DCB BANK

<u>അനുബന്ധം 7: ഉപഭോക്തൃ അവബോധം–സൈബർ ഭീഷണികളും തട്ടിപ്പുകളും</u>

സോഷ്യൽ മീഡിയ ടെക്നിക്കുകൾ, മൊബൈൽ ഫോൺ കോളുകൾ തുടങ്ങി നൂതനമായ പ്രവർത്തനരീതികൾ ഉപയോഗിച്ച് പല തട്ടിപ്പുകാരും പൊതുജനങ്ങളെ വഞ്ചിക്കുകയും തെറ്റിദ്ധരിപ്പിക്കുകയും ചെയ്യുന്നതായി കണ്ടു വരുന്നു. ഇത് കണക്കിലെടുത്ത്, ഇളവുകൾ ഉറപ്പാക്കുന്നതിന് സഹായം വാഗ്ദാനം ചെയ്ത് /ബാങ്കുകളിൽ നിന്നും സാമ്പത്തിക സേവന ദാതാക്കളിൽ നിന്നും പ്രതികരണം വേഗത്തിലാക്കാമെന്നും വാഗ്ദാനം ചെയ്ത് വ്യാജ സന്ദേശങ്ങൾ, വ്യാജ കോളുകൾ, അജ്ഞാതമായ ലിങ്കുകൾ , തെറ്റായ അറിയിപ്പുകൾ, അനധികൃത ക്യുആർ കോഡുകൾ മുതലായവയെക്കുറിച്ച് ജാഗ്രത പാലിക്കണമെന്ന് ഡിസിബി ബാങ്ക് പൊതുജനങ്ങൾക്ക് മുന്നറിയിപ്പ് നൽകുന്നു.

യൂസർ ഐഡി, ലോഗിൻ/ട്രാൻസാക്ഷൻ പാസ്വേഡ്, വൺടൈം പാസ്വേഡ് (ഒടിപി), പിൻ, സിവിവി, എക്സ്പയറി ഡേറ്റ്, മറ്റ് വ്യക്തിഗത വിവരങ്ങൾ തുടങ്ങിയ പോലുള്ള ഡെബിറ്റ്/ക്രെഡിറ്റ് കാർഡ് രഹസ്യ വിവരങ്ങൾ ലഭിക്കാൻ തട്ടിപ്പുകാർ ശ്രമിക്കുന്നു. തട്ടിപ്പുകാർ ഉപയോഗിക്കുന്ന സാധാരണ പ്രവർത്തനരീതി ഇവയാണ്:

• കെവൈസി അപ്ഡേറ്റ് ചെയ്യൽ, അക്കൗണ്ട്/സിം കാർഡ് അൺബ്ലോക്ക് ചെയ്യൽ, ഡെബിറ്റഡ് തുക ക്രെഡിറ്റ് ചെയ്യൽ തുടങ്ങിയവയുടെ മറവിൽ രഹസ്യസ്വഭാവമുള്ള വിശദാംശങ്ങൾ പങ്കിടാൻ ഉപഭോക്താക്കളെ പ്രേരിപ്പിക്കാൻ ബാങ്ക്/ബാങ്ക് ഇതര ഇ–വാലറ്റ് ദാതാക്കൾ/ടെലികോം സേവന ദാതാക്കളിൽ നിന്നാണെന്ന് നടിക്കുന്ന വ്യാജ ഫോൺ കോളുകൾ.

• ഫിഷിംഗ് – തങ്ങളുടെ ബാങ്ക്/ഇ–വാലറ്റ് ദാതാവിൽ നിന്ന് വരുന്നതാണെന്ന് തോന്നിപ്പിക്കുന്ന വിധം തയ്യാറാക്കിയ തട്ടിപ്പ് ഇമെയിലുകളും കൂടാതെ/അല്ലെങ്കിൽ എസ്എംഎസും. ഇതിൽ രഹസ്യസ്വഭാവമുള്ള വിശദാംശങ്ങൾ എക്സ്ട്രാക്റ്റുചെയ്യുന്നതിനുള്ള ലിങ്കുകൾ അടങ്ങിയിട്ടുള്ളതും ഉപഭോക്താക്കളെ കബളിപ്പിക്കാൻ ഉദ്ദേശിച്ചുള്ളതും ആയിരിക്കും.

• റിമോട്ട് ആക്സസ് – ഉപഭോക്താവിന്റെ ഉപകരണത്തിലെ ഡാറ്റ ആക്സസ് ചെയ്യാൻ കഴിയുന്ന ഒരു ആപ്ലിക്കേഷൻ തങ്ങളുടെ മൊബൈൽ ഫോണിൽ/കമ്പ്യൂട്ടറിൽ ഡൗൺലോഡ് ചെയ്യാൻ ഉപഭോക്താക്കളെ പ്രേരിപ്പിക്കുന്നു.

• പണം സ്വീകരിക്കുന്നതിന് 'നിങ്ങളുടെ യുപിഐ പിൻ നൽകുക' എന്നതുപോലുള്ള സന്ദേശങ്ങളുള്ള വ്യാജ പേയ്മെന്റ് അഭ്യർത്ഥനകൾ അയച്ചുകൊണ്ട് യുപിഐയുടെ 'കളക്ട് റിക്വസ്റ്റ്' ഫീച്ചർ ദുരുപയോഗം ചെയ്യുന്നു.

• വെബ്പേജുകളിൽ/സോഷ്യൽ മീഡിയയിൽ ബാങ്കുകളുടെ/ഇ–വാലറ്റ് ദാതാക്കളുടെ വ്യാജ കോൺടാക്റ്റ് നമ്പറുകൾ, സെർച്ച് എഞ്ചിനുകൾ മുതലായവ പ്രദർശിപ്പിക്കുന്നു.

ഏതെങ്കിലും ഡിജിറ്റൽ (ഓൺലൈൻ/മൊബൈൽ) ബാങ്കിംഗ്/പേയ്മെന്റ് ഇടപാടുകൾ നടത്തുമ്പോൾ, എല്ലാ മുൻകരുതലുകളും സ്വീകരിച്ചുകൊണ്ട് സുരക്ഷിത ഡിജിറ്റൽ ബാങ്കിംഗ് പരിശീലിക്കാൻ ഡിസിബി ബാങ്ക് പൊതുജനങ്ങളോട് അഭ്യർത്ഥിക്കുന്നു. സാമ്പത്തികമായ ഒപ്പം/അല്ലെങ്കിൽ മറ്റ് നഷ്ടങ്ങൾ തടയാൻ ഇവ സഹായിക്കും.

സുരക്ഷിത ഡിജിറ്റൽ ബാങ്കിംഗ് ശീലങ്ങൾ

• അക്കൗണ്ട് നമ്പർ, ലോഗിൻ ഐഡി, പാസ്വേഡ്, പിൻ, യുപിഐ–പിൻ, ഒടിപി, എടിഎം/ഡെബിറ്റ് കാർഡ്/ക്രെഡിറ്റ് കാർഡ് എന്നിവ പോലുള്ള നിങ്ങളുടെ അക്കൗണ്ട് വിശദാംശങ്ങൾ ആരുമായും, ബാങ്ക് ഉദ്യോഗസ്ഥരുമായി പോലും പങ്കിടരുത്, അവ എത്ര യഥാർത്ഥമാണെന്നു തോന്നിയാൽ പോലും.

• കെവൈസി അപ്ഡേറ്റ് ചെയ്യാത്തതിന്റെ പേരിൽ നിങ്ങളുടെ അക്കൗണ്ട് ബ്ലോക്ക് ചെയ്യുമെന്ന് ഭീഷണിപ്പെടുത്തുന്ന ഫോൺ കോളും/ഇമെയിലും അത് അപ്ഡേറ്റ് ചെയ്യുന്നതിന് ലിങ്ക് ക്ലിക്ക് ചെയ്യാനുള്ള നിർദ്ദേശവും തട്ടിപ്പുകാരുടെ ഒരു സാധാരണ പ്രവർത്തനരീതിയാണ്. കെവൈസി അപ്ഡേറ്റ്/വേഗത്തിലാക്കാനുള്ള ഓഫറുകളോട് പ്രതികരിക്കരുത്. എപ്പോഴും നിങ്ങളുടെ ബാങ്ക്/എൻബിഎഫ്സി/ഇ–വാലറ്റ് ദാതാവിന്റെ ഔദ്യോഗിക വെബ്സൈറ്റ് ആക്സസ് ചെയ്യുക അല്ലെങ്കിൽ ബ്രാഞ്ചുമായി ബന്ധപ്പെടുക.

• നിങ്ങളുടെ ഫോണിലോ ഉപകരണത്തിലോ അറിയാത്ത ആപ്പ് ഒന്നും ഡൗൺലോഡ് ചെയ്യരുത്. ആപ്പ് നിങ്ങളുടെ രഹസ്യ വിവരങ്ങൾ രഹസ്യമായി ആക്സസ് ചെയ്തേക്കാം.

• പണം സ്വീകരിക്കുന്നത് ഉൾപ്പെടുന്ന ഇടപാടുകൾക്ക് ബാർകോഡുകളോ ക്യുആർ കോഡുകളോ സ്കാൻ ചെയ്യുകയോഎംപിൻ നൽകുകയോ ചെയ്യേണ്ട ആവശ്യമില്ല. അതിനാൽ, അങ്ങനെ ചെയ്യാൻ ആവശ്യപ്പെട്ടാൽ ജാഗ്രത പാലിക്കുക.

• ബന്ധപ്പെടാനുള്ള വിശദാംശങ്ങൾക്കായി എപ്പോഴും ബാങ്ക്/എൻബിഎഫ്സി/ഇ–വാലറ്റ് ദാതാവിന്റെ ഔദ്യോഗിക വെബ് സൈറ്റ് ആക്സസ് ചെയ്യുക. ഇന്റർനെറ്റ് സെർച്ച് എഞ്ചിനുകളിലെ കോൺടാക്റ്റ് നമ്പറുകൾ വ്യാജമായിരിക്കാം.

• ഇമെയിലുകളിലും എസ്എംഎസുകളിലും ലഭിച്ച യുആർഎല്ലുകളിലും ഡൊമെയ്ൻ നാമങ്ങളിലും സ്പെല്ലിംഗ് പിശകുകൾ ഉണ്ടോ എന്ന് പരിശോധിക്കുക. ഓൺലൈൻ ബാങ്കിങ്ങിനായി പരിശോധിച്ചുറപ്പിച്ചതും സുരക്ഷിതവും വിശ്വസനീയവുമായ വെബ്സൈറ്റുകളും ആപ്പുകളും മാത്രം ഉപയോഗിക്കുക, അതായത് "https'' എന്ന് തുടങ്ങുന്ന വെബ്സൈറ്റുകൾ. സംശയാസ്പദമായ ഒരു യുആർഎൽ അല്ലെങ്കിൽ വെബ്സൈറിനെ കുറിച്ച് ഉടൻ തന്നെ ലോക്കൽ പോലീസ്/സൈബർ ക്രൈം ബ്രാഞ്ചിനെ അറിയിക്കണം.

• നിങ്ങൾക്ക് അറിവില്ലാത്ത ഒരു ഇടപാടിന് നിങ്ങളുടെ അക്കൗണ്ടിൽ നിന്ന് ഡെബിറ്റ് ചെയ്യാൻ ഒരു കാരണം ലഭിക്കുകയാണെങ്കിൽ, ഉടൻ തന്നെ നിങ്ങളുടെ ബാങ്ക്/ഇ–വാലറ്റ് ദാതാവിനെ അറിയിക്കുക. നടത്താത്ത ഇടപാടിന് ഡെബിറ്റ് എസ്എംഎസ് ലഭിക്കുകയാണെങ്കിൽ, ഉടൻ തന്നെ നിങ്ങളുടെ ബാങ്ക്/ഇ–വാലറ്റ് ദാതാവിനെ അറിയിക്കുകയും യുപിഐ ഉൾപ്പെടെയുള്ള എല്ലാ ഡെബിറ്റ് മോഡുകളും ബ്ലോക്ക് ചെയ്യുകയും ചെയ്യുക. നിങ്ങളുടെ അക്കൗണ്ടിൽ എന്തെങ്കിലും തട്ടിപ്പ് നടന്നതായി നിങ്ങൾ സംശയിക്കുന്നുവെങ്കിൽ, ഇന്റർനെറ്റ്/മൊബൈൽ ബാങ്കിങ്ങിനായി പ്രവർത്തനക്ഷമമാക്കിയിട്ടുള്ള ഗുണഭോക്തൃ ലിസ്റ്റിൽ പുതിയ കൂട്ടിചേർക്കൽ ഉണ്ടോ എന്ന് പരിശോധിക്കുക.

• നിങ്ങളുടെ ബാങ്ക്/ഇ–വാലറ്റ് അക്കൗണ്ടുമായി ലിങ്ക് ചെയ്തിരിക്കുന്ന നിങ്ങളുടെ ഇമെയിലിന്റെ പാസ്വേഡ് ആരുമായും പങ്കിടരുത്. ഇ–കൊമേഴ്സ്/സോഷ്യൽ മീഡിയ സൈറ്റുകൾക്ക് പൊതുവായി കൊടുക്കുന്ന പാസ്വേഡുകളും നിങ്ങളുടെ ബാങ്ക് അക്കൗണ്ടിന്റെയും നിങ്ങളുടെ ബാങ്ക് അക്കൗണ്ടുമായി ലിങ്ക് ചെയ്തിരിക്കുന്ന ഇമെയിലിന്റെയും പാസ്വേഡുകൾ ഒന്നുതന്നെ ആകരുത് . പൊതു, ഓപ്പൺ അല്ലെങ്കിൽ സൗജന്യ വൈഫൈ അല്ലെങ്കിൽ ഇന്റർനെറ്റ് നെറ്റ്വർക്കുകൾ വഴിയുള്ള ബാങ്കിംഗ് ഒഴിവാക്കുക.

• നിങ്ങളുടെ ഇമെയിൽ യൂസർ ഐഡിയായി ഏതെങ്കിലും വെബ്സൈറ്റിൽ/ ആപ്ലിക്കേഷനിൽ രജിസ്റ്റർ ചെയ്യുമ്പോൾ നിങ്ങളുടെ ഇമെയിൽ പാസ്വേഡ് ''പാസ്വേഡ്'' ആയി സജ്ജീകരിക്കരുത്. നിങ്ങളുടെ ഇമെയിൽ ആക്സസ് ചെയ്യാൻ ഉപയോഗിക്കുന്ന പാസ്വേഡ്, പ്രത്യേകിച്ചും നിങ്ങളുടെ ബാങ്ക് അക്കൗണ്ടുമായി ലിങ്ക് ചെയ്തിട്ടുണ്ടെങ്കിൽ, അത് അദ്വിതീയവും ഇമെയിൽ ആക്സസ്സിനായി മാത്രം ഉപയോഗിക്കുന്നതും മറ്റേതെങ്കിലും വെബ്സൈറ്റോ അപ്ലിക്കേഷനോ ആക്സസ്സുചെയ്യുന്നതിന് ഉപയോഗിക്കാൻ പാടില്ലാത്തതുമാണ്.

• വിദേശത്തു നിന്ന് പണമയയ്ക്കുന്നതിനോ കമ്മീഷൻ സ്വീകരിക്കുന്നതിനോ ലോട്ടറി അടിച്ച പണം നിക്ഷേപിക്കുന്നതിനോ വേണ്ടി ആർബിഐയിൽ നിങ്ങളുടെ പേരിൽ പണം നിക്ഷേപിക്കുന്നതിനെക്കുറിച്ചോ ഉള്ള സന്ദേശങ്ങൾ വിശ്വസിക്കരുത്.

• നിങ്ങളുടെ സാമ്പത്തിക സേവന ദാതാവിൽ നിന്നുള്ള അലേർട്ടുകൾക്കായി നിങ്ങളുടെ ഇമെയിൽ, ഫോൺ സന്ദേശങ്ങൾ പതിവായി പരിശോധിക്കുക. നിങ്ങളുടെ അക്കൗണ്ടിൽ ഏതെങ്കിലും അനധികൃത ഇടപാട് സംശയിക്കപ്പെട്ടാൽ ഉടൻ തന്നെ കാർഡ്, അക്കൗണ്ട്, വാലറ്റ് എന്നിവ ബ്ലോക്ക് ചെയ്യുന്നതിനായി നിങ്ങളുടെ ബാങ്ക്/എൻബിഎഫ്സി/സേവന ദാതാവിനെ അറിയിക്കുക.

• നിങ്ങളുടെ എടിഎം, ഡെബിറ്റ്, ക്രെഡിറ്റ് കാർഡുകൾ സുരക്ഷിതമാക്കുകയും ഇടപാടുകൾക്ക് പ്രതിദിന പരിധി നിശ്ചയിക്കുകയും ചെയ്യുക. ഡൊമസ്റ്റിക്/അന്താരാഷ്ട്ര ഉപയോഗത്തിനായി നിങ്ങൾക്ക് പരിധികൾ സജ്ജമാക്കുകയും സജീവമാക്കുകയും/നിർജ്ജീവമാക്കുകയും ചെയ്യാം. ഇത് തട്ടിപ്പ് മൂലമുള്ള നഷ്ടം പരിമിതപ്പെടുത്തും.