HSBC

ઓનલાઈન સિક્યુરિટી અને સંરક્ષિત ઉપયોગિતા માર્ગદર્શિકા

તમારા ઓનલાઈન બેન્ક વ્યવહાર સંરક્ષિત રાખવા માટે અમે નીચે મુજબ મદદરૂપ થઈ શકીએ છીએ.

બેન્ક તરીકે અમે સલામતી વિશે વિચારવા ટેવાયેલા છીએ. ઈન્ટરનેટની વૃદ્ધિએ આપણા બધાને ઉત્તમ સાનુકૂળતા આપી છે, પરંતુ તે નવાં જોખમો પણ લાવે છે, જેની સામે રક્ષણ આવશ્યક હોય છે. એચએસબીસીમાં અમે ઉદ્યોગના ધોરણની સલામતી ટેકનોલોજી અને વ્યવહારોનો ઉપયોગ કરીએ છીએ, જે ત્રણ મુખ્ય વિસ્તારો પર ધ્યાન કેન્દ્રિત કરે છેઃ ગોપનીયતા, ટેકનોલોજી અને કોઈ પણ અનધિકૃત પહોંચથી તમારા ખાતાના રક્ષણની ઓળખ.

તો તમારા ઓનલાઈન બેન્ક વ્યવહારનું રક્ષણ અમે કઈ રીતે કરીએ અને તમારી પોતાની ઓનલાઈન સલામતી સુધારવા માટે તમે પણ કેવાં પગલાં લઈ શકો તે વિશે આગળ વાંચો.

છેતરપિંડીના પ્રકાર

ઠગો તમારી અંગત અને સલામતીની વિગતો તેમને આપવા માટે તમને ફસાવવા ઘણી બધી રીત અજમાવી શકે છે. તેઓ આ વિગતો પછી બેન્ક સાથે તમારી નાણાકીય માહિતીને પહોંચ મેળવવા માટે ઉપયોગ કરે છે અને તમારા અકાઉન્ટમાંથી તેમના અકાઉન્ટમાં નાણાં ફેરવે છે.

તમને સામનો કરવો પડી શકે એવા છેતરપિંડીના અમુક વધુ સામાન્ય પ્રકાર નીચે મુજબ છે.

ક્રેડિટ / ડેબિટ કાર્ડનું સ્કિમિંગ અથવા ક્લોનિંગ

ઠગો તમારા ક્રેડિટ અથવા ડેબિટ કાર્ડ પર મેગ્નેટિક પટ્ટી પરની માહિતી ચોરી શકે છે. તેઓ એટીએમના કાર્ડ સ્લોટમાં સ્કિમિંગ ડિવાઈસીસ છુપાવીને અથવા તમારું મર્ચન્ટ પેમેન્ટ ટર્મિનલ્સ ખાતે તમારું ધ્યાન નહીં હોય ત્યારે આવું કરી શકે છે. આ ડિવાઈસીસ તમારા કાર્ડની વિગતો સ્કેન અને સ્ટોર કરી શકે છે. તમારો પિન ચોરી કરવા માટે ઠગો એટીએમમાં અથવા વેપારી આસ્થાપના ખાતે તમારું ધ્યાન નહીં જાય તે રીતે કેમેરા ગોઠવી શકે છે.

યુપીઆઈ એપ્સમાં સ્કેમ અથવા પેમેન્ટની છેતરપિંડી

ઠગો મેસેજિંગ એપ્સ થકી તમને ક્યુઆર કોડ્સ મોકલીને તમને ક્યુઆર કોડ સ્કેન કરવા અથવા તેમના અકાઉન્ટમાં નાણાં ફેરવવા માટે 'કલેક્ટ' વિનંતી મંજૂર કરવા પૂછે છે. તેઓ બોગસ વાર્તા કહીને તમને છેતરવાનો પ્રયાસ કરી શકે છે, જેમ કે, તમે વેચી રહ્યા છો પ્રોડક્ટ તેમને ખરીદી કરવી છે. તેઓ તમારે માટે રિફંડ્સ, દાવો નહીં કરેલી કેશ બેક ઓફરો અથવા રિવોર્ડ પોઈન્ટ્સની પ્રક્રિયા કરવાની ઓફર કરીને બેન્ક અથવા શોપિંગ કંપનીના એક્ઝિક્યુટિવને નામે તમને છેતરી શકે છે. અજાણ પીડિત પછી ક્યુઆર કોડ સ્કેન કરી શકે અથવા તેમના યુપીઆઈ પિનનો ઉપયોગ કરીને 'કલેક્ટ' વિનંતી મંજૂર કરતાં ઠગના અકાઉન્ટમાં નાણાં ફેરવાઈ શકે છે.

બિઝનેસ મેઈલ્સ અને મેસેજિંગ એપ્સ થકી પેમેન્ટ છેતરપિંડી

ઠગો તમારા વિશે વધુ જાણવા માટે તમારા ઈમેઈલ્સ અથવા ચેટ્સ હેક કરી શકે અથવા એન્ક્રિપ્ટેડ મેસેજીસ આંતરી શકે છે. તેઓ તમારા વિશે જાણી જાય પછી તેઓ હેક / બાંધછોડ / સ્પૂફ કરેલી આઈડી પરથી મેસેજીસ મોકલીને તમને વાસ્તવિક લાગે તેવા હેતુઓ માટે તુરંત પેમેન્ટ કરવા માટે તમને પૂછી શકે છે, જેમ કે, વહાલાજનને હોસ્પિટલમાં દાખલ કરાયો છે અથવા બાકી બિલ નવા અકાઉન્ટમાં ચૂકવવાની જરૂર છે અથવા તેમની વિનંતી પર તેઓ ભરોસો રાખી શકે એવું લાગે છે, એવું કહીને છેતરી શકે છે. પીડિત જાતે પેમેન્ટ કરે ત્યારે બેન્ક દ્વારા તેમને લેણદેણ એલર્ટસ મોકલવામાં નહીં આવે. આથી આ પ્રકારની છેતરપિંડી શોધી કાઢવાનું મુશ્કેલ બને છે.

નકલી સંપર્ક નંબરો

ઠગો બેન્કો અને સેવા પ્રદાતા સંપર્ક કેન્દ્રો માટે નકલી સંપર્ક વિગતો આપી શકે છે. અજાણ પીડિત સર્ચ એન્જિનનો ઉપયોગ કરીને સંપર્ક વિગતો જોઈ શકે છે અને બોગસ નંબર પર કોલ કરી શકે છે. તેઓ તે પછી "વેરિફિકેશન પ્રક્રિયા'' થકી લઈ જાય છે, જ્યાં તેમને તેમના ડેબિટ / ક્રેડિટ કાર્ડ અને બેન્ક અકાઉન્ટ વિશે સંવેદનશીલ માહિતી આપવા માટે છેતરવામાં આવે છે.

તમે હંમેશાં તમને જરૂરી સંપર્ક વિગતો જોતા હોય તે બેન્ક અથવા સેવા પ્રદાતાની વિધિસર વેબસાઈટની જ વિઝિટ કરવાની ખાતરી રાખીને પોતાનું રક્ષણ કરી શકો છો. સતર્ક રહો અને ખાસ કરીને મોબાઈલ નંબર હોય તો સૌપ્રથમ તપાસ કર્યા વિના સર્ચ રિઝલ્ટ્સમાં પ્રદર્શિત નંબરો પર કોલ કરવાનું ટાળવું જોઈએ.

ઈમેઈલ્સનું ફિશિંગ અથવા સ્પૂફિંગ

ઠગો શક્ય તેટલા ઘણા બધા ઈમેઈલ એડ્રેસ ઈમેઈલ પર મોકલીને પીડિતને ફિશ કરી શકે છે. તેઓ બેન્ક, ઓનલાઈન પેમેન્ટ સર્વિસ, રિટેઈલર કે અન્ય આવી સેવાઓ જેવી કાયદેસર સંસ્થાનો હિસ્સો હોવાનો દેખાડો મોટે ભાગે કરે છે. તેઓ તેમની આઈડી સ્પૂફ કરે છે, જેથી ઈમેઈલ ઠગ સિવાયની કોઈકે મોકલ્યો હોય તેવું લાગે છે.

તમારે અંગત અથવા નાણાકીય માહિતી પૂછતા ઈમેઈલ્સને પ્રતિસાદ નહીં આપીને ફિશિંગ સ્કેમ સામે પોતાનું રક્ષણ કરવું જોઈએ. તમારે શંકાસ્પદ ઈમેઈલ્સની લિંક્સ ક્યારેય સિલેક્ટ નહીં કરવી જોઈએ.

એચએસબીસી ઈમેઈલથી તમારી અંગત અથવા સલામતીની વિગતો જાહેર કરવા ક્યારેય પૂછતી નથી. જો તમને પ્રાપ્ત ઈમેઈલ એચએસબીસી પાસેથી આવ્યો હોવાનો દાવો કરવામાં આવે તો તેને પ્રતિસાદ નહીં આપો. ઈમેઈલ તુરંત ડિલીટ કરો. અને યાદ રાખો, તમારી ક્રિડેન્શિયલ્સ ક્યારેય કોઈને પણ આપવી નહીં, જેમ કે, તમારું યુઝરનેમ, પાસવર્ડ અથવા અન્ય સલામતીની વિગતો.

મની મુલ અથવા વધારાની આવકના ઈમેઈલ સ્કેમ્સ

મની મૂલ સ્કેમમાં ઠગ તમને નાણાં ટ્રાન્સફર કરવામાં મદદ કરવા પૂછી શકે છે. તેઓ તમારા અકાઉન્ટમાં નાણાં ટ્રાન્સફર કરવાની ઓફર કરી શકે છે, જેથી તમે અન્ય અકાઉન્ટમાં નાણાં ટ્રાન્સફર કરવા તમે મદદ કરી શકો. આ સામે તેઓ તમને કમિશન આપવાની લાલચ આપે છે.

તમારા આવી વિનંતીઓની અવગણના કરવી જોઈએ, કારણ કે તેમાં મોટે ભાગે મની લોન્ડરિંગ જેવા ગુના સંકળાયેલા હોય છે. જો કોઈ પણ જ્ઞાત રીતે સહભાગી થાય તો ગુનામાં સાગરીત ગણવામાં આવી શકે અને કાનૂની પગલાંનો સામનો કરવો પડી શકે છે. જો સાચા જેવું જ દેખાતું હોય તો તે સંભવિત રીતે ઠગાઈ છે !

એડવાન્સ ફી છેતરપિંડી ('419' સ્કેમ)

ઠગો સામાન્ય રીતે યુએસ ડોલરમાં તમને અધધધ મોટી રકમ લાવવામાં તેમને મદદરૂપ થવા માટે આકર્ષક પુરસ્કાર ઓફર કરતા અનિચ્છનીય પત્રો અથવા ઈમેઈલ્સ મોકલી શકેછે. આ ઠગો વાસ્તવમાં તમારા બેન્ક વ્યવહારની વિગતો મેળવવા માગતા હોય છે. તેઓ સામાન્ય રીતે સોદો પૂરો કરવા માટે ફી, અમુક કર અથવા લાંચ ચૂકવવા માટે પૂછી શકે છે, જેને એડવાન્સ ફી કહેવાય છે. પીડિતો સામાન્ય રીતે આવા ઠગની વાતોમાં આવી જતા હોય છે.

જો તમને શંકા હોય કે તમારી ઓનલાઈન બેન્ક વ્યવહારની વિગતો કોઈકની પાસે છે તો તમારે ઓનલાઈન બેન્કિંગ પર લોગઓન કરીને તુરંત પાસવર્ડ બદલી નાખવો જોઈએ. તમારે અમને સતર્ક કરવા માટે તુરંત કોલ પણ કરવો જોઈએ. અમારી લાઈન 24/7* ચાલુ હોય છે. અઅમારા હોટલાઈન નંબરોની યાદી અહીં આપવામાં આવી છે.

સોશિયલ મિડિયા હેક્સ

ઠગો ફેસબુક, વ્હોટ્સએપ અથવા ઈન્સ્ટાગ્રામ જેવાં સોશિયલ મિડિયા મંચો પર નિકટવર્તી મિત્ર કે સંબંધી તરીકે પોતાની ઓળખ આપીને તેમને તુરંત નાણાં ટ્રાન્સફર કરવા તમને પૂછી શકે છે. આ વિનંતી તમે જાણો છો તેની પાસેથી જ કરાઈ છે કે કેમ તેની ખાતરી કરવા તમારે તેમને કોલ કરવો જોઈએ અથવા અન્ય માધ્યમથી સંપર્ક કરીને જાણી લેવું જોઈએ.

વિશિંગ કોલ્સ

ઠગો બેન્કના કર્મચારી અથવા કસ્ટમર સર્વિસ એક્ઝિક્યુટિવ હોવાનું જણાવે છે અને સંભવિત પીડિતની બેન્ક અકાઉન્ટની વિગતો જેવી સંવેદનશીલ માહિતી ચોરી કરવા કોલ કરે છે. પીડિતનો વિશ્વાસ જીતવા માટે ઠગો પીડિતને તેની અમુક અંગત માહિતી આપી શકે છે, જે તેણે સોશિયલ એન્જિનિયરિંગ થકી ચોરેલી હોય છે. તેઓ થોડો વિશ્વાસ સંપાદન કર્યા પછી પીડિત તેમની બેક વિગતો અને વન–ટાઈમ પાસકોડ (ઓટીપી) જેવી તેમની ગોપનીય માહિતી આપી દેશ એવી આશામાં અમુક વિશેષ સેવા કે પ્રોડક્ટ ઓફર કરી શકે છે.

ટ્રોજન વાઈરસીસ

ઠગો એવા અનિચ્છનીય ઈમેઈલ્સ તમને મોકલી શકે છે, જેમાં ફાઈલ્સ, પેજીસ અથવા એટેચમેન્ટ્સ હોઈ શકે છે, જે તમને ખોલવા માટે પૂછવામાં આવે છે. જોકે તે ખોલતાં જ તમારા કોમ્પ્યુટરમાં ગોપનીય રીતે પ્રોગ્રામ ઈન્સ્ટોલ થઈ જાય છે, જેના થકી ઠગ તમારી ઓનલાઈન પ્રવૃત્તિઓ અને વિવિધ વેબસાઈટ્સ પર તમે શું ટાઈપ કરી રહ્યા છો તેની પર દેખરેખ રાખી શકે છે. આથી તમે ઓનલાઈન શોપિંગ કરતી વખતે તમારા ક્રેડિટ કાર્ડની વિગતો એન્ટર કરો ત્યારે ઠગ તમે એન્ટર કરતા હોય તે માહિતી જોઈ શકે છે.

ઓનલાઈન સલામતી માટે એચએસબીસી દ્વારા લેવાયેલાં પગલાં

બહુ-સ્તરીય લોગ ઓન વેરિફિકેશન

તમારી નાણાકીય માહિતીનું અજોડ યુઝરનેમ અને પાસવર્ડ તેમ જ તમારા પ્રત્યક્ષ સિક્યુરિટી ડિવાઈસ અને ડિજિટલ સિક્યોર કી દ્વારા ઊપજાવવામાં આવતા વન– ટાઈમ સિક્યુરિટી કોડના અત્યાધુનિક સંયોજનથી રક્ષણ કરવામાં આવે છે.

લેણદેણ વેરિફિકેશન

કાર્ડસ પર 3ડી સંરક્ષિત લેણદેણ પેમેન્ટ પ્રણાલીમાં લેણદેણ અને ભરોસો સંરક્ષિત રાખવામાં મદદ કરે છે. ક્યારેય કોઈને પણ લેણદેણ માટે ઊપજાવેલો ઓટીપી આપવો નહીં.

128- બિટ સિક્યોર સોકેટ લેયર (એસએસએલ) એન્ક્રિપ્શન

એચએસબીસી ઈન્ટરનેટ બેન્કિંગ સત્ર દરમિયાન પરિવર્તિત માહિતી માટે 128– બિટ સિક્યોર સોકેટ લેયર (એસએસએલ) એન્ક્રિપ્શનનો ઉપયોગ કરે છે, જે એન્ક્રિપ્શન માટે ઉદ્યોગનું ધોરણ તરીકે સ્વીકાર્ય છે.

ઓટોમેટિક 'ટાઈમ-આઉટ' વિશિષ્ટતા

સલામતીનાં પગલાં તરીકે તમારું ઈન્ટરનેટ બેન્કિંગ સત્ર ઉપયોગ નહીં કર્યાના સમયગાળા પછી આપોઆપ બંધ અથવા ટાઈમ– આઉટ થઈ જશે. તમારે હંમેશાં તમારું ઈન્ટરનેટ બેન્કિંગ સત્ર પૂરું થયા પછી ક્લોઝ કરી દેવું જોઈએ.

સિક્યુરિટી ડિવાઈસ / ડિજિટલ સિક્યોર કી

તમારી પ્રત્યક્ષ સિક્યુરિટી ડિવાઈસ / ડિજિટલ સિક્યોર કી ઓનલાઈન સલામતીને નવી ઊંચાઈએ લઈ જાય છે. તમારા અકાઉન્ટમાં લોગઓન કરવા માટે તમારે સામાન્ય મુજબ તમારું મોજૂદ યુઝરનેમ અને પાસવર્ડ એન્ટર કરવાનું રહે છે, જે પછી તમારી પ્રત્યક્ષ સિકયુરિટી ડિવાઈસ અથવા ડિજિટલ સિક્યોર કી દ્વારા ઊપજનારો યુનિટ સિક્યુરિટી કોડ એન્ટર કરવાનો રહે છે. આ બે પગલાંની ઓથેન્ટિકેશન પ્રક્રિયા તમે ઈન્ટરનેટ બેન્કિંગ કરો ત્યારે ત્યારે સલામતીનું બહેતર કવચ તમને પૂરું પાડે છે.

ઓનલાઈન સલામતીમાં તમારી ભૂમિકા

ઈન્ટરનેટ બેન્કિંગની સલામતીની ખાતરી રાખવા માટે શું કરવું જોઈએ અને શું નહીં કરવું જોઈએ:

શું કરવું જોઈએ:

- તમારું કોમ્પ્યુટર સર્વ સમયે નવા એન્ટી– વાઈરસ અને ફાયરવોલ પ્રોટેકશન સોફ્ટવેરથી સુરક્ષિત હોય તેની ખાતરી રાખો. તમને નવામાં નવું રક્ષણ મળે તેની ખાતરી રાખવા માટે નિયમિત અપડેટ્સ ડાઉનલોડ કરો.
- પાસવર્ડ તમને યાદ રહે એવો ચૂંટો પણ અન્ય કોઈ આસાનીથી અનુમાન લગાવી શકે એવો નહીં હોવો જોઈએ. પાસવર્ડમાં આલ્ફા અને ન્યુમેરિક કેરેક્ટર્સનું સંયોજન હોય તો સામાન્ય રીતે અનુમાન લગાવવાનું મુશ્કેલ હોય છે.(દા.ત. a7g3cy91)
- તમારો ઈન્ટરનેટ બેન્કિંગનો પાસવર્ડ નિયમિત ધોરણે બદલતા રહો.
- ફિશિંગ ઈમેઈલ્સથી સાવધાન. હંમેશાં સર્વ અક્ષરો અને કેરેક્ટર્સ સહિત આખું ઈમેઈલ એડ્રેસ ધ્યાનથી વાંચો.
- ફિશિંગમાં બોગસ હોવા છતાં અત્યંત સમાન દેખાતા ઈમેઈલ એડ્રેસ હોય છે, દા.ત. hsdc.co.in અથવા hsbcbank.com. આવા સંજોગોમાં તેનું અસલ ડેસ્ટિનેશન જાણવા માટે યુઆરએલ પર તમારું માઉઝનું પોઈન્ટર ફેરવો, જે તમારા બ્રાઉઝરના તળિયે ડાબે ખૂણે પ્રદર્શિત થશે. જો સુમેળ નહીં ખાતો હોય તો લિંક પર ક્લિક નહીં કરો. યુઆરએલમાં અક્ષરોમાં ભૂલ, ખોટું વ્યાકરણ કે આગળપાછળ થઈ ગયેલા અક્ષરો જેવાં ચિહનોનું ધ્યાન રાખો.
- જો તમારા અકાઉન્ટમાં ઉમેરાયેલા લાભાર્થીઓની આવશ્યકતા નહીં હોય તો તેને ડિલીટ કરો.
- લોગઓન વિગતો યાદ રાખતી તમારા કોમ્પ્યુટર કે બ્રાઉઝર પરની ફંકશનાલિટી ડિઝેબલ કરો.
- તમારી પ્રણાલી અને વેબ બ્રાઉઝર અપડેટેડ રાખો. ઉત્પાદકો નિયમિત રીતે તેમની પ્રણાલીઓ અને બ્રાઉઝરોમાં નબળાઈઓની ખોજ કરે ત્યારે સિક્યુરિટી પેચીસ જારી કરે છે. આ અપડેટ્સ માટે તમારા સોફ્ટવેર પ્રદાતા પાસે નિયમિત ધોરણે તપાસ કરાવો.
- એચએસબીસીની વેબસાઈટ પર પહોંચવા માટે બ્રાઉઝરમાં હંમેશાં બેન્કની યુઆરએલ ટાઈપ કરો.
- પેડલોક સિમ્બોલ અને સાઈટ સર્ટિફિકેટ ચેક કરો. એચએસબીસી ઓનલાઈન બેન્કિંગમાં લોગઈન કરો ત્યારે સાઈટ સર્ટિફિકેટ એચએસબીસીનું જ છે તેની ખાતરી રાખવા માટે તમારા બ્રાઉઝરના તળિયે પેડલોક સિમ્બોલ પર ડબલ ક્લિક કરો. આને કારણે 'ફેક' સાઈટ પર તમારી વિગતો એન્ટર કરવામાં તમે છેતરાશો નહીં.
- તમારાં ખાતાં નિયમિત તપાસ કરતાં રહો. જો કોઈ લેણદેણ અંગે શંકા હોય તો વિગતો નોંધ કરો અને અમને કોલ કરો.
- હંમેશાં ઓનલાઈન બેન્કિંગનો ઉપયોગ કર્યા પછી લોગ–આઉટ કરો. ફક્ત લોગ–આઉટ બટન સિલેક્ટ કરો અને ક્યારેય સેવામાં લોગ કર્યું હોય ત્યારે તમારું પીસી છોડીને જવું નહીં.
- જો તમે બેન્કનો કસ્ટમર કેર નંબર, ઓનલાઈન શોપિંગ વેબસાઈટ વગેરે જોતા હોય તો ઈન્ટરનેટ પર સૂઝબૂઝપૂર્વક સર્ચ કરો. ઠગો તેમના દ્વારા ઉપયોગ કરાતા મોબાઈલ નંબરો સાથે રિઝલ્ટ રિટર્ન આવે તે માટે સર્ચમાં ચેડાં કરે છે. તમને બેન્કના કસ્ટમર કેર નંબર કે ઈ–કોમર્સ વેબસાઈટને બદલે ઠગ દ્વારા કોલ કરીને ઠગવામાં આવી શકે છે.
- તમારા બેન્કના સંપર્ક કેન્દ્રનો નંબર તમારા ડિવાઈસીસમાં સ્ટોર કરો અથવા તમારા ક્રેડિટ / ડેબિટ કાર્ડની પાછળ લખેલો નંબર જુઓ.
- કાર્ડ નંબર અને સમાપ્તિ તારીખો ઓનલાઈન વેબસાઈટ પર સ્ટોર કરવા સમયે સાવચેતી રાખો. આ વિગતો ભાગ્યે જ ઉપયોગ કરાતી વેબસાઈટની બિન– ભરોસાપાત્ર વેબસાઈટ પર સ્ટોર નહીં કરો.
- તમારા પર્સનલ કોમ્પ્યુટર કે મોબાઈલ ડિવાઈસીસ પર સ્ક્રીન શેરિંગ એપ્લિકેશન્સથી સતર્ક રહો. ઠગો આવા એપ્લિકેશન ડાઉનલોડ કરવા અને તમારી પાસેથી કોડ માગીને એક્સેસ મેળવવા પ્રેરિત કરી શકે છે. એક્સેસને મંજૂરી આપતાં જ તેઓ રિમોટથી તમારું ડિવાઈસ જોઈ / નિયંત્રણ કરીને તમારા ખાતામાંથી ચુકવણી પણ કરી શકે છે.
- તમારું ઈન્ટરનેટ કનેકશન સંરક્ષિત રાખો. હંમેશાં તમારા ઘરનું વાયરલેસ નેટવર્ક પાસવર્ડથી સુરક્ષિત રાખો.
- કમિશન કે મદદ માટે પણ તમારા ખાતામાં નાણાં જમા કરવાની જેમાં જરૂર પડે તે યોજના / ઓફર વિશે સાવચેત રહો. ઠગ તમારા ખાતામાં ગુનાની પ્રાપ્તિઓ મોકલી શકે છે અને તેમને નાણાં ટ્રાન્સફર કરવા કે રોકડ પૂરી પાડવા પૂછી શકે છે. ઠગો નાણાંનું પગેરું રાખવા માગતો નથી અને તેથી તમને મની મ્યુલ તરીકે ઉપયોગ કરી શકે છે.
- છેતરપિંડીની જાણ કરવા તુરંત બેન્કનો સંપર્ક કરો.

શું નહીં કરવું જોઈએ

- તમે અન્ય સેવા માટે ઉપયોગ કરતા હોય તેવો પાસવર્ડ ઉપયોગ નહીં કરો. તમારો પાસવર્ડ ઈન્ટરનેટ બેન્કિંગને અજોડ હોવો જોઈએ.
- ઈમેઈલ / એસએમએસમાં લિંક ખૂલી જાય તેવા વેબપેજીસ પર તમારી યુઝર આઈડી, પાસવર્ડ, કાર્ડ નંબર, સમાપ્તિ તારીખ, સીવીવી વગેરે જેવી વિગતો જાહેર નહીં કરવી જોઈએ.
- જો આઈટી વિભાગ, આરબીઆઈ વગેરે જેવી સરકારી સંસ્થા અથવા બેન્ક કર્મચારી હોવાનો દાવો કરીને આવી વિગતો માટે પૂછે તો પ્રતિસાદ નહીં આપો. એચએસબીસીના કોઈ પણ કર્મચારી ક્યારેય આ વિગતો માટે કોલ કરતા નથી કે પૂછતા નથી.
- તમારું ઈન્ટરનેટ બેન્કિંગ યુઝરનેમ સાથે તમારો પાસવર્ડ એકત્ર લખશો નહીં. તમારો પાસવર્ડ ઓળખક્ષમ ફોર્મેટમાં લખશો નહીં અને તમારી પ્રત્યક્ષ સિક્યુરિટી ડિવાઈસ / ડિજિટલ સિક્યોર કી સાથે વિગતો તમારા લોગઓન પર છોડવી નહીં.
- તમારું મોબાઈલ બેન્કિંગ એપ્લિકેશન અપડેટેડ રાખો. તે ડાઉનલોડ અને તેની પર કોઈ પણ અપડેટ કરવા માટે તમારા ડિવાઈસની વિધિસર એપ સ્ટોરની વિઝિટ કરો.
- ક્યારેય અવિશ્વસનીય સ્રોતોમાંથી ઈમેઈલમાં લિંકમાંથી મોબાઈલ બેન્કિંગ / પેમેન્ટ એપ્લિકેશન્સ ડાઉનલોડ નહીં કરવું જોઈએ.
- તમારો કાર્ડ નંબર અને સમાપ્તિ તારીખો ઓનલાઈન વેબસાઈટ્સ પર ક્યારેય સ્ટોર નહીં કરવી. ભાગ્યેજ ઉપયોગ કરાતી વેબસાઈટ્સની અવિશ્વસનીય વેબસાઈટ્સ પર આ વિગતો સ્ટોર નહીં કરો.
- તમારો પિન કોઈને આપશો નહીં. પોતે ઉપયોગ કરો. તમારા પિન સાથે બાંધછોડ થઈ હોવાની શંકા જાય તો તે તુરંત બદલી કરો.

જો તમને યુપીઆઈ પિન માટે પૂછવામાં આવે તો યાદ રાખો કે તમે ચુકવણી કરી રહ્યા છો અને ચુકવણી પ્રાપ્ત કરવા સમયે તમને યુપીઆઈ પિનની જરૂર નથી.

જાહેર કોમ્પ્યુટરોનો ઉપયોગ કરવા સમયે સતર્ક રહો.

હંમેશાં આ યાદ રાખોઃ

- જો તમે થોડી વાર માટે પણ કોમ્પ્યુટર છોડીને જતા હોય તો લોગ આઉટ કરો. જો શક્ય હોય તો લોગઈન નહીં કરો ત્યાં સુધી કોમ્પ્યુટર છોડી જવું નહીં.
- કોમ્પ્યુટરમાંથી લોગઆઉટ કરવા પૂર્વે તમારા બ્રાઉઝિંગ ઈતિહાસને ડિલીટ કરો. ઈન્ટરનેટ બ્રાઉઝરો તમારા પાસવર્ડ અને તમે વિઝિટ કરેલા પેજની માહિતી સ્ટોર કરે છે. ઈન્ટરનેટ બ્રાઉઝરના ટૂલ્સ મેનુમાં જાઓ અને ઓપ્શન્સ કે ઈન્ટરનેટ ઓપ્શન્સ સિલેક્ટ કરો. બ્રાઉઝર કોઈ ઓટો કમ્પ્લીટ ફંકશન બંધ ધરાવતું નથી ને તેની ખાતરી રાખો, કોઈ પણ કૂકીઝ ડિલીટ કરો અને હિસ્ટરી ક્લિયર કરો.
- લાઈબ્રેરીઓ, ઈન્ટરનેટ કેફે અને સ્કૂલો સહિત પબ્લિક કોમ્પ્યુટરનો ઉપયોગ તમારા બેન્ક વ્યવહાર માટે કરવાનું ટાળો.

સંવેદનશીલ માહિતી ટાઈપ કરવાનું ટાળો. જો તમે બધી સાવચેતીઓ રાખો તો પણ જાહેર કોમ્પ્યુટર પર કીસ્ટ્રોક લોગર નામે બદઈરાદાભર્યું સોફ્ટવેર ડાઉનલોડ કરવામાં આવેલું હોઈ શકે છે. આ પ્રોગ્રામ તમારો પાસવર્ડ, ક્રેડિટ કાર્ડ નંબર અને બેન્કની વિગતો ચોરી શકે છે. સંવેદનશીલ માહિતી ચોરાઈ શકે તેવી કોઈ પણ નાણાકીય લેણદેણ નહીં કરવી જોઈએ.

મહત્ત્વપૂર્ણઃ જો તમને એચએસબીસીનો હોવાનો દાવો કરતા પણ અવિશ્વસનીય સ્રોતમાંથી ઈમેઈલ પ્રાપ્ત થાય અથવા અંગત માહિતી પૂછતો અનિચ્છનીય ઈમેઈલ આવે તો વધુ તપાસ માટે તેને અમારી પાસે **phishing@hsbc.com** પર રિપોર્ટ કરો.