સાયબર સેક્યુરીટી જાગૃતિ - ઓક્ટોબર ૨૦૧૭

ફિશિંગ ઇ-મેલ્સથી સાવચેત રહો

- ફિશિંગ એ વિશાળ ઇમેઇલ ઝુંબેશ દ્વારા એક છેતરપિંડીની રણનીતિ છે જેના દ્વારા વપરાશકર્તાઓને ગંભીર નાણાકીય અથવા વ્યક્તિગત માહિતી જાહેર કરવા માટે કપટ કરવામાં આવી શકે છે. આ પ્રકારની માહિતીમાં યુઝરના નામ અને પાસવર્ડ, એટીએમ અથવા ક્રેડિટ કાર્ડ વિગતો જેવી કે પિન નંબર, સીવીવી નંબર, કાર્ડ સમાપ્તિની વિગતોનો સમાવેશ થાય છે.
- ફિશીંગ સાયબરઅપરાધ લોકોમાં લોકપ્રિય છે, કારણ કે કમ્પ્યુટરના સંરક્ષણ દ્વારા તોડી નાખવાનો પ્રયાસ કરતાં કોઈકને કાયદેસરની ઇમેઇલમાં દુર્ભાવનાપૂર્ણ લિંકને ક્લિક કરવા માટે કોઈની સાથે યુક્તિ કરવી સરળ છે.
- પીડિતને સંદેશ પ્રાપ્ત થાય છે જે જાણીતા સંપર્ક અથવા સંગઠન દ્વારા મોકલવામાં આવ્યો હોવાનું જણાય છે. સંદેશમાં જોડાણ અથવા લિંક્સ વપરાશકર્તાના ઉપકરણ પર માલવેર ઇન્સ્ટોલ કરી શકે છે અથવા તેને વ્યક્તિગત અને નાણાંકીય માહિતી જાહેર કરવા માટે તેમને કપટ કરવા માટે રચવામાં આવેલી દૂષિત વેબસાઇટ પર દિશામાન કરી શકે છે.
- આ ફિશિંગ સંદેશાઓ જાણીતા કંપનીની જેમ બનાવવા માટે, તે કંપનીના વેબસાઇટ પરથી સીધી લીધેલા લોગો અને અન્ય ઓળખાણની માહિતીનો સમાવેશ કરે છે.
- આ નકલી ઓળખ અને આકર્ષક ઓફર દ્વારા વપરાશકર્તા ફસાઇ જાય છે અને આ લિંક પર સંવેદનશીલ માહિતી પ્રદાન કરે છે.
- આ દૂષિત લિંક ભ્રામક નિયંત્રણ હેઠળ છે અને આ માહિતીનો ઉપયોગ હવે યુઝરના ખાતામાંથી પૈસા પાછા લેવા અથવા ટ્રાન્સફર જેવી છેતરપિંડી કરવા માટે કરવામાં આવે છે. ઘણા કિસ્સાઓમાં, એટીએમ / ક્રેડિટ કાર્ડની વિગતોનો ઉપયોગ કરીને ઓનલાઇન શોપિંગ કરવામાં આવે છે.

કેવી રીતે ફિશિંગ હુમલા ટાળવા અને સલામત રહેવું?

શુ કરવુ?

1. સરનામાં બારમાં URL ને ટાઇપ કરીને બેંકની વેબસાઇટ્સનો ઉપયોગ કરવાનું હંમેશા પ્રાધાન્ય આપો. બેન્કિંગ સાઇટના સરનામાં પહેલા પેડલોક પ્રતીક અને https ટેક્સ્ટની ખાતરી કરો.
2. તમારા ઓનલાઇન એકાઉન્ટ્સ માટે બે પરિબળ પ્રમાણીકરણ (2FA) ગોઠવો. ઇન્ટરનેટ/મોબાઇલ બેન્કિંગ પાસવર્ડ અને એટીએમ પિન નિયમિતપણે બદલો.
3. એસ.એમ.એસ. ચેતવણીઓ માટે નોંધણી કરો કે જે તમારા એકાઉન્ટ્સ પરના વ્યવહારો પર જાતે અપડેટ થાય. નિયમિત ધોરણે તમારી બેંક એકાઉન્ટ સ્ટેટમેન્ટ તપાસો.
4. લાઇસન્સિત એન્ટીવાયરસ સૉફ્ટવેરનો ઉપયોગ કરો, તેને અપ-ટૂ-ડેટ રાખો અને નિયમિતપણે સિસ્ટમ સ્કેન કરો.
5. જો તમને આમાંની કોઈપણ સંવેદનશીલ માહિતીના સમાધાન અંગે શંકા હોય તો, તરત જ નેટ બેન્કિંગ પાસવર્ડ અને એટીએમ પિન બદલો. તમારા બેંક એકાઉન્ટમાંથી કોઈ અનધિકૃત વ્યવહારના કિસ્સામાં તરત જ બેંકનો સંપર્ક કરો.

શું નહીં કરવુ?

1. અજ્ઞાત તરફથી કોઈપણ મેઇલનો પ્રતિસાદ આપશો નહીં. અજ્ઞાત દ્વારા ઈ-મેલ સામગ્રીમાં આપવામાં આવેલા કોઈપણ લિંક્સ પર ક્લિક કરશો નહીં.
2. વપરાશકર્તા નામ અને પાસવર્ડ, એટીએમ / ક્રેડિટ કાર્ડ વિગતો જેવી કે પીન, સીવીવી નંબર અને કાર્ડ સમાપ્તિ વિગતો જેવી બેંક એકાઉન્ટ વિગતો ક્યારેય શેર કરશો નહીં. બેન્ક આવા માહિતી માટે પૂછતી નથી.
3. તમારા બેંક એકાઉન્ટને ઍક્સેસ કરવા માટે ઇમેઇલ સામગ્રીમાં આપેલ કોઈપણ લિંક્સ પર ક્લિક કરશો નહીં.
4. સાર્વજનિક કમ્પ્યુટરો, ફ્રી અને અસુરક્ષિત Wi-Fi કનેક્શન્સથી તમારા બેંક એકાઉન્ટને ઍક્સેસ કરવાનું ટાળો.