

සයිබර් අවකාශයේ
උවදුරු වලින් ගැලවෙමු
V 1.0 12/06/2020



COVID-19 වසංගත අවදානම හමුවේ ලොව පුරා රටවල් වල විදිහෙන කටයුතු වලට බරපතල සීමාවන් පැනවීමට සිදුවූ අවස්ථාවේදී ජනතාව භාණ්ඩ මිලදීගැනීම, රැකියා කටයුතු සහ අධ්‍යාපන කටයුතු ඇතුළු බොහෝ දේ සඳහා වැඩි වැඩියෙන් අන්තර්ජාලය භාවිතා කිරීමට යොමු වූහ. මෙය සැබෑවින්ම කාලෝචිත පරිවර්තනයක් වුවත් මෙම වෙනස්කම් සමග නව අභියෝග රාශියක්ද මතු වී තිබේ.

ජනතාව සයිබර් අවකාශය තුළ වැඩි කාලයක් ගතකිරීමට පටන් ගැනීමත් සමග සයිබර් අපරාධකරුවන්ද වඩාත් සක්‍රීය වී සිටිති. එය අන්තර්ජාලය භාවිතා කරන කාණේන් පෞද්ගලිකත්වයට මෙන්ම උපාංග වලටද බරපතල තර්ජනයකි. රහස් තොරතුරු ලබාගැනීම සඳහා කාර්යාලීය තොරතුරු ජාලයන්ට අනවසරයෙන් පිවිසීම, ඔත්තු බලන මෘදුකාංග ඇතුළු කිරීම සහ බැංකු ගිණුම් වලට අනවසරයෙන් පිවිසීම ඇතුළු බොහෝ අපරාධ නිසා ලොව පුරා විශාල පිරිසකට දැනටමත් බලපෑම් වල්ල වී ඇත.

මෙබඳු තර්ජන දිනෙන් දින ඉහළ යමින් තිබෙන පසුබිමක, ඔබගේ ආරක්ෂාව මෙන්ම ඔබ සතු ඩිජිටල් උපාංග වල ආරක්ෂාවද තහවුරු කරගැනීම සඳහා ලබාදෙන මගපෙන්වීමක් වශයෙන් මෙම උපදෙස් මාලාව පිළියෙල කර තිබේ.

අන්තර්ජාලය ඔස්සේ භාණ්ඩ මිලදීගැනීම

ආක්‍රමණිකයන් අන්තර්ජාලය තුළදී පාරිභෝගිකයන් ගොදුරු කරගන්නේ කෙසේද?

ඔබගේ පෞද්ගලික තොරතුරු වංචනිකයන් අතට පත්වීම වැළැක්වීම සඳහා අතිශයින් සැලකිලිමත් විය යුතුය. එම නිසා, අන්තර්ජාලය ඔස්සේ ගනුදෙනු සිදුකිරීමේදී ඔබ අනිවාර්යයෙන් මතක තබාගත යුතු කරුණු කිහිපයක් ඇත.

සාමාන්‍යයෙන් ආක්‍රමණිකයන් අන්තර්ජාලයේදී පාරිභෝගිකයන් ගොදුරු කරගැනීම සඳහා භාවිතා කරන ක්‍රම කිහිපයක් තිබේ.

01 වංචනික වෙබ් අඩවි සහ ඊමේල් පණිවිඩ මගින්:

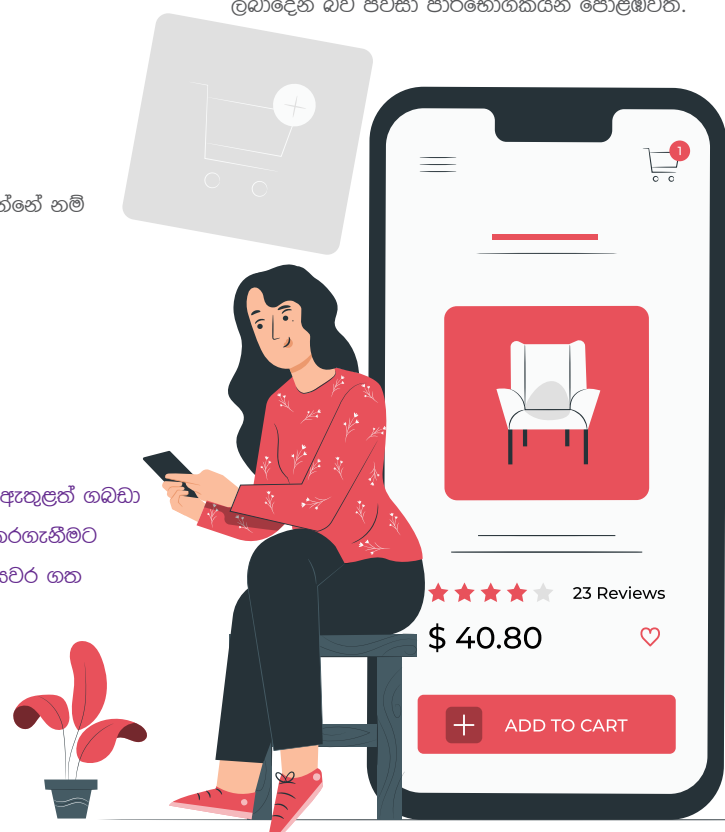
- සැබෑ ලෝකයේදී ඔබ සුපිරි වෙළඳසැලක් වැනි ස්ථානයක් වෙත ගිය විට, එම ස්ථානය ගැන ඔබට ප්‍රමාණවත් අවබෝධයක් තිබේ. එහෙත් අන්තර්ජාලය ඔස්සේ භාණ්ඩ මිලදීගන්නා අවස්ථා වලදී, ඔබ නොදැනුවත්ම ව්‍යාජ වෙබ් අඩවි වලට පිවිසීමට ඉඩ ඇත.
- ආක්‍රමණිකයන් ඇතැම් විට අව්‍යාජ සේ පෙනෙන වෙබ් අඩවි හෝ ඊමේල් පණිවිඩ නිර්මාණය කරති. නැතිනම් පිළිගත් සමාගම් හෝ පුණ්‍ය ආයතන ආදිය ලෙසද පෙනී සිටිති.
- විශේෂයෙන්ම ස්වාභාවික උපද්‍රව වලින් පසුව සහ නිවාඩු කාල වලදී මෙම වංචනිකයන් ව්‍යාජ වෙබ් අඩවි හෝ ඊමේල් පණිවිඩ නිර්මාණය කර, පුණ්‍යාධාර ලබාදීම සහ විවිධ භාණ්ඩ මිලදී ගැනීම වැනි දේ සඳහා ජනතාව යොමු කරවීමට උත්සාහ කරති. ඇතැම් විට ඔවුහු නොමිලේ සිලිවර් සේවාවන් සහ වෙනත් දීමනා ආදිය ලබාදෙන බව පවසා පාරිභෝගිකයන් පොළඹවති.

02 අනාරක්ෂිත සම්බන්ධතා ආක්‍රමණය කිරීම:

- කිසියම් අලෙවිකරුවෙකු සුරක්ෂිත අන්තර්ජාල සම්බන්ධතා ක්‍රමයක් භාවිතා නොකරන්නේ නම් එම අලෙවිකරුවා සතු තොරතුරු ආක්‍රමණිකයන් අතට පත්වීමට වැඩි ඉඩක් ඇත.

03 අනාරක්ෂිත පරිගණක ආක්‍රමණය කිරීම:

- ඔබේ පරිගණකය වෛරස හෝ වෙනත් ආක්‍රමණික වැඩසටහන් ආදියෙන් ආරක්ෂා කිරීමට පියවර ගෙන නොමැති නම්, ආක්‍රමණිකයන් එම පරිගණකයට පිවිසී එහි ඇති තොරතුරු සොරාගැනීමට ඉඩ ඇත.
- තම පාරිභෝගිකයන්ගේ දත්ත ඇතුළත් ගබඩා ආක්‍රමණිකයන්ගෙන් ආරක්ෂා කරගැනීමට අලෙවිකරුවන් විශේෂයෙන් පියවර ගත යුතුය.



ඔබට ගතහැකි ආරක්ෂක පියවර මොනවාද?

- පෞද්ගලික හෝ මූල්‍යමය තොරතුරු ලබාදීමට පෙර, ඔබ ගනුදෙනු කරමින් සිටින්නේ පිළිගත්, විශ්වාසනීය අලෙවිකරුවෙකු සමඟ බව තහවුරු කරගන්න. ඇතැම් ආක්‍රමණිකයන් පාරිභෝගිකයන් නොමග යැවීම සඳහා ව්‍යාජ වෙබ් අඩවි නිර්මාණය කරන බැවින් මේ සම්බන්ධයෙන් අතිශයින් සැලකිලිමත් විය යුතු වේ.
- ගනුදෙනුව හෝ බිල්පත සම්බන්ධයෙන් ගැටලුවක් ඇතිවූ අවස්ථාවකදී භාවිතා කිරීම සඳහා, අලෙවිකරුවන්ගේ ලිපිනයන් සහ දුරකථන අංක සොයාගෙන සටහන් කර තබාගන්න.
- ඔබේ තොරතුරු සුරක්ෂිත ලෙස කේතකරණය (encrypt) කර ඇති බව තහවුරු කරගන්න. එමෙන්ම වෙබ් අඩවියේ ලිපිනය දැක්වෙන කොටස සහ ඒ ආසන්නයේ සඳහන් වන තොරතුරු (උදා: 'පැඩ්ලොක්' සලකුණ සහ i-Information වැනි) භාවිතා කරන්නේ කෙසේද යන්න සම්බන්ධයෙන් දැනුවත් වන්න.
- තොරතුරු ඉල්ලමින් විවෘත ලබන ඊමේල් සම්බන්ධයෙන් බෙහෙවින් සැලකිලිමත් වන්න. ගනුදෙනු හෝ ගිණුම් තොරතුරු තහවුරු කරන ලෙස දන්වමින් ආක්‍රමණිකයන් විසින් ඔබ වෙත ව්‍යාජ ඊමේල් ලිපි විවීමට ඉඩ ඇත. සත්‍ය ව්‍යාපාරික ආයතන ඊමේල් මගින් මෙවැනි තොරතුරු විමසීම සිදු නොකරයි. එම නිසා, මෙවැනි ඊමේල් ලිපියක් ලැබුණු විට එහි ඇති සබැඳිය (link) ක්ලික් (click) නොකර, ව්‍යාපාරයට අදාළ සත්‍ය වෙබ් අඩවියේ ලිපිනය ඔබට රයිප් කර වියට පිවිසී පරීක්ෂා කරන්න.
- අන්තර්ජාලයෙන් භාණ්ඩ මිලදී ගැනීමේදී පහළ ණය සීමාවක් සහිත, තනි ක්‍රෙඩිට් කාඩ්පතක් භාවිතා කිරීම මගින් ඔබට අවදානම අවම කරගත හැක. ක්‍රෙඩිට් කාඩ්පතක් භාවිතා කිරීම සෑම විටම ඩෙබිට් කාඩ්පතක් භාවිතා කිරීමට වඩා සුරක්ෂිතය. පිළිගත් ආයතන වල වෙබ් අඩවි විවිධ කාඩ්පත් වර්ග වලින් ගෙවීම් භාරගන්නා අතර ව්‍යාජ වෙබ් අඩවි වැඩිදුර තහවුරු කරගැනීම සඳහා බව පවසමින් ඔබේ ක්‍රෙඩිට්/ඩෙබිට් කාඩ්පත් අංක ඉල්ලා සිටීමට ඉඩ ඇත.
- ඔබ භාවිතා කරන shopping apps වල settings පරීක්ෂා කරන්න. ඔබගේ දත්ත සුරක්ෂිතව තබාගන්නා ආකාරය සහ ඒවා භාවිතා කරන්නේ කුමන අරමුණු වලටද යන්න පැහැදිලිව දක්වන apps මොනවාද යන්න සොයා බලන්න.
- ඔබේ ගිණුම් ප්‍රකාශ පරීක්ෂා කරන්න. ඔබේ මිලදීගැනීම් හා ඒවා සම්බන්ධයෙන් ලැබුණු තහවුරු කිරීම් සම්බන්ධ වාර්තා විධිමත්ව පවත්වාගන්න. එම වාර්තා සහ ගිණුම් ප්‍රකාශ වල සඳහන් තොරතුරු සංසන්දනය කරන්න. නොගැළපීමක් පවතින බව පෙනී යන්නේ නම් වහාම විය වාර්තා කරන්න.

වෙබ් අඩවියේ ලිපිනයට වම් පසින් හෝ දකුණු පසින් ඇති 'පැඩ්ලොක්' සලකුණ ක්ලික් (click) කර 'View Certificate' සබැඳිය (link) ක්ලික් (click) කරන්න. එවිට 'Certificate dialog box' විවෘත වේ. SSL සහතිකය සම්බන්ධ තොරතුරු එහි දිස්වනු ඇත.



Phishing ආක්‍රමණිකයන්ගේ ගොදුරක් නොවන්න

වර්තමාන ලෝකයේ කාර්යබහුලත්වය මෙන්ම නව අභියෝග හමුවේ මුහුණපෑමට සිදුවී ඇති සීමා මායිම් ආදිය නිසා බොහෝ දෙනෙක් වැඩි වශයෙන් අන්තර්ජාලය භාවිතා කිරීමට යොමුවී සිටිති. මෙහිදී ඇතැම් අය සැක සහිත ඊමේල් හෝ ඉල්ලීම් සම්බන්ධයෙන් අඩු අවධානයක් දැක්වීමට ඉඩ ඇත. එවැනි අවස්ථා වලදී තමන් නොදැනුවත්ම වැදගත් තොරතුරු අනාවරණය කරමින් ඔවුන් phishing ආක්‍රමණිකයන්ගේ ගොදුරක් බවට පත්වීමට ඉඩ තිබේ.

Phishing ආක්‍රමණ කල්තබා හඳුනාගනිමු:

- **යවත්තාගේ ලිපිනය සැකසහිත වන ඊමේල් ලිපි**
යවත්තාගේ ලිපිනය පිළිගත් ව්‍යාපාරයක් සේ පෙනී යාමට ඉඩ ඇත. සයිබර් අපරාධකරුවන් බොහෝ විට පිළිගත් සමාගම්වල නම් වලට සමාන වන, අකුරක හෝ දෙකක වෙනසක් වැනි සුළු වෙනස්කම් සහිත ඊමේල් ලිපින යොදාගනිති.
- **පොදු ආමන්ත්‍රණ සහ අත්සන්**
විශේෂ ආමන්ත්‍රණ වලින් තොරව 'හිතවත් පාරිභෝගිකයන්' හෝ 'මහත්මයාණනි/ මහත්මියනි' වැනි පොදු ආමන්ත්‍රණ භාවිතා කිරීම මෙන්ම, යවත්තාගේ නම/අත්සන සඳහන් වන ස්ථානයේ සම්බන්ධතා තොරතුරු ඇතුළත් නොවීම ආදිය phishing ආක්‍රමණිකයන් හඳුනා ගැනීමට උපකාරී වේ. සාමාන්‍යයෙන් විශ්වාසදායී, පිළිගත් සමාගම් ඔබේ නමින් ඔබ ආමන්ත්‍රණය කරන අතර, තම සම්බන්ධතා තොරතුරු නොසඟවා ලබාදෙයි.
- **ව්‍යාජ hyperlinks සහ වෙබ් අඩවි**
ඊමේල් ලිපියේ සඳහන් වන සබැඳි (links) මගින් ඔබේ කර්සරය ගෙනයන විට පෙනෙන අකුරු සහ සබැඳියේ (link) සඳහන් අකුරු අතර පරස්පරතා ඇත්නම්, එම සබැඳිය (link) ව්‍යාජ එකක් වීමට ඉඩ තිබේ. ව්‍යාජ වෙබ් අඩවි සත්‍ය වෙබ් අඩවි වලට පෙනුමින් සමාන වුවද වෙබ් ලිපිනයේ (URL) වෙනස්කම් ඇත.

- **අක්ෂර වින්‍යාසය සහ පෙනුම**
අක්ෂර හෝ ව්‍යාකරණ දෝෂ, අවිධිමත් සැලසුම් සහ වෙනත් දුර්වලතා, phishing ආක්‍රමණයක් හඟවන ඉඟියක් වීමට ඉඩ තිබේ. පිළිගත් ආයතන සාමාන්‍යයෙන් ව්‍යාකරණ දෝෂ ආදිය නිවැරදි කිරීමට සහ වෙබ් අඩවියේ පෙනුම විධිමත් ලෙස සකස් කිරීමට කටයුතු කරයි.

- **සැක සහිත ඇමුණුම් (attachments)**
නොදන්නා මූලාශ්‍රයකින් එවනු ලබන ඊමේල් ලිපියක් මගින් ලබන්නාට කිසියම් ඇමුණුමක් (attachment) බාගත (download) කරන ලෙස ඉල්ලා සිටීම, සාමාන්‍යයෙන් 'malware' වර්ගයේ හානිකර පරිගණක වැඩසටහන් බෙදාහරින ප්‍රකට ක්‍රමයකි. මෙවැනි ඊමේල් වලදී අපරාධකරුවන් කිසියම් හදිසි තත්ත්වයක් හඟවමින් ලබන්නා, කලබල කර, විමසිලිමත් වීමෙන් තොරව ඇමුණුම (attachment) බාගත (download) කිරීමට හා විවෘත කිරීමට යොමුකරවීමට ඉඩ ඇත.



සයිබර් අවකාශය හා දරුවන්

අන්තර්ජාලය නිසා දරුවන්ට නව ලෝකයක් විවෘත වී ඇත. අන්තර්ජාලය භාවිතා කරන කාණ්ඩ අතින් වැඩියෙන් වර්ධනය පෙන්වන කාණ්ඩයද දරුවන්ය. මෙහි යහපත් පැතිමානයන් මෙන්ම අයහපත් පැතිමානයන්ද ඇති බව අමුතුවෙන් කිවයුතු නොවේ. එම නිසා දෙමාපියන් ලෙස ඔබ සැම විටම, දරුවන් අන්තර්ජාලය තුළදී මුහුණදීමට සිදුවිය හැකි අවදානම් පිළිබඳව සැලකිල්ලෙන් පසුවිය යුතුය. තාක්ෂණයෙන් උපරිම ප්‍රයෝජන ගන්නා අතරම තම ආරක්ෂාව සලසා ගන්නා ආකාරය සම්බන්ධයෙන් ඔවුන් දැනුවත් කළ යුතුය.

දරුවන්ට විශේෂයෙන් බලපාන අවදානම්:

- දරුවන් ඔබගේ පරිගණකය භාවිතා කරන විට, දරුවන්ට විශේෂයෙන් බලපාන, තාක්ෂණික ක්‍රම මගින් පාලනය කළ නොහැකි අවදානම්ද මතුවීමට ඉඩ ඇත.
- මෙසේ වන්නේ දරුවන් අහිංසක, කුතුහලයෙන් පිරි සහ ස්වාධීන ගතිලක්ෂණ වලින් යුක්ත වන නිසාය. එමෙන්ම ඔවුන් නොදැනුවත්ම යමක් කිරීම නිසා දැඩුවම් විඳීමට බිය වන නිසාය.
- දරුවන් අන්තර්ජාලය ඔස්සේ ඉගෙනුම් කටයුතු වල යෙදෙන අතරවාරයේ වැරදිමතින්, කුට අරමුණු සහිත වෙබ් අඩවි වෙත පිවිසීමට ඉඩ තිබේ. එමගින් ඔබේ පරිගණකයට වෛරස ආදිය ඇතුළු වීමට ඉඩ ඇති අතර, දැඩුවම් විඳීමට සිදුවෙතැයි යන බිය නිසා දරුවා මේ බව ඔබට නොපවසා සිටීමට ඉඩ ඇත.
- එමෙන්ම දරුවන් phishing ආක්‍රමණිකයන්ගේ ගොදුරක් බවට පත්වීමටද ඉඩ තිබේ. දරුවන් සාමාන්‍යයෙන් ව්‍යාජ ඊමේල් සහ පණිවිඩ සම්බන්ධයෙන් සැකයක් නොසිතති.
- මේ වනවිට උඩුදුවමින් පවතින තවත් ගැටලුවක් වන්නේ අන්තර්ජාලයේ ඔස්සේ පීඩාවන් පැමිණවීම හෙවත් 'cyberbullying' ය. දරුවා ඊමේල්, පණිවිඩ යැවීමේ apps සහ සමාජ මාධ්‍ය ආදිය භාවිතා කරන්නේ නම් මෙම අවදානම තවත් දරුණු වේ.



දෙමාපියන්ගේ වගකීම:

- මෘදුකාංග යාවත්කාලීන කර තබන්න. දරුවා භාවිතා කරන පරිගණක වල 'වෛරස් ගාඩ්' ඇතුළුව සයිබර් ආරක්ෂාව සම්බන්ධ අංග යාවත්කාලීනව පවතින බව තහවුරු කරගන්න.
- සඳහා දරුවාට සහය වීම වැදගත් වේ. එමගින් දරුවන්ගේ අන්තර්ජාල හැසිරීම නිරීක්ෂණය කිරීමට අවස්ථාවක් ලැබෙන අතරම ඔවුන් තුළ යහපත් පරිගණක චර්යාවන් ඇතිකරවීමටද අවස්ථාව ලැබෙනු ඇත.
- දෙමාපියන් දරුවන් සමග සම්පව කටයුතු කළ යුතුය. දරුවන් පරිගණකය භාවිතා කරමින් යමක් සොයන විට, පරිගණක ක්‍රීඩා වල යෙදෙන විට හෝ ඉගෙනුම් කටයුතු වල යෙදෙන විට, දෙමාපියන්ද සුනඳුහිඳි ලෙස එම කටයුතු
- පරිගණකය විවෘත ස්ථානයක තබන්න. දරුවා කරන්නේ කුමක්ද යන්න පහසුවෙන් නිරීක්ෂණය කිරීමට දෙමාපියන්ට හැකියාව තිබිය යුතුය. දරුවන් සාමාන්‍යයෙන් නොකළ යුතු දෙයක් කරන්නේ නම්, වචන මැදිහත් වී එය නතර කරවීමට දෙමාපියන්ට එවිට අවස්ථාව ලැබේ.

සීමාවන් පනවන්න; අනතුරු අඟවන්න.

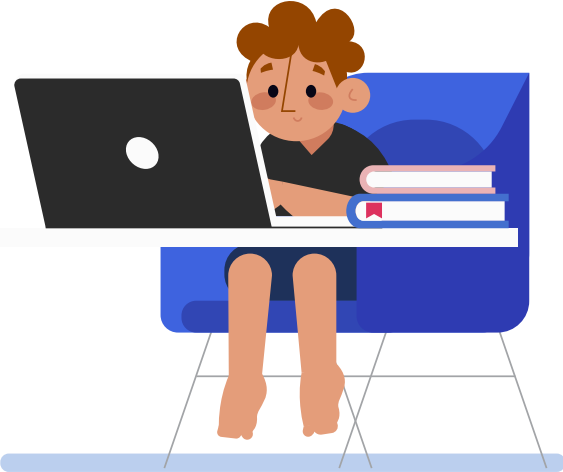
දුරුවන්ට පරිගණක භාවිතය සම්බන්ධයෙන් ලබාදී ඇති නිදහසෙහි සීමාවන් මොනවාද යන්න පිළිබඳව ඔවුන් දැනුවත් කරන්න. දුරුවන්ගේ වයස, දැනුම හා පරිණතභාවය අනුව සීමාවන් පනවිය හැකි අතර, ඔවුන්ට පරිගණකය භාවිතා කිරීමට කෙතරම් කාලයක් ලබාදෙනවාද, ඔවුන්ට පිවිසීමට අවසර ඇති වෙබ් අඩවි මොනවාද, භාවිතා කළ හැකි මෘදුකාංග මොනවාද ආදිය මෙන්ම පරිගණකය භාවිතයෙන් සිදුකිරීමට අවසර ඇති දේවල් මොනවාද යන්නද තීරණය කළ යුතුය. අන්තර්ජාලය හරහා පැමිණෙන අනතුරු සම්බන්ධයෙන් දුරුවන් නිසි පරිදි දැනුවත් කර තැබීම මගින් ඔවුන්ට විවේචනීය අනතුරු කල්තබා හඳුනාගැනීමට හැකිවනු ඇත.

- පරිගණක ක්‍රියාකාරකම් නිරීක්ෂණය කරන්න. දුරුවා පිවිසෙන වෙබ් අඩවි ඇතුළුව, ඔහු/ඇය පරිගණකය භාවිතයෙන් සිදුකරන ක්‍රියාකාරකම් පිළිබඳව සැලකිල්ලෙන් පසුවන්න. ඔහු/ඇය ඊමේල්, පණිවිඩ සේවාවන් හෝ වැට් රෂම් වැනි දේවල් භාවිතා කරන්නේ නම්, දුරුවා සම්බන්ධතා පවත්වන්නේ කා සමගද, දුරුවා එම පුද්ගලයන් සැබැවින්ම හඳුනන්නේද යනාදිය ගැන විමසිලිමත් වන්න.
- ඔබත් සමග පහසුවෙන් කතාබස් කළ හැකි බව දැරුවාට දැනෙන්නට ඉඩහරන්න. සයිබර් අවකාශය වැනි ස්ථානයකදී ඇතිවන ගැටලු සහ දැඩි හැසිරීම් ආදිය සම්බන්ධයෙන් කුතුහලයක් ඇතිවූ විට ඒ සම්බන්ධ ඕනෑම කරුණක් ඔබ සමග කතාබහ කළ හැකි බවට විශ්වාසයක් දුරුවා තුළ ගොඩනංවන්න.

- දුරුවාට වෙනම පරිශීලක ගිණුමක් පවත්වා ගැනීමට ඉඩ දෙන්න. බොහෝ මෙහෙයුම් පද්ධති පරිශීලකයන්ට වෙන වෙනම පරිශීලක ගිණුම් (user account) පවත්වාගෙන යාමට අවස්ථාව සලසා දෙයි. ඔබේ දුරුවා අත්වැරදීමකින් ඔබේ තොරතුරු භාවිතා කිරීම, වෙනස් කිරීම හෝ මකා දැමීම සිදුකිරීමට ඉඩ ඇති බව ඔබ සිතන්නේ නම්, ඔවුන්ට වෙනම පරිශීලක ගිණුමක් සකස් කර දීමත්, පරිගණක භාවිතය සම්බන්ධ වරප්‍රසාද සීමිතව ලබාදීමත් සිදුකළ හැක.
- දෙමාපිය පාලන සීමාවන් යෙදීම ගැන සලකා බලන්න. ඔබ භාවිතා කරන බ්‍රවුසරය තුළ දෙමාපිය පාලන සීමාවන් (parental controls) යොදන්න. උදාහරණයක් ලෙස Internet

Explorer තුළ ඇතැම් වෙබ් අඩවි වලට පිවිසීමට අවසර දීමට හෝ නොදීමට ඔබට හැකියාව ඇති අතර, එම settings වලට password යොදා ආරක්ෂා කළ හැක. මෙම options සොයාගැනීම සඳහා menu bar කොටසේ Tools ක්ලික් (click) කර, Internet Options තෝරාගෙන, 'Content' tab ක්ලික් (click) කර, Content Advisor යටතේ Enable කොටස ක්ලික් (click) කරන්න.

- ඔබගේ අන්තර්ජාල සේවා සමාගම ලබාදෙන සහය සේවාවන් භාවිතා කරන්න. ඇතැම් අන්තර්ජාල සේවා සමාගම්, අන්තර්ජාලය තුළ දුරුවන්ගේ ආරක්ෂාව තහවුරු කිරීම සඳහා විශේෂයෙන් සැලසුම් කළ සේවාවන් ලබාදෙයි. මෙම සේවාවන් ලබාගත හැකිද යන්න දැනගැනීම සඳහා, ඔබට සේවාව ලබාදෙන සමාගම අමතන්න.



වගකීම් අන්තර්ගත ප්‍රකාශය: ඔබටත් ඔබගේ පවුලේ අයටත් සයිබර් තර්ජන වලින් ආරක්ෂා වීමට අත්වැලක් වීම සඳහා මෙම මාර්ගෝපදේශ මාලාව පිළියෙල කර තිබේ. මෙහි සඳහන් කරුණු වැඩිදුරටත් පැහැදිලි කරගැනීමට හෝ එම කරුණු ප්‍රායෝගිකව ක්‍රියාවට නැංවීමට අවශ්‍ය නම් කරුණාකර විශේෂඥ සහය ලබාගන්න.

ඇමරිකා එක්සත් ජනපදයේ ස්වදේශ ආරක්ෂක දෙපාර්තමේන්තුව මගින් ප්‍රකාශයට පත්කරන ලද තොරතුරු සහ ෆෙඩරල් ඉන්ෂුරන්ස් සමාගමේ තොරතුරු තාක්ෂණ අංශයේ මගපෙන්වීම අනුව මෙම ලේඛනය පිළියෙල කරන ලදී.