

# STATE LEVEL BANKERS' COMMITTEE, KERALA

(Under Lead Bank Scheme of RBI )

Convenor:



Ref: Kerala SLBC/129FLC/52/GN/2018

Date: 2018 May 29<sup>th</sup>

ഡിജിറ്റൽ ബാങ്കിംഗ് തട്ടിപ്പിനിരയായാൽ എന്ത് ചെയ്യണം ?  
ഒരു അംഗീകൃത നടപടി ക്രമം (A standard operating procedure )

ആമുഖം

ഡിജിറ്റൽ ബാങ്കിങ്ങിന്റെ യുഗമാണിത്. എ ടി എം, ഡെബിറ്റ് കാർഡ്, ക്രെഡിറ്റ് കാർഡ്, ഇന്റർനെറ്റ് ബാങ്കിംഗ്, മൊബൈൽ ബാങ്കിംഗ് , ഇ-വലറ്റ് തുടങ്ങിയവയിൽ ഏതെങ്കിലും ഒരു ഡിജിറ്റൽ മാധ്യമം ഉപയോഗിക്കാത്ത ബാങ്ക് ഇടപാടുകാർ ചുരുക്കമായിരിക്കും

ഡിജിറ്റൽ ബാങ്കിംഗ് പൊതുവേ സുരക്ഷിതമാണ്. തട്ടിപ്പ് തടയുവാൻ വേണ്ട മുൻകരുതലുകൾ എന്തൊക്കെയാണെന്ന് വിവരിക്കുന്ന ലേഖനങ്ങളും അറിയിപ്പുകളും ഇന്ന് വിവിധ മാധ്യമങ്ങളിൽ ലഭ്യമാണ്. അവ പാലിച്ചാൽ ഡിജിറ്റൽ സുരക്ഷ ഉറപ്പാക്കാൻ സാധിക്കുകയും ചെയ്യും

എന്നാൽ അപൂർവമായെങ്കിലും തട്ടിപ്പുകാർ നമ്മുടെ ഈ മുൻകരുതലുകളൊക്കെ മറി കടന്ന് നമ്മുടെ പണം അപഹരിക്കാറുണ്ട് . അത് സൈബർജാലകം വഴി വിദൂരത്ത് നിന്നാകാം. അല്ലെങ്കിൽ ATM കാർഡ്, മൊബൈൽ, ഫോൺ തുടങ്ങിയ ഉപകരണങ്ങൾ കൈവശപ്പെടുത്തി നമ്മുടെ കൺവെട്ടത്തു വച്ചും ആകാം. അങ്ങിനെ ഒരു നിർഭാഗ്യം ആർക്കെങ്കിലും സംഭവിച്ചാൽ പിന്നെ എന്താണ് ചെയ്യേണ്ടത് എന്ന് മലയാള ഭാഷയിൽ വിവരിക്കുന്ന പ്രസിദ്ധീകരണങ്ങൾ കുറവാണ്.

തട്ടിപ്പിന് ഇരയാകുന്ന പലരും അജ്ഞത കൊണ്ട് തുടർനടപടികൾ എടുക്കതെയിരിക്കുന്നു. അല്ലെങ്കിൽ അതിനു കാല താമസം വരുത്തുന്നു. ഇതിനാൽ ഇരയാകുന്ന വ്യക്തിയുടെ പണം നഷ്ടപ്പെടുന്നതു മാത്രമല്ല, തട്ടിപ്പുകാർക്ക് യഥേഷ്ടം മറ്റു പലരെയും പറ്റിക്കുവാനും സാധിക്കുന്നു . ചിലപ്പോൾ ഇതേ വ്യക്തി തന്നെ അവരുടെ അടുത്ത തട്ടിപ്പിന് ഇരയാകുന്ന സാഹചര്യവും ഉണ്ടായിട്ടുണ്ട്

ഈ അറിവിന്റെ അപര്യാപ്തത (knowledge gap) പൊതു ജനങ്ങൾക്കിടയിൽ മാത്രമല്ല ധനകാര്യ സ്ഥാപനങ്ങളിൽ പോലുമുണ്ട് എന്നതാണ് സത്യം . അത് പരിഹരിക്കുന്നതിനാണ് ഭാരതീയ റിസർവ് ബാങ്കിന്റെ നിർദ്ദേശാനുസരണം, കേരള സംസ്ഥാന തല ബാങ്കേഴ്സ് സമിതി (SLBC KERALA ) ഈ അംഗീകൃത നടപടി ക്രമം (Standard operating procedure ) പ്രസിദ്ധീകരിക്കുന്നത്

സമയമാണ് പ്രധാനം

തട്ടിപ്പോ അതിനുള്ള സാധ്യതയോ ശ്രദ്ധയിൽപെട്ടാൽ എത്രയും പെട്ടെന്ന് പ്രതികരിക്കുകയാണ് ധന നഷ്ടം തടയുവാൻ അല്ലെങ്കിൽ കുറയ്ക്കുവാൻ പ്രധാനം

അപ്രകാരം ഉടനടി ചെയ്യേണ്ടതായ കാര്യങ്ങൾ നാലു വിഭാഗങ്ങളായി തിരിക്കാം

1. ഉപയോഗിക്കുന്ന ആപ്പ്ളിക്കേഷൻ ബ്ലോക്ക് ചെയ്യുക

**Disclaimer:** While SLBC had taken every effort to furnish up-to-date and accurate information, general public should be aware that SLBC accepts no responsibility for the accuracy or completeness of the aspects mentioned herein and recommends that general public exercise their own care and judgment with respect to its use.

2. ബാങ്കിൽ വിവരം അറിയിക്കുക
3. പോലീസ് സൈബർസെല്ലിൽ വിവരം അറിയിക്കുക
4. പോലീസ് കേസ് രജിസ്റ്റർ ചെയ്യുക

1. ഉപയോഗിക്കുന്ന ആപ്ലിക്കേഷൻ ബ്ലോക്ക് ചെയ്യുക

- മൊബൈൽ അലേർട്ട് ഉള്ള അക്കൗണ്ട് ആണെങ്കിൽ പണം പിൻവലിക്കപ്പെട്ടതായോ, ക്രെഡിറ്റ് കാർഡ് / വലറ്റ് വഴി വ്യാപാരം നടന്നതായോ എസ് എം എസ് അലേർട്ട് വരുമ്പോഴാണ് പണം നഷ്ടപ്പെട്ട വിവരം സാധാരണയായി അക്കൗണ്ട് ഉടമ അറിയുക
- ഈ ഇടപാട് അനധികൃതമാണെന്ന് ഉറപ്പാണെങ്കിൽ, ആ എസ് എം എസ് സന്ദേശം നിങ്ങളുടെ ഫോണിൽ സേവ് ചെയ്യുക
- നിങ്ങളുടെ ഡെബിറ്റ് / ക്രെഡിറ്റ് കാർഡ് ലോക്ക് ചെയ്യുവാനുള്ള അപ്ലിക്കേഷനിൽ നിങ്ങൾ രജിസ്റ്റർ ചെയ്തിട്ടുണ്ടെങ്കിൽ ഉടൻ തന്നെ അതുപയോഗിച്ച് കാർഡ് ലോക്ക് ചെയ്യുക
- നെറ്റ് ബാങ്കിംഗ് / മൊബൈൽ ബാങ്കിംഗ് തുടങ്ങിയ ഏതെങ്കിലും അപ്ലിക്കേഷനിൽ ലോഗിൻ ചെയ്തിട്ടുണ്ടെങ്കിൽ ഉടൻ തന്നെ ലോഗ് ഔട്ട് ചെയ്യുക
- തുടർന്ന് ഏതു ഡിവൈസ് വഴിയാണോ നിങ്ങൾ ഇന്റർനെറ്റിൽ പ്രവേശിച്ചിട്ടുള്ളത് , ആ ഉപകരണം ഓഫ് ലൈൻ ആക്കുക (ഇന്റർനെറ്റിൽനിന്ന് പുറത്തു വരിക)
- അതിനു ശേഷം ആ ഡിവൈസ് റീ ബൂട്ട് ചെയ്തു വീണ്ടും ഇന്റർനെറ്റ് ഓൺലൈൻ ആയി , അതെ അപ്ലിക്കേഷനിൽ ലോഗിൻ ചെയ്ത് നിങ്ങളുടെ പാസ് വേർഡ് റീ സെറ്റ് ചെയ്യുക .
- അതേപോലെ , പാസ് വേർഡ് മറന്നു പോയാൽ റീ സെറ്റ് ചെയ്യാൻ നൽകിയിട്ടുള്ള സെക്യൂരിറ്റി ചോദ്യവും റീ സെറ്റ് ചെയ്യണം
- ഏതെങ്കിലും വെബ് സൈറ്റിൽ കയറുമ്പോൾ , ഇതേപോലെ സംശയാ സ്ഫുരമായ പ്രതികരണം ഉണ്ടായാലും , ആ സൈറ്റിൽനിന്ന് പുറത്ത് വന്ന് മേൽപറഞ്ഞതു പോലെ പാസ് വേർഡും സെക്യൂരിറ്റി ചോദ്യവും റീ സെറ്റ് ചെയ്യുക
- നിങ്ങളുടെ അടുത്ത് അതേ ബാങ്കിന്റെ ATM ഉണ്ടെങ്കിൽ അവിടെ നിന്ന് കാർഡിന്റെ PIN റെസ്റ്റ് ചെയ്യുക

2. ബാങ്കിൽ വിവരം അറിയിക്കുക

- മേൽപറഞ്ഞ കാര്യങ്ങൾ ചെയ്യുന്നതിനൊപ്പം തന്നെ , ബാങ്കിന്റെ ടോൾ ഫ്രീ നമ്പരിലോ , IVRS-ലോ വെബ് സൈറ്റ് വഴിയോ , ഇ-മെയിൽ വഴിയോ , ബാങ്കിന്റെ ശാഖയിലെ ഫോണിൽ വിളിച്ചോ , നേരിട്ട് ചെന്നോ നിങ്ങളുടെ കാർഡ് ബ്ലോക്ക് ചെയ്യണം (ഇതു വളരെ പ്രധാനമാണ്)
- ഏറ്റവും അടുത്ത പ്രവൃത്തി ദിവസം , നിങ്ങളുടെ ബാങ്ക് ശാഖ സന്ദർശിച്ച് രേഖാ മൂലം പരാതി സമർപ്പിക്കുക (ഇതും വളരെ പ്രധാനമാണ്)
- പഴയ കാർഡ് മാറി പുതിയ കാർഡ് വാങ്ങുക
- ഇന്റർനെറ്റ് ബാങ്കിംഗ് / മൊബൈൽ ബാങ്കിംഗ് പാസ് വേർഡ് മാറിയിട്ടുണ്ടെന്ന് ഉറപ്പാക്കുക

3. പോലീസ് സൈബർസെല്ലിൽ വിവരം അറിയിക്കുക

- കേരളത്തിലെ സ്ഥിര താമസക്കാരനാണ് നിങ്ങളെങ്കിൽ, മേൽപറഞ്ഞ രീതിയിൽ തട്ടിപ്പിന് ഇരയായാൽ കേരള പോലീസിന്റെ സൈബർസെല്ലിൽ എത്രയും പെട്ടെന്ന് വിവരം അറിയിക്കണം. താങ്കൾ താമസിക്കുന്ന ജില്ലയിലെ ജില്ലാ സൈബർ സെല്ലിലാണ് പരാതിപ്പെടെണ്ടത്

**Disclaimer:** While SLBC had taken every effort to furnish up-to-date and accurate information, general public should be aware that SLBC accepts no responsibility for the accuracy or completeness of the aspects mentioned herein and recommends that general public exercise their own care and judgment with respect to its use.

- സംഭവം നടന്ന രണ്ടു മണിക്കൂറിനകം അറിയിക്കുന്ന പക്ഷം, ആ ഇടപാട് ബ്ലോക്ക് ചെയ്യിക്കുവാനും തുക തിരിച്ചു കിട്ടുവാനുള്ള സാധ്യതയുണ്ട്
- താമസിക്കും തോറും ആ സാധ്യത കുറഞ്ഞു വരും
- ബാങ്കിന്റെ പേര്, ഡെബിറ്റ്/ക്രെഡിറ്റ് കാർഡ് നമ്പർ, അക്കൗണ്ട് നമ്പർ, നഷ്ടപ്പെട്ട തുക , സംഭവം നടന്ന സമയം എന്നിവ അത്യവശ്യമാണ്, transaction id യും ഉണ്ടെങ്കിൽ നന്ന്
- താഴെ കൊടുത്തിരിക്കുന്ന ഇമെയിൽ/ ഫോൺ നമ്പർവഴി വിവരം നൽകിയാൽ മതിയാകും, (ഇ-മെയിൽ ആണ് അനുയോജ്യം). ഫോൺ നമ്പരും ഇ-മെയിൽ അഡ്രസ്സും, മേൽവിലാസവും നല്ലാൻ മറക്കരുത്

	യൂണിറ്റ്	ലാൻഡ് ഫോൺ	മൊബൈൽ	ഇ-മെയിൽ
1	തിരുവനന്തപുരം സിറ്റി	0471 2329107, 1090	9497975998	cybercelltvmcity@keralapolice.gov.in
2	തിരുവനന്തപുരം റൂറൽ	0471 2435066, 2303066		cybercelltvmrl@keralapolice.gov.in
3	കൊല്ലം സിറ്റി		9497960777	cybercellklmcity@keralapolice.gov.in
4	കൊല്ലം റൂറൽ	04742450168	9495434040, 9495207362	cybercellklmrl@keralapolice.gov.in
5	പത്തനംതിട്ട	0468 2327914	9497961078, 9497976001	cybercellpta@keralapolice.gov.in
6	ആലപ്പുഴ	0477 2230804	9497981288	cybercellalpy@keralapolice.gov.in
7	കോട്ടയം	0481 2561304	9497976002	cybercellktm@keralapolice.gov.in
8	ഇടുക്കി	0486 2232354	9497976003	cybercellidk@keralapolice.gov.in
9	കൊച്ചി സിറ്റി	0484 2382600	9497976004	cybercellekmcity@keralapolice.gov.in
10	എറണാകുളം റൂറൽ	0484 2630238	9497976005	cybercellekmrl@keralapolice.gov.in
11	തൃശ്ശൂർ സിറ്റി		9497962836	cybercelltsrcity@keralapolice.gov.in
12	തൃശ്ശൂർ റൂറൽ		9497976006	cybercelltsrri@keralapolice.gov.in
13	പാലക്കാട്		9497976007	cybercellpkd@keralapolice.gov.in
14	മലപ്പുറം	0483 2738660	9497976008	cybercellmpm@keralapolice.gov.in
15	കോഴിക്കോട് സിറ്റി	0495 2720090	9497976009	cybercellkkdcity@keralapolice.gov.in
16	കോഴിക്കോട് റൂറൽ	0496 2523091	9497976010, 9497976043	cybercellkkdri@keralapolice.gov.in
17	വയനാട്	04936 202525	9497976011, 9497976045	cybercellwynd@keralapolice.gov.in
18	കണ്ണൂർ	0497 2763332, 2763330,	9497976012	cybercellknr@keralapolice.gov.in

**Disclaimer:** While SLBC had taken every effort to furnish up-to-date and accurate information, general public should be aware that SLBC accepts no responsibility for the accuracy or completeness of the aspects mentioned herein and recommends that general public exercise their own care and judgment with respect to its use.

**4. പോലീസ് കേസ് രജിസ്റ്റർ ചെയ്യുക**

- ബാങ്കി നിയമ നടപടികൾക്ക് പോലീസ് കേസ് കൂടി രജിസ്റ്റർ ചെയ്യണം
- നിങ്ങളുടെ താമസ സ്ഥലത്തിന്റെ പരിധിയിലെ പോലീസ് സ്റ്റേഷനിൽ ആണ് കംപ്ലൈന്റ് രജിസ്റ്റർ ചെയ്യേണ്ടത്
- കേരള പോലീസിന് ഓൺ ലൈൻ ആയി പരാതി സ്വീകരിക്കുവാനും സജ്ജീകരണമുണ്ട് (<http://thuna.keralapolice.gov.in>)
- സൈബർ സെല്ലിൽ പരാതി കൊടുക്കുന്നതും, പോലീസ് സ്റ്റേഷനിൽ പരാതി നൽകുന്നതും രണ്ടു വ്യത്യസ്ത നടപടികളാണ്. അത് രണ്ടും ചെയ്യുക

**അക്കൗണ്ട് ഉടമയുടെ ബാധ്യത**

ഇലക്ട്രോണിക് ബാങ്ക് തട്ടിപ്പുകളിൽ, അക്കൗണ്ട് ഉടമയുടെ ബാധ്യതയ്ക്ക്, റിസർവ് ബാങ്ക് നിശ്ചയിച്ചിട്ടുള്ള പരിധികൾ (Ref RBI Cir No 2017-18/15 DBR. No. Leg. BC. 78/09.07.005/ 2017-18 July 6, 2017)

നം:	ഇനം	അക്കൗണ്ട് ഉടമയുടെ ബാധ്യത *
1	ബാങ്കിന്റെ ഭാഗത്തു നിന്നുള്ള പോരായ്മ/തെറ്റ് കൊണ്ടാണ് തട്ടിപ്പിന് അവസരം ഉണ്ടായതെങ്കിൽ	ബാധ്യതയില്ല
2	ബാങ്കിന്റേയോ അക്കൗണ്ട് ഉടമയുടേയോ ഭാഗത്തെ തെറ്റ് കൊണ്ടല്ല മറിച്ച് പൊതു സമ്പ്രദായത്തിൻറെ ന്യൂനത കൊണ്ടാണ് തട്ടിപ്പിന് അവസരം ഉണ്ടായതെങ്കിൽ	
2 എ	ഇടപാടിനെപ്പറ്റി ബാങ്കിൽ നിന്ന് SMS അലേർട്ട് കിട്ടി മൂന്നു ബാങ്കു പ്രവൃത്തി ദിനങ്ങൾക്കകം ഇടപാടിൽ തട്ടിപ്പുണ്ടെന്ന് ബാങ്കിനെ അറിയിച്ചാൽ	ബാധ്യതയില്ല
2 ബി	തട്ടിപ്പ് നടന്നെന്ന് ബാങ്കിനെ അറിയിക്കുന്നത് SMS അലേർട്ട് കിട്ടി നാലു മുതൽ ഏഴു ദിവസത്തിനുള്ളിൽ ആണെങ്കിൽ	രൂ 5000 മുതൽ 25000 വരെ (അക്കൗണ്ടിന്റെ ഘടന /കാർഡിന്റെ പരിധി അനുസരിച്ച്)
2 സി	തട്ടിപ്പ് നടന്നെന്ന് ബാങ്കിനെ അറിയിക്കുന്നത് SMS അലേർട്ട് കിട്ടി ഏഴു ദിവസം കഴിഞ്ഞ് ആണെങ്കിൽ	അതതു ബാങ്കിന്റെ നിയമം അനുസരിച്ച്
3.	അക്കൗണ്ട് ഉടമയുടെ ഭാഗത്തെ വീഴ്ച കൊണ്ടാണ് തട്ടിപ്പിന് അവസരം ഉണ്ടായതെങ്കിൽ	തട്ടിപ്പിനെ പറ്റി ബാങ്കിൽ അറിയിക്കുന്നത് വരെയുള്ള ബാധ്യതകൾ അക്കൗണ്ട് ഉടമ വഹിക്കണം. അതിനു ശേഷം ഈ ഇടപാട് മൂലം ഉണ്ടാകുന്ന ബാധ്യത ബാങ്ക് വഹിക്കും

- ഈ പരിധി ആനുകൂല്യം SMS അലേർട്ടിനായി മൊബൈൽ നമ്പർ ബാങ്കിൽ രജിസ്റ്റർ ചെയ്ത അക്കൗണ്ടുകൾക്ക് മാത്രമേ ലഭിക്കൂ

**Disclaimer:** While SLBC had taken every effort to furnish up-to-date and accurate information, general public should be aware that SLBC accepts no responsibility for the accuracy or completeness of the aspects mentioned herein and recommends that general public exercise their own care and judgment with respect to its use.