HSBC

ഓൺലൈൻ സുരക്ഷാ സവിശേഷതകളും സുരക്ഷിതമായ ഉപയോഗ മാർഗ്ഗനിർദ്ദേശങ്ങളും

നമുക്കൊന്നിച്ച് ഓൺലൈൻ ബാങ്കിംഗ് എങ്ങനെ സുരക്ഷിതമാക്കാം എന്ന് പരിശോധിക്കാം

ഒരു ബാങ്ക് എന്ന നിലയിൽ ഞങ്ങൾ പതിവായി സുരക്ഷയെക്കുറിച്ച് ചിന്തിച്ചുകൊണ്ടിരിക്കുന്നു. ഇൻറർനെറ്റിന്റെ വളർച്ച നമുക്കെല്ലാവർക്കും കൂടുതൽ സൗകര്യങ്ങൾ ലഭ്യമാക്കിയിട്ടുണ്ട്, എന്നാൽ ഇത് പുതിയ അപകടസാധ്യതകളും ഒപ്പം കൊണ്ടു വന്നിട്ടുണ്ട്. എച്ച്എസ്ബിസിയിൽ, ഇൻഡസ്ട്രി സ്റ്റാൻഡേർഡ് സുരക്ഷാ സാങ്കേതികവിദ്യയും പ്രയോഗങ്ങളും ആണ് ഞങ്ങൾ ഉപയോഗിക്കുന്നത്. ഇതിനായി ഏതെങ്കിലും അനധികൃത ആക്സസ്സിൽ നിന്ന് നിങ്ങളുടെ അക്കൗണ്ടിനെ പരിരക്ഷിക്കുന്നതിന് പ്രധാനമായും മൂന്ന് മേഖലകളിൽ ഞങ്ങൾ ശ്രദ്ധ കേന്ദ്രീകരിക്കുന്നു – സ്വകാര്യത, സാങ്കേതികവിദ്യ, തിരിച്ചറിയൽ.

നിങ്ങളുടെ ഓൺലൈൻ ഇന്റർനെറ്റ് ബാങ്കിംഗ് സുരക്ഷ മെച്ചപ്പെടുത്തുന്നതിന് ഞങ്ങൾ എന്തുചെയ്യുന്നുവെന്നും നിങ്ങൾക്ക് വ്യക്തിപരമായി എന്തെല്ലാം നടപടികൾ കൈക്കൊള്ളാനാകുമെന്നും അറിയാൻ തുടർന്ന് വായിക്കുക

തട്ടിപ്പിന്റെ തരങ്ങൾ

നിങ്ങളുടെ വ്യക്തിഗത വിവരങ്ങളും സുരക്ഷാസംബന്ധമായ വിശദാംശങ്ങളും നിങ്ങളിൽ നിന്ന് ചോർത്തിയെടുക്കാൻ തട്ടിപ്പുകാർ പല മാർഗ്ഗങ്ങളും അവലംബിച്ചേക്കാം. ഈ വിവരങ്ങൾ നേടുന്നതിനും നിങ്ങളുടെ അക്കൗണ്ടിൽ നിന്ന് പണം അവരുടെ അക്കൗണ്ടിലേക്ക് മാറ്റുന്നതിനും അവർ ഈ വിശദാംശങ്ങൾ ഉപയോഗിക്കുന്നു.

നിങ്ങൾ നേരിട്ടേക്കാവുന്ന ചില സാധാരണ തട്ടിപ്പുകൾ ഇവയാണ്:

ക്രെഡിറ്റ് / ഡെബിറ്റ് കാർഡ് സ്കിമ്മിംഗ് / ക്ലോണിംഗ്:

നിങ്ങളുടെ ക്രെഡിറ്റ് അല്ലെങ്കിൽ ഡെബിറ്റ് കാർഡിന്റെ മാഗ്നറ്റിക് സ്ട്രിപ്പിൽ ഉള്ള വിവരങ്ങൾ മോഷ്ടിച്ചേക്കാം. എടിഎമ്മുകളിൽ അവർ കാർഡ് ഇടുന്ന സ്ലോട്ടിൽ സ്കിമ്മർ ഉപകരണങ്ങൾ ഒളിപ്പിച്ച് വച്ചും അല്ലെങ്കിൽ മർച്ചന്റ് പേയ്മെന്റ് ടെർമിനലുകളിൽ നിങ്ങളുടെ കാർഡ് സ്വൈപ്പുചെയ്യുന്നതിന് മുമ്പ് നിങ്ങളുടെ ശ്രദ്ധ തെറ്റിച്ചും ആണ് വിവരങ്ങൾ തട്ടിയെടുക്കുന്നത്. ഈ ഉപകരണം കാർഡ് വിശദാംശങ്ങൾ സ്കാൻ ചെയ്ത് വിവരങ്ങൾ സംഭരിക്കുന്നു. പിൻ മോഷ്ടിക്കാൻ എടിഎമ്മുകളിലോ അല്ലെങ്കിൽ വ്യാപാരി സ്ഥാപനങ്ങളിലോ നിങ്ങളുടെ ശ്രദ്ധ എത്താത്ത ഭാഗങ്ങളിൽ തട്ടിപ്പുകാർ ക്യാമറ സ്ഥാപിക്കുകയും ചെയ്യുന്നു.

യുപിഐ ആപ്പുകളിലൂടെയുള്ള പേയ്മെന്റ് തട്ടിപ്പ്:

തട്ടിപ്പു നടത്തുന്നവർ സന്ദേശമയയ്ക്കൽ അപ്ലിക്കേഷനുകൾ വഴി ഇരകളുടെ ഫോണുകളിലേക്ക് ക്യുആർ കോഡുകൾ അയയ്ക്കുന്നു. ക്യുആർ കോഡ് സ്കാൻ ചെയ്യാൻ ഇരകളെ പ്രേരിപ്പിക്കുകയോ അല്ലെങ്കിൽ അവരുടെ അക്കൗണ്ടിലേക്ക് ഫണ്ട് കൈമാറുന്നതിനുള്ള ഒരു 'കളക്ട് റിക്വസ്റ്റ്' ന് അംഗീകാരം നൽകാൻ ആവശ്യപ്പെടുകയോ ചെയ്യുന്നു. മിക്കപ്പോഴും ഇത്തരം തട്ടിപ്പുകാർ ഇരകളെ വിശ്വസനീയമായ കഥകളിലൂടെ വിശ്വാസത്തിലെടുക്കുന്നു. ഇര ഓൺലൈനിൽ വിൽക്കാൻ വച്ച ഒരു സാധനം വാങ്ങാൻ എന്ന വ്യാജേനയോ അല്ലങ്കിൽ ഒരു ഓൺലൈൻ ഷോപ്പിംഗ് കമ്പനി എക്സിക്യൂട്ടീവ് ആയോ ഒക്കെയാണ് അവർ ഇരയെ ബന്ധപ്പെടുന്നത്. തട്ടിപ്പുകാർ പിന്നീട് റീഫണ്ടുകൾ, ക്ലെയിം ചെയ്യാത്ത ക്യാഷ്ബാക്ക് ഓഫർ, റിവാർഡ് പോയിന്റുകൾ തുടങ്ങിയവ പ്രോസസ്സ് ചെയ്യുന്നതതായി വാഗ്ദാനം ചെയ്യുന്നു, സംശയമില്ലാത്ത ഇരകൾ ക്യുആർ കോഡ് സ്കാൻ ചെയ്യുകയോ അവരുടെ യുപിഐ പിൻ ഉപയോഗിച്ച് 'കളക്ട് റിക്വസ്റ്റ്' അംഗീകരിക്കുകയോ ചെയ്യുന്നു. ഇരയുടെ അക്കൗണ്ടിൽ നിന്ന് അതോടെ പണം നഷ്ടമാകുന്നു.

ബിസിനസ്സ് ഇമെയിൽ, സന്ദേശമയയ്ക്കൽ അപ്ലിക്കേഷൻ വഴിയുള്ള പേയ്മെന്റ് തട്ടിപ്പുകൾ

തട്ടിപ്പുകാർ ഇമെയിലുകൾ അല്ലെങ്കിൽ ചാറ്റ് ഹാക്ക് ചെയ്യുകയോ അല്ലെങ്കിൽ സന്ദേശങ്ങളും ഇരയുടെ പ്രൊഫൈലും മനസിലാക്കാൻ എൻക്രിപ്റ്റ് ചെയ്യാത്ത ഇമെയിലുകളിൽ / സന്ദേശങ്ങളിൽ ഇടപെടലുകൾ നടത്തുകയോ ചെയ്യുന്നു. കൂടുതൽ വിവരങ്ങൾ ലഭിച്ച ശേഷം തട്ടിപ്പുകാർ ഹാക്കുചെയ്ത / കടന്നു കയറിയ / സ്പൂഫ് ചെയ്ത ഐഡിയിൽ നിന്ന് നിങ്ങളുടെ കോണ്ടാക്ടിലുള്ളവർക്ക് പ്രിയപ്പെട്ടവരുടെ അടിയന്തിര ആശുപത്രി ചിലവിനോ മുൻകാല കുടിശ്ശികകൾ അടിയന്തിരമായി അടയ്ക്കേണ്ടതിനോ പുതിയൊരു അക്കൗണ്ടിലേക്ക് പണം അയക്കുന്നതിന് ആവശ്യപ്പെടും. അയച്ച ആളോടുള്ള വിശ്വാസമോ അടിയന്തിര സ്ഥിതിയോ കാരണം ഇരകൾ തട്ടിപ്പുകാരന്റെ അക്കൗണ്ടിലേക്ക് പണമടയ്ക്കുന്നു. പണമടയ്ക്കൽ ഇര തന്നെ നടപ്പിലാക്കുന്നതിനാൽ ബാങ്കുകളിൽ നിന്നുള്ള ഇടപാട് അലേർട്ടുകൾ സംശയമുണ്ടാകുന്നില്ല. അതിനാൽ അത്തരം തട്ടിപ്പുകൾ കണ്ടെത്തുന്നത് ബുദ്ധിമുട്ടാണ്.

വ്യാജ കോൺടാക്റ്റ് നമ്പറുകൾ:

തട്ടിപ്പുകാർ ബാങ്കുകളുടെയോ അല്ലെങ്കിൽ സേവന ദാതാവിന്റെയോ കോണ്ടാക്ട് സെന്ററുകളുടെ വ്യാജ കോൺടാക്റ്റ് വിശദാംശങ്ങൾ നൽകും. സംശയമില്ലാത്ത ഇരകൾ സെർച്ച് എഞ്ചിൻ വഴി ലഭിക്കുന്ന ഈ വ്യാജ നമ്പറുകളിൽ വിളിക്കും. പിന്നീട് ഉപഭോക്താക്കളെ ഒരു 'പരിശോധന പ്രക്രിയ'യിലൂടെ കൊണ്ടു പോകുകയും പിന്നെ എന്തെങ്കിലും സൂത്രങ്ങൾ ഉപയോഗിച്ച് അവരുടെ ഡെബിറ്റ് / ക്രെഡിറ്റ് കാർഡുകൾ, ബാങ്ക് അക്കൗണ്ടുകൾ എന്നിവയെക്കുറിച്ചുള്ള തന്ത്രപ്രധാനമായ വിവരങ്ങൾ ലഭ്യമാക്കി തട്ടിപ്പ് നടത്തുന്നു.

നിങ്ങൾക്ക് ആവശ്യമുള്ള കോൺടാക്റ്റ് വിശദാംശങ്ങൾക്കായി എല്ലായ്പ്പോഴും ഒരു ബാങ്കിന്റെയോ സേവന ദാതാവിന്റെയോ ഔദ്യോഗിക വെബ്സൈറ്റ് സന്ദർശിക്കുന്നുണ്ടെന്ന് ഉറപ്പുവരുത്തിക്കൊണ്ട് നിങ്ങൾക്ക് സ്വയം പരിരക്ഷിക്കാൻ കഴിയും. തിരയൽ ഫലങ്ങളിൽ ദൃശ്യമാകുന്ന കോളിംഗ് നമ്പറുകൾ പരിശോധിക്കാതെ വിളിക്കാതിരിക്കാൻ ജാഗ്രത പാലിക്കുക. പ്രത്യേകിച്ചും അവ ഒരു മൊബൈൽ നമ്പറാണെങ്കിൽ.

ഫിഷിംഗ് / സ്പൂഫിംഗ് ഇമെയിലുകൾ:

തട്ടിപ്പുകാർ തങ്ങൾക്ക് ലഭിക്കുന്ന എല്ലാ ഇമെയിൽ വിലാസങ്ങളിലേക്കും ഒരു ഇമെയിൽ സന്ദേശം അയക്കുന്നു. നിയമാനുസൃത സ്ഥാപനങ്ങളായ ഒരു ബാങ്ക്, ഓൺലൈൻ പേയ്മെന്റ് സേവനം, ഓൺലൈൻ റീട്ടെയിലർ അല്ലെങ്കിൽ സമാനമായ സ്ഥാപനങ്ങളിൽ നിന്നുള്ളതാണെന്ന് അവകാശപ്പെട്ടുകൊണ്ടാണ് പലപ്പോഴും ഇത് അയക്കുന്നത്. സ്പൂഫിംഗ് സാധാരണയായി യഥാർത്ഥ ഉറവിടമത്തിൽ നിന്നല്ലാതെ മറ്റൊരാൾ അയക്കുന്ന എന്നാൽ യഥാർത്ഥമാണെന്നു തോന്നിപ്പിക്കുന്ന ഇമെയിലുകളാണ്.

ഫിഷിംഗിൽ നിന്ന് നിങ്ങളെ സ്വയം സംരക്ഷിക്കുന്നതിനായി, വ്യക്തിപരമോ സാമ്പത്തികമോ ആയ വിവരങ്ങൾ അഭ്യർത്ഥിക്കുന്ന ഇമെയിൽ സന്ദേശങ്ങളോട് നിങ്ങൾ ഒരിക്കലും പ്രതികരിക്കരുത്, അത്തരമൊരു ഇമെയിലിലെ ലിങ്കിൽ ഒരിക്കലും സെലക്ട് ചെയ്യരുത്.

മണി മ്യൂൾ അല്ലെങ്കിൽ അധിക വരുമാന ഇമെയിൽ തട്ടിപ്പ്

മണി മ്യൂൾ തട്ടിപ്പിൽ, തട്ടിപ്പുകാർ ഒരു ട്രാൻസ്ഫർ നടത്താൻ നിങ്ങളുടെ സഹായം തേടുന്നു. നിങ്ങളുടെ അക്കൗണ്ടിലേക്ക് ഫണ്ട് അടയ്ക്കാമെന്നും അത് മറ്റൊരു അക്കൗണ്ടിലേക്ക് ട്രാൻസ്ഫർ ചെയ്യാൻ നിങ്ങൾ സഹായിക്കണമെന്നും അവർ ആവശ്യപ്പെടും. അതിനു പകരമായി, നിങ്ങൾക്ക് ഒരു കമ്മീഷൻ നൽകാമെന്ന് പറയും.

കള്ളപ്പണം വെളുപ്പിക്കൽ പോലുള്ള കുറ്റകൃത്യങ്ങളിൽ നിന്നുള്ള പണം ആയിരിക്കാം ഇത്. വിവരങ്ങൾ അറിഞ്ഞുകൊണ്ട് ഇതിൽ പങ്കെടുക്കുന്ന ഏതൊരു ഉപഭോക്താവും സാങ്കേതികമായി കുറ്റകൃത്യത്തിൽ ഏർപ്പെടുതിനാൽ നിങ്ങൾ നിയമപരമായ നടപടികൾ നേരിടേണ്ടി വന്നേക്കാം. സത്യമാണെന്നു വിശ്വസിക്കാൻ പ്രയാസം തോന്നുന്ന ഏതൊരു മെയിലും ഒരു തട്ടിപ്പ് തന്നെ ആയിരിക്കും.

അഡ്വാൻസ്ഡ് ഫീസ് തട്ടിപ്പ് (‘419’ തട്ടിപ്പ്):

വിദേശ രാജ്യങ്ങളിൽ അവകാശികളില്ലാതെ കിടക്കുന്ന വലിയൊരു തുക, സാധാരണ ഗതിയിൽ യുഎസ് ഡോളറിൽ, നീക്കാൻ സഹായിക്കുന്നതിന് സഹായം തേടി തട്ടിപ്പുകാർ പലർക്കും ഇമെയിൽ അയക്കുന്നു. നിങ്ങളുടെ ബാങ്കിംഗ് വിവരങ്ങൾ ലഭ്യമാക്കുകയാണ് അവരുടെ ലക്ഷ്യം. ഒരു ഫീസ്, ടാക്സ് അല്ലെങ്കിൽ ഒരു കൈക്കൂലി കൊടുക്കാനായി ഒരു തുക നൽകാനും നിങ്ങളോട് ആവശ്യപ്പെടുന്നു. ഈ പണം സാധാരണ നഷ്ടപ്പെടുകയും ചെയ്യുന്നു.

നിങ്ങളുടെ ഇന്റർനെറ്റ് ബാങ്കിംഗ് വിശദാംശങ്ങൾ ആരെങ്കിലും മനസ്സിലാക്കിയെന്നു നിങ്ങൾ സംശയിക്കുന്നുവെങ്കിൽ, ഉടൻ ഇന്റർനെറ്റ് ബാങ്കിംഗിലേക്ക് ലോഗിൻ ചെയ്ത് നിങ്ങളുടെ പാസ്വേഡ് മാറ്റുക. അല്ലെങ്കിൽ ഉടനെ ഞങ്ങളുടെ ഫോൺ ബാങ്കിംഗ് നമ്പറുകളിൽ ഞങ്ങളെ വിളിക്കുക. ഞങ്ങളുടെ ഫോൺ ബാങ്കിംഗ് നമ്പറുകൾ 24/ 7* പ്രവർത്തിക്കുന്നതാണ്. ഞങ്ങളുടെ ഹോട്ട്ലൈൻ നമ്പർ ഇവിടെ കാണാവുന്നതാണ്.

സോഷ്യൽ മീഡിയ ഹാക്കുകൾ:

തട്ടിപ്പുകാർ ഫേസ്ബുക്ക്, വാട്ട്സ്ആപ്പ്, ഇൻസ്റ്റാഗ്രാം മുതലായവ സോഷ്യൽ മീഡിയ ചാനലിലെ ഒരു ഉറ്റ സുഹൃത്ത് ആണെന്ന വ്യാജേന അവരുടെ കൂട്ടുകാരിൽ നിന്നോ ബന്ധുക്കളിൽ നിന്നോ അടിയന്തിരമായി പണം അഭ്യർത്ഥിക്കും. ഒരു ഫോൺ കോൾ വഴിയോ മറ്റ് രീതികളിലൂടെയോ അത്തരമൊരു അഭ്യർത്ഥനയുടെ നിജസ്ഥിതി അന്വേഷിച്ച ശേഷം മാത്രം പ്രവർത്തിക്കുക.

വിഷിംഗ് കോളുകൾ:

തട്ടിപ്പുകാർ പലപ്പോഴും ഇരകളെ അവരുടെ ഫോൺ നമ്പറുകളിലേക്ക് വിളിച്ച് ബാങ്ക് സ്റ്റാഫ് അല്ലെങ്കിൽ വ്യാപാരി സ്ഥാപനത്തിന്റെ കസ്റ്റമർ സർവീസ് എക്സിക്യൂട്ടീവ് എന്ന വ്യാജേന സംസാരിച്ച് ബാങ്ക് അക്കൗണ്ട് വിശദാംശങ്ങൾ പോലുള്ള സെൻസിറ്റീവ് വിവരങ്ങൾ കരസ്ഥമാക്കുന്നു. സോഷ്യൽ എഞ്ചിനീയറിംഗ് വഴി നേരത്തെ തന്നെ ഇരയെ കുറിച്ച് ലഭ്യമാക്കിയ ചില വിവരങ്ങൾ ഇരയ്ക്ക് നൽകി അവർ ഇരയുടെ വിശ്വാസം നേടുന്നു. വിശ്വാസം സ്ഥാപിച്ചുകഴിഞ്ഞാൽ, അവർ ചില ഓഫറുകൾ തിരഞ്ഞെടുക്കുന്നതിനായി ഇരകളെ കബളിപ്പിക്കുകയോ വശീകരിക്കുകയോ ചെയ്യുന്നു. ബാങ്ക് വിശദാംശങ്ങളും വൺടൈം പാസ് കോഡുകളും (ഒടിപി) ഉൾപ്പെടെയുള്ള രഹസ്യവിവരങ്ങൾ ഇരതിൽ നിന്ന് നേടിയെടുക്കുന്നതിനു വേണ്ടിയാണിത്.

ട്രോജൻ:

തട്ടിപ്പുകാർ ഫയലുകൾ, പേജുകൾ അല്ലെങ്കിൽ അറ്റാച്ചുമെന്റുകൾ അടങ്ങിയ നിങ്ങൾ ആവശ്യപ്പെട്ടിട്ടില്ലാത്ത ഇമെയിലുകൾ നിങ്ങൾക്കയച്ച് അറ്റാച്ച്മെന്റുകൾ തുറക്കാൻ ആവശ്യപ്പെടും. നിങ്ങൾ മെയിൽ തുറന്നുകഴിഞ്ഞാൽ, നിങ്ങളുടെ ഓൺലൈൻ പ്രവർത്തനം നിരീക്ഷിക്കാൻ കഴിയുന്ന ഒരു പ്രോഗ്രാം അവർക്ക് രഹസ്യമായി നിങ്ങളുടെ സിസ്റ്റത്തിൽ ഇൻസ്റ്റാൾ ചെയ്യാൻ കഴിയും, ഏത് വെബ്സൈറ്റിൽ എന്തു വിവരം ആണ് ടൈപ്പ് ചെയ്യുന്നതെന്ന് കണ്ടെത്താനും അവർക്ക് സാധിക്കും. ഓൺലൈൻ ഷോപ്പിംഗ് വെബ്സൈറ്റിൽ അടുത്ത തവണ ക്രെഡിറ്റ് കാർഡ് വിശദാംശങ്ങൾ നൽകുമ്പോൾ, നിങ്ങൾ ടൈപ്പുചെയ്തതെല്ലാം തട്ടിപ്പുകാർക്ക് ലഭിക്കുമെന്നർത്ഥം.

ഓൺലൈൻ സുരക്ഷയ്ക്കായി എച്ച്എസ്ബിസി കൈക്കൊണ്ട നടപടികൾ

മൾട്ടി–ലെയർ ലോഗോൺ വെരിഫിക്കേഷൻ

തനത് യൂസർ നെയിമിന്റെയും പാസ്വേഡിന്റെയും സങ്കീർണ്ണമായ സംയോജനവും നിങ്ങളുടെ ഫിസിക്കൽ സെക്യൂരിറ്റി ഡിവൈസ് / ഡിജിറ്റൽ സെക്യുവർ കീ സൃഷ്ടിച്ച വൺ ടൈം സെക്യൂരിറ്റി കോഡും ഉപയോഗിച്ച് നിങ്ങളുടെ സാമ്പത്തിക വിവരങ്ങൾ പരിരക്ഷിച്ചിരിക്കുന്നു.

ഇടപാട് സ്ഥിരീകരണം

കാർഡുകളിലെ 3ഡി സുരക്ഷിത ഇടപാടുകൾ, ഇടപാടുകൾ സുരക്ഷിതമാക്കാനും പേയ്മെന്റ് സിസ്റ്റത്തിലുള്ള വിശ്വാസം ഉറപ്പിക്കാനും സഹായിക്കുന്നു. ഇടപാടിനായി സൃഷ്ടിച്ച ഒടിപികൾ ഒരിക്കലും ആരുമായും പങ്കിടരുത്.

128–ബിറ്റ് സെക്യൂർ സോക്കറ്റ് ലെയർ (എസ്എസ്എൽ) എൻക്രിപ്ഷൻ

ഇൻറർനെറ്റ് ബാങ്കിംഗ് സെഷനിൽ കൈമാറുന്ന വിവരങ്ങൾക്കായി എച്ച്എസ്ബിസി 128–ബിറ്റ് സെക്യൂർ സോക്കറ്റ് ലെയർ (എസ്എസ്എൽ) എൻക്രിപ്ഷൻ ആണ് ഉപയോഗിക്കുന്നത്. എൻക്രിപ്ഷനുള്ള ഇൻഡസ്ട്രി നിലവാരമായി അംഗീകരിക്കപ്പെടുന്നതാണ് ഇത്.

ഓട്ടോമാറ്റിക് 'ടൈം-ഔട്ട്' സവിശേഷത

ഒരു സുരക്ഷാ നടപടിയെന്ന നിലയിൽ, നിങ്ങളുടെ ഇന്റർനെറ്റ് ബാങ്കിംഗ് സെഷൻ ഒരു നിശ്ചിത സമയം നേരം ഉപയോഗിക്കാതിരിക്കുകയാണെങ്കിൽ അത് ഓട്ടോമാറ്റിക് ആയി ഷട്ട്ഡൗൺ ആകും അല്ലെങ്കിൽ ടൈം ഔട്ട് ആകും. നിങ്ങൾ പൂർത്തിയാക്കുമ്പോൾ എല്ലായ്പ്പോഴും നിങ്ങളുടെ ഇന്റർനെറ്റ് ബാങ്കിംഗ് സെഷൻ ക്ലോസ് ചെയ്യേണ്ടതാണ്.

സുരക്ഷാ ഉപകരണം / ഡിജിറ്റൽ സെക്യൂവർ കീ

നിങ്ങളുടെ ഫിസിക്കൽ സെക്യൂരിറ്റി ഡിവൈസ് / ഡിജിറ്റൽ സെക്യൂർ കീ ഓൺലൈൻ സുരക്ഷയെ ഉയർന്ന തലങ്ങളിലെത്തിക്കുന്നു. ഇന്റർനെറ്റ് ബാങ്കിംഗിൽ നിങ്ങളുടെ അക്കൗണ്ടിലേക്ക് ലോഗിൻ ചെയ്യുമ്പോൾ, പതിവുപോലെ നിങ്ങളുടെ നിലവിലുള്ള യൂസർനെയിമും പാസ്വേഡും തുടർന്ന് ഫിസിക്കൽ സെക്യൂരിറ്റി ഡിവൈസ് / ഡിജിറ്റൽ സെക്യൂർ കീ സൃഷ്ടിച്ച യുണീക് സെക്യൂരിറ്റി കോഡും നൽകേണ്ടതുണ്ട്. ഈ 2 സ്റ്റെപ്പ് പ്രാമാണീകരണ പ്രക്രിയ നിങ്ങളുടെ ഇന്റർനെറ്റ് ബാങ്കിംഗിലേക്കുള്ള ആക്സസിന് മെച്ചപ്പെട്ട സുരക്ഷ നൽകുന്നു.

ഓൺലൈൻ സുരക്ഷയിൽ നിങ്ങളുടെ പങ്ക്

ഇന്റർനെറ്റ് ബാങ്കിംഗ് സുരക്ഷ ഉറപ്പാക്കാൻ ഇനിപ്പറയുന്ന ചെയ്യേണ്ടതും ചെയ്യരുതാത്തതുമായ നടപടികൾ സ്വീകരിക്കുക:

ചെയ്യേണ്ടത്

- നിങ്ങളുടെ കമ്പ്യൂട്ടർ എല്ലായ്പ്പോഴും ഏറ്റവും പുതിയ ആന്റി വൈറസ്, ഫയർവാൾ പരിരക്ഷണ സോഫ്റ്റ്വെയർ ഉപയോഗിച്ച് പരിരക്ഷിച്ചിട്ടുണ്ടെന്ന് ഉറപ്പാക്കുക. നിങ്ങൾക്ക് ഏറ്റവും പുതിയ പരിരക്ഷ ഉണ്ടെന്ന് ഉറപ്പാക്കാൻ പതിവായി അപ്ഡേറ്റുകൾ ഡൗൺലോഡുചെയ്യുക.
- നിങ്ങൾക്ക് ഓർത്തു വയ്ക്കാവുന്നതും എന്നാൽ മറ്റൊരാൾക്ക് ഊഹിക്കാൻ എളുപ്പമല്ലാത്തതുമായ ഒരു പാസ്വേഡ് തിരഞ്ഞെടുക്കുക. ആൽഫ ന്യൂമെറിക് പ്രതീകങ്ങളുടെ സംയോജനം അടങ്ങിയിരിക്കുന്ന പാസ്വേഡുകൾ സാധാരണയായി ഊഹിക്കാൻ പ്രയാസമാണ് (ഉദാ. A7g3cy91)
- നിങ്ങളുടെ ഇന്റർനെറ്റ് ബാങ്കിംഗ് പാസ്വേഡ് പതിവായി മാറ്റുക.
- ഫിഷിംഗ് ഇമെയിലുകൾ സൂക്ഷിക്കുക. എല്ലാ അക്ഷരമാലകളും പ്രതീകങ്ങളും ഉൾപ്പെടെ മുഴുവൻ ഇമെയിൽ വിലാസവും എല്ലായ്പ്പോഴും ശ്രദ്ധാപൂർവ്വം വായിക്കുക.
- സമാനമായി തോന്നിക്കുന്ന ഇമെയിൽ വിലാസങ്ങളിലൂടെയാണ് സാധാരണ ഫിഷിംഗ് നടക്കുന്നത്. ഉദാ. hsdc.co.in അല്ലെങ്കിൽ hsbcbank.com. നിങ്ങളുടെ മൗസ് പോയിന്റർ അതിന്റെ യഥാർത്ഥ ലക്ഷ്യസ്ഥാനം വെളിപ്പെടുത്തുന്നതിന് യൂആർ എല്ലിലൂടെ റോൾ ചെയ്യുക; ഇത് നിങ്ങളുടെ ബ്രൗസറിന്റെ ചുവടെ ഇടത് കോണിൽ കാണിക്കുന്നതാണ്. പൊരുത്തക്കേട് ഉണ്ടെങ്കിൽ ലിങ്കിൽ ക്ലിക്കുചെയ്യരുത്. യൂആർ എല്ലിൽ അക്ഷര പിശകുകൾ, വ്യാകരണ പിശകുകൾ,അല്ലെങ്കിൽ ക്രമം മാറിയ അക്ഷരങ്ങൾ തുടങ്ങിയ അടയാളങ്ങൾ ശ്രദ്ധിക്കുക
- നിങ്ങളുടെ അക്കൗണ്ടിൽ ആവശ്യമില്ലെങ്കിൽ അധികമായുള്ള ഗുണഭോക്താക്കളെ ഇല്ലാതാക്കുക
- നിങ്ങളുലോഗോൺ വിശദാംശങ്ങൾ ഓർത്തു വയ്ക്കുന്ന കമ്പ്യൂട്ടറിലോ ബ്രൗസറുകളിലോ പ്രവർത്തനം അവസാനിപ്പിക്കുക
- നിങ്ങളുടെ സിസ്റ്റവും വെബ് ബ്രൗസറും അപ്ഡേറ്റ് ചെയ്യുക. സിസ്റ്റങ്ങളിലും ബ്രൗസറുകളിലും പോരായ്മകൾ കണ്ടെത്തുമ്പോൾ നിർമ്മാതാക്കൾ പതിവായി സുരക്ഷാ പാച്ചുകൾ പുറത്തിറക്കുന്നു. ഈ അപ്ഡേറ്റുകൾക്കായി നിങ്ങളുടെ സോഫ്റ്റ്വെയർ ദാതാക്കളെ പതിവായി പരിശോധിക്കുക.
- നിങ്ങളുടെ മൊബൈൽ ബാങ്കിംഗ് അപ്ലിക്കേഷൻ അപ്ഡേറ്റ് ചെയ്യുക. ഡൗൺലോഡിനും ആപ്പിന്റെ തുടർന്നുള്ള അപ്ഡേറ്റുകൾക്കും പ്ലേ സ്റ്റോർ സന്ദർശിക്കുക. വിശ്വസനീയമല്ലാത്ത ഉറവിടങ്ങളിൽ നിന്ന് വന്ന മെയിലുകളിലെ ലിങ്കുകളിൽ നിന്ന് ഒരിക്കലും മൊബൈൽ ബാങ്കിംഗ് / പേയ്മെന്റ് ആപ്പ് ഡൗൺലോഡ് ചെയ്യരുത്.
- ബാങ്കിന്റെ വെബ്സൈറ്റിൽ എത്താൻ എല്ലായ്പ്പോഴും ബ്രൗസറിൽ ബാങ്കിന്റെ യുആർ എൽ ടൈപ്പുചെയ്യുക.
- പാഡ്ലോക്ക് ചിഹ്നവും സൈറ്റ് സർട്ടിഫിക്കറ്റും പരിശോധിക്കുക. സൈറ്റ് സർട്ടിഫിക്കറ്റ് എച്ച്എസ്ബിസിയുടേതാണെന്ന് ഉറപ്പാക്കാൻ നിങ്ങൾ എച്ച്എസ്ബിസി ഓൺലൈൻ ബാങ്കിംഗിലേക്ക് ലോഗിൻ ചെയ്യുമ്പോൾ നിങ്ങളുടെ ബ്രൗ സറിന്റെ ചുവടെയുള്ള പാഡ്ലോക്ക് ചിഹ്നത്തിൽ ഡബിൾക്ലിക്കുചെയ്യുക. ഒരു 'വ്യാജ' സൈറ്റിൽ നിങ്ങളുടെ വിശദാംശങ്ങൾ നൽകുന്നില്ലെന്ന് ഉറപ്പാക്കാൻ ഇത് സഹായിക്കും.
- നിങ്ങളുടെ അക്കൗണ്ടുകൾ പതിവായി പരിശോധിക്കുക. എന്തെങ്കിലും ഇടപാടുകളെക്കുറിച്ച് സംശയമുണ്ടെങ്കിൽ, വിശദാംശങ്ങൾ ശ്രദ്ധിച്ച ശേഷം ഞങ്ങളെ വിളിക്കുക.

- ഓൺലൈൻ ബാങ്കിംഗ് ഉപയോഗിച്ചതിന് ശേഷം എല്ലായ്പ്പോഴും ലോഗ് ഔട്ട് ചെയ്യുക. ഇതിനായി ലോഗ് ഔട്ട് ബട്ടൺ ക്ലിക്ക് ചെയ്യുക. നിങ്ങൾ സേവനത്തിലേക്ക് ലോഗിൻ ചെയ്താൽ നിങ്ങളുടെ പിസി ശ്രദ്ധിക്കാതെ വിടരുത്.
- ബാങ്കുകളുടെ കസ്റ്റമർ കെയർ നമ്പറുകൾ, ഓൺലൈൻ ഷോപ്പിംഗ് വെബ്സൈറ്റ് എന്നിവ ഇന്റർനെറ്റിൽ തിരയുമ്പോൾ വിവേകത്തോടെ തിരയുക. തട്ടിപ്പുകാർ തിരച്ചിലിൽ അവരുടെ മൊബൈൽ നമ്പറുകൾ ലഭിക്കുന്ന വിധത്തിൽ തിരയലുകൾ ക്രമീകരിച്ചിട്ടുണ്ടാകും. ബാങ്കിന്റെ യഥാർത്ഥ കസ്റ്റമർ കെയർ നമ്പറിനോ ഇ-കൊമേഴ്സ് വെബ്സൈറ്റിനോ പകരം നിങ്ങൾ തട്ടിപ്പുകാരെ വിളിക്കുകയും നിങ്ങൾ വഞ്ചിക്കപ്പെടുകയും ചെയ്തേക്കാം.
- നിങ്ങളുടെ ബാങ്കിന്റെ കോൺടാക്റ്റ് സെന്റർ നമ്പർ നിങ്ങളുടെ ഉപകരണങ്ങളിൽ സേവ് ചെയ്തു വയ്ക്കുക. അല്ലെങ്കിൽ നിങ്ങളുടെ ക്രെഡിറ്റ് / ഡെബിറ്റ് കാർഡിന് പിന്നിൽ എഴുതിയ നമ്പർ ഉപയോഗിക്കുക

ചെയ്യരുതാത്തവ

- മറ്റ് സേവനങ്ങൾക്കായി നിങ്ങൾ ഉപയോഗിക്കുന്ന പാസ്വേഡ് ഇവിടെ തിരഞ്ഞെടുക്കരുത്. നിങ്ങളുടെ പാസ്വേഡ് ഇന്റർനെറ്റ് ബാങ്കിംഗിന് മാത്രമായിരിക്കണം
- ഇമെയിൽ / എസ്എംഎസിലൂടെ ലഭിച്ച ലിങ്കുകൾ അശ്രദ്ധമായി ക്ലിക്കുചെയ്യുകയാണെങ്കിൽ തുറക്കുന്ന വെബ്പേജുകളിൽ യൂസർ ഐഡി, പാസ്വേഡ്, കാർഡ് നമ്പർ, കാലഹരണപ്പെടൽ തീയതി സിവിവി മുതലായ വിശദാംശങ്ങൾ വെളിപ്പെടുത്തരുത്.
- ബാങ്ക് ജീവനക്കാരിൽ നിന്നോ അല്ലെങ്കിൽ ഇൻകം ടാക്സ് വകുപ്പ്, ആർബിഐ പോലുള്ള സർക്കാർ സ്ഥാപനങ്ങളിൽ നിന്നോ ആണെന്ന് അവകാശപ്പെട്ടുകൊണ്ട് അത്തരം വിശദാംശങ്ങൾ ആവശ്യപ്പെടുന്ന സന്ദേശങ്ങളോട് പ്രതികരിക്കരുത്. എച്ച്എസ്ബിസിയിൽ നിന്ന് ആരും ഒരിക്കലും ഇത്തരം വിവരങ്ങൾ നിങ്ങളോട് ആവശ്യപ്പെടില്ല.
- നിങ്ങളുടെ പാസ്വേഡ് തിരിച്ചറിയാവുന്ന രൂപത്തിൽ എഴുതരുത്, നിങ്ങളുടെ ലോഗോൺ വിശദാംശങ്ങൾ നിങ്ങളുടെ ഫിസിക്കൽ സെക്യൂരിറ്റി ഡിവൈസ് / ഡിജിറ്റൽ സെക്യൂരിറ്റി കീ എന്നിവയ്ക്കൊപ്പം ഒരിക്കലും ഇടരുത്.
- നിങ്ങളുടെ മൊബൈൽ ബാങ്കിംഗ് അപ്ലിക്കേഷൻ അപ്ഡേറ്റ് ചെയ്യുക. ഡൗൺലോഡിനും ആപ്പിന്റെ തുടർന്നുള്ള അപ്ഡേറ്റുകൾക്കും പ്ലേ സ്റ്റോർ സന്ദർശിക്കുക.
- വിശ്വസനീയമല്ലാത്ത ഉറവിടങ്ങളിൽ നിന്ന് വന്ന മെയിലുകളിലെ ലിങ്കുകളിൽ നിന്ന് ഒരിക്കലും മൊബൈൽ ബാങ്കിംഗ് / പേയ്മെന്റ് ആപ്പ് ഡൗൺലോഡ് ചെയ്യരുത്.
- ഓൺലൈൻ വെബ്സൈറ്റുകളിൽ കാർഡ് നമ്പറും കാലഹരണപ്പെടൽ തീയതികളും സേവ് ചെയ്യുന്നതിൽ ജാഗ്രത പാലിക്കുക. അപൂർവ്വമായി ഉപയോഗിക്കുന്ന വെബ്സൈറ്റുകളിലും വിശ്വസനീയമല്ലാത്ത വെബ്സൈറ്റുകളിലും ഈ വിശദാംശങ്ങൾ സേവ് ചെയ്യാൻ അനുമതി നൽകരുത്.
- നിങ്ങളുടെ പിൻ മറ്റാരുമായും ഷെയർ ചെയ്യരുത്. അത് നിങ്ങൾ മാത്രമേ ഉപയോഗിക്കാബൂ. നിങ്ങളുടെ പിൻ മാറ്റാരെങ്കിലും മനസ്സിലാക്കി എന്നു തോന്നിയാലുടൻ അത് മാറ്റുക.
- യുപിഐ പിൻ ചോദിക്കുകയാണെങ്കിൽ ഓർക്കുക, നിങ്ങൾ പണം അടയ്ക്കുകയാണ് ചെയ്യുന്നത്. ഒരു പേയ്മെന്റ് സ്വീകരിക്കുന്നതിന് യുപിഐ പിൻ ഉപയോഗിക്കേണ്ട ആവശ്യമില്ല.
- പൊതു കമ്പ്യൂട്ടറുകൾ ഉപയോഗിക്കുമ്പോൾ ജാഗ്രത പാലിക്കുക

എല്ലായ്പോഴും

- ഒരു നിമിഷത്തേക്കാണെങ്കിൽ പോലും നിങ്ങൾ കമ്പ്യൂട്ടർ വിട്ടിട്ടു പോകുകയാണെങ്കിൽ, അത് ലോഗ് ഔട്ട് ചെയ്യുക. സാധ്യമെങ്കിൽ, നിങ്ങൾ ലോഗിൻ ചെയ്തിരിക്കുമ്പോൾ കമ്പ്യൂട്ടർ ശ്രദ്ധിക്കാതെ വിടരുത്.
- കമ്പ്യൂട്ടറിൽ നിന്ന് ലോഗ് ഔട്ട് ചെയ്യുന്നതിന് മുമ്പ് നിങ്ങളുടെ ബ്രൗസിംഗ് ഹിസ്റ്ററി ഡിലീറ്റ് ചെയ്യുക: ഇന്റർനെറ്റ് ബ്രൗസറുകൾ നിങ്ങളുടെ പാസ്വേഡുകളെയും നിങ്ങൾ സന്ദർശിക്കുന്ന പേജുകളെയും കുറിച്ചുള്ള വിവരങ്ങൾ സേഫ്വ് ചെയ്തു വയ്ക്കുന്നു. ഇന്റർനെറ്റ് ബ്രൗസറിന്റെ ടൂൾസ് മെനുവിലേക്ക് പോയി ഓപ്ഷനുകൾ അല്ലെങ്കിൽ ഇന്റർനെറ്റ് ഓപ്ഷനുകൾ തിരഞ്ഞെടുക്കുക. ഓട്ടോ കംപ്ലീറ്റ് പ്രവർത്തനം ഓഫാക്കുക, കുക്കികൾ ഉണ്ടെങ്കിൽ അവയെ ഇല്ലാതാക്കി ഹിസ്റ്ററി ഡിലീറ്റ് ചെയ്യുക.
- ലൈബ്രറികൾ, ഇൻറർനെറ്റ് കഫേകൾ, സ്കൂളുകൾ എന്നിവിടങ്ങൾ ഉൾപ്പെടെ പൊതു കമ്പ്യൂട്ടറുകളിൽ നിങ്ങളുടെ ബാങ്കിംഗ് ചെയ്യുന്നത് ഒഴിവാക്കുക.

പ്രധാനപ്പെട്ട വിവരങ്ങൾ ടൈപ്പ് ചെയ്യരുത്: മുകളിൽ കൊടുത്തിരിക്കുന്ന മുൻകരുതലുകൾ നിങ്ങൾ എടുക്കുകയാണെങ്കിലും, പൊതു ഇടങ്ങളിലെ കമ്പ്യൂട്ടറിൽ ഒരു കീസ്ട്രോക്ക് ലോഗർ എന്ന ക്ഷുദ്ര സോഫ്റ്റ്വെയർ ഇൻസ്റ്റാൾ ചെയ്യാനുള്ള സാധ്യതയുണ്ട്. ഇവയ്ക്ക് നിങ്ങളുടെ പാസ്വേഡ്, ക്രെഡിറ്റ് കാർഡ് നമ്പർ, ബാങ്ക് വിശദാംശങ്ങൾ എന്നിവ മോഷ്ടിക്കാൻ കഴിയും. പ്രധാനപ്പെട്ട വിവരങ്ങൾ വെളിപ്പെട്ടേക്കാവുന്ന സാമ്പത്തിക ഇടപാടുകൾ നടത്തുന്നത് ഒഴിവാക്കുക.

പ്രധാനപ്പെട്ട കാര്യം: വിശ്വസനീയമല്ലാത്ത ഉറവിടത്തിൽ നിന്ന് നിങ്ങൾക്ക് എച്ച്എസ്ബിസി എന്ന പേരിൽ ഇമെയിൽ ലഭിച്ചിട്ടുണ്ടെങ്കിൽ അല്ലെങ്കിൽ വ്യക്തിഗത വിവരങ്ങൾ തേടുന്ന, നിങ്ങൾ ആവശ്യപ്പെടാത്ത ഇമെയിൽ ലഭിച്ചാൽ; കൂടുതൽ അന്വേഷിക്കുന്നതിന് ഞങ്ങൾക്ക് ഇത് **phishing@hsbc.com** ൽ റിപ്പോർട്ടുചെയ്യുക.

Issued by The Hongkong and Shanghai Banking Corporation Limited, India. Incorporated in Hong Kong SAR with limited liability.