനംദിന ജീവിതത്തിന്റെ ഭാഗമായി മാറിയിരിക്കുന്നു. നിങ്ങളുടെ പ്രദേശത്തെ പലചരക്ക് കടകളിൽ പണം നൽകുന്നതും ഫോണുകൾ റീചാർജ് ചെയ്യുന്നതും മുതൽ വിമാന ടിക്കറ്റ് ബുക്കിംഗ് വരെയുള്ള വിവിധ കാര്യങ്ങൾക്കായി നമ്മൾ UPI പേയ്മെന്റ് ഉപയോഗിക്കുന്നു. അതിനാൽ UPI ആപ്ലിക്കേഷനുകൾ ഉപയോഗിച്ച് ആളുകളെ വഞ്ചിക്കാൻ തട്ടിപ്പുകാർ പുതിയ രീതികൾ സ്വീകരിക്കാൻ തുടങ്ങി.

അവരുടെ ഔദ്യോഗിക പദാവലികളിലും പ്രൊഫഷണൽ ഭാഷയിലും ഒരിക്കലും വീണുപോകരുത്. ഇനിപ്പറയുന്ന നുറുങ്ങുകൾ ഓർമ്മിച്ചിരിക്കുക:

ലിങ്കുകളിൽ ജാഗ്രത പുലർത്തുക: റീഫണ്ട് ക്ലെയിം ചെയ്യാൻ രജിസ്റ്റർ ചെയ്യുന്നതിന് പ്രേരിപ്പിച്ചുകൊണ്ട് സ്കാമർമാർ നിങ്ങൾക്ക് ഒരു ലിങ്ക് അയച്ചേക്കാം.

ഉയർന്ന സമ്മർദ്ദമുണ്ടാക്കുന്ന തന്ത്രങ്ങൾ: പെട്ടന്ന് പണം ലഭിക്കാനായി ബാങ്ക് വിശദാംശങ്ങൾ അല്ലെങ്കിൽ UPI PIN പൂരിപ്പിക്കാൻ അവർ നിങ്ങളെ സമ്മർദ്ദത്തിലാക്കും.

യോഗ്യത പരിശോധിച്ചുറപ്പിക്കുക നിങ്ങൾക്ക് ഒരു റീഫണ്ടിന് യോഗ്യതയുണ്ടെന്ന് ഉറപ്പാക്കുക. ഉണ്ടെങ്കിൽ, വിശ്വസനീയമായ ഒരു ഉറവിടത്തിനായി പരിശോധിക്കുക.

ബാങ്കോ മറ്റ് ഉദ്യോഗസ്ഥരോ അത്തരം സെൻസിറ്റീവ് വിശദാംശങ്ങൾ നിങ്ങളോട് ഒരിക്കലും ചോദിക്കില്ലെന്ന കാര്യം ഓർമ്മിക്കുക.

ഫിഷിംഗ് തട്ടിപ്പുകൾ

നിങ്ങൾ നിങ്ങളുടെ സ്വന്തം കാര്യം നോക്കി തെളിഞ്ഞ കുളത്തിൽ നീന്തുകയാണെന്ന് സങ്കൽപ്പിക്കുക. പെട്ടന്ന്, തിളക്കമുള്ള, പ്രലോഭിപ്പിക്കുന്ന ചൂണ്ട നിങ്ങളുടെ മുന്നിൽ തൂങ്ങിക്കിടക്കുന്നതായി കാണുന്നു. നിങ്ങൾക്ക് ആകാംക്ഷയുണ്ട് പക്ഷേ കാത്തിരിക്കുക - എന്തോ കെണിയാണ്!

ഡിജിറ്റൽ മേഖലയിൽ ഫിഷിംഗ് സ്കാമുകൾ ഉപയോഗിച്ച് നടക്കുന്നത് ഇതാണ്.

ഒരു മത്സ്യം ചൂണ്ടയിലേക്ക് ആകർഷിക്കപ്പെടുന്നത് പോലെ, സെൻസിറ്റീവായ വിവരങ്ങൾ വെളിപ്പെടുത്തുന്നതിന് നിങ്ങളെ കബളിപ്പിക്കാൻ സൈബർ കുറ്റവാളികൾ വിശ്വാസ്യതയുള്ള വ്യക്തികളായി ഭാവിക്കുന്നു. അവർ വ്യാജ ഇമെയിലുകൾ, സന്ദേശങ്ങൾ, അല്ലെങ്കിൽ നിയമാനുസൃതമെന്ന് തോന്നുന്ന വെബ്സൈറ്റുകൾ അയയ്ക്കുന്നു, പലപ്പോഴും ബാങ്കുകളെയോ സോഷ്യൽ മീഡിയയെയോ അല്ലെങ്കിൽ നിങ്ങളുടെ ബോസിനെ പോലും അനുകരിക്കുന്നു.

ഈ ഡിജിറ്റൽ കെണികൾ ഒഴിവാക്കാൻ, ചുവടെ പറയുന്ന നുറുങ്ങുകൾ ഓർക്കുക:

URL-കൾ രണ്ട് തവണ പരിശോധിക്കുക: അവ യഥാർത്ഥത്തിൽ എവിടേക്കാണ് നയിക്കുന്നതെന്ന് കാണുന്നതിന് ലിങ്കുകൾ പരിശോധിക്കുക.

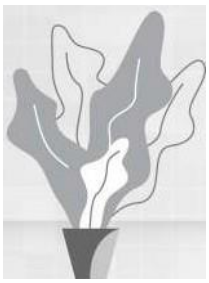
വ്യക്തിഗത വിവരങ്ങൾ പങ്കിടരുത്: നിയമാനുസൃതമായ സ്ഥാപനങ്ങൾ ഇമെയിൽ വഴി സെൻസിറ്റീവായ കാര്യങ്ങൾ ആവശ്യപ്പെടാൻ ആഗ്രഹിക്കുന്നില്ല.

rl2J **സംശയിക്കുന്നത് തുടരുക:** അപ്രതീക്ഷിതമായ അഭ്യർത്ഥനകൾ ലഭിച്ചോ? നടപടി എടുക്കും മുമ്പ് മറ്റ് മാർഗങ്ങളിലൂടെ പരിശോധിക്കുക.

l@l:"\. **സുരക്ഷാ സോഫ്റ്റ്വെയർ അപ്ഡേറ്റ് ചെയ്യുക:** നിങ്ങളുടെ ഡിജിറ്റൽ കുളം ഏറ്റവും പുതിയ പ്രതിരോധങ്ങളോടെ സൂക്ഷിക്കുക.

ജാഗ്രതയുള്ള മത്സ്യത്തെപ്പോലെ, ജാഗ്രത പുലർത്തുക, ഇന്റർനെറ്റിന്റെ വിശാലമായ സമുദ്രത്തിൽ സമർത്ഥമായി നീന്തുക!

വിഷിംഗ് തട്ടിപ്പുകൾ



a

നിങ്ങളുടെ ഫോൺ റിംഗ് ചെയ്യുന്നു, **അത്**'നിങ്ങളുടെ ബാങ്കാണ്, നിങ്ങളുടെ അക്കൗണ്ടിൽ അതിക്രമിച്ച് കടന്നുവെന്ന് പറഞ്ഞുകൊണ്ടുള്ള ഒരു 'അടിയന്തിര' കോൾ ആണ്, അല്ലെങ്കിൽ നിങ്ങൾ ഇന്ന് ഒരു സർപ്രൈസ് സമ്മാനം നേടിയെന്ന് പറയുന്ന 'വിജയം' അറിയിക്കുന്ന കോൾ ആയിരിക്കാം.

ഫോൺ ഹോൾഡ് ചെയ്യുക (അക്ഷരാർത്ഥത്തിൽ തന്നെ)!

അത്തരം തട്ടിപ്പുകളിൽ നിന്ന് സുരക്ഷിതരായിരിക്കാൻ, ചുവടെ പറയുന്ന നുറുങ്ങുകൾ ഓർക്കുക:

I നിങ്ങളുടെ സ്വകാര്യ വിവരങ്ങൾ ഒരിക്കലും ഫോൺ വഴി നൽകരുത്.

<@> ഷെർലക് ഹോംസ് ആകുക, വിളിക്കുന്നയാളുടെ ഐഡന്റിറ്റി പരിശോധിക്കുക.

നാടകത്തിൽ വീഴരുത്! അവർ ചൂടാകുമ്പോൾ ശാന്തമായിരിക്കുക.

ഓൺലൈനിൽ അപരിചിതരുമായി വിവരങ്ങൾ പങ്കിടുന്നതിൽ ജാഗ്രത പാലിക്കുക - നിങ്ങളുടെ കാര്യങ്ങൾ സുരക്ഷിതമായി സൂക്ഷിക്കാൻ ബുദ്ധിപരമായി പെരുമാറുക!

യുപിഐ തട്ടിപ്പുകൾ - പണമായി ആവശ്യപ്പെടുക

ഒരു ഓൺലൈൻ വാങ്ങൽ, വിൽപ്പന ആപ്പിൽ സ്നേഹ തന്റെ ഫർണിച്ചർ പരസ്യം നൽകി. പാരാമിലിട്ടറി ഉദ്യോഗസ്ഥനാണെന്ന് അവകാശപ്പെട്ട വാങ്ങുന്നയാൾ വാട്ട്സാപ്പിൽ പേയ്മെന്റിനായി ഒരു QR കോഡ് അയച്ചു. അവൾ അത് സ്കാൻ ചെയ്യുകയും 75,000 നഷ്ടപ്പെടുകയും ചെയ്തു.

ഇത് പരിചയമുള്ളത് പോലെ തോന്നുന്നുണ്ടോ? നിങ്ങൾ UPI പേയ്മെന്റ് പ്ലാറ്റ്ഫോമുകൾ പതിവായി ഉപയോഗിക്കുന്നതിനാൽ UPI തട്ടിപ്പിന് ഇരയാകുമെന്ന് ഭയപ്പെടുന്നുണ്ടോ?

എല്ലായ്പ്പോഴും ഓർക്കുക:

പേയ്മെന്റ് നടത്തുന്നതിന് മാത്രമാണ് UPI PIN ആവശ്യമുള്ളത്, പേയ്മെന്റ് സ്വീകരിക്കുന്നതിന് അത് ആവശ്യമില്ല.

പേയ്മെന്റ് സ്വീകരിക്കാൻ നിങ്ങളുടെ UPI PIN ആവശ്യപ്പെടുന്ന നിമിഷം തന്നെ ഇടപാട് നിർത്തുക! ഇത് യഥാർത്ഥത്തിൽ പണം ലഭിക്കാനുള്ള അഭ്യർത്ഥനയല്ല, പണമടയ്ക്കാനുള്ള അഭ്യർത്ഥനയായിരിക്കാം.

നിങ്ങളുടെ OTP, UPI PIN അല്ലെങ്കിൽ ഏതെങ്കിലും രഹസ്യ വിവരങ്ങൾ ആരുമായും പങ്കിടരുത്.

ഏതെങ്കിലും പേയ്മെന്റ് ആരംഭിക്കുന്നതിന് മുമ്പ് UPI അപ്ലിക്കേഷനിലെ മൊബൈൽ നമ്പറും പേരും എല്ലായ്പ്പോഴും പരിശോധിക്കുക.

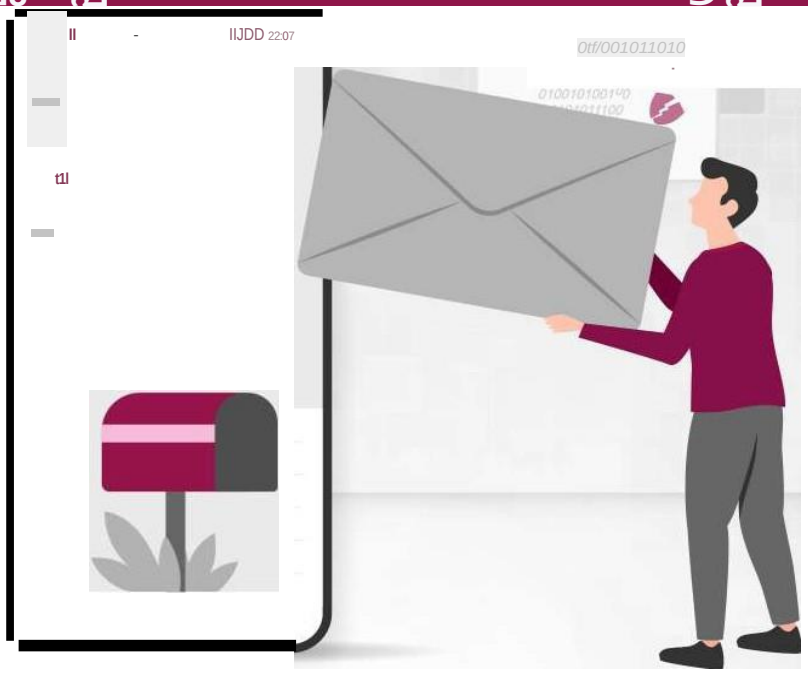
QR കോഡ് സ്കാൻ തട്ടിപ്പ്

പേയ്മെന്റ് ആപ്പുകളിലെ QR കോഡുകൾ ജാഗ്രതയോടെ സ്കാൻ ചെയ്യുക; പണം കൈമാറ്റം ചെയ്യുന്നതിനുള്ള അക്കൗണ്ട് വിശദാംശങ്ങൾ അവയിൽ അടങ്ങിയിട്ടുണ്ട്.

പണം സ്വീകരിക്കാൻ QR കോഡുകൾ സ്കാൻ ചെയ്യരുത്; പണം സ്വീകരിക്കുന്നതിനുള്ള ഇടപാടുകളിൽ ബാർകോഡുകൾ / QR കോഡുകൾ സ്കാൻ ചെയ്യുകയോ മൊബൈൽ ബാങ്കിംഗ് PIN (m-PIN), പാസ്വേഡുകൾ മുതലായവ നൽകേണ്ട ആവശ്യമില്ല.

വാങ്ങുന്നയാൾ / വിൽപ്പനക്കാരൻ അനാവശ്യമായ തിടുക്കമോ അത്യാവശ്യമോ കാണിക്കുന്നുവെങ്കിൽ മിക്കവാറും ഒരു തട്ടിപ്പുകാരനായിരിക്കും. ശാന്തത പാലിക്കുക, എല്ലായ്പ്പോഴും വ്യക്തത തേടുക, ആവശ്യമായ ചോദ്യങ്ങൾ ചോദിക്കുക.

പരിശോധിച്ചുറപ്പിക്കാത്ത മൊബൈൽ ആപ്പ് തട്ടിപ്പുകൾ



നിങ്ങൾക്ക് ഒരു SMS, ഇമെയിൽ, അതല്ലെങ്കിൽ ഏറെക്കാലമായി യാതൊരു വിവരവും ഇല്ലാതിരുന്ന ഒരു ബന്ധുവിന്റെ സന്ദേശം പോലും ലഭിക്കും. അതിലെല്ലാം നിങ്ങളുടെ പ്രിയപ്പെട്ട അംഗീകൃത സ്ഥാപനത്തിൽ നിന്നുള്ള ഒരു നിയമാനുസൃത ആപ്പ് പോലെ കാണപ്പെടുന്ന ഒരു ലിങ്കും ഉണ്ടാവും.

ഒരു നിമിഷം നിൽക്കുക! ഇവ സൗഹൃദപരമായ ഡൗൺലോഡുകളല്ല; നിങ്ങൾ തീർച്ചയായും പങ്കെടുക്കാൻ ആഗ്രഹിക്കാത്ത ഒരു ഡിജിറ്റൽ പാർട്ടിയിലേക്കുള്ള ക്ഷണങ്ങളാണിവ!

സ്കാമർമാർ SMS, ഇമെയിൽ അല്ലെങ്കിൽ സോഷ്യൽ മീഡിയ വഴി വ്യാജ ആപ്പ് ലിങ്കുകൾ അയയ്ക്കുന്നു. അവയിൽ ക്ലിക്ക് ചെയ്യാൻ അവർ ഉപയോക്താക്കളെ പ്രേരിപ്പിക്കുന്നു, ഇത് അജ്ഞാതമായ ആപ്പുകൾ ഡൗൺലോഡ് ചെയ്യുന്നതിലേക്ക് നയിക്കുന്നു. ഇൻസ്റ്റാൾ ചെയ്തുകഴിഞ്ഞാൽ, രഹസ്യ വിവരങ്ങളും OTP-കളും ഉൾപ്പെടെ സ്കാമർമാർക്ക് ഉപകരണത്തിലേക്ക് പ്രവേശനം ലഭിക്കും.

അജ്ഞാത ഉറവിടങ്ങളിൽ നിന്നോ അപരിചിതർ ആവശ്യപ്പെട്ടോ ആപ്പുകൾ ഡൗൺലോഡ് ചെയ്യുന്നത് ഒഴിവാക്കുക.

ഡൗൺലോഡ് ചെയ്യുന്നതിന് മുമ്പ് ആപ്പ് പ്രസാധകരെയും ഉപയോക്തൃ റേറ്റിംഗുകളും പരിശോധിക്കുക.

അനുമതികളും ആപ്പ് അഭ്യർത്ഥനകളും അവലോകനം ചെയ്യുക (ഉദാഹരണത്തിന് കോൺടാക്റ്റുകൾ, ഫോട്ടോകൾ), ആവശ്യമുള്ളവ മാത്രം അനുവദിക്കുക.

ബാങ്കോ മറ്റ് ഉദ്യോഗസ്ഥരോ അത്തരം സെൻസിറ്റീവ് വിശദാംശങ്ങൾ നിങ്ങളോട് ഒരിക്കലും ചോദിക്കില്ലെന്ന കാര്യം ഓർമ്മിക്കുക.

എടിഎം കാർഡ് സ്കിമ്മിംഗ് തട്ടിപ്പ്

ഒരു ഡിജിറ്റൽ പോക്കറ്റടി പോലെ എടിഎം സ്കിമ്മിംഗിനെ മനസ്സിലാക്കുക. പണം പിൻവലിക്കാനോ ബാലൻസ് പരിശോധിക്കാനോ നിങ്ങൾ എടിഎം ഉപയോഗിക്കുമ്പോൾ നിങ്ങളുടെ കാർഡ് വിവരങ്ങൾ രേഖപ്പെടുത്തുന്നതിനായി തട്ടിപ്പുകാർ മെഷീനിൽ മറഞ്ഞിരിക്കുന്ന ഉപകരണങ്ങൾ സജ്ജമാക്കുന്നു. ഈ ഉപകരണങ്ങൾ ഒരു വ്യാജ കാർഡ് സ്ലോട്ട് അല്ലെങ്കിൽ ഒരു ചെറിയ ക്യാമറ പോലെ പെട്ടന്ന് കാണാനാവാത്തവയാണ്.

എടിഎം പരിശോധിക്കുക: എടിഎം ഉപയോഗിക്കുന്നതിന് മുമ്പ് ഏതെങ്കിലും അസാധാരണമായ അറ്റാച്ച്മെന്റുകൾ, അയഞ്ഞ ഭാഗങ്ങൾ അല്ലെങ്കിൽ മറഞ്ഞിരിക്കുന്ന ക്യാമറകൾ എന്നിവയുണ്ടെയെന്നറിയാൻ എല്ലായ്പ്പോഴും കാർഡ് സ്ലോട്ടും കീപാഡും പരിശോധിക്കുക.

നിങ്ങളുടെ PIN മൂടി വയ്ക്കുക: കൈകളോ ശരീരമോ ഉപയോഗിച്ച് നിങ്ങളുടെ PIN എന്റർ ചെയ്യുന്നത് മറയ്ക്കുക, ഇത് ക്യാമറകളോ അതിനായി നോക്കുന്നവരോ അത് കാണുന്നത് പ്രയാസകരമാക്കുന്നു.

സ്റ്റേറ്റ്മെന്റുകൾ സ്ഥിരമായി പരിശോധിക്കുക: നിങ്ങളുടെ ബാങ്ക് സ്റ്റേറ്റ്മെന്റുകളിലും ഇടപാടുകളിലും ശ്രദ്ധപുലർത്തുക. അപരിചിതമായ ഏതെങ്കിലും പ്രവർത്തനം കണ്ടാൽ ഉടൻ ബാങ്കിൽ റിപ്പോർട്ട് ചെയ്യുക.

കോളുകളെ സൂക്ഷിക്കുക: നിങ്ങളുടെ ബാങ്കിൽ നിന്ന് ആരെങ്കിലും വിളിക്കുകയും സെൻസിറ്റീവായ വിവരങ്ങൾ ആവശ്യപ്പെടുകയും ചെയ്താൽ, ജാഗ്രത പാലിക്കുക. ബാങ്കുകൾ ഫോണിൽ പിൻ നമ്പറുകൾ അല്ലെങ്കിൽ പൂർണ്ണമായ കാർഡ് നമ്പറുകൾ ചോദിക്കുന്നത് അപൂർവ്വമാണ്.

സുരക്ഷിതമായ എടിഎമ്മുകൾ ഉപയോഗിക്കുക: നല്ല പ്രകാശമുള്ള പ്രദേശങ്ങളിലെയോ അല്ലെങ്കിൽ ബാങ്ക് ശാഖകളോട് ചേർന്നുള്ളതോ ആയ എടിഎമ്മുകൾ തിരഞ്ഞെടുക്കുക, കാരണം അവ തകർക്കപ്പെടാനുള്ള സാധ്യത കുറവാണ്.

പുതിയ വിവരങ്ങൾ അറിഞ്ഞുകൊണ്ടിരിക്കുക: സ്വയം മികച്ച രീതിയിൽ പരിരക്ഷിക്കുന്നതിന് ഏറ്റവും പുതിയ തട്ടിപ്പുകളെയും വഞ്ചനാ തന്ത്രങ്ങളെയും കുറിച്ച് അറിഞ്ഞിരിക്കുക.

ജാഗ്രതയോടെയിരിക്കുകയും ഈ നുറുങ്ങുകൾ പാലിക്കുകയും ചെയ്യുന്നതിലൂടെ നിങ്ങൾക്ക് എടിഎം കാർഡ് സ്കിമ്മിംഗ് തട്ടിപ്പിന് ഇരയാകുന്നത് ഒഴിവാക്കാനും പണം സുരക്ഷിതമായി സൂക്ഷിക്കാനും കഴിയും എന്നത് ഓർമ്മിക്കുക.

റിമോട്ട് ആക്സസ് തട്ടിപ്പ്

സ്ക്രീൻ ഷെയറിംഗ് അപ്ലിക്കേഷൻ ഡൗൺലോഡ് ചെയ്യാൻ സ്കാമർമാർ ഉപഭോക്താക്കളെ പ്രലോഭിപ്പിക്കുന്നു. ഇത് ഉപയോഗിച്ച്, അവർ നിങ്ങളുടെ ഉപകരണത്തിലേക്ക് നുഴഞ്ഞുകയറുന്നു, നിങ്ങളുടെ വിവരങ്ങൾ ചോർത്തുന്നു, നിങ്ങളുടെ സാമ്പത്തിക വിവരങ്ങൾ അപഹരിക്കുന്നു. അങ്ങനെ നിങ്ങളുടെ പണവുമായി അവർ ഷോപ്പിംഗിന് പോകുന്നു!

ഇത്തരം തട്ടിപ്പുകൾ ഒഴിവാക്കാൻ ഇനി പറയുന്ന നുറുങ്ങുകൾ ഓർമ്മിക്കുക:

വിളിക്കുന്നവരെ പരിശോധിച്ചുറപ്പിക്കുക: അവർ പ്രതിനിധീകരിക്കുന്ന സ്ഥാപനത്തിന്റെ ഔദ്യോഗിക കോൺടാക്റ്റ് വിവരങ്ങൾ നോക്കിക്കൊണ്ട് വിളിക്കുന്നയാളുടെ ഐഡന്റിറ്റി എല്ലായ്പ്പോഴും രണ്ടുവട്ടം പരിശോധിക്കുക.

തിരക്കിട്ടുള്ള തീരുമാനങ്ങൾ വേണ്ട: സമ്മർദ്ദം മൂലം വേഗത്തിലുള്ള തീരുമാനങ്ങൾ എടുക്കരുത്. ആക്സസ് നൽകുന്നതിനോ സെൻസിറ്റീവായ വിവരങ്ങൾ പങ്കിടുന്നതിനോ മുമ്പ് ചിന്തിക്കാനും പരിശോധിക്കാനും സമയമെടുക്കുക.

നിങ്ങളുടെ ഉപകരണങ്ങൾ സുരക്ഷിതമാക്കുക: ഏറ്റവും പുതിയ സുരക്ഷാ പാച്ചുകൾ ഉപയോഗിച്ച് നിങ്ങളുടെ ഉപകരണങ്ങൾ അപ്ഡേറ്റ് ചെയ്യുകയും ഓരോ അക്കൗണ്ടിനും ശക്തവും സവിശേഷവുമായ പാസ്വേഡുകൾ ഉപയോഗിക്കുകയും ചെയ്യുക.

സ്വയം പഠിക്കുക: പൊതുവായ തട്ടിപ്പുകളെയും തന്ത്രങ്ങളെയും കുറിച്ച് പഠിക്കുക, അതുവഴി അവ സംഭവിക്കുമ്പോൾ തന്നെ നിങ്ങൾക്ക് തിരിച്ചറിയാൻ കഴിയും.

വ്യക്തിഗത വിവരങ്ങൾ സംരക്ഷിക്കുക: അഭ്യർത്ഥനയുടെ നിയമസാധുതയെക്കുറിച്ച് നിങ്ങൾക്ക് ഉറപ്പില്ലെങ്കിൽ ഫോൺ, ഇമെയിൽ അല്ലെങ്കിൽ ഓൺലൈനിൽ വ്യക്തിഗതമോ അല്ലെങ്കിൽ സാമ്പത്തികമോ ആയ വിവരങ്ങൾ പങ്കിടുന്നതിൽ ജാഗ്രത പുലർത്തുക.

നിങ്ങളുടെ ഡിജിറ്റൽ ജീവിതത്തിലേക്ക് വിദൂരമായിരുന്ന് നുഴഞ്ഞുകയറാൻ ശ്രമിക്കുന്ന തട്ടിപ്പുകാർക്കെതിരെ വെർച്വൽ വാതിൽ അടച്ചിടാൻ ജാഗ്രത പാലിക്കുക.

ദയവായി ശ്രദ്ധിക്കുക - ഒരു കറുത്ത/ശൂന്യമായ സ്ക്രീൻ ശ്രദ്ധയിൽപ്പെട്ടാൽ, ദയവായി നിങ്ങളുടെ സിസ്റ്റത്തിൽ ഏതെങ്കിലും പ്രവർത്തനം തുടരരുത്. നിങ്ങളുടെ സ്ക്രീൻ മറ്റുള്ളവർക്ക് ദൃശ്യമാകുന്നതിന്റെ അടയാളമായിരിക്കാം ഇത്.

സിം സ്വാപ്പ് തട്ടിപ്പ്

സ്കാമർമാർ ഒരു ഫോൺ കവർച്ച നടത്തുന്നത് സങ്കൽപ്പിക്കുക! അവർ നിങ്ങളാണെന്ന് നടിക്കുന്നു, നിങ്ങളുടെ സിം കാർഡ് നഷ്ടപ്പെട്ടുവെന്ന് പറയുന്നു, അവർക്ക് നിങ്ങളുടെ നമ്പർ ലഭിച്ചു. അതുപയോഗിച്ച്, നിങ്ങളുടെ ബാങ്ക് അല്ലെങ്കിൽ ഇമെയിൽ പോലുള്ള നിങ്ങളുടെ ഓൺലൈൻ അക്കൗണ്ടുകൾ ക്രാഷ് ചെയ്യുകയും കുഴപ്പമുണ്ടാക്കുകയും ചെയ്യുന്നു!

സ്വാപ്പ് തട്ടിപ്പ് തടയുക! ചുവടെ പറയുന്ന നുറുങ്ങുകൾ ഓർക്കുക.

സിം കാർഡ് ഐഡന്റിറ്റി വിശദാംശങ്ങൾ പങ്കിടരുത്.

നിങ്ങളുടെ ഫോണിന്റെ നെറ്റ്‌വർക്ക് ആക്സസ് നിരീക്ഷിക്കുക.

കുറച്ച് സമയത്തേക്ക് നെറ്റ്‌വർക്ക് ഇല്ലെങ്കിൽ, ഡ്യൂപ്ലിക്കേറ്റ് **SIM-കൾ** ഉണ്ടോയെന്ന് പരിശോധിക്കാൻ നിങ്ങളുടെ ഓപ്പറേറ്ററുമായി ബന്ധപ്പെടുക.

നിങ്ങളുടെ ഡിജിറ്റൽ ജീവിതത്തിലേക്ക് വിദൂരമായിരുന്ന് നുഴഞ്ഞുകയറാൻ ശ്രമിക്കുന്ന തട്ടിപ്പുകാർക്കെതിരെ വെർച്വൽ വാതിൽ അടച്ചിടാൻ ജാഗ്രത പാലിക്കുക.

ഒരു വഞ്ചനാപരമായ ഇടപാട് എങ്ങനെ റിപ്പോർട്ട് ചെയ്യാം?

www.axisbank.com സന്ദർശിച്ച് > പിന്തുണ > 'ഞങ്ങളിലേക്ക് ഇവിടെ എത്തിച്ചേരുക' വിഭാഗത്തിലേക്ക് താഴേക്ക് സ്ക്രോൾ ചെയ്യുക > ഞങ്ങളോട് സംസാരിക്കുക > 'ഒരു തട്ടിപ്പ് അല്ലെങ്കിൽ തർക്കം റിപ്പോർട്ട് ചെയ്യുക' > തിരഞ്ഞെടുക്കുക ഒരു തട്ടിപ്പ് റിപ്പോർട്ട് ചെയ്യുക>
നിങ്ങളുടെ അന്വേഷണത്തിന്റെ ഡ്രോപ്പ്-ഡൗൺ ലിസ്റ്റിൽ നിന്ന് പ്രസക്തമായ ഓപ്ഷൻ തിരഞ്ഞെടുക്കുക> കോളിൽ ക്ലിക്ക് ചെയ്യുക

ആർബിഐയിൽ ഒരു പരാതി നൽകാൻ https://cms.rbi.org.in സന്ദർശിക്കുക

ടോൾ ഫ്രീ നമ്പറിൽ വിളിക്കുക 14448 (തിങ്കൾ മുതൽ വെള്ളി വരെ, രാവിലെ 9:30 മുതൽ വൈകുന്നേരം 5:15 വരെ, ദേശീയ അവധി ദിനങ്ങൾ ഒഴികെ).

ഒരുകടലാസ് രൂപത്തിലുള്ളപരാതി അയയ്ക്കുക: കത്ത്/ ഈ വിലാസത്തിൽ പോസ്റ്റ് ചെയ്യുക 'സെൻട്രലൈസ്ഡ് റെസീപ്റ്റ് ആൻഡ് പ്രൊസസ്സിംഗ് സെന്റർ, 4-ാം നില, റിസർവ്ബാങ്ക് ഓഫ് ഇന്ത്യ, സെക്ടർ-17, സെൻട്രൽ വിസ്റ്റ, ചണ്ഡിഗഢ് - 160 017'. **ആവശ്യമായ** ഫോർമാറ്റിനെക്കുറിച്ചുള്ള കൂടുതൽ വിവരങ്ങൾക്ക് ദയവായി https://cms.rbi.org.in സന്ദർശിക്കുക.

ഒരു സൈബർ കുറ്റകൃത്യം റിപ്പോർട്ട് ചെയ്യുന്നതിന്, ഹെൽപ്പ് ലൈൻ നമ്പർ 155260 **അല്ലെങ്കിൽ** 1930 ഡയൽ ചെയ്യുക അല്ലെങ്കിൽ സംഭവം ദേശീയ സൈബർ ക്രൈം റിപ്പോർട്ടിംഗ് പോർട്ടലിൽ **(www.cybercrime.gov.in)**-ൽ റിപ്പോർട്ട് ചെയ്യുക.