Australian Government

હાલ જ પગલાં લો. સુરક્ષિત રહો.

તમે કઇ રીતે ઓનલાઇન સલામત રહી શકો છો

સરળતાથી વાંચી શકાય તેવી આવૃત્તિ

Easy Read

આ માર્ગદર્શિકાનો ઉપયોગ કેવી રીતે કરવો

અમે ઓસ્ટ્રેલિયાની સરકાર છીએ.

અમે આ માર્ગદર્શિકા લખી છે.

અમે અમુક શબ્દો **ઘાટા** લખ્યાં છે.

આ શબ્દોનો અર્થ શું થાય છે તે અમે સમજાવીએ છીએ.

પાન 28 પર પણ આ શબ્દોની યાદી છે.

તમે જેના પર વિશ્વાસ કરતાં હોવ તેવા કોઇ પાસેથી મદદ માંગી કહો કે:

- આ માર્ગદર્શિકા વાંચી આપે
- વધુ માહિતી મેળવી આપે.

આ અન્ય એક માર્ગદર્શિકાનો સરળતાથી વાંચી શકાય તેવો સાર છે.

આમાં ફક્ત ખૂબ જ મહત્વનાં વિચારોનો જ સમાવેશ છે.

તમે અમારી વેબસાઇટ પર તે બીજી માર્ગદર્શિકા જોઇ શકો છો.

www.actnowstaysecure.gov.au

આ માર્ગદર્શિકામાં શું છે?

આ માર્ગદર્શિકા વિશે	4
તમારા ખાતાં સલામત રાખો	6
તમારી માહિતીને સુરક્ષિત રાખવા તમારા સેટિંગો તપાસો	10
તમારા ઉપકરણોને સુરક્ષિત રાખો	16
છેતરપિંડીઓ	20
અવાજ ઉઠાવો	25
શબ્દાવલી	28
અમારો સંપર્ક કરો	30

આ માર્ગદર્શિકા વિશે

આપણે કઇ રીતે ઓનલાઇન સલામત રહી શકીએ તે આપણે બધાં એ વિચારવાની જરૂર છે.

અમે તેને **સાયબર** સલામતી કહીએ છીએ.

સાયબર એટલે ઇન્ટરનેટને લગતું કશુંક.

તમે તમારી જાતનું ઓનલાઇન રક્ષણ કરી શકો તે માટે તમે શું કરી શકો તે આ માર્ગદર્શિકા સમજાવે છે.

ઉદાહરણ તરીકે, **સાયબર ગુનાઓ** માંથી.

જ્યારે ગુનેગારો ગુનો કરવા માટે ઇન્ટરનેટનો ઉપયોગ કરે છે ત્યારે તે સાયબર ગુનો કહેવાય છે.

ઉદાહરણ તરીકે, તેઓ ઇન્ટનેટનો ઉપયોગ:

- તમારી અંગત માહિતી ચોરવા કરે
- તમારાં ઓનલાઇન ખાતાં અથવા વ્યક્તિગત માહિતી (પ્રોફાઇલો) પર કાબુ મેળવી લેવા કરે.

સાયબર ગુનો કોઇ પણ ઉપકરણ પર થઇ શકે છે.

તેમાં તમારાં:

- કોમ્પ્યુટર
- સ્માર્ટફોન
- સ્માર્ટ વોચનો સમાવેશ થાય છે.

સાયબર ગુનાઓથી સલામત રહેવા તમે કરી શકો તેવી કેટલીક બાબતો છે.

તમે શું કરી શકો તે અમે હવે પછીનાં પાનાંઓમાં સમજાવીએ છીએ.

તમારા ખાતાં સલામત રાખો

તમે તમારા ઓનલાઇન ખાતાં કેવી રીતે સલામત રાખી શકો તે વિશે તમારે વિચારવું જોઇએ.

મજબૂત અને જુદા-જુદા સાંકેતિક શબ્દો (પાસફ્રેઝો) વાપરો

પાસફ્રેઝ એ એક વધુ મજબૂત પ્રકારનો પાસવર્ડ છે.

અન્ય લોકો માટે તે શું હોય શકે તેનું અનુમાન લગાવવું ખૂબ મુશ્કેલ હોય છે.

મજબૂત અને જુદાજુદા પાસફ્રેઝો વાપરવા એ તમારા ખાતાંઓની રક્ષા કરવાનાં ઉત્તમ રસ્તાઓમાંનો એક છે.

તમારાં દરેક ઓનલાઇન ખાતા માટે તમારે જુદાં પાસફ્રેઝ વાપરવા જોઇએ.

મજબૂત પાસફ્રેઝોમાં નીચેનાનો સમાવેશ થાય છે:

- ૪ કે વધુ યાદૃચ્છિક શબ્દો
- ૧૫ કે વધુ અક્ષરો અને આંકડા.

તમે કેટલાક મોટી એબીસીડીનાં અક્ષરોનો સમાવેશ કરી શકો છો.

તમે ચિન્હોનો પણ ઉપયોગ કરી શકો છો જેમ કે:

- એક લીટી
- ડૉલર ચિન્હ,
- ઇમેઇલ @ ચિન્હ.

તમારા પાસફ્રેઝમાં તમારે કોઇ અંગત માહિતીનો ઉપયોગ ન કરવો જોઇએ.

ઉદાહરણ તરીકે,

- તમારી જન્મતારીખ
- તમારાં પરિવારજનો કે પાલતુ પ્રાણીઓનાં નામ.

તમારા ખાતામાં લોગીન કરવા માટે વધારાનાં પગલાં ઉમેરો

તમે તમારા ઓનલાઇન ખાતાંઓ **બહુપરિબળ પ્રમાણક (મલ્ટી-ફેક્ટર ઓથેન્ટીકેટર (એમએફએ))** વડે સુરક્ષિત કરી રાખી શકો છો.

એમએફએ એટલે કે દર વખતે તમારા ખાતાંમાં લોગીન કરવા માટે તમે ૨ કે વધુ જુદાજુદા રસ્તાઓનો ઉપયોગ કરો.

ઉદાહરણ તરીકે, કદાચ તમારે પહેલાં તમારો પાસફ્રેઝ દાખલ કરવો પડે.

ત્યારે બાદ તમારા ફોન પર આવેલો કોડ તમારે દાખલ કરવો પડે.

તમે કદાચ પસંદગી કરી શકો કે:

- તમને કોડ આપી શકે તે માટે તમારા ફોનમાં એપ નાંખો

- ઇમેઇલમાં કોડ મેળવો

- લેખિત સંદેશામાં કોડ મેળવો.

એમએફએ અન્ય લોકો માટે તમારા ઓનલાઇન ખાતાઓમાં ઘુસવું અઘરું બનાવે છે.

તેમને તમારો પાસફ્રેઝ ખબર પડી જાય તો પણ.

તમારી માહિતીને સુરક્ષિત રાખવા તમારા સેટિંગો તપાસો

તમારા સેટિંગો તમારી માહિતીને ઓનલાઇન સલામત રાખી રહ્યાં છે તેની તપાસ તમે કરી શકો છો.

તેમાં નીચેનાનાં સેટિંગોનો સમાવેશ થાય છે:

- ઓનલાઇન ખાતાઓ
- ઉપકરણો
- એપ્લિકેશનો.

તમે:

- તમારા સેટિંગો બદલી શકો છો
- તમારી માહિતીનો ઉપયોગ કઇ એપ્લિકેશનો કરી શકે તે નક્કી કરી શકો છો.

તમારા ઉપરકરણ પર સેટિંગો શોધવા તમે:

- ગિયરનું ચિન્હ શોધી શકો છો

  અથવા

- તમારા ઉપકરણનાં સર્ચ બારમાં 'settings' ટાઇપ કરી શકો છો.

તમે એપ અથવા ઓનલાઇન ખાતામાં મેન્યુ ખોલીને પણ કદાચ સેટિંગો શોધી શકશો.

મેન્યુ ઘણું કરીને 3 સીધી લીટીઓ જેવું દેખાતું હોય છે.

આમાંનાં કેટલાંક સેટિંગો નીચેના બાબતની માહિતીની આપલે કરી શકે છે:

- તમે કોણ છો
- તમે ક્યાં છો
- તમે ક્યાં રહો છો.

આ માહિતીઓની આપલે તમને સાયબર ગુનાઓનાં જોખમમાં મુકી શકે છે.

સાયબર ગુનેગારો તમારી માહિતીનો ઉપયોગ, તમે જ છો તેવો ડોળ કરવા માટે કરી શકે છે.

ઉદાહરણ તરીકે, તેઓ એવી માહિતીનો ઉપયોગ કરી શકે છે કે:

- તમે ક્યાં રહો છો

- તમારાં પરિવારજનોનાં નામ

- તમારાં પાલતું પ્રાણીઓનાં નામ.

તમે તમારા ખાતાને એવી રીતે સેટ કરી શકો છો કે ફક્ત તમારા જાણીતાં લોકો જ તમારો સોશીયલ મીડિયા પ્રોફાઇલ જોઇ શકે.

ઉદાહરણ તરીકે, તમારો ફેસબુક પ્રોફાઇલ.

આ સેટિંગોને બહુધા ગોપનીયતા (પ્રાઇવસી) સેટિંગો કહે છે.

તમે તમારા **સ્થાનનાં (લોકેશન) સેટિંગોને** પણ કાબૂમાં રાખી શકો છો.

લોકેશન સેટિંગો તમારું ઉપકરણ ક્યાં છે તે દર્શાવે છે.

તમે લોકેશન સેટિંગોને ચાલુ અથવા બંધ કરી શકો છો.

કઇ એપ્લિકેશનો તમારા લોકેશન સેટિંગોનો ઉપયોગ કરે તે પણ તમે નક્કી કરી શકો છો.

આવું તમે તમારા:

- ઓનલાઇન ખાતાંઓ
- ઉપકરણો
- એપ્લિકેશનો માટે કરી શકો છો.

કેટલીક એપ્લિકેશનો તમને એવું પણ પુછી શકે છે કે શું તે:

- તમારો કેમેરા વાપરી શકે

- ફોટા જોઇ શકે.

તમે જેનાથી વાકેફ હોવ ફક્ત એવી એપ્લિકેશનોને જ તમારે તમારો કેમેરા અને ફોટાનો ઉપયોગ કરવા દેવો જોઇએ.

તમારા ઉપકરણોને સુરક્ષિત રાખો

તમે તમારા ઉપકરણોને કઇ રીતે સુરક્ષિત રાખી શકો જેથી તે તમને ઓનલાઇન સુરક્ષિત રહેવામાં મદદ કરી શકે તે વિશે તમારે વિચારવું જોઇએ.

ઉદાહરણ તરીકે, તમારા ફોન અથવા સ્માર્ટ વોચ.

ઇન્ટરનેટ સાથે જોડાઇ શકે તેવા ઉપકરણો માટે આ અગત્યનું છે.

તમારા ઉપકરણોને અપડેટ કરો

તમે તમારા ઉપકરણોને ઓનલાઇન સુરક્ષિત રાખવા તેમને અપડેટ કરી શકો છો.

ઉદાહરણ તરીકે, તમારા ફોન અને લેપટોપ.

તમારુ ઉપકરણ તેને સોફ્ટવેર અપડેટ કહે તેવું બને.

ઉપકરણોને પોતાને સાયબર ગુનાઓથી સુરક્ષિત રાખવામાં અપડેટો મદદ કરે છે.

તમે ઉપકરણને જાતે અપડેટ કરી શકે તેમ સેટ કરી શકો છો.

તમારા ઉપકરણોને કેવી રીતે અપડેટ કરવા તે વિશે તમે અમારી વેબસાઇટ પર વધુ જાણી શકો છો.

www.actnowstaysecure.gov.au/cyber-safe-actions

જાહેર વાઇ-ફાઇ નેટવર્કો

જ્યારે તમે **જાહેર વાઇ-ફાઇ** વાપરતા હોવ ત્યારે તમારે સાવચેત રહેવું જોઇએ.

જાહેર વાઇ-ફાઇ એક તાર વગરનું ઇન્ટરનેટ છે જે તમે જાહેર જગ્યાઓએ વાપરી શકો છો.

ઉદાહરણ તરીકે,

- કાફેમાં
- હવાઇમથકમાં
- હોટલમાં.

જાહેર વાઇ-ફાઇનો ઉપયોગ કરીને તમે વેબસાઇટ પર શું માહિતી આપી રહ્યા છો તે વિશે તમારે સાવચેત રહેવું જોઇએ.

ઉદાહરણ તરીકે, તમારા:

- બેંકની માહિતી
- ઇમેઇલ એકાઉન્ટો
- સોશિયલ મીડિયા પ્રોફાઇલો.

કેટલાંક સાયબર ગુનેગારો જાહેર વાઇ-ફાઇનો ઉપયોગ કરીને:

- તમે ઓનલાઇન શું કરો છો તે જોઇ શકે છે
- તમારી માહિતી ચોરી શકે છે.

આનું કારણ એ છે કે:

- તેનો ઉપયોગ કોઇ પણ કરી શકે છે

- તમારા ઉપકરણોને સુરક્ષિત રાખવા અઘરાં છે.

જાહેર વાઇ-ફાઇનો ઉપયોગ કરતી વખતે સુરક્ષિત કેવી રીતે રહેવું તે અમારી વેબસાઇટ પર જાણો.

www.actnowstaysecure.gov.au/cyber-safe-actions

છેતરપિંડીઓ

અમે તેને **છેતરપિંડી** કહીએ છીએ, જ્યારે કોઇ પ્રયત્ન કરે છે:

- તમને બનાવવાનો
- તમારા નાણાં લેવાનો

છેતરપિંડી કરનારને **સ્કેમર** કહે છે.

સ્કેમરો તમને:

- એક લેખિત સંદેશ અથવા ફોન કોલ
- ઇમેલ
- સોશિયલ મીડિયા
- વેબસાઇટ દ્વારા છેતરવા પ્રયત્ન કરી શકે.

તેઓ મૈત્રીપૂર્ણ લાગી શકે છે.

પરંતુ તે તમને છેતરીને તમારી પાસેથી તમારી માહિતી કઢાવી શકે છે.

તેઓ તેનો ઉપયોગ:

- તમારા ઓનલાઇન ખાતામાં દાખલ થવા

- તમે હોવાનો ડોળ કરવા

- તમારા નાણાં ચોરવામાં કરી શકે છે.

સ્કેમરો:

- તમને છેતરવા ખોટાં ખાતાં બનાવી શકે છે

- તમે તેના પર ક્લીક કરો તે માટે લીંક કે જાહેરાતો મોકલી શકે છે.

છેતરપિંડીને કેવી રીતે ઓળખવી

એ છેતરપિંડી હોય શકે છે જો તે:

- તમને કશુંક ઝડપથી કરવાનું કહે

- તમને ઘણાં બધાં નાણાં આપવાનું કહે

- તમારી પાસે નાણાં માંગે

- તમને કોઇ લિંક પર ક્લીક કરવાનું કહે.

સ્કેમરો તમે જાણતા હોવ અને વિશ્વાસ કરતાં હોવ તેવી સંસ્થા હોવાનો ડોળ પણ કરી શકે.

ઉદાહરણ તરીકે, તમારી બેંક.

તમે તેમને તમારી અંગત માહિતી આપો તે માટે સ્કેમરો આવું કરે છે.

જો તમને લાગે કે વ્યક્તિ સ્કેમર છે તો તમારે તેમની સાથે વાત કરવાનું બંધ કરી દેવું જોઇએ.

વ્યક્તિ પોતે જે હોવાનો ડોળ કરે છે તે સાચે છે કે કેમ તેની તમારે તપાસ કરવી જોઇએ.

તમે પોતે શોધેલી અને તમને વિશ્વાસ હોય તેવી સંપર્ક વિગતોનો ઉપયોગ કરીને તમે તે વ્યક્તિ અથવા સંસ્થાનો સંપર્ક કરી શકો છો.

જો કંઇક ખોટું જણાય તો પોતાને સુરક્ષિત કરવા ઝડપથી પગલાં લો.

છેતરપિંડીની જાણ કરવી

ઓસ્ટ્રેલિયાનાં લોકોને નીચેની બાબતોમાં સ્કેમવોચ મદદ કરે છે:

- છેતરપિંડીઓ સમજવામાં
- છેતરપિંડીની જાણ કરવામાં.

છેતરપિંડીનો અનુભવ કર્યો હોય તેવા ઓસ્ટ્રેલિયાનાં લોકોને પણ સ્કેમવોચ મદદ કરે છે.

તમે સ્કેમવોચ વેબસાઇટ પર છેતરપિંડીની જાણ કરી શકો છો.

www.scamwatch.gov.au/report-a-scam

અવાજ ઉઠાવો

અન્ય લોકો કઇ રીતે પોતાની જાતને ઓનલાઇન સુરક્ષિત રાખી શકે છે તે વિશે તમારે અવાજ ઉઠાવવો જોઇએ.

આમાં નીચેનાનો સમાવેશ થાય છે:

- સાયબર ગુનાની જાણ કરવી

- તમે જે જાણતાં હોવ તેની પરિવારજનો અને મિત્રોને જાણ કરવી.

તમે અવાજ કઇ રીતે ઉઠાવી શકો છો તે અમે હવે પછીનાં પાનાંઓમાં સમજાવીશું.

સાયબર ગુનાની જાણ કરો

સાયબર ગુનાની જાણ કરવાથી સરકારને મદદ થાય છે:

- સાયબર ગુનેગારો કઇ રીતે લોકો પર હુમલો કરવાનો પ્રયત્ન કરે છે તે જાણો

- વધુ લોકોને સુરક્ષિત કરો.

તમે રીપોર્ટસાયબર વેબસાઇટ પર સાયબર ગુનાની જાણ કરી શકો છો.

www.cyber.gov.au/report

ઓનલાઇન સુરક્ષિત રહેવા અંગે પરિવારજનો અને મિત્રો સાથે વાતચીત કરો.

તમારે તમારા પરિવારજનો અને મિત્રોને તમારી ઓનલાઇન સુરક્ષિત રહેવાની યુક્તિઓની જાણ કરવી જોઇએ.

તમે પણ તેમની પાસેથી શીખી શકો છો.

ઓનલાઇન સુરક્ષિત રહેવા અંગે તમે જે જાણતાં હોવ તેની આપલે કરીને તમે પોતાની અને તમારી આસપાસનાં લોકોની સુરક્ષા કરી શકો છો.

જો તમે અને બીજા લોકો એક જ ઉપકરણ વાપરતાં હોય તો પણ મહત્વપૂર્ણ છે.

શબ્દાવલી

આ સૂચિ આ માર્ગદર્શીકામાં આવતાં **ઘાટા** શબ્દોનો અર્થ શું થાય છે તે સમજાવે છે.

સાયબર

સાયબર એટલે ઇન્ટરનેટને લગતું કશુંક.

સાયબર ગુનો

સાયબર ગુનો એટલે જ્યારે ગુનેગારો ગુનો કરવા માટે ઇન્ટરનેટનો ઉપયોગ કરે.

ઉદાહરણ તરીકે, તેઓ ઇન્ટરનેટના ઉપયોગથી:

- તમારી અંગત માહિતી ચોરે
- તમારા ઓનલાઇન ખાતાને કાબૂમાં લઇ લે.

લોકેશન સેટિંગો

લોકેશન સેટિંગો તમારું ઉપકરણ ક્યાં છે તે દર્શાવે છે.

બહુપરિબળ-પ્રમાણક (મલ્ટી-ફેક્ટર ઓથેન્ટીકેટર (એમએફએ)

એમએફએ એટલે કે જ્યારે તમે તમારા ખાતામાં લોગીન કરવા માટે દર વખતે ૨ કે તેથી વધુ જુદાજુદા રસ્તાઓનો ઉપયોગ કરો.

પાસફ્રેઝ

પાસફ્રેઝ એ મજબૂત પ્રકારનો પાસવર્ડ છે.

તે શું હોય શકે તેનું અનુમાન કરવું અન્ય લોકો માટે ઘણું અઘરું હોય છે.

જાહેર વાઇ-ફાઇ

જાહેર વાઇ-ફાઇ તાર વગરનું મફત ઇન્ટરનેટ છે જે તમે જાહેર સ્થળોએ વાપરી શકો છો.

છેતરપિંડી

અમે એને છેતરપિંડી કહીએ છીએ કે જ્યારે કોઇ પ્રયાસ કરે:

- તમને છેતરવાનો
- તમારા નાણાં પડાવવાનો.

સ્કેમરો

જે છેતરપિંડી કરે તે સ્કેમર છે.

અમારો સંપર્ક કરો

તમે ઓસ્ટ્રેલિયન સાયબર સીક્યોરિટી હોટલાઇનને ફોન કરી શકો છો.

1300 292 371

તમે અમારી વેબસાઇટની મુલાકાત લઇ શકો છો.

www.actnowstaysecure.gov.au

તમે રીપોર્ટસાયબર વેબસાઇટ પર સાયબર ગુનાની જાણ કરી શકો છો.

www.cyber.gov.au/report

ઇન્ફોર્મેશન એક્સેસ ગ્રુપે સ્ટોક ફોટોગ્રાફી અને ખાસ તૈયાર કરેલ છબીઓનો ઉપયોગ કરીને આ સરળ વાંચન દસ્તાવેજ બનાવ્યો છે. પરવાનગી વગર છબીઓનો પુર્નઉપયોગ ન કરી શકાય તેવું બને. છબીઓ અંગે કોઇ પણ પુછપરછ માટે www.informationaccessgroup.comની મુલાકાત લો. કામ નંબર ૬૩૪૨ આપો.