ആർ.ബി.ഐ. ഓംബുഡ്സ്മാന്റെ ഓഫീസ്
തിരുവനന്തപുരം

BE (A)WARE

അറിവുള്ളവരാകൂ!
ജാഗരൂകരാകൂ

സാമ്പത്തിക തട്ടിപ്പുകാരുടെ പ്രവർത്തന രീതികളെക്കുറിച്ചുള്ള ഒരു ലഘുലേഖ

ആർ.ബി.ഐ. ഓംബുഡ്സ്മാന്റെ ഓഫീസ്
തിരുവനന്തപുരം

ക്യൂ ആർ കോഡ് (QR code): ക്യൂ ആർ കോഡ് എന്നാൽ വിവരങ്ങൾ ശേഖരിച്ചിട്ടുള്ള ദ്വിമാന ബാർകോഡാണ്. അത് സെൽ ഫോൺ പോലെയുള്ള ഉപകരണം കൊണ്ട് വായിക്കുവാൻ സാധിക്കുന്നതാണ്. വെളുത്ത പശ്ചാത്തലത്തിൽ ചതുര പാളിൽ കറുത്ത ചതുരങ്ങൾ അടങ്ങിയിരിക്കുന്ന ക്യൂ ആർ. കോഡിൽ പണം സ്വീകരിക്കുന്ന വ്യക്തിയെക്കുറിച്ചുള്ള വിവരങ്ങൾ ഉണ്ടായിരിക്കും. വ്യാപാര കേന്ദ്രങ്ങളിൽ ഉപഭോക്താവിന്റെ അക്കൗണ്ട് കിഴിവ് ചെയ്ത് മൊബൈൽ വഴി ഇടപാടുകൾ നടത്തുവാൻ ക്യൂ ആർ കോഡ് സൗകര്യമുണ്ടാക്കുന്നു.

വിദൂരപ്രാപ്തി (റിമോട്ട് ആക്സസ്-Remote Access): ഉപഭോക്താവിനെ പ്രലോഭനത്തിലൂടെ അവരുടെ മൊബൈൽ ഫോണിൽ/കംപ്യൂട്ടറിൽ ആപ്പ് ഡൗൺലോഡ് ചെയ്യിക്കുന്നു. ഈ ആപ്പ് വഴി മൊബൈൽ ഫോണിൽ/കമ്പ്യൂട്ടറിൽ ഉപഭോക്താവിനെ സംബന്ധിച്ചുള്ള എല്ലാ വിവരങ്ങളും ലഭ്യമാകും.

ഏകീകൃത പേയ്മെന്റ് ഇന്റർഫേസ് (യു പി ഐ): ഉപഭോക്താവ് UPIയ്ക്ക് വേണ്ടി ബാങ്കിൽ രജിസ്റ്റർ ചെയ്തുകഴിഞ്ഞാൽ, സവിശേഷ വെർച്വൽ ഐഡന്റിഫയർ (VPA) സൃഷ്ടിക്കപ്പെടുകയും അത് ഇടപാടുകൾ ആരംഭിക്കുന്നതിന് മൊബൈൽ ഫോണിലേക്ക് സംയോജിപ്പിക്കുകയും ചെയ്യുന്നു. ഗുണഭോക്താവിന്റെ ഈ VPA യു പി ഐ അഭ്യർത്ഥിക്കുകയും തത്സമയം പണം കൈമാറുകയും ചെയ്യുന്നു. ഇടപാടുകൾക്ക് അംഗീകാരം നൽകാൻ അഥവാ സ്ഥിരീകരണത്തിനായി UPI-PIN ആണ് ഉപയോഗിക്കുന്നത്. അത് സ്വകാര്യമായതിനാൽ മറ്റുള്ളവരുമായി പങ്കുവയ്ക്കുവാന് പാടില്ല.

വിഷിങ് (Vishing): ബാങ്ക്/ബാങ്കിതര ഇ-വാലറ്റ് ദാതാക്കൾ/ടെലികോം സേവന ദാതാക്കൾ എന്ന വ്യാജേന ഉപഭോക്താക്കളെ പ്രലോഭിപ്പിച്ച് KYC പുതുക്കൽ, അക്കൗണ്ട്/SIM- കാർഡ് അൺബ്ലോക്ക് ചെയ്യുവാൻ, ഡെബിറ്റ് ചെയ്ത തുക ക്രെഡിറ്റ് ചെയ്യുവാൻ എന്നീ കാരണങ്ങൾ പറഞ്ഞ് അവരിൽ നിന്നും രഹസ്യ വിവരങ്ങൾ ചോർത്തുന്നു.

വാലെറ്റ് (Wallet): നിക്ഷേപം/മുതൽ കൈവശം വയ്ക്കുന്നതിനുള്ള ഒരു അക്കൗണ്ടാണ് വാലെറ്റ്, അത് വിവിധ വാങ്ങലുകൾക്ക് ഉപയോഗിക്കാം. വാലെറ്റ് സാങ്കല്പികം (വെർച്വൽ) ആകാം (ഉദാ:- Paytm, Phonepe പോലുള്ള മൊബൈൽ വാലെറ്റ്)അല്ലെങ്കിൽ മൂർത്തമായ (ഫിസിക്കൽ) പ്രീപെയ്ഡ് കാർഡുകൾ ആകാം.

ഉള്ളടക്കം

	വിഷയം	പേജ് നം
	ആമുഖം	1
	ഭാഗം ഒന്ന് – വഞ്ചനാപരമായ സാമ്പത്തിക ഇടപാടുകളുടെ പ്രവർത്തന രീതികളും അവയ്ക്കെതിരെ സ്വീകരിക്കേണ്ട മുൻകരുതലുകളും – ബാങ്കുകൾ	2
1.	ഫിഷിംഗ് ലിങ്കുകൾ	3
2.	വിഷിങ് കോളുകൾ	4
3.	ഓൺലൈൻ വിൽപ്പന പ്ലാറ്റ്ഫോമുകൾ ഉപയോഗിച്ചുള്ള തട്ടിപ്പുകൾ	5
4.	അപരിചിതമായ/സ്ഥിരീകരിക്കാത്ത മൊബൈൽ ആപ്ലിക്കേഷനുകൾ മുഖേനയുള്ള തട്ടിപ്പുകൾ	6
5.	എ.ടി.എം. കാർഡ് സ്കിമ്മിംഗ്	7
6	സ്ക്രീൻ പങ്കിടൽ ആപ്പ്/റിമോട്ട് ആക്സസ് (Remote Access) ഉപയോഗിച്ചുള്ള തട്ടിപ്പുകൾ	8
7	സിം സ്വാപ്പ്/സിം ക്ലോണിംഗ്	9
8	സെർച്ച് എഞ്ചിനുകളിലൂടെ വ്യക്തിഗത വിവരങ്ങൾ കൈമാറുന്നതു മൂലം ഉണ്ടാകുന്ന തട്ടിപ്പുകൾ	10
9	ക്യൂ ആർ കോഡ് (QR Code) സ്കാൻ വഴിയുള്ള തട്ടിപ്പുകൾ	11
10	സാമൂഹ്യ മാദ്ധ്യമങ്ങളിൽ കൂടിയുള്ള ആൾമാറാട്ടം	12
11	ഹാർഡ്‌വെയർ ഉപയോഗിച്ചുള്ള മാൽവെയർ(Malware) ആക്രമണം (Juice Jacking)	13
12	ഭാഗ്യക്കുറി (Lottery) തട്ടിപ്പ്	14
13	ഓൺലൈൻ തൊഴിൽ തട്ടിപ്പ്	15
14	മണി മ്യൂൾസ് (നിയമവിരുദ്ധമായി ആർജ്ജിച്ച പണം കൈമാറ്റം ചെയ്യുന്നവർ) (Money mules)	16
	ഭാഗം രണ്ട് –വഞ്ചനാപരമായ സാമ്പത്തിക ഇടപാടുകളുടെ പ്രവർത്തനരീതികളും അവയ്ക്കെതിരെ സ്വീകരിക്കേണ്ട മുൻകരുതലുകളും–ബാങ്കിതര ധനകാര്യ സ്ഥാപനങ്ങൾ	17
1	വായ്പ വാഗ്ദാനം ചെയ്യുന്ന ചെയ്യുന്ന വ്യാജ പരസ്യങ്ങൾ	18
2	എസ്.എം.എസ്./ഇമെയിൽ/ഇൻസ്റ്റന്റ് മെസ്സേജിംഗ്/ കോൾ തട്ടിപ്പ്	19
3	ഒ.ടി.പി അടിസ്ഥാനത്തിലുള്ള തട്ടിപ്പ്	20
4	വായ്പകളെ സംബന്ധിച്ച വ്യാജ വെബ്സൈറ്റുകൾ / ആപ്ലിക്കേഷൻ (Application) മുഖേനയുള്ള തട്ടിപ്പുകൾ	21
5	മണി സർക്കുലേഷൻ / പോൻസി / മൾട്ടി ലെവൽ മാർക്കറ്റിംഗ് (MLM) പദ്ധതികലുടെ പേരിലുള്ള തട്ടിപ്പുകൾ	22
6	വ്യാജരേഖകൾ ഉപയോഗിച്ചുള്ള വായ്പാ തട്ടിപ്പുകൾ	23
	ഭാഗം മൂന്ന് – സാമ്പത്തിക ഇടപാടുകൾക്കായി സ്വീകരിക്കേണ്ട പൊതുവായ മുൻകരുതലുകൾ	24
	പദാവലി	32

ആമുഖം

സമീപ വർഷങ്ങളിൽ ഡിജിറ്റൽ പേയ്മെന്റ് രീതികളുടെ ഉപയോഗത്തിൽ കുതിച്ചു ചാട്ടം ഉണ്ടായിട്ടുണ്ട്. കോവിഡ് മൂലം സംജാതമായ ലോക്ക് ഡൗൺ കാലയളവിൽ ഇത് കൂടുതൽ വേഗത കൈവരിച്ചു. ഉപഭോക്തൃ സൗകര്യം മെച്ചപ്പെടുത്തുന്നതിനോടൊപ്പം സാമ്പത്തിക ഉൾപ്പെടുത്തൽ എന്ന ദേശീയ ലക്ഷ്യം കൈവരിക്കുന്നതിനും ഇത് കാരണമായി. പക്ഷേ വേഗത്തിലും, അനായാസമായും സാമ്പത്തിക ഇടപാടുകൾ നടത്തുവാൻ സാധിച്ചതിനാൽ, ചില്ലറ (Retail) സാമ്പത്തിക ഇടപാടുകളിലെ തട്ടിപ്പുകളുടെ എണ്ണവും വർദ്ധിച്ചു. സാധാരണക്കാരും എളുപ്പം കബളിപ്പിക്കപ്പെടാവുന്നവരുമായ, പ്രത്യേകിച്ച് സാങ്കേതിക-സാമ്പത്തിക വ്യവസ്ഥ (Techno-Financial Eco-system) കളുമായി പൂർണമായും പരിചിതമല്ലാത്തവരുമായ ആളുകളുടെ, കഠിനാദ്ധ്വാനത്തിൽ കൂടി നേടിയ പണം അപഹരിക്കുവാൻ നൂതനമായ രീതികളാണ് തട്ടിപ്പുകാർ ഉപയോഗിക്കുന്നത്.

ഡിജിറ്റൽ/ഇലക്ട്രോണിക് രീതിയിലുള്ള സാമ്പത്തിക ഇടപാടുകളിൽ അനുഭവ പരിചയമില്ലാത്തവർക്ക് പരമാവധി പ്രായോഗിക വിവരങ്ങൾ ലഭ്യമാക്കുന്നതിന് വേണ്ടിയാണ്, ഓംബുഡ്സ്മാന്റെ ഓഫീസുകളിൽ ലഭിച്ച വിവിധ പരാതികളിൽ നിന്നും റിപ്പോർട്ട് ചെയ്യപ്പെട്ട തട്ടിപ്പുകളിൽ നിന്നും ലഭ്യമായ വിവരങ്ങൾ ഉൾക്കൊള്ളിച്ചുകൊണ്ട് ഈ ലഘുലേഖ പ്രസിദ്ധീകരിക്കുന്നത്.

സാമ്പത്തിക ഇടപാടുകൾ നടത്തുമ്പോൾ സ്വീകരിക്കേണ്ട മുൻകരുതലുകളെക്കുറിച്ച് ചില വിവരങ്ങൾ നൽകുന്നതോടൊപ്പം, തട്ടിപ്പുകാരുടെ പ്രവർത്തനരീതിയെക്കുറിച്ച് അവബോധം സൃഷ്ടിക്കുന്നതിനുമുള്ള ഒരു ശ്രമമാണ് ഈ ലഘുലേഖ. ഒരാളുടെ സ്വകാര്യ വിവരങ്ങൾ (പ്രത്യേകിച്ച് സാമ്പത്തിക വിവരങ്ങൾ) സുരക്ഷിതമായി സൂക്ഷിക്കുക, അജ്ഞാത ഫോൺ കാളുകൾ/സന്ദേശങ്ങൾ/ഇമെയിലുകൾ എന്നിവ ലഭിക്കുമ്പോൾ ജാഗ്രത പാലിക്കുക, സാമ്പത്തിക ഇടപാടുകൾ നടത്തുമ്പോൾ പാലിക്കേണ്ട മുൻകരുതലുകളെക്കുറിച്ച് ബോധവൽക്കരണം നടത്തുക, സുരക്ഷിതമായ വ്യക്തിഗത വിവരങ്ങൾ, പാസ്‌വേഡുകൾ എന്നിവയിൽ കൂടെക്കൂടെ മാറ്റം വരുത്തുക എന്നീ കാര്യങ്ങളിൽ അവബോധം സൃഷ്ടിക്കുന്നതിനാണ് ഈ ലഘുലേഖ. അതിനാലാണ് BE(A)WARE – അറിവുള്ളവരാകൂ... ജാഗരൂകരാകൂ എന്ന തലക്കെട്ട് നൽകിയിരിക്കുന്നത്.

ഈ ലഘുലേഖ ഭാരതീയ റിസർവ് ബാങ്കിലെ കൺസ്യൂമർ എഡ്യുക്കേഷൻ ആൻഡ് പ്രൊട്ടക്ഷൻ ഡിപ്പാർട്ടമെന്റിന്റെ (CEPD-Consumer Education and Protection Department) ജനകീയ ബോധവൽക്കരണ സംരംഭത്തിന്റെ ഭാഗമാണ്.

വഞ്ചനാപരമായ സാമ്പത്തിക ഇടപാടുകളുടെ പ്രവർത്തന രീതികളും അവയ്ക്കെതിരെ സ്വീകരിക്കേണ്ട മുൻകരുതലുകളും - ബാങ്കുകൾ

1. ഫിഷിംഗ് ലിങ്കുകൾ

പ്രവർത്തന രീതി

- തട്ടിപ്പുകാർ ബാങ്കിന്റെ വെബ്സൈറ്റ് അല്ലെങ്കിൽ ഇ-കൊമേഴ്സ് വെബ്സൈറ്റ് അല്ലെങ്കിൽ സെർച്ച് എഞ്ചിൻ, എന്നിവയുടെ നിലവിലുള്ള യഥാർത്ഥ വെബ സൈറ്റ് പോലെ തോന്നിക്കുന്ന ഒരു മൂന്നാം കക്ഷി ഫിഷിംഗ് വെബ്സൈറ്റ് സൃഷ്ടി ക്കുന്നു.
- തട്ടിപ്പുകാർ ഈ ലിങ്കുൾ സാധാരണയായി എസ്.എം.എസ്./സാമൂഹ്യ മാദ്ധ്യമ ങ്ങൾ/ഇ മെയിൽ/ഇൻസ്റ്റന്റ് മെസ്സഞ്ചർ തുടങ്ങിയവ വഴി പ്രചരിപ്പിക്കുന്നു.
- മിക്കപ്പോഴും, ഉപഭോക്താക്കൾ വിശദമായ URL അഥവാ വെബ്സൈറ്റ് അഡ്രസ് പരിശോധിക്കാതെ ഒറ്റ നോട്ടത്തിൽ ലിങ്കിൽ ക്ലിക്കു ചെയ്ത് വ്യക്തിഗത തിരിച്ച റിയൽ നമ്പർ (PIN), ഒരിക്കൽ മാത്രം ഉപയോഗിക്കാവുന്ന പാസ്സ്വേർഡ് (OTP), പാസ്സ്വേർഡ് മുതലായ സുപ്രധാന വിവരങ്ങൾ നൽകുമ്പോൾ, അത് തട്ടിപ്പു കാർ പിടിച്ചെടുക്കുകയും ഉപയോഗിക്കുകയും ചെയ്യുന്നു.

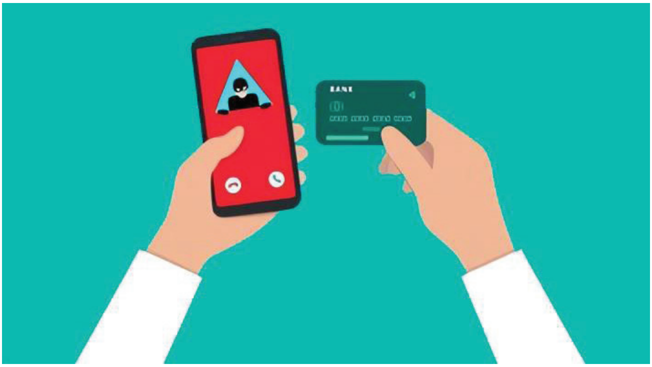
മുൻകരുതൽ

- പരിചിതമല്ലാത്ത/സ്ഥിരീകരിക്കാത്ത ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യരുത്, കൂടാതെ, ഇത്തരം എസ്.എം.എസ്/ഇ-മെയിൽ എന്നിവ ഭാവിയിൽ ഉപയോഗിക്കു ന്നത് ഒഴിവാക്കാൻ ഉടൻതന്നെ നീക്കം (delete) ചെയ്യുക.
- ബാങ്ക്/ഇ-കൊമേഴ്സ്/സെർച്ച് എൻജിൻ വെബ്സൈറ്റുകളിലേക്ക് ബന്ധപ്പെ ടുവാനുള്ള ലിങ്കുകൾ നൽകുന്ന മെയിലുകൾ നീക്കം (delete) ചെയ്യുന്ന തിന് മുമ്പ് അവ അൺസബ്സ്ക്രൈബ് (Unsubscribe) ചെയ്യുകയും, അയച്ച ആളിന്റെ ഇ മെയിൽഐ.ഡി. ബ്ലോക്ക് ചെയ്യേണ്ടതുമാണ്.
- ബാങ്കിന്റെ/സേവന ദാതാവിന്റെ ഔദ്യോഗിക വെബ്സൈറ്റ് മാത്രം ഉപയോ ഗിക്കുക. വെബ്സൈറ്റിന്റെ വിശദാംശങ്ങൾ ശ്രദ്ധാപൂർവം പരിശോധിക്കുക, പ്രത്യേകിച്ചും സാമ്പത്തിക ഇടപാടുകൾക്കുള്ള സമ്മതം നൽകേണ്ടി വരു മ്പോൾ. സുരക്ഷിത വിവരങ്ങൾ നൽകുന്നതിന് മുൻപായി വെബ്സൈറ്റിൽ സുരക്ഷിത അടയാളം (https നോടൊപ്പം താഴിന്റെ ചിഹ്നം) ഉണ്ടോ എന്ന് പരി ശോധിക്കുക.
- ഇ മെയിലിൽ ലഭിച്ച URL, domain name എന്നിവയിൽ അക്ഷരപ്പിശകില്ല എന്ന് ഉറപ്പുവരുത്തുക. സംശയമുണ്ടെങ്കിൽ ഉടൻ ബന്ധപ്പെട്ടവരെ അറിയി ക്കുക.

2. വിഷിംഗ് കോളുകൾ

പ്രവർത്തനരീതി

- തട്ടിപ്പുകാർ ഫോൺ സന്ദേശങ്ങൾ/സാമൂഹ്യ മാദ്ധ്യമങ്ങൾ വഴി, ബാങ്കർമാർ/കമ്പനി എക്സിക്യൂട്ടീവുകൾ/ഇൻഷുറൻസ് ഏജന്റുമാർ/സർക്കാർ ഉദ്യോഗസ്ഥർ എന്ന വ്യാജേന ഉപഭോക്താക്കളെ വിളിക്കുകയോ സമീപിക്കുകയോ ചെയ്യുന്നു. കൂടാതെ വിശ്വാസം നേടുന്നതിന് ഉപഭോക്താവിന്റെ പേര് അല്ലെങ്കിൽ ജനനത്തീയതി പോലുള്ള ചില വിശദാംശങ്ങൾ പങ്കുവയ്ക്കുന്നു.
- ചില സന്ദർഭങ്ങളിൽ, ഇടപാട് ഉടനടി തടയാൻ ആവശ്യമായ വിശദാംശങ്ങൾ, പിഴ ഒഴിവാക്കുവാൻ ആവശ്യമായ പണം അടയ്ക്കൽ, ആകർഷകമായ കിഴിവ് മുതലായവ ഉദ്ധരിച്ചുകൊണ്ട് അടിയന്തിരമായി/തൽക്ഷണം പാസ്സ്‌വേർഡ് (OTP)/PIN/ കാർഡ് വെരിഫിക്കേഷൻ വാല്യു (CVV) എന്നീ രഹസ്യ വിവരങ്ങൾ നല്കാൻ തട്ടിപ്പുകാർ ഉപഭോക്താക്കളിൽ സമ്മർദം ചെലുത്തുകയും കബളിപ്പിക്കുകയും ചെയ്യുന്നു. ഈ രഹസ്യ വിവരങ്ങൾ ഉപഭോക്താക്കളെ വഞ്ചിക്കാൻ പിന്നീട് ഉപയോഗിക്കുന്നു.



മുൻകരുതൽ

- ബാങ്ക് ഉദ്യോഗസ്ഥർ/ധനകാര്യ സ്ഥാപനങ്ങൾ/ആർ.ബി.ഐ./ഏതെങ്കിലും യഥാർത്ഥ സ്ഥാപനം, ഉപഭോക്താക്കളോട് ഉപയോക്തൃ നാമം (User Name) /പാസ്‌വേഡ്/കാർഡ് വിശദാംശങ്ങൾ/സി വി വി/ ഒ ടി പി പോലുള്ള രഹസ്യ വിവരങ്ങൾ പങ്കിടാൻ ഒരിക്കലും ആവശ്യപ്പെടില്ല.
- നിങ്ങളുടെ കുടുംബാംഗങ്ങളുമായോ സുഹൃത്തുക്കളുമായോ മറ്റാരുമായോ ഇത്തരം രഹസ്യവിവരങ്ങൾ പങ്കുവയ്ക്കരുത്.

3. ഓൺലൈൻ വിൽപ്പന പ്ലാറ്റ്ഫോമുകൾ ഉപയോഗിച്ചുള്ള തട്ടിപ്പുകൾ

പ്രവർത്തന രീതി.

- തട്ടിപ്പുകാർ ഓൺലൈൻ വിൽപ്പന പ്ലാറ്റ്ഫോമിൽ വാങ്ങുന്നവരാണെന്ന് നടിക്കുകയും നിങ്ങളുടെ ഉൽപ്പന്നത്തിൽ താൽപര്യം കാണിക്കുകയും ചെയ്യുന്നു. നിങ്ങളുടെ വിശ്വാസം ആർജ്ജിക്കുന്നതിനായി പല തട്ടിപ്പുകാരും, വിദൂര സ്ഥലങ്ങളിൽ സൈനിക സേവനം നടത്തുന്നവരാണെന്ന് നടിക്കുന്നു.

- നിങ്ങൾക്ക് പണം നൽകുന്നതിനുപകരം, അവർ ഡജക ആപ്പ് വഴി “റിക്വസ്റ്റ് മണി” (Request money) ഓപ്ഷൻ ഉപയോഗിക്കുകയും നിങ്ങളുടെ ബാങ്ക് അക്കൗണ്ടിൽ നിന്ന് പണം പിൻവലിക്കുന്നതിനുള്ള അഭ്യർത്ഥന UPI PIN നൽകിക്കൊണ്ട് അംഗീകരിക്കാൻ നിർബന്ധിക്കുകയും ചെയ്യുന്നു. വിൽപ്പനക്കാരൻ PIN രേഖപ്പെടുത്തിക്കഴിഞ്ഞാൽ ഉടൻ തട്ടിപ്പുകാരന്റെ അക്കൗണ്ടിലേക്കു പണം കൈമാറ്റം ചെയ്യപ്പെടുന്നു.

മുൻകരുതൽ

- ഓൺലൈൻ വില്പന പ്ലാറ്റുഫോമുകളിൽ കൂടി ഉത്പന്നങ്ങൾ വാങ്ങുകയോ വിൽക്കുകയോ ചെയ്യുമ്പോൾ എപ്പോഴും ജാഗരൂകരായിരിക്കുക.

- പണം സ്വീകരിക്കാൻ നിങ്ങളുടെ **PIN/പാസ്സ്‌വേഡ് എന്നിവ, എവിടെയും നൽകേണ്ടതില്ല** എന്ന കാര്യം എപ്പോഴും ഓർമ്മയിൽ വയ്ക്കുക.

- UPI അല്ലെങ്കിൽ മറ്റേതെങ്കിലും ആപ്പ്, ഇടപാട് പൂർത്തിയാക്കുവാൻ നിങ്ങളുടെ PIN നൽകണമെന്ന് ആവശ്യപ്പെടുകയാണെങ്കിൽ, ആ ഇടപാട് നിങ്ങൾക്ക് പണം ലഭിക്കുന്നതിനു പകരം പണം അയയ്ക്കാനുള്ളതാണ് എന്ന് മനസ്സിലാക്കുക

4. അപരിചിതമായ/സ്ഥിരീകരിക്കാത്ത മൊബൈൽ ആപ്ലിക്കേഷനുകൾ മുഖേനയുള്ള തട്ടിപ്പുകൾ

പ്രവർത്തന രീതി

- അംഗീകൃത സ്ഥാപനങ്ങളുടെ നിലവിലുള്ള ആപ്പിന് സമാനമായ ചില ആപ്പ് ലിങ്കുകൾ SMS /ഇ മെയിൽ/സാമൂഹ്യ മാധ്യമങ്ങൾ/ ഇൻസ്റ്റന്റ് മെസ്സഞ്ചർ, എന്നിവ വഴി തട്ടിപ്പുകാർ പ്രചരിപ്പിക്കുന്നു.
- തട്ടിപ്പുകാർ, സമർത്ഥമായി ഉപഭോക്താവിനെക്കൊണ്ട് ഇത്തരം ലിങ്കുകളിൽ ക്ലിക് ചെയ്യുവാൻ പ്രേരിപ്പിക്കുന്നു. ഉടൻ അപരിചിതമായ/സ്ഥിരീകരിക്കാത്ത ആപ്പുകൾ നിങ്ങളുടെ മൊബൈൽ ഉപകരണം/ലാപ്ടോപ്പ്/ഡെസ്ക്ടോപ് എന്നിവയിലേക്ക് ഡൗൺലോഡ് ചെയ്യപ്പെടുന്നു.
- മാരകമായ ഇത്തരം ആപ്പുകൾ ഡൗൺലോഡ് ചെയ്യപ്പെട്ടു കഴിഞ്ഞാൽ തട്ടിപ്പുകാരന് ഉപഭോക്താവിന്റെ ഉപകരണത്തിലുള്ള എല്ലാ വിവരങ്ങളും (ഉദാഹരണം: ഉപകരണത്തിൽ സംഭരിച്ചുവച്ചിട്ടുള്ള എല്ലാ സ്വകാര്യ വിവരങ്ങളും ആപ്പ് ഡൗൺലോഡ് ചെയ്യുന്നതിന് മുൻപും അതിനു ശേഷവും ലഭിച്ച മെസ്സേജ് / OTP) എന്നിവ ലഭിക്കുന്നു.

മുൻകരുതൽ

- അപരിചിതമായ/സ്ഥിരീകരിക്കാത്ത ഉറവിടങ്ങളിൽ നിന്നോ, അല്ലെങ്കിൽ അജ്ഞാതനായ വ്യക്തിയുടെ നിർദ്ദേശപ്രകാരമോ ഒരിക്കലും ആപ്ലിക്കേഷൻ ഡൗൺലോഡ് ചെയ്യരുത്.
- ഡൗൺലോഡ് ചെയ്യുന്നതിന് മുൻപ് മുൻകരുതലായി, ആപ്പിന്റെ പ്രസാധകർ/ഉടമസ്ഥർ ആരെന്നും ഉപയോക്താക്കൾ ആപ്പിന് നൽകിയിരിക്കുന്ന റേറ്റിംഗ് എന്താണെന്നും പരിശോധിക്കുക.
- ഡൗൺലോഡ് ചെയ്യുമ്പോൾ ഫോട്ടോ, കോൺടാക്ട് അങ്ങനെ എന്തൊക്കെ വിവരശേഖരങ്ങളിലാണ് ആപ്പ് അനുമതിയും പ്രവേശനവും/പ്രാപ്യതയും തേടുന്നത് എന്ന് പരിശോധിക്കുക. ആപ്പ് ഉപയോഗിക്കുവാൻ തികച്ചും ഉചിതമായ അനുമതി മാത്രം നൽകുക.

5. എടിഎം കാർഡ് സ്കിമ്മിംഗ്

പ്രവർത്തനരീതി

- തട്ടിപ്പുകാർ എ ടി എം മെഷീനുകളിൽ സ്കിമ്മിംഗ് ഉപകരണങ്ങൾ സ്ഥാപിക്കുകയും ഉപഭോക്താവിന്റെ കാർഡിലെ വിവരങ്ങൾ മോഷ്ടിക്കുകയും ചെയ്യുന്നു.
- യഥാർത്ഥ കീപാഡിന്റെ വ്യാജ പതിപ്പ് (ഡമ്മി കീപാഡ്), കാഴ്ചയിൽ നിന്ന് നന്നായി മറഞ്ഞിരിക്കുന്ന ചെറിയ/പിൻഹോൾ ക്യാമറ എന്നിവ സ്ഥാപിച്ചുകൊണ്ട് PIN പിടിച്ചെടുക്കുന്നു.
- ചിലപ്പോൾ, തട്ടിപ്പുകാർ മറ്റ് ഉപഭോക്താക്കളാണെന്ന വ്യാജേന നിങ്ങളുടെ സമീപത്ത് നിന്ന് നിങ്ങൾ PIN നൽകുമ്പോൾ അത് നോക്കി മനസ്സിലാക്കുന്നു.
- ഈ വിവരങ്ങൾ പിന്നീട് കാർഡിന്റെ പകർപ്പ് (Duplicate card) സൃഷ്ടിക്കുവാനും ഉപഭോക്താവിന്റെ അക്കൗണ്ടിൽ നിന്ന് തുക പിൻവലിക്കുവാനും ഉപയോഗിക്കുന്നു.

മുൻകരുതൽ

- ഇടപാട് നടത്തുമ്പോൾ എ ടി എം കാർഡ് ഇടുന്ന സ്ലോട്ട് അല്ലെങ്കിൽ എ ടി എം മെഷീന്റെ കീപാഡിന് സമീപം മറ്റ് ഉപകരണങ്ങൾ ഘടിപ്പിച്ചിട്ടില്ലെന്ന് ഉറപ്പുവരുത്തുക.
- നിങ്ങളുടെ പിൻ നൽകുമ്പോൾ കീപാട് കൈകൊണ്ട് മറയ്ക്കുക.
- നിങ്ങളുടെ പിൻ ഒരിക്കലും എ ടി എം കാർഡിൽ എഴുതി വയ്ക്കരുത്.
- നിങ്ങളുടെ അടുത്ത് നിൽക്കുന്ന മറ്റൊരാളുടെ സാന്നിധ്യത്തിൽ പിൻ നൽകരുത്.
- പണം പിൻവലിക്കുന്നതിനായി നിങ്ങളുടെ എ ടി എം കാർഡ് മറ്റാർക്കും നൽകരുത്.
- എ ടി എമ്മിൽ അപരിചിതർ നൽകുന്ന നിർദേശം പാലിക്കുകയോ അവരിൽ നിന്നും സഹായം/മാർഗനിർദ്ദേശം സ്വീകരിക്കുകയോ ചെയ്യരുത്.
- എ ടി എമ്മിൽ നിന്നും പണം ലഭിച്ചില്ലെങ്കിൽ ക്യാൻസൽ (Cancel) ബട്ടൺ അമർത്തി ഹോം സ്ക്രീൻ കണ്ടതിനുശേഷം മാത്രം എ ടി എമ്മിൽ നിന്നും മടങ്ങുക.

6. സ്ക്രീൻ പങ്കിടൽ ആപ്പ്/റിമോട്ട് അക്സസ് (Remote access) ഉപയോഗിച്ചുള്ള തട്ടിപ്പുകൾ

പ്രവർത്തനരീതി

- സ്ക്രീൻ പങ്കിടൽ ആപ്പുകൾ ഡൗൺലോഡ് ചെയ്യുവാൻ തട്ടിപ്പുകാർ ഉപഭോക്താവിനെ പ്രലോഭിപ്പിക്കുന്നു.
- അതിലൂടെ അവർക്ക് ഉപഭോക്താവിന്റെ മൊബൈൽ/ലാപ്ടോപ്പ് നിരീക്ഷിക്കുവാനും നിയന്ത്രിക്കുവാനും ഉപഭോക്താവിന്റെ സാമ്പത്തിക രഹസ്യ വിവരങ്ങൾ നേടിയെടുക്കുന്നതിനും സാധിക്കുന്നു.
- പിന്നീട് തട്ടിപ്പുകാർ ഉപഭോക്താവിന്റെ ഇന്റർനെറ്റ് ബാങ്കിംഗ്/പേയ്മെന്റ് ആപ്പുകൾ ഉപയോഗിച്ച് പണം കൈമാറ്റം നടത്തുന്നു.

മുൻകരുതൽ

- നിങ്ങളുടെ കംപ്യൂട്ടറിന് എന്തെങ്കിലും സാങ്കേതിക തകരരാർ ഉണ്ടാകുകയും സ്ക്രീൻ പങ്കിടൽ ആപ്പ് ഡൗൺലോഡ് ചെയ്യേണ്ട ആവശ്യകത ഉണ്ടാകുകയും ചെയ്താൽ ബന്ധപ്പെട്ട എല്ലാ ആപ്പുകളും പ്രവർത്തനരഹിതമാക്കുക/ലോഗ് ഔട്ട് ചെയ്യുക.
- കമ്പനിയുടെ ഔദ്യോഗിക ടോൾ-ഫ്രീ നമ്പറിൽ (ഔദ്യോഗിക വെബ്സൈറ്റിൽ പറഞ്ഞിരിക്കുന്ന നമ്പർ) നിന്നും അറിയിപ്പ് ലഭിക്കുമ്പോൾ മാത്രമേ ഇത്തരം ആപ്പുകൾ ഡൗൺലോഡ് ചെയ്യാവൂ. കമ്പനിയുടെ ഉദ്യോഗസ്ഥൻ അയാളുടെ ഫോൺ നമ്പറിൽ നിന്നും നിങ്ങളെ വിളിച്ച് ആപ്പുകൾ ഡൗൺലോഡ് ചെയ്യുവാൻ ആവശ്യപ്പെടുകയാണെങ്കിൽ അത്തരം ആപ്പുകൾ ഡൗൺലോഡ് ചെയ്യരുത്.
- പ്രവൃത്തി പൂർത്തിയാലുടൻ സ്ക്രീൻ പങ്കിടൽ ആപ്പ് കംപ്യൂട്ടറിൽ നിന്നും നീക്കം (Delete) ചെയ്യുക.

7. സിം സ്വാപ്പ്/സിം ക്ലോണിംഗ്

പ്രവർത്തനരീതി

- ഉപഭോക്താവിന്റെ അക്കൗണ്ട് രജിസ്റ്റർ ചെയ്ത മൊബൈൽ നമ്പറുമായി ബന്ധിപ്പിച്ചിരിക്കുന്നതിനാൽ, തട്ടിപ്പുകാർ സിം കാർഡിലേക്ക് പ്രവേശനം നേടുവാനോ അല്ലെങ്കിൽ ഡ്യൂപ്ലിക്കേറ്റ് സിം കാർഡ് (ഇലക്ട്രോണിക് - SIM ഉൾപ്പെടെ) നേടുവാനോ ശ്രമിക്കുന്നു.
- തട്ടിപ്പുകാർ അത്തരം സിം പകർപ്പ് (duplicate SIM) ൽ നിന്ന് ലഭിക്കുന്ന ഒ ടി പി (OTP) ഉപയോഗിച്ച് വ്യാജ ഇടപാടുകൾ നടത്തുന്നു.
- 3G യിൽ നിന്ന് 4G യിലേക്ക് സിം കാർഡ് സൗജന്യമായി അപ്ഗ്രേഡ് ചെയ്യുന്നതിന് അല്ലെങ്കിൽ 4G സിം കാർഡിൽ അധിക ആനുകൂല്യം നൽകുന്നതിന് വിശദാംശങ്ങൾ അഭ്യർത്ഥിച്ചുകൊണ്ട്, ഒരു ടെലിഫോൺ/ മൊബൈൽ നെറ്റ്‌വർക്ക് ജീവനക്കാരാണെന്ന വ്യാജേന, തട്ടിപ്പുകാർ ഉപഭോക്താവിനെ വിളിച്ച് വ്യക്തിഗത വിവരങ്ങൾ ശേഖരിക്കുന്നു.

മുൻകരുതൽ

- സിം കാർഡുമായി ബന്ധപ്പെട്ട വ്യക്തിഗത വിവരങ്ങൾ ഒരിക്കലും പങ്കിടരുത്.
- സാധാരണ പരിതസ്ഥിതിയിൽ നിങ്ങളുടെ ഫോണിൽ ഗണ്യമായ സമയം മൊബൈൽ നെറ്റ്‌വർക്ക് ഇല്ലെങ്കിൽ നിങ്ങളുടെ സിമ്മിന് ഡ്യൂപ്ലിക്കേറ്റ് സിം നൽകുന്നില്ലെന്ന് ഉറപ്പുവരുത്തുവാൻ ഉടൻ തന്നെ മൊബൈൽ ഓപ്പറേറ്ററെ ബന്ധപ്പെടേണ്ടതാണ്.

8. സെർച്ച് എഞ്ചിനുകളിലൂടെ വ്യക്തിഗത വിവരങ്ങൾ കൈമാറുന്നതു മൂലം ഉണ്ടാകുന്ന തട്ടിപ്പുകൾ

പ്രവർത്തനരീതി

- ഉപഭോക്താക്കൾ അവരുടെ ബാങ്ക്, ഇൻഷുറൻസ് കമ്പനി, ആധാർ അപ്ഡേഷൻ സെന്ററുകൾ മുതലായവയുടെ സമ്പർക്ക വിശദാംശങ്ങൾ/അഥവാ Customer Care Number ലഭിക്കുന്നതിന് സെർച്ച് എഞ്ചിനുകൾ ഉപയോഗിക്കുന്നു. സെർച്ച് എഞ്ചിനുകളിൽ ലഭിക്കുന്ന സമ്പർക്ക വിശദാംശങ്ങൾ ആ സ്ഥാപനങ്ങളുടേത് ആവണമെന്നില്ല. മറിച്ച് തട്ടിപ്പുകാർ ആ രീതിയിൽ പ്രദർശിപ്പിച്ചവയാവാം.
- ബാങ്ക്, കമ്പനി എന്നിവയുടേതെന്ന വ്യാജേന തട്ടിപ്പുകാർ സെർച്ച് എഞ്ചിനിൽ ഈ രീതിയിൽ പ്രദർശിപ്പിച്ചിരിക്കുന്ന അപരിചിതമായ/സ്ഥിരീകരിക്കാത്ത സമ്പർക്ക നമ്പറുകളുമായി ഉപഭോക്താക്കൾ ബന്ധപ്പെടുന്നു.
- ഉപഭോക്താക്കൾ അവരെ ഒരിക്കൽ വിളിച്ചുകഴിഞ്ഞാൽ, തട്ടിപ്പുകാർ ഉപഭോക്താക്കളോട് അവരുടെ കാർഡ് വിവരങ്ങൾ/വിശദാംശങ്ങൾ സ്ഥിരീകരിക്കാൻ ആവശ്യപ്പെടുന്നു.
- തട്ടിപ്പുകാരൻ സ്ഥാപനത്തിന്റെ യഥാർത്ഥ പ്രതിനിധി ആണെന്ന ധാരണയിൽ ഉപഭോക്താവ് തന്റെ സുപ്രധാന വിവരങ്ങൾ കൈമാറുകയും വഞ്ചനക്കിരയാവുകയും ചെയ്യുന്നു.

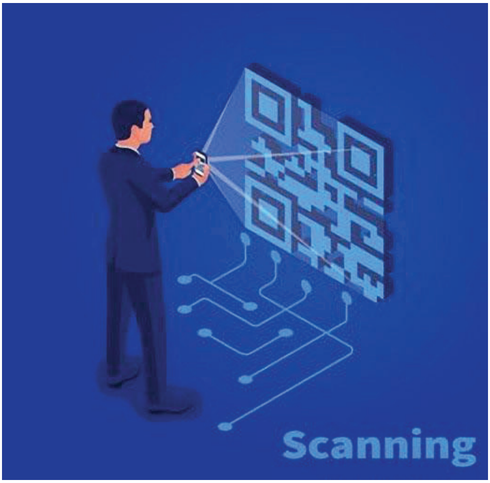
മുൻകരുതൽ

- കസ്റ്റമർ കെയർ സമ്പർക്കവിശദാംശങ്ങൾ ലഭിക്കുന്നതിന് എപ്പോഴും ബാങ്കുകളുടെ/കമ്പനികളുടെ ഔദ്യോഗിക വെബ് സൈറ്റുകൾ ഉപയോഗിക്കുക.
- സെർച്ച് എഞ്ചിൻ റിസൾട്ട് പേജിൽ പ്രദർശിപ്പിച്ചിരിക്കുന്ന നമ്പറുകൾ തട്ടിപ്പുകാരുടേതാവാൻ സാദ്ധ്യതയുള്ളതിനാൽ ആ നമ്പറിൽ വിളിക്കരുത്.
- കസ്റ്റമർ കെയർ നമ്പർ ഒരിക്കലും മൊബൈൽ നമ്പറിന്റെ രൂപത്തിലായിരിക്കുകയില്ല എന്ന് മനസ്സിലാക്കുക.

9. ക്യൂ ആർ കോഡ് സ്കാൻ (QR Code) വഴിയുള്ള തട്ടിപ്പുകൾ

പ്രവർത്തന രീതി

- തട്ടിപ്പുകാർ പലപ്പോഴും ഉപഭോക്താക്കളുമായി പല കാരണങ്ങൾ ഉന്നയിച്ച് ബന്ധപ്പെടുകയും ഉപഭോക്താവിന്റെ ഫോണിലെ ആപ്പുകൾ ഉപയോഗിച്ച് ക്യൂ ആർ കോഡുകൾ സ്കാൻ ചെയ്യുവാൻ അവരെ നിർബന്ധിക്കുകയും ചെയ്യുന്നു.
- ക്യൂ ആർ കോഡുകൾ സ്കാൻ ചെയ്യുന്നതോടുകൂടി ഉപഭോക്താക്കളുടെ അറിവില്ലാതെ അവരുടെ അക്കൗണ്ടിൽ നിന്ന് പണം പിൻവലിക്കുവാൻ തട്ടിപ്പുകാർക്ക് സാധിക്കുന്നു.



മുൻകരുതൽ

- ധന കൈമാറ്റത്തിനുള്ള ആപ്പുകൾ ഉപയോഗിച്ച് ക്യൂ ആർ (QR) കോഡുകൾ സ്കാൻ ചെയ്യുമ്പോൾ ജാഗ്രത പാലിക്കുക. QR കോഡുകളിൽ ഒരു പ്രത്യേക അക്കൗണ്ടിലേക്ക് പണം കൈമാറുന്നതിനുള്ള വിവരങ്ങൾ ഉൾച്ചേർത്തിട്ടുണ്ടാവാം.
- പണം സ്വീകരിക്കുന്നതിന് ഒരു ക്യൂ ആർ കോഡും സ്കാൻ ചെയ്യരുത്. പണം സ്വീകരിക്കുന്ന ഇടപാടുകൾക്ക് ബാർ കോഡ്/ക്യൂ ആർ (QR) കോഡ് എന്നിവ സ്കാൻ ചെയ്യുകയോ മൊബൈൽ ബാങ്കിങ് PIN (m-PIN), പാസ്സ്‌വേർഡ് എന്നിവ നൽകുകയോ ചെയ്യേണ്ട ആവശ്യമില്ല.

10. സാമൂഹ്യ മാദ്ധ്യമങ്ങളിൽ കൂടിയുള്ള ആൾമാറാട്ടം

പ്രവർത്തനരീതി

- ഫെയ്സ്ബുക്ക്, ഇൻസ്റ്റാഗ്രാം, ടിറ്റെർ തുടങ്ങിയ ജനപ്രിയ സാമൂഹ്യ മാദ്ധ്യമങ്ങളിൽ ഉപയോക്താക്കളുടെ വിവരങ്ങൾ ഉപയോഗിച്ച് തട്ടിപ്പുകാർ വ്യാജ അക്കൗണ്ട് സൃഷ്ടിക്കുന്നു.
- അടിയന്തിര ചികിൽസാ സംബന്ധിയായ ആവശ്യങ്ങൾക്കോ പണമടയ്ക്കലിനോ മറ്റോ പണം ആവശ്യപ്പെട്ട് അവർ ഉപയോക്താക്കളുടെ സുഹൃത്തുക്കൾക്ക് ഒരു അഭ്യർത്ഥന അയയ്ക്കുന്നു.
- തട്ടിപ്പുകാർ വ്യാജ വിവരങ്ങൾ ഉപയോഗിച്ച് ഉപയോക്താക്കളെ ബന്ധപ്പെട്ട് ഒരു നിശ്ചിത കാലയളവിനുള്ളിൽ വിശ്വാസ്യത നേടുന്നു. പിന്നീട് ഉപയോക്താക്കൾ വ്യക്തിപരവും സ്വകാര്യവുമായ വിവരങ്ങൾ പങ്കുവയ്ക്കുമ്പോൾ തട്ടിപ്പുകാർ അവ നിങ്ങളെ ഭീഷണിപ്പെടുത്തി പണം അപഹരിക്കുന്നതിനോ ഭീഷണിപ്പെടുത്തുന്നതിനോ ഉപയോഗിക്കുന്നു.

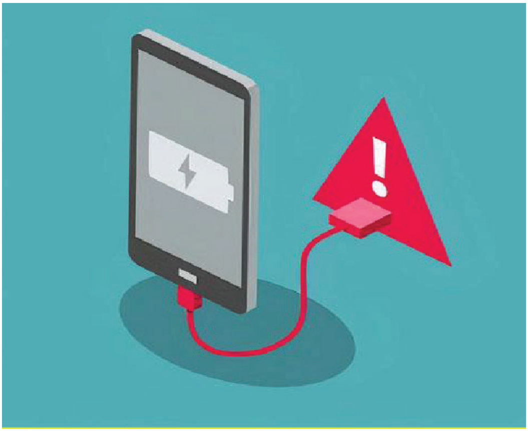
മുൻകരുതൽ

- പ്രൊഫൈലിൽ ആൾമാറാട്ടം നടത്തിയിട്ടില്ലെന്ന് ഉറപ്പുവരുത്തുന്നതിനായി സുഹൃത്തിന്റെ/ബന്ധുവിന്റെ ഫണ്ട് അഭ്യർത്ഥനയുടെ സത്യസന്ധത ഫോൺ കോൾ/കൂടിക്കാഴ്ച വഴി എപ്പോഴും സ്ഥിരീകരിക്കുക.
- അജ്ഞാതരായ വ്യക്തികൾക്ക് ഓൺലൈനിലൂടെ പണം നൽകരുത്.
- സാമൂഹ്യ മാദ്ധ്യമ പ്ലാറ്റ്ഫോമുകളിൽ വ്യക്തിപരവും രഹസ്യവുമായ വിവരങ്ങൾ പങ്കിടുന്നത് ഒഴിവാക്കുക.

11. ഹാർഡ്‌വെയർ ഉപയോഗിച്ചുള്ള മാൽവെയർ (Malware) ആക്രമണം (Juice Jacking)

പ്രവർത്തന രീതി

- ഒരു മൊബൈലിന്റെ ചാർജിംഗ് പോർട്ട്, ഫയലുകൾ/ ഡാറ്റ കൈമാറ്റത്തിനായും ഉപയോഗിക്കാം.
- നിങ്ങളുടെ മൊബൈൽ ഫോൺ പൊതുസ്ഥലത്തുള്ള ചാർജിംഗ് പോർട്ടുകളുമായി ബന്ധിപ്പിച്ചുകഴിഞ്ഞാൽ, മാൽവെയർ (Malware) ഇൻസ്റ്റാൾ ചെയ്ത് തട്ടിപ്പുകാർക്ക് സുപ്രധാന വിവരങ്ങൾ, ഇ മെയിൽ, എസ്.എം.എസ്., സുരക്ഷിത പാസ്സ്‌വേർഡ്കൾ എന്നിവ ഉപയോഗിക്കുവാനോ നിയന്ത്രിക്കുവാനോ മോഷ്ടിക്കുവാനോ കഴിയും (ജ്യൂസ് ജാക്കിംഗ്).



മുൻകരുതൽ

- പൊതുസ്ഥലങ്ങളിലെ/അപരിചിതമായ ചാർജിംഗ് പോർട്ടുകൾ/കേബിളുകൾ എന്നിവ ഉപയോഗിക്കുന്നത് ഒഴിവാക്കുക.

12. ഭാഗ്യക്കുറി (Lottery) തട്ടിപ്പ്

പ്രവർത്തനരീതി

- ഉപഭോക്താവിന്, ഭാഗ്യക്കുറിയിൽ നിന്നും വൻതുക സമ്മാനം നേടിയതായി തട്ടിപ്പുകാർ ഫോൺ/ഇ മെയിൽ വഴി അറിയിക്കുന്നു. എന്നാൽ പണം സ്വീകരിക്കുന്നതിനായി ഉപഭോക്താവിനോട് തന്റെ വ്യക്തിഗത വിവരങ്ങൾ സ്ഥിരീകരിക്കുന്നതിനായി ബാങ്ക് അക്കൗണ്ട്/ക്രെഡിറ്റ് കാർഡ് വിവരങ്ങൾ അവരുടെ വെബ്സൈറ്റിൽ നൽകാൻ ആവശ്യപ്പെടുക. എന്നിട്ട് ഈ വിവരങ്ങൾ അവർ പിടിച്ചെടുക്കുന്നു.
- ചില സന്ദർഭങ്ങളിൽ, ലോട്ടറി സമ്മാനം/ഉൽപ്പന്നം ലഭിക്കുന്നതിന് തട്ടിപ്പുകാർ മുൻകൂട്ടി നികുതി അടയ്ക്കുവാനോ ഷിപ്പിംഗ് തുക, പ്രോസസ്സിംഗ് ഫീസ് മുതലായവ അടയ്ക്കുവാനോ ആവശ്യപ്പെടുന്നു.
- തട്ടിപ്പുകാർ ചില സന്ദർഭങ്ങളിൽ റിസർവ് ബാങ്ക്/വിദേശ ബാങ്ക്/കമ്പനി/അന്താരാഷ്ട്ര സാമ്പത്തിക സ്ഥാപനം എന്നിവയുടെ പ്രതിനിധിയാണെന്ന് അവകാശപ്പെടുകയും അവരുടെ സ്ഥാപനത്തിൽ നിന്നും വൻതുക വിദേശ കറൻസിയിൽ ലഭിക്കുന്നതിനായി ഒരു ചെറിയ തുക കൈമാറ്റം ചെയ്യുവാൻ ഉപഭോക്താവിനോട് ആവശ്യപ്പെടുകയും ചെയ്യുന്നു.

- സാധാരണയായി ആവശ്യപ്പെടുന്ന തുക വാഗ്ദാനം ചെയ്യുന്ന സമ്മാനത്തിന്റെ/ഉൽപ്പന്ന വിലയുടെ വളരെ ചെറിയ ശതമാനമായതിനാൽ, ഇരകൾ തട്ടിപ്പുകാരന്റെ കെണിയിൽ വീഴുകയും പണം അടയ്ക്കുകയും ചെയ്തേക്കാം.

മുൻകരുതൽ

- അവിശ്വസനീയമായ ഇത്തരം ലോട്ടറി/സമ്മാനങ്ങൾ വാഗ്ദാനം ലഭിക്കുമ്പോൾ ജാഗ്രത പാലിക്കുക, ആരും സൗജന്യമായി പണം നൽകില്ല, പ്രത്യേകിച്ചും വൻതുകകൾ.
- ലോട്ടറി കോളുകൾ/ഇ-മെയിലുകൾ എന്നിവയുടെ മറുപടിയായി പണം കൈമാറ്റം നടത്തുകയോ സുരക്ഷിത വിവരങ്ങൾ പങ്കിടുകയോ ചെയ്യരുത്.
- റിസർവ് ബാങ്ക് പൊതുജനങ്ങളിൽ നിന്നും നിക്ഷേപം സ്വീകരിക്കുകയോ അക്കൗണ്ട് തുറക്കുകയോ ചെയ്യുന്നതല്ല. അത്തരം സന്ദേശങ്ങൾ വ്യാജമാണ്.
- വ്യക്തിപരമായതോ ബാങ്കിനെപ്പറ്റിയോ ഉള്ള ഒരു വിവരവും റിസർവ് ബാങ്ക് പൊതുജനങ്ങളോട് ചോദിക്കാറില്ല. റിസർവ് ബാങ്കിന്റെ വ്യാജമായ മുദ്രയ്ക്കും സന്ദേശങ്ങൾക്കും എതിരെ ജാഗ്രത പാലിക്കുക.
- സമ്മാനത്തുക, സർക്കാർ സഹായം എന്നിവ വാഗ്ദാനം ചെയ്തുകൊണ്ടുള്ള സന്ദേശങ്ങൾ, സമ്മാനത്തുക ലഭിക്കുന്നതിന് KYC പുതുക്കുവാൻ ആവശ്യപ്പെട്ടുകൊണ്ട് ബാങ്കുകളിൽ നിന്നോ മറ്റു സ്ഥാപനങ്ങളിൽ നിന്നോ ലഭിക്കുന്ന സന്ദേശങ്ങൾ എന്നിവയോടു പ്രതികരിക്കരുത്.

13. ഓൺലൈൻ തൊഴിൽ തട്ടിപ്പ്

പ്രവർത്തനരീതി

- തട്ടിപ്പുകാർ വ്യാജ ജോലി അന്വേഷണ പോർട്ടലുകൾ സൃഷ്ടിക്കുകയും, ഉദ്യോഗാർത്ഥികൾ രജിസ്റ്റർ ചെയ്യുന്നതിനു വേണ്ടി ഈ വെബ്സൈറ്റുകളിൽ ബാങ്ക് അക്കൗണ്ട്/ക്രെഡിറ്റ് കാർഡ്/ഡെബിറ്റ് കാർഡ് എന്നിവയുടെ സുരക്ഷിത വിശദാംശങ്ങൾ പങ്കുവയ്ക്കുമ്പോൾ അക്കൗണ്ട് വിവരങ്ങൾ അപഹരിക്കുകയും ചെയ്യുന്നു.
- തട്ടിപ്പുകാർ പ്രശസ്ത കമ്പനിയുടെ ഉദ്യോഗസ്ഥരായി സ്വയം അവതരിപ്പിക്കുകയും വ്യാജ അഭിമുഖങ്ങൾ നടത്തിയ ശേഷം ജോലി വാഗ്ദാനം ചെയ്യുകയും ചെയ്യുന്നു. ശേഷം, ലാപ്ടോപ്പ്, രജിസ്ട്രേഷൻ, നിർബന്ധിത പരിശീലന പരിപാടി മുതലായവയ്ക്ക് പണമടയ്ക്കുവാൻ ഉദ്യോഗാർത്ഥികളെ പ്രേരിപ്പിക്കുന്നു.

മുൻകരുതൽ

- വിദേശ സ്ഥാപനങ്ങളുടേതുൾപ്പെടെ, ഏതു ജോലി വാഗ്ദാനവും, സ്വീകരിക്കുന്നതിന് മുമ്പ് സ്ഥാപനത്തിന്റെയും അതിന്റെ പ്രതിനിധിയുടെയും വിലാസവും മറ്റു വിവരങ്ങളും സ്ഥിരീകരിക്കേണ്ടതാണ്.
- ജോലി വാഗ്ദാനം ചെയ്യുന്ന ഒരു യഥാർത്ഥ സ്ഥാപനം ഒരിക്കലും പണം ആവശ്യപ്പെടില്ലെന്ന് എപ്പോഴും ഓർക്കുക.
- അജ്ഞാതമായ ജോലി അന്വേഷണ പോർട്ടലുകളിൽ പണമടയ്ക്കരുത്.

14. മണി മ്യൂൾസ് (നിയമവിരുദ്ധമായി ആർജിച്ച പണം കൈ മാറ്റം ചെയ്യുന്നവർ) (Money mules)

പ്രവർത്തനരീതി

- തട്ടിപ്പുകാരുടെ കൈവശമുള്ള മോഷ്ടിച്ച/നിയമവിരുദ്ധമായി നേടിയ പണം അവരുടെ വലയിൽ കുടുങ്ങുന്ന നിരപരാധികളായ ഇരകളുടെ ബാങ്ക് അക്കൗണ്ടുകളിൽ കൂടി വെളുപ്പിക്കുന്നു. ഈ നിരപരാധികളെ വിശേഷിപ്പിക്കുന്ന പദമാണ് മണി മ്യൂൾസ്.
- ഇ-മെയിൽ, സാമൂഹ്യ മാധ്യമങ്ങൾ എന്നിവയിൽ കൂടി തട്ടിപ്പുകാർ ഇടപാടുകാരെ ബന്ധപ്പെടുകയും ആകർഷണീയമായ പ്രതിഫലത്തിന് പകരമായി അവരുടെ അക്കൗണ്ടിൽ തട്ടിപ്പുകാരുടെ പണം നിക്ഷേപിക്കുവാന് ആവശ്യപ്പെടുകയും ചെയ്യുന്നു.
- അതിനു ശേഷം, ആ പണം മറ്റൊരു നിരപരാധിയുടെ അക്കൗണ്ടിലേക്കു മാറ്റുവാൻ ആവശ്യപ്പെടുകയും അവിടെ നിന്നും പല അക്കൗണ്ടിലേക്കും അവസാനം തട്ടിപ്പുകാരന്റെ അക്കൗണ്ടിലേക്ക് എത്തുകയും ചെയ്യുന്നു.
- മറ്റു ചിലപ്പോൾ, പണം പിൻവലിച്ച് മറ്റൊരാൾക്ക് നൽകാൻ തട്ടിപ്പുകാരൻ ആവശ്യപ്പെടുന്നു.
- എപ്പോഴെങ്കിലും ഇത് റിപ്പോർട്ട് ചെയ്യപ്പെട്ടാൽ, മണി മ്യൂൾ പോലീസ് അന്വേഷണത്തിന് പാത്രമായി മാറുന്നു.

മുൻകരുതൽ

- പ്രതിഫലത്തിന് വേണ്ടി നിങ്ങളുടെ അക്കൗണ്ടിൽ കൂടി പണം നിക്ഷേപിക്കുവാനോ കൈമാറ്റം ചെയ്യുവാനോ മറ്റാരെയും അനുവദിക്കരുത്.
- ബാങ്ക് അക്കൗണ്ട് വിശദാംശങ്ങൾ ആവശ്യപ്പെട്ടുകൊണ്ട് വരുന്ന ഇ-മെയിലുകളോടും പ്രതികരിക്കരുത്.
- ആകർഷകമായ വാഗ്ദാനങ്ങൾ/പ്രതിഫലം എന്നിവയിൽ പ്രലോഭിതരാകരുത്. അനധികൃതമായ പണം സ്വീകരിച്ച് മറ്റുള്ളവർക്ക് കൈമാറ്റം ചെയ്യുവാനോ പണം പിൻവലിച്ച് മറ്റുള്ളവർക്ക് നൽകുവാനോ സമ്മതിക്കരുത്.
- പണത്തിന്റെ ഉറവിടം വ്യാജമാണെങ്കിൽ/ആസ്പദമായ ഇടപാടിന്റെ പ്രമാണം അധികാരികൾക്ക് മുൻപിൽ ബോധ്യപ്പെടുത്തുവാൻ കഴിഞ്ഞിട്ടില്ലെങ്കിൽ പണം സ്വീകരിച്ച വ്യക്തി പോലീസിന്റെയും നിയമ നിർവ്വഹണ ഏജൻസികളുടെയും പക്കൽ നിന്നും ഗൗരവമായ പ്രശ്നങ്ങൾ നേരിടേണ്ടി വരും.

ഭാഗം - രണ്ട്

വഞ്ചനാപരമായ സാമ്പത്തിക ഇടപാടുകളുടെ പ്രവർത്തനരീതികളും അവയ്ക്കെതിരെ സ്വീകരിക്കേണ്ട മുൻകരുതലുകളും - ബാങ്കിതര ധനകാര്യ സ്ഥാപനങ്ങൾ

വായ്പ വാഗ്ദാനം ചെയ്യുന്ന വ്യാജ പരസ്യങ്ങൾ

പ്രവർത്തനരീതി

- തട്ടിപ്പുകാർ വളരെ ആകർഷകമായ, കുറഞ്ഞ പലിശ നിരക്കിലുള്ളതോ, എളുപ്പത്തിലുള്ള തിരിച്ചടവ് സൗകര്യമുള്ളതോ, ഈട്/ജാമ്യം നൽകേണ്ടാത്തതോ ആയ വ്യക്തിഗത വായ്പാ വാഗ്ദാനങ്ങളുടെ വ്യാജ പരസ്യങ്ങൾ പ്രസിദ്ധീകരിക്കുന്നു.
- തട്ടിപ്പുകാർ, ഈ വാഗ്ദാനങ്ങൾ ഇ-മെയിൽ വഴി അയച്ചുകൊടുക്കുകയും ഉപഭോക്താക്കളോട് ബന്ധപ്പെടുവാൻ ആവശ്യപ്പെടുകയും ചെയ്യുന്നു. ഉപഭോക്താക്കളുടെ വിശ്വാസ്യത നേടുന്നതിനും ആത്മവിശ്വാസം വളർത്തുന്നതിനും, ഈ ഇ-മെയിൽ ഐഡികൾ പ്രസിദ്ധ/യഥാർത്ഥ ബാങ്കിതര ധനകാര്യ സ്ഥാപനങ്ങളിലെ മുതിർന്ന ഉദ്യോഗസ്ഥരുടെ ഇ-മെയിൽ ഐഡികളെന്നു തോന്നിപ്പിക്കുന്ന വിധമായിരിക്കും.
- വായ്പകൾക്കായി ഉപഭോക്താക്കൾ തട്ടിപ്പുകാരെ സമീപിക്കുമ്പോൾ, തട്ടിപ്പുകാർ പ്രോസസിംഗ് ഫീസ്, ജി എസ് ടി, ഇന്റർസിറ്റി ചാർജ്, അഡ്വാൻസ് ഇ എം ഇ തുടങ്ങിയവ ഈടാക്കി വായ്പകൾ നൽകാതെ കടന്നുകളയുന്നു.
- വായ്പകൾ മുതലായവ കണ്ടെത്തുവാൻ ആളുകൾ തിരയുന്ന സെർച്ച് എഞ്ചിനുകളിൽ കാണുന്ന രീതിയിൽ തട്ടിപ്പുകാർ വ്യാജ വെബ്സൈറ്റ് ലിങ്കുകളും സൃഷ്ടിക്കുന്നു.

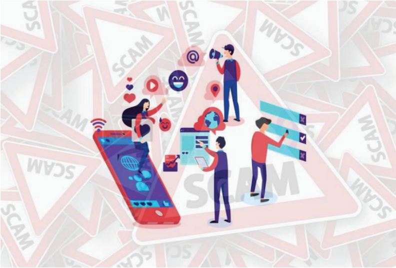
മുൻകരുതൽ

- ബാങ്കുകൾ/ബാങ്കിതര ധനകാര്യ സ്ഥാപനങ്ങൾ എന്നിവ, പ്രോസസിംഗ് ഫീസ് വായ്പ തുകയിൽ നിന്ന് കുറയ്ക്കും. ഒരിക്കൽ മുൻകൂർ ഫീസ് ആവശ്യപ്പെടുകയില്ല.
- ഒരിക്കലും മുൻകൂറായി പ്രോസസിംഗ് ഫീ നൽകരുത്. കാരണം വായ്പ അപേക്ഷയുടെ പ്രോസസിംഗിന് മുമ്പ് എൻ ബി എഫ് സികൾ/ബാങ്കുകൾ എന്നിവ ഒരിക്കലും ഫീസ് ചോദിക്കില്ല.
- യഥാർത്ഥ സ്രോതസ്സുകളിലൂടെ വിശദാംശങ്ങൾ പരിശോധിക്കാതെ കുറഞ്ഞ പലിശയ്ക്ക് വായ്പ നൽകുന്നു എന്ന് അവകാശപ്പെടുന്നവർക്ക് പണം നൽകുകയോ സുരക്ഷിത വ്യക്തിഗത വിവരങ്ങൾ നൽകുകയോ ചെയ്യരുത്.

2 എസ് എം എസ്/ഇ-മെയിൽ/ ഇൻസ്റ്റന്റ് മെസ്സേജിംഗ് (Instant Messaging) /കോൾ തട്ടിപ്പ്

പ്രവർത്തനരീതി

- ആകർഷകമായ വായ്പകളുടെ ലഭ്യത സംബന്ധിച്ച് തട്ടിപ്പുകാർ ഇൻസ്റ്റന്റ് മെസ്സഞ്ചർ/എസ് എം എസ്/സാമൂഹ്യ മാധ്യമങ്ങൾ എന്നിവയിലൂടെ വ്യാജ സന്ദേശങ്ങൾ പ്രചരിപ്പിക്കുകയും, വിശ്വാസ്യതയുണ്ടാക്കാൻ അവർ പങ്കിട്ട മൊബൈൽ നമ്പറിൽ അറിയപ്പെടുന്ന ഏതെങ്കിലും എൻ ബി എഫ് സിയുടെ ലോഗോ പ്രൊഫൈൽ ചിത്രമായി ഉപയോഗിക്കുകയും ചെയ്യുന്നു.
- തട്ടിപ്പുകാർ അവരുടെ ആധാർ കാർഡും പാൻ കാർഡും വ്യാജ എൻ ബി എഫ് സി ഐഡി കാർഡും പങ്കിട്ടേക്കാം.
- വായ്പ തേടുന്നവർക്ക് അത്തരം സന്ദേശങ്ങൾ/എസ് എം എസ്/ഇ-മെയിൽ അയച്ചതിനുശേഷം, തട്ടിപ്പുകാർ ക്രമരഹിതമായി ആളുകളെ വിളിക്കുകയും വ്യാജ അനുമതി കത്തുകൾ, വ്യാജ ചെക്കുകളുടെ പകർപ്പുകൾ തുടങ്ങിയവ പങ്കിടുകയും, വിവിധ ചെലവുകൾക്കായി പണം അടയ്ക്കുവാൻ ആവശ്യപ്പെടുകയും ചെയ്യുന്നു. ഇരകൾ, ഒരിക്കൽ ഈ പണം അടച്ചുകഴിഞ്ഞാൽ, തട്ടിപ്പുകാർ പണവുമായി അപ്രത്യക്ഷമാകുന്നു.



മുൻകരുതൽ

- സ്വന്തം ടെലിഫോണുകൾ/ഇ-മെയിലുകൾ മുതലായവയിലൂടെ വായ്പാ വാഗ്ദാനങ്ങൾ നൽകുന്നത് ഒരിക്കലും വിശ്വസിക്കരുത്.
- അത്തരം വാഗ്ദാനങ്ങൾ വിശ്വസിച്ച് ഒരിക്കലും പണമടയ്ക്കരുത് അല്ലെങ്കിൽ മറ്റ് ഉറവിടങ്ങളിലൂടെ യഥാർത്ഥമാണോ എന്ന് പരിശോധിക്കാതെ അവരുമായി വ്യക്തിഗത/സാമ്പത്തിക വിവരങ്ങൾ പങ്കിടരുത്.
- എസ് എം എസ്/ഇ-മെയിലുകൾ വഴി അയച്ച ലിങ്കുകളിൽ ക്ലിക്ക് ചെയ്യരുത് അല്ലെങ്കിൽ വിളംബര എസ് എം എസ്/ഇ-മെയിലുകൾക്ക് മറുപടി നൽകരുത്
- സംശയാസ്പദമായ അനുബന്ധം (Attachment) അല്ലെങ്കിൽ ഫിഷിംഗ് ലിങ്കുകൾ അടങ്ങിയ പരിചിതമല്ലാത്ത ഉറവിടങ്ങളിൽ നിന്നുള്ള ഇ-മെയിലുകൾ ഒരിക്കലും തുറക്കരുത്/പ്രതികരിക്കരുത്.

3. ഒ ടി പി അടിസ്ഥാനത്തിലുള്ള തട്ടിപ്പ്

പ്രവർത്തനരീതി

- ഉപഭോക്താക്കൾക്ക്, എൻ ബി എഫ് സികളിൽ നിന്നെന്ന വ്യാജേന, തട്ടിപ്പുകാരിൽ നിന്ന് വായ്പ വാഗ്ദാനം ചെയ്യുന്നതോ വായ്പാ പരിധി ഉയർത്തുന്നതോ ആയി എസ് എം എസ്/സന്ദേശങ്ങൾ കിട്ടുകയും തട്ടിപ്പുകാരന്റെ മൊബൈൽ നമ്പറിൽ ബന്ധപ്പെടാൻ ആവശ്യപ്പെടുകയും ചെയ്യുന്നു.
- ഉപഭോക്താക്കൾ ഈ നമ്പറിൽ വിളിക്കുമ്പോൾ, തട്ടിപ്പുകാർ സാമ്പത്തിക വിശദാംശങ്ങൾ അടങ്ങിയ ഏതാനും ഫോമുകൾ (ഓൺലൈനിൽ പോലും) പൂരിപ്പിക്കുവാൻ ആവശ്യപ്പെടുന്നു. അവർ ഒ ടി പി അല്ലെങ്കിൽ PIN വിശദാംശങ്ങൾ പങ്കിടാൻ പ്രേരിപ്പിക്കുകയും/ബോധ്യപ്പെടുത്തുകയും ചെയ്യുന്നു. അതുപയോഗിച്ച് ഉപഭോക്താവിന്റെ അക്കൗണ്ടിൽ നിന്നും അനധികൃതമായി പണം കൈമാറ്റം ചെയ്യുന്നു.

മുൻകരുതൽ

- ഒ ടി പി/പിൻ/വ്യക്തിഗത വിവരങ്ങൾ മുതലായവ ഒരിക്കലും ഒരു രൂപത്തിലും, നിങ്ങളുടെ സുഹൃത്തും കുടുംബാംഗങ്ങളും ഉൾപ്പെടെ, ആരുമായും പങ്കിടരുത്.
- നിങ്ങളുടെ അറിവില്ലാതെ ഒ ടി പി സൃഷ്ടിക്കപ്പെടുന്നില്ലെന്ന് ഉറപ്പുവരുത്തുവാൻ പതിവായി എസ് എം എസ്/ഇ-മെയിലുകൾ പരിശോധിക്കുക.
- സേവനങ്ങളെക്കുറിച്ചുള്ള വിവരങ്ങൾക്കും വിശദീകരണങ്ങൾക്കും ബാങ്ക്, എൻ ബി എഫ് സി, ഇ-വാലറ്റ് ദാതാവ് എന്നിവരുടെ ഔദ്യോഗിക വെബ്സൈറ്റ് സന്ദർശിക്കുകയോ ശാഖയെ നേരിട്ട് ബന്ധപ്പെടുകയോ ചെയ്യേണ്ടതാണ്.

4. വായ്പകളെ സംബന്ധിച്ച വ്യാജ വെബ്സൈറ്റുകൾ /ആപ്ലിക്കേഷൻ (Application)മുഖേനയുള്ള തട്ടിപ്പുകൾ

പ്രവർത്തനരീതി

- തൽക്ഷണ, ഹ്രസ്വകാല വായ്പ വാഗ്ദാനം ചെയ്യുന്ന നിരവധി അനൈതികമായ വായ്പാ ആപ്പുകൾ ഉണ്ട്. ഈ ആപ്പുകൾ വായ്പയെടുക്കുന്നവരെ കബളിപ്പിക്കുകയും ഗണ്യമായ ഉയർന്ന പലിശ ഈടാക്കുകയും ചെയ്യും.
- എളുപ്പം കബളിപ്പിക്കാവുന്ന ഉപഭോക്താക്കളെ ആകർഷിക്കുവാൻ, തട്ടിപ്പുകാർ 'പരിമിത കാലയളവിലെ വാഗ്ദാനങ്ങൾ' എന്ന് പരസ്യം ചെയ്യുകയും സമ്മർദ്ദ തന്ത്രങ്ങൾ ഉപയോഗിച്ച് അടിയന്തിര തീരുമാനങ്ങൾ എടുക്കുവാൻ അപേക്ഷകരോട് ആവശ്യപ്പെടുകയും ചെയ്യുന്നു.

മുൻകരുതൽ

- സംശയാസ്പദമായ വായ്പാ അപ്പ് മുതലായവയിൽ നിന്ന് വായ്പ എടുക്കുന്നതിന് മുമ്പ് ഇനിപ്പറയുന്ന കാര്യങ്ങൾ പരിശോധിക്കുക.
- വായ്പ നൽകുന്നയാൾ സർക്കാർ/അംഗീകൃത ഏജൻസികളിൽ രജിസ്റ്റർ ചെയ്തിട്ടുണ്ടോ എന്ന് പരിശോധിക്കുക.
- കടം കൊടുക്കുന്നയാൾ ഒരു പ്രത്യക്ഷമായ വിലാസമോ ബന്ധപ്പെടുന്നതിനുള്ള വിവരമോ നൽകിയിട്ടുണ്ടോ എന്ന് പരിശോധിക്കുക; അല്ലാത്തപക്ഷം പിന്നീട് അവരെ ബന്ധപ്പെടുവാൻ ബുദ്ധിമുട്ടായേക്കാം.
- ക്രെഡിറ്റ് സ്കോറുകൾ പരിശോധിക്കുന്നതിനുപകരം വ്യക്തിഗത വിശദാംശങ്ങൾ അറിയാൻ കടം കൊടുക്കുന്നയാൾ കൂടുതൽ താൽപ്പര്യം കാണിക്കുന്നെങ്കിൽ ജാഗ്രത പാലിക്കുക.
- ലോൺ അപേക്ഷ കൈകാര്യം ചെയ്യുന്നതിന് മുമ്പ് ഏതെങ്കിലും പ്രശസ്തമായ എൻ ബി എഫ് സി/ബാങ്ക് പണമടയ്ക്കാൻ ആവശ്യപ്പെടില്ലെന്ന് ഓർക്കുക.
- രേഖകൾ പരിശോധിക്കാതെ യഥാർത്ഥ വായ്പാ ദാതാക്കൾ ഒരിക്കലും പണം വാഗ്ദാനം ചെയ്യുകയില്ല.
- ഈ എൻ ബി എഫ് സി- പിന്തുണയുള്ള വായ്പാ ആപ്പുകൾ യഥാർത്ഥമാണോയെന്ന് പരിശോധിക്കുക.

5. മണി സർക്കുലേഷൻ/പോൻസി/മൾട്ടി ലെവൽ മാർക്കറ്റിംഗ് (MLM) പദ്ധതികളുടെ പേരിലുള്ള തട്ടിപ്പുകൾ

പ്രവർത്തനരീതി

- എം എൽ എം/ചെയിൻ മാർക്കറ്റിംഗ്/പിരമിഡ് ഘടന പദ്ധതികൾ അംഗമായി ചേരുമ്പോൾ/അംഗങ്ങളെ ചേർക്കുമ്പോൾ, എളുപ്പത്തിൽ അല്ലെങ്കിൽ ഉടൻ പണം വാഗ്ദാനം ചെയ്യുന്നു.
- ഈ പദ്ധതികൾ ഉയർന്ന വരുമാനം ഉറപ്പു നൽകുക മാത്രമല്ല, വ്യക്തികളുടെ ആത്മവിശ്വാസം നേടുവാനും വാക്കാലുള്ള പ്രചാരണത്തിലൂടെ കൂടുതൽ നിക്ഷേപകരെ ആകർഷിക്കുവാനും, വാഗ്ദാനം ചെയ്തതുപോലെ ആദ്യം കുറച്ച് തവണകൾ നൽകുകയും ചെയ്യും.

- ഈ പദ്ധതി കൂടുതൽ അംഗങ്ങളെ കണ്ണിയിൽ/സംഘത്തിൽ ചേർക്കുന്നതിന് പ്രോത്സാഹിപ്പിക്കുന്നു. അതിനായി ഉൽപ്പനങ്ങളുടെ വിൽപ്പനയിൽ നിന്നുള്ള പ്രതിഫലത്തിനു പകരം, അംഗങ്ങളെ കണ്ണിയിൽ ചേർക്കുന്നവർക്ക് പ്രതിഫലം നൽകുന്നു.
- ഈ മാതൃക കാരണം, കുറച്ച് സമയത്തിന് ശേഷം പദ്ധതിയിൽ പുതിയതായി ചേരുന്ന ആളുകളുടെ എണ്ണം കുറയാൻ തുടങ്ങുമ്പോൾ പദ്ധതി അസന്തുലിതമാകുന്നു. അതിനുശേഷം, തട്ടിപ്പുകാർ പദ്ധതി അവസാനിപ്പിക്കുകയും നിക്ഷേപകരുടെ പണവുമായി അപ്രത്യക്ഷമാവുകയും ചെയ്യുന്നു.

മുൻകരുതൽ

- പോൻസി/എം എൽ എം പദ്ധതികളിൽ നിക്ഷേപം നടത്തുമ്പോൾ വരുമാനം (Returns) അപകടസാധ്യതകൾക്ക് (Risks) ആനുപാതികമാണ്. ഉയർന്ന വരുമാനത്തിന് അപകടസാധ്യത കൂടുതലാണ്.
- അതിനാൽ, ഏതെങ്കിലും പദ്ധതി അസാധാരണമായി (ഓരോ വർഷവും 40-50 ശതമാനം വരെ) ഉയർന്ന വരുമാനം വാഗ്ദാനം ചെയ്യുന്നുണ്ടെങ്കിൽ, അത് ഉണ്ടാകുവാൻ സാദ്ധ്യതയുള്ള തട്ടിപ്പിന്റെ ആദ്യ സൂചനയാണ്. അതിനാൽ ജാഗ്രത പുലർത്തണം.
- സാധനങ്ങളുടെ/സേവനത്തിന്റെ യഥാർത്ഥ വിൽപ്പനയില്ലാതെ ഏതെങ്കിലും പണമടയ്ക്കൽ/പ്രതിഫലം/ കമ്മീഷൻ/ബോണസ്/ലാഭത്തിന്റെ ശതമാനം നൽകുന്ന പദ്ധതികൾ സംശയാസ്പദമാണെന്നും വഞ്ചനയിലേക്ക് നയിച്ചേക്കാമെന്നും എപ്പോഴും ശ്രദ്ധിക്കുക.
- മൾട്ടി ലെവൽ മാർക്കറ്റിംഗ്/ചെയിൻ മാർക്കറ്റിംഗ്/പിരമിഡ് സ്ട്രക്ച്ചറുകൾ/പദ്ധതികൾ നടത്തുന്ന സ്ഥാപനങ്ങൾ വാഗ്ദാനം ചെയ്യുന്ന ഉയർന്ന വരുമാനത്തിൽ പ്രലോഭിതരാവരുത്.
- മണി സർക്കുലേഷൻ/മൾട്ടി ലെവൽ മാർക്കറ്റിംഗ്/പിരമിഡ് സ്ട്രക്ച്ചറുകൾക്ക് കീഴിൽ പണം സ്വീകരിക്കുന്നത് 1978 ലെ പ്രൈസ് ചിറ്റ് ആൻഡ് മണി സർക്കുലേഷൻ (നിരോധനം) നിയമം അനുസരിച്ച് പ്രത്യക്ഷമായ കുറ്റമാണ്.
- അത്തരം വാഗ്ദാനങ്ങൾ ശ്രദ്ധയിൽ പെട്ടാൽ ഉടൻ തന്നെ സംസ്ഥാന പോലീസിൽ പരാതി നൽകണം.

6. വ്യാജ രേഖകൾ ഉപയോഗിച്ചുള്ള വായ്പാ തട്ടിപ്പുകൾ

പ്രവർത്തനരീതി

- തട്ടിപ്പുകാർ, സാമ്പത്തിക സ്ഥാപനങ്ങളിൽ നിന്ന് സേവനങ്ങൾ ലഭിക്കുന്നതിന് വ്യാജ രേഖകൾ ഉപയോഗിക്കുന്നു.
- തട്ടിപ്പുകാർ, ഉപഭോക്താവിന്റെ ഐഡന്റിറ്റി കാർഡ്, ബാങ്ക് അക്കൗണ്ട് വിവരങ്ങൾ മുതലായ സ്വകാര്യ വിവരങ്ങൾ മോഷ്ടിക്കുന്നു. ഈ വിവരങ്ങളും വ്യക്തിഗത വിവരങ്ങളും ഉപയോഗപ്പെടുത്തി സാമ്പത്തിക സ്ഥാപനങ്ങളിൽ നിന്നും ആനുകൂല്യങ്ങൾ കൈപ്പറ്റുന്നു.
- തട്ടിപ്പുകാർ, എൻ ബി എഫ് സി ജീവനക്കാരൻ എന്ന വ്യാജേന ഉപഭോക്താവിന്റെ KYC അനുബന്ധ രേഖകൾ കൈക്കലാക്കുന്നു.

മുൻകരുതൽ

- ഏതൊരു സ്ഥാപനത്തിൽ നിന്നും വായ്പയ്ക്ക് അനുമതി/വായ്പാ സൗകര്യങ്ങൾ ലഭ്യമാക്കുവാൻ ഉപഭോക്താക്കൾ KYC യും NACH ഫോം ഉൾപ്പെടെയുള്ള മറ്റ് വ്യക്തിഗത രേഖകളും നൽകുമ്പോൾ തികഞ്ഞ ജാഗ്രതയും ശ്രദ്ധയും പാലിക്കേണ്ടതാണ്.
- അത്തരം രേഖകൾ സ്ഥാപനത്തിന്റെ അംഗീകൃത വ്യക്തികളുമായോ സ്ഥാപനങ്ങളുടെ അംഗീകൃത ഇ-മെയിൽ ഐഡികളുമായോ മാത്രമേ പങ്കിടാവൂ.
- കൂടാതെ, വായ്പ അനുവദിക്കാത്ത അവസരത്തിലും വായ്പ അവസാനിപ്പിക്കുന്ന സമയത്തും ഉപഭോക്താവ് സ്ഥാപനങ്ങൾക്ക് നൽകിയ രേഖകൾ നീക്കം ചെയ്യുവാൻ ആവശ്യപ്പെടേണ്ടതാണ്.

ഭാഗം – മൂന്ന്
സാമ്പത്തിക ഇടപാടുകൾക്കായി സ്വീകരിക്കേണ്ട പൊതുവായ മുൻകരുതലുകൾ

പൊതുവായ മുൻകരുതലുകൾ

- നിങ്ങളുടെ ഇന്റർനെറ്റ് ഉപയോഗിക്കുന്ന സമയത്ത് (browsing session) പ്രത്യക്ഷപ്പെടുന്ന സംശയാസ്പദമായ പോപ്പ്-അപ്പ് (Pop-up) കൾക്കെതിരെ ജാഗ്രതപാലിക്കുക.
- ഓൺലൈൻ പണമിടപാടുകൾ നടത്തുന്നതിന് മുമ്പ് എല്ലായ്പ്പോഴും സുരക്ഷിതമായ പേയ്മെന്റ് ഗേറ്റ്‌വേ (https:// താഴിന്റെ (padlock) ചിഹ്നമുള്ള URL) പരിശോധിക്കുക.
- നിങ്ങളുടെ പിൻ (വ്യക്തിഗത തിരിച്ചറിയൽ നമ്പർ) പാസ്‌വേഡ്, ക്രെഡിറ്റ് അല്ലെങ്കിൽ ഡെബിറ്റ് കാർഡ് നമ്പർ, സി വി വി എന്നീ സ്വകാര്യ സാമ്പത്തിക വിവരങ്ങൾ ബാങ്ക്, സാമ്പത്തിക സ്ഥാപനങ്ങൾ, കൂട്ടുകാർ, കുടുംബാംഗങ്ങൾ എന്നിവരുമായി പങ്കുവയ്ക്കാതിരിക്കുക.
- വെബ്സൈറ്റുകൾ/ഉപകരണങ്ങൾ/പൊതു ലാപ്ടോപ്പ്/ഡെസ്ക്ടോപ്പുകൾ എന്നിവയിൽ കാർഡ് വിശദാംശങ്ങൾ സൂക്ഷിക്കുന്നത് ഒഴിവാക്കുക.

- സൗകര്യം ലഭ്യമാകുന്നിടത്ത്, ദ്വിഘടക സാധൂകരണം (two-factor authentication) പ്രവർത്തനക്ഷമമാക്കുക.
- സംശയാസ്പദമായ അനുബന്ധം (Attachment) അല്ലെങ്കിൽ ഫിഷിംഗ് ലിങ്കുകൾ ഉണ്ടായേക്കാം എന്നതിനാൽ അജ്ഞാതമായ/പരിചിതമല്ലാത്ത ഉറവിടങ്ങളിൽ നിന്നുള്ള ഇ-മെയിലുകൾ ഒരിക്കലും തുറക്കരുത്.
- ചെക്ക്ബുക്ക്, KYC രേഖകളുടെ പകർപ്പുകൾ അപരിചിതരുമായി പങ്കിടരുത്.

ഉപകരണം/കമ്പ്യൂട്ടർ സുരക്ഷയ്ക്കായി

- കൃത്യമായ ഇടവേളകളിൽ പാസ്‌വേഡുകൾ മാറ്റുക.
- ഉപകരണത്തിൽ ആന്റി വൈറസ് ഇൻസ്റ്റാൾ ചെയ്യുക, ലഭ്യമാകുമ്പോഴെല്ലാം അപ്ഡേറ്റുകൾ ഇൻസ്റ്റാൾ ചെയ്യുക.
- ഉപയോഗിക്കുന്നതിന് മുമ്പ്, എല്ലായ്പ്പോഴും അജ്ഞാത USB ഡ്രൈവുകൾ/ഉപകരണങ്ങൾ സ്കാൻ ചെയ്യുക.
- നിങ്ങളുടെ ഉപകരണം ലോക്ക് ചെയ്യാതെ മാറ്റി വയ്ക്കരുത്.
- ഉപകരണത്തിന്റെ ഓട്ടോ ലോക്ക് നിർദ്ദിഷ്ട സമയത്തേക്ക് ക്രമീകരിക്കുക.
- നിങ്ങളുടെ ഫോണിൽ/ലാപ്ടോപ്പിൽ പരിചിതമല്ലാത്ത ആപ്ലിക്കേഷനുകളോ സോഫ്റ്റ്‌വെയറോ ഇൻസ്റ്റാൾ ചെയ്യരുത്.

- പാസ്‌വേഡുകളോ രഹസ്യ വിവരങ്ങളോ ഉപകരണങ്ങളിൽ സൂക്ഷിക്കരുത്.

സുരക്ഷിത ഇന്റർനെറ്റ് ബ്രൗസിംഗിനായി

- സുരക്ഷിതമല്ലാത്ത വെബ്സൈറ്റുകൾ സന്ദർശിക്കുന്നത് ഒഴിവാക്കുക.
- അജ്ഞാതമായ/പരിചിതമല്ലാത്ത ബ്രൗസറുകൾ ഉപയോഗിക്കുന്നത് ഒഴിവാക്കുക.
- പൊതു ഉപകരണങ്ങളിൽ പാസ്‌വേഡുകൾ സൂക്ഷിക്കുന്നതോ/ഉപയോഗിക്കുന്നതോ ഒഴിവാക്കുക.
- പരിചയമില്ലാത്ത വെബ്സൈറ്റുകളിൽ സുരക്ഷിതമായ വ്യക്തിഗത വിവരങ്ങൾ നൽകുന്നത് ഒഴിവാക്കുക.
- ആരുമായും സ്വകാര്യ വിവരങ്ങൾ പങ്കിടരുത്, പ്രത്യേകിച്ചും സമൂഹ മാദ്ധ്യമങ്ങളിലെ അജ്ഞാതരായ വ്യക്തികളുമായി.
- ഒരു ഇ-മെയിൽ അല്ലെങ്കിൽ എസ് എം എസ് ലിങ്ക് പുനപ്രേഷണം (redirect) ചെയ്യപ്പെട്ടാൽ, പേജിന്റെ സുരക്ഷ (https:// താഴിന്റെ ചിഹ്നമുള്ള URL) എപ്പോഴും പരിശോധിക്കുക.

സുരക്ഷിത ഇന്റർനെറ്റ് ബാങ്കിങ്ങിനായി

- പൊതു ഉപകരണങ്ങളിൽ എല്ലായ്പ്പോഴും വെർച്വൽ കീബോർഡ് (virtual keyboard) ഉപയോഗിക്കുക, കാരണം നിങ്ങൾ ടൈപ്പ് ചെയ്യുന്ന കാര്യങ്ങൾ വിട്ടുവീഴ്ച ചെയ്യപ്പെട്ട ഉപകരണങ്ങൾ, കീബോർഡ് മുതലായവയിലൂടെയും പിടിച്ചെടുക്കുവാൻ കഴിയും.
- ഉപയോഗം കഴിഞ്ഞയുടനെ ഇന്റർനെറ്റ് ബാങ്കിംഗ് സെഷനിൽ നിന്ന് പുറത്തുകടക്കുക (Logout).
- നിശ്ചിത കാലയളവിൽ പാസ്‌വേഡുകൾ മാറ്റുക.
- ഇ-മെയിൽ, ഇന്റർനെറ്റ് ബാങ്കിംഗ് എന്നിവയ്ക്കായി ഒരേ പാസ്‌വേഡുകൾ ഉപയോഗിക്കരുത്.
- സാമ്പത്തിക ഇടപാടുകൾക്കായി പൊതു ഉപകരണങ്ങൾ (സൈബർ കഫെ മുതലായവ) ഉപയോഗിക്കുന്നത് ഒഴിവാക്കുക.

ഫോൺ, തട്ടിപ്പുകാരുടെ നിരീക്ഷണത്തിലാണ് എന്ന് സൂചിപ്പിക്കുന്ന ഘടകങ്ങൾ

- അപരിചിതമായ ആപ്പുകൾ ഫോണിൽ ഡൗൺലോഡ് ചെയ്യപ്പെട്ടിരിക്കുന്നു.
- ബാറ്ററിയുടെ ചാർജ് സാധാരണയിൽ നിന്നും വേഗത്തിൽ കുറയുന്നു.
- ഫോൺ ചൂടാകുന്നത് ഫോണിലെ വിവരങ്ങൾ ചോർത്തുന്നതിനായി പശ്ചാത്തലത്തിൽ സ്പൈ വെയർ പ്രവർത്തിക്കുന്നത് കൊണ്ടാകാം.
- ഫോണിലെ ഡാറ്റ ഉപയോഗം ക്രമാതീതമായി വർധിക്കുന്നതും പശ്ചാത്തലത്തിൽ സ്പൈവെയർ പ്രവർത്തിക്കുന്നത് കൊണ്ടാകാം.
- സ്പൈ വെയർ ആപ്പുകൾ ഫോണിന്റെ ഷട്ട് ഡൗൺ പ്രക്രിയയെ ബാധിച്ചേക്കാം. ചിലപ്പോൾ ഫോൺ കൃത്യമായി ഷട്ട് ഡൗൺ ആകുന്നില്ല അല്ലെങ്കിൽ പതിവിൽ കവിഞ്ഞ സമയം എടുത്തേക്കാം.
- സ്പൈ വെയറിനും മാൽവെയറിനും വിവരങ്ങൾ അയയ്ക്കാനും സ്വീകരിക്കാനും ടെക്സ്റ്റ് മെസ്സേജ് ഉപയോഗിക്കാൻ കഴിയുമെന്നും മനസ്സിലാക്കുക.

ഒരു തട്ടിപ്പ് നടന്നാൽ സ്വീകരിക്കേണ്ട നടപടികൾ

- ഡെബിറ്റ് കാർഡ്/ക്രെഡിറ്റ് കാർഡ് ബ്ലോക്ക് ചെയ്യുക മാത്രമല്ല, ബാങ്കിന്റെ വെബ് സൈറ്റിൽ ലഭ്യമായ കസ്റ്റമർ കെയർ നമ്പറിൽ വിളിക്കുകയോ ശാഖ സന്ദർശിക്കുകയോ ചെയ്ത്, കാർഡുമായി ലിങ്ക് ചെയ്തിരിക്കുന്ന ബാങ്ക് അക്കൗണ്ട് മരവിപ്പിക്കേണ്ടതാണ്. തട്ടിപ്പ് നടന്നതിനു ശേഷം ഡെബിറ്റ്/ക്രെഡിറ്റ് കാർഡുകൾ ബ്ലോക്ക് ചെയ്താലും നിരന്തരമായ തട്ടിപ്പിൽ നിന്നും രക്ഷ നേടുന്നതിനായി മറ്റു ബാങ്കിങ് ചാനലുകളായ നെറ്റ് ബാങ്കിങ്, മൊബൈൽ ബാങ്കിങ് തുടങ്ങിയവ പരിശോധിക്കുകയും അവയുടെ സുരക്ഷിതത്വം ഉറപ്പുവരുത്തുകയും വേണം.
- ഹെൽപ് ലൈൻ നമ്പർ 155260 ൽ വിളിക്കുകയോ നാഷണൽ സൈബർ ക്രൈം റിപ്പോർട്ടിങ് പോർട്ടലിൽ (www.cybercrime.gov.in) വിവരം അറിയിക്കുകയോ വേണം.
- മൊബൈൽ റീസെറ്റ് ചെയ്യുക: മൊബൈൽ ഫോണിൽ നിന്നും വിവരങ്ങൾ ചോർന്നത് കൊണ്ടാണ് തട്ടിപ്പ് നടന്നതെങ്കിൽ മൊബൈൽ റീസെറ്റ് ചെയ്യുക (സെറ്റിങ്-റീ സെറ്റ്-ഫാക്ടറി ഡേറ്റ) (setting→ reset-factory data).

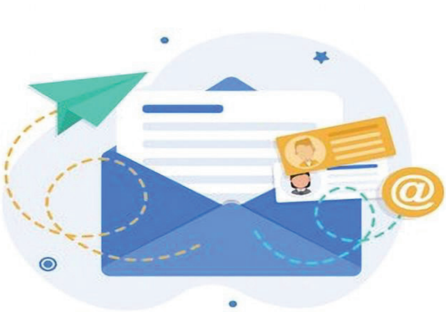
ഡെബിറ്റ്/ക്രെഡിറ്റ് കാർഡുകളുമായി ബന്ധപ്പെട്ട മുൻകരുതൽ

- തൽക്കാലത്തേക്ക് നിങ്ങൾ ക്രെഡിറ്റ്/ഡെബിറ്റ് കാർഡുകൾ ഉപയോഗിക്കുന്നില്ലെങ്കിൽ അവയുടെ പല പ്രവർത്തനങ്ങളും, ഉദാഹരണത്തിന്, പ്രാദേശികവും അന്താരാഷ്ട്രവുമായ ഓൺലൈൻ ഇടപാടുകൾ നിഷ്ക്രിയമാക്കേണ്ടതും കാർഡ് ഉപയോഗിക്കേണ്ടപ്പോൾ മാത്രം അവ പ്രയോഗക്ഷമമാക്കേണ്ടതുമാണ്.
- അതുപോലെ തന്നെ, കാർഡ് ഉപയോഗിക്കുന്നില്ലെങ്കിൽ സമീപ ഫീൽഡ് ആശയ വിനിമയം (near field communication-NFC) നിഷ്ക്രിയമാക്കേണ്ടതാണ്.
- കച്ചവട സ്ഥാപനത്തിലെ വിൽപ്പന പോയിന്റ് (POS) സൈറ്റിലോ അഥവാ NFC റീഡർ ഉപയോഗിക്കുമ്പോഴോ പിൻ നൽകുന്നതിനു മുൻപ് സ്ക്രീനിൽ/റീഡറിൽ കാണുന്ന തുക കൃത്യമായി പരിശോധിക്കേണ്ടതാണ്.

- ഇടപാട് നടത്തുമ്പോൾ മെഷീനിൽ സൈ്വപ് ചെയ്യുന്നതിനായി വ്യാപാരിയുടെ കൈവശം കാർഡ് കൊടുക്കുമ്പോൾ നമുക്ക് കാണാൻ കഴിയാത്ത സ്ഥലത്തേക്ക് കൊടുത്തുവിടരുത്.
- വ്യാപാരസ്ഥാപനങ്ങളിൽ/ATM ൽ PIN രേഖപ്പെടുത്തുമ്പോൾ കീപാഡ് കൈ കൊണ്ട് മറയ്ക്കുക.

ഇ-മെയിൽ അക്കൗണ്ട് സുരക്ഷയ്ക്കായി

- അജ്ഞാതമായ/പരിചിതമല്ലാത്ത വിലാസങ്ങളിൽ/പേരുകളിൽ നിന്നുള്ള ഇ-മെയിലുകളിൽ ക്ലിക്ക് ചെയ്യരുത്.
- പൊതുവായ അല്ലെങ്കിൽ സൗജന്യ നെറ്റ്‌വർക്കുകളിൽ ഇ-മെയിലുകൾ ഉപയോഗിക്കുന്നത് ഒഴിവാക്കുക.
- സുരക്ഷിത വ്യക്തിഗത വിവരങ്ങൾ/ ബാങ്ക്പാസ്‌വേഡുകൾ മുതലായവ ഇ-മെയിലുകളിൽ സൂക്ഷിക്കരുത്.



പാസ്‌വേഡ് സുരക്ഷയ്ക്കായി

- നിങ്ങളുടെ പാസ്‌വേഡിൽ അക്കങ്ങൾ, അക്ഷരങ്ങൾ, (ആൽഫാന്യൂമെറിക്), പ്ര ത്യേക പ്രതീകങ്ങൾ (special characters) എന്നിവ ചേർത്ത് ഉപയോഗിക്കുക.
- സൗകര്യം ലഭ്യമാണെങ്കിൽ നിങ്ങളുടെ എല്ലാ അക്കൗണ്ടുകൾക്കും ദ്വിഘടക സാധൂകരണം (two factor authentication) നിലനിർത്തുക.
- നിശ്ചിത കാലയളവിൽ പാസ്‌വേഡുകൾ മാറ്റുക.
- നിങ്ങളുടെ ജന്മദിനം, ജീവിത പങ്കാളിയുടെ പേര്, വാഹനത്തിന്റെ നമ്പർ മുത ലായവ പാസ്‌വേഡ് ആയി ഉപയോഗിക്കരുത്.

ഒരു എൻ ബി എഫ് സി നിക്ഷേപം സ്വീകരിക്കുന്നത് യഥാർത്ഥ മാണോ അല്ലയോ എന്ന് നിങ്ങൾക്ക് എങ്ങനെ അറിയാം?

- നിക്ഷേപങ്ങൾ സ്വീകരിക്കുന്നതിന് അർഹതയുള്ള എൻ ബി എഫ് സികളുടെ പട്ടികയിൽ ഈ എൻ ബി എഫ് സി ഉണ്ടോ എന്ന് നിക്ഷേപകൻ പരിശോധിക്കണം. ഇത് https://rbi.org.in ൽ ലഭ്യമാണ്. കൂടാതെ നിക്ഷേപങ്ങൾ സ്വീകരിക്കുന്ന തിൽ നിന്ന് വിലക്കപ്പെട്ട കമ്പനികളുടെ പട്ടികയിൽ അത് പ്രത്യക്ഷപ്പെടുന്നില്ലെന്ന് ഉറപ്പുവരുത്തുകയും വേണം.

- റിസർവ് ബാങ്ക് നൽകിയ സർട്ടിഫിക്കറ്റ് ഓഫ് രജിസ്ട്രേഷൻ (CoR) എൻ ബി എഫ് സികൾ അവരുടെ വെബ്സൈറ്റിൽ വ്യക്തമായി പ്രദർശിപ്പിച്ചിരിക്കണം. ഈ സർട്ടി ഫിക്കറ്റിൽ എൻ ബി എഫ് സിയ്ക്ക് നിക്ഷേപങ്ങൾ സ്വീകരിക്കുന്നതിന് റിസർവ് ബ ാങ്ക് സവിശേഷമായ അംഗീകാരം നൽകിയിട്ടുണ്ടെന്നും സ്പഷ്ടമാക്കണം. നിക്ഷേ പങ്ങൾ സ്വീകരിക്കുവാൻ എൻ ബി എഫ് സിക്ക് അധികാരമുണ്ടെന്ന് ഉറപ്പാക്കു വാൻ നിക്ഷേപകർ ഈ സാക്ഷ്യപത്രം പരിശോധിക്കണം.

- എൻ ബി എഫ് സികൾക്ക് 12 മാസത്തിൽ കുറവുള്ളതും 60 മാസത്തിൽ കൂടു തൽ കാലാവധിയുള്ളതുമായ നിക്ഷേപം സ്വീകരിക്കുവാൻ സാദ്ധ്യമല്ല. കൂടാതെ ഒരു എൻ ബി എഫ് സിക്ക് ഒരു നിക്ഷേപകന് നൽകാൻ കഴിയുന്ന പരമാവധി പലിശ നിരക്ക് 12.5% കവിയരുത്.

- റിസർവ് ബാങ്ക് പലിശ നിരക്കിലെ മാറ്റം https://rbi.org.in➤site map➤NBFC List➤FAQs ൽ പ്രസിദ്ധീകരിക്കുന്നു.

നിക്ഷേപകർ സ്വീകരിക്കേണ്ട മുൻകരുതലുകൾ

- ബാങ്ക്/എൻ ബി എഫ് സി/കമ്പനി എന്നിവയിൽ നിക്ഷേപിക്കുന്ന ഓരോ തുകയ്ക്കും കൃത്യമായ രസീത് നൽകണമെന്ന് നിക്ഷേപകൻ നിർബന്ധിക്കണം.
- കമ്പനി അംഗീകരിച്ച ഒരു ഉദ്യോഗസ്ഥൻ രസീത് ഒപ്പിടുകയും, നിക്ഷേപ തീയതി, നിക്ഷേപകന്റെ പേര്, വാക്കുകളിലും അക്കങ്ങളിലും തുക, കൊടുക്കേണ്ടതായ പലിശ നിരക്ക്, കാലാവധി പൂർത്തിയാകുന്ന തീയതി, കാലാവധി തുക, എന്നിവ രസീതിൽ രേഖപ്പെടുത്തുകയും വേണം.
- എൻ ബി എഫ് സികളുടെ പേരിൽ പൊതു നിക്ഷേപങ്ങൾ ശേഖരിക്കുന്ന ബ്രോക്കർമാർ/ഏജന്റുമാർ മുതലായവയുടെ കാര്യത്തിൽ, ബ്രോക്കർമാരും/ഏജന്റുമാരും എൻ ബി എഫ് സിയുടെ ക്രമപരമായ അംഗീകാരമുള്ളവരാണെന്ന് നിക്ഷേപകർ സ്വയം സ്ഥിരീകരിക്കണം.
- എൻ ബി എഫ് സികളുടെ നിക്ഷേപകർക്ക് ഡെപ്പോസിറ്റ് ഇൻഷുറൻസ് പരിരക്ഷ ലഭ്യമല്ലെന്ന് നിക്ഷേപകൻ ഓർമ്മിക്കണം.

ഒരു ഓൺലൈൻ പരാതി എങ്ങനെ നൽകാം

ആർ ബി ഐ ഓംബുഡ്സ്മാന് പരാതി

- ഓൺലൈൻ ആയി പരാതി നൽകുന്നതിന് https://cms.rbi.org.in/ എന്ന ലിങ്ക് സന്ദർശിക്കുക.
- crpc@rbi.org.in എന്ന ഇ-മെയിലിൽ പരാതി അയയ്ക്കാവുന്നതാണ്
- എഴുതി തയ്യാറാക്കിയ പരാതികൾ സി ആർ പി സി, റിസർവ് ബാങ്ക് ഓഫ് ഇന്ത്യ, സെൻട്രൽ വിസ്ത, സെക്ടർ -17, ചണ്ഡീഗഡ് - 160 017 എന്ന വിലാസത്തിൽ അയയ്ക്കാവുന്നതാണ്.

സെക്യൂരിറ്റി ആൻഡ് എക്സ്ചേഞ്ച് ബോർഡ് ഓഫ് ഇന്ത്യയ്ക്ക് (സെബി) (SEBI) പരാതി

- https://sebi.gov.in/ എന്ന ലിങ്ക് ഓൺലൈൻ ആയി പരാതി നൽകുന്നതിന് സന്ദർശിക്കുക.

ഇൻഷുറൻസ് റെഗുലേറ്ററി ആൻഡ് ഡെവലപ്മെന്റ് അതോറിറ്റി ഓഫ് ഇന്ത്യ (ഐ ആർ ഡി എ ഐ) യ്ക്ക് പരാതി

- https://irda.gov.in/ എന്ന ലിങ്ക് സന്ദർശിക്കുക

നാഷണൽ ഹൗസിംഗ് ബാങ്കിന് (എൻ എച്ച് ബി) പരാതി

- https://nhb.org.in/ എന്ന ലിങ്ക് സന്ദർശിക്കുക

സൈബർ പോലീസ് സ്റ്റേഷനിൽ പരാതി

- https://cybercrime.gov.in/ എന്ന ലിങ്ക് സന്ദർശിക്കുക

പദാവലി

മുൻകൂർ ഫീസ്/നടപടിക്രമങ്ങൾക്കുള്ള ഫീസ്/ടോക്കൺ ഫീസ് (Advance fee/processing fee/token fee): പ്രമാണങ്ങൾ തയ്യാറാക്കുന്നതിനുള്ള തുക, യോഗ ചെലവുകൾ, ബാധകമായ നടപടിക്രമങ്ങൾക്കുള്ള ഫീസുകൾ, കടം വാങ്ങുന്നയാൾക്ക് ലോൺ വിതരണത്തിനായി ചുമത്തിയേക്കാവുന്ന മറ്റേതെങ്കിലും ചാർജുകൾ എന്നിങ്ങനെ എല്ലാ പ്രാരംഭ പ്രവർത്തനങ്ങൾക്കുമായി വായ്പ വാങ്ങുന്നയാൾ നൽകേണ്ട തുക.

ദ്വിഘടക സാധൂകരണം (Two factor Authentication): ദ്വിഘടക സാധൂകരണം (2FA എന്നും അറിയപ്പെടുന്നു) എന്നാൽ ഇടപാടുകൾ സാധൂകരിക്കുന്നതിന് രണ്ട് വ്യത്യസ്ത ഘടകങ്ങളുടെ ഉപയോഗം. ഇടപാടുകളുടെ സാധൂകരണത്തിനായി ഉപയോഗിക്കുന്ന മൂന്ന് അടിസ്ഥാന ഘടകങ്ങൾ – നിങ്ങളുടെ പക്കലുള്ള കാർഡ് (നമ്പർ, കാലഹരണ തീയതി, കാർഡിൽ അച്ചടിച്ചിരിക്കുന്ന CVV, നിങ്ങൾക്ക് അറിയാവുന്ന പിൻ (സ്ഥിരമായ/ഒരിക്കൽ മാത്രം ഉപയോഗിക്കാവുന്ന), നിങ്ങൾ തന്നെ (ബ്രയോമെട്രിക്-സവിശേഷം വിരലടയാളം). ഇടപാടുകൾ സാധുവാക്കുവാൻ ഇതിൽ ഏതെങ്കിലും രണ്ടു ഘടകങ്ങളുടെ ഉപയോഗത്തിലൂടെ ഉപയോക്താക്കളുടെ വ്യക്തമായ തിരിച്ചറിയൽ ലഭിക്കുന്നു.

ഓതറൈസേഷൻ (അംഗീകാരം) (Authorisation): ഇടപാട് അംഗീകരിക്കുവാനുള്ള വ്യാപാരിയുടെ അഭ്യർത്ഥനയ്ക്ക് പേയ്മെന്റ് വിവരങ്ങൾ സാധുതയുള്ളതാണെന്നും ഉപഭോക്താവിന്റെ ക്രെഡിറ്റ് കാർഡിൽ ഫണ്ടുകൾ ലഭ്യമാണെന്നും സൂചിപ്പിക്കുന്ന കാർഡ് നൽകിയ ബാങ്കിൽ നിന്നുള്ള പ്രതികരണം.

കാർഡ് നമ്പർ (Card Number): കാർഡ് ഉടമയ്ക്ക് ക്രെഡിറ്റ് കാർഡ് അസോസിയേഷൻ അല്ലെങ്കിൽ കാർഡ് നൽകിയ ബാങ്ക് നൽകുന്ന അക്കൗണ്ട് നമ്പർ. ക്രെഡിറ്റ് കാർഡ് പേയ്മെന്റ് നടത്തുന്നതിന് ഉപഭോക്താവ് ഈ വിവരങ്ങൾ വ്യാപാരിക്ക് നൽകണം. മറ്റുള്ളവരുമായി നമ്പർ പങ്കുവയ്ക്കുവാൻ പാടില്ല. കാർഡ് നമ്പർ കാർഡിൽ അച്ചടിച്ചിട്ടുണ്ട്.

ക്രെഡിറ്റ് കാർഡുകൾ (Credit Cards): ഒരു ധനകാര്യ സ്ഥാപനത്തിൽ നിന്ന് ഈടോടെയോ അല്ലാതെയോ കടമായി, ഉൽപ്പന്നങ്ങൾക്കോ സേവനങ്ങൾക്കോ പണമടയ്ക്കാൻ അനുവദിക്കുന്ന കാർഡുകൾ.

ക്രെഡിറ്റ് ലിമിറ്റ് (Credit Limit): വായ്പാപരിധി എന്നത് ഒരു സാമ്പത്തിക സ്ഥാപനം ഇടപാടുകാരന് നൽകുന്ന പരമാവധി വായ്പ തുകയെ സൂചിപ്പിക്കുന്നു. വായ്പ നൽകുന്ന സ്ഥാപനം ക്രെഡിറ്റ് കാർഡിലോ മുൻകൂട്ടി നിശ്ചയിച്ച വായ്പയിലോ അതിന്റെ പരമാവധി വായ്പാപരിധി നിശ്ചയിക്കുന്നു. കടം കൊടുക്കുന്നവർ സാധാരണയായി വായ്പാപരിധി നിശ്ചയിക്കുന്നത് അപേക്ഷകൻ നൽകുന്ന വിവരങ്ങളെ അടിസ്ഥാനമാക്കിയാണ്. ഉപഭോക്താക്കളുടെ ക്രെഡിറ്റ് സ്കോറുകളെ ബാധിക്കുന്ന ഒരു ഘടകമാണ് വായ്പാപരിധി. ഭാവിയിൽ വായ്പ നേടാനുള്ള അവരുടെ കഴിവിനെ ഇത് ബാധിക്കും.

CVV – കാർഡ് സ്ഥിരീകരണ മൂല്യത്തെ സൂചിപ്പിക്കുന്നു. ഇത് കാർഡിനു പുറകിൽ അച്ചടിച്ചിരിക്കുന്ന മൂന്നക്ക നമ്പർ ആണ്. ഓൺലൈൻ ഇടപാടുകൾ പൂർത്തിയാക്കുന്നതിന് ഈ നമ്പർ അത്യന്താപേക്ഷിതമാണ്. അത് ഒരിക്കലും ആരുമായും പങ്കിടരുത്.

ഡെബിറ്റ് കാർഡുകൾ (Debit Cards): സാധനങ്ങൾ വാങ്ങുമ്പോൾ ആ വ്യക്തിയുടെ ബാങ്ക് അക്കൗണ്ടിൽ നിന്നും കിഴിവ് വരുത്തി പണം നൽകുവാൻ അനുവദിക്കുന്ന കാർഡുകൾ.

ഇ–കൊമേഴ്സ് പ്ലാറ്റ് ഫോം (E-commerce Platform): ഉൽപ്പന്നങ്ങളും സേവനങ്ങളും (ഡിജിറ്റൽ ഉൽപ്പന്നങ്ങൾ ഉൾപ്പെടെ) ഡിജിറ്റൽ, ഇലക്ട്രോണിക് ശൃംഖലകളിൽ കൂടി വാങ്ങുവാനും വിൽക്കുവാനും സാധ്യമാക്കുന്ന പ്ലാറ്റ്ഫോം/വെബ്സൈറ്റ്.

ഇ എം ഐ (EMI) (തുല്യ പ്രതിമാസ തവണകൾ): ലഭിച്ച വായ്പ പലിശ സഹിതം തീർത്ത് അടയ്ക്കുന്നത് വരെ മാസം തോറും മുതലും പലിശയുമായി നിശ്ചിത തുക വായ്പ എടുത്ത ആൾ വായ്പ നൽകിയവർക്ക് (ബാങ്ക്, NBFC) നല്കുന്നതിനെയാണ് EMI എന്ന് വിളിക്കുന്നത്.

എൻക്രിപ്ഷൻ (Encryption): രഹസ്യ സ്വഭാവം സൂക്ഷിക്കുന്നതിനായി പ്രോസസിംഗ് വിവരങ്ങൾ പരിവർത്തനം ചെയ്ത് ഇലക്ട്രോണിക് കോഡ് ആയി മാറ്റുന്ന പ്രക്രിയ.

കാലഹരണപ്പെടുന്ന തീയതി (Expiry date): ഒരു കാർഡ്, ഉടമ്പടി, സമ്മത പത്രം, പ്രമാണം എന്നിവയുടെ സാധുത കാലഹരണപ്പെടുന്ന തീയതി. കാലഹരണപ്പെടാത്ത കാർഡുകളിലൂടെ നടത്തുന്ന ഇടപാടുകൾക്ക് മാത്രമേ അംഗീകാരം ലഭിക്കൂ.

ഗേറ്റ്‌വേ(Gateway): നേരിട്ടുള്ള ഇടപെടലില്ലാതെ ഇടപാടുകൾ, ഉപഭോക്തൃ വിവരങ്ങൾ, അപകട സാധ്യത നിയന്ത്രണം എന്നീ സേവനങ്ങളുടെ വിവര ക്രമീകരണം നടത്തുന്നതിനുള്ള സാങ്കേതിക വിദ്യയുടെ അടിസ്ഥാന സൗകര്യങ്ങൾ നൽകുന്ന ഇടനിലക്കാരൻ. പണമിടപാടുകളിൽ ഉൾപ്പെടാതെ ഓൺലൈൻ പണം ഇടപാടുകളുടെ വിവര കൈകാര്യം സുഗമമാക്കുവാനുള്ള സാങ്കേതിക വിദ്യയുടെ അടിസ്ഥാന സൗകര്യങ്ങൾ നൽകുന്ന സ്ഥാപനമാണ് പേയ്മെന്റ് ഗേറ്റ്‌വേയ്സ് (Payment Gateways).

ഐ എം പീ എസ് (IMPS) : മൊബൈൽ ഫോണിൽ കൂടി (ഒരു പരിധി വരെ) കൈമാറ്റം ചെയ്യുകയും ഗുണഭോക്താവിന് തത്സമയം പണം നൽകുകയും ചെയ്യുന്ന (NPCI) എൻ പി സി ഐയുടെ ഉൽപ്പന്നമാണ് ഐ എം പി എസ്. സേവനങ്ങൾ.

നിങ്ങളുടെ ഉപഭോക്താവിനെ അറിയുക KYC: ഒരു സാമ്പത്തിക സ്ഥാപനം ഉപഭോക്താവിന്റെ അസ്തിത്വം, അനുയോജ്യത/അയാൾ കാരണം ഉണ്ടായേക്കാവുന്ന അപായ സാധ്യത എന്നിവ മനസ്സിലാക്കുവാനായി ഒരുകൂട്ടം രേഖകൾ, കൃത്യമായ ശ്രദ്ധയോടെ പരിശോധിക്കുന്ന പ്രക്രിയ.

മണി മ്യൂൾസ്: തട്ടിപ്പുകാരുടെ കൈവശമുള്ള മോഷ്ടിച്ച/നിയമവിരുദ്ധ മായി നേടിയ പണം നിരപരാധികളായ ഇരകളുടെ ബാങ്ക് അക്കൗണ്ടിൽ കൂടി വെളുപ്പിക്കുന്നു. ഈ നിരപരാധികളെ വിശേഷിപ്പിക്കുന്ന പദമാണ് മണി മ്യൂൾസ്.

മൾട്ടി–ലെവൽ മാർക്കറ്റിംഗ്: പങ്കെടുക്കുന്നവർക്ക് അവരുടെ വിൽപ്പന യിലും അവർ അംഗമായി ചേർക്കുന്നവരുടെ വിൽപ്പനയിലും കമ്മീഷൻ അഥവാ പ്രതിഫലം ലഭിക്കുന്ന വിധത്തിൽ ഒരു കമ്പനിയുടെ പേരിൽ സാധനങ്ങളോ സേവനങ്ങളോ വിൽക്കുന്ന രീതി.

നാഷണൽ ഓട്ടോമേറ്റഡ് ക്ലിയറിങ് ഹൗസ് (NACH): നാഷണൽ പേയ് മെന്റ് കോർപ്പറേഷൻ ഓഫ് ഇന്ത്യ (NPCI) പ്രവർത്തിപ്പിക്കുന്ന ഒരു കേന്ദ്രീ കൃത ഇലക്ട്രോണിക് ക്ലിയറിങ് സേവനം (ECS) ആണിത്.

നിയർ ഫീൽഡ് കമ്മ്യൂണിക്കേഷൻ (NFC) : ഒരു NFC സജ്ജീകരിച്ച മൊബൈൽ ഫോണിൽ നിന്ന് പ്രാപ്തിയുള്ള ഒരു ഉപകരണത്തിലേക്ക് ഇടപാട് വിവരങ്ങൾ കൈമാറാൻ ഉപയോഗിക്കുന്ന ഒരു ആശയവിനിമയ സാങ്കേതികവിദ്യ NFC ഘടിപ്പിച്ച യന്ത്രത്തിനടുത്ത് സ്മാർട്ഫോൺ/ കാർഡ് കാണിച്ചാൽ കാർഡിന്റെ സ്പർശനമില്ലാതെ പണംകൊടുക്കൽ സാദ്ധ്യമാകും.

എൻ ഇ എഫ് ടി (NEFT): RBI യുടെ ഉടമസ്ഥതയിലുള്ളതും RBI പ്രവർ ത്തിപ്പിക്കുന്നതുമായ ദേശവ്യാപകവും കേന്ദ്രീകൃതവുമായ പണമിടപ ാട് വ്യവസ്ഥയാണ് (System) എൻ ഇ എഫ് ടി. ഭാരതത്തിലെ ബാങ്ക് ഉപഭോക്താക്കൾക്ക് എൻ ഇ എഫ് ടി സജ്ജമായ രണ്ടു ബാങ്ക് അക്കൗ ണ്ടുകളിൽ പരസ്പരം പണം കൈമാറ്റം ചെയ്യാവുന്നതാണ്.

വൺ ടൈം പാസ്‌വേഡ് (ഒ ടി പി) (OTP): നിങ്ങളുടെ ഓൺലൈൻ ഇടപാടു കൾക്കുള്ള ദ്വിഘടക സാധൂകരണത്തിൽ ഉൾപ്പെടുന്ന അധിക സുരക്ഷാ നടപടിയാണ് ഒ ടി പി അല്ലെങ്കിൽ വൺ ടൈം പാസ്‌വേഡ്. ഇത് രഹ സ്യമായി സൂക്ഷിക്കേണ്ടതാണ്. മറ്റാരുമായും പങ്കുവയ്ക്കരുത്.

ഫിഷിംഗ് (Phishing) – ഉപഭോക്താക്കളെ വഞ്ചിക്കുന്നതിനു വേണ്ടി തങ്ങ ളുടെ ബാങ്കിൽ നിന്നോ ഇ–വാലറ്റ് ദാതാക്കളിൽ നിന്നോ അയച്ചതാ ണെന്ന് തോന്നിപ്പിക്കുന്ന രീതിയിലുള്ള വ്യാജ ഇ–മെയിൽ. ഇതിൽ രഹസ്യ വിവരങ്ങൾ ചോർത്തുന്നതിനുള്ള ലിങ്ക് ഉണ്ടാകും.

പോയിന്റ് ഓഫ് സെയിൽ (POS) / അക്സപ്റ്റൻസ് ഡിവൈസ് (mPOS): കാർഡ് വഴിയുള്ള (ക്രെഡിറ്റ് കാർഡ്, ഡെബിറ്റ് കാർഡ്,ഗിഫ്റ്റ് കാർഡ് മുതലായവ) പണം സ്വീകരിക്കാൻ വ്യാപാരികളെ പ്രാപ്തരാക്കുന്ന വ്യാപാര സ്ഥാപനങ്ങളിൽ സ്ഥാപിച്ചിട്ടുള്ള QR code ഉപകരണങ്ങൾ.