Australian Government

දැන්ම ක්‍රියාත්මක වන්න.
ආරක්ෂිතව සිටින්න.

ඔබට ආරක්ෂා සහිතව මාර්ගගත විය හැක්කේ කෙසේද

පහසුවෙන් කියවිය හැකි සංස්කරණය

Easy Read

මේ මාර්ගෝපදේශය භාවිතා කරන්නේ කෙසේද

අපි ඔස්ට්‍රේලියානු රජය වෙමු.

මේ මාර්ගෝපදේශය සකසන ලද්දේ අප විසිනි.

සමහර වචන අපි **තද වර්ණයෙන්** මුද්‍රණය කර ඇත්තෙමු.

එම වචනවල අර්ථය අපි පැහැදිලි කර දී ඇත.

එම වචන ලැයිස්තුව 28 වන පිටුවේද දැක්වේ.

ඔබට විශ්වාස කටයුතු අයෙකු වෙතින් පහත දැක්වෙන සහය ඉල්ලා සිටීමට ඔබට පුළුවන:

- මේ මාර්ගෝපදේශය කියවා දීමට
- වැඩිදුර තොරතුරු සොයා ගැනීමට.

මේ වෙනත් මාර්ගෝපදේශයක පහසුවෙන් කියවිය හැකි සංස්කරණයයි.

මෙහි අඩංගු කර ඇත්තේ වඩාත්ම වැදගත් අදහස් පමණි.

මාර්ගෝපදේශය අපගේ වෙබ් අඩවියෙන් ඔබට ලබා ගත හැක.

www.actnowstaysecure.gov.au

මේ මාර්ගෝපදේශයේ අඩංගු මොනවාද?

මේ මාර්ගෝපදේශය ගැන	4
ඔබේ ගිණුම් ආරක්ෂිතව තබාගන්න	6
ඔබේ තොරතුරු ආරක්ෂා කරගැනීම පිණිස ඔබේ සැකසුම් පිරික්සන්න	10
ඔබේ උපාංග ආරක්ෂා කරගන්න	16
වංචා	20
කතා කරන්න	25
වචන ලැයිස්තුව	28
අප අමතන්න	30

මේ මාර්ගෝපදේශය ගැන

ආරක්ෂිතව මාර්ගගත විය හැක්කේ කෙසේද යන්න පිළිබඳව අපි සැමදෙනා සිතා බැලිය යුතුය.

මෙය **සයිබර් ආරක්ෂාව** ලෙස අපි හඳුන්වමු.

සයිබර් යන්නෙහි තේරුම යම්කිසි දෙයක් අන්තර්ජාලය හා සම්බන්ධ වී තිබීමයි.

ආරක්ෂිතව මාර්ගගත වීම පිණිස ඔබට කළහැකි දේවල් සමහරක් මේ මාර්ගෝපදේශයෙන් පැහැදිලි කර ඇත.

උදාහරණයක් ලෙස, **සයිබර් අපරාධවලින්** ආරක්ෂාවීමට.

අපරාධකරුවන් විසින් අපරාධ සඳහා අන්තර්ජාලය භාවිතා කරන විට එය සයිබර් අපරාධ ලෙස හැඳින්වේ.

උදාහරණයක් ලෙස, ඔවුන් පහත දෑ සඳහා අන්තර්ජාලය භාවිතා කිරීමට ඉඩ ඇත:

- ඔබේ පුද්ගලික තොරතුරු සොරකම් කිරීම සඳහා
- ඔබේ මාර්ගගත ගිණුම් සහ ඔබේ වැදගත් තොරතුරු (profiles) අත්කර ගැනීම සඳහා.

සයිබර් අපරාධ ඕනෑම මෙවලමක සිදුවිය හැක.

ඔබේ පහත දැක්වෙන මෙවලම් මීට ඇතුලත් වේ:

- පරිගණකය
- ස්මාර්ට් ජංගම දුරකථනය
- ස්මාර්ට් ඔරලෝසුව.

සයිබර් අපරාධවලින් ආරක්ෂිතව සිටීමට ඔබ විසින් කල හැකි දේ ඇත.

ඔබට කල හැකි දෑ පහත පිටුවල අප පැහැදිලි කරන්නෙමු.

ඔබේ ගිණුම් ආරක්ෂිතව තබාගන්න

ඔබේ මාර්ගගත ගිණුම් ආරක්ෂිතව තබාගන්නේ කෙසේද යන්න ගැන ඔබ සිතා බැලිය යුතුය.

ශක්තිමත් සහ අසමාන මුරපද භාවිතා කරන්න

මුරපදයක් යනු වඩා ශක්තිමත් මුරවචනයකි.

අන් අයට එය අනුමාන කිරීම ඉතා අසීරුය.

ශක්තිමත් සහ අසමාන මුරපද භාවිතය ඔබේ ගිණුම් ආරක්ෂිතව තබාගැනීමට මනා උපක්‍රමයකි.

ඔබේ සෑම මාර්ගගත ගිනුමකටම එකිනෙකට අසමාන මුරපදයන් භාවිතා කල යුතුය.

ශක්තිමත් මුරපදයන්ට පහත දෑ ඇතුලත් වේ:

- අහඹු වචන 4ක් හෝ ඊට වැඩි ගණනක්
- අකුරු සහ අංක 15ක් හෝ ඊට වැඩි ගණනක්.

කැපිටල් අකුරු කීපයක් ඔබට අඩංගු කල හැකිය.

මෙවැනි සංකේත ඔබට පාවිච්චි කල හැකිය:

- කඩ ඉරක්
- ඩොලර් ලකුණ
- ඊමේල් @ ලකුණ.

ඔබේ මුරපදවල කිසිම පුද්ගලික තොරතුරක් ඔබ භාවිතා නොකළ යුතුය.

උදාහරණ ලෙස:

- ඔබේ උපන් දිනය
- ඔබේ පවුලේ සාමාජිකයන්ගේ හෝ සුරතල් සතුන්ගේ නම්.

ඔබේ ගිණුම්වලට ඇතුල්වීම සඳහා අමතර පියවර එකතු කරන්න

බහු-සාධක සත්‍යාපනය (MFA) මගින් ඔබේ මාර්ගගත ගිණුම් ආරක්ෂා කරගත හැකිය.

MFA යනු ඔබේ ගිණුමට ඇතුල්වීම සඳහා සෑම විටකම අසමාන ක්‍රම 2ක් හෝ ඊට වැඩි ක්‍රම ගණනක් භාවිතා කිරීමයි.

උදාහරනයක් ලෙස, ඔබට පළමුවෙන් ඔබේ මුරපදය ඇතුල් කිරීමට යොදා ගත හැක.

ඉන් පසු ඔබේ දුරකතනයට ලැබෙන කේතයක් ඇතුල් කල හැකිය.

ඔබට පහත විකල්ප තිබිය හැකිය:

- කේතයක් ලබා ගැනීම පිණිස ඔබේ දුරකථනයට යෙදුමක් (app) ස්ථාපනය කරගන්න

- කේතය ඊමේල් හරහා ලබාගන්න

- කේතය කෙටි පණිවිඩයක් හරහා ලබාගන්න.

MFA මගින් ඔබේ මාර්ගගත ගිණුම්තුලට අන් අයට ඇතුල්වීම අපහසු කරයි.

ඔබේ මුරපදය ඔවුන් විසින් සොයාගනු ලැබුවද.

ඔබේ තොරතුරු ආරක්ෂා කරගැනීම පිණිස ඔබේ සැකසුම් පිරික්සන්න

ඔබේ සැකසුම් මගින් ඔබේ මාර්ගගත තොරතුරු ආරක්ෂා කරයිද යන්න ඔබට පිරික්සා බැලීමට පුළුවන.

මෙයට පහත පෙනෙන ඔබේ සැකසුම් අඩංගු වේ:

- මාර්ගගත ගිණුම්
- උපාංග
- යෙදුම්.

ඔබට මෙසේ කල හැකිය:

- ඔබේ සැකසුම් වෙනස් කරන්න
- ඔබේ තොරතුරු භාවිතා කල හැක්කේ කුමන යෙදුම්වලට (app) දැයි තෝරාගන්න.

ඔබේ උපාංගයේ සැකසුම් ඔබට මෙසේ සොයා ගත හැකිය:

- ගියර් නිරූපකය බැලීමෙන්

  හෝ

- ඔබේ උපාංගයේ සෙවුම් තීරුවෙහි 'settings' යන වචනය ටයිප් කිරීමෙන්.

ඔබේ යෙදුමේ හෝ මාර්ගගත ගිණුමේ මෙනු පත විවෘත කිරීමෙන් සැකසුම් ඔබට බලා ගත හැකිය.

මෙනු පත බොහෝ විට තිරස් රේඛා තුනක් ලෙස පෙන්නුම් කරයි.

සමහර සැකසුම්වල පහත තොරතුරු සටහන් වියහැක:

- ඔබ කවුද
- ඔබ සිටින ස්ථානය
- ඔබ පදිංචි ස්ථානය.

මේ තොරතුරු මාර්ගගතව බෙදා ගැනීම ඔබව සයිබර් අපරාධවලට ගොදුරුවීමේ අවදානමට ලක් කරයි.

සයිබර් අපරාධකරුවන්ට ඔබ වෙනුවෙන් පෙනී සිටීමට මේ තොරතුරු භාවිතා කල හැකිය.

උදාහරණයක් ලෙස, ඔවුන් පහත තොරතුරු භාවිතා කිරීමට ඉඩ ඇත:

- ඔබ පදිංචි කොහිද

- ඔබේ පවුලේ සාමාජිකයන්ගේ නම්

- ඔබේ සුරතල් සතුන්ගේ නම්.

ඔබ පිළිබඳ සමාජ මාධ්‍යතුල ඇති තොරතුරු, ඔබ දන්නා අයට පමණක් පෙනෙන සේ ඔබේ ගිණුම් සකසා ගත හැකිය.

උදාහරණයක් ලෙස, ඔබේ ෆේස්බුක් පැතිකඩ තොරතුරු.

මේ සැකසුම් සාමාන්‍යයෙන් පුද්ගලිකත්ව (privacy) සැකසුම් ලෙස හැඳින්වේ.

ඔබට ඔබේ **ස්ථාන සැකසුම්ද (location settings)**.

පාලනය කල හැකිය.

ස්ථාන සැකසුම් ඔබේ උපාංගය තිබෙන ස්ථානය පෙන්වයි.

ඔබට ස්ථාන සැකසුම් සක්‍රීය හෝ අක්‍රීය කර ගත හැකිය.

ඔබේ ස්ථාන සැකසුම් භාවිතා කලහැක්කේ කිනම් යෙදුම් විසින්ද යන්න ඔබට තොරාගත හැක.

මෙය ඔබට පහත දේවල් සඳහා යොදා ගත හැක:

- මාර්ගගත ගිණුම්
- උපාංග
- යෙදුම්.

සමහර යෙදුම් පහත සඳහන් දේ සඳහාද ඔබෙන් අවසර ඉල්ලනු ඇත:

- ඔබේ කැමරාව භාවිතා කිරීමට

- ඔබේ ඡයාරූප බැලීමට.

ඔබේ කැමරාව සහ ඡයාරූප භාවිතා කිරීමට අනුමැතිය ලබාදිය යුත්තේ ඔබ දන්නා හුරු පුරුදු යෙදුම්වලට පමණි.

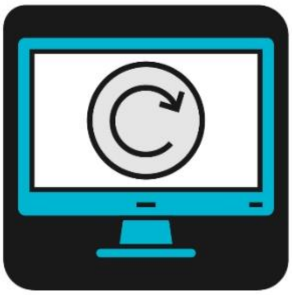
ඔබේ උපාංග ආරක්ෂා කරගන්න

මාර්ගගතව ඔබ ආරක්ෂා වීම පිණිස ඔබේ උපාංග ආරක්ෂා කරගත හැක්කේ කෙසේද යන්න පිළිබඳ ඔබ සිතා බැලිය යුතුය.

උදාහරණ ලෙසට, ඔබේ දුරකථනය සහ ස්මාර්ට් ඔරලෝසුව.

අන්තර්ජාලයට සම්බන්ධ වන උපාංග සඳහා මෙය වැදගත් වේ.

ඔබේ උපාංග යාවත්කාලීන කරගන්න



ඔබේ උපාංග මාර්ගගතව ආරක්ෂිතව තබා ගැනීම පිණිස ඒවා යාවත්කාලීන කරගැනීමට ඔබට හැකිය.

උදාහරණ ලෙසට, ඔබේ දුරකථනය සහ ලැප්ටොප්.

ඔබේ උපාංගය විසින් මෙය හඳුන්වන්නේ මෘදුකාංග යාවත්කාලීන කිරීම ලෙසටය.

යාවත්කාලීන කිරීමේ උපාංගයක් සයිබර් අපරාධවලින් ආරක්ෂා වීමට උපකාරී වේ.

උපාංගයකට එමගින් යාවත්කාලීන වීමට ඔබට සැලැස්විය හැකිය.

අපේ වෙබ්අඩවිය තුලින් ඔබේ උපාංග යාවත්කාලීන කරගන්නා අන්දම ගැන වැඩිදුර ඔබට උගත හැකිය.

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

පොදු වයි-ෆයි ජාල

පොදු වයි-ෆයි භාවිතා කිරීමේදී ඔබ ප්‍රවේසම් විය යුතුය.

පොදු වයි-ෆයි යනු පොදු ස්ථාන වලදී ඔබට නොමිලේ භාවිතා කල හැකි රැහැන් රහිත අන්තර්ජාලයයි.

උදාහරණ ලෙසට මේ ස්ථාන වලදී:

- කැෆේ
- ගුවන්තොටුපල
- හෝටලයක.

පොදු වයි-ෆයි හරහා භාවිතාකල වෙබ්අඩවිවලට ඔබ ඇතුල් කරන තොරතුරු ගැන ඔබ ප්‍රවේසම් විය යුතුයි.

උදාහරණ ලෙස, ඔබේ:

- බැංකු තොරතුරු
- ඊමේල් ගිණුම්
- සමාජ මාධ්‍ය පැතිකඩ.

සමහර සයිබර් අපරාධකරුවන් මේ දේ සඳහා පොදු වයි-ෆයි භාවිතාකිරීමට ඉඩ ඇත:

- ඔබ මාර්ගගතව කරන්නේ කුමක්දැයි බැලීමට
- ඔබේ තොරතුරු සොරකම් කිරීමට.

ඒ පහත හේතු නිසාය:

- ඕනෑම අයෙකුට එය භාවිතා කිරීමට හැකි නිසා

- ඔබේ උපාංගය ආරක්ෂාකිරීම වඩාත් උගහට නිසා.

පොදු වයි-ෆයි භාවිතා කරන විට ඔබට ආරක්ෂා වියහැක්කේ කෙසේද යන්න අපේ වෙබ්අඩවිය තුලින් ඔබට උගත හැක.

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

වංචා

යමෙකු පහත දෑ කිරීමට උත්සාහ කරනවිට අපි එය **වංචාවක්** ලෙස හඳුන්වන්නෙමු:

- ඔබව රැවටීමට
- ඔබේ මුදල් ලබාගැනීමට.

වංචා කරන පුද්ගලයා **වංචනිකයෙකි.**

වංචනිකයින් ඔබ පහත ආකාරයට රැවටීම උත්සාහ කිරීමට ඉඩ ඇත:

- කෙටි පණිවිඩයක් හෝ දුරකථන ඇමතුමක් මගින්
- ඊමේල් මගින්
- සමාජ මාධ්‍ය මගින්
- වෙබ් අඩවියකින්.

ඔවුන් මිත්‍රශීලී ලෙස පෙනෙනු ඇත.

නමුත් ඔබේ තොරතුරු ඔවුන්ට ලබා දෙන ලෙසට ඔබ රැවටීමට පුළුවන.

ඔවුන්ට පහත පෙනෙන අන්දමට භාවිතා කිරීමට හැකිය:

- ඔබේ මාර්ගගත ගිණුම්වලට ඇතුල්වීමට

- ඔබ ලෙසින් පෙනීසිටීමට

- ඔබේ මුදල් සොරා ගැනීමට.

වංචනිකයින් විසින් පහත සඳහන් දේ කිරීමටද පුළුවන:

- බව රැවටීමට ව්‍යාජ ගිණුම් නිර්මාණය කිරීම

- ඔබව රැවටීමට සබැඳියා සහ දැන්වීම් බෙදාගැනීම.

වංචාවක් හඳුනාගන්නේ කෙසේද

පහත දේ සිදු වේ නම් එය වංචාවක් විය හැකිය:

- යම් දෙයක් කඩිනමින් කරන ලෙස ඔබෙන් ඉල්ලීම

- ඔබට විසාල මුදල් ප්‍රමාණයක් පිරිනැමීම

- ඔබෙන් මුදල් ඉල්ලීම

- යම් සබැඳියක් මත ක්ලික් කරන ලෙස ඔබෙන් ඉල්ලීම.

ඔබ දන්නා සහ ඔබට විශ්වාස කටයුතු සංවිධානයක් ලෙස වංචනිකයින් පෙනී සිටීමටද පුළුවන.

උදාහරනයක් ලෙස, ඔබේ බැංකුව.

වංචනිකයින් එසේ කරනුයේ ඔබේ පුද්ගලික තොරතුරු ඔවුන් සමග බෙදාගැනීම සිදුකිරීමටය.

යමෙකු වංචනිකයෙකු යයි ඔබ සිතන්නේ නම් ඔබ ඔවුන් සමග කතාකිරීම නැවැත්විය යුතුය.

ඒ පුද්ගලයා ඔවුන් කියන පුද්ගලයාම ද යන්න ඔබ පිරික්සා බැලිය යුතුය.

ඔබ විශ්වාසකරන සහ ඔබ විසින්ම සොයාගත් විස්තර අනුසාරයෙන් ඔබට එම පුද්ගලයා හෝ සංවිධානය ඇමතීමට පුළුවන .

යමක් අසත්‍ය බව ඔබට හැඟුනහොත් ඔබ ආරක්ෂාවීම පිණිස ඉක්මනින් ක්‍රියා කරන්න .

වංචාවක් පිළිබඳ වාර්තා කිරීම

ඔස්ට්‍රේලියානුවන්ට Scamwatch මගින් පහත සහය ලබා දේ:

- වංචා තේරුම් ගැනීම
- වංචා වාර්තා කිරීම.

වංචාවන්ට මුහුණදුන් ඔස්ට්‍රේලියානුවන්ටද Scamwatch උදවු කරයි.

වංචාවක් පිළිබඳව ඔබට Scamwatch වෙබ් අඩවියෙහි වාර්තා කල හැකිය.

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

කතා කරන්න

අන් උදවියට මාර්ගගතව ආරක්ෂා විය හැක්කේ කෙසේද යන්න ගැන ඔබ විසින් කතාබහ කල යුතුය.

මීට ඇතුලත් වනුයේ:

- සයිබර් අපරාධ වාර්තා කිරීම

- ඔබ දන්නා දේ පවුලේ උදවිය සහ මිතුරන් අතර බෙදාගැනීම.

ඔබට මේ පිළිබඳව කතා කලහැක්කේ කෙසේද යන්න පහත පිටු වලින් අපි ඔබට පැහැදිලි කර දෙන්නෙමු.

සයිබර් අපරාධ වාර්තා කරන්න

සයිබර් අපරාධ වාර්තා කිරීමෙන් රජය උපකාරී වේ:

- සයිබර් අපරාධකරුවන් පුද්ගලයන් හට ප්‍රහාර එල්ල කරන අන්දම ඉගෙනීම

- පුද්ගලයින් වැඩිදෙනෙකු ආරක්ෂා කිරීම.

සයිබර් අපරාධ වෙබ් ReportCyber අඩවියෙහි ඔබට වාර්තාකිරීමට පුළුවන.

www.cyber.gov.au/report

ආරක්ෂා සහිතව මාර්ගගතව සිටීම ගැන පවුලේ අය සහ මිතුරන් සමග කතාකරන්න

ආරක්ෂා සහිතව මාර්ගගතව සිටීම පිළිබඳ ඔබේ හෝඩුවාවන් ඔබේ පවුලේ අය සහ මිතුරන් සමග බෙදාගන්න.

ඔබටද ඔවුන්ගෙන් ඉගෙනීමට පුළුවන.

ආරක්ෂිතව මාර්ගගතව සිටීම ගැන ඔබ දන්නා දේ බෙදාගැනීමෙන් ඔබ සහ ඔබ වටා සිටින අයවද ඔබට ආරක්ෂා කල හැකිය.

ඔබ අන් අය සමග උපාංග බෙදාගන්නේ නම් මෙය වැදගත් ය.

වචන ලැයිස්තුව

මේ මාර්ගෝපදේශයේ **තද වර්ණයෙන් මුද්‍රිත** වචනවල තේරුම මේ ලැයිස්තුවෙන් පැහැදිලි කරනු ලැබේ.

සයිබර්

සයිබර් යන්නෙහි තේරුම යම් දෙයක් අන්තර්ජාලය හා සම්බන්ධ වී තිබීමයි.

සයිබර් අපරාධ

අපරාධකරුවන් අපරාධ පිණිස අන්තර්ජාලය භාවිතා කරන විට එය සයිබර් අපරාධ වේ.

උදාහරණ ලෙස, ඔවුන් පහත දෑ සඳහා අන්තර්ජාලය භාවිත කිරීමට පුළුවන:

- ඔබේ පුද්ගලික තොරතුරු සොරකම් කිරීමට
- ඔබේ මාර්ගගත ගිණුම් අත්කර ගැනීමට.

ස්ථාන සැකසුම්

ස්ථාන සැකසුම් මගින් ඔබේ උපාංගය තිබෙන්නේ කොහිද යන්න පෙන්නුම් කෙරේ.

බහු සාධක සත්‍යාපනය (MFA)

MFA යනු ඔබේ ගිණුමට ඇතුල්වීම සඳහා සැම විටකම ක්‍රම 2ක් හෝ ඊට වැඩි ක්‍රම ගණනක් පාවිච්චි කිරීමයි.

මුරපදය

මුරපදයක් යනු වඩා ශක්තිමත් මුරවචන වර්ගයකි.

අන් අයට එය අනුමානකිරීම ඉතාමත් අසීරුය.

පොදු වයි-ෆයි

පොදු වයි-ෆයි යනු පොදු ස්ථාන වලදී ඔබට නොමිලේ භාවිතා කිරීමට හැකි රැහැන් රහිත අන්තර්ජාලයයි.

වංචා

කෙනෙක් පහත දෑ කිරීමට උත්සාහ කරන විට අපි එය වංචාවක් ලෙස හඳුන්වන්නෙමු:

- ඔබව රැවටීමට
- ඔබේ මුදල් ගැනීමට.

වංචනිකයෝ

වංචා කරන පුද්ගලයා වංචනිකයෙකි.

අප අමතන්න

Australian Cyber Security Hotline ක්ෂණික ඇමතුම් සේවය 1300 292 371

ඔබට අපගේ වෙබ් අඩවියට පිවිසීමට හැක.

www.actnowstaysecure.gov.au

ඔබට ReportCyber වෙබ් අඩවියෙහි සයිබර් අපරාධ වාර්තා කළහැක.

www.cyber.gov.au/report

Information Access Group විසින්මෙම Easy Read (පහසුවෙන් කියවිය හැකි) ලේඛනය මේ සඳහාම නිර්මිත ඡයාරූප සහ පෙර පැවති පිළිරූ ආශ්‍රයෙන් නිර්මාණය කරන ලදී. මෙකී පිළිරූ අවසර රහිතව යළි භාවිතා නොකළ යුතුය. මෙකී පිළිරූ පිළිබඳ විමසීම් සඳහා කරුණාකර www.informationaccessgroup.com වෙබ් අඩවියට පිවිසෙන්න. කාර්ය අංක 6342 ලෙස පවසන්න.