

નવ આવશ્યક સાઇબર સુરક્ષિત આદતો આજે જ અપનાવો



૧. તમે ક્લિક કરો તે પહેલા થોભો ;

લિંક પર ક્લિક કરતાં પહેલા અથવા એટેચમેન્ટ ખોલતા પહેલા બે વાર વિચારો, પછી ભલે તે તમે જાણતા હોય એવા કોઈ વ્યક્તિ તરફથી આવતા હોય.

- અજાણી લિંક પર ક્લિક કરવાને બદલે હંમેશા જાણીતા, કાયદેસર સ્ત્રોત (દા.ત. HTTPS) દ્વારા વેબસાઈટ્સ પર નેવિગેટ કરો.
- જો કોઈ એટેચમેન્ટ અનપેક્ષિત લાગે , વિશ્વનીયતાની પદ્ધતિથી મોકલનારની સાથે કન્ફર્મ કરો અથવા સુરક્ષિત બાજુ માટે, ક્લિક ન કરવાનું પસંદ કરો .



૨. વ્યક્તિગત માહિતીની વિનંતી ચકાસો.

હંમેશા પ્રાઇવેટ ડેટા ચકાસો પછી તે ભલે તમારો હોય અથવા બીજા કોઈપણ નો.

- સ્કેમર્સ સરળતાથી વિશ્વસનીય સંપર્કો નો ઢોંગ કરી શકે છે .
- અસમાન્ય પ્રવૃત્તિ માટે નાણાકીય નિવેદનો અને ક્રેડિટ રિપોર્ટ્સ ની નિયમિત સમીક્ષા કરો
- ઘણા ફિશિંગ સંદેશામાં જોડણી અને વ્યાકરણ ની ભૂલો હોય છે.
- વિનંતી કાયદેસર છે કે કેમ તે ધ્યાનમાં લો. શું વ્યક્તિ અથવા સંસ્થાને તે માહિતીની જરૂર છે ?



૩. તમારા પાસવર્ડ્સ ને નિયંત્રણ કરો.

તમારા એકાઉન્ટ્સ ને સુરક્ષિત રાખવા માટે મજબૂત, જટિલ પાસવર્ડ્સ બનાવવા અને તેમને સમજદારીપૂર્વક મેનેજ કરવા જરૂરી છે.

- અલગ અલગ એકાઉન્ટ્સ માટે યુનિક પાસવર્ડ્સ નો ઉપયોગ કરો.
- ઓફિસ કામના અને પર્સનલ કામના પાસવર્ડ્સ અલગ અલગ રાખો.
- ક્ષારેય પાસવર્ડ્સ શેર કરશો નહિ.
- સમય સમય પર પાસવર્ડ્સને બદલતા રહો.
- બ્રાઉઝરમાં પાસવર્ડ્સને સાચવવાનું રાખશો નહિ.
- વધારાની સુરક્ષા માટે મલ્ટી-ફેક્ટર ઓથેન્ટિકેશન (MFA) સક્ષમ કરો.



૪. તમારા ઉપકરણોને સુરક્ષિત કરો.

તમારી કામકાજ ની જગ્યા ને લોક કરવાનું રાખો અને દૂર જાઓ ત્યારે તમારા ઉપકરણોને સુરક્ષિત કરો.

- તમારા કોમ્પ્યુટર સ્ક્રીનને હંમેશા લોક કરો.
- તમારા ફોન અને પોર્ટેબલ ઉપકરણોને તમારી સાથે લઈ જાઓ અથવા તેમને સુરક્ષિત રીતે સ્ટોર કરો.
- જ્યારે પણ શક્ય હોય ત્યારે મજબૂત પ્રમાણીકરણ પદ્ધતિનો ઉપયોગ કરો.



પ. મહત્વપૂર્ણ ફાઇલોનો બેકઅપ રાખો

ખાતરી કરો કે તમારા મહત્વપૂર્ણ ડેટાનું નિયમિત બેકઅપ લેવામાં આવે છે.

- બેકઅપને તેના મૂળ સ્થાન ના બદલે અલગ જગ્યા પર સ્ટોર કરો.
- સંસ્થાના માન્ય સ્ટોરેજ સોલ્યુશન્સ નો ઉપયોગ કરો.
- તેઓ યોગ્ય રીતે કાર્ય કરે છે તેની ખાતરી કરવા માટે નિયમિતપણે બેકઅપનું પરીક્ષણ કરો.



દ. શંકાસ્પદ પ્રવૃત્તિની જાણ કરો

જો કંઈક શંકાસ્પદ લાગે, તો તમારી વૃત્તિ પર વિશ્વાસ કરો –રિપોર્ટ કરો;

- તમારા સુપરવાઇઝરને જાણ કરો ને શંકાસ્પદ કૌભાંડો અથવા શંકાસ્પદ પ્રવૃત્તિઓ માટે તમારી સંસ્થાના રિપોર્ટિંગ પ્રોટોકોલ ને અનુસરો.



૭. તમારી જાતને અને અન્યોને શિક્ષિત કરો

નવીનતમ સાયબર સુરક્ષા જોખમો અને વલણો વિશે માહિતગાર રહો.

- તાલીમ સત્રોમાં હાજરી આપો અને જ્યારે તમને તક મળે ત્યારે સહકર્મીઓ સાથે જ્ઞાન શેર કરો .
- સારી રીતે માહિતગાર ટીમ એ સાયબર ધમકીઓ સામે રક્ષણ કરવા તમારું પ્રથમ પગથિયું છે.



૮. સુરક્ષિત નેટવર્ક્સનો ઉપયોગ કરો

હમેશા સુરક્ષિત નેટવર્ક્સ સાથે કનેક્ટ કરો, ખાસ કરીને જ્યારે સંવેદનશીલ માહિતી એક્સેસ કરો.

- નાણાકીય વ્યવહારો અથવા સંવેદનશીલ કામ માટે જાહેર Wi-Fi ટાળો.
- વધારાની સુરક્ષા માટે જરૂરી હોય ત્યારે વર્ચ્યુઅલ પ્રાઇવેટ નેટવર્ક (VPN) નો ઉપયોગ કરો.



૯. સોશિયલ મીડિયાથી સાવધાન રહો.

તમે ઓનલાઇન શેર કરો છો તે વ્યક્તિગત માહિતીની માત્રાને મર્યાદિત કરો. તેથી તમે તમારી ગોપનીયતાને સુરક્ષિત કરી શકો છો, તમારી સલામતી વધારી શકો છો અને વધુ સકારાત્મક ઓનલાઇન અનુભવ બનાવી શકો છો.

- સોશિયલ મીડિયા પ્લેટફોર્મ પર ગોપનીયતા સેટિંગ્સની સમીક્ષા કરો.
- મિત્રની વિનંતિઓ અને તમારી માહિતી કોણ મેળવી રહ્યું છે તેનું ધ્યાન; લોક કરેલ પ્રોફાઇલથી આવતી વિનંતિઓ સ્વીકારશો નહીં.
- સંભવિત જોખમો ઘટાડવા માટે તમારી ઓનલાઇન હાજરીનું નિયમિતપણે નિરીક્ષણ કરો.

યાદ રાખો : સાયબર સુરક્ષા એ દરેક વ્યક્તિની જવાબદારી છે ;