National Cyber Security Centre
PART OF THE GCSB

Ministry for Ethnic Communities
Te Tari Mātāwaka

ઓનલાઇન સુરક્ષિત રાખવા

શા માટે સાયબર સુરક્ષા મારા માટે મહત્વપૂર્ણ છે?

ઈન્ટરનેટ અને સોશિયલ મીડિયા એ અદભૂત પ્લેટફોર્મ્સ છે જે આપણને માહિતી શેર કરવામાં અને મિત્રો અને પરિવાર સાથે સંપર્કમાં રહેવામાં મદદ કરે છે.

જો કે, ગુનેગારો અને અન્ય ગેરકાનૂની સંસ્થાઓ તમારા પૈસા, તમારી માહિતી મેળવવા અથવા તમને ડરાવવા માટે પણ તેનો ઉપયોગ કરે છે.

વિશ્વમાં ગમે ત્યાંથી તેઓ કામ કરી શકે છે, મોટાભાગની ભાષાઓ અસ્ખલિત રીતે બોલી શકે છે અને ખાતરી આપતી નકલી વેબસાઇટ્સ બનાવી શકે છે. ઈમેઇલ, સોશિયલ મીડિયા અને ટેક્સ્ટ મેસેજ દ્વારા તેઓ તમારો સંપર્ક કરશે અને તેઓ તમને ડર અથવા બેચેન અનુભવવાનો પ્રયત્ન કરશે, જેથી તમે સ્પષ્ટ રીતે વિચારી શકતા નથી.

આ બધાનો અર્થ એ છે કે તમારે તૈયાર રહેવાની જરૂર છે અને તેઓ જે યુક્તિઓનો ઉપયોગ કરે છે તેનાથી હંમેશા વાકેફ રહેવું જોઈએ.

કેટલીક સામાન્ય સમસ્યાઓ શું છે જે મને ઓનલાઈન આવી શકે છે?

આ કેટલીક સૌથી સામાન્ય પરિસ્થિતિઓ છે જે આપણે જોઈએ છીએ.

- તમને શંકાસ્પદ ઇમેઇલ અથવા ટેક્સ્ટ સંદેશ મળે છે જે તમને લિંક પર ક્લિક કરવાનું કહે છે.
  - આ લિંક્સ ઘણીવાર નકલી વેબસાઇટ્સ તરફ દોરી જાય છે જે તમારા લૉગિન અથવા નાણાકીય વિગતોની ચોરી કરવા માટે ડિઝાઇન કરવામાં આવી છે.
- તમને એક શંકાસ્પદ કોલ મળે છે જે વ્યક્તિગત માહિતી માંગે છે.
  - ઉપર મુજબ કોલ કરનાર તમારી બેંકમાંથી હોવાનો ડોળ કરશે અને માહિતી માંગશે.
- સત્તાધારી વ્યક્તિ હોવાનો ઢોંગ કરતી કોઈ વ્યક્તિ પાસેથી તમે સંદેશાવ્યવહાર મેળવો છો, જે તમને કંઈક કરાવવાનો પ્રયાસ કરે છે.
  - કેટલીકવાર વ્યક્તિ અમુક પ્રકારની ધમકી આપે છે.
- કોઈ તમારા એક અથવા વધુ ઑનલાઇન એકાઉન્ટ્સમાં પ્રવેશ કરે છે (ઉદાહરણ તરીકે: ઇમેઇલ અથવા સોશિયલ મીડિયા).
  - જો કોઈ વ્યક્તિ તમારા ઑનલાઇન એકાઉન્ટમાં પ્રવેશ કરે છે, તો તે માહિતી ચોરી શકે છે, ચૂકવણીઓ રીડાઇરેક્ટ કરી શકે છે અને તમે હોવાનો ડોળ કરીને તમારા મિત્રો અથવા કુટુંબને સંભવિત રૂપે લક્ષ્ય બનાવી શકે છે.
- તમારા ક્રેડિટ કાર્ડની વિગતો ચોરાઈ ગઈ છે, અથવા નકલી વેચાણ અથવા રોકાણમાં તમારી પાસેથી નાણાંની છેતરપિંડી થઈ છે.
  - સ્કેમર્સ આશા રાખે છે કે તમે સારો સોદો જુઓ છો અને વિચાર્યા વિના ચૂકવણી કરવા માંગો છો. અથવા કદાચ કોઈ વાસ્તવિક વેબસાઈટ ડેટાના ભંગમાં ફસાઈ ગઈ હોય અને તમારી વિગતો ઓનલાઈન લીક થઈ જાય.

અહીં વધુ દૃશ્યો છે:
હમણાં જ મદદ મેળવો - તમારી ઑનલાઇન રાખો

હું ઑનલાઇન કેવી રીતે સુરક્ષિત રહી શકું?

- **લાંબા અને અનન્ય પાસવર્ડ્સ**.
    - પાસવર્ડ જેટલો લાંબો હોય તેટલો મજબૂત છે.
    - ચાર અવ્યવસ્થિત શબ્દોને એકસાથે જોડીને (ઉદાહરણ તરીકે: TriangleRhinoOperationShoes) અને જો જરૂરી હોય તો સંખ્યાઓ, મોટા અક્ષરો અને પ્રતીકો ઉમેરીને 16 કરતાં વધુ અક્ષરોનો યાદગાર પાસવર્ડ બનાવો (ઉદાહરણ તરીકે: Triangle&"Rhino"Operation2Shoes).
    - અગત્યની વાત એ છે કે, તમારા પાસવર્ડને રિપીટ કરશો નહીં. જો કોઇ ગુનેગારને તમારો પાસવર્ડ મળી જાય છે તો તેઓ અન્ય એકાઉન્ટ્સ પર પણ તેનો પ્રયાસ કરશે.
    - આપના માટે પાસવર્ડ યાદ રાખવા અને નવા પાસવર્ડ બનાવવા પાસવર્ડ મેનેજરનો ઉપયોગ કરો.
    - સારા પાસવર્ડ બનાવો - તમારી ઑનલાઇન માલિકી રાખો
- **ટુ-ફેક્ટર પ્રમાણીકરણને ચાલું કરેલું રાખો.**
    - આ માહિતીનો વધારાનો ભાગ છે – સામાન્ય રીતે તમારા ફોન પરનો કોડ – તમારે વેબસાઇટમાં લૉગ ઇન કરવાની જરૂર છે.
    - આ ટેકનિક અતિ મજબૂત છે અને તમારા એકાઉન્ટમાં પ્રવેશવાના મોટાભાગના પ્રયાસોને રોકી શકે છે.
    - અમે 'ઓથેન્ટિકેટર એપ'નો ઉપયોગ કરવાની ભલામણ કરીએ છીએ, જ્યાં આ સમર્થીત છે.
    - ટુ-ફેક્ટર ઓથેન્ટિકેશન (2FA) સેટ કરો - તમારી ઓનલાઈન માલિકી રાખો
- **ઑનલાઇન ખાનગી રહો**.
    - સોશિયલ મીડિયા પર સુરક્ષિત રહેવાનો શ્રેષ્ઠ વિકલ્પ એ છે કે તમારી ગોપનીયતા સેટિંગ્સ ચાલુ કરો.
    - આનાથી સાયબર અપરાધીઓ સહિત રેન્ડમ લોકો તમારી પોસ્ટ જોવા અથવા તમને સંદેશા મોકલવામાં સમર્થ થવાનું બંધ કરશે.
    - છતાંય આપની, આપના પરિવાર કે આપના મિત્રોની વ્યક્તિગત માહિતી પોસ્ટ કરતી વખતે કાળજી રાખો.
    - સંપર્કો તેઓ જે હોવાનો દાવો કરે છે તેમના જ છે, તેની ખાતરી કરો.
    - નકલી ફ્રેન્ડ રીક્વેસ્ટને ઓળખો. પત્રકારો હોવાનો દાવો કરનારા લોકો અથવા તો તમે જેમને જાણતા ના હોય તેવા અન્ય લોકોથી સાવધ રહો.
    - તમારી ગોપનીયતાને ઓનલાઈન સુરક્ષિત કરો - તમારી ઓનલાઈન માલિકી રાખો
- **દરેક વસ્તુને અપડેટ રાખો.**
    - જ્યારે તમે તમારા ફોન, કોમ્પ્યુટર અથવા સોફ્ટવેરને અપડેટ કરો છો ત્યારે તે સુરક્ષામાં કોઈપણ છિદ્રોને પ્લગ કરે છે.
    - ગુનેગારો હંમેશા અંદર પ્રવેશવાના રસ્તાઓ શોધતા હોય છે અને અપડેટ્સ નબળાઈઓને ઠીક કરે છે.
    - તમારા ડીવાઇઝને નિયમિતપણે રીસ્ટાર્ટ કરો.

- [તમારા અપડેટ્સ સાથે રાખો - તમારી ઓનલાઈન માલિકી રાખો]()

- **સ્કેમ્સ વિષે સાવધ રહો.**
    - ઉત્તમ સલાહ એ છે કે આ કૌભાંડોથી વાકેફ રહો અને જો ગુનેગારો કોઈપણ ઓનલાઈન પ્લેટફોર્મ પર તમારો સંપર્ક કરવાનો પ્રયાસ કરે તો તેના પર નજર રાખો.
    - જો કંઈપણ ખોટું લાગતું હોય, તો જે વ્યક્તિએ તમારો સંપર્ક કર્યો છે તેની સાથે સંલગ્ન રહો નહીં. ખાસ કરીને સાવધ રહો જો તેઓ પૈસા માંગે, ભલે તેઓ મૈત્રીપૂર્ણ લાગે.
    - અપરિચિત લિંક્સ અને ઇમેઇલ સરનામાંઓ માટે જુઓ (ઉદાહરણ તરીકે: તમારી બેંક તમને gmail એકાઉન્ટમાંથી ઇમેઇલ મોકલશે નહીં).
    - ટેક્સ્ટ મેસેજમાં રહેલી લીંક્સ પર ક્યારેય ક્લિક *ન* કરો.
    - માત્ર ઓફિસીયલ એપ સ્ટોર્સ પરથી આપની ડિવાઈસ પર એપ ડાઉનલોડ કરો.
    - જો શંકામાં હોવ તો, સંસ્થાનો સીધો સંપર્ક કરો અને તમને મોકલવામાં આવેલી કોઈપણ લિંક અથવા ફોન નંબરને અનુસરશો નહીં.
    - તમારા, તમારા સમુદાય અને તમે જેની સાથે સંકળાયેલા હો તેવા કોઇ ગ્રૂપ માટે ઓનલાઇન સુરક્ષા જોખમોથી સાવધ રહેવાનો પ્રયત્ન કરો.
- **તમારી માહિતીને સુરક્ષિત બનાવો.**
    - સિગ્નલ જેવી એન્ક્રીપ્ટેડ મેસેજિંગ એપ્સનો ઉપયોગ કરો. તેનાથી અન્ય કોઈ વ્યક્તિ તમારા મેસેજો વાંચી શકશે નહીં.
    - જે વેબસાઇટનું એડ્રેસ HTTPS થી શરૂ થતું હોય ફક્ત તેવી જ વેબસાઇટ પર માહિતીને શૅર કરો. અહીં S નો અર્થ 'secure' (સલામત) થાય છે અને તેનો અર્થ એ પણ છે કે તમારી અને વેબસાઇટ વચ્ચે આદાનપ્રદાન થયેલી કોઈ પણ માહિતી એન્ક્રીપ્ટ થયેલી છે.
    - વર્ચ્યુઅલ પ્રાઇવેટ નેટવર્ક (VPN)નો ઉપયોગ કરવા અંગે વિચારો, જે તમારા ડેટાને સુરક્ષિત રાખી શકે છે અને તમારી લૉકેશનને છુપાવી દે છે.
    - તમારી એપ્સને કયા ડેટા અને મંજૂરીઓનું ઍક્સેસ છે, તે ચેક કરો. ઉદાહરણ તરીકે, ફિટનેસ એપને તમારા સંપર્ક નંબરોના ઍક્સેસની જરૂર નથી.

જો મારી સાથે છેતરપિંડી થાય અથવા તેનાથી પણ ખરાબ થાય તો મારે શું કરવું જોઈએ?

એવી ઘણી બધી જગ્યાઓ છે, જ્યાં તમે મદદ માટે જઈ શકો છો. તમે જ્યાં સુધી તમારી સંમતિ ન આપો ત્યાં સુધી આ તમામ સંસ્થાઓ તમારી વિગતો અન્ય કોઈની સાથે શેર કરશે નહીં.

- તમે CERT NZ પોર્ટલ દ્વારા NCSCને સાયબર ઘટનાઓની જાણ કરી શકો છો અને અમે તમને મદદ કરી શકીએ છીએ અથવા અન્ય એજન્સીનો સંપર્ક કરી શકીએ છીએ:
  [તમે ઘટનાની જાણ કરો| CERT NZ]()
- જો તમે પૈસા ગુમાવી દીધા હોય, તો તમારે તરત જ તમારી બેંકનો સંપર્ક કરવો જોઇએ.
- આંતરિક બાબતોના વિભાગ દ્વારા ચલાવવામાં આવતી સેવા 7726 પર, કૌભાંડના ટેક્સ્ટ સંદેશાઓ મફતમાં ફોરવર્ડ કરી શકાય છે.