සුහුරුකතා 2020

eWomen

තෘතීය කලාපය

කාන්තා හා ළමා සංවර්ධන, පෙර පාසල් හා ප්‍රාථමික අධ්‍යාපන,
පාසල් යටිතල පහසුකම් හා අධ්‍යාපන සේවා රාජ්‍ය අමාත්‍යාංශය

තෙවන කලාපය

උපදේශනය

කේ.එම්.එස්.ඩී.ජයසේකර
රාජ්‍ය ලේකම්
කාන්තා හා ළමා සංවර්ධන,පෙර පාසල් හා ප්‍රාථමික අධ්‍යාපන, පාසල් යටිතල පහසුකම් හා අධ්‍යාපන සේවා රාජ්‍ය අමාත්‍යාංශය

මග පෙන්වීම

ජේ.පී.එස්.ජයසිංහ
අධ්‍යක්ෂ (සැලසුම් හා අධීක්ෂණ)
කාන්තා හා ළමා සංවර්ධන,පෙර පාසල් හා ප්‍රාථමික අධ්‍යාපන, පාසල් යටිතල පහසුකම් හා අධ්‍යාපන සේවා රාජ්‍ය අමාත්‍යාංශය

සංස්කරණය

ප්‍රමුෂ්කා හිරුනි විතානගේ
සහකාර අධ්‍යක්ෂ (තොරතුරු තාක්ෂණ)
කාන්තා හා ළමා සංවර්ධන,පෙර පාසල් හා ප්‍රාථමික අධ්‍යාපන, පාසල් යටිතල පහසුකම් හා අධ්‍යාපන සේවා රාජ්‍ය අමාත්‍යාංශය

සංස්කරණ සහාය

අමා රත්නසිරි මහත්මිය
තුෂාරා සුරවීර මහත්මිය
අවලා වීරසිංහ මෙනවිය
ප්‍රියානි ඉන්දිකා මෙනවිය

පිටකවර නිර්මාණය කිරීම

අවලා වීරසිංහ මෙනවිය

දායක ලේඛකයින්

හිරුනි විතානගේ මහත්මිය
අමා රත්නසිරි මහත්මිය
ප්‍රියානි ඉන්දිකා මෙනවිය

ප්‍රකාශනය

තොරතුරු හා සන්නිවේදන තාක්ෂණ ඒකකය
කාන්තා හා ළමා සංවර්ධන,පෙර පාසල් හා ප්‍රාථමික අධ්‍යාපන, පාසල් යටිතල පහසුකම් හා අධ්‍යාපන සේවා රාජ්‍ය අමාත්‍යාංශය

පටුන

පෙරවදන

ලොව සියළු තාක්ෂණික අංශ වේගවත්ව දියුණු වෙමින් පවතී. ඒ අතරතුර තොරතුරු තාක්ෂණික අංශය අධිවේගයෙන් දියුණුවෙමින් පවතී. සුවිශේෂ කරුණක් වනුයේ ලොව අන් සියළු අංශවල ඉදිරිගමනද තොරතුරු තාක්ෂණය හා සබැඳී තිබීමයි. අධ්‍යාපන, සන්නිවේදන, විනෝද, ක්‍රීඩා, ව්‍යාපාර, සංචාර, සෞඛ්‍ය ආදී මෙකී නොකී අංශයන් සඳහා ඉහත ප්‍රකාශය සාධාරණ වේ. එබැවින් තොරතුරු තාක්ෂණය තමාට අවශ්‍ය නොවේ යැයි කිසිවෙකුට පැවසිය නොහැකි තැනට අද ලොව පැමිණ තිබේ.

ශ්‍රී ලාංකික පවුල යනු මාතෘ කේන්ද්‍රිය ඒකකයකි. ශ්‍රී ලාංකික සමාජ, දේශපාලන වපසරිය තුල කාන්තාව පුරුෂයා සමඟ උරෙනුර ගැටී කටයුතු කරන්නීය. වර්තමානයේදී ශ්‍රී ලාංකීක ශ්‍රම බලකායෙන් 32.5% ක් කාන්තාවෝ වෙති. මෙවන් පසුබිමක් තුල තොරතුරු තාක්ෂණ දැනුම ඇයට අත්‍යාවශ්‍ය අංගයක් වී තිබේ.

නමුත් මෑත කාලයේ තොරතුරු තාක්ෂණයේ අනිසි ඵලවිපාක වලින් පීඩාවිදින පිරිස වැඩිවෙමින් පවතී. අවාසනාවකට මෙන් එවැනි අවස්ථාවලදී කාන්තාවන්ට එහි ඇතිවන අනිටු බලපෑම පිරිමි පාර්ශ්වයට වඩා සාපේක්ෂව වැඩිය.

කාන්තා හා ළමා සංවර්ධන, පෙර පාසල් හා ප්‍රාථමික අධ්‍යාපන, පාසල් යටිතල පහසුකම් හා අධ්‍යාපන සේවා රාජ්‍ය අමාත්‍යාංශයේ තොරතුරු තාක්ෂණ අංශය මේ සඟරාව සකසන්නේ තොරතුරු තාක්ෂණ දැනුමෙන් සන්නද්ධ කාන්තා පරපුරක් ගොඩනැංවීමේ අරමුණෙනි. ඒ හරහා තොරතුරු තාක්ෂණයේ යහඵලවලින් ඇය පොහොසත් වන අතර, එහි අනිටු විපාක තුල ඇය අතරමං නොවීම දැක ගැනීම අපේ අවංක උවමනාවයි.

මේ ඒවෙනුවෙන් අප පල කරන ලද "සුහුරුකත" සඟරාවේ තුන්වන කලාපයයි. ඔබේ සියළු අදහස් / යෝජනා අපි ඉතා අගය කොට සලකන්නෙමු.

ශ්‍රී ලංකාව තොරතුරු තාක්ෂණ භාවිතයන් හා හැකියාවන් වඩා ඵලදායීව භාවිතා කරන සහ එහි ප්‍රතිලාභයන්ද අත් විඳින වඩාත් ශක්තිමත් සහ පිරිපුන් කාන්තා පරපුරක් සිටින සෞභාග්‍යමත් රටක් වේවායි ප්‍රර්ථනා කරමු.

කාන්තා හා ළමා සංවර්ධන,පෙර පාසල් හා ප්‍රාථමික අධ්‍යාපන, පාසල් යටිතල පහසුකම් හා අධ්‍යාපන සේවා රාජ්‍ය අමාත්‍යතුමාගේ පණිවුඩය

ජාතියක අනාගත සෞභාග්‍ය හා අභිමානය රදා පවතින්නේ එහි ජනතාවට කෙතරම් දුරට අනාගතයේ වගකීම් හා කාර්යභාරය දැරීමට හැකියාවක් හා ශක්තියක් ඇත්දැයි යන්න මතයි. විශේෂයෙන්ම ඒ සඳහා ඔවුන්ගේ දැනුම හා නිර්මාණශීලී කුසලතාවයන්ද ඔප් නැංවා තිබීම යථෝක්ත ඉදිරි ගමනට මහත් පිටුවලක් ගෙන දෙයි. අප රටේ කාන්තාවන් හා ළමා පරපුරද හෙට දවස සඳහා අභියෝග භාරගැනීමට සූදානම් නැණ ගුණ සහ බලය සපිරි පිරිසක් බවට පත් කිරීම මාගේ රාජ්‍ය ආමාත්‍යාංශයේ සුමුඛතම කාර්ය භාරයයි. රටේ අනාගතය භාරගන්නා ළමුන්ටත් එමෙන්ම සමාජ හා ආර්ථික ප්‍රගමනයට ඉතා සුවිශාල කාර්යභාරයක් ඉටුකරන කාන්තාවටත් සංවර්ධනයේ අවස්ථා විවර කරවීම මහත් වැදගත් වේ. ඒ නිසා අද සමාජයේ ඉදිරි ගමනට හා පැවැත්මට සෘජුවම දායක වන්නා වූ තොරතුරු හා සන්නිවේදන තාක්ෂණය ළමුන් හා කාන්තාවන් අතරේ යහපත් ආකාරයට භාවිතා කරවන්නේ කෙසේදැයි යන්න පිළිබඳව ප්‍රචලිත කිරීමේ මෙහෙවරට මෙම සඟරාව මගින් දායකත්වයක් සපයයි. තමන්ට මුහුණදීමට සිදුවන ගැටලු, ඒවාට විසඳුම් මෙන්ම තමන් ඉදිරියේ උදා වී ඇති නව අභියෝග හා අවස්ථාවන් හඳුනා ගැනීමට තොරුතුරු තාක්ෂණය භාවිතාව මහෝපකාරී වේ.

විධිමත් දැනුවත් භාවයකින් හෝ පාලනයකින් තොරව ළමුන්, කාන්තාවන් මෙන්ම සමස්ථ ප්‍රජාවම සමාජ මාධ්‍ය ඇතුළු තොරතුරු තාක්ෂණ මෙවලම් භාවිතයට යොමුවීම රටේ සාරධර්ම හා සංවර්ධනය පිරිහීමට රුකුලක් වන නිසා එය වළක්වාලමින් නිවැරදි භාවිතයන් පිළිබඳ දැනුම හා අත්දැකීම් ඔවුන් වෙත ගලා යාමට සැලැස්වීම අපගේ වගකීමයි.

තොරතුරු තාක්ෂණ ක්ෂේත්‍රයේ වත්මන් හා අනාගත ප්‍රවණතාවයන්ද සැලකිල්ලට ගනිමින් ජනතාවගේ සිත් වලට ආමන්ත්‍රණය කල යුතු තාක්ෂණික කරුණු බොහොමයක් මෙම සඟරාවේ ගැබ් ව ඇත.එසේ හෙයින් දුදරු, මාපිය, ස්වාමිපුරුෂයා, බිරිඳ සහ අනෙකුත් සියළු අනොන්‍යය සම්බන්ධතාවයන් ගුණාත්මක අයුරින් වර්ධනය කොට එතුලින් සෞභාග්‍ය කරා පිය නැගීමට අප රටේ ජනතාව වාසනාවන්ත වනු අතැයි ප්‍රාර්ථනා කරමි.

පියල් නිශාන්ත ද සිල්වා
කාන්තා හා ළමා සංවර්ධන,පෙර පාසල් හා ප්‍රාථමික අධ්‍යාපන,
පාසල් යටිතල පහසුකම් හා අධ්‍යාපන සේවා රාජ්‍ය ඇමති

කාන්තා හා ළමා සංවර්ධන,පෙර පාසල් හා ප්‍රාථමික අධ්‍යාපන, පාසල් යටිතල පහසුකම් හා අධ්‍යාපන සේවා රාජ්‍ය ලේකම්තුමියගේ පණිවුඩය

සමාජමය ව්‍යුහයන්, සබඳතා හා හරපද්ධතීන් වෙනස් වෙමින් හා සංකීර්ණ වෙමින් ප්‍රගමණය වේ . එම තත්වය තවදුරටත් අඛණ්ඩව, විවිධ මානයන් ඔස්සේ වෙනස්වීම් වලට භාජනය වන අතර දෛනික ජන ජීවිතය ඊට සරිලන අයුරින් ගලපා ගැනීම අපේ පැවැත්මට හා රටේ සංවර්ධනයට අත්‍යවශ්‍යය. පෞද්ගලික, ආර්ථික හා සමාජ ව්‍යුහයන් නව දැනුම හා තොරතුරු තාක්ෂණය ඔස්සේ සවිබල ගැන්වීම මේ තත්වය තුල කාලීන අවශ්‍යතාවයකි. ශ්‍රී ලාංකික කාන්තාව මානුෂීය වටිනාකම් හා ගුණධර්මයන්ගෙන් බැහැර නොවීමට වග බලා ගන්නා අතරම නවීන සමාජයට ගැලපෙන තාක්ෂණික කුසලතාවයන්ගෙන් හා දැනුමෙන් සන්නද්ධ කිරීම සඳහාද පෙලගැස්විය යුතු වන්නේය.

කාන්තාවන්ගේ එදිනෙදා කටයුතු මෙන්ම සමාජීය හා ආර්ථික මෙහෙයුම් වඩාත් ඵලදායිව හා කාර්යක්ෂමව ඉටු කර ගැනීම සඳහා තොරතුරු තාක්ෂණ දැනුම ඉහල නැංවීමේ අපෙක්ෂාවෙන් සෑම වර්ෂයකම "සුහුරුකත" සහරා කලාප දෙකක් එළි දක්වයි. සෞභාග්‍යයේ දැක්ම සඳහා වන ජාතික සංවර්ධන ප්‍රතිපත්ති යථාර්තයක් බවට පත්කර ගැනීමට ද මෙයින් දායකත්වයන් සැලසේ. දේශීය කාන්තාවට අවශ්‍යය තොරතුරු තාක්ෂණ දැනුම හා නිපුණතාවයන් ලබා දීමට මෙමගින් ප්‍රයත්න දරණ අතර ඒ සඳහා නව ක්‍රමෝපායන් හා භාවිතයන් තුලින් අවශ්‍ය සහය සැපයීම අපගේ කාර්ය භාරයයි.

සෞභාග්‍යයේ දැක්ම යථාර්තයක් බවට පත් කිරීම සඳහා ගරු අධ්‍යාපන අමාත්‍යතුමා හා රාජ්‍ය ඇමතිතුමාගේ මඟ පෙන්වීම මත දැනුමෙන් හා කුසලතාවයෙන් සපිරි ශ්‍රී ලංකීය කාන්තා පරපුරක් පත්කිරීමට කාන්තා හා ළමා සංවර්ධන,පෙර පාසල් හා ප්‍රාථමික අධ්‍යාපන, පාසල් යටිතල පහසුකම් හා අධ්‍යාපන සේවා රාජ්‍ය අමාත්‍යාංශය දරන මෙම ප්‍රයත්නය සාර්ථක වේවායි ප්‍රාර්ථනා කරමි.

කේ.එම්.එස්.ඩී.ජයසේකර
ලේකම්
කාන්තා හා ළමා සංවර්ධන,පෙර පාසල් හා ප්‍රාථමික අධ්‍යාපන,
පාසල් යටිතල පහසුකම් හා අධ්‍යාපන සේවා රාජ්‍ය අමාත්‍යාංශය

තොරතුරු තාක්ෂණය සතුරකු නොවන්නට නම්.....

"සතර වටින් එන සුළඟට ඔබේ නිවසේ දොරගුළු විවෘතව තබන්න
ඒ සමඟ තිබෙන වටිනා දේ රඳවා තබා ගන්න
නිවසේ තිබෙන වටිනා දේ ගසා ගෙන යාමට ඉඩ නොදෙන්න"

මහත්මා ගාන්ධි

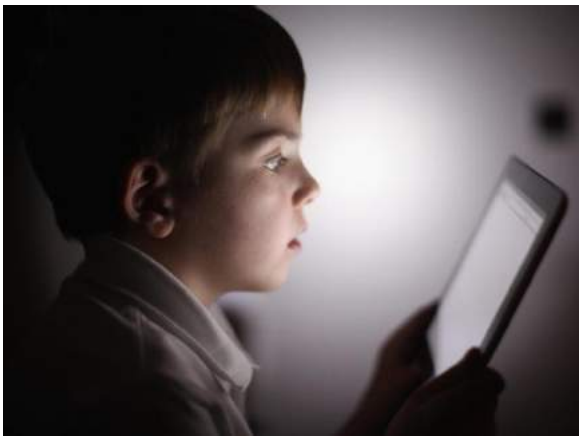
අසු ගිය මාස කීපය තුල මුළු ලෝකය ම මුහුණ දුන් දරුණුතම බෙදවාචකය වූ කොරෝනා වසංගතය හේතුවෙන් සියලු දෙනාගේම දෛනික ජීවිතය සම්පූර්ණයෙන් වෙනස් වන්නට විය. කිසිවකුට තම දෛනික ජීවිතය සුපුරුදු පරිදි සිදු කර ගෙන යාමට නොහැකි වූයෙන් ඒ සියලු කාර්යයන් සුපුරුදු පරිදි ඉටු කිරීමට දායක වූයේ අන්තර්ජාලයයි. විශේෂයෙන්ම මාස ගණනාවක් පාසල් වසා තැබීමෙන් අඩාල වන අධ්‍යාපන කටයුතු නැවත යථා තත්ත්වයට ගෙන ඒමට අන්තර්ජාලය හරහා ඉගැන්වීම් කටයුතු සිදු කිරීමට ගුරුවරුන්ට සිදු විය.

අන්තර්ජාලය යනු ගෝලීයකරණයත් සමඟ අපට දායාද වූ ලෝකය තනි යායක් කළ සුවිශේෂී පද්ධතියකි. එය සාම්ප්‍රදායික ක්‍රම අභිබවමින් යන සුවිශේෂී මාධ්‍යයකි. අප කළ යුත්තේ ඉන් ලබා ගත හැකි යහපත් දේ ළඟ තබා ගෙන අපට නොගැලපෙන දේ බැහැර කිරීමයි. නමුත් සිදුවන ඇතැම් දේ දෙස බැලීමේ දී පෙනී යන්නේ අප තුල තිබූ යහපත් දේ පවා අහිමි වී ඇති බවකි. පාසල් දරුවන්ට නවීන තාක්ෂණය තුලින් ලද හැකි ප්‍රයෝජන බොහෝය. නමුත් පසුගිය කාලය තුල පාසල් දරුවන් බොහෝ දෙනෙක් මෙම අන්තර්ජාල අපරාධවලට ගොදුරු වූ බව වාර්තා වීම කණගාටුවට කරුණකි.

වට්ස්අප්, වයිබර් හරහා පාසල් අධ්‍යාපනික වැඩසටහන් සිදු කිරීම නිසා දරුවන්ට ස්මාර්ට් ජංගම දුරකථන ලබා දීමට සිදු විය. ඇතැම්විට මේවායේ සිදු කරන ක්‍රියාවන් පිළිබඳ බොහෝ දෙමාපියන්ට දැනුමක් නැත. නමුත් දරුවන් එහි පරතෙරටම දැනුමැත්තෝය. තවත් කොටසක් රැකියාවල නිරත වීම හේතුවෙන් නිරන්තර මේ පිළිබඳ අවධානය යොමු කිරීමට අපොහොසත් වේ. තමා කරන දේ නිවැරදිව තෝරා බේරා ගන්නා දරුවා ඉන් නිසි ප්‍රයෝජන ලබා ගන්නා අතර, ඇතැම් දරුවකුට මෙය වදුරාට දැලි පිහිය දුන්නා මෙන් වූ අවස්ථා පිළිබඳ ව අසන්නට ලැබිණි.

වයස අවුරුදු 13 ක් වූ අට වසර පන්තියේ ඉගෙනුම ලබන දියණියකට පාසල් වැඩ කිරීම සඳහා දෙමාපියන් ජංගම දුරකථනයත් ලබා දී තිබූ අතර, ඇය බොහෝ දිනවල රාත්‍රියේදීත් අධ්‍යාපන වැඩ කටයුතුවල නියැලුණාය. ඇය පාසල් වැඩ බව සැක හැර දැනගන්නා දෙමව්පියෝ නින්දට ගිය පසු ඇය සිදු කර ඇත්තේ වෙනත් දෙයකි. මේ වන විට ඇයගේ සිත නතර වී තිබුණේ පාසල් අධ්‍යාපනය මත නොව වයස අවුරුදු 18 පමණ තවත් සිසු දරුවකු විසින් සිදු කරන ලද ප්‍රේම ආරාධනාවක් වෙත ය. ඇය බොහෝ දිනවල රාත්‍රියේ කළේ ඔහු සමග චැට් කිරීමයි. එහිදී ඇයගේ නිරුවත් ඡායාරූප පවා ලබා දීමට ඇය නොපැකලි වූ අතර, රාත්‍රියේ නිවස අසළට පැමිණ ඇය නිවසින් එළියට කැඳවා ගැනීමට ද ඔහු සමත් වී ඇත. මේ කිසිවක් දෙමාපියන් දැන ගෙන සිටියේ නැත.

මේ අප ඇසූ එක් සිදුවීමක් පමණකි. මෙම කාලය තුල මෙවන් සිදු වීම් බොහෝ සෙයින් සිදු වන්නට ඇත. ඇතැම් ඒවා වාර්තා වන අතර ඇතැම් ඒවා වාර්තා නොවීම කාලයේ වැලිතලාවෙන් සැගව යනවා ඇත. කල හැකි යහපත් බොහෝ දේ තිබිය දී අපගේ අනාගත පරපුර මෙසේ මං මුලා වීම කණගාටුවට කරුණකි. මේ සඳහා ඔවුන්ට නිසි මඟ පෙන්වීමක් ලබා දිය යුතුය. මේවායින් සිදුවන යහපත් අයහපත් දේ පිළිබඳ දරුවන් දැනුවත් කළ යුතුය. දෙමාපියන් නිරන්තර අවධානයෙන් සෙවිල්ලෙන් සිටිය යුතුය.



විශේෂයෙන්ම වර්තමානය වන විට අන්තර්ජාලය තුල දරුවන් මෙන් ම වැඩිහිටියන් අතර ජනප්‍රිය ප්‍රධානම අංශයක් වන්නේ මුහුණ් පොතයි. දන්නා නොදන්නා සියළු දෙනාම තම යහළුවන් ලෙස එකතු කර ගන්නා බොහෝ දෙනා අවසානයේ ඉතා ඛේදජනක අවස්ථාවන්ට මුහුණ දෙති. මෙහි සිදුවන ඇතැම් අපරාධයන්හි වින්දිතයන් බවට පත් වන්නේ බොහෝ විට පාසල් දරුවන් ය. මෙහිදී අසභ්‍ය වීඩියෝ පට, අසභ්‍ය හැසිරීම් හා හමුවීම් වලට බලකිරීම් මෙන් ම ෆේස්බුක් සාද වැනි දේවල් පිළිබඳව වර්ථමානයේ බහුලව අසන්නට ලැබේ. ඇතැම් විට මේවා කෙළවර වන්නේ ජීවිත වලින් ද වන්දි ගෙවීමෙනි.

දරුවකු ඉතා ඉක්මණින් වැරදි මාර්ගය, නිවැරදි යයි පූර්ව නිගමනය කර ක්ෂණිකව විවිධ අපචාර හා අපයෝජන වලට ලක් විය හැකි බැවින් ඔවුන්ගේ හොඳම මිතුරා/මිතුරිය ලෙස ඔවුන් සමඟ සමීප සම්බන්ධතා පැවැත්වීම දෙමාපියන්ගේ වගකීමකි. එවිට බාහිර සමාජයෙන් ඔවුන් කරා එන මෙවන් අභියෝග මුල් අවස්ථාවේදීම මඟහැර ගැනීමට දරුවන්ට සහය ලබා දීම දෙමාපියන් හා වැඩිහිටියන් විසින් සිදු කල යුතුමය. දරුවන්ගේ අනාගතය සුරක්ෂිත කිරීමේ මෙම සමාජ වගකීම දෙමාපියන් සහ වැඩිහිටියන් භාර නොගන්නා තෙක් රජයට හෝ අමාත්‍යාංශයට එය තනිව කල හැකි දෙයක් නොවනු ඇත.

නව තාක්ෂණික යුගය තුල අපට අන්තර්ජාලයෙන් බැහැර වී සිටීම කළ නොහැකිය. ගහට පොත්ත සේ එය අපගේ ජීවිත සමඟ බද්ධ වී හමාරය. ඒ නිසා අප කළ යුත්තේ නිසි පරිදි දැනුවත් වී යන ගමන නිවැරදි මාවතේ ගමන් කිරීමය. ඒ සඳහා විශේෂයෙන්ම නිවැරදි අන්තර්ජාල භාවිතය පිළිබඳ දරුවන් දැන්වත් කිරීම සියලු දෙනාගේ වගකීමකි. දරුවාට දුරකතනයක් ලබා දී ඉන් බැහැරවීම නොකළ යුතු අතර එය නිරන්තර පරීක්ෂාවට ලක් කල යුතුය. ඒ සඳහා යම් යම් සීමාවන් පැනවිය යුතුය. දරුවන්ට ඇති වන ගැටලු පිළිබඳව ඔවුන් සමඟ සාකච්ඡා කල යුතුය. ඒවායින් ලබා ගත හැකි යහපත් දේ ලබා ගැනීමටත් , බැහැර කල යුතු දේ බැහැර කිරීමටත්, දරුවන්ට කියා දිය යුතුය.

කේ.ජී.ගිතා රෝෂණී ද සිල්වා
සංවර්ධන නිලධාරී

පරිගණක වෛරස් ගැන ඔබ දැනුවත් ද?

පරිගණක ලෝකයේ සිදු වූ සිඝ්‍ර සංවර්ධනයත් සමඟ සමාජයට හිතකර මෙන්ම අහිතකර තත්ත්වයන් ද නිර්මාණය විය. මෙමගින් ඇති වූ එක් අහිතකර තත්ත්වයක් විදියට මිනිසුන් විසින් පරිගණක වෛරස් එනම් පරිගණකයට හානි කර

ක්‍රමලේඛන නිර්මාණය කිරීමට පටන් ගත්හ. මෙම වෛරස් පරිගණකයට CD, DVD, පරිගණක ජාල හරහා, USB Flash Drive, Data card, අන්තර්ජාලය, විද්‍යුත් තැපෑල වැනි කිසියම් ක්‍රමයක් හරහා පරිගණකයට ඇතුළු වූ පසු එයට පිටපත් වන අතර පරිශීලකයාගේ අනු දැනුම හෝ අවසර නොමැතිව ස්වයංක්‍රීය පරිගණකය ආසාදනය කිරීමට පටන් ගනී. පරිගණකයක සම්පූර්ණ ක්‍රියාකාරිත්වයම අඩාල කොට අවුල්

කර දැමීමට පරිගණක වෛරසයට හැකියාව ඇත.

පරිගණක වෛරසයක ප්‍රධාන ගති ලක්ෂණ

- පරිශීලකයාගේ උපදෙස්වලින් තොරව ක්‍රියාත්මක වේ.
- ස්වයංක්‍රීයව ප්‍රගුණ වීමේ හැකියාවෙන් යුක්ත වේ.
- අනෙක් පරිගණක වැඩසටහන් මත බලපෑම් ඇති කර ඒවා වෙනස් කිරීම හා විනාශ කිරීමට හැකියාවක් ඇත.
- සොයා ගැනීම අපහසු වන අතර සෑම විටම සැඟවී සිටීමට උත්සාහ දරයි.

- පරිගණකයේ සාමාන්‍ය ක්‍රියාකාරිත්වයට බාධා පමුණුවයි.
- වෛරසයක් ඉවත් කලත් ඒවා නැවතත් තමා විසින්ම නැවත නැවත උත්පාදනය කිරීමට උත්සාහ දරයි. (Replicate)

පරිගණක වෛරස් පැතිරෙන ආකාරය

- ආසාධනය වූ Floppy Disk , CD, DVD මගින්
- නිත්‍යානුකූල නොවන Software CD,DVD භාවිතය මගින්
- විද්‍යුත් තැපෑල මගින්
- අන්තර්ජාලය මගින්

පරිගණයේ වෛරස් ඇත් දැයි හඳුනා ගන්නේ කෙසේද?

බොහෝ පරිගණක වෛරස් මගින් පර්ගණකයේ බාහිර සැකසුම් ඇති කරන නිසා පරිගණකයේ වෛරසයක් ඇති බව පහසුවෙන් හඳුනාගත හැකි වේ.

ඔබේ පරිගණකයේ වෛරස් තර්ජනයක් ඇත්නම්,

- අන්තර්ජාලය සමඟ සම්බන්ධ වී සිටින විට ඔබගේ විධානයකින් තොරවම ඔබට අනවශ්‍ය වෙබ් පිටුවකට ඔබව යොමු කරයි.
- ඔබ විසින් නිර්මාණය නොකරන ලද නව අයිකන පරිගණක තිරය මත දිස්වේ.
- ඔබට නුහුරු පණිවුඩ පරිගණක තිරයේ දිස්වේ.
- ඔබ විසින් පරිගණකයෙන් ඉවත් නොකරන ලද වැඩ සටහන් පරිගණකයෙන් ඉවත්ව ඇති ලෙස දිස්වේ.
- පරිගණකයේ ක්‍රියාකාරී වේගය අඩු වේ.
- ඔබ විසින් නිර්මාණය නොකරන ලද කෙටි මං අයිකන පරිගණක තිරය මත දිස්වේ.
- ඔබ විසින් ස්ථාපිත කරන ලද මෘදුකාංග සොයා ගත නොහැකි වීම
- පරිගණකය නිතර නිතර ක්‍රියා විරහිත වීම.
- පරිගණක ගොනු ඉබේම මැකී තිබීම

පරිගණක වෛරස් වර්ග

- Boot Sector Virus - මෙම වෛරසය දෘඩ තැටියේ හෝ වෙනත් දත්ත ගබඩා කිරීමේ මාධ්‍යයක ආරම්භක කොටස්වල පැතිරේ.
- Companion Virus - මෙම වෛරසය මගින් දැනට පරිගණකයේ ඇති .exe ආකාරයේ ගොනු .com ආකාරයේ ගොනු ලෙස පරිවර්තනය කර වෛරසය ඒවා තුළ තැන්පත් කරයි.
- Email Virus - මෙම වෛරසය විද්‍යුත් තැපෑල මාර්ගයෙන් පැතිරේ. සාමාන්‍යයෙන්

මෙම වෛරසය විද්‍යුත් තැපෑල් ලිපින එකතුවේ (address book) ඇති විද්‍යුත් තැපැල් ලිපින වලට තැපැල් කර යැවීමෙන් පැතිරීම සිදු කරයි.

- Logic Bombs and Time Bombs මෙම වෛරස් කිසියම් ක්‍රියාවක් හා අනුබද්ධව ප්‍රතිචාර දක්වයි. මෙම වෛරසය නියමිත කාලයකට අනුව ප්‍රතිචාර දක්වයි නම් එම වෛරසය Time Bomb යනුවෙන් හඳුන්වයි.
- Macro Virus - Microsoft Office පැකේජයන් හා භාවිතා වන පරිගණක නියෝග (commands) මාර්ගයෙන් පැතිරේ.
- Cross – site Scripting Virus - මෙම වැඩ සටහන් සත්‍යය වශයෙන්ම වෛරස නොවූවත් සිදුවන හානිය ගැන සලකා වෛරස සේ වර්ග කරයි.
- Trojan Horses - පිටතින් වෙන වැඩ සටහනක් මෙන් පෙනීසිට, පරිගණකයට අනවසර පුද්ගලයන්ට ඇතුලුවීමට සැලැස්වීම හා පරිගණකයේ ඇති දත්ත පිටස්තරයන්ට ලබාදීම මෙමගින් සිදු කරයි.
- Worms - මෙම වෛරසය පරිගණක ජාල හරහා පරිශීලකයාට කිසිදු දැනුම් දීමකින් තොරව පැතිරේ. බොහෝ විට ඉලක්ක කරන ලද පරිගණක වල දත්ත විනාශ කිරීම හෝ දූෂණය කිරීම සිදු කරයි.

පරිගණක වෛරසය මගින් සිදුවන හානි

- ක්‍රම ලේඛන / මෘදුකාංග වෙනස් වීම, විනාශ වීම හෝ අක්‍රිය වීම
- මෘදුකාංගයක් ගබඩා වීමට දිගු කාලයක් ගත වීම
- වෙනත් මෘදුකාංග ස්ථාපනය කිරීමේ නොහැකියාව
- ක්‍රම ලේඛන අතුරුදහන් වීම
- පරිගණකයේ ඇති මතකයේ ප්‍රමාණය අඩු වීම
- අන්තර්ජාල වේගය අඩු කිරීම
- මෙහෙයුම් පද්ධතිය මන්දගාමී කිරීම
- පරිගණක මතකයෙන් (Ram හා Cache) වැඩි ඉඩක් ලබා ගැනීම
- පරිගණකයේ දත්ත විනාශ කිරීම
- පරිගණකයේ කාර්යක්ෂමතාවයට බලපෑම් ඇතිකිරීම
- පරිගණක දෘඩාංග දුර්වල කිරීම
- පරිගණක ජාලයන්ට හානි කිරීම

වෛරස් වලින් වැළකීම හා ප්‍රතිකර්ම

- පිටස්තර අයට පරිගණකයට ඇතුළුවීම සීමා කළ යුතුය
- උසස් වර්ගයේ ප්‍රතිවෛරස් මෘදුකාංගයක් පරිගණකයට ස්ථාපත කිරීම. සෑම විටෙම නව මුහුණුවරින් යුත් පරිගණක වෛරස් පැමිණෙන හෙයින් මෙම මෘදුකාංගයද දින

පතා හෝ සති පතා යාවත්කාලීන කළ යුතුය.

- නොදන්නා ප්‍රභවයන්ගෙන් එන ඉ-තැපැල් ඇමුණුම් විවෘත නොකිරීම.
- දන්නා ප්‍රභවයකින් වුවද, අන්තර්ගතය නොදන්නා ඉ-තැපැල් ඇමුණුම් විවෘත නොකිරීම.
- ඉ-තැපැල් ඇමුණුම් විවෘත කිරීමට

පෙර වෛරස පරීක්ෂාවක් සිදු කිරීම.

- සැක කටයුතු යෙදුම්, ආරක්ෂිත නොවන වැඩසටහන් බාගත නොකරන්න. සෑම විටම අවසරලත් මෘදුකාංග පමණක් ස්ථාපනය කරන්න.
- ආරක්ෂිත වැඩසටහන් පමණක් භාවිතා කරන්න.
- ඊ-මේල් තුළ ඇති සැක සහිත සබැදි ක්ලික් නොකිරීම
- මුරපද වැනි ඔබගේ ආරක්ෂක තොරතුරු අන් අය සමග බෙදා නොගැනීම
- අන්තර්ජාලය වෙත පිවිසීමේදී ආරක්ෂිත වෙබ් බ්‍රවුසරයක් භාවිතා කිරීම.
- අන්තර්ජාලය සඳහා ෆයර් වෝල් (වෙනත් පිටස්තර පරිගණක ජාලයකින් අපගේ පරිගණක ජාලයක් වෙත පැමිණෙන දත්ත ඇතුලු වීමට අවසර ලබාදෙන හෝ ඇතුලු වීම වළක්වන මෘදුකාංගයක් හෝ දෘඩාංගයකි) එකක් භාවිතා කිරීම.
- පරිගණකයේ මෙහයුම් පද්ධතිය හා භාවිතා කරන මෘදුකාංග යාවත්කාලීන කිරීම.
- සැකසහිත වෙබ් අඩවිවලට ප්‍රවේශ වීමෙන් වැළකීම.
- අන්තර්ජාලයෙහි නොදන්නා ප්‍රභවයන්ට ඔබගේ වැදගත් පුද්ගලික තොරතුරු (ඉ-තැපැල් ලිපිනය, බැංකු ගිණුම් අංක, ක්‍රෙඩිට් කාඩ් අංක) සැපයීමෙන් වැළකීම.
- අන්තර්ජාලයෙන් බාගත කිරීමේදී විශ්වාසදායී වෙබ් අඩවිවලින් පමණක් සිදු කිරීම.

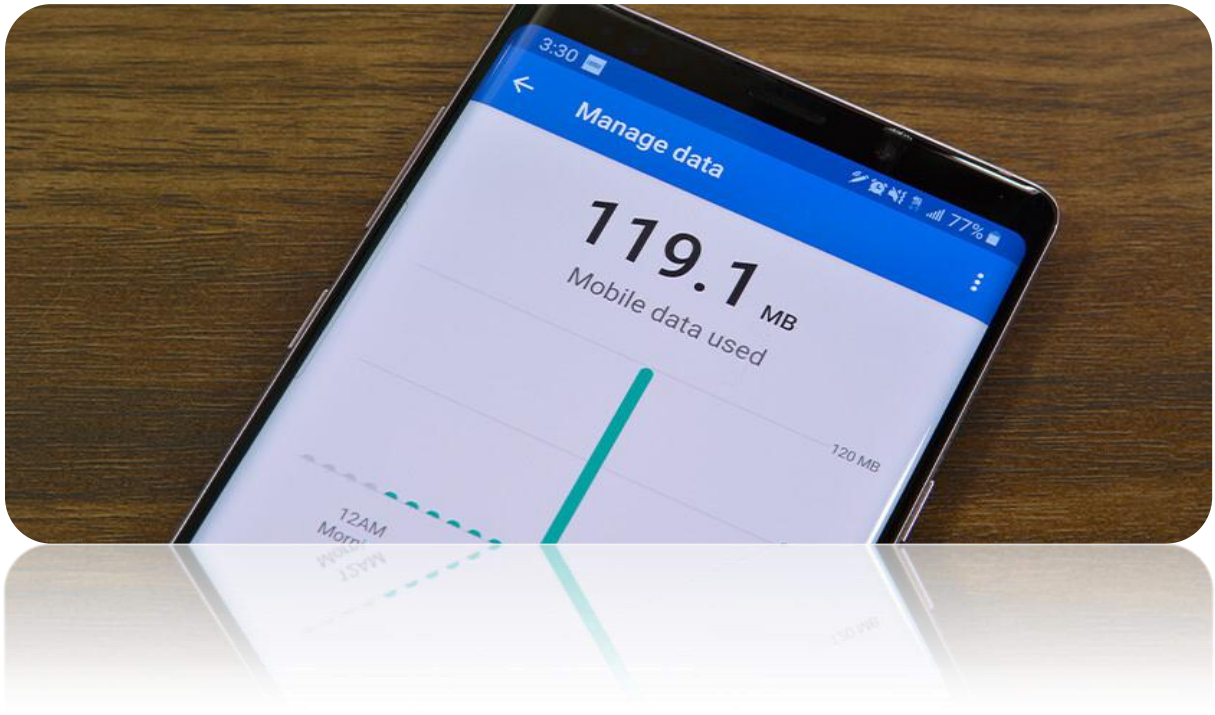
ප්‍රතිවෛරස මෘදුකාංගයක් තෝරා ගැනීමේදී සැලකිලිමත් විය යුතු කරුණු

වෙළඳපොලෙහි මිලදී ගත හැකි ප්‍රති වෛරස් මෘදුකාංග බොහොමයක් ඇත. එමෙන්ම අන්තර්ජාලය හරහා නොමිලයේම භාගත කළ හැකි ප්‍රති වෛරස් මෘදුකාංග ද බොහොමයක් ද ඇත. නමුත් මේවායින් ඔබගේ පරිගණකයට ගැලපෙන ප්‍රතිවෛරස් මෘදුකාංගය තෝරා ගැනීමේ දී ප්‍රධානව සලකා බැලිය යුතු කරුණු වන්නේ,

ඔබ ස්ථාපිත කරන ප්‍රති වෛරස් මෘදුකාංගය ස්වයංක්‍රීයව යාවත්කාලීන කළ හැකි ද යන්න පිළිබඳව.

1. ප්‍රතිවෛරස් මෘදුකාංගය නිර්මාණය කරන ආයතනය විසින් ක්‍රමානුකූලව යාවත්කාලීන කරන වෛයිරස පිළිබඳ විග්‍රහයක් සපයයි ද යන්න පිළිබඳව.
2. වයිරස පරීක්ෂාවන් ස්වයංකීයව සිදුකළ හැකිදැයි යන්න පිළිබඳව.
3. ප්‍රතිවෛරස් මෘදුකාංගය නිර්මාණය කරන ආයතනය විසින්, අලුතෙන් සොයාගන්නා ලද වෛයිරස පිළිබඳ නිවැරදි හා කාලෝචිත තොරතුරු ප්‍රකාශයට පත් කරන්නේද යන්න පිළිබඳව.

Data පරිස්සම් කර ගනිමු



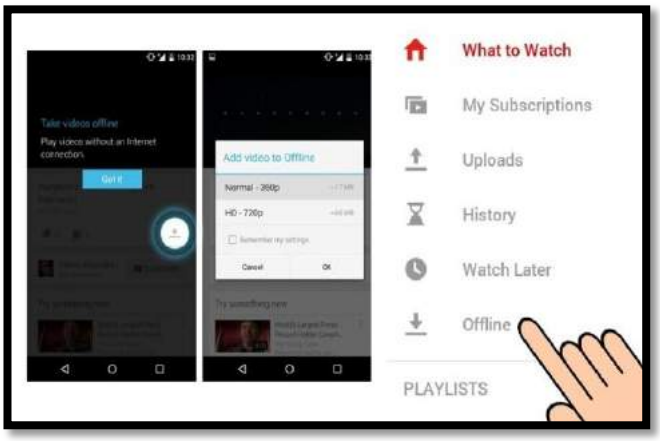
අන්තර්ජාලය හරහා ඔබ වීඩියෝ එකක් බලන වෙලාවක හරි සිංදුවක් අසමින් සිටින විට ජංගම දුරකතනයේ ඩේටා ඉවරයි කියලා හරි ඩේටා ඉවර වෙන්න ළඟයි කියලා එන මැසේජ් එක ඔබට පුරුදු ඇති. මේ වෙලාවට අපි ඩේටා භාවිතා කරන දුරකථන සේවා සපයන්නා සමඟ ලොකු තරහක් ඇති කර ගන්නවා ඔවුනගේ සේවාව පිළිබඳ දුර්වලතාවන් සඳහන් කරමින්. එහෙම නැත්නම් අපිට හිතෙනවා මෙතරම් ඉක්මනින් ඩේටා අඩු වුණේ කොහොමද කියලා. මෙයට ප්‍රධාන හේතුව වන්නේ ඩේටා භාවිතය පිළිබඳව ඔබගේ නොදැනුවත්කමයි.

නමුත් ඔබ දන්නවාද ඔබ භාවිතා කල ඩේටා කාර්යක්ෂමව භාවිතා කලා නම් ඔබේ ජංගම දුරකතනයෙන් ඩේටා කැපෙන වේගය අඩු කර ගත හැකි බව. අපි දැන් කතා කරන්න යන්නේ අන්න ඒ ඩේටා කොහොමද පරිස්සමින් භාවිතා කරන්නේ කියලා. අපි බලමු ඒ සඳහා ඔබට කල හැකි සරල පියවර කිහිපයක්.

ඩේටා සීමාවක් (Data limit) සාදා ගැනීම

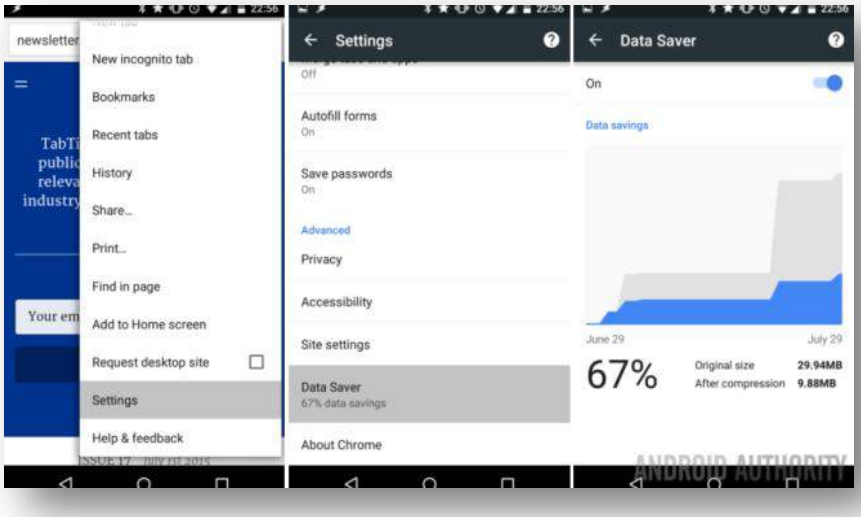
ඔබේ ජංගම දුරකතනයේ ඩේටා භාවිතය සඳහා ඩේටා ලිමිට් එකක් තබා ගැනීම වැදගත් වෙනවා. මෙමගින් ඔබ භාවිතයට ගන්නා ඩේටා ප්‍රමාණය පිළිබඳව අවබෝධයක් ලබා ගත හැකි වෙනවා. එසේම වැඩිපුර ඩේටා භාවිතා කිරීමට යෑමේදී දැනුම්දීමක් (notification) හෝ අනතුරු හැඟවීමක් (warning) ලබා ගන්න පුළුවන්. ඒ සඳහා ඔබේ දුරකථනයේ **Settings > Connections > Data Usage** හරහා Android දුරකථනයක මෙම සේවාව සක්‍රීය කර ගත හැක. එසේම ඔබේ දුරකථනයේ දත්ත සුරැකුම (Data Saver) අංගය ක්‍රියාත්මක කිරීමෙන්, වැඩිපුර ඩේටා භාවිතා කරන ඔබේ දුරකථන යෙදුම් (Apps) මොනවා ද යන්න පිළබඳ තොරතුරු ලබා ගත හැකි අතර සීමිත දත්ත සැලැස්මක් මත අඩු ජංගම දත්ත භාවිතා කිරීමට උදව් කර ගත හැක.

Offline වැඩ කිරීම



අන්තර්ජාලයේ නරඹන වීඩියෝවක හෝ වෙබ් පිටුවක 'watch offline' හෝ save an offline version යන අංග දෙක භාවිතා කර ගනිමින් offline වැඩ කල හැක. ඒ වගේම ඔබ වීඩියෝවක් නරඹන විට ඉතා ඉහළ ප්‍රමිතියේ වීඩියෝවක් හෙවත් high-quality කියන option එක ඉවත් කර වීඩියෝව නැරඹීම සිදු කරන්න. ඔබ Google Maps App එක සම්පූර්ණයෙන්ම බාගත(download) කරගත් පසු Google Maps App එක ඩේටා නැතුව භාවිතා කරන්න පුළුවන් කියන එක බොහෝ දෙනෙක් නොදන්න දෙයක් ඔබ වයි-ෆයි භාවිතයේන් එක වරක් download කර පසු එය මාසයක් පමණ භාවිතා කළ හැක. ඔබට මසකට වරක් පමණ නැවත යාවත්කාලීන කිරීම (update) කළ හැක. Google Maps App එකේ වම්පස ඇති ඉරි තුන මත ඇති offline map සේවාව හරහා ඔබට මෙය පහසුවෙන් කර ගත හැකියි.

Google Chrome Data Saver භාවිතා කරන්න



ගූගල් ක්‍රෝම් යනු වඩාත් ජනප්‍රිය ඇන්ඩ්‍රොයිඩ් බ්‍රව්සර් වලින් එකකි. ඇන්ඩ්‍රොයිඩ් හි දත්ත පරිභෝජනය සැලකිය යුතු ලෙස අඩු කළ හැකි ඉන්බිල්ට් අංගයක් වන දත්ත සුරැකුමක් එහි ඇත.මෙය දත්ත සම්පීඩනය ලෙස ද භාවිතා කිරීමට, Google Chrome විවෘත කරන්න, ඉහළ දකුණු කෙළවරේ ඉරි තුන මෙනුව(menu) මත click කරන්න.ඉන්පසු සැකසීම් (Settings option) තෝරන්න, මෙම දත්ත සුරැකුම (data saver) සක්‍රිය කිරීමෙන් අනිෂ්ට පිටු (malicious pages) හඳුනා ගැනීම සහ අනිෂ්ට මෘදුකාංග (malicious software) හා හානිකර අන්තර්ගතයන්ගෙන් ආරක්ෂා කිරීමට Google Chrome හි ආරක්ෂිත බ්‍රවුසින් (browsing) පද්ධතිය ක්‍රියාත්මක කරයි.මෙහි ප්‍රතිඵලය වනුයේ දත්ත පරිභෝජනය අඩු වීම සහ වෙබ් අන්තර්ගතයේ සැලකිය යුතු වෙනසක් නොමැතිව වෙබ් පිටු පැටවීම වේගවත් කිරීමයි. මෙම අංගය ක්‍රියාත්මක කිරීමට Google Chromeහි මෙනුවේ Settings > Data Saver හරහා මෙය සක්‍රිය කර ගත හැකියි.

පසුබිම් යෙදවුම් (Background Apps) වලින් ඩේටා භාවිතය වැළැක්වීම

පසුබිම් යෙදවුම් (Background Apps) වලින් ඩේටා භාවිතයේ වාසි වගේම අවාසිත් තිබේ. එක වාසියක් නම් යෙදවුම් (Apps) එකක අලුත් යාවත්කාලීන කිරීම ආ සැණින් ඉබේම එය යාවත්කාලීන වීමය, අවාසිය නම් ජංගම දුරකතන පාවිච්චි නොකරන වෙලාවටත් එම යෙදවුම් (Apps) නිතරම ධාවනය වෙමින් පැවතීමය. ඒ නිසා එය අවහිර කිරීම වාසි දායක වේ. මේ සඳහා Settings > Apps වෙත යන්න. එතැන දී ඔබේ ජංගම දුරකතනයේ දැනට භාවිතයේ ඇති Apps ලැයිස්තුවක් දකින්න ලැබේ. එයින් එකක් ක්ලික් කළ විට එම ඇප් එක පෙරබිමේ (foreground) භාවිත කරන ඩේටා ප්‍රමාණය සහ පසුබිමේ (background) ධාවනය වන අවස්ථාවේ භාවිත කරන ඩේටා ප්‍රමාණය දකින්න ලැබේ. App එක තිරයේ පෙනෙන්න තිබෙන වෙලාවේ භාවිත කරන ඩේටා foreground ඩේටා නම් වේ. "Allow background data usage" තේරීම අක්‍රිය කළ පසුබිමේ ඩේටා භාවිතය නවත්වන්න පුළුවන්.

- **අනිෂ්ට මෘදුකාංග (malware) ඉවත් කරන්න**

ඔබගේ දුරකථනයේ සාමාන්‍ය ඇන්ඩ්‍රොයිඩ් යෙදුම් පමණක් නොව, සෑම විටම දත්ත සීමාව අවසන් වීමට වෙනත් හේතුද තිබිය හැකිය.හොඳ ප්‍රති-වයිරස යෙදුමක් සමඟ අනිෂ්ට මෘදුකාංග සඳහා ඔබේ ඇන්ඩ්‍රොයිඩ් දුරකථනය නිතිපතා පරිලෝකනය (scan) කරන්න. මෙමඟින් ඔබගේ ඇන්ඩ්‍රොයිඩ් දුරකථනය වේගවත් කිරීමට උපකාරී වේ.

- **වීඩියෝ Auto play වීම නැවැත් වීම**

ඔබගේ ජංගම දුරකථනයේ ඔබ නොදැනුවත්ම වීඩියෝ auto play වෙන අංගය සක්‍රීය වී තිබෙන්න පුළුවනි. මේ හරහා බොහෝවිට YouTube වලින් ඩේටා වැඩි ප්‍රමාණයක් නාස්ති වේ. මෙවැනි යෙදුම් භාවිතා කිරීමේදී අඩු නමුත් ඔබට ලේසියෙන්ම මෙම Auto play අංගය අක්‍රිය කිරීම මඟින් පහසුවෙන් ඩේටා නාස්තිය නතර කර ගත හැක. ජංගම දුරකථනයේ settings හරහා මෙය සිදු කිරීමට ද පුළුවනි.

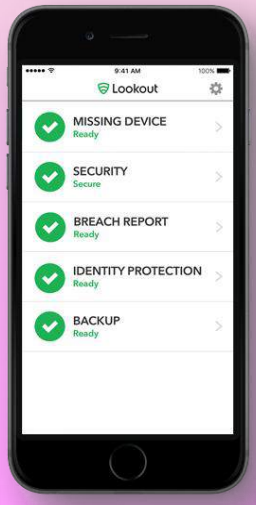
- **ඔබගේ යෙදුම් (app) පිළිබඳව විමසිල්ලෙන් සිටින්න.**

විශාල වශයෙන් දත්ත-යොදා ගන්නා යෙදුම් (app) භාවිතය ඔබගේ ජංගම දුරකථන ජාලයේ සිටින විට ඔබගේ දත්ත පරිභෝජනයට බරපතල ලෙස බලපායි.ෆේස්බුක් සහ ඉන්ස්ටග්‍රෑම් වැනි සමාජ මාධ්‍ය යෙදුම් විශාල දත්ත ප්‍රමාණයක් පරිභෝජනය කරයි.එම යෙදුම්වල වීඩියෝ සහ GIF නැරඹීමෙන් වළකින්න.අඩු දත්ත ප්‍රමාණයක් පරිභෝජනය කරන අතරම අවශ්‍ය කාර්යයන් තවමත් ඉටු කරන සමහර යෙදුම් සඳහා විකල්ප භාවිතා කිරීමට උත්සාහ කරන්න. උදාහරණයක් ලෙස, ෆේස්බුක් ලයිට් යනු ෆේස්බුක් යෙදුමට බෙහෙවින් සැහැල්ලු විකල්පයකි. එපමණක් නොව, එය බැටරි ආයු කාලය සහ දත්ත භාවිතය ඉතිරි කරයි. TweetCaster යනු ට්විටර් යෙදුම සඳහා සමාන විකල්පයකි.

ඔබගේ ස්මාර්ට් දුරකථනය සුරක්ශිතද?

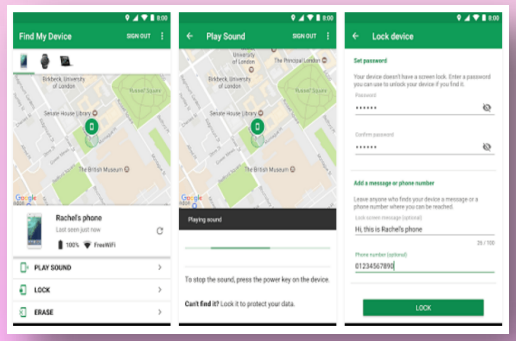
නිරතුරුව වෙනස්වන තාක්ෂණය සහ පහසුවෙන් ගෙනයා හැකි බව හේතුවෙන් විශාල ලෙස ස්මාර්ට් ජංගම දුරකථන මත යැපීමට අප පුරුදුව සිටී. වැඩිදියුණුවූ පහසුකම් හේතුවෙන් එදිනෙදා ජීවිතයේ බොහෝ කාර්යයන් සඳහා ස්මාර්ට් ජංගම දුරකථන යොදා ගනිමින් පවති. වෙබ් පිටු පිරික්සීම, ක්ෂණික පණිවිඩ යැවීම, වීඩියෝ ඇමතුම් ලබා ගැනීම, ලිපි ගොනු බෙදා හැරීම, ජංගම බැංකුකරණය වැනි කාර්යයන් මේ සඳහා උදාහරණ ලෙස දැක්විය හැක.

ස්මාර්ට් ජංගම දුරකථන වල ඇති මෙම පහසුකම් නිසා එය අන්තර්ජාල අපරාධවල නිරන්තර ඉලක්කයක් බවට පත්වී ඇත. මෙවැනි බොහෝ අපරාධ සඳහා, ජංගම දුරකථන සඳහාම විශේෂයෙන් සැකසූ, "malware" මෘදුකාංගය යොදා ගනිමින් පවති. උදාහරණ වශයෙන් "spyware" මෘදුකාංග දැක්විය හැකියි. එසේම තව දුරටත් ස්මාර්ට් ජංගම දුරකථන භාවිතා කරන්නන්හට අවමාන, තර්ජනය කිරීම්, අනන්‍යතා සොරාගැනීම්, මුලාකිරීම් සහ අනෙකුත් සොරකම් සඳහා භාජනය වීමේ අවධානමක් පවතී. ඔබේ ස්මාර්ට් ජංගම දුරකථනය මෙම තර්ජනය සඳහා නිරාවරණය වීමේ අවදානම අඩුකිරීමේ



ප්‍රායෝගික පියවර කිහිපයක් මෙලෙස දැක්විය හැක.

1. ශක්තිමත් මුරපද හෝ ආරක්ෂිත රටාවන් (Pattern) භාවිතාකිරීම.
2. භාවිතා නොවන මිනිත්තු/තප්පර කිහිපයකට පසුව, දුරකථන තිරය අගුලු දැමීම. (මේ සඳහා ස්වයංක්‍රීය අගුලු දැමීම (Auto Lock) භාවිතා කරන්න).
3. දුරකථන මෙහෙයුම් පද්ධතිය සහ යෙදවුම් නිරතුරුව යාවත්කාලීන කිරීම.
4. උපාංග සංකේතනය භාවිතා කිරීම (Encryption).
5. වයිෆයි පහසුකම් භාවිතා නොකරන අවස්ථාවලදී එය විසන්ධිකර තැබීම.
6. බ්ලූටූත් පහසුකම් භාවිතා නොකරන අවස්ථාවල දී එය විසන්ධි කරතැබීම.
7. අත්‍යවශය යෙදවුම් (Apps) පමණක් දුරකථනයෙහි ස්ථාපනය කිරීම සහ ස්ථාපනය කිරීමට පෙර අවශ්‍ය අවසර ලැයිස්තුව (Permission Set) නිසි පරිදි පරීක්ෂා කිරීම. (එම යෙදවුම් භාගත කිරීමේදී නිවැරදි (official) "play store"හෝ "App Store" භාවිතා කිරීම සහ එම යෙදවුම පිළිබඳව ඇති අදහස් (Comments) කියවීම අත්‍යවශ්‍යවේ.)
8. සමාජජාල මාධ්‍ය භාවිත කිරීමේදී හෝ අන්තර්ජාල පිරික්සුම්වල දී හඳුනා නොගත් සබැඳියන් (Links) තුලට පිවිසීමෙන් වැළකීම.
9. දුරකථනය අස්ථානගත වීමකදී ප්‍රයෝජනයටගත හැකි “Find my device” පහසුකම සක්‍රීය කිරීම. (දුරකථනය අස්ථානගත වූ අවස්ථාවකදී නැවත එය සොයා ගැනීම සඳහා "TRC" ආයතනය හා "ineed.police.lk" මගින් සහය ලබාගැනීමට හැකිය.)
10. Remote wipe පහසුකම සක්‍රීය කිරීම.
11. ප්‍රති-වයිරස මෘදුකාංගයක් ස්ථාපනය කිරීම සහ එය නිරතුරුව යාවත්වකාලීන කිරීම.
12. සියලු වැදගත් තොරතුරු සඳහා “backup” යෙදවුම් පවත්වා ගැනීම.



13. කිසියම් අවස්ථාවකදී දුරකථනය තෙවන පාර්ශවයකට භාරදෙනවිට, එය “Factory Reset” ක්‍රියාවලියට භාජනය කිරීම හෝ එහි ඇති දත්ත (පින්තූර, පණිවිඩ, ඉතිහාසය) ස්ථීර ලෙස මකා දැමීම.

සෞඛ්‍ය ක්ෂේත්‍රය සඳහා තොරතුරු තාක්ෂණය භාවිතය

අතීතයේ මිනිසුන්ට තම වෛද්‍ය පහසුකම් ලබා ගැනීම වෙනුවෙන් දැඩි වෙහෙසක් හා කාලයක් ගත කිරීමට සිදුවිය. නාගරික ප්‍රදේශ වලට පමණක් සීමාවූ සමහර වෛද්‍ය පහසුකම් නවීන තාක්ෂණය හරහා ග්‍රාමීය ජනතාව වෙත ඉතා පහසුවෙන් ළඟා කරදීම සඳහා තොරතුරු තාක්ෂණ භාවිතයන් මේ වන විට උපයෝගි කර ගනී. ලොව පුරා තොරතුරු තාක්ෂණ දිරි ගැන්වීම් භාවිතය වැඩිවීමත් සමගම සෞඛ්‍ය ක්ෂේත්‍රය සඳහාද නව තාක්ෂණික යොදා ගැනීම් පිළිබඳ විශාල නැඹුරු වීමක් දක්නට ලැබේ. විශේෂයෙන්ම සෞඛ්‍යය සත්කාර සේවා සැපයීමේදී මෙන්ම පරිපාලන සහ සායනික අංශ දෙක සඳහාද තොරතුරු තාක්ෂණය පුළුල් ලෙස යොදා ගනිමින් පවතී.

සෞඛ්‍ය ක්ෂේත්‍රයේ පහත අංශ සඳහා සඳහා තොරතුරු සන්නිවේදන තාක්ෂණය බොහෝ සෙයින් වැදගත් වේ.

- දුරස්ථ සෞඛ්‍ය රැකවරණය
- වෛද්‍ය දත්ත සහ වාර්තා ගබඩා කිරීම සහ පවත්වා ගෙන යෑම
- නවීන උපකරණ භාවිතය
- වෛද්‍ය පරීක්ෂණ
- පර්යේෂණ සහ නව සොයා ගැනීම්

දුරස්ථ සෞඛ්‍ය රැකවරණය හරහා තොරතුරු හා සන්නිවේදන තාක්ෂණය යොදා ගනිමින් රෝහලකින් පිටත ස්ථානයක සිටින රෝගියෙකු හා සම්බන්ධවෙමින් රෝගියාට අවශ්‍ය ඉතා ඉහළ ගුණාත්මක බවින් යුත් සත්කාරයන් ලබා ගැනීමට පහසුකම් සැලසෙයි.

දුරස්ථ සෞඛ්‍ය රැකවරණයේ මූලික ලක්ෂණ වනුයේ,

- දුරස්ථ සෞඛ්‍ය උවටැන් (Remote clinical care) නිසා සමහර අවස්ථාවලදී වෛද්‍යවරයා වෙත යාමට අවශ්‍ය නොවීම.
- වෛද්‍ය උපදෙස් මාර්ගගත ආකාරයට ලබා ගත හැකි වීම.
- රෝගියා නිවසේ සිටීම අධීක්ෂණය කිරීමට හැකිවීම.

මීට අමතරව සමහර අවස්ථාවලදී, සෞඛ්‍ය සේවා නිළධාරීන් සඳහා දුරස්ථ පුහුණුව ලබා දීමටද මෙය යොදාගත හැක.

නවීන තාක්ෂණික උපකරණ හා මෙවලම් භාවිතා කරමින් සුවිශේෂී වෛද්‍ය පරීක්ෂණ සිදු කිරීමට හැකියාව ලැබීමද සෞඛ්‍ය ක්ෂේත්‍රය අත් කර ගත් සුවිශේෂී ජයග්‍රහණයකි.

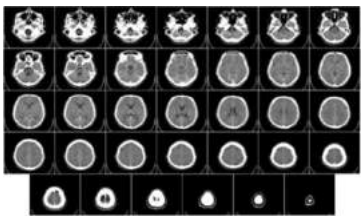
- ශල්‍යකර්ම සඳහා යොදා ගන්නා වීඩියෝ දසුන් ලබා ගත හැකි කැමරා සහිත උපකරණ. (Endoscopy)
- රෝගීන්ගේ තොරතුරු සහ වෛද්‍ය වාර්තා සඳහා පරිගණක දත්ත පද්ධති යොදා ගැනීම.
- සෞඛ්‍ය ක්ෂේත්‍රයේ නිළධාරීන් හා කාර්ය මණ්ඩලය පුහුණු කිරීමට නවීන උපකරණ යොදා ගැනීම.

තොරතුරු හා සන්නිවේදන තාක්ෂණය භාවිතා කරමින් සිදු කෙරෙන සෞඛ්‍ය පරීක්ෂණ.

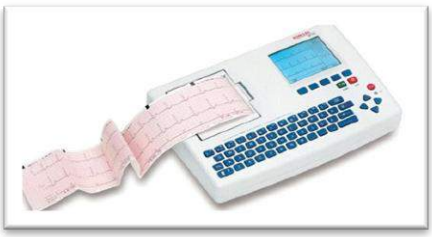
සෞඛ්‍ය ක්ෂේත්‍රයේ නවීන පරීක්ෂණ ගණනාවටම තොරතුරු හා සන්නිවේදන තාක්ෂණ මෙවලම් භාවිතා කරයි.

1) **CAT – Computerized Axial Tomography - (පරිගණකගත ආක්ෂක ශරීර ස්ථර එක්ස්රේ ස්කෑනර්)**

මෙම යන්ත්‍රය මගින් එක්ස්රේ තාක්ෂණය යොදා ගනිමින් මිනිස් සිරුරේ අභ්‍යන්තර කොටස් වෙන් වෙන් වශයෙන් ත්‍රිමාන ආකාරයට ජායාරූප ලබා ගැනීම සිදු කරණු ලබයි.



2) **ECG – (Electrocardiogram) -ඊ.සී.ජී පරීක්ෂණය**



මෙම යන්ත්‍රය මඟින් හෘදයේ සිට ශරීරයේ අනෙකුත් ඉන්ද්‍රියයන් වෙත රුධිරය සැපයීමේදී හෘදයේ ඇතිවන විද්‍යුත් ස්පන්දනය අනුව නිපදවෙන තරංග ප්‍රස්ථාරික කඩදාසියක සටහන් කිරීම සිදු කෙරේ. මෙය හෘදයාබාධ අවස්ථා ඉක්මනින් හඳුනාගෙන රෝගියාගේ හදවතේ තත්වය නිරීක්ෂණය කිරීමට කෙරෙන පරීක්ෂණයකි.

3) MRI – (Magnetic Resonance Imaging Machine) - චුම්භක අනුනාද මූර්තන යන්ත්‍රය

රේඩියෝ තරංග සහ ප්‍රබල චුම්භක අනුනාද මගින් ශරීරයේ අභ්‍යන්තර කොටස්වල (විශේෂයෙන්ම සංවේදී අවයවයන් වන මොළය, හෘදය වස්තුව, පෙනහළු) ඇති ආබාධ විවිධ පැතිවලින් ඡායාරූපගත කර පරිගණක තිරයක් මගින් ලබා ගැනීම සහ අවශ්‍ය විට ප්‍රතිබිම්භ නැවත ප්‍රතිනිර්මාණය කර ගැනීමද මෙමගින් සිදු කෙරේ.

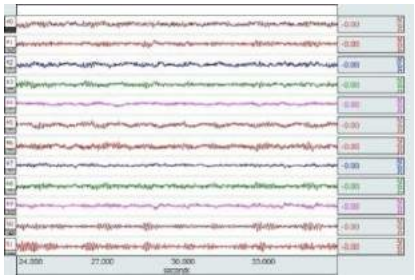
4) 2D Echo- Cardiac Machine - හෘද රෝග තිර ගැන්වීමේ යන්ත්‍ර

හෘදයේ ක්‍රියාකාරීත්වය පරිගණක තිරයක දැක්වීම මෙම යන්ත්‍රය මගින් සිදුවේ. හෘදයේ රුධිර නාල සිහින් වීම සහ කපාටගත අබාධ වැනි විවිධ තත්වයන් හඳුනා ගැනීමට මෙම පරීක්ෂණය මගින් හැකියාව ඇත.

5) EEG –Electro (Encephalography)

මොළයේ ක්‍රියාකාරීත්වය පරීක්ෂා කිරීම සඳහා මෙම යන්ත්‍රය භාවිතා කරයි. මොළයෙන් නිකුත්කරන ලද විද්‍යුත් ස්පන්ධන ග්‍රහණය කර මොළයේ ක්‍රියාකාරීත්වය තිරයක සටහන් කර ගනී. අපස්මාර රෝගීන්ගේ රෝග නිර්ණය සඳහා මෙය බොහෝ උපකාරීවේ.

තම නිවසේ සිටම නිවසින් බැහැරව නොගොස් තම රෝගය පාලනය පිළිබඳ අවබෝධයක් ලබා ගැනීමට පහත උපකරන අවස්ථාවක් ලබා දේ.



6) **Blood Sugar Testing Machine - රුධිරයේ සීනි මට්ටම පරීක්ෂා කිරීමේ උපකරණය**

රුධිර සාම්පලවල ඇති සීනි තත්වය මෙම යන්ත්‍රය මගින් පෙන්නුම් කරයි.

7) **Blood Pressure Testing Machine - රුධිර පීඩනය මනින යන්ත්‍රය**

මෙම උපකරණය මගින් රෝගියා විවේකීව මෙන්ම ක්‍රියාකාරීව සිටින විටද අවස්ථාව අනුව රුධිර පීඩනයේ වෙනස්කම් මැන ගත හැකිය.

මානව සංහතියේ යහපත උදෙසා **සෞඛ්‍ය** ක්ෂේත්‍රයේ නිතිපතා සිදුවෙන දියුණුවීම්වලදී මේ අයුරින් තොරතුරු තාක්ෂණයේ යෙදීම් අපට දැක හැකිය.

අධ්‍යාපන ක්ෂේත්‍රය සඳහා තොරතුරු තාක්ෂණය යොදා ගැනීම

සම්ප්‍රදායිකව භාවිතා වූ ඉගෙණුම් ඉගැන්වීම් ක්‍රියාවලියෙන් ඔබ්බට යමින් නවීන තාක්ෂණය භාවිතයෙන් අධ්‍යාපනයට යොමුවීමට විශේෂයෙන්ම ලෝකයේ සියලු රටවල් වලට වසංගතයක්වූ covid-19 වලින් පසු ලංකාවේද මේ සඳහා විශේෂ අවධානයක් යොමු කර ඇත. මේ දක්වා පන්ති කාමරයට

පමණක් සීමාවී තිබූ අධ්‍යාපනය අද පරිගණක හා අන්තර්ජාලය සමඟ සම්බන්ධ වී සිදුකිරීමට

හැකියාවන් ලැබීම නිසා භූගෝලීය සීමා නොතකා අධ්‍යාපන පුළුල් ලෙස ව්‍යාප්ත වීමට අවකාශ උදාවී ඇත.

මෙම ඉගෙනුම් ක්‍රියාවලියේ ඇති විශේෂත්වය නම් එකවර විශාල පිරිසකට ලෝකයේ ඕනෑම තැනක සිට ඕනෑම වෙලාවක අධ්‍යයන කටයුතු කිරීමට අවස්ථාව උදා වීමයි. පන්ති කාමරයේදී සිදුකරන ඉගෙනුම් වලදී ළමුන් කියිප දෙනෙකුට පමණක් සීමා වීමත්, කාලසටහනකට අනුව ඉගෙනුම් ක්‍රියාවලි කිරීමත් යන බාධක මෙමගින් මග හැරේ.

මාර්ගගත අධ්‍යාපනයේදී බහු මාධ්‍ය තාක්ෂණය හරහා වඩාත් ආකර්ශනීය ආකාරයට වචන, රූප, ශබ්ධ,චලනරූප හැසිරවිය හැකි නිසා ඇතැම් සංකල්ප මතක තබා ගැනීමේ හැකියාවද වැඩිකර ගැනීමට රුකුලක් වී ඇත.

සිසුන්ගේ කුසලතා වර්ධනය කිරීම සඳහා අවශ්‍ය ස්වයං අධ්‍යාපන අභ්‍යාස සහ ඒ සඳහා අවශ්‍ය මගපෙන්වීම් ආදියද මෙවැන් අධ්‍යාපනික ක්‍රම මගින් කලමණාකරණය කර ගත හැක.

මාර්ගගත අධ්‍යාපනය ක්‍රම කිහිපයකින්ම ලබා දිය හැක.

(1) Computer Based Training (CBT)
(2) Learning Management System (LMS)
(3) Distance Education System (DES)
(4) Web Based Training (WBT)
(5) Computer Assisted Learning (LAL)

ලංකාවේ ශිෂ්‍යයන්ට මාර්ගගත අධ්‍යාපණය ලබා ගත හැකි වෙබ් අඩවි.

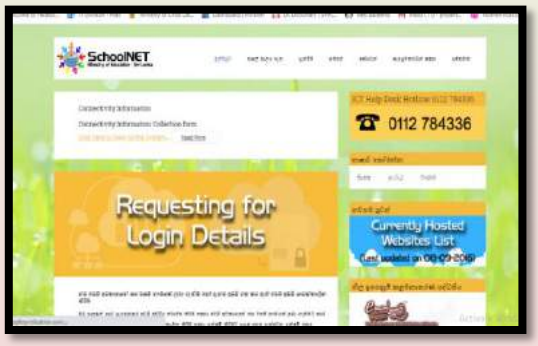
- www.schoolnet.lk
- www.myschool.lk
- www.nenasala.lk
- www.e-thaksalawa.mov.gov.lk

- www.vidumanpwtha.com

මාර්ගගත ඉගෙනුම් කළමනාකරණ පද්ධතියෙන් සිසුන්ට අත්වන වාසි.

1. ඕනෑම ස්ථානයක සිට ඕනෑම වෙලාවක ඉගෙනුම් ක්‍රියාවලියට සම්බන්ධ වීමට හැකි වීම
2. සංවාද මණ්ඩප හා එක්වී ගැටළු නිරාකරණය නිරීමට හැකිවීම
3. පැවරුම් , අභ්‍යාස සිදුකර උඩුගත කිරීමේ හැකියාව

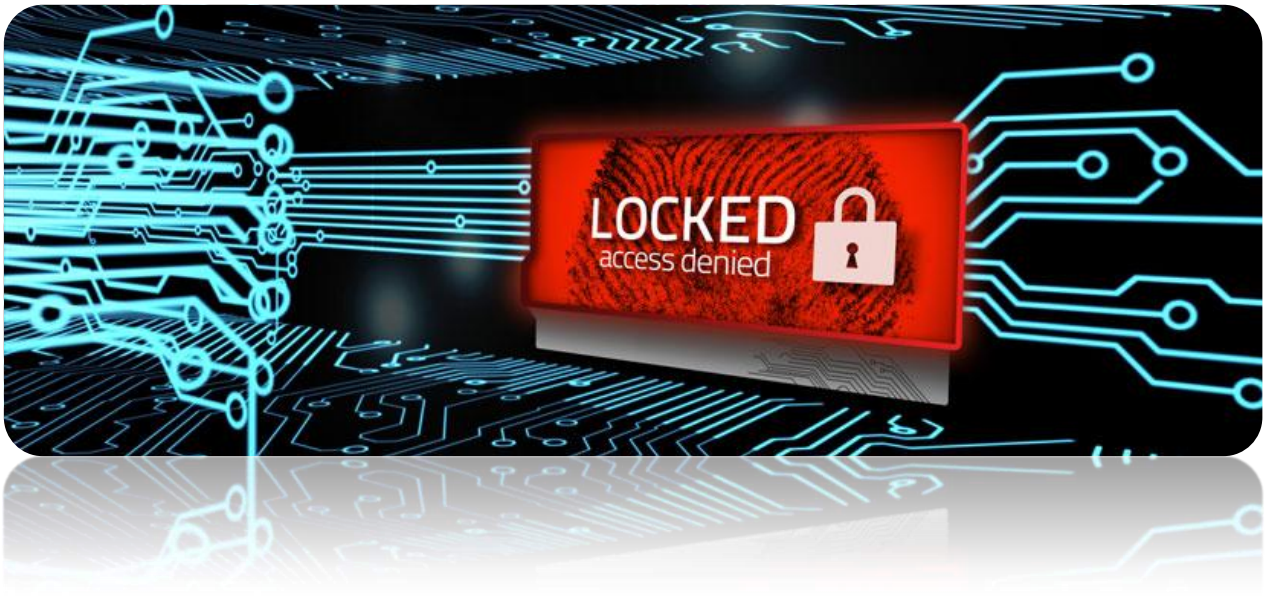
4. දෙමාපියන්ට තම දරුවන්ගේ ප්‍රගති මට්ටම් නිවසේ සිටම දැනගත හැකි වීම.



5. තොරතුරු තාක්ෂණයේ දියුණුවත් සමගම ඕනෑම රටක සිට තමන්ට කැමති ආකාරයේ අධ්‍යාපන ආයතනයන් හා සම්බන්ධ වීම තුලින් ඉතා අඩුවියදමකින් උසස් පාඨමාලාවක් හැදෑරීමට මාර්ගගත අධ්‍යාපණය යොදා ගත හැක.

අන්තර්ජාලය අධ්‍යාපනයට නිවැරදිව උචිත ලෙස යොදාගතහොත් එය අධ්‍යාපනයට මහත් පිටුවහලක් සපයනු බව නොඅනුමානය.

Ransomware - කප්පම් මෘදුකාංග හා ඒවායින් බේරීම



ඔබ බොහෝ දුරට Ransomware යන වචනය අසා ඇත. මේ Ransomware ගැන යම් පිරිසක් දැනුවත් වෙලා හිටියත් මේ වෙද්දී ලෝකය පුරාම දිනෙන් දින වර්ධනය වන මේ Ransomware බලපෑම ගැන සෑම දෙනාම දැනුවත් වීමක් අවශ්‍යය වෙනවා. ඒ ඇයි කිව්වොත් ලෝකේ පුරාම මේ Ransomware බලපෑම 50% කින් විතර වර්ධනය වෙලා තියෙනවා. එම නිසා මෙම මාතෘකාව ගැන කතා කිරීම කලෝචිතය යන්න අපගේ හැගීමයි.

Ransomware යනු සයිබර් ප්‍රහාරයේ දියුණු ආකාරයක් වන අතර ලොව පුරා දත්ත ආරක්ෂක (Data Protection) කණ්ඩායම් මුහුණ දෙන විශාලතම තර්ජනයකි. කුඩා කණ්ඩායම්වල සිට විශාල ව්‍යාපාර,

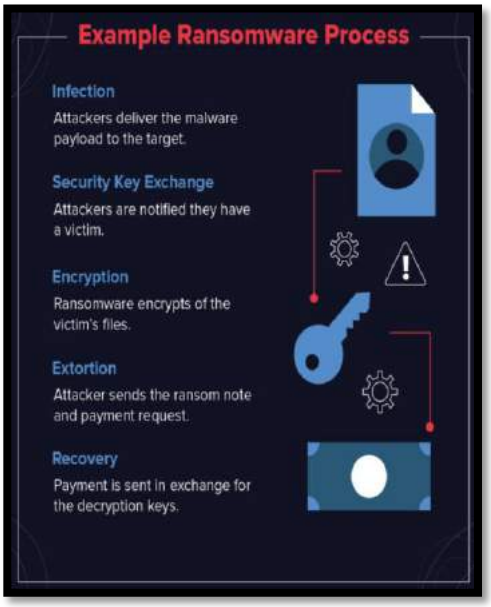
රාජ්‍ය පද්ධති සහ රජයේ ජාල දක්වා සියලුම සංවිධාන ඉලක්ක කර ගැනීමට Ransomware භාවිතා කරයි.

Ransomware මෘදුකාංග කප්පම් මෘදුකාංග ගණයට වැටෙන අතර අතිශයින්ම හානිකරය. තවමත් Ransomware කියන්නේ මොකද්ද කියලා හරි දැනුමක් නැති අයට පොඩි හැදින්වීමක් කරන්නට පෙර අනිෂ්ට මෘදුකාංග (Malware) ගැන කතා කරන්න අවශ්‍යය වෙනවා . අනිෂ්ට මෘදුකාංග (Malware) කියන්නේ සරලවම කිව්වොත් එය විශේෂ මෘදුකාංගයක්. මෙය සෑදීමේ ප්‍රදාන අරමුණ තමයි පරිගණක පද්ධති වලට හානි කිරීම එහෙම නැත්නම් පරිගණක පද්ධති අක්‍රීය කිරීම.

මේ කතාකරන යන අපේ මාතෘකාව Ransomware ගත්තොත් ඇත්තටම එය අයිතිවෙන්නෙත් මෙන්න මේ කියපු අනිෂ්ට මෘදුකාංග (Malware) ගනයටම තමයි.එය උපාංගයකට බාගත (download) කළ විට, යථා තත්වයට පත් කිරීම සඳහා මුදල් කප්පමක් ගෙවන තුරු සියලු දත්ත සිරීමට හෝ මකා දැමීමට සිදුවේ. Ransomware එක ගැන කෙටියෙන් කිව්වොත් මෙයින් ප්‍රදානව සිදු වන්නේ පරිගණකයක හෝ ජංගම දුරකථනයක හෝ ඕනම උපාංගයක තිබෙන දත්ත සංකේතනයක් (encryption) මගින් අගුල (lock) දැමීමක්ය. සංකේතනයකදී (encryption) සිදු වන්නේ දත්ත එක තැනක ඉදලා තව තැනකට සම්ප්‍රේෂනය කරද්දි හරි ගබඩා කරල තියෙද්දි හරි කාටවත් හොරකම් කරන්න බැරි විදිහකට දත්ත වෙනස් කරන එකයි. ඉන්පසු එම අගුල (lock) ඉවත් කිරීම සඳහා රහස් යතුරක් (key) අවශ්‍යය වෙනවා.ඒ රහස් යතුර (key) දුන්නොත් තමයි අපිට පුළුවන් වෙන්නේ අපේ සංකේතනය කරන ලද (encrypt වී ඇති) දත්ත ටික අයෙත් විකේතනය - (decrypt) කර ලබාගන්න. එහෙම නැත්නම් දත්ත සිරීමට හෝ මකා දැමීමට ලක් වූ දත්ත නැවත ලබා ගැනීමට හැකි වන්නේ.

Ransomware එකක ප්‍රධාන අරමුණ තමයි අපෙන් මුදල් ලබා ගැනීම. Ransomware මගින් සංකේතනය (encrypt) කරන ලද දත්ත ආපසු ලබාගැනීමට නම් Ransomware එක හදපු අයට යම්කිසි මුදලක් ගෙවීමට සිදුවෙනවා. අප හට එවන යතුරු (key) එකෙන් විතරම තමයි ඉතිං අපිට අපේ data ටික decrypt කරලා නැවත ලබාගන්න පුළුවන් වෙන්නේ. ඉතිං ඊළඟට අපි මේ මුදල් ගෙවන විදිය ගැන කතාකලොත් Ransomware පහර දෙන්නන් මුදල් ගෙවන්න සිද්දවෙන්නේ ක්‍රිප්ටො මුදල් (crypto currency) එකක් මාර්ගයෙන්. අන්න ඒ නිසා අපිට කිසිම හැකියාවක් නැතුව යනවා මේ පුද්ගලයන් ගැන කිසිම තොරතුරක් සොයා ගන්න.

Ransomware ක්‍රියා කරන ආකාරය



1. ආසාදනය (infection)
   පලමුව Ransomware ප්‍රහාරකයන් අනිෂ්ට මෘදුකාංග ඉලක්කගත පරිගණකය වෙත පහර දේ.
2. ආරක්ෂක යතුරු හුවමාරුව (Security Key Exchange) Ransomware ප්‍රහාරකයන් විසින් පහර දුන් අයට ඔවුන් ගොදුරු වී ඇති බව දැනුම් දීම
3. ගුප්ත කේතනය (Encryption)
   ගුප්ත කේතනයක් මගින් වින්දිතයාගේ ගොනුව Ransomware සංකේතනය (encrypt) කරයි
4. කප්පම් ගැනීම (Extortion)
   ප්‍රහාරකයා කප්පම් ගාස්තුව සහ ගෙවීම් ඉල්ලීම යවයි
5. නැවත ලබා ගන්න (Recovery)
   විකේතන (decryption) යතුරු ලබා ගැනීම සඳහා මුදල් ගෙවීම් යැවීම

Ransomware පැතිරෙන්නේ කෙසේද?

මේවා ලෝකේ පුරා පැතිරෙන ප්‍රධානම ක්‍රම කිහිපයක් වන්නේ ඊ මේල් , Ransomware මඟින් හානි වූ දත්ත ගබඩා උපාංග විවෘත කිරීම, වෙබ් අඩවි හෝ මෘදුකාංග මාර්ගයෙනි. Ransomware එකක් අපේ පරිගණකයට හෝ ජංගම දුරකථනයට ඇතුල් වීමට නම් ඒ සඳහා අනිවාර්යන්ම අපි කරන කුමන හෝ ක්‍රියාකාරකමක් හේතු වෙනවා. එනම්

1. නොදන්නා වෙබ් අඩවිය එකක් විවෘත කිරීම.
2. නොදන්නා මෘදුකාංග ස්ථාපනය කිරීම
3. නොදන්නා තැපෑල් වල ඇමුණුම් බාගත කර ගැනීම(attachments download). Ransomware සාමාන්‍යයෙන් විද්‍යුත් තැපැල් ඇමුණුමක් ලෙස වෙස්වලාගෙන සැලකිලිමත් පරිශීලකයින් වෙත යවනු ලැබේ. පරිශීලකයා එවැනි විද්‍යුත් තැපැල් ඇමුණුම් විවෘත කරන්නේ නම්, එය කෙලින්ම ආසාදනයකට තුඩු දිය හැකිය.

ඉහත ක්‍රියාකාරකම අපි නොදැනුවත්ව කරන දෙයක් වන්නට පුළුවන් නැත්නම් නොසැලිකිලිමත් කමකින් වුවද සිදු විය හැක. ඒ කොහොම වුවත් අපි කරන බොහොම පුංචි දෙයක් නිසා Ransomware එකකට හැකියාව ලැබෙනවා අපේ වැදගත් දත්ත මුළුමුනින්ම ඔවුන් අතට ගන්න.

Ransomware විවිධ වර්ග දක්නට ලැබෙනවා ඒවායින් කිහිපයක් නම්

CryptoLocker

මෙම **Ransomware වර්ගය** පසුගිය දශක දෙකක පමණ කාලයක සිට පැවත එන පැරණිතම සයිබර් ප්‍රහාර වලින් එකකි. ක්‍රිප්ටෝ ලොකර් ශක්තිමත් සංකේතාංකන ඇල්ගොරිතම භාවිතා කරයි. එබැවින් මෙය Ransomware හි වඩාත්ම විනාශකාරී ආකාරයයි. කප්පම් මුදල නොගෙවා ක්‍රිප්ටෝ Ransomware ආසාදිත පරිගණකය සහ ලිපිගොනු විකේතනය කිරීම (ප්‍රතිෂ්ඨාපනය කිරීම - restore) බොහෝ විට කළ නොහැක.

Cerber

සර්බර් යනු වලාකුළු මත පදනම් වූ ඔෆිස් 365 (Office 365) භාවිතා කරන්නන් ඉලක්ක කරන තවත් Ransomware ප්‍රභේදයකි. ඔෆිස් 365 භාවිතා කරන්නන් මිලියන ගණනක් සර්බර් කප්පම් මෘදුකාංගය විසින් සිදු කරන ලද පුළුල් තතුබෑම් වෛරසයක් ගොදුරු වී ඇත.

Locky

ලොකී යනු තවත් කප්පම් මෘදුකාංග ප්‍රභේදයක් වන අතර එය වින්දිතයාගේ පරිගණකය අගුළු දමා කප්පම් මුදලක් ගෙවන තුරු ඒවා භාවිතා කිරීමෙන් වලක්වනු ඇත. එය සාමාන්‍යයෙන් ව්‍යාප්ත වන්නේ ඉන්වොයිසියක් ලෙස වෙස්වළාගත් ඊමේල් පණිවිඩයක් හරහා ය.පරිශීලකයෙකු ඊමේල් ඇමුණුම විවෘත කළ විට, ඉන්වොයිසිය ස්වයංක්‍රීයව මකා දැමෙන අතර, ගොදුරට ලේඛනය කියවීමට මැක්‍රෝස් (macro) සක්‍රීය කිරීමට යොමු කෙරේ. වින්දිතයා මැක්‍රෝස් සක්‍රීය කළ විට, ලොකි AES සංකේතනය භාවිතයෙන් ගොනු වර්ග කිහිපයක් සංකේතනය කිරීමට පටන් ගනී.

Jigsaw

ජිග්සෝ යනු කප්පම් ගෙවන තෙක් සංකේතාත්මක ලිපිගොනු සංකේතනය කර ක්‍රමානුකූලව මකාදමන Ransomware වර්ගයේ වඩාත් විනාශකාරී වර්ගයකි. එය පැය 72 ක සලකුණ තෙක් පැයකට වරක් ලිපිගොනු මකා දැමීමට පටන් ගනී.

DoubleLocker

ලගදී අපිට අහන්න ලැබෙන අලුත්ම Ransomware එක තමයි මේ DoubleLocker කියන්නේ. මෙය සම්පූර්නයෙන්ම android උපාංග ඉලක්ක කරපු Ransomware එකක්.

Ransomware ප්‍රහාර වැළැක්වීම සඳහා ගත යුතු පියවර

1. Ransomware යනු ඔබේ පරිගණකයට සහ ඔබේ දත්ත වලට බරපතල තර්ජනයකි. ආරක්ෂිත පරිගණක පුරුදු පුහුණු වීමෙන් සහ යාවත්කාලීන ආරක්ෂක මෘදුකාංග භාවිතා කිරීමෙන් ඔබට කප්පම් මෘදුකාංග වලින් ආරක්ෂා විය හැකිය. සුපරීක්ෂාකාරීව සිටීමෙන් සහ විශ්වාසදායක ආරක්ෂක මෘදුකාංග ස්ථාපනය කිරීමෙන් එය වළක්වා ගත හැක.
2. ඔබගේ දත්ත වලට ප්‍රවේශය නැවත ලබා ගැනීමේ වේගවත්ම ක්‍රමය උපස්ථයකින් ඔබගේ ගොනු ප්‍රතිස්ථාපනය කිරීමයි.
3. විශ්වාස කළ නොහැකි ඊමේල් ඇමුණුම් විවෘත නොකරන්න.
   විද්‍යුත් තැපෑලකට, ඉල්ලීමක් නොකළ දුරකථන ඇමතුමකට, කෙටි පණිවිඩයකට හෝ ක්ෂණික පණිවිඩයකට පිළිතුරු දෙන විට පුද්ගලික තොරතුරු ලබා නොදෙන්න.
   පිළිගත් ප්‍රති-වයිරස මෘදුකාංගයක් (antivirus software) සහ ෆයර්වෝලයක් (Firewall) භාවිතා කරන්න. ශක්තිමත් ෆයර්වෝලයක්(Firewall) පවත්වා ගැනීම සහ ඔබගේ ආරක්ෂක මෘදුකාංග (Software) යාවත්කාලීනව තබා ගැනීම ඉතා වැදගත්ය.
4. ඊ-තැපැල් සේවාදායකයන්ගේ ඊ-තැපැල් පණිවිඩ අන්තර්ගතය පරීක්ෂා කිරීමට පරිලෝකනය සහ පෙරීම (scanning and filtering) භාවිතා කරන්න. දන්නා තර්ජන සඳහා අභ්‍යන්තර විද්‍යුත් තැපැල් පරිලෝකනය කළ යුතු අතර තර්ජනයක් විය හැකි ඕනෑම ඇමුණුම් වර්ග අවහිර කළ යුතුය.
5. ඔබේ මෘදුකාංග සහ මෙහෙයුම් පද්ධතිය යාවත්කාලීනව තබා ගන්න.
   සියලුම පද්ධති සහ මෘදුකාංග යාවත්කාලීනව පවතින බවට වග බලා ගන්න. අනිෂ්ට මෘදුකාංග පැතිරවීම සඳහා සම්මුති විරහිත වෙබ් අඩවි වල සත්කාරක සූරාකෑම බහුලව භාවිතා වේ.
6. Ransomware සඳහා කප්පම් ගෙවීමෙන් වලකින්න. එය මෙම ප්‍රහාරකයින් දිරිමත් කිරීම සහ අරමුදල් සැපයීම පමණි. කප්පම් මුදල ගෙවනු ලැබුවද, ඔබේ ලිපිගොනු වෙත නැවත ප්‍රවේශය ලබා ගත හැකි බවට සහතිකයක් නොමැත.

මුලිකවම ආයෙත් පාරක් කියන්න පුළුවන් දේ තමයි මේ Ransomware අපේ උපාංග වලට ඇතුල් වෙන්නේ අපේ ක්‍රියාකාරකම් හරහාම තමයි කියන එක.

අන්තර්ජාලය ඵලදායී ලෙස භාවිතයට හුරු වෙමු

තොරතුරු හා සන්නිවේදන තාක්ෂණයේ වැදගත් අංශයක් වන, වර්තමානයේ නැතිවම බැරි, පවුලේ අය, යහළු යෙහෙළියන් හැරුණු විට අපට ආසන්නයේම සිටින්නේ අපි කවුරුත් හොඳින්ම දන්නා අන්තර්ජාලයයි. මුළු විශ්වයේම තොරතුරු අප අතට ගෙන දෙන්නා වූ මේ අන්තර්ජාලය අපට සිතාගන්නටවත් බැරි තරම් බලවත් වේ. එදිනෙදා ජීවිතයේ අපට අවශ්‍ය සියලුම සේවා සැපයුම් මධ්‍යස්ථානයක් ලෙස අන්තර්ජාලය ප්‍රමුඛව සිටී.උදාහරණ :-ජංගම බැංකුකරණය (mobile banking),

මාර්ගගත අධ්‍යාපනය (online learning)

තවද මේ දිනවල සුලභ ඉගෙනුම් ක්‍රියාවලියක් වන online learning සඳහා zoom හා cisco webex යනාදි යෙදවුම් ක්‍රමලේඛ (apps) හරහා ඉගෙනුම් කටයුතු කරගත හැක.

තවද විකිපීඩියා වෙබ්අඩවිය හරහා අපට වැදගත් වන බොහෝ තොරතුරු අධ්‍යනය කර හැක.

සන්නිවේදන පහසුකම් (communicating)

අද වන විට අන්තර්ජාල පහසුකම් මත ක්‍රියා කරන බොහෝ සමාජජාල වෙබ් අඩවි මගින් සන්නිවේදනය පහසු කිරීමත්, ලොව වටා ඕනෑම අය සමග සබඳතා පැවැත්වීමටත් ඉඩ පහසුකම් සපයයි.

උදාහරණ :-

Facebook Whatsapp Viber Messenger

මාර්ගගත සාප්පු (online shopping)

ප්‍රවාහන පහසුකම් (transport service)

Uber, Pickme හරහා ගමනාගමන පහසුකම් සපයා ගත හැක.

මේ ඇතුළුව තවත් බොහෝ දේ අන්තර්ජාලය මගින් ඉටුවේ.

මෙවැනි බොහෝ පහසුකම් සපයන අන්තර්ජාලය හරහා අපරාධ කිරීමට තැත් කරන පිරිස් ද වෙති.

අනවසරයෙන් පරිගණක දත්ත එක් රැස් කිරීම, පරිගණක වලට වයිරස් ඇතුළු කර පරිගණක ක්‍රියාවලි පාලනය කිරීම හා සයිබර් ප්‍රහාර එල්ල කිරීම, දත්ත විකෘති කිරීම යනාදිය මෙවැනි අපරාධකරුවන් විසින් කරනු ලබයි. එවැනි තර්ජන වලින් ආරක්ෂා වීමට ඔවුන්ගේ ක්‍රියාකලාපයට වාසිදායක වන තත්වයන් ඇති නොකිරීමට අවදානයෙන් සිටීම අප සතු වගකීමකි.

අන්තර්ජාලය සැබවින්ම යහපත් ද අයහපත් ද යන වග තීරණය වන්නේ එය භාවිතා කරන්නාගේ අරමුණ හා ආකල්ප මතය. එහි යහපත් හා අයහපත් යන දෙ අංශයම පවතින බැවින් තමාගේ යහපතට හේතු වන දේ පමණක් තොරා ගෙන එදිනෙදා අවශ්‍යතාවන් ඉටු කර ගැනීම අපේ යුතු කමයි.

දුල්මි වගීෂා
10 ශ්‍රේණිය
ක්‍රිස්තුරාජ විදුහල - පන්නිපිටිය

කාන්තා හා ළමා සංවර්ධන, පෙර පාසල් හා ප්‍රාථමික අධ්‍යාපන,
පාසල් යටිතල පහසුකම් හා අධ්‍යාපන සේවා රාජ්‍ය අමාත්‍යාංශය
පස්වන මහල, දෙවන අදියර, සෙත්සිරිපාය,
බත්තරමුල්ල.
දුරකථන :- 0112186176
ෆැක්ස්:- 0112186431
ඊ මේල් :- it@childwomenmin.gov.lk
වෙබ් අඩවිය :- www.childwomenmin.gov.lk

රජයේ මුද්‍රණ දෙපාර්තමේන්තුව