સાવધાન

નાણાકીય છેતરપિંડી કરનારાઓની કાર્યપ્રણાલી વિશેની બુકલેટ
આરબીઆઇ ઓમ્બડ્સમેન કાર્યાલય (મુંબઈ-2)
મહારાષ્ટ્ર અને ગોવા

વિષયોની માહિતી

પ્રસ્તાવના
હાલનાં વર્ષોમાં ડિજિટલ માધ્યમે ચુકવણી કરવાનું પ્રમાણ વધ્યું છે. ડિજિટલ ચુકવણીથી ગ્રાહકોને સરળતા થવા ઉપરાંત ગ્રાહકોને સુવિધા ઉપલબ્ધ થવાની સાથે નાણાકીય સર્વસમાવેશના રાષ્ટ્રીય લક્ષ્યાંક સિધ્ધ કરવાના ક્ષેત્રે પણ મોટું યોગદાન પ્રાપ્ત થયું છે. નાણાકીય વ્યવહારોમાં સરળતા વધવાની સાથે રિટેલ ફાઇનાન્સિયલ ટ્રાન્ઝેકશન્સમાં કૌભાંડ પણ વધ્યાં છે. ગુનેગારો સામાન્ય અને ભોળા નાગરિકો, ખાસ કરીને ટેકનોફાઇનાન્સિયલથી વધુ અવગત ના હોય તેવા લોકોના મહેનતથી કમાયેલા પૈસાને ચોરવા માટે નિતનવી પ્રણાલીનો ઉપયોગ કરી રહ્યા છે.

આ બુકલેટમાં બને તેટલી વાસ્તવિક માહિતી પ્રદાન કરવામાં આવી છે, જે નાણાકીય ટ્રાન્ઝેક્શન્સમાં બિનઅનુભવી હોય તેમના માટે છે. આમાં ઘટનાઓની માહિતી ઉપરાંત વિવિધ સ્રોતથી માહિતી એકત્ર કરવામાં આવી છે. બૅન્કિંગ ઓમ્બડ્સમેનની ઓફિસમાં જે ફરિયાદો આવી છે તેના આધારે માહિતીનું સંકલન કરવામાં આવ્યું છે. આ પુસ્તિકાના માધ્યમથી લોકોમાં જાગૃતિ ફેલાવવાનો પ્રયત્ન કરવામાં આવી રહ્યો છે, જેથી તેમને સમજાય કે ગુનેગારો કઇ રીતે છેતરપિંડી કરે છે. વ્યક્તિ પોતાની અંગત માહિતી સુરક્ષિત રાખે, અજાણ્યા ફોન/ઈમેઇલ્સથી સાવચેત રહે, નાણાકીય ટ્રાન્ઝેકશન્સ વ્યવસ્થિત કરે અને પોતાના ક્રેડેન્શિયલ્સ/પાસવર્ડસ સુરક્ષિત રાખે એ જ આ પુસ્તિકાનો હેતુ છે. એટલે જ બુકલેટનું શીર્ષક બીવેર છે બી અવેર અને બીવેર!

આ ઓફિસ દ્વારા લોકોમાં જાગૃતિ ફેલાવવાની પહેલના ભાગરૂપ આ પુસ્તિકા છે.

છેતરપિંડીવાળા ટ્રાન્ઝેકશન્સની કાર્યપ્રણાલી અને સાવચેતી – બૅન્કો

1.ફિશિંગ લિન્ક્સ

કાર્યપ્રણાલી

- ગુનેગારો થર્ડપાર્ટી વેબસાઇટ બનાવે છે જે ખરી વેબસાઇટ જેવી જ દેખાય છે, જેમ કે બૅન્કની વેબસાઈટ અથવા ઇકોમર્સ વેબસાઇટ અથવા સર્ચ એન્જિન વગેરે.
- ગુનેગારો એસએમએસ/સોશિયલ મીડિયા/ઈમેલ/ત્વરિત મેસેન્જરના માધ્યમથી આ લિન્ક ફેલાવે છે.
- મોટા ભાગે ગ્રાહકો યુઆરએલને ધ્યાનથી તપાસ્યા વિના પોતાના ક્રેડેન્શિયલ ટાઇપ કરે છે.
- લિન્ક ખરી વેબસાઇટ જેવી જ દેખાય છે પરંતુ વાસ્તવિકમાં ગ્રાહકો ફિશિંગ વેબસાઇટના ભરડામાં આવે છે.
- જ્યારે ગ્રાહક પોતાના ક્રેડેન્શિયલ એન્ટર કરે ત્યારે આ માહિતી ગુનેગારો મેળવી લે છે અને તેનો દુરુપયોગ કરે છે.

સાવચેતી

- અજાણી લિન્ક ઉપર ક્લિક કરવું નહીં અને ભવિષ્યમાં સંપર્કની શક્યતા ન રહે તે માટે એસએમએસ/ઈમેઇલને ત્વરિત ડિલિટ કરી દેવા. નાણાકીય ક્રેડેન્શિયલ એન્ટર કરવા પડે તેવી વેબસાઇટને પહેલાં ચકાસવી કે તે ખરી છે કે નહીં.

2. બનાવટી કોલ્સ

કાર્યપ્રણાલી

- સોશિયલ મીડિયામાં બૅન્કર્સ/કંપની કર્મચારી/વિમા એજન્ટ/સરકારી અધિકારી વગેરેના નામે ગ્રાહકોનો ટેલિફોન સંપર્ક કરી ક્રેડેન્શિયલ માગવા પહેલાં નામ અથવા જન્મતારીખ પૂછવામાં આવે છે, જેથી ગ્રાહકને એક વિશ્વાસ આવે.
- અમુક કેસોમાં ગુનેગારો ચાલાકી વાપરીને ગ્રાહકો ઉપર દબાણ કરે છે કે તેઓ ત્વરિત પોતાની માહિતી આપે, જેથી ટ્રાન્ઝેક્શન બ્લોક થઇ શકે અથવા દંડથી બચી શકાય, ડિસ્કાઉન્ટ મળે વગેરે કહેવામાં આવે છે. ક્રેડેન્શિયલ મેળવ્યા બાદ કૌભાંડ કરવામાં આવે છે.

સાવચેતી

- બૅન્ક અધિકારીઓ/નાણાકીય સંસ્થાઓ/અન્ય પ્રતિષ્ઠિત કંપનીઓ ક્યારે પણ ગ્રાહકો પાસે તેમની અંગત માહિતી જેવી કે યુઝરનેમ/પાસવર્ડ/કાર્ડની વિગતો/સીવીવી/ ઓટીપી માગતા નથી.

3. ઓનલાઇન સેલિંગ પ્લેટફોર્મ્સના માધ્યમે છેતરપિંડી

કાર્યપ્રણાલી

- ઓનલાઇન સેલિંગ પ્લેટફોર્મ્સમાં ગુનેગારો પોતાને ખરીદદાર બતાવીને તમારા પ્રોડક્ટમાં રસ દર્શાવે છે.
- તમને નાણાં ચૂકવવાની બદલે તેઓ 'રિકવેસ્ટ મની'નો વિકલ્પ યુપીઆઇ એપમાં કરે છે અને આ રિકવેસ્ટ મંજૂર કરવા માટે આજીજી કરે છે જેથી તેઓ તમારા બૅન્ક ખાતામાંથી નાણાં ખેંચી શકે.

સાવચેતી

- ઓનલાઇન પ્રોડક્ટ્સમાં નાણાકીય ટ્રાન્ઝેક્શન કરતા સમયે સાવચેતી રાખવી.
- હંમેશા યાદ રાખો કે નાણાં મેળવતી વખતે તમારે ક્યાંય પણ પીન/પાસવર્ડ એન્ટર કરવાની જરૂર નથી.
- જો યુપીઆઇ કે અન્ય કોઇ પણ એપ તમને ટ્રાન્ઝેક્શન પૂરો કરવા માટે પીન એન્ટર કરવાનું કહે તો તમને નાણાં મળશે નહીં પરંતુ તમે નાણાં મોકલશો.

4. અજાણી/વેરિફાઇ કર્યા વિનાની મોબાઇલ એપ્સમાં છેતરપિંડી

કાર્યપ્રણાલી

- તમે કોઇ અજાણી/વેરિફાઇડ વિનાની મોબાઇલ એપ્સ ડાઉનલોડ કરો તે પછી ગુનેગારો તમારા મોબાઇલ ડિવાઇઝ/લેપટોપ/ડેસ્કટોપમાં એક્સેસ (સંપર્ક) મેળવશે.
- આવા પ્રકારની એપ્લિકેશનની લિન્ક્સ એસએમએસ/સોશિયલ મીડિયા/ત્વરિત મેસેન્જર વગેરેના માધ્યમે શેર કરવામાં આવે છે. લિન્કમાં તમને ખરાઇપણું લાગશે પરંતુ હકીકતમાં કોઇ અજાણી એપ્લિકેશન ડાઉનલોડ થશે.

- આવી ખોટી એપ્લિકેશન ડાઉનલોડ થયા બાદ ગુનેગારો તમારા ડિવાઇઝનો સંપૂર્ણ નિયંત્રણ ધરાવે છે.

સાવચેતી

- ક્યારે પણ વેરિફાઇડ વિનાની/અજાણ્યા સ્ત્રોતથી એપ્લિકેશન ડાઉનલોડ કરવી નહીં.

5. એટીએમ કાર્ડ સ્કિમિંગ

કાર્યપ્રણાલી

- ગુનેગારો એટીએમ મશીન્સમાં સ્કિમિંગ ડિવાઇસ મૂકીને કાર્ડની વિગતોની ચોરી કરે છે.
- ખોટા કીપેર્ડ, છુપાવેલા નાના/પીનહોલ કેમેરાથી પીન પણ મેળવી લે છે.
- ઘણી વખત ગુનેગારો ગ્રાહક બનીને અન્ય ગ્રાહકની બાજુમાં ઊભા રહીને પીન જોઇ લઈને બાદમાં એક્સેસ મેળવે છે.
- આ ડેટાનો ઉપયોગ ડુપ્લિકેટ કાર્ડ માટે વપરાય છે ત્યાર બાદ ગ્રાહકના ખાતામાંથી નાણાં ઉપાડી લેવાય છે.

સાવચેતી

- કાર્ડ એટીએમમાં નાખવા માટેની જગ્યા (ઇન્સરશન સ્લોટ) નજીક કોઇ વધારાનું ડિવાઇઝ છે કે નહીં તે તપાસો, તેમ જ એટીએમ મશીનના કીપેડમાં પણ કોઇ વધારાનું ડિવાઇઝ છે કે નહીં તે તપાસો.
- પીન એન્ટર કરતા સમયે કીપેડને ઢાંકો.
- અન્ય કોઇ વ્યક્તિ તમારી બાજુમાં ઊભી હોય ત્યારે પીન એન્ટર કરવો નહીં, તેમ જ તમારા કાર્ડની વિગતો કોઇની પણ સાથે શેર કરવી નહીં.

6. સ્ક્રિન શેરિંગ એપ/રિમોટ એક્સેસથી છેતરપિંડી

કાર્યપ્રણાલી

- ગુનેગારો તમને સ્ક્રીન શેરિંગ એપ ડાઉનલોડ કરવા માટે ફસાવશે જેથી તેઓ તમારા મોબાઇલ/લેપટોપનો એક્સેસ મેળવીને નાણાકીય ક્રેડેન્શિયલ જાણી શકે.
- ત્યાર બાદ ગુનેગારો ઇન્ટરનેટ બેન્કિંગ/ચુકવણી એપ દ્વારા ચુકવણી કરે છે.

સાવચેતી

- સ્ક્રિન શેરિંગ એપ ડાઉનલોડ ન કરો અથવા અજાણી વ્યક્તિ સાથે શેર સ્ક્રીન ફીચર સક્રિય ન કરો.

7. સિમ સ્વેપ/સિમ ક્લોનિંગ

કાર્યપ્રણાલી

- તમારા મોબાઇલ નંબરમાં મોટા ભાગના ખાતાની વિગતો અને પ્રમાણીકરણ હોવાથી ગુનેગારો તમારા સીમ કાર્ડનો એક્સેસ મેળવે છે અથવા ડુપ્લિકેટ સિમ કાર્ડ બનાવીને ઓટીપીનો ઉપયોગ કરીને ડિજિટલ ટ્રાન્ઝેકશન કરે છે.
- મોટા ભાગે ગુનેગારો ટેલિફોન/મોબાઇલ નેટવર્ક સ્ટાફ બનીને સિમ કાર્ડને થ્રીજીથી ફોરજીમાં મફતમાં અપગ્રેડેશન અથવા સિમ કાર્ડમાં વધુ લાભો આપવાના નામે ફોન કરે છે.

સાવચેતી

- સિમ કાર્ડને લગતા ક્રેડેન્શિયલ ક્યારે પણ શેર ન કરો.
- તમારા ફોનમાં મોબાઇલ નેટવર્ક ન દેખાય તો તરત જ શંકાશીલ બનવું અને સમય ન વેડફતાં મોબાઇલ ઓપરેટરનો સંપર્ક કરવો, જેથી ખબર પડે કે તમારુ ડુપ્લિકેટ સિમ બન્યુ છે કે નહીં.

8. સર્ચ એન્જિનમાંથી ક્રેડેન્શિયલ મેળવીને છેતરપિંડી

કાર્યપ્રણાલી

- ગ્રાહકો બૅન્કો, વિમા કંપનીઓ, આધાર કાર્ડ કેન્દ્રો વગેરેની વિગતો મેળવવા માટે સર્ચ એન્જિનનો ઉપયોગ કરતા હોય છે અને ઘણી વાર સર્ચ એન્જિનમાં તેઓ અજાણ્યા કોન્ટેક્ટ/વેરિફાઇડ કર્યા વિનાના કોન્ટેક્ટ નંબરોનો સંપર્ક કરે છે.
- સર્ચ એન્જિનમાં આ ખોટા નંબરો ગુનેગારોએ જ ગ્રાહકો સાથે છેતરપિંડી કરવા માટે રાખ્યા હોય છે.
- ગ્રાહકો આ નંબર પર ફોન કરતાં તેમની પાસેથી કાર્ડના ક્રેડેન્શિયલ/અન્ય વિગતો વેરિફિકેશન માટે માગવામાં આવે છે.
- ગ્રાહકો આ સંપર્કને સાચા સમજીને પોતાની અંગત નાણાકીય વિગતો વેરિફિકેશન માટે આપે છે.

સાવચેતી

- સર્ચ એન્જિનમાં કસ્ટમર કૅર કોન્ટેક્ટ વિગતો સર્ચ ન કરો, કારણ કે આમાં ગુનેગારો દ્વારા દાખલ કરાયેલા ખોટા નંબરો હોઈ શકે છે. હંમેશા બૅન્કો/કંપનીઓની અધિકૃત વેબસાઇટ્સમાંથી જ સંપર્ક કરવા માટેની માહિતી પ્રાપ્ત કરો.

9. ક્યુઆર કોડ સ્કેનના માધ્યમથી કૌભાંડ

- કાર્યપ્રણાલી
- ગુનેગારો વિવિધ બહાનાં અને યુક્તિથી પેમેન્ટ એપમાં ક્યુઆર કોડ વાપરવાનું કહે છે. પરિણામે ગુનેગારો ગ્રાહકોના ખાતામાંથી નાણાં ઉપાડી શકે છે.

સાવચેતી

- પેમેન્ટ્સ એપમાં ક્યુઆર કોડ્સ વાપરતી વખતે સાવચેતી રાખો. ક્યુઆર કોડ્સમાં ખાતાની વિગતો જોડાયેલી હોય છે જેથી યોક્કસ ખાતામાં નાણાં ટ્રાન્સફર થાય છે.

10. સોશિયલ મીડિયાના માધ્યમે નકલ કરવી

- કાર્યપ્રણાલી
- ગુનેગારો ફેસબુક અને ઇન્સ્ટાગ્રામ જેવા પ્રચલિત સોશિયલ મીડિયા પ્લેટફોર્મમાં બનાવટી અકાઉન્ટ બનાવે છે. ત્યાર બાદ તમારા મિત્રોને તબીબી સહાય કે અન્ય યુકવણી વગેરે માટે ત્વરિત નાણાંની જરૂર હોવાનું જણાવીને રૂપિયા મોકલવાની વિનંતી કરે છે. ગુનેગારો સમય જતા વિશ્વાસ જીતે છે અને ત્યાર બાદ અંગત માહિતીનો ઉપયોગ ખંડણી અને ધમકી માટે કરે છે.

સાવચેતી

- ઓનલાઇન અજાણી વ્યક્તિને ચુકવણી ન કરો.
- સોશિયલ મીડિયા પ્લેટફોર્મ્સમાં તમારી અંગત વિગતો જાહેર ન કરો.
- તમારો મિત્ર/સગાસંબંધી નાણાંની માગણી કરે તો તે વ્યક્તિને એક ફોન કરીને પહેલાં ખાતરી કરી લો.

11. જ્યુસ જેકિંગ

- કાર્યપ્રણાલી
- મોબાઈલના ચાર્જિંગ પોઈન્ટનો ઉપયોગ ફાઈલ્સ/ડેટા ટ્રાન્સફર કરવા માટે થઈ શકે છે.
- જ્યુસ જેકિંગ એક પ્રકારની સાયબર ચોરી છે, જેમાં તમારો મોબાઈલ અજાણી/વેરિફાઇડ વિનાના ચાર્જિંગ પોર્ટ્સમાં જોડાય ત્યારે અજાણી એપ/માલવેર ડાઉનલોડ થાય છે ત્યાર બાદ ગુનેગારો અંગત માહિતી, ઈમેઇલ, એસએમએસ, સેવ કરેલા પાસવર્ડનું નિયંત્રણ/એક્સેસ મેળવે છે.

સાવચેતી

- સાર્વજનિક/અજાણ્યા ચાર્જિંગ પોર્ટ્સ/કેબલ્સનો ઉપયોગ ટાળો.

12. લોટરી કૌભાંડ

કાર્યપ્રણાલી

- ગુનેગારો એવો ઈમેઇલ મોકલે છે કે ફોન કોલ કરે છે કે તમે મોટી લોટરી જીત્યા છો. જોકે, નાણાં પ્રાપ્ત કરવા તમારે અમારી વેબસાઈટ પર તમારા બેન્ક ખાતા / ક્રેડિટ કાર્ડ મારફતે તમારી ઓળખની પુષ્ટિ કરવી પડશે એમ જણાવી ડેટા હાંસલ કરવામાં આવે છે.
- કેટલાક કિસ્સાઓમાં, ષડયંત્રકારો લોટરીની રકમ કે પ્રોડક્ટની પ્રાપ્તિ માટે વેરાની એકસામટી ચુકવણી અથવા શિપિંગ ચાર્જીસ, પ્રોસેસિંગ ફી વગેરે ચુકવવાનું કહે છે.
- આ ચુકવવાની રકમ લોટરી કે ઈનામની રકમની તુલનાએ બહુ ઓછી હોવાથી લોકો ગુનેગારોની જાળમાં સપડાઇ જઇ ચુકવણી કરે છે.

સાવચેતી

- લોટરીના ફોન કોલ્સ કે ઈમેઇલ્સ માટે કોઇ ચુકવણી ન કરો કે તમારી કોઇ પણ સલામત વિગતો પૂરી ન પાડો.

13. ઓનલાઇન જોબ ફ્રોડ

કાર્યપ્રણાલી

- બનાવટી જોબ સર્ચ પોર્ટલ સર્જવામાં આવે અને જ્યારે શિકાર તેની બેન્ક ખાતા/ક્રેડિટ કાર્ડ/ડેબિટ કાર્ડની વિગતો આ વેબસાઇટ્સ પર રજિસ્ટ્રેશન માટે દાખલ કરે ત્યારે ખાતા સામે જોખમ ઊભું થાય છે.

- કેટલાક કિસ્સાઓમાં, ષડયંત્રકારો પોતાને પ્રતિષ્ઠિત કંપનીના અધિકારી તરીકે ઓળખાવે છે અને બનાવટી ઈન્ટરવ્યૂ લઈને પછી તમને પસંદ કરવામાં આવ્યા હોવાનું જણાવાય છે. આમાં શિકાર બનેલાને ફરજિયાત તાલીમ વગેરે બહાના હેઠળ ચુકવણી કરવા માટે પ્રેરવામાં આવે છે.

સાવચેતી

- હંમેશાં યાદ રાખો કે ખરેખર નોકરી ઓફર કરનારી સાચી કંપની કઈ નાણાં માગતી નથી.
- અજાણ્યા જોબ પોર્ટલ્સ પર કદી ચુકવણી ન કરો.

બનાવટી ટ્રાન્ઝેક્શન્સની કાર્યપ્રણાલી અને તેની સામે રાખવી જોઈતી સાવચેતીઓ એનબીએફસીઝ

પાર્ટ - બી નોનબેન્કિંગ ફાઈનાન્સિયલ કંપની

1. ગુનેગારો દ્વારા લોનને લંબાવવા માટેની વિજ્ઞાપનો

- ગુનેગારો ઘણા આકર્ષક નીચા વ્યાજદરે અંગત લોન ઓફર કરતી બનાવટી વિજ્ઞાપનો અથવા પુનઃ ચુકવણીના સરળ વિકલ્પો ધરાવતી અથવા સિક્યુરિટી વગેરે વિના લોન મેળવવા સંપર્ક કરવાનું ગ્રાહકોને કહેતી વિજ્ઞાપનો પ્રકાશિત કરે છે.
- ભોળા ગ્રાહકોનો વિશ્વાસ જીતવા અને તેમને ભરોસો બેસે એ માટે તેઓ એવા ઈમેઈલ આઈડી રાખે છે જેવા કે કોઈ જાણીતી /સાચી એનબીએફસીના સિનિયર અધિકારીઓના આઈડી હોય.
- જ્યારે ગ્રાહકો ગુનેગારો પાસે લોન માટે સંપર્ક કરે છે ત્યારે તેઓ વિવિધ આગોતરા ચાર્જીસ જેવા કે પ્રોસેસિંગ ફી, જીએસટી, ઈન્ટરસિટી ચાર્જ, એડવાન્સ ઈએમઆઈ, અનહોલ્ડ ચાર્જીસ વગેરેના નામે નાણાં પડાવે છે અને પછી લોનો આપ્યા વિના રફુચક્કર થઈ જાય છે.
- લોન્સ માટે સર્ચ કરતા હોય એવા ગ્રાહકોની નજરે પડવા માટે આ ઠગો સર્ચ એન્જિન્સમાં બનાવટી લિન્ક્સ સર્જે છે.

સાવચેતી

- એનબીએફસી/બેન્કર કદી પણ લોન અરજી પ્રોસેસ કરવા પૂર્વે કોઈ એડવાન્સ ફી માગતી નથી.
- બેન્ક્સ/એનબીએફસીઝ જે પ્રોસેસિંગ ફી ચાર્જ કરે છે એ લોનની રકમમાંથી બાદ કરવામાં આવે છે.
- ઓછા વ્યાજની ઓનલાઈન લોન્સ વગેરેની ઓફર સામે સાચા સ્રોતો મારફત ચકાસણી કર્યા વિના કોઈ ચુકવણી ન કરો કે તમારા ક્રેડેન્સિયલ્સ દાખલ ન કરો.

2. એસએમએસ/ઈમેઈલ/ઈન્સ્ટન્ટ મેસેજિંગ/કોલ સ્કેમ

- ઠગો ઈન્સ્ટન્ટ મેસેન્જર/એસએમએસ/સોશિયલ મીડિયામાં આકર્ષક લોન્સ ઉપલબ્ધ હોવાના સંદેશા પ્રસારિત કરે છે અને શેર કરેલા મોબાઈલ નંબર સાથે કોઈ જાણીતી

એનબીએફસીનો લોગો પ્રોફાઇલ પિક્ચર તરીકે વાપરે છે કે જેથી ગ્રાહકોને વિશ્વાસ આવે. આ ઠગો આધાર કાર્ડ /પેન કાર્ડ અને બનાવટી એનબીએફસી આઇડી કાર્ડ પણ શેર કરે છે.

- આવા જથ્થાબંધ સંદેશાઓ/એસએમએસ/ઇમેઇલ/લોન વાંછુઓને મોકલ્યા બાદ તેઓ લોકોને આડેધડ કોલ કરે છે અને બનાવટી સેન્કશન લેટર્સ, બનાવટી ચેક્સની કોપીઓ વગેરે શેર કરે છે અને વિવિધ ચાર્જીસ માગે છે. એક વાર શિકાર આ ચાર્જીસ ચૂકવી દે એટલે તેઓ નાણાં સાથે ગાયબ થઇ જાય છે. આવા કિસ્સામાં નાણાં પરત મળવાની શક્યતા બહુ ઓછી હોય છે.

સાવચેતી

- એસએમએસ/ઇમેઇલ અથવા પ્રમોશનલ એસએમએસ/ઇમેઇલ મારફત આવેલી લિન્ક્સને કદી ક્લિક ન કરો કે જવાબ ન આપો.
- લોકોએ ટેલિફોન/ઇમેઇલ્સ વગેરે મારફત મોકલેલી લોન ઓફર્સને કદી સાચી માનવી નહિ.
- આવી કોઇ પણ ઓફર સામે કોઇ ચુકવણી કદી ન કરો અથવા તમારી અંગત /નાણાકીય માહિતી ન આપો.

ઓટીપી આધારિત છેતરપિંડી

- આમાં ભોગગ્રસ્તને એનબીએફસીઝ હોવાનો ડોળ કરી ઠગો તરફથી લોન્સ કે ક્રેડિટ લિમિટ વધારવા માટેના એસએમએસ/ઇન્સ્ટન્ટ મેસેજીસ મળે છે, જેમાં કોઇ ઠગના મોબાઇલ પર સંપર્ક કરવાનું જણાવાયું હોય છે.
- જ્યારે કોઇ શિકાર એ નંબર પર ફોન કરે એટલે તેની પાસે ઠગો કેટલાંક ફોર્મ ભરાવે છે (ઓનલાઇન પણ) જેમાં નાણાકીય વિગતો ભરવાની હોય છે અને તેઓ ગ્રાહકને ઓટીપી કે પિન જણાવવા માટે સમજાવે છે. જો આ વિગતો આપવામાં આવે તો ગ્રાહક નાણાં ગુમાવે છે.

સાવચેતી

- કદી પણ ઓટીપી/પિન નંબર્સ/અંગત માહિતી વગેરે કોઇની પણ સાથે કોઇ પણ રૂપમાં શેર ન કરો.
- એસએમએસ/ઇમેઇલ્સને નિયમિત ચકાસતા રહો જેથી તમારી જાણ વિના કોઇ ઓટીપી જનરેટ કરવામાં ન આવે.

બનાવટી લોન્સ વેબસાઇટ્સ/એપ દ્વારા ઠગાઇ

- એવાં ઘણાં ધૂર્ત લોન એપ છે, જે તરત જ ટૂંકા ગાળાની લોન્સ ઓફર કરે છે. આ એપ્સ નાણાં ઉધાર લેનારને છેતરે છે અને તેઓ બહુ ઊંચા દરે વ્યાજ ચાર્જ કરે છે.
- ભોળા ગ્રાહકોને આકર્ષવા આ ઠગો "ઓફર મર્યાદિત સમયગાળા માટે" એવી જાહરેરાત કરે છે અને અરજદારોને ડરાવનારી યુક્તિઓ પ્રયોજી તત્કાળ નિર્ણય લેવાનું કહે છે.

સાવચેતી

- શંકાસ્પદ લોન એપ વગેરે પાસેથી લોન લેવા પૂર્વે નીચેના મુદ્દા તપાસો

- ધિરાણકર્તા તમારો ક્રેડિટ સ્કોર તપાસવાને બદલે તમારી અંગત વિગતો જાણવામાં રુચિ રાખી રહ્યો છે? ધિરાણકર્તા સરકાર/અધિકૃત એજન્સીમાં રજિસ્ટર્ડ છે?

ધિરાણકર્તાએ ફિઝિકલ સરનામું અથવા સંપર્ક માટેની માહિતી પૂરી પાડી છે કે નહિ એ ચકાસો. અન્યથા બાદમાં તેનો સંપર્ક કરવાનું મુશ્કેલ બની શકે છે.

- યાદ રાખો કોઈ પણ પ્રતિષ્ઠિત એનબીએફસી/બેન્ક લોન અરજીનું પ્રોસેસિંગ કર્યા પૂર્વે કદી ચુકવણી કરવાનું કહેતી નથી.
- સાચે જ લોન આપનારાઓ દસ્તાવેજોની ચકાસણી કર્યા વિના કદી નાણાં ઓફર કરતા નથી.
- એનબીએફસીનું પીઠબળ ધરાવતાં લોન એપ્સ સાચાં છે કે નહિ તેની ચકાસણી કરો.

5. નાણાં સરક્યુલેશન/પોન્ઝી/મલ્ટીલેવલ માર્કેટિંગ (એમએલએમ) સ્કીમ્સ દ્વારા છેતરપિંડી

- એમએલએમ/ચેઈન માર્કેટિંગ/પિરામિડ સ્ટ્રક્ચર સ્કીમમાં જોડાવા/સભ્યો વધારવા સાથે સરળ કે ઝડપી નાણાં બનાવવાનું વચન અપાય છે.
- સ્કીમ્સમાં ઊંચા વળતરની ખાતરી આપવામાં આવે છે એટલું જ નહિ પરંતુ ભોળા રોકાણકારોનો વિશ્વાસ જીતવા અને કર્ણોપકર્ણ જાહેરાત મારફત વધુને વધુ રોકાણકારોને આકર્ષવા પ્રથમ થોડા હપ્તા પણ ચૂકવવામાં આવે છે.
- સ્કીમ્સ ચેઈન/ ગ્રુપમાં વધુને વધુ લોકોને ઉમેરવા માટે પ્રોત્સાહન આપે છે જે માટે મેમ્બર્સ લઈ આવનારાને પ્રોડક્ટ્સના વેચાણથી અધિક કમિશન ચૂકવવામાં આવે છે.
- આ મોડેલને કારણે કેટલાક સમય બાદ જ્યારે સ્કીમમાં જોડાનારા લોકોની સંખ્યા ઘટવા માંડે એટલે સ્કીમ ટકી શકતી નથી. એ પછી ઠગો સ્કીમને બંધ કરી દઈ લોકોએ રોકેલાં નાણાં લઈને ગાયબ થઈ જાય છે.

સાવચેતી

- પોન્ઝી/એમએલએમ સ્કીમ્સમાં રોકાણ કરતી વખતે
- વળતર જોખમના પ્રમાણમાં હોય છે. ઊંચું જોખમ, ઊંચું વળતર. એટલે જો કોઈ સ્કીમ અસામાન્યપણે (પ્રતિ વર્ષ 40-50 ટકા) સતત ઊંચું વળતર આપે તો તે સંભવિત છેતરપિંડીની પ્રથમ નિશાની છે અને સાવધ થઈ જવું.
- કોઈ ચુકવણી/કમિશન/બોનસ/નફાની ટકાવારી માલ/સર્વિસના ખરેખરા વેચાણ વિના અપાય તો સ્કીમ શંકાસ્પદ છે અને તે ઠગાઈમાં પરિણમી શકે છે.
- લોકોએ ઊંચા વળતરનાં વચનો આપતી હસ્તીઓ કે જે મલ્ટીલેવલ માર્કેટિંગ/ચેઈન માર્કેટિંગ/ પિરામિડ ચલાવતી હોય તેની તરફ લલચાવું નહિ.
- નાણાંનું સર્કયુલેશન/મલ્ટીલેવલ માર્કેટિંગ/પિરામિડ સ્ટ્રક્ચર્સ સ્કીમ્સ હેઠળ નાણાં સ્વીકારવાં એ પ્રાઈઝ ચિટ એન્ડ મની સર્ક્યુલેશન (બેનિંગ) એક્ટ 1978 હેઠળ ગુનો છે. લોકોએ આવી ઓફર્સ કરતી સ્કીમ્સની ખબર પડે કે તરત જ રાજ્યની પોલીસને જાણ કરવી જોઈએ.

6.બનાવટી દસ્તાવેજો દ્વારા ખોટી રીતે લોન્સ લેવી

- બનાવટી દસ્તાવેજો દ્વારા એવી રીતે છેતરપિંડી કરવામાં આવે છે કે વ્યક્તિ અથવા કોઇ હસ્તી નાણાકીય સંસ્થાઓ પાસેથી કોઇ પણ રૂપની સેવાઓ પ્રાપ્ત કરવા બનાવટી દસ્તાવેજોનો ઉપયોગ કરે છે.
- એનબીએફસી કર્મચારી/એનબીએફસીના ઇમેઇલ આઇડીની અધિકૃતતા ચકાસ્યા વિના જ્યારે કેવાયસી સંબંધિત દસ્તાવેજો સુપરત કરવામાં આવે ત્યારે આવી છેતરપિંડી થાય છે.
- છેતરપિંડીનો ભોગ બનેલા લોકોની અંગત માહિતી જેવી કે આઇડેન્ટિટી કાર્ડ્સ, બેન્ક એકાઉન્ટની વિગતો વગેરે ચોરી તેનો ઉપયોગ કરી ખોટી લોન્સ મંજૂર કરવામાં આવે છે અને તેમની ઓળખ સંબંધિત માહિતીનો ઉપયોગ નાણાસંસ્થા પાસેથી લાભો પ્રાપ્ત કરવા માટે કરવામાં આવે છે.

સાવચેતી

- ગ્રાહકોએ લોન લેતી વખતે કેવાયસી માટે અને લોનના ડિસ્બર્સમેન્ટ માટે અન્ય અંગત દસ્તાવેજો અને નેશનલ ઓટોમેટેડ ક્લિયરિંગ હાઉસ સહિતના દસ્તાવેજો પૂરા પાડવામાં સાવધાની રાખવી જોઇએ.
- આવા દસ્તાવેજો માત્ર હસ્તીના અધિકૃત કર્મચારી અથવા હસ્તીઓના અધિકૃત ઇમેઇલ આઇડીઝ પર જ સુપરત કરવા જોઇએ.
- લોન મંજૂર ન કરાય ત્યારે અને લોન ક્લોઝર પછી ગ્રાહકે હસ્તીઓને અવશ્ય વિનંતી કરવી જોઇએ કે તેના દસ્તાવેજોને સિસ્ટમમાંથી કાયમ માટે દૂર કરાય.

પાર્ટ-સી

નાણાકીય વ્યવહારો માટે રાખવી જોઇતી સર્વસામાન્ય સાવચેતીઓ

- સર્વસામાન્ય
- તમે બ્રાઉઝિંગ કરો ત્યારે શંકાસ્પદ પોપ અપ્સ દેખાય તો સાવચેત બની જાઓ.
- ઓનલાઇન પેમેન્ટ કરવા પૂર્વે હંમેશા ચેક કરો કે સલામત પેમેન્ટ ગેટવે (https://યુઆરએલ હોય કે જેની સાથે પેડ લોકનો સિમ્બોલ) હોય.
- તમારો પીન (પર્સનલ આઇડેન્ટિફિકેશન નંબર), પાસવર્ડ અને ક્રેડિટ અથવા ડેબિટ કાર્ડ નંબર, સીવીવી ગુપ્ત રાખો.
- કાર્ડની વિગતો વેબસાઇટ્સ/ડિવાઇસીસ/પબ્લિક લેપટોપ/ડેસ્કટોપ્સ પર સેવ કરવાનું નિવારો.
- જ્યાં ઉપલબ્ધ હોય ત્યાં ટુફેક્ટર ઓથેન્ટિફિકેશન ચાલુ કરો.
- શંકાસ્પદ એટેચમેન્ટ અથવા ફિશિંગ લિન્ક્સ ધરાવતા અજાણ્યા સ્રોત પાસેથી આવેલા કોઇ પણ ઇમેઇલને ન ખોલો.
- તમારા ડિવાઇસને કદી અનલોક ન રાખો.
- અજાણ્યા એપ્લિકેશન્સ અથવા સોફ્ટવેરને ઇન્સ્ટોલ ન કરો.
- અજાણ્યા ડિવાઇસ પર પાસવર્ડ્સ અથવા ગુપ્ત માહિતી સંગ્રહો નહિ.

સલામત બ્રાઉઝિંગ માટે

- બિનસલામત વેબસાઈટ્સ પર જવાનું નિવારો/
- અજાણ્યા બ્રાઉઝર્સ વાપરવાનું ટાળો.
- સાર્વજનિક ડિવાઈસ પર પાસવર્ડ સેવ કરવાનું ટાળો
- અજાણી વેબસાઈટ્સ પર સલામત માહિતી દાખલ કરવાનું નિવારો.
- સોશિયલ મીડિયા પર અજાણી વ્યક્તિઓને અંગત માહિતી આપવાનું નિવારો.
- રિડાયરેક્ટ કરતો ઈમેઈલ કે એસએમએસ હોય એવા કિસ્સામાં હંમેશ પેજની સલામતી ચકાસો.

સલામત ઈન્ટરનેટ બેન્કિંગ માટે

- સાર્વજનિક ડિવાઈસીસ પર હંમેશ વર્ચ્યુઅલ કીબોર્ડનો ઉપયોગ કરો, કારણ કે હલકાં ડિવાઈસીસ અને કીબોર્ડ મારફતે કીસ્ટ્રોક્સને શોધી શકાય છે.
- ઉપયોગ કરી લીધા બાદ તરત જ ઈન્ટરનેટમાંના બેન્કિંગ સેશનમાંથી લોગઆઉટ કરો.
- સમયાંતરે પાસવર્ડ અપડેટ કરતા રહો.
- ઈમેઈલ અને ઈન્ટરનેટ બેન્કિંગ માટે એક જ પાસ વર્ડનો ઉપયોગ ન કરો.
- નાણાકીય વ્યવહારો માટે પબ્લિક ટર્મિનલ્સનો ઉપયોગ કરવાનું ટાળો.

ઈમેઈલ એકાઉન્ટની સલામતી માટે

- અજાણ્યા સરનામેથી આવેલા ઈમેઈલ્સ ક્લિક ન કરો.
- સાર્વજનિક અથવા ફ્રી નેટવર્ક્સ પર ઈમેઈલ્સનો ઉપયોગ કરવાનું નિવારો.
- ઈમેઈલ્સમાં તમારી સલામત માહિતી/બેન્ક પાસવર્ડ્સ વગેરે ન સંઘરો.

પાસવર્ડની સલામતી માટે

- આંકડા સાથેના મૂળાક્ષરો (આલ્ફાન્યુમેરિક) અને સ્પેશિયલ કેરેક્ટર્સ તમારા પાસવર્ડમાં ઉમેરો.
- જો સુવિધા ઉપલબ્ધ હોય તો ટુ ફેક્ટર ઓથેન્ટિફિકેશન્સ રાખો.
- સમયાંતરે પાસવર્ડ બદલતા રહો.
- ડિપોઝિટ લઈ રહેલી એનબીએફસી સાચી છે કે નહિ એ તમે કઈ રીતે જાણશો?
- ડિપોઝિટરે https://rbi.org.in પર ઉપલબ્ધ ડિપોઝિટ સ્વીકારવાની છૂટ ધરાવતી એનબીએફસીની યાદીમાં કંપનીનું નામ છે કે નહિ તે ચકાસવું જોઈએ અને એની ખાતરી કરવી જોઈએ કે સંબંધિત એનબીએફસીનો સમાવેશ ડિપોઝિટ સ્વીકારવાની જેમને મનાઈ ફરમાવવામાં આવી હોય એવી કંપનીઓની યાદીમાં નથી.
- એનબીએફસીએ તેની સાઈટ પર રિઝર્વ બેન્ક દ્વારા ઈશ્યુ કરવામાં આવેલા સર્ટિફિકેટ ઓફ રજિસ્ટ્રેશનને નજરે ચડે એ રીતે દર્શાવવું જોઈએ. આ સર્ટિફિકેટમાં ડિપોઝિટ્સ સ્વીકારવાની મંજૂરી આપવામાં આવી હોવાનો ખાસ ઉલ્લેખ હોવો જોઈએ. ડિપોઝિટરોએ આ

સર્ટિફિકેટની ચકાસણી કરી એની ખાતરી કરવી જોઇએ કે કંપનીને ડિપોઝિટ સ્વીકારવાની માન્યતા પ્રાપ્ત છે.
- એનબીએફસી 12 મહિનાથી ઓછા સમયગાળા માટે અને 60 મહિનાથી અધિક સમયગાળા માટે ડિપોઝિટ સ્વીકારી શકતી નથી અને તે ડિપોઝિટરને 12.5 ટકાથી અધિક દરે વ્યાજ આપી શકે નહિ.
- રિઝર્વ બેન્ક વ્યાજદરોમાં ફેરફારને https://rbi.org.in પરના સાઇટ મેપમાં એનબીએફસી લિસ્ટ વિભાગમાંના એફએક્યુઝમાં પ્રસિધ્દ કરે છે.

ડિપોઝિટર્સએ રાખવી જોઇતી સાવધાનીઓ

- કંપનીમાં મૂકેલી પ્રત્યેક ડિપોઝિટ માટેની યોગ્ય રસીદ પ્રાપ્ત કરવાનો આગ્રહ રાખો.
- રસીદ પર કંપનીની અધિકૃત વ્યક્તિની સહી, ડિપોઝિટની તારીખ, ડિપોઝિટરનું નામ, રકમ આંકડામાં અને શબ્દોમાં, ચૂકવવાપાત્ર વ્યાજ દર, પાકતી તારીખ અને પાકતી રકમ દર્શાવેલી હોવી જોઇએ.
- એનબીએફસી વતીથી બ્રોકર્સ/એજન્ટ્સ વગેરે ડિપોઝિટ્સ ઉઘરાવતા હોય એવા કિસ્સામાં ડિપોઝિટર્સે એની ખાતરી કરવી જોઇએ કે બ્રોકર્સ/એજન્ટ્સને એનબીએફસીએ અધિકૃત કર્યા હોય.
- ઓનલાઇન ફરિયાદ કઇ રીતે કરવી
- આરબીઆઇને ફરિયાદ કરવા માટે
- કૃપયા ક્લિક કરો https://cms.rbi.org.in/
- સેબીને ફરિયાદ કરવા માટે
- કૃપયા ક્લિક કરો https://scores.gov.in/
-
- ઇન્સ્યુરન્સ રેગ્યુલેટરી એન્ડ ડેવલપમેન્ટ ઓથોરિટી ઓફ ઇન્ડિયા (આઇઆરડીએઆઇ)ને ફરિયાદ કરવા
- કૃપયા ક્લિક કરો https://igms.irda.gov.in/
- નેશનલ હાઉસિંગ બેન્ક (એનએચબી)ને ફરિયાદ કરવા
- કૃપયા ક્લિક કરો https://grids.nhbonline.org.in/
- સાયબર પોલીસ સ્ટેશનને ફરિયાદ કરવા
- કૃપયા ક્લિક કરો https://cybercrime.gov.in/

*પારિભાષિક શબ્દાવલી

- **એડવાન્સ ફી/પ્રોસેસિંગ ફી/ટોકન ફીઃ** બધી એવી પ્રારંભિક ચુકવણીઓ જે માત્ર ડોક્યુમેન્ટેશનના રિએમ્બર્સમેન્ટ, મીટિંગ ખર્ચાઓ, લાગુ પડતી પ્રોસેસિંગ ફીઝ પૂરતા સીમિત નથી અને લોન લેનારાને લોનની રકમ ચૂકવાય એ માટેના લાગુ પડતા ચાર્જીસ.

- **ટુફેક્ટર ઓથેન્ટિફિકેશનઃ** ટુફેક્ટર ઓથેન્ટિફિકેશન (ટુએફએ તરીકે પણ ઓળખાય છે) બે પરિબળના સંયોજન દ્વારા વપરાશકારની સ્પષ્ટ ઓળખ પૂરી પાડે છે. તેમાં બે ફેક્ટર હોય છે. એક કાર્ડ પરની (નંબર, એક્સપાયરી ડેટ અને સીવીવી જેવી)વિગતો અને બીજો પીન (સ્થિર અથવા એક વાર માટે જનરેટ કરાયેલો) કે જે ઓળખને પ્રસ્થાપિત કરે છે.
- **૩ડી સિક્યોરઃ** ૩ડી સિક્યોર ઓનલાઈન ક્રેડિટ અને ડેબિટ કાર્ડ વ્યવહારો માટેનો એક્સએમએલ આધારિત ડિઝાઈન કરેલો અતિરિક્ત સુરક્ષા પ્રોટોકોલ છે. એને વેરીફાઇ બાય વિઝા, માસ્ટરકાર્ડ સિક્યોર કોડ અથવા અમેરિકન એક્સપ્રેસ સેફકી તરીકે પણ ઓળખવામાં આવે છે.
- **એક્વાયરિંગ બેન્કઃ** એક્વાયરિંગ બેન્ક એ બેન્ક છે જે ક્રેડિટ અથવા ડેબિટ કાર્ડ પ્રોસેસ કરે છે. એક્વાયરિંગ બેન્ક મલ્ટીપલકાર્ડ સ્કીમ્સ જેવી કે વિઝા, માસ્ટરકાર્ડ, માસ્ટ્રો અને રૂપેને સામાન્યપણે સપોર્ટ કરે છે.
- **ઓથોરાઇઝેશનઃ** કાર્ડ ઇશ્યુ કરનારી બેન્ક પાસેથી મર્ચન્ટ ટ્રાન્ઝેક્શન વિનંતીને પ્રાપ્ત થતો પ્રતિભાવ, જે દર્શાવે છે કે ચુકવણીની માહિતી યોગ્ય છે અને ગ્રાહકના ક્રેડિટ કાર્ડ પર ફંડ ઉપલબ્ધ છે.
- **બેન્ક આઇડેન્ટિફિકેશન નંબર (બીઆઇએન):** વિઝા અને માસ્ટરકાર્ડે તેની મેમ્બર નાણાકીય સંસ્થાઓ, બેન્કો અને પ્રોસેસર્સ માટે નિયુક્ત કરેલો નંબર.
- **બીઆઇએન વેલિડેશનઃ** બીઆઇએનમાં સામેલ સંસ્થાઓની યાદી સામે કાર્ડના બીઆઇએન નંબરની ચકાસણીની પ્રક્રિયા.
- **બ્લેકલિસ્ટિંગઃ** ઠગાઇ કરતા ખરીદદારો અથવા વધુ જોખમ ધરાવતા વેપારીઓની માહિતી એકત્ર કરવાની પ્રથા

(*સ્રોત ઇન્ટરનેટ અને અન્ય પ્રકાશનો)

કાર્ડ કેપ્ચર પેજઃ

- સલામત પેજ કે જેના પર કાર્ડની વિગતો ઝિલાય (કેપ્ચર થાય) છે. હસ્તીઓ કે જેઓ પીસીઆઇ ડીએસએસ સર્ટિફિકેશન ધરાવે છે, તેમને વિગતો કેપ્ચર કરવા દેવાય છે.
- એક્વાયરિંગ બેન્ક (ઉદા.ત., એસબીઆઇ, એચડીએફસી)
- એગ્રેગેટર (ઉદા.ત., પેયુ)
- મર્ચન્ટ (ઉદા.ત., ફ્લિપકાર્ટ, એમેઝોન)
- **કાર્ડ નંબર**
  - ખાતા નંબર કે જે ક્રેડિટ કાર્ડ એસોસિયેશન અથવા કાર્ડ ઇશ્યુ કરનારી બેન્ક દ્વારા કાર્ડધારકને આપવામાં આવતો ખાતા નંબર. ક્રેડિટ કાર્ડ દ્વારા ચુકવણી કરવા માટે આ માહિતી ગ્રાહકે વેપારીને આપવાની રહે છે.
  - કાર્ડના આગળના ભાગમાં આંકડાઓની હાર હોય છે (આ આંકડા બેન્ક આઇડેન્ટિફિકેશન નંબર, કેટેગરી, કરન્સી વગેરે દર્શાવે છે.)
  - વિઝા, માસ્ટરકાર્ડ, માસ્ટ્રો, રુપેઃ 16 આંકડા
  - એમેક્સઃ 15 આંકડા

- **કાર્ડ પ્રેઝેન્ટ (સીપી):** ટ્રાન્ઝેક્શન દરમિયાન, કાર્ડધારક અથવા કાર્ડ વેચાણના સ્થળે રજૂ કરાય, ઉદાહરણ કરીકે કરિયાણા સ્ટોરાં કાર્ડ સ્વેપ કરાય. સામાન્ય રીતે સીપી કેસોમાં ટીડીઆર/એમડીઆર કાર્ડ નોટ પ્રેઝન્ટ (સીએનપી) કેસોની તુલનાએ ઓછા હોય છે, કારણ કે સીપી વ્યવહારોમાં (જોખમ માટે રેટ્સ એડજસ્ટેડ હોઇ) જોખમ ઓછું હોય છે.
- **કાર્ડ વોલ્ટિંગ:** કાર્ડની વિગતો (કાર્ડ નંબર અને સીવીવી) સંધરવાની પ્રક્રિયા. પીસીઆઇ ડીએસએસ સર્ટિફાઇડ હસ્તી (એક્વાયરિંગ બેન્ક, એગ્રેગેટર અથવા વેપારી) દ્વારા કાર્ડની વિગતો સંધરવામાં આવે છે જે પછીના વ્યવહારોમાં દર્શાવવામાં આવે છે.
- **ક્લોઝ્ડલૂપ પ્રીપેઇડ કાર્ડ્સ/વોલેટ:** કાર્ડ્સ/વોલેટ માત્ર એક મર્ચન્ટ ખાતે વાપરી શકાય છે અને ભંડોળ ખાતામાંથી કે એટીએમ દ્વારા ઉપાડી શકાતાં નથી.
- **કોબ્રાન્ડેડ કાર્ડ્સ:** કાર્ડ્સ જે નાણાકીય સંસ્થા દ્વારા કાર્ડ સ્કીમ સાથે ઈશ્યુ કરાયું હોય અને જેનું કોર્પોરેટ બ્રાન્ડિંગ હોય.
- **કલેક્શન એકાઉન્ટ:** વેપારીનું બેન્ક એકાઉન્ટ કે જેમાં પેમેન્ટ ગેટવેની રકમ જમા કરવામાં આવે છે. કલેક્શન એકાઉન્ટ કરન્ટ એકાઉન્ટ, નોડલ એકાઉન્ટ અથવા એસ્ક્રો એકાઉન્ટ હોઇ શકે છે.
- **ક્રેડિટ કાર્ડ્સ:** એ કાર્ડ્સ જે નાણાકીય સંસ્થા પાસેથી નાણાં ઉધાર લઇ પ્રોડક્ટ્સ કે સર્વિસીસ માટેની ચુકવણી કરવા દે છે.
- **ચાર્જબેક**
  - ઈશ્યુઇંગ બેન્ક સમક્ષ કાર્ડહોલ્ડર દ્વારા ઉપસ્થિત કરવામાં આવેલો વિવાદ
  - ચાર્જબેક સર્જાવા પાછળવાં વિવિધ કારણ હોઇ શકે:
    - સર્વિસ કે પ્રોડક્ટની ડિલિવરી ન કરાઇ હોય
    - રદ કરાય ત્યારે રિફંડ ન કરાયું હોય.
    - કાર્ડ હેક કરાયું હોય.
- આવા સંજોગોમાં ઈશ્યુઇંગ બેન્ક એક્વાયરર બેન્કને ચાર્જબેક મોકલશે અને એક્વાયરિંગ બેન્ક વેપારીનો સીધો (જો એક્વાયરિંગ બેન્ક વેપારી સાથે સીધું સંકલન ધરાવતી હોય) સંપર્ક કરશે અથવા એગ્રેગેટર (જો વ્યવહાર એગ્રેગેટર મારફત થયો હોય)નો સંપર્ક કરી ડિલિવરી અથવા રિફંડ માટેની સાબિતી નિશ્ચિત સમયમર્યાદામાં રજૂ કરશે અથવા ચાર્જબેકને માન્ય રાખશે અને વેપારી ચાર્જબેક રકમ પરત કરશે.
- **ક્રેડિટ લિમિટ:** ક્લાયન્ટને નાણાસંસ્થા દ્વારા જે મહત્તમ રકમની ક્રેડિટની છૂટ આપવામાં આવે છે તેને ક્રેડિટ લિમિટ કહેવામાં આવે છે. ધિરાણકર્તાઓ સામાન્ય રીતે ક્રેડિટ પ્રાપ્ત કરવા ઇચ્છુક અરજદારો દ્વારા પૂરી પાડવામાં આવેલી માહિતીના આધારે ક્રેડિટ લિમિટ અથવા ક્રેડિટ લાઇન નક્કી કરે છે. ક્રેડિટ લિમિટ એવું પરિબળ છે જે ગ્રાહકના ક્રેડિટ સ્કોરને અને ભવિષ્યમાં ક્રેડિટ પ્રાપ્ત કરવાની ક્ષમતાને અસર કરે છે.
- **સીવીવી:** સીવીવી એટલે કાર્ડ વેરિફિકેશન વેલ્યુ. આ નંબર ઓનલાઇન વ્યવહારો પૂરા કરવા માટે મહત્ત્વનો છે અને તેની જાણ કોઇને પણ કરવી જોઇએ નહિ.
- **ડેબિટ કાર્ડ્સ:** આ એવાં કાર્ડ્સ છે જેનો વપરાશ ખરીદી કરવા માટે સીધા બેન્ક ખાતામાંથી ફંડની ચુકવણી માટે કરવામાં આવે છે.

- **ડિક્લાઇન્ડ પેમેન્ટ્સ:** જે વ્યવહારો કાર્ડ ઇશ્યુ કરનારી બેન્ક દ્વારા મંજૂર કરવામાં આવતા નથી તેને ડિક્લાઇન્ડ પેમેન્ટ્સ તરીકે માર્ક કરવામાં આવે છે. ડિક્લાઇન્ડ વ્યવહારો માટે કોઇ પગલું લેવાનું હોતું નથી અને ગ્રાહકે ચુકવણીનો પુનઃ પ્રયત્ન કરવાનો રહે છે.
- **ડિજિટલ સિગ્નેચર:** એક ઇલેક્ટ્રોનિક ફાઇલ જેમાંની માહિતીનો ઉપયોગ સંસ્થા કે વ્યક્તિની ભરોસાપાત્રતા ચકાસવા માટે કરવામાં આવે છે. ડિજિટલ સર્ટિફિકેટ્સ સર્ટિફિકેટ ઓથોરિટી દ્વારા ઇશ્યુ કરવામાં આવે છે અને તેમાં સિક્યોર સોકેટ્સ લેયર (એસએસએલ)નો ઉપયોગ કરવામાં આવે છે.
- **ઇકોમર્સ પ્લેટફોર્મ:** સોફ્ટવેર કે જેમાં ઇકોમર્સ વેપાર ચલાવવા આવશ્યક વિવિધ કાર્યો જેવાં કે વેબસાઇટ, કેટેગરી મેનેજમેન્ટ, પ્રાઇસિંગ મેનેજમેન્ટ, ઓર્ડર મેનેજમેન્ટ અને પેમેન્ટ મેનેજમેન્ટની જોગવાઇ હોય. દાખલા તરીકે શોપીફાઇ, મેજેન્ટો અને અન્ય.
- **ઇએમઆઇ (ઇક્વેટેડ મંથલી ઇન્સ્ટોલમેન્ટ્સ):**
- બેન્ક દ્વારા કાર્ડધારકને ટ્રાન્ઝેક્શનની રકમ વિભાજિત કરી મહિનાના ધોરણે નાની રકમ ચૂકવવાની સુવિધાને ઇએમઆઇ કહેવાય છે. આ સર્વિસ માટે બેન્ક પ્રોસેસિંગ ફી અથવા વ્યાજ ચાર્જ કરી શકે છે.
- **ઇએમવી:** યુરોપે, માસ્ટરકાર્ડ અને વિઝા એ પોઇન્ટઓફસેલ ખાતે છેતરપિંડીમાં ઘટાડો કરવા માઇક્રોચિપ આધારિત ટેકનોલોજી છે.
- **એન્ક્રિપ્શન:** પ્રોસેસિંગ માહિતીને સ્પેશિયલ જાણકારી ધરાવનારા સિવાયના કોઇ પણ વાપરી ન શકે એવા રૂપમાં પરિવર્તન કરવાની પ્રક્રિયા, જેને સામાન્ય રીતે કી કહેવામાં આવે છે.
- **એક્સપાયરી ડેટ:** એ તારીખ જે તારીખે કાર્ડની માન્યતા સમાપ્ત થતી હોય. જે કાર્ડની મુદ્દત સમાપ્ત ન થઇ હોય એવા ટ્રાન્ઝેક્શન્સને માન્ય કરવામાં આવે છે.
- **ફ્લેટ ફી:** ટ્રાન્ઝેક્શનની રકમની ટકાવારી નહિ પણ ટ્રાન્ઝેક્શન દીઠ ચાર્જીસ.
- **ગિફ્ટ કાર્ડ:** ચોક્કસ વેપારીઓ પાસેથી ખરીદી કરવા વાપરવામાં આવતા પ્રીપેઇડ/પ્રીલોડેડ મર્ચન્ટ ઇન્સ્ટ્રુમેન્ટ.
- **ગેટવે:** ડિજિટલ ફાઇનાન્સિયલ સર્વિસીસ પ્રોવાઇડર માટે વિવિધ કામગીરી કરતી આઉટસોર્સ્ડ ધોરણે ચાલતીએન્ટરપ્રાઇઝ.
- **ઇન્ટરચેન્જ ફીઝ:** ટ્રાન્ઝેક્શન સંબંધિત ખર્ચાને સરભર કરવા એક્વાયરર દ્વારા ઇશ્યુઅરને ચૂકવાતી ફી.
- **આઇએમપીએસ:** ઇમિજિયેટ પેમેન્ટ સર્વિસીસ એ એનપીસીઆઇનું પ્રોડક્ટ છે, જે એક લાખ રૂપિયા સુધીની રકમ મોબાઇલ નંબરના આધારે રિયલ ટાઇમ ધોરણે લાભાર્થીને ચુકવણી કરે છે.
- **નો યોર કસ્ટમર (કેવાયસી):** વ્યક્તિ અથવા હસ્તીની ભરોસાપાત્ર માહિતી સ્થાપિત કરવા માટેના દસ્તાવેજોનો સેટ.
- **મલ્ટીલેવલ માર્કેટિંગ:** કંપની વતીથી માલ કે સર્વિસીસનું વેચાણ કરવા માટેની એવી પદ્ધતિ જેમાં સહભાગીઓ વેચાણ ઉપરાંત તેઓ જે સહભાગીઓને નિયુક્ત કરે એમના વેચાણમાંથી પણ કમિશન પ્રાપ્ત થાય.

- **નીયર ફીલ્ડ કોમ્યુનિકેશન એનએફસીઃ** એનએફસી સજ્જ મોબાઇલ ફોન કેપેબલ ટર્મિનલ, જેમાં પેમેન્ટ્સને પેમેન્ટ ડેટામાં ટ્રાન્સફર કરવા માટે વપરાતી ટેકનોલોજી.
- **એનઇએફટીઃ** નેશનલ ઇલેક્ટ્રોનિક ફંડ ટ્રાન્સફરઃ લાભાર્થીઓને બેચ પ્રમાણે ચુકવણીઓ કરવા માટેનું આરબીઆઇનું પ્રોડક્ટ.
- **વન ટાઇમ પાસવર્ડ (ઓટીપી):** તમારા ઓનલાઇન ટ્રાન્ઝેક્શન્સની સલામતી માટે ઓથેન્ટિફિકેશનની અતિરિક્ત દ્વિસ્તરીય પગલું. મોટા ભાગની નાણાકીય સંસ્થાઓમાં મોટા ભાગના નાણકીય વ્યવહારો માટે આ સમયબદ્ધ ઓટીપી પદ્ધતિ બહુ લોકપ્રિય બની છે.
- **ફિશિંગઃ** પ્રતિષ્ઠિત કંપનીઓએ જાણે મોકલી હોય એવા ઇમેઇલ્સ મોકલવા કે જેથી વ્યક્તિઓ તેમની અંગત માહિતી જેવી કે પાસવર્ડ્સ અને ક્રેડિટ કાર્ડ નંબર જાહેર કરવા લલચાઇ જાય.
- **પોઇન્ટ ઓફ સેલ ડિવાઇસ ટર્મિનલ, એક્સેપ્ટન્સ ડિવાઇસ, પીઓએસ, એમપીઓએસઃ** ઇલેક્ટ્રોનિક પેમેન્ટ્સ પ્રાપ્તિને મેનેજ કરતું કોઇ પણ સાધન.
- **પીસીઆઇડીએસએસઃ** એન્ટરપ્રાઇઝીસ અંતિમ વપરાશકારના ડેટાને રક્ષવા અપનાવે છે એ પદ્ધતિઓ. પીસીઆઇડીએસએસ એ કાર્ડ ઇન્ડસ્ટ્રીનું આ માટેનું સ્ટાન્ડર્ડ છે.
- **પીટુપી; રિમોટ ક્રોસબોર્ડર ટ્રાન્સફર ઓફ વેલ્યુ, ક્રોસબોર્ડર રેમિટન્સઃ** અન્ય દેશમાં અન્ય વ્યક્તિને પેમેન્ટ કરવું કે પેમેન્ટ પ્રાપ્ત કરવું.
- **ક્વિક રિસ્પોન્સ કોડ (ક્યુઆર):** ક્વિક રિસ્પોન્સ કોડ એ બારકોડ ટાઇપનો કોડ છે જેમાં માહિતી સંઘરાય છે અને ડિજિટલ ડિવાઇસ જેવા કે સેલ ફોન પર વાંચી શકાય.
- **રિકન્સિલિયેશનઃ** રિકન્સિલિયેશન એ એવી હિસાબી પ્રક્રિયા છે, જેમાં આંકડા સાચા છે અને તાળો મળે એની ખાતરી માટે રેકોર્ડ્સના બે સેટ્સનો ઉપયોગ કરે છે. તે એની ખાતરી કરે છે કે જે નાણાં ખાતામાંથી જઇ રહ્યાં છે એટલી રકમ ખર્ચાઇ છે અને રેકોર્ડના અંતે બંને એકસમાન છે.
- **રિકરિંગ પેમેન્ટ્સઃ** સમયાંતરે કરવામાં આવતી ચુકવણીઓ અને તે સમયગાળો સાપ્તાહિક, માસિક, ત્રિમાસિક, છ માસિક કે વાર્ષિક હોઇ શકે. દાખલા તરીકે વીજળીનું બિલ, વિમાનું પ્રીમિયમ.
- **સ્વિચ (નેશનલ ફાઇનાન્સિયલ સ્વિચ):** એ હસ્તી કે જે એક પ્રોવાઇડર પાસેથી ટ્રાન્ઝેક્શન્સ પ્રાપ્ત કરી અન્ય પ્રોવાઇડરને મોકલે છે. સ્વિચ માલિકીની અથવા ભાડાની સ્કીમ અથવા વ્યક્તિગત પ્રોવાઇડર્સ દ્વારા ભાડે લેવાયેલી હોઇ શકે. સ્વિચ ઇન્ટરપાર્ટિસિપન્ટ સેટલમેન્ટ માટે સેટલમેન્ટ સિસ્ટમ સાથે જોડાયેલી હશે.
- **ટીએટીઃ** ટર્ન એરાઉન્ડ ટાઇમઃ ખાસ સર્વિસ ડિલિવર કરવા માટેનો વચનબદ્ધ સમય (દાખલા તરીકે સેટલમેન્ટ માટે ટીએટી ટી પ્લસ ટુ છે).
- **યુનિફાઇડ પેમેન્ટ ઇન્ટરફેસ (યુપીઆઇ):** યુપીઆઇ એનપીસીઆઇ દ્વારા કરવામાં આવેલી ડિજિટલ પેમેન્ટ પહેલ છે. તેનો હેતુ ભારતમાં ડિજિટલ પેમેન્ટ્સને વેગ આપવાનો અને ઇન્ટઓપરેબિલિટી પૂરી પાડવાનો છે. એક વાર ગ્રાહક બેન્કમાં યુપીઆઇ માટે નોંધણી કરાવે એટલે એક યુનિક વર્ચ્યુઅલ આઇડેન્ટિફાયર સર્જવામાં આવે છે અને તેને પેમેન્ટ કરવા હેતુ મોબાઇલ સાથે મેપ કરવામાં આવે છે. યુપીઆઇ લાભાર્થીની વર્ચ્યુઅલ ઓળખ સક્રિય કરે છે

અને રિયલ ટાઇમ ધોરણે નાણાં ટ્રાન્સફર કરે છે. તે સિંગલ ક્લિકમાં ટુફેક્ટર ઓથેન્ટિફિકેશન પર કામ કરે છે.

- **યુટીઆરઃ** યુટીઆર એ યુનિક ટ્રાન્ઝેક્શન રેફરન્સ નંબર છે જે આઇએપીએસમાં જનરેટ થાય છે. એનઇએફટી અને આરટીજીએસ સિસ્ટમ કોઇ પણ ટ્રાન્ઝેક્શનને ઓળખી કાઢે છે. યુટીઆરનું ફોર્મેટ પૂર્વવ્યાખ્યાયિત છે અને તે ટ્રાન્ઝેક્શન શરૂ કરીને બેન્ક દ્વારા સર્જવામાં આવે છે.

- **વોલેટઃ** વોલેટ ફંડ રાખવા માટેનું ખાતું છે અને તેનો વિવિધ ખરીદી માટે ઉપયોગ થઇ શકે છે. વોલેટ વર્ચ્યુઅલ (દાખલા તરીકે મોબાઇલ વોલેટ જેવા કે પેટીએમ, ફોનપે)અથવા ફિઝિકલ (પ્રિપેઇડ કાર્ડ) હોઇ શકે.
