# පරිගණක වයිරස හඳුනාගනිමු

## ■ පරිගණක වයිරසයක් යනු කුමක්ද ?

පරිගණක වයිරසයක් යනු, එක් පරිගණකයක සිට තවත් පරිගණකයකට පැතිර යා හැකි, පරිගණකයේ ක්‍රියාකාරිත්වයට බලපෑම් කළ හැකි ස්වයං ප්‍රතිගුණනය විය හැකි කුඩා පරිගණක වැඩසටහන් වේ. මෙවැනි වයිරසයකට ඔබේ පරිගණකයේ ඇති වැදගත් දත්ත වෙනස් කිරීමට හෝ විනාශ කිරීමට හැක.බොහො මයක් වයිරස අපගේ පරිගණක තුලට පැමිණෙන්නේ ක්‍රියාත්මක කළ හැකි ගොනු (Executable files) සමඟ ඇමුණුමක් ලෙසිනි. එබැවින් අප මෙම ගොනු ක්‍රියාත්මක කළ විට හෝ විවෘත කළ විට වයිරසවල ක්‍රියාකාරිත්වය ආරම්භ විය හැක

## ■ බහුලව පවතින වයිරස ආකාර

පරිගණක වයිරස, ස්පයිවෙයා(ර්), ඇඩ්වෙයා(ර්), ට්‍රෝජන් හෝර්ස්, වෝ(ර්)ම් යනාදී සියල්ල මැල්වෙයා(ර්) ආකාර වේ. එනම් ඔබගේ පරිගණකයට හානි පැමිණවිය හැකි, ඔබගේ  අනුදැනුමකින් තොරව දත්ත සොරාගන්නා හෝ විනාශ කරන  ඕනෑම වැඩසටහනක් මැල්වෙයා(ර්) ආකාරයකි.

ස්පයිවෙයා(ර්) - වඩාත් බහුල වයිරස ආකාරයකි. යමෙකුගේ පරිගණක ආශ්‍රිත ක්‍රියාකාරකම් පිළිබඳව ඔහුගේ අනුදැනුමකින් තොරව දත්ත රැස්කරයි.

ඇඩ්වෙයා(ර්) - ඔබගේ  අනුදැනුමකින් තොරව පරිගණකයේ ස්ථාපනය වී තිරය මත වෙළඳ දැන්වීම් ප්‍රදර්ශනය කිරීම සිදු කරයි. මේවා මඟින් යමෙකුගේ අන්තර්ජාලය භාවිතා කිරීමේ පුරුදු යනාදිය පිළිබඳව දත්ත රැස්කරයි.

ට්‍රෝජන් හෝර්ස් - මෙම වයිරසවලට ස්වයං ප්‍රතිගුණනය වීමේ හැකියාවක් නැත. මේවා ප්‍රයෝජනවත් වැඩසටහන් ලෙස පැමිණෙන හානිකර වැඩසටහන් වේ. මෙමඟින් ඔබගේ පරිගණකයෙන් පුද්ගලික තොරතුරු සොරකම් කිරීම, නිශ්චිත දිනයකදී හෝ කාලයකදී පරිගණකයට හානි පැමිණවීම ආදිය සිදුකෙරේ.

වෝ(ර්)ම් - මේවා සාම්ප්‍රදායික වයිරස ආකාරවලින් වෙනස්ය. මේවා එක් පරිගණකයක සිට තවත් පරිගණකයකට පැතිර යාමේදී කිසිදු මිනිස් ක්‍රියාකාරිත්වයක බලපෑමකින් තොරව එය සිදු වේ. ඔබගේ පරිගණකය තුලදී ස්වයං ප්‍රතිගුණනය වීමේ හැකියාවක් ඇත. උදාහරණයක් ලෙසට  මේවා ඔබගේ පරිගණකය තුලදී පිටපත් සිය දහස් ගණනක් ඉබේම ඇති වී ඔබගේ ඉ-තැපැල් ලිපින පොතෙහි සියලුම ලිපිනයන්ට යැවිය හැක. ඉන්පසු එම  ලිපිනයන්හිදීද මෙම ක්‍රියාවලිය මෙලෙසම සිදු වේ. එබැවින් මෙම වෝ(ර්)ම් ආකාර වයිරසවලට පරිගණක ජාලයන් හරහා ස්වයංක්‍රීයව පැතිරීමට හැක.

## ■ ඔබේ පරිගණකයට වයිරස ඇතුලු වන්නේ  කෙසේද ?

පරිගණක වයිරස, ඉ-තැපැල් පණිවුඩ සහ ඉ-තැපැල් ඇමුණුම් මඟින් පහසුවෙන්ම පැතිරිය හැකිය. ඉ-තැපැල මඟින් පැතිරෙන වයිරස බොහොමයක් ආකර්ෂණීය පින්තූර, සුබ පැතුම්පත්, සිත් ඇදගන්නා ශ්‍රව්‍ය දෘශ්‍යගොනු යනාදිය ලෙසින් වෙස්වළාගෙන ඔබ වෙත පැමිණිය හැක.එම නිසා මෙලෙස ඔබ වෙත  එන අනපේක්ෂිත හෝ කා විසින් එවන ලද දැයි නොදන්නා ඉ-තැපැල් ඇමුණුම් විවෘත නොකර සිටීම නුවණට හුරුය. එපමණක්ද නොව, ඔබ අන්තර්ජාලයෙන් බාගත  කිරීම් සිදුකරන විටද මෙම පරිගණක වයිරස ඔබගේ පරිගණකයට ඇතුලු විය හැක.

## පරිගණක වයිරස් ආසාදනයන්හි ලක්ෂණ

■ පරිගණකය සාමාන්‍ය තත්වයට වඩා අඩු වේගයකින්  ක්‍රියා කිරීම.

■ පරිගණකය නිරතුරුවම ස්වයංක්‍රීයව නැවත පණ  ගැන්වීම හා අසාමාන්‍ය ලෙස ක්‍රියා කිරීම.

■ පරිගණකයේ ඇති වැඩසටහන් නිසියාකාරව ක්‍රියා  නොකිරීම.

■ අසාමාන්‍ය වැරදි පණිවුඩ දිස්වීම.

■ ඔබ විසින් නිර්මාණය නොකරන ලද නව අයිකන පරිගණක තිරය මත දිස්වීම.

■ ඔබ විසින් පරිගණකයෙන් ඉවත් නොකරන ලද වැඩ සටහන් පරිගණකයෙන් ඉවත්ව ඇති ලෙස දිස්වීම.

## ඔබගේ පරිගණකය වයිරස ආක්‍රමණයන්ගෙන් වළකා ගන්නේ කෙසේද ?

■ අන්තර්ජාලය සඳහා ෆයර්වෝල් භාවිතා කිරීම.

■ පරිගණකයේ මෙහෙයුම් පද්ධතිය හා භාවිතා කරන මෘදුකාංග යාවත්කාලීන කිරීම.

■ යාවත්කාලීන කරන ලද විශ්වාසදායී ප්‍රති වයිරස මෘදුකාංගයක් භාවිතා කිරීම.

■ නොදන්නා ප්‍රභවයන්ගෙන් එන ඉ-තැපැල් ඇමුණුම් විවෘත නොකිරීම.

■ දන්නා ප්‍රභවයකින් වුවද, අන්තර්ගතය නොදන්නා ඉ-තැපැල් ඇමුණුම් විවෘත නොකිරීම.

■ ඉ-තැපැල් ඇමුණුම් විවෘත කිරීමට පෙර වයිරස පරීක්ෂාවක් සිදු කිරීම.

■ සැකසහත 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.

## ෆයර්වෝලයක් යනු කුමක්ද ?

ෆයර්වෝලයක් යනු, වෙනත් පිටස්තර පරිගණක ජාලයකින් අපගේ පරිගණක ජාලයක් වෙත පැමිණෙන දත්ත ඇතුලු වීමට අවසර ලබාදෙන හෝ ඇතුලු වීම වළක්වන මෘදුකාංගයක් හෝ දෘඩාංගයකි. උදාහරණයක් ලෙස, යම්කිසි ආයතනයක් තුළ ඇති පරිගණක ජාලයක් මගින් අන්තර්ජාලයට ප්‍රවේශ වීමේදී පිටස්තර පුද්ගලයින් විසින් අන්තර්ජාලය හරහා ආයතනික දත්ත ලබාගැනීම වැළැක්වීමටත්, ආයතනය තුළට අන්තර්ජාලයෙන් පැමිණෙන දත්ත පාලනය කිරීමටත් ෆයර්වෝල් ස්ථාපනය කරනු ලැබේ.

මෙලෙසින්ම, අපගේ පුද්ගලික පරිගණකවලටද, ෆයර්වෝල් ස්ථාපනය කර ගැනීමෙන් පරිගණකයට අන්තර්ජාලයෙන් පැමිණිය හැකි වයිරස් උවදුරු වළකා ගත හැක. ෆයර්වෝල් මගින් එය හරහා යන එන සියලුම දත්ත පරීක්ෂා කර එම දත්තවල ගමනාන්තය සඳහා අවසර දීම තීරණය කෙරේ. මෙය සිදුකෙරෙන්නේ පරිශීලකයා විසින් සකසනු ලබන නීති පද්ධතියකට අනුවය.

## ප්‍රති වයිරස මෘදුකාංගයක් යනු කුමක්ද ?

ප්‍රති වයිරස මෘදුකාංගයක් යනු, පරිගණක වයිරස ඇතුලු සියලුම වෝ(ර්)ම්, ට්‍රෝජන් හෝර්ස් යනාදී හානිකර වැඩසටහන් අපගේ පරිගණක තුළට ඇතුලු වීම වැළැක්වීම, ඇතුලු වූ වයිරස අනාවරණය හා ඉවත් කිරීම උදෙසා නිපදවන ලද පරිගණක මෘදුකාංග වේ.

## ප්‍රති වයිරස මෘදුකාංගයක් ක්‍රියා කරන්නේ කෙසේද ?

ප්‍රති වයිරස මෘදුකාංගයක් වයිරස හඳුනාගැනීමේදී හා පරීක්ෂා කිරීමේදී ආකාර 2කට ක්‍රියා කරයි.

1 කලින් හඳුනාගන්නා ලද වයිරස තිබේදැයි පරීක්ෂා කිරීම. (Virus Dictionary Approach)

2 වයිරස බවට සැකකළ හැකි පරිගණක වැඩසටහන් තිබේදැයි පරීක්ෂා කිරීම. (Suspicious Behavior Approach)

## කලින් හඳුනාගන්නා ලද වයිරස තිබේදැයි පරීක්ෂා කිරීම.

මෙහිදී ප්‍රති වයිරස මෘදුකාංගය නිර්මාණය කරන විටදීම හඳුනාගෙන ඇති වයිරස ආකාර පිළිබඳ දත්ත ඇතුලත් දත්ත ගබඩාවක් භාවිතා කෙරේ. නව ගොනුවක් පිරික්සීමේදී එම ගොනුවේ හඳුනාගත් වයිරස තිබේදැයි පරීක්ෂා කර බලා එසේ නම් ගොනුව විනාශ කිරීම හෝ නිරෝධායනය කිරීම (Move to quarantine) හෝ ගොනුව ප්‍රතිසංස්කරණය කිරීම සිදු කෙරේ. මෙමඟින් එම වයිරසය තවදුරටත් පැතිර යාම වැළැකේ. නව වයිරස සොයාගැනීමත් සමගම ප්‍රති වයිරස මෘදුකාංග දත්ත ගබඩාද යාවත්කාලීන වන බැවින් අපගේ පරිගණකවල ස්ථාපනය කරන ලද ප්‍රති වයිරස මෘදුකාංග නිතර යාවත්කාලීන කිරීමෙන් නව වයිරසයන්ගේ ආක්‍රමණයන්ට ලක්වීමේ අවදානම අඩුකරගත හැක. මේවා ස්ථාපනය කළ පසු අපගේ පරිගණකය පණගැන්වීමේදී වයිරස පරීක්ෂා වැඩටහනද ක්‍රියාත්මක

## වයිරස බවට සැකකළ හැකි පරිගණක වැඩසටහන් තිබේදැයි පරීක්ෂා කිරීම.

මෙහිදී දන්නා වයිරස හඳුනාගැනීම වෙනුවට පරිගණකයේ සෑම ගොනුවක්ම, වැඩසටහනක්ම පරීක්ෂාවට ලක්කිරීමක් සිදුකෙරේ. නිදසුනක් ලෙස යම්කිසි වැඩසටහනක් මඟින් පරිගණකයේ ක්‍රියාත්මක කළ හැකි ගොනුවලට (Executable files) ලිවීමට උත්සාහ දරන බව දුටුවහොත් එම වැඩසටහන සැකසහිත වැඩසටහනක් ලෙස ඔබට අනතුරු ඇඟවීමක් සිදු කෙරේ. මෙහිදී පරිශීලකයාට අනතුරු ඇඟවීම අනුව වැඩසටහන තවදුරටත් ධාවනය කරන්නේද පරිගණකයෙන් ඉවත් කරනනේද යන්න තීරණය කළ හැක. එමනිසා මෙම තාක්ෂණය භාවිතා කරන මෘදුකාංග මඟින් තවමත් හඳුනානොගත් වයිරසයන්ගේ ආක්‍රමණයන්ට ලක්වීමේ අවදානම අඩුකරගත හැක.

## ප්‍රති වයිරස මෘදුකාංගයක් තෝරා ගැනීමේදී සැලකිලිමත් විය යුතු කරුණු

අද ලෝකයේ ප්‍රති වයිරස මෘදුකාංග නිපදවන්නන් බොහොමයකි. මේවායින් ඔබගේ පරිගණකයට ගැලපෙන මෘදුකාංගය තෝරාගැනීම පරිශීලකයාගේ අවශ්‍යතා අනුව වෙනස් වේ. නමුත් ඕනෑම ප්‍රති වයිරස මෘදුකාංගයක් සඳහා ප්‍රධානව සලකා බැලිය යුතු කරුණු වන්නේ,

- ස්වයංක්‍රීයව යාවත්කාලීන වීමේ හැකියාව.
- මෘදුකාංග නිපදවන්නා ක්‍රමානුකූලව යාවත්කාලීන වයිරස විග්‍රහයක් සපයන්නේද යන බව.
- මෘදුකාංගයට ඔබගේ ඉ-තැපැල් වැඩසටහන සමග එක්ව ක්‍රියා කළ හැකිද යන්න.
- වයිරස පරීක්ෂාවන් ස්වයංක්‍රීයව සිදුකළ හැකිවේද යන්න.
- මෘදුකාංග නිපදවන්නා විසින්, අලුතෙන් සොයාගන්නා ලද වයිරස පිළිබඳ නිවැරදි හා කාලෝචිත තොරතුරු ප්‍රකාශයට පත් කරන්නේද යන බව.

## අද ලෝකයේ බහුලවම භාවිතා වන ප්‍රති වයිරස මෘදුකාංග

| | |
|---|---|
| 1 Kaspersky lab | 6 Trend Micro |
| 2 McAfee | 7 F-Secure |
| 3 Symantec | 8 Sophos |
| 4 Avast | 9 Bitdefender |
| 5 ESET | 10 Microsoft Security Essentials |

ඔබගේ ගැටලු පහත ක්‍රමයන් මගින් අපට දන්වන්න.

https://techcert.lk/en/report-form
දුරකථන - +94 11 4 462 562
ඊ-තැපැල් - help@techcert.lk

මෙම ලිපිය ලක් වසම් අධිකාරිය සහ අන්තර්ජාල සමාජයේ ශ්‍රී ලාංකීය ශාඛාව එක්ව සකසන ලද්දකි. වැඩි විස්තර සඳහා පිවිසෙන්න. http://nic.lk/index.php/training-materials.



Sri Lanka Chapter
HELPING YOU SECURE YOUR INFORMATION ASSETS