એચ ડી એફ સી બેંક

SECURE BANKING

આ ક્યારેય કોઈને જણાવશો નહીં

ઓટીપી • કાર્ડ નંબર • યુપીઆઈ પિન • બેંકની વિગતો

• કસ્ટમર આઈડી અને પાસવર્ડ

ફિશિંગ અને સ્મિશિંગ લિંક્સ

દગાખોરી

- દગાખોરો થર્ડ પાર્ટી વેબસાઇટ્સ બનાવીને SMS, ઈમેઈલ, સોશિયલ મીડિયા પોસ્ટ્સ, ઇન્સ્ટંટ મૅસેજીસ ઇત્યાદિ મારફત લિંક પ્રસારિત કરે છે.
- તમે આ લિંક પર ક્લિક કરો ત્યારે, તમને ફિશિંગ વેબસાઇટ પર લઈ જવામાં આવે છે જે તદ્દન વાસ્તવિક લાગે છે અને તમે તમારી બેંકની માહિતી જણાવવા તૈયાર થઈ જાઓ છો.
- એક વાર તમે આ પ્રક્રિયા પૂર્ણ કરો પછી દગાખોર ગુનાને અંજામ આપવા તમારી વિગતોનો દુરુપયોગ કરશે.

સુરક્ષા સૂચનો

- ફિશિંગ સામે સુરક્ષાની પ્રથમ હરોળ એ જાણવું છે કે તમારી બેંક ક્યારેય તમારા ઓળખ ચિહ્નો (ક્રીડેન્શિયલ્સ) માટે નહીં પૂછે કે ન તો તેમની વેબસાઇટની લિંક્સ તમને મોકલશે.
- તમારું કાર્ડ તરત જ બ્લૉક કરી દો અથવા તમારો પાસવર્ડ બદલી નાખો જેથી જોખમ ટાળી શકાય.

વિશિંગ કૉલ્સ

દગાખોરી

- કોઈ દગાખોર દ્વારા બેંકર, કંપનીના પ્રતિનિધિ અથવા ઇન્શ્યૉરન્સ એજન્ટ બનીને ઑનલાઇન મેળવેલી માહિતીના ઉપયોગ દ્વારા તમારો સંપર્ક કરવામાં આવી શકે છે.
- તેઓ આને અર્જન્ટ બાબત જણાવીને અને તમારી બેંક તથા શાખા વિશેની મૂળભૂત હકીકતો જણાવીને તમારા ક્રીડેન્શિયલ્સ મેળવવા તમારો વિશ્વાસ જીતે છે.
- એક વાર દગાખોર તમારો વિશ્વાસ જીતી લે છે પછી તેઓ તમને તમારું KYC અપડેટ કરવા કહેશે, તમને આકર્ષક ડિસ્કાઉંટ્સ ઑફર કરશે, દંડથી બચવા ચુકવણી કરવા વિનંતી અને આવું કંઈક કેટલુંયે કરશે, આ બધું તમને મૂર્ખ બનાવવા માટે હોય છે.

સુરક્ષા સૂચનો

- તમારું કાર્ડ તરત જ બ્લૉક કરી દો.
- તમારો પાસવર્ડ વારંવાર રીસેટ કરો.

ઑનલાઈન સેલિંગ માધ્યમોની મદદથી કરાતી દગાબાજી

દગાખોરી

- દગાખોરો ઑનલાઈન સેલિંગ પ્લેટફોર્મ્સ પર બાયર્સ તરીકે નોંધણી કરાવે છે અને તમારા ઉત્પાદનમાં રૂચિ દર્શાવે છે.
- પૈસા ચુકવવાને બદલે તેઓ UPI ઍપ્સ દ્વારા ''પૈસાની વિનંતી'' કરે છે અને તમારા અકાઉન્ટ માંથી પૈસા ઉપાડ કરવા તમને તે માન્ય કરવા આગ્રહ કરે છે.

સુરક્ષા સૂચનો

- તમારી નાણાકીય સંસ્થાને તરત જ અનધિકૃત ટ્રાન્ઝેક્શન થયાની જાણ કરો.
- તમારી ફરિયાદ દાખલ કરવા નૅશનલ સાયબર ક્રાઈમ હેલ્પલાઈન નંબર 155260 પર સંપર્ક કરો.

ક્રીડેન્શિયલ્સ ચોરી કરવા ખોટી હેલ્પલાઈન અને સ્ક્રીન શૅરિંગ ઍપ

દગાખોરી

- ગ્રાહકો વેપારોના હેલ્પલાઈન નંબર્સ જાણવા માટે સર્ચ ઍંજિન્સનો ઉપયોગ કરે છે, જ્યાં ગ્રાહકને કૉલ કરવા પ્રોત્સાહિત કરવાના હેતુસર સ્કૅમ કરનાર વ્યક્તિએ બોગસ નંબર્સ અપલોડ કરેલા છે.
- દગાખોર બૅંકના પ્રતિનિધિ હોવાનો ઢોંગ કરે છે અને તમને ઍપ ડાઉનલોડ કરવાનું અને તમારી સ્ક્રીન શૅર કરવાનું કહી કે પછી ચકાસણી માટે તમારા કાર્ડની વિગતો પૂછીને તમારા ડિવાઈસની પહોંચ મેળે છે.
- તેઓ અસલ છે એવું અનુમાન કરીને આપણે આપણી સલામત વિગતો સાથે બાંધછોડ કરીએ છીએ.
- જેના દ્વારા તેઓ તમારા બૅંકિંગ ક્રીડેન્શિયલ્સની પહોંચ મેળવે છે અને પછી પેમેન્ટ ઍપ્સ અથવા ઈન્ટરનેટ બૅંકિંગનો ઉપયોગ કરીને પૈસા ઉપાડ કરી લે છે.

સુરક્ષા સૂચનો

- ક્યારેય ઍપ્સ ડાઉનલોડ ન કરો અને તમારી સ્ક્રીન અજાણી વ્યક્તિ સાથે શૅર કરશો નહીં.
- જો તમને કોઈ સમસ્યા હોય તો હંમેશા તમારી શાખાની મુલાકાત લો.

સોશિયલ મીડિયા મારફત નકલ કરવી

દગાખોરી

- દગાખોરો લોકપ્રિય સોશિયલ મીડિયા પ્લેટફોર્મ્સ પર ફોની અકાઉન્ટ્સ તૈયાર કરે છે અને મૅડિકલ બિલ્સ ચુકવવા અથવા પેમેન્ટ્સ માટે પૈસા માંગે છે.
- તેઓ સમય જતા તમારો વિશ્વાસ સંપાદન કરે છે અને પાછળથી બ્લૅકમેઈલ કરવા અને પૈસા કઢાવવા તમારી ખાનગી માહિતીનો ઉપયોગ કરે છે.

સુરક્ષા સૂચનો

- ઑનલાઈન અકાઉન્ટની અસલિયત હંમેશા ચકાસી લો અને જો તેઓ ગોપનીય માહિતી વિશે પૂછે તો શંકા ઊભી કરો.
- તમારી ફરિયાદ દાખલ કરવા નૅશનલ સાયબર ક્રાઈમ હેલ્પલાઈન નંબર 155260 પર સંપર્ક કરો.

લૉટરી દગો

દગાખોરી

- દગાખોરો તમે લૉટરીમાં મોટું ઈનામ જીત્યાનો દાવો કરતો ઈમેઈલ તમને લખી શકે અથવા કૉલ કરી શકે છે. જો કે, ફંડ્સ મેળવવા, જ્યાં ડેટા કલેક્ટ કરવામાં આવે છે ત્યાં તેમની વેબસાઈટ પર બેંક અકાઉન્ટ અથવા ક્રેડિટ કાર્ડ મારફત ઓળખની ખાતરી કરવી આવશ્યક રહે છે.
- અમુક સંજોગોમાં, દગાખોરો લૉટરી/સામાન મેળવવા કરવેરા, શિપિંગ ફી, પ્રોસેસિંગ ફી અને અન્ય ફીની સીધી ચુકવવાની માંગ કરે છે.
- વિનંતી કરવામાં આવેલી રકમ લૉટરી/સામાનની નજીવી ટકાવારી બરાબર હોવાથી પીડિત વ્યક્તિ દગાખોરની ઝાળમાં ફસાઈ શકે છે અને ચુકવણી કરે છે.

સુરક્ષા સૂચનો

- લૉટરી જીત્યા સંબંધિત કૉલ્સ, SMS, ઈમેઈલ્સનો ક્યારેય પ્રતિભાવ ન આપો.
- તમારી બેંક અથવા ક્રેડિટ કાર્ડ જારી કરનારને સૂચિત કરી અગવડતા ઊભી થતા ટાળો.

લોન આપવા માટે દગાખોરો દ્વારા કરાતી ખોટી જાહેરાતો

દગાખોરી

- દગાખોરો અત્યંત આકર્ષક વ્યાજ દર, સરળ પુનઃચુકવણી વિકલ્પો અને આવી અનેક ઑફરો સાથે પર્સનલ લોન માટેની લોભામણી જાહેરાતો તૈયાર કરે છે, અને પછી ગ્રાહકોને તેમનો સંપર્ક કરવા જણાવે છે.
- આ ઈમેઈલ IDઓ કોઈ સીનિયર બેંક એક્ઝિક્યુટિવ્સના ઈમેઈલ ID જેવી જ દેખાય છે જેથી વિશ્વાસુ ગ્રાહકો સાથે વિશ્વસનીયતા સ્થાપિ અને વિશ્વાસ જીતી શકાય.
- જ્યારે ગ્રાહકો લોન માટે દગાખોરનો સંપર્ક કરે ત્યારે તેઓ જુદી જુદી અપફ્રન્ટ ફીની માંગણી કરે છે જેમ કે પ્રોસેસિંગ ફી, GST, આંતરરાજ્ય ખર્ચ અને આવી અનેક, અને પછી પૈસાની ફાળવણી કર્યા વગર ગાયબ થઈ જાય છે.

સુરક્ષા સૂચનો

- વાતચીતમાં રોકાણ કરવાનું ટાળો અને લોન મેળવવા માટે તમારા રિલેશનશિપ મૅનેજરનો સંપર્ક કરો.
- સાવચેત રહો અને તેઓ જેનો જવાબ જાણતા હોય એવા એકથી વધુ પ્રશ્નો પૂછો.

ઑનલાઈન જૉબમાં થતા દગાઓ

દગાખોરી

- નકલી જૉબ સર્ચ પોર્ટલ્સ વિકસાવવામાં આવે છે અને જ્યારે પીડિત વ્યક્તિ સીક્યોર બેંક અકાઉન્ટ, ક્રેડિટ કાર્ડ અથવા ડેબિટ કાર્ડ ક્રીડેન્શિયલ્સ આ વેબસાઈટ્સ પર નોંધણી માટે પૂરાં પાડે છે ત્યારે અકાઉન્ટ સાથે છેડછાડ થાય છે.
- અમુક સંજોગોમાં, ચોર કલાકારા કોઈ પ્રતિષ્ઠિત નિગમના અધિકારીઓનું રૂપ ધારણ કરે છે અને નકલી ઈન્ટરવ્યૂના આયોજન પછી પસંદ કરાયાની પુષ્ટિ કરે છે.

સુરક્ષા સૂચનો

- હંમેશા પ્રમાણિત જૉબ પોર્ટલ્સનો જ ઉપયોગ કરો.
- કોઈ અજાણી કંપની તરફથી મળેલા જાહેર ઈમેઈલ્સનો પ્રતિભાવ ન આપો કેમ કે આ ષડયંત્ર હોઈ શકે છે.

ATM કાર્ડ સ્કિમિંગ

દગાખોરી

- ATM મશીન્સમાં સ્કિમિંગ ડિવાઈસીસ મળી આવ્યાં છે, જે દગાખોરોને તમારા કાર્ડ માંથી વિગતો મેળવવા અને નકલી કીપૅડ અને નાનો/પિનહૉલ કૅમેરો કે જે નજરમાં ન આવે તેમ ઈન્સ્ટોલ કરીને તમારો પિન મેળવવામાં સહાયક બને છે.
- બીજીવાર, દગાખોરો તમારી આસપાસ અન્ય ગ્રાહક તરીકે જોવા મળે છે અને તમે તમારો PIN એન્ટર કરતા હો ત્યારે તેની પહોંચ મેળવી લે છે. ત્યારબાદ આ માહિતીનો ઉપયોગ ડુપ્લિકેટ કાર્ડ બનાવવા અને ગ્રાહકના અકાઉન્ટ માંથી પૈસા મેળવી લેવા માટે કરાય છે.

સુરક્ષા સૂચનો

- ATM સાથે કોઈ છેડછાડ કરવામાં આવી છે કે કેમ તે ચકાસી લો.
- તમારી આસપાસ કોઈ શંકાસ્પદ વ્યક્તિ પર હંમેશા નજર રાખો.

સિમ સ્વેપ

દગાખોરી

- તમારો રજિસ્ટર્ડ મોબાઈલ નંબર તમારી મોટાં ભાગની અકાઉન્ટ માહિતી અને પ્રમાણભૂતતા સાથે સંકળાયેલો હોવાથી, દગાખોરો તમારા SIM કાર્ડની પહોંચ મેળવવા અથવા તો નકલી SIM કાર્ડ મેળવવા પ્રયાસ કરે છે, જેથી ડુપ્લિકેટ SIM કાર્ડ પર મેળવેલા OTPની મદદથી ડિજિટલ ટ્રાન્ઝેક્શન્સ કરી શકાય.
- દગાખોરો સામાન્ય રીતે નેટવર્ક કંપની માંથી હોવાનો ડોળ કરીને ગ્રાહકોને કૉલ કરે છે અને 3G થી 4Gમાં મફત અપગ્રેડ કે પછી SIM કાર્ડ પર બોનસ જેવી ઑફરોની બદલીમાં માહિતીની માંગણી કરે છે.

સુરક્ષા સૂચનો

- જો તમારા મોબાઈલમાં લાંબા સમય સુધી મોબાઈલ નેટવર્ક ન મળે તો શંકા ઊભી કરો.
- મોબાઈલ ઑપરેટરને કૉલ કરીને સુનિશ્ચિત કરો કે તમારા SIM માટે કોઈ ડુપ્લિકેટ સિમનો ઉપયોગ તો નથી થઈ રહ્યો.

બનાવટી દસ્તાવેજો સાથે દગા ભરી લોન

દગાખોરી

- આવા દગાઓ ત્યારે થાય છે જ્યારે કોઈ વ્યક્તિ અથવા સંસ્થા નાણાકીય સંસ્થાઓ પાસેથી કોઈપણ પ્રકારની સેવાઓ મેળવવા બનાવટી દસ્તાવેજોનો ઉપયોગ કરે છે.
- આવા દગાઓ કોઈ સંસ્થા સાથે NBFC કર્મચારી/NBFCના ઈમેઈલ આઈડીની ખાતરી કર્યા વગર KYC સંબંધિત દસ્તાવેજો શૅર કરતી વખતે થાય છે.
- પીડિત વ્યક્તિની વ્યક્તિગત માહિતી જેવી કે ઓળખ પત્રો, બેંક અકાઉન્ટની વિગતો ઈત્યાદિ ચોરી કરીને ઓળખ ચોરવાના આધારે લોન મંજૂર પણ કરવામાં આવે છે અને નાણાકીય સંસ્થા પાસેથી લાભો મેળવવા આ માહિતીનો ઉપયોગ કરાય છે.

સુરક્ષા સૂચનો

- તમારા ક્રીડેન્શિયલ્સ શૅર કરતા પહેલા હંમેશા NBFC કર્મચાર/કંપનીની પ્રમાણભૂતતાની ખાતરી કરી લો.
- ઓળખ ચોરી થતી ટાળવા તમારા ઓળખ પત્રો, બેંક અકાઉન્ટની વિગતો સલામત રાખો.

આધાર OTPમાં બાંધછોડ

દગાખોરી

- આધાર આધારિત OTP સાથે ડિજિટલ અકાઉન્ટ્સ ખોલાવી શકાય છે.
- એવી ઘટનાઓ પણ બની છે જેમાં ગ્રાહકો તેમનો UIDAI OTP ૩જા પક્ષકાર વેન્ડર્સ સાથે શૅર કરે છે અને આમ દગાખોરોને બેનામી અકાઉન્ટ્સ તૈયાર કરવામાં મદદ કરે છે.

સુરક્ષા સૂચનો

- ખાતરી ન કરેલ સંસ્થાઓ સાથે તમારો આધાર OTP શૅર કરશો નહીં.
- કોઈપણ માહિતી શૅર કરતા પહેલા જે તે વ્યક્તિની ઓળખ હંમેશા ચકાસી લો.

એચ ડી એફ સી બેંક

INDIA'S No.1* BANK

SECURE BANKING

વધુ વિગતો માટે,
એચડીએફસી બેંકના સીક્યોર બેંકિંગ પાનાની મુલાકાત કરો.
https://www.hdfcbank.com/personal/useful-links/security

*રિટેલ લોન બૂક સાઇઝ પર આધારિત (મોર્ગેજીસ સિવાય). સ્રોત : વાર્ષિક રિપોર્ટ FY 19–20
અને નં. 1 માર્કેટ કૅપિટલાઈઝેશન 31મી ડિસેંબર 2020 ના BSE ડાટા પર આધારિત.