National Cyber Security Centre

તમારા સંગઠનને ઓનલાઇન સલામત રાખો

કમ્યુનિટી ગ્રૂપ્સ અને સંગઠનો માટે શા માટે સાઇબર સુરક્ષા મહત્વપૂર્ણ છે?

આ પેજ પર તમારા કમ્યૂનિટી ગ્રૂપ્સ અને સંગઠનોને સાઇબર સુરક્ષાના જોખમોથી સુરક્ષિત રાખવા માટે કેટલીક સલાહ અને કેટલાક પગલાં સૂચવવામાં આવ્યાં છે. લોકો પોતાને ઓનલાઇન સલામત રાખી શકે તે માટે અલગ વ્યક્તિગત માર્ગદર્શિકા પણ આપવામાં આવી છે.

આ સલાહ સર્વસામાન્ય અને ગંભીર જોખમો પર આધારિત છે.

અપડેટ્સ

સુરક્ષામાં રહેલા કોઈ પણ છીંડાને બંધ કરવા માટે તમારા ઉપકરણમાં રહેલા સોફ્ટવેરને અપડેટ થયેલા રાખો.

- તમારા કમ્યુનિટી ગ્રૂપ કે સંગઠનના ઉપકરણને અપડેટ થયેલા રાખો. તેમાં ફોન, કમ્પ્યૂટર, વાઈફાઈ રાઉટર અને સ્માર્ટ ઉપકરણ સહિત ઇન્ટરનેટ સાથે જોડાઈ શકતા હોય તેવા કોઈ પણ ઉપકરણનો સમાવેશ થાય છે.
- જ્યાં પણ શક્ય હોય ત્યાં ઑટોમેટિક અપડેટ્સનો ઉપયોગ કરો.

ટુ-ફેક્ટર ઑથેન્ટિકેશન (2FA)

તમારા એકાઉન્ટ્સને વધારાની સુરક્ષા પૂરી પાડે છે, જેના માટે તમારે પાસવર્ડ અને વધુ એક પગલાની જરૂર પડે છે, જેમ કે તમારા ફોન પર એપ તરફથી પૂરો પાડવામાં આવતો કોડ.

- નોંધ: તેને મલ્ટિ-ફેક્ટર ઑથેન્ટિકેશન (MFA), ટુ-સ્ટેપ વેરિફિકેશન (2SV) અને બીજા ઘણાં નામોથી ઓળખવામાં આવે છે.
- તમારા તમામ કમ્યુનિટી ગ્રૂપ કે સંગઠનના એકાઉન્ટ્સ પર 2FA ને ચાલું કરો.
- જો શક્ય હોય તો, 2FA ના ફોર્મનો ઉપયોગ કરો, જે ફિશિંગ પ્રતિરોધી હોય છે, જેનો અર્થ એ થયો કે તેઓ તમને તે સોંપીને છેતરી શકાતા નથી. તે ફીઝિકલ સિક્યુરિટી કી અથવા તો ફિંગરપ્રિન્ટ કે ફેસ ID જેવું કંઈક હોઈ શકે છે.

તમારા ઓનલાઇન એકાઉન્ટ્સને ટ્રેક કરો

ભૂતપૂર્વ સભ્યો ગ્રૂપ કે સંગઠનને છોડ્યાં પછી એકાઉન્ટ્સનું ઍક્સેસ ધરાવતા ના હોય તેની ખાતરી કરો.

- જો એક જ એકાઉન્ટનું ઍક્સેસ એકથી વધારે લોકો પાસે હોય તો તે પ્રત્યેક વ્યક્તિ પાસે અલગ-અલગ લૉગઇન હોય અને તે તમામે 2FA ને ચાલું કરેલું હોય તેની ખાતરી કરો.
- તમામ યુઝર એકાઉન્ટ્સની યાદી બનાવો અને જેમની જરૂર નથી તેને ડીએક્ટિવેટ કરી દો, જેમ કે, જ્યારે કોઈ સ્ટાફ નોકરી છોડીને જાય.
- તમે તમારા સભ્યોને આપેલા હોય તેવા કોઈ પણ ઉપકરણનું એક રજિસ્ટર રાખો અને જો તે વ્યક્તિ સંગઠન છોડી દે તો તેમની પાસેથી આ ઉપકરણ પાછું મેળવવાનું અને તેને ફેક્ટરી રીસેટ કરવાનું યાદ રાખો. તમારે બિલ્ડિંગના ઍક્સેસ માટેના ફીઝિકલ કૉડ પણ બદલવાની જરૂર છે.

તમારા ઓનલાઇન એકાઉન્ટ્સનું ઍક્સેસ કોની પાસે છે, તે ચકાસો

તમારા કમ્યુનિટી ગ્રૂપ કે સંગઠનમાં રહેલા લોકોને જેની જરૂર હોય એટલું જ ઍક્સેસ હોવું જોઇએ.

- જો કોઈ એક વ્યક્તિનું એકાઉન્ટ હેક થઈ જાય તો આ પગલાં એટેકર દ્વારા થઈ શકતા નુકસાનને મર્યાદિત કરી શકે છે.
- બિનજરૂરી મંજૂરીઓને નિયમિતપણે ચેક કરો અને તેને દૂર કરો.
- જો તમારી પાસે સિંગલ 'એડમિન' એકાઉન્ટ હોય, જેનો ઉપયોગ એકથી વધારે લોકો કરતાં હોય તો, તેમાં કોઈ અસામાન્ય પ્રવૃત્તિ તો થતી નથી તેના માટે નજર રાખો. આ પ્રકારના એકાઉન્ટ્સને મર્યાદિત રાખવાનો પ્રયત્ન કરો, ખાસ કરીને રોજબરોજની કામગીરી માટે.
- આ નિયમો ડીવાઇઝના એડમિનિસ્ટ્રેટર ઍક્સેસ પર પણ લાગુ થાય છે, જેમ કે, રાઉટર્સ.

સર્વિસ પ્રોવાઇડરની સાથે થયેલા તમારા કોન્ટ્રાક્ટ્સની સમીક્ષા કરો

જો તમે તમારા માટે IT સેવાઓનું સંચાલન કરવા માટે કોઈને કામે રાખ્યાં હોય તો.

- તમારા કમ્યુનિટી ગ્રૂપ કે સંગઠનની જરૂરિયાતોને પૂરી કરવા માટે તેમની પાસે સાઇબર સુરક્ષા પ્રોટેક્શન હોય તેની ખાતરી કરો.

તમારા તમામ એકાઉન્ટ્સ અને સિસ્ટમ્સ એકસાથે કેવી રીતે કામ કરે છે તે જાણો

કનેક્શનોને સમજવાથી એટેકર ક્યાંથી અંદર ઘૂસી શકે છે, તે જાણવામાં મદદ મળી રહે છે.

- તમારી સિસ્ટમોની વચ્ચેના કનેક્શનોની સમીક્ષા કરો, ઉદાહરણ તરીકે, ઈ-મેઇલ, ક્લાઉડ સ્ટોરેજ અને એકાઉન્ટિંગ પ્લેટફૉર્મ્સ.
- ઓનલાઇન વધારાની સુરક્ષા માટે વર્ચ્યુઅલ પ્રાઇવેટ નેટવર્ક (VPN)નો ઉપયોગ કરવા અંગે વિચારો. VPN નો ઉપયોગ કરવાથી તમારી ઓનલાઇન પ્રવૃત્તિ તમને ટ્રેક કરવા માંગતા લોકોથી છુપાઈ જાય છે. તે ખાસ કરીને ત્યારે ફાયદારૂપ થાય છે, જ્યારે તમારા કમ્યુનિટી ગ્રૂપ કે સંગઠનના કોઈ સભ્ય રીમોટલી કનેક્ટ થતાં હોય.

તમારા લોકોને 'સાઇબર સ્માર્ટ' બનાવો

તમારી સિસ્ટમ કરતાં તમારા કમ્યુનિટી ગ્રૂપ કે સંગઠનમાં રહેલા લોકોને ટાર્ગેટ કરવામાં આવે તેવી શક્યતા વધુ હોય છે.

- તમામ સ્ટાફને સાઇબર સુરક્ષાની મૂળભૂત બાબતોમાં તાલીમ આપો. ઑઉન યોર ઓનલાઇન વેબસાઇટ ઓઉન યોર ઓનલાઇન | NCSC તમને ઓનલાઇન સલામત રાખવા અને છેતરપિંડીને પકડી પાડવામાં મદદરૂપ થવા માટે સલાહ-સૂચનોની વ્યાપક રેન્જ ધરાવે છે.
- તેમને યાદ કરાવો કે તે તેમના વ્યક્તિગત એકાઉન્ટ્સ માટે તેમજ તેઓ તેમના સંગઠન માટે જે એકાઉન્ટ્સનો ઉપયોગ કરે છે, તેના માટે મહત્વપૂર્ણ છે.
- તેમને ઓનલાઇન સલામત રાખવા માટે અમારી પાસે વ્યક્તિગત માર્ગદર્શિકા પણ છે.

ઘટના માટેનો પ્લાન

જ્યારે પણ આવી કોઈ ઘટના ઘટે ત્યારે લોકોને ગભરાઈ જતાં અટકાવવા માટે કોઈ રીસ્પોન્સ પ્લાન હોવો ખૂબ જ મહત્વપૂર્ણ છે.

- એક ઇન્સિડેન્ટ રીસ્પોન્સ પ્લાનમાં ઘટના દરમિયાન કોણે શું કરવાનું છે, તેને રેખાંકિત કરવામાં આવે છે. ટેમ્પલેટ્સ અહીં ઉપલબ્ધ છે ઇન્સિડેન્ટ મેનેજમેન્ટ |NCSC
- જો ફોન, કમ્પ્યૂટર કે અન્ય કોઈ સિસ્ટમ નિષ્ફળ થઈ જાય ત્યારે શું કરવું, તેના માટેના પ્લાનને સામેલ કરો. આ પ્લાનને અપડેટ થયેલો રાખો.
- જો સૌ કોઈની સાથે સંપર્ક કરવાનું મુખ્ય જોડાણ તૂટી જાય (જેમ કે ઈ-મેઇલ) તો તમામ આવશ્યક વ્યક્તિઓના સંપર્કની વિગતો અને બેકઅપ વિગતોને જાળવી રાખો.
- તમારા પ્લાનને તમારી સિસ્ટમની ક્યાંક બહાર પણ રાખો, જો તમે તેના સુધી ના પહોંચી શકો તેવા કિસ્સામાં.≥÷≤µ