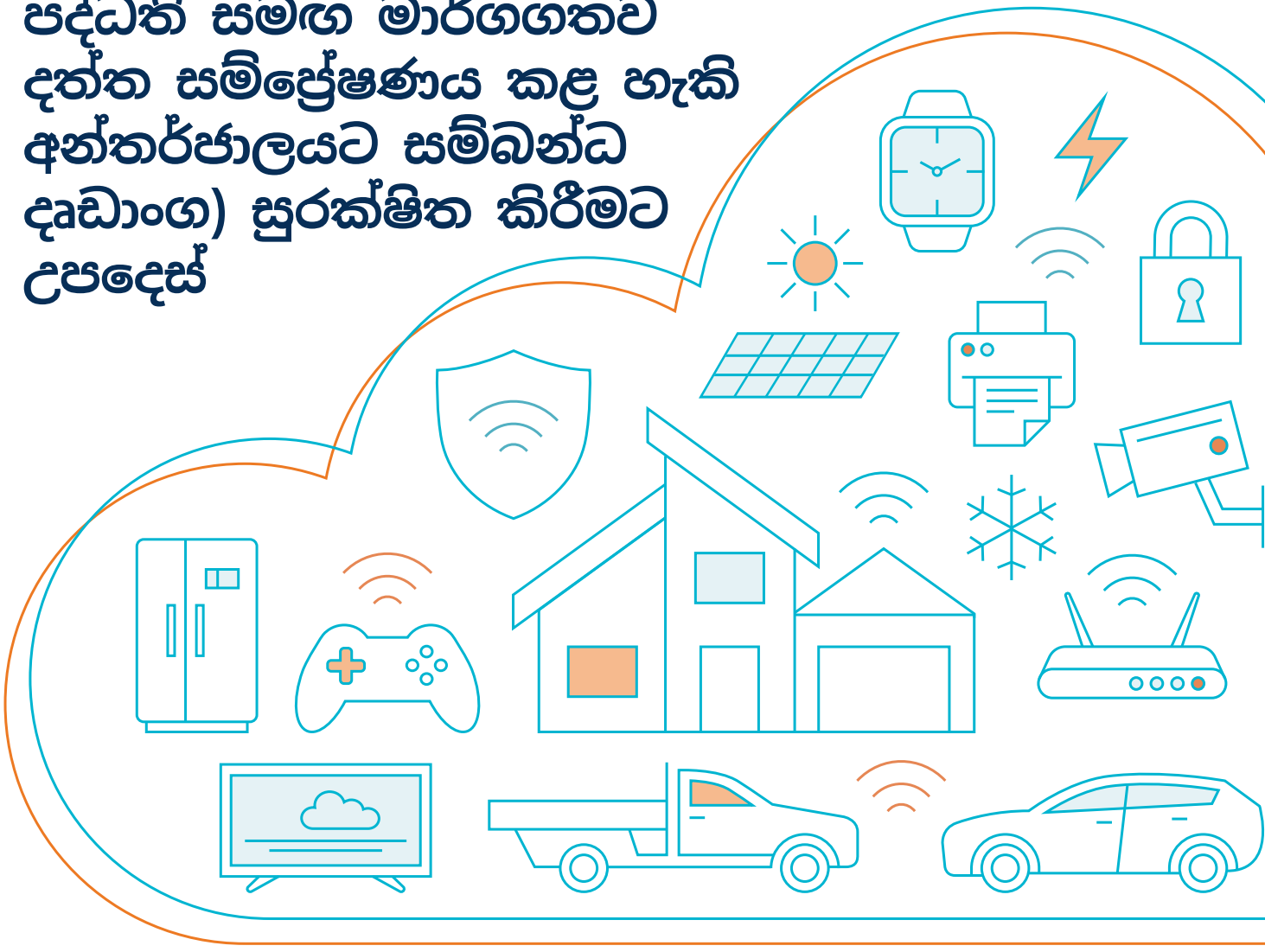
ඔබගේ IoT උපාංග (වෙනත් පද්ධති සමඟ මාර්ගගතව දත්ත සම්ප්‍රේෂණය කළ හැකි අන්තර්ජාලයට සම්බන්ධ දෘඩාංග) සුරක්ෂිත කිරීමට උපදෙස්



ඔස්ට්‍රේලියානු සයිබර් ආරක්ෂක මධ්‍යස්ථානය මෙම තොරතුරු සකස් කර ඇත්තේ ප්‍රජාවට IoT උපාංග ආරක්ෂිතව මිලදී ගැනීමට සහ භාවිතා කිරීමට උපකාර කිරීම සඳහා ය. IoT උපාංගයක් යනු අන්තර්ජාලය හා සම්බන්ධතාව එකතු කර ඇති එදිනෙදා භාවිතා කරන අයිතමයකි. IoT උපාංග සඳහා උදාහරණ ලෙස ළදරු මොනිටර, ඩ්‍රෝන යානා, ආරක්ෂක කැමරා, ස්මාර්ට් රූපවාහිනී සහ සූර්ය ඉන්වර්ටර් ඇතුළත් වේ. නිවාස සහ ව්‍යාපාර තුළ ඇති IoT උපාංග සාමාන්‍යයෙන් අන්තර්ජාලයට සම්බන්ධ කිරීමට Wi-Fi හෝ 4G හෝ 5G වැනි සෙලියුලර් ජාල භාවිතා කරයි.

ඔස්ට්‍රේලියානු නිවාස සහ ව්‍යාපාර තුළ තිබෙන බොහෝ IoT උපාංග ආරක්ෂාව ගැන ප්‍රමුඛත්වයක් දෙමින් නිර්මාණය කර නොමැත. මෙහි ප්‍රතිඵලයක් ලෙස මෙම උපාංග අන්තර්ජාලය හරහා අවදානමට ලක්වෙමින් පවතියි. එවැනි සිදුවීම් හේතුවෙන් සයිබර් අපරාධකරුවන්ට ද්වේශසහගත අරමුණු සඳහා ඔබගේ උපාංගයට සහ පුද්ගලික දත්ත වලට ප්‍රවේශ විය හැකිය.

IoT උපාංගයක් මිලදී ගැනීමට පෙර

නිෂ්පාදකයින් විවිධ මට්ටමේ ආරක්ෂාවක් සපයන බැවින්, මිලදී ගැනීමට පෙර උපාංග ගැන පර්යේෂණ කිරීම වැදගත් වේ. උපාංගයක් මිලදී ගැනීමට පෙර, විවිධ නිෂ්පාදකයින් විසින් විකුණන ලද සමාන උපාංග සංසන්දනය කරන්න. සලකා බැලිය යුතු කරුණු වන්නේ:

1. **උපාංගය ප්‍රසිද්ධ කීර්තිමත් සමාගමක් විසින් නිෂ්පාදනය කර ප්‍රසිද්ධ කීර්තිමත් වෙළඳසැලක් විසින් විකුණනු ලබන දෙයක් ද?** ප්‍රසිද්ධ කීර්තිමත් සමාගම් ආරක්ෂාවට ප්‍රමුඛතාවය දෙමින් උපාංග නිෂ්පාදනය කිරීමට වැඩි ඉඩක් ඇත. ප්‍රසිද්ධ කීර්තිමත් වෙළඳසැල් විසින් ප්‍රසිද්ධ කීර්තිමත් සමාගම් මගින් නිපදවන උපාංග පමණක් අලෙවි කිරීමට වැඩි ඉඩක් ඇති අතර, නිෂ්පාදකයා විසින් අදහස් කරන පරිදි උපාංගය ඔබ වෙත ලැබෙන බව සහතික කරන දැඩි සැපයුම් දාමයක් ඇත.

2. **මුරපදය වෙනස් කිරීමට හැකිද?** සෑමවිටම මුරපදය වෙනස් කිරීම යෝග්‍ය වේ. කෙසේ වෙතත්, උපාංගය දුර්වල, ස්වයංක්‍රීයව තෝරාගත් විකල්පය මුරපදයක් සහිතව සපයා ඇත්නම්, මෙය වඩාත් වැදගත්. හොඳ ආරක්ෂාවක් ඇති උපාංගයකට අද්විතීය, අනපේක්ෂිත, සංකීර්ණ හා අනුමාන කිරීමට නොහැකි මුරපද තිබිය යුතුය. ඒ මන්ද යත් දුර්වල, ස්වයංක්‍රීයව තෝරාගත් විකල්පය මුරපද, උපාංගයකට ප්‍රහාරයක් එල්ල කිරීමට ඇති පහසුම ක්‍රම වේ.

3. **නිෂ්පාදකයා යාවත්කාලීන කිරීම් සපයන්නේ ද?** උපාංග අවදානම් සොයා ගත් විට ඒවා නිවැරදි කිරීමට සමාගම් විසින් යාවත්කාලීන කිරීම් ලබා දීම වැදගත් වේ. උදාහරණයක් ලෙස, උපාංගයේ ඇති මෘදුකාංගවල දැන හඳුනාගත් අවදානම් තිබේ නම් හෝ හැකර්වරු ඔබේ උපාංගයට හානි කිරීමට නව ක්‍රම සංවර්ධනය කරන්නේ නම්, නිවැරදි කිරීම් සැපයීමට යාවත්කාලීන කිරීම් අවශ්‍ය වේ.

4. **උපාංගය කුමන දත්ත රැස් කරන්නේද සහ දත්ත බෙදා ගන්නේ කා සමඟද?** කුමන දත්ත රැස් කරන්නේද සහ එය භාවිතා කරන්නේ කෙසේද යන්න පිළිබඳ තොරතුරු නිෂ්පාදකයාගේ වෙබ් අඩවිය හෝ ඔවුන්ගේ රහස්‍යතා ප්‍රතිපත්තිය වෙතින් පහසුවෙන් ලබා ගත හැකිය. මාර්ගගත හෝ ජංගම යෙදුම මගින් රැස් කරන තොරතුරු සෑමවිටම සලකා බැලීම වැදගත් වේ.

5. **උපාංගය සිදු කරන්නේ ඔබට අවශ්‍ය දේ පමණක්ද?** අන්තර්ජාලයට සම්බන්ධ වීම ඇතුළුව ඔබට අවශ්‍ය දේට වඩා වැඩි යමක් කරන උපාංගයක් මිලදී ගැනීමෙන් ඔබේ ආරක්ෂාව අඩු විය හැකිය. ඔබ භාවිතා නොකරන උපාංග හැකියාවන් ඔබට කිසිදු ප්‍රතිලාභයක් ලබා නොදී උපාංගය ප්‍රහාරවලට ලක්වීමට ඇති අවදානම වැඩි කළ හැකිය.

IoT උපාංගය

ඔබගේ උපාංගය සැකසීමේදී සරල ප්‍රශ්න කිහිපයක් මතක තබා ගැනීමෙන්, ඔබේ ජාලය සහ දත්ත වඩාත් ආරක්ෂිතව තබා ගැනීමට ඔබට උපකාරී වේ.

1. **උපාංගය අන්තර්ජාලයට සම්බන්ධ කළ යුතුද?** එය සම්බන්ධ කළ හැකි නිසා එය එසේ කළ යුතු යැයි අදහස් නොවේ. අන්තර්ජාලයට සම්බන්ධ නොකරන ලද උපාංග අවදානමට ලක්වීමට ඇති ඉඩකඩ බෙහෙවින් අඩුය. න්තර්ජාල සම්බන්ධතාවය අවශ්‍ය වන විශේෂාංග ඔබ භාවිතා නොකරන්නේ නම්, එම සම්බන්ධය කළ යුතුද යන්න.

2. **උපාංගය තබ ඇත්තේ ආරක්ෂිත ස්ථානයක ද?** උපාංගය අනාරක්ෂිත තැනක ස්ථාපනය කිරීමට අවශ්‍ය නොවේ නම්, එය ආරක්ෂිත ස්ථානයක ස්ථාපනය කිරීම මගින් භෞතික අවදානමට ලක්වීමේ අනතුර අඩු කළ හැකිය.

3. **ස්වයංක්‍රීයව තෝරාගත් විකල්ප පරිශීලක නාමය සහ මුරපදය මා වෙනස්?** ඔබ ශක්තිමත් මුරපදයක් හෝ දිගු මුරපදයක් භාවිතා කිරීම. ඔබගේ උපාංගය අද්විතීය, අනපේක්ෂිත, සංකීර්ණ සහ අනුමාන කිරීමට නොහැකි මුරපදයක් සහිතව ප්‍රවහනය කර නොමැති නම් එම මුරපදය වෙනස් කළ යුතුය. ස්වයංක්‍රීයව තෝරාගත් විකල්ප පරිශීලක නාම සහ මුරපද එකතු කර මාර්ගගතව පළ කරනු ලැබේ. එමඟින් ඔබේ උපාංගය අවදානමට ලක් වේ.

4. **මම මගේ Wi-Fi ජාලය ආරක්ෂිතව සකසා තිබේද, එමෙන්ම එයට ආරක්ෂිත මුරපදයක් තිබේද?** ප්‍රහාරකයන්ට ඔබේ උපාංගයට සහ ඔබේ ජාලයට ප්‍රවේශ වීම දුෂ්කර කිරීම සඳහා ඔබේ Wi-Fi ජාලය සහ රවුටරය සුරක්ෂිත කරන්න.

අමතර වෑයමක් දරන්න

IoT උපාංග සඳහා පමණක් ඔබේ රවුටරයේ අමතර Wi-Fi ජාලයක් සකසන්න. ඔබගේ Wi-Fi රවුටරය මෙය 'ආගන්තුක' ජාලයක් ලෙස දැන සිටිය හැකිය. ඔබගේ IoT උපාංගයට එකිනෙකා අතර සන්නිවේදනය අවශ්‍ය නොවේ නම්, 'සේවාදායක හුදකලා කිරීමේ' විශේෂාංගය. ඔබගේ IoT උපාංග ඔබගේ සංවේදී දත්ත වලින් හුදකලා කර තබා ගැනීමෙන් IoT උපාංගයක් අවදානමට ලක්වීම මගින් ඔබගේ අනෙකුත් උපාංග හෝ දත්ත වෙත ප්‍රවේශය ලබා නොදෙන බව සහතික කෙරේ.

5. **අනවශ්‍ය උපාංග විශේෂාංග අක්‍රිය කර තිබේද?** ඔබගේ උපාංගයේ උවමනා නොකරන හෝ අනවශ්‍ය විශේෂාංග (කැමරා හෝ මයික්‍රෆෝන වැනි) තිබේ නම්, හැකි සෑම විටම ඒවා අක්‍රිය කළ යුතුය.

අමතර වෑයමක් දරන්න

දේශීය LAN හෝ WAN/අන්තර්ජාලය මගින් උපාංගයේ වෙබ් පරිපාලන අතුරුමුහුණතට දුරස්ථ ප්‍රවේශය සක්‍රීය කිරීම සඳහන් කෙරෙන වින්‍යාස සැකසුමක් සොයන්න. ඔබට දුරස්ථ ප්‍රවේශය අවශ්‍ය වන්නේ නම් මිස, එය දේශීය LAN වෙත සකසා ඇති බවට වග බලා ගන්න.

IoT උපාංගයක් නඩත්තු කිරීම

ඔබේ IoT උපාංගය සකසා භාවිතයට ගත් පසු මතක තබා ගත යුතු වැදගත් දේවල් කිහිපයක් තිබේ. ඒවාට ඇතුළත් වන්නේ:

1. **ඔබේ උපාංග නිතිපතා නැවත ආරම්භ කරන්න.** IoT උපාංගය මන්දගාමී වීමට පටන් ගන්නේ නම් හෝ ක්‍රියාත්මක කිරීමට නොහැකි නම්, බොහෝ අනිෂ්ට මෘදුකාංග මතකයේ ගබඩා කර ඇති අතර උපාංගය නැවත ආරම්භ කිරීමෙන්, එනම් උපාංගය ක්‍රියා විරහිත කර සක්‍රිය කිරීමෙන්. නැවත ආරම්භ කිරීමෙන් පසුව උපාංගය මන්දගාමී හෝ ක්‍රියාත්මක කිරීමට නොහැකිව පවතී නම්, එය මුල් තත්වයට යළි සකස් කිරීමට උත්සාහ කරන්න. කෙසේ වෙතත් මෙය ඔබගේ සියලු පරිශීලක දත්ත සහ පුද්ගලාරෝපිත සැකසුම් මකා දැමිය හැකි බව මතක තබා ගන්න.

2. **නිතිපතා යාවත්කාලීන කිරීම් යොදන්න.** සමහර උපාංග ස්වයංක්‍රීයව යාවත්කාලීන කිරීම් යොදයි. එසේ නොකරන ඒවා සඳහා, නිෂ්පාදකයා සමඟ නිතිපතා පරීක්ෂා කර යාවත්කාලීන කිරීම් ලබා ගත හැකි වූ විට ඒවා යොදන්න. ඔබේ උපාංගය සඳහා යාවත්කාලීන කිරීම් තවදුරටත් ලබාගත නොහැකි වූ විට, යාවත්කාලීන කිරීම් ලබා ගත හැකි නව උපාංගයකට උත්ශ්‍රේණි කිරීම සලකා බලන්න. නව අවදානම් අනාවරණය වුවහොත්, ආරක්ෂක යාවත්කාලීන කිරීම් සඳහා ප්‍රවේශය නොමැති උපාංග ආරක්ෂා නොවනු ඇති අතර, ඒවා ඔබගේ ජාලය, ඔබගේ පෞද්ගලිකත්වය සහ ඔබගේ දත්ත අවදානමට පත් කළ හැකිය.

3. **ඔබේ උපාංගය භාවිතා නොකරන විට එය ක්‍රියා විරහිත කරන්න.** භාවිතයට නොගත් සහ නිරීක්ෂණය නොකළ උපාංග දිගු කාලයක් ඔබගේ Wi-Fi ජාලයට සම්බන්ධ කර තැබීමෙන් ඔබගේ උපාංග වලට ප්‍රහාරයක් එල්ල වීමට ඇති හැකියාව වැඩි විය හැකිය. මෙය ස්වයංක්‍රීයව සපුරා ගැනීම සඳහා එක් විකල්පයක් නම්, නිශ්චිත වේලාවන් තුළ පමණක් උපාංගයට විදුලිය සැපයීම සඳහා විදුලි බල පිටවීමේ ටයිමරයක් භාවිතා කිරීමයි.

4. **ඔබේ මාසික අන්තර්ජාල භාවිතයේ හෝ බිල්පතේ සැලකිය යුතු වැඩි වීමක් සම්බන්ධව විමසිල්ලෙන් සිටින්න.** අන්තර්ජාල භාවිතයේ හෝ බිල්පත් ගාස්තුවල සැලකිය යුතු වැඩි වීමක් මගින් ඔබගේ උපාංගය අවදානමට ලක්ව ඇති බව පෙන්නුම් කළ හැකිය. මෙය ඔබේ ව්‍යාපාරයේ IT දෙපාර්තමේන්තුව විසින් විමර්ශනයට ලක් නොකරන්නේ නම්, මුල් තත්වයටයළි සකස් කිරීමක් යෙදිය යුතුය (කෙසේ වෙතත් මෙය ඔබගේ සියලු පරිශීලක දත්ත සහ පුද්ගලාරෝපිත සැකසුම් මකා දැමිය හැකි බව මතක තබා ගන්න), ඉන්පසු ඔබේ මුරපදය වෙනස් කළ යුතුය.

බැහැර කිරීම IoT උපාංගයක්

උපාංගයක් බැහැර කිරීම (එය ඉවත දැමීමෙන් හෝ විකිණීමෙන්) මගින් වෙනත් පුද්ගලයින්ට ඔබේ පුද්ගලික තොරතුරු හෝ දත්ත වෙත පහසුවෙන් ප්‍රවේශ වීමට ඉඩ ලබාදිය හැකිය. මෙය වැළැක්වීමේ ක්‍රම අතරට ඇතුළත් වන්නේ:

1. **සියලුම දත්ත සහ පුද්ගලික තොරතුරු මකා දැමීම.** උපාංගයෙන් සහ ඒ ආශ්‍රිත යෙදුම් යන දෙකෙන්ම ඔබේ දත්ත සහ පුද්ගලික තොරතුරු මකා දැමීම සඳහා නිෂ්පාදකයා ක්‍රමයක් සැපයිය යුතුය. ඔබේ පුද්ගලික තොරතුරු මකා දැමීම මගින් ඔබ උපාංගය බැහැර කළ පසු කිසිවෙකු එයට ප්‍රවේශ නොවන බව සහතික කරයි. IoT උපාංගය නොමැතිව ඔබේ මාර්ගගත ගිණුම තවදුරටත් අවශ්‍ය නොවේ නම්, එම ගිණුම මකා දමන්න.

2. **උපාංගය එහි මුල් තත්වයට යළි සකස් කිරීමට සිදු කරන්න.** මුල් තත්වයට යළි සකස් කිරීම සැලසුම් කර ඇත්තේ දේශීය ගබඩාවේ තබා ඇති දත්ත මකා දැමීමට සහ මුරපද, පරිශීලක නාම සහ සැකසුම් නැවත ස්වයංක්‍රීයව තෝරාගත් විකල්ප තත්වයට නැවත සැකසීම ය. මුල් තත්වයට යළි සකස් කිරීමක් සිදු කරන්නේ කෙසේද යන්න පිළිබඳ තොරතුරු සඳහා උපාංගයේ පරිශීලක අත්පොත හෝ නිෂ්පාදකයාගේ වෙබ් අඩවිය පරීක්ෂා කරන්න.

3. **ජංගම දුරකථන සහ අනෙකුත් උපකරණ වලින් උපාංගය විසන්ධි කරන්න.** ඔබගේ අනෙකුත් උපාංග, ජාල හෝ සබැඳි ගිණුම් වෙත තවමත් ප්‍රවේශය ඇති උපාංගයක් බැහැර කිරීම මගින් අන් අයට ප්‍රවේශය ලබා ගැනීමේ පුළුවන. ඔබගේ අනෙකුත් උපාංග පරීක්ෂා කර ඔබ බැහැර කරන උපාංගය සමඟ ඇති යම් යුගලීම් ඉවත් කිරීමට වග බලා ගන්න. තවදුරටත් අවශ්‍ය නොවන ජංගම යෙදුමට ලබා දී ඇති ඕනෑම අවසරයන් ඉවත් කරන්න.

4. **උපාංගයට අමුණා ඇති ඕනෑම ඉවත් කළ හැකි මාධ්‍යයක් (උදා: USB ෆ්ලෑෂ් ඩ්‍රයිව්, මතක කාඩ්පත් ආදිය) ඉවත් කරන්න.** මුල් තත්වයට යළි සකස් කිරීමකදී මකා නොදැමූ පුද්ගලික දත්ත ඉවත් කළ හැකි මාධ්‍යයේ අඩංගු විය හැකි අතර ඒවා භෞතිකව ඉවත් කර, භෞතිකව විනාශ කර උපාංගයෙන් වෙන වෙනම බැහැර කළ යුතුය.

සහාය

asd.assist@defence.gov.au විද්‍යුත් තැපෑලෙන් හෝ **1300 CYBER1 (1300 292 371)** ඔස්සේ හදිසි සහාය සඳහා 24/7 ක්ෂණික ඇමතුම් අංශය අමතන්න.

සයිබර් අපරාධ www.cyber.gov.au/report හරහා ReportCyber වෙත වාර්තා කරන්න

ඔබ අනන්‍යතා සොරකමකට මුහුණ දී ඇත්නම් IDCARE ඔවුන්ගේ වෙබ් අඩවිය වන www.idcare.org හරහා අමතන්න.

ඔබට සහ ඔබේ පවුලේ අයට උපදෙස් ලබා ගැනීම සඳහා www.cyber.gov.au වෙත පිවිසෙන්න. මෑත කාලීන මාර්ගගත තර්ජන පිළිබඳ නොමිලේ ACSC අනතුරු ඇඟවීම් සේවාව සඳහා ලියාපදිංචි වන්න.

ඔස්ට්‍රේලියාව මාර්ගගතව සම්බන්ධ වීමට වඩාත්ම ආරක්ෂිත ස්ථානය බවට පත් කරමු.

සයිබර් ආරක්ෂණ උපදෙස් සඳහා, පිවිසෙන්න www.cyber.gov.au

හිමිකම් අත්හැරීම

මෙම මාර්ගෝපදේශයේ ඇති තොරතුරු සාමාන්‍ය ස්වභාවයක් ගන්නා අතර එය නීති උපදෙසක් ලෙස හෝ කිසියම් විශේෂිත අවස්ථාවකදී හෝ හදිසි අවස්ථාවකදී සහාය සඳහා විශ්වසනීය දෙයක් ලෙස නොසැලකිය යුතුය. ඕනෑම වැදගත් කාරණයකදී, ඔබ ඔබේම තත්වයන් සම්බන්ධව සුදුසු ස්වාධීන වෘත්තීය උපදෙස් ලබා ගත යුතුය.

මෙම මාර්ගෝපදේශයේ අඩංගු කරුණු මත විශ්වාසය තැබීමේ ප්‍රතිඵලයක් ලෙස සිදුවන ඕනෑම හානියක්, අලාභයක් හෝ වියදමක් සඳහා මධ්‍යම රජය කිසිදු වගකීමක් හෝ වගකීමක් භාර නොගනී.

වැඩි විස්තර සඳහා, හෝ සයිබර් ආරක්ෂණ සිදුවීමක් වාර්තා කිරීමට, අපව අමතන්න:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

ඔස්ට්‍රේලියාව ඇතුලත පමණක් මෙම අංකය භාවිතා කිරීමේ හැකියාව පවතී.

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre