પરિશિષ્ટ 7: ગ્રાહક જાગૃતિ-સાયબર ધમકીઓ અને છેતરપિંડી

એવું જોવામાં આવ્યું છે કે અનૈતિક તત્વો સોશિયલ મીડિયાની ટેકનિકો, મોબાઈલ ફોન કોલ્સ વગેરે સહિતની નવીન કાર્યપ્રણાલીનો ઉપયોગ કરીને લોકોને છેતરે છે અને ગેરમાર્ગે દોરે છે. આ બાબતને ધ્યાનમાં રાખીને, ડીસીબી બેંક લોકોને બેંકો અને નાણાકીય સેવા પ્રદાતાઓ તરફથી કોઈપણ રીતે છૂટ મેળવવા/ઝડપી પ્રતિસાદ મેળવવામાં મદદનું વચન આપતા છેતરપિંડીભર્યા સંદેશાઓ, બનાવટી કોલ્સ, અજાણી લિંક્સ, ખોટા નોટિફિકેશન્સ, અનધિકૃત QR કોડ્સ, વગેરેથી સાવચેત રહેવાની ચેતવણી આપે છે.

છેતરપિંડી કરનારાઓ યુઝર આઈડી, લોગઈન/ટ્રાન્ઝક્શન પાસવર્ડ, વન ટાઈમ પાસવર્ડ (ઓટીપી), ડેબિટ/ક્રેડિટ કાર્ડની વિગતો જેવી કે પિન, સીવીવી, એક્સપાયરી ડેટ અને અન્ય વ્યક્તિગત માહિતી જેવી ગોપનીય વિગતો મેળવવાનો પ્રયાસ કરે છે. છેતરપિંડી કરનારાઓ દ્વારા ઉપયોગમાં લેવાતી ખાસ કાર્યપ્રણાલી નીચે મુજબ છેઃ

- KYC–અપડેટ કરવા, એકાઉન્ટ/સિમ કાર્ડને અનબ્લોક કરવા, ડેબિટ થયેલી રકમ ક્રેડિટ કરવા વગેરેના બહાના હેઠળ ગ્રાહકોને ગોપનીય વિગતો તેમને આપવા લલચાવવા માટે બેંક/નોન–બેંક ઈ–વોલેટ પ્રદાતાઓ/ટેલિકોમ સેવા પ્રદાતાના હોવાનો ડોળ કરતા વિશિંગ–ફોન કોલ્સ.
- ફિશિંગ – નકલી ઈમેઈલ અને/અથવા એસએમએસ જે ગ્રાહકોને એમ વિચારીને છેતરવા માટે બનાવવામાં આવેલા છે કે સંદેશાવ્યવહાર તેમની બેંક/ઈ–વોલેટ પ્રદાતા પાસેથી મળ્યો છે અને તે ગોપનીય વિગતો મેળવવા માટેની લિંક્સ ધરાવતી હોય છે.
- રિમોટ એક્સેસ – ગ્રાહકોને તેમના મોબાઈલ ફોન/કમ્પ્યુટર પર ઍપ્લિકેશન ડાઉનલોડ કરવા માટે લલચાવીને જે ગ્રાહકના ઉપકરણમાંથી ડેટા મેળવી કરી શકે છે.
- નાણાં મેળવવા માટે 'તમારો UPI પિન દાખલ કરો' જેવા સંદેશાઓ સાથે ચુકવણી માટેની નકલી વિનંતીઓ મોકલીને UPI ની 'કલેક્ટ રિક્વેસ્ટ' સુવિધાનો દુરુપયોગ કરે છે.
- વેબપેજ/સોશિયલ મીડિયા પર અને સર્ચ એન્જિન વગેરે દ્વારા બેંકો/ઈ–વોલેટ પ્રદાતાઓના નકલી સંપર્ક નંબરો પ્રદર્શિત થાય છે.

ડીસીબી બેંક કોઈપણ ડિજિટલ (ઓનલાઈન/મોબાઈલ) બેન્કિંગ/ચુકવણી ટ્રાન્ઝક્શન કરતી વખતે તમામ યોગ્ય સાવચેતીઓ રાખીને સુરક્ષિત ડિજિટલ બેન્કિંગનો ઉપયોગ કરવા લોકોને વિનંતી કરે છે. આ બાબત નાણાકીય અને/અથવા અન્ય નુકસાનને અટકાવવામાં મદદ કરશે.

સુરક્ષિત ડિજિટલ બેન્કિંગ પ્રથાઓ

- તમારા એકાઉન્ટની વિગતો જેવી કે, એકાઉન્ટ નંબર, લોગઈન આઈડી, પાસવર્ડ, PIN, UPI-PIN, OTP, ATM/ડેબિટ કાર્ડ/ક્રેડિટ કાર્ડની વિગતો ક્યારેય કોઈની સાથે શેર કરશો નહીં, બેંક અધિકારીઓ સાથે પણ નહીં, ભલે તે ગમે તેટલા સાચા લાગતા હોય.
- KYC અપડેટ કરવાના બહાને તમારા એકાઉન્ટને બ્લોક કરી દેવાની ધમકી આપતો કોઈપણ ફોન કોલ/ઈમેઈલ અને તેને અપડેટ કરવા માટે લિંક પર ક્લિક કરવાનું સૂચન એ છેતરપિંડી કરનારાઓની સામાન્ય કાર્યપ્રણાલી છે. KYC અપડેટ કરાવવાની/ઝડપથી કાર્ય કરાવવા માટેની ઓફરોનો જવાબ આપશો નહીં. હંમેશાં તમારી બેંક/એનબીએફસી/ઈ–વોલેટ પ્રદાતાની અધિકૃત વેબસાઈટનો ઉપયોગ કરો અથવા બ્રાંચનો સંપર્ક કરો.
- તમારા ફોન અથવા ઉપકરણ પર કોઈપણ અજાણી ઍપ્લિકેશન ડાઉનલોડ કરશો નહીં. ઍપ્લિકેશન તમારા ગોપનીય ડેટાને ગુપ્ત રીતે મેળવી શકે છે.
- નાણાંની રસીદ સાથે સંકળાયેલા ટ્રાન્ઝક્શન માટે બારકોડ અથવા QR કોડ સ્કેન કરવાની અથવા MPIN દાખલ કરવાની જરૂર નથી હોતી. આથી, જો આવું કરવાનું કહેવામાં આવે તો સાવચેતી રાખો.
- સંપર્ક વિગતો માટે હંમેશાં બેંક/એનબીએફસી/ઈ–વોલેટ પ્રદાતાની અધિકૃત વેબસાઈટનો ઉપયોગ કરો. ઈન્ટરનેટ સર્ચ એન્જિન પરના સંપર્ક નંબરો છેતરપિંડી કરનારા હોઈ શકે છે.
- ઈમેઈલ અને SMS માં મળતા URL અને ડોમેન નેમમાં સ્પેલિંગની ભૂલો તપાસો. ઓનલાઈન બેન્કિંગ માટે માત્ર ચકાસણી કરવામાં આવેલી, સુરક્ષિત અને વિશ્વસનીય વેબસાઈટ અને ઍપ્સનો ઉપયોગ કરો, એટલે કે ''https'' થી શરૂ થતી વેબસાઈટ. કોઈ શંકાસ્પદ URL અથવા વેબસાઈટ અંગે તાત્કાલિક સ્થાનિક પોલીસ/સાયબર ક્રાઈમ બ્રાંચને જાણ કરવી જોઈએ.

- જો તમારા દ્વારા શરૂ કરવામાં ન આવ્યું હોય તેવા ટ્રાન્ઝક્શન માટે તમારા એકાઉન્ટને ડેબિટ કરવા માટે તમે OTP મળ્યો, તો તરત જ તમારી બેંક/ઈ–વોલેટ પ્રદાતાને જાણ કરો. જો તમે કોઈ ટ્રાન્ઝક્શન ન કર્યું હોય અને ડેબિટ SMS મળે, તો તાત્કાલિક તમારી બેંક/ઈ–વોલેટ પ્રદાતાને જાણ કરો અને UPI સહિત ડેબિટના તમામ માર્ગોને બ્લોક કરી દો. જો તમને તમારા એકાઉન્ટમાં કોઈ છેતરપિંડીની પ્રવૃત્તિ થયાની શંકા હોય, તો ઈન્ટરનેટ/મોબાઈલ બેન્કિંગ માટે સક્ષમ કરવામાં આવેલા લાભાર્થીની યાદીમાં કરવામાં આવેલા વધારાની તપાસ કરો.
- તમારી બેંક/ઈ–વોલેટ એકાઉન્ટ સાથે લિંક કરેલ તમારા ઈમેઈલનો પાસવર્ડ શેર કરશો નહીં. તમારી પાસે ઈ–કોમર્સ/સોશિયલ મીડિયા સાઈટ્સ અને તમારા બેંક એકાઉન્ટ અને તમારા બેંક એકાઉન્ટ સાથે લિંક કરેલ ઈમેઈલ માટે એક જ પાસવર્ડ રાખશો નહીં. સાર્વજનિક, ખુલ્લા અથવા વિના મૂલ્યે વાઈ–ફાઈ અથવા ઈન્ટરનેટ નેટવર્ક દ્વારા બેન્કિંગ કરવાનું ટાળો.
- કોઈપણ વેબસાઈટ/ઍપ્લિકેશનમાં તમારા ઈમેઈલને યુઝર આઈડી તરીકે રજીસ્ટર કરાવતી વખતે તમારા ઈમેઈલ પાસવર્ડને ''પાસવર્ડ'' શબ્દ તરીકે સેટ કરશો નહીં. તમારા ઈમેઈલને ખોલવા માટે વપરાતો પાસવર્ડ, ખાસ કરીને જો તમારા બેંક એકાઉન્ટ સાથે લિંક કરવામાં આવેલ હોય, તો તે એકમાત્ર (યુનિક) હોવો જોઈએ અને તેનો ઉપયોગ માત્ર ઈમેઈલ ખોલવા માટે જ હોવો જોઈએ અને અન્ય કોઈ વેબસાઈટ અથવા ઍપ્લિકેશનને ખોલવા માટે નહીં.
- વિદેશથી મોકલવામાં આવતા નાણાં, કમિશનની રસીદ અથવા લોટરી જીતવા માટે તમારા વતી RBI માં નાણાં જમા કરાવવાની સૂચનાને કારણે ગેરમાર્ગે દોરાશો નહીં.
- તમારા નાણાકીય સેવા પ્રદાતા તરફથી એલર્ટ્સ માટે તમારા ઈમેઈલ અને ફોનના મેસેજ નિયમિતપણે તપાસો. તમારા એકાઉન્ટમાં કોઈપણ બિન–અધિકૃત ટ્રાન્ઝક્શનની જાણ તમારી બેંક/એનબીએફસી/સેવા પ્રદાતાને તાત્કાલિક કાર્ડ, એકાઉન્ટ, વોલેટને બ્લોક કરવા માટે કરો, જેથી વધુ નુકસાન અટકાવી શકાય.
- તમારા ATM, ડેબિટ અને ક્રેડિટ કાર્ડને સુરક્ષિત રાખો અને ટ્રાન્ઝક્શન માટે દૈનિક મર્યાદા નક્કી કરો. તમે મર્યાદા પણ નક્કી કરી શકો છો અને સ્થાનિક/આંતરરાષ્ટ્રીય ઉપયોગ માટે સક્રિય/નિષ્ક્રિય કરી શકો છો. આ બાબત છેતરપિંડીથી થતા નુકસાનને મર્યાદિત કરી શકે છે.