සයිබර් සුරැකුම

හෙට දිනන පරපුරේ සයිබර් ආරක්ෂාවට අත්පොත

හිතවතී වෙතිනි

සයිබර් සුරැකුම

හිතවතී වෙතිනි

සයිබර් සුරැකුම

හිතවතී වෙනිති

අගෝස්තු 2021

ISBN 978-624-5622-00-9

කංචුක නිර්මාණය : පුෂ්පානන්ද ඒකනායක

චිත්‍ර : ධනංජා සුබසිංහ

තොරතුරු සැකසුම : තඹරු විජේසේකර

මෙම පොත ප්‍රකාශයට පත්කලේ නිර්මාණශීලී පොදු බලපත්‍රය (Creative Commons License) යටතේ ශ්‍රී ලංකා තොරතුරු හා සන්නිවේදන තාක්ෂණ නියෝජිතායතනය (ICTA) වීසින් නිකුත් කරන ලද "AdBhashitha" (යුනිකෝඩ්) අකුරු භාවිතයෙනි.

ප්‍රකාශනය

ලංකා වසම් ලේඛකාධිකාරිය
බර්නාඩ් ව්‍යාපාරික උද්‍යානය,
106, දුටුගැමුණු වීදිය, දෙහිවල.

දුරකථනය : (011) 421-6062
ඉ-මේල් : help@hithawathi.lk
වෙබ් : www.hithawathi.lk

අන්තර්ජාලය අද අපට නැතිවම බැරි දෙයක් වෙලා තිබෙනවා. අපේ පෞද්ගලික කටයුතු, රාජකාරි කටයුතු මෙන්ම අධ්‍යාපනික කටයුතු අපි දැන් කරන්නෙ පරිගණකයෙන් නැත්නම් ෆෝන් එකෙන්. අපි මින් පෙර නොසිතූ පරිදි අපගේ කටයුතු බොහොමයක්ම ඔන්ලයින් කළ හැකි බව දැන් ඔප්පු වෙලා.

අන්තර්ජාලයේ යහපත් දෑ බොහොමයක් තිබුනත් එහි අයහපත් පැත්තකුත් තියනවා. එහෙ මෙහෙ නොබලා මහපාර හරහා දුවන එක අනතුරුදායකයි. ඒ වගේම, නොසැලකිලිමත්ව අන්තර්ජාලයේ සැරිසැරීමත් අනතුරුදායකයි. එම අනතුරු පිළිබඳ හොඳින් දැනුවත් වී, කළ යුතු නොකළ යුතු දෑ පිළිබඳව අවබෝධයෙන් සිටීම පාසල් දරුවන්ට විශේෂයෙන් වැදගත් වෙනවා. අද දවසේ, අපේ ආරක්ෂාව රැකගෙන, අන්තර්ජාලයෙන් වඩා හොඳ ප්‍රයෝජනයක් ලබා ගන්නේ එහෙමයි.

හිතවතී ව්‍යාපෘතිය ඒ සඳහා ඉතා වටිනා උත්සාහයක් මේ පොත් පිංචෙන් ඉදිරිපත් කරනවා.

කාන්තාවන්ට, තරුණියන්ට, යෞවනයන්ට හා දරු දැරියන්ට අන්තර්ජාලය සහ එහි සේවා භාවිත කිරීමේදී සිදු වන අපහසුතා, වැරදි යොමු කිරීම්, වැරදි හා අනවශ්‍ය බලපෑම් ආදිය පිළිබඳ ඔබ සමග කතා කරන්න හා ඔබව දැනුවත් කරන්න හිතවතී ඉන්නවා. එවැනි අවස්ථා වලදී කළ යුතු දෑ මෙන්ම එවන් අනතුරු වළක්වාගත හැකි අයුරු හිතවතී ඔබට කියා දෙනවා. හිතවතී, ලංකා වසම් ලේඛකාධිකාරිය (LK Domain Registry) මගින් සිදු කරන ව්‍යාපෘතියක්.

මහාචාර්ය ගිහාන් ඩයස්

හිතවතී ගැන...

අන්තර්ජාලය භාවිතයේදී හමුවන විවිධ ආකාරයේ පුද්ගලයන් සහ ක්‍රියාකාරකම් නිසා ඇතිවන ගැටලුවලට මුහුණ දෙන්නටත් ඒ පිළිබඳ නිවැරදි අවබෝධය සහ ඒවායින් ආරක්ෂා වී සිටීම සඳහා වන මග පෙන්වීමත් ජනතාවට ලබාදීම හිතවතී ව්‍යාපෘතියේ මූලික අරමුණුවේ. නොමිලයේ ලබාදෙන සේවාවක් වන "හිතවතී" උපකාරක සේවය ලංකා වසම් ලේඛකාධිකාරියේ (LK Domain Registry) පූර්ණ අනුග්‍රහය සහිතව වසර ගණනාවක් මුළුල්ලේ ශ්‍රී ලාංකිකයන් රැසකට සෙත සලසමින් මෙම ක්‍රියාවලින්හි සක්‍රියව නිරතව සිටී. මීට අමතරව මනා සේවාවක් ලබාදීම සඳහා රාජ්‍ය, රාජ්‍ය නොවන සහ ජාත්‍යන්තර සංවිධාන වලින්ද සහයෝගය ලබා ගනිමින් හිතවතී ව්‍යාපෘතිය ක්‍රියාත්මක වේ.

පිදුම

ඔබේ ළබැඳි හිතවතියගෙන්

සියලුම දූ දරුවන්ට සෙනෙහසින්

පටුන

හැඳින්වීම i

1. අපේ තොරතුරු හරිම වැදගත් 1

2. සයිබර් ප්‍රහාරවලට උපකාර නොකරමු 7

3. උපාංගවල ආරක්‍ෂාව සුළුකොට නොතකමු 12

4. අන්තර්ජාල වංචාවන්ට හසු නොවෙමු 16

5. සමාජ ජාල දැනගෙන පාවිච්චි කරමු 20

6. සයිබර් හිරිහැරවලට බිය වෙන්න එපා 24

7. නීති පද්ධතිය ඔබ වෙනුවෙන් සූදානම් 28

8. මානසික ගැටළු වලට මුල පුරන සයිබර් අපරාධ 32

9. තාක්ෂණය කියන්නේ හරිම වටිනා දෙයක් 36

10. සයිබර් හිරිහැරයකට මුහුණ දුන්නොත් අමතන්න 40

පාරිභාෂික වචන මාලාව 43

යොමුව 46

ඔබේ දැනුම උරගා බලන්න 47

හැඳින්වීම

හිතවතී සංවිධානය විසින් ගෙන එනු ලබන මෙම අත්පොත පාසල් දරුවන්ට මෙන්ම අන්තර්ජාල ආධුනිකයන්ට සයිබර් ආරක්ෂාව පිළිබඳව එනම්, අන්තර්ජාලයේ සැරිසැරීමට පෙර එහි ඇති අනතුරු සම්බන්ධව දැන සිටිය යුතු මූලික කරුණු ආවරණය කරනු ලබයි.

දරුවන්ට වඩාත් තේරුම් ගත හැකි වාග් ශෛලියක්, රූප, දෙබස්, සහ තාක්ෂණික දැනුම සරලව මෙහි ඉදිරිපත් කෙරෙනු ඇති අතර, ඕනෑම වයසක හා තාක්ෂණික දැනුමක් නොමැති කෙනෙකුට වුව අවබෝධ කරගත හැකි සේ පමණ නොඉක්මවූ සිංහල පාරිභාෂික වදන් භාවිතයකින් තොරව, සාමාන්‍ය වහරේදී එන යෙදුම් භාවිතයෙන් දැනුම ගෙන එනු ඇත.

යල්පැනගිය තොරතුරු වෙනුවට මෙම ග්‍රන්ථය සම්පාදනය කරන අවස්ථාව වන තෙක් නවීනතම තොරතුරු මෙහි අන්තර්ගත කර තිබේ. එසේම, සමාජ ජාල ඇතුළු අන්තර්ජාලය යනු දරුවන්ට නුසුදුසු තැනක් නොව, අවබෝධයෙන් භාවිතා කළහොත් බොහෝ වාසි ලැබිය හැකි එකක් ය යන මතය සමාජ ගත කිරීමත්, දරුවන් පරිගණක/දුරකථන භාවිතය විනාශකාරී දෙයකැයි යන දුර්මතය බිඳලීමත් හරහා පරිගණක සාක්ෂරතාවයෙන් සපිරි දරු පරපුරක් දැයට දායාද කිරීමට මින් උත්සාහ ගැනෙනු ඇත.

1. අපේ තොරතුරු හරිම වැදගත්

මෙම කොටසින් ආවරණය වන කරුණු:

- තොරතුරු යනු ඔබේ වත්කමක් බව
- පෞද්ගලිකත්ව ප්‍රතිපත්ති (Privacy Policy) කියවිය යුතු බව

දත්ත සුරක්ෂිතතා (Data Security) ක්ෂේත්‍රය නිර්වචනය කරන ආකාරයට, අපේ දත්ත සහ ඒවායෙන් ගොඩනැගෙන තොරතුරු කියන්නේ වත්කමක්. ඒ කියන්නේ, එයට වටිනාකමක් තිබෙනවා. ඉතින් ඒවා අපි පණ වගේ ආරක්ෂා කරගන්න ඕනි.

දත්තවලට මූල්‍යමය වටිනාකමක් තිබෙනවා

පරිගණක මෘදුකාංග, අන්තර්ජාලය ඇතුළු සෑම සේවාවක්ම අපේ තොරතුරු (දුරකථන අංකය, උපන් දිනය, ඡායාරූප, අදහස්, ඇතැම්විට බැංකු තොරතුරු) රැස් කරගන්න බලාගෙනයි ඉන්නේ.

වෙබ් අඩවියක් හෝ සේවාවක් හදන්න වගේම නඩත්තු කරන්න ලොකු පිරිසක් මහන්සි වෙනවා. ඔවුන්ට වැටුප් ගෙවන්න, ආයතනික වියදම් පියවා ගන්න වගේම, නිෂ්පාදනය සම්බන්ධ වෙළඳ දැන්වීම් පළ කරන්නත් වෙනවා.

ඉතින් මේ තරම් වියදමක් එක්ක එයාලා ඒවා නොමිලේ දෙන්නේ කොහොමද?

ඔවුන් රැස් කරන දත්ත අතර අපි කැමති/අකමැති දේවල්, බලන්න කැමති වීඩියෝ/ඡායාරූප වර්ග, search කරන දේවල් යනාදිය ඇතුලත් වෙනවා. අපිට නොමිලේ දෙන සේවාවට අපි ගෙවීම කරන්නේ අපේ පෞද්ගලික දත්ත වලිනුයි.

ඔබට, පවුලේ අයට මෙන්ම රටටත් බලපානවා

මගේ තොරතුරු ගත්තාම මට මොකද?

මම ඇමරිකාවේ ජනාධිපති නෙවෙයිනේ

ගූගල් මැප්ස් වගේ සේවාවන් GPS දත්ත යොදාගෙන අපි යා යුතු පාර සොයාගන්න උදව් කරනවා වගේම, ඒ සමාගමටත් ඔබ සිටින ස්ථානය දැක ගත හැකි වෙනවා.

මේකෙන් සිදුවන තරක මොකක්ද?

හිතන්න.. කිසියම් ත්‍රස්තවාදී සංවිධානයක් මුළු ලංකාවෙම GPS දත්ත ලබා ගත්තොත් ඔවුන්ට වැඩිම පිරිසක් එක්රැස්ව සිටින ස්ථාන දැනගෙන විශාල හානියක් කරන්නට හැකි වෙනවා.

ෆේස්බුක් මෙන්ම Truecaller වැනි ඇප් Install කරද්දී අපේ ෆෝන් එකේ save කර තිබෙන, අනෙක් අයගේ දුරකථන අංකත් ඔවුන්ට ලබා දෙන ලෙස දන්වනවා. ඇතැම්විට මේවා තෙවන පාර්ශවයකගේ අතටත් යන්න පුළුවන්.

ඉතින් ඒකෙන් ඔයා ගෙදර අයගේ, යාළුවන්ගේ ඇතුළු හැම කෙනෙක්ගේම දත්ත නොසැලකිලිමත්ව තෙවන පාර්ශවයකට ලබා දෙනවා.

දත්ත භාවිතා වෙන්නේ කොහොමද කියලා දැනුවත් වෙන්න

වෙබ් අඩවිවල, ඇප්ස්වල පෞද්ගලිකත්ව ප්‍රතිපත්ති (Privacy Policy) නමැති ලේඛනයක් දක්වනවා.

එහි ඔවුන් දත්ත භාවිතා කරන හැටි, ගබඩා කර තබා ගන්නා කාලය ඇතුළු විස්තර අඩංගු වෙනවා. එය කියවා සේවාවක් පාවිච්චි කරනවා ද නැද්ද කියා තීරණය කළ යුතු වෙනවා.

අපේ තොරතුරු රැක ගන්නේ කොහොමද?

ඔබේ දෙමව්පියන්ගේ අවසරයකින් තොරව සම්පූර්ණ නම, ලිපිනය, පාසලේ නම හෝ දුරකථන අංකය වැනි පුද්ගලික තොරතුරු කිසිම කෙනෙකුට ලබා දෙන්න එපා.

මතක තබා ගන්න, යමෙකු පෞද්ගලික තොරතුරු ඉල්ලූ පමණින් ඒවා දිය යුතු වන්නේ නැහැ. හොඳම දේ, එවන් සංවේදී තොරතුරු ලියා තැබීමෙන් හෝ ගබඩා කිරීමෙන් වැළකීමයි.

ඔයා Vlogs (YouTube Videos / TikTok) කරනවා නම්, නිවස අභ්‍යන්තරය, මුහුණ වැනි ඔයාගේ අනන්‍යතාව තහවුරු වන ආකාරයේ දර්ශන ඇතුලත් කරන්න එපා. පාවිච්චි නොකරන අවස්ථාවලදී ලැප්ටොප් කැමරාවත් ආවරණය කර තබන්න.

තොරතුරුවල ආරක්ෂාව ගැන වැඩි විස්තර දැනගන්න කැමති නම්, hithawathi.lk වෙබ් අඩවියේ ඇති සටහන බලන්න මේ QR Code එක ස්කෑන් කරන්න.
https://www.hithawathi.lk/si/help-center-si/cyber-security-tips-si/internet-safety-tips-for-children-and-teens-si/

අපි ආරක්ෂා වෙන්න ඕන කොහොමද?

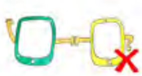
කියලා සචිනි එයාගේ IT ගුරුතුමියගෙන් ඇහුවා. ටීචර් ඒවා මේ විදියට ලැයිස්තු ගත කළා.

මුරපද රැකගන්න

ඔයාගේ මුරපදය ඔබේ දෙමාපියන් හැර වෙන කිසිවෙකු සමග කියන්න එපා. ඔබ පොදු පරිගණකයක් එහෙමත් නැත්නම් වෙනත් කෙනෙකුගේ පරිගණකයක් භාවිතා කරන විට, බ්‍රවුසරය close කිරීමට පෙර ඔබ ප්‍රවේශ වූ සියළුම ගිණුම්වලින් Log out වෙන්න.

ඡායාරූප පළ කරන්න එපා

දෙමාපියන්ගේ/භාරකරුවන්ගේ අවසරය ලබා නොගෙන ඡායාරූප හෝ වීඩියෝ ඉන්ටර්නෙට් එකේ දාන්න එපා. වෙනත් අය ඒවා අරගෙන ඔයාලාගේ ප්‍රොෆයිල් හදන්න, පේජ් වලින් share කරන්න ඉඩ තිබෙනවා.



සබැඳි මිතුරන් (Online Friends) භයානකයි

දෙමව්පියන්ගේ/භාරකරුවන්ගේ අවසරය නොමැතිව සබැඳි මිතුරෙකු හමුවීමට යන්න එපා. අවාසනාවකට, සමහර මිනිස්සු ව්‍යාජ සහ වංචනික විදියට පෙනී ඉන්නවා.

එයාලා ඔයාලාට උදව් කරන බව, දුකට පිහිට වෙන බව වැනි කතාවලින් සමීප වෙලා අපයෝජන වලට යොදා ගන්නවා.

අසත්‍ය පුවත් ගැන කල්පනාවෙන්

ඔයා අන්තර්ජාලයෙන් කියවන සෑම දෙයක්ම සත්‍ය නැහැ. පිළිගන්නට පෙර ඒවායේ ඇත්ත නැත්ත සොයා ගන්න.

"තේරුණා නේද?" කියා ටීචර් අහද්දී සචිනි හිස වනා "ඔව්" කිව්වා.

මුරපද භාවිතයේදී මේ දේවල් ගැන සැලකිලිමත් වෙන්න

මුරපදයක් කියන්නේ ගෙදර යතුර වගේ දෙයක්. ඔයාලා ඒක ගෙදරින් පිට වෙන කාටවත් දෙන්නේ නැහැ වගේම, පාස්වර්ඩ් එකත් බොහොම ආරක්ෂිතව තබා ගන්න ඕනේ.

විශේෂයෙන් ඉ-මේල් ගිණුමේ පාස්වර්ඩ් එක කොහේ හෝ ලියා තැබුවොත්, වෙනත් කෙනෙක්ගේ අතකට පත් වුණොත් එය භාවිතයෙන් ලියාපදිංචි කළ ෆේස්බුක්, ස්කයිප් වගේ ගිණුම් විශාල ප්‍රමාණයක් එක්වරම එයාලාට අයිති කරගන්න අවස්ථාව ලැබෙනවා.

හොඳ මුරපදයක් දාන්නේ මෙහෙමයි

ඉංග්‍රීසි සිම්පල් සහ කැපිටල් අකුරු මිශ්‍ර කරන්න.

අතරින් පතර ඉලක්කම් ඇතුලත් කරන්න.

අංක, සහ විශේෂ සලකුණු (උදා: ?, !, -, %) පාවිච්චි කරන්න.

උපන් දිනය, සමීප අයෙකුගේ නමක්, හැඳුනුම්පත් අංකය වගේ වෙනත් කෙනෙක්ට පහසුවෙන් සොයාගත හැකි දේවල් යොදන්න එපා.

හොඳ මුරපදයක් පහසුවෙන් සකසා ගන්න පහත වෙබ් අඩවි පාවිච්චි කරන්න පුළුවන්.

- https://passwordsgenerator.net
- https://www.lastpass.com/password-generator
- https://www.dashlane.com/features/password-generator
- https://1password.com/password-generator/
- https://www.avast.com/random-password-generator

> මතක හිටින වචනයක් දාගන්න අවශ්‍ය නම්, උදාහරණයක් ලෙස SriLanka1948 යන්න 1$ri9L@n4K@8 ලෙස සකසා ගත හැකියි. කිසිම වෙලාවක එකම මුරපදය එක ගිණුමකට වඩා පාවිච්චි කරන්න එපා.

ඊටත් වඩා හොඳ ක්‍රමයක් තමයි LastPass, DashLane, Keeper වැනි සේවාවක් පාවිච්චි කරන එක. එතකොට මතක තියාගන්න වෙන්නේ අදාල සේවාවේ ප්‍රධාන (master) පාස්වර්ඩ් එක විතරයි.

එවිට පිවිසෙන ගිණුම්වල පාස්වර්ඩ් ටයිප් කරන්නවත් අවශ්‍ය වෙන්නේ නැති නිසා අපේ කීබෝඩ් එකේ ටයිප් කරන දේවල් සොරාගන්නා කීලොගර් (Keylogger) වැනි සැහැසි මෘදුකාංගවලට පාස්වර්ඩ් සොරකම් කරන්න පුළුවන් වෙන්නෙත් නැහැ.

ෆෝන් ලොක් එකට නම්, ෆින්ගර්ප්‍රින්ට් හෝ FaceID ආරක්ෂාව දාගන්න එක පහසුයි. එනමුත්, ඔබ නිදා සිටින අවස්ථාවක වෙනත් කෙනෙක්ට ඔබේ ඇඟිල්ල තබා හෝ මුහුණ වෙත දුරකථනය යොමුකර අන්ලොක් කරගත හැකි වෙනවා. එනිසා මුරපදයක් යෙදීම සෑමවිටම ආරක්ෂිත ක්‍රමවේදයක්.

2. සයිබර් ප්‍රහාරවලට උපකාර නොකරමු

මෙම කොටසින් ආවරණය වන කරුණු:

- ලියාපදිංචි කළ මෘදුකාංග භාවිතයේ වැදගත්කම
- තමා නොදැනුවත්වම හැකර්වරුන්ගේ අතකොළු වන බව
- වෛරස වලින් ආරක්ෂා වන ආකාරය

චිරස්ථි- මට ලියුමක් ටයිප් කරගන්න ඔෆිස් දාගන්න ඕන. ඔයා ගාව ක්‍රැක් එකක් තියෙද?

ප්‍රබෝද- ක්‍රැක් කරපු සොෆ්ට්වේයා පාවිච්චි කරන එක නීති විරෝධියි. අනික ඒකෙන් කම්පියුටර් එකට වෛරස් එන්නත් පුළුවන්. මම ඔයාට OpenOffice දාලා දෙන්නම්.

පරිගණකයට මෙහෙයුම් පද්ධතිය, සහ මෘදුකාංග ස්ථාපනයේදී මුදලක් ගෙවන්නට සිදු වෙනවා. ඒක එසේ නොකර බොහෝ දෙනෙක් ක්‍රැක් කරපු මෘදුකාංග පාවිච්චි කරනවා. එතකොට අපි සයිබර් ප්‍රහාරයකට (botnet එකකට) උදව් දෙන කෙනෙක් බවට පත් වෙනවා. ඒ වගේම, පරිගණකයේ තිබෙන වටිනා දත්ත විනාශ කරන රැන්සම්වෙයා (Ransomware) වෛරසවලට ගොදුරු වෙන්නත් ඉඩ තියෙනවා.

ක්‍රැක් මෘදුකාංග සකසන හැකර්වරු ඒවා අපිට ආදරයට හදන්නේ නැහැ. ඔවුන් එම ටොරන්ට් (Torrents) සකසන්නේ ඔවුන්ගේ වාසියකුත් සපුරා ගන්නා අතරේයි.

වෛරස් ගාඩ් අක්‍රිය කරන්න එපා

ක්‍රැක් කළ මෘදුකාංගවල වෛරස තිබෙනවා. ඒ නිසා ඒවායේ ස්ථාපන පියවරවල වෛරස් ගාඩ් එක අක්‍රිය කරන ලෙසත් දක්වා තිබෙනවා. ඉතින් ඔබ මුදලක් ගෙවා වෛරස් ගාඩ් (Virus guard / Antivirus software) එකක් දාගෙන හිටියත්, දැන් ඔන්න කැමැත්තෙන්ම අපි වෛරස්වලට දොර හැර දෙනවා.

> එසේ පිවිසුණාට පස්සේ, ඔවුන්ට අපේ පරිගණකය පාවිච්චි කරමින් සයිබර් ප්‍රහාර (Cyber-attacks) දියත් කිරීමේ හැකියාව ලැබෙනවා.

ඊට අමතරව, අපේ ගොනු සියල්ලම ආකේතනය (Encrypt) කර, ඒවා නැවත ලබා දෙන්නට නම් මුදලක් ගෙවන්නැයි කියන රැන්සම්වෙයා වෛරස ද දැන් ශීඝ්‍රයෙන් පැතිර යනවා. ගැටළුව වන්නේ අපි ඒ මුදල ගෙවූවත් ආයෙත් වතාවක් ආකේතනය කරලා, නැවත නැවතත් කප්පම් ඉල්ලීමට එයාලාට හැකි වෙන එකයි.

රැන්සම්වෙයා වලින් ගැලවෙන හැටි ගැන hithawathi.lk වෙබ් අඩවියේ ඇති සටහන බලන්න මේ QR Code එක ස්කෑන් කරන්න.

https://www.hithawathi.lk/si/help-center-si/security-alerts-si/cyber-security-alert-si/

හැම විටම, ඔබ බාගත කරන්නේ කුමක්ද, එම මෘදුකාංග ස්ථාපනය කිරීමට අවශ්‍ය ද යන්න ගැන සැලකිලිමත් වෙන්න. ඇතැම් අවස්ථාවලදී වීඩියෝ හෝ චිත්‍රපට බාගත කරගැනීමේදී වීඩියෝ ෆයිල් මුවාවෙන් ද වෛරස, ඇඩ්වෙයා (Adware) පැමිණිය හැකියි. වෛරස් ගාඩ් එක නිතරම යාවත්කාලීන (Update) කර තබාගන්න.

වෛරසයක් හඳුනා ගන්නේ කොහොමද?

අනුරාධගේ පරිගණකය වෙනදාට වඩා වේගය අඩු වෙලා තිබෙන බව එයාට තේරුණා. පරිගණකය පණ ගැන්වෙන විටත්, මෘදුකාංග විවෘත කරද්දීත් වැඩි කාලයක් ගත වෙනවා වගේම, තිරය මත විවිධ පණිවිඩ දිස් වෙන්නටත් පටන් ගත්තා. මේ ගැන වැඩිදුර හොයාගන්න හිතපු එයා "reasons why a computer runs slow" ලෙස ගූග්ල් සර්ච් කළා.

එවිට හේතුව වශයෙන් අනුරාධ ට දකින්න ලැබුණේ පරිගණකයේ වේගය අඩු වෙන්නට වෛරසයක් පැමිණ තිබීමත් හේතුවක් වෙන්න පුළුවන් කියලායි. පහත දේවලුත් රෝග ලක්ෂණ ලෙස දකින්න පුළුවන් බව මීට අමතරව සඳහන් වුණා.

- පරිගණකය සාමාන්‍ය තත්වයට වඩා අඩු වේගයකින් ක්‍රියා කිරීම.
- පරිගණකය නිරතුරුවම ස්වයංක්‍රියව 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 වැඩසටහන් පරිගණකයෙන් ඉවත්ව ඇති ලෙස දිස්වීම.

පරිගණකය වෛරස ආක්‍රමණයන්ගෙන් වලක්වා ගන්නේ කොහොමද?

ෆයර්වෝල් භාවිතය	මෘදුකාංග යාවත්කාලීන කිරීම	ව්‍යාජ බලපත් ඇති මෘදුකාංග භාවිතයෙන් වැළකීම
යාවත්කාලීන කළ විශ්වාසදායි ප්‍රතිවෛරස මෘදුකාංග භාවිතය	විශ්වාසදායී ප්‍රතිවෛරස මෘදුකාංග භාවිතය	නොදන්නා ප්‍රභවයන් ගෙන් එන ඉ-තැපැල් ඇමුණුම් විවෘත නොකිරීම

නිදහස් හා විවෘත මෘදුකාංග පාවිච්චි කරන්න

සංවර්ධනය වෙමින් පවතින රටක් වශයෙන් අපිට හැම මෘදුකාංගයම මිලදී ගන්නට අපහසු බව සත්‍යයක්. ඒත්, ඉන් ක්‍රැක් කළ මෘදුකාංග භාවිතය කොහෙත්ම සාධාරණීකරණය වෙන්නේ නැහැ. ඒ වෙනුවට නොමිලේ ලබා දී ඇති මෘදුකාංගවලට යොමු වෙන්න පුළුවන්. පහත දැක්වෙන්නේ එවන් ආදේශක කිහිපයක්.

ගෙවා ලබා ගත යුතු මෘදුකාංග / වෙබ් සේවා / මෙහෙයුම් පද්ධති	නොමිලේ ලද හැකි ආදේශක
Microsoft Windows	Linux (Ubuntu, Linux Mint)
Microsoft Office	OpenOffice.org, LibreOffice
Adobe Photoshop	GIMP
Autodesk 3ds Max	Blender
Shopify	WordPress (WooCommerce)

3. උපාංගවල ආරක්ෂාව සුළුකොට නොතකමු

මෙම කොටසින් ආවරණය වන කරුණු:

- උපාංග අන්සතු වීමෙන් ඇති විය හැකි විපාක
- අස්ථානගත වීමකදී කළ යුතු දේ

ධනුෂ්කි එයාගේ ෆෝන් එකේ ඩිස්ප්ලේ එක වැඩ කරන්නේ නැති නිසා අලුත්වැඩියා කරන සේවා ස්ථානයකට ලබා දුන්නා. නැවත ගෙනාවාට පස්සේ එයාට නිතරම විවිධ නොදන්නා අංක වලින් ඇමතුම් ආවා. "නංගි දැන් ෆෝන් එක හරි ද?" "ඔයාගෙ ෆෝන් එකේ තිබුණු ෆොටෝස් හරිම ලස්සනයි" වැනි අනවශ්‍ය පණිවිඩ ඇයට ලැබෙන්නට පටන් ගත්තා. විවිධ ස්ථානවලට පැමිණ හමුවන ලෙසත්, එසේ නොකළහොත් ඇගේ ඡායාරූප අන්තර්ජාලයේ පළ කරන බවට තර්ජනය කිරීම් ද ඒ අතර තිබුණා.

නොදන්නා අයට උපාංග දෙන්නේ කල්පනාවෙන්

> මුරපද යෙදුවත් වෙනත් ක්‍රම වලින් හාඩ් ඩිස්කවල ඇති දෑ බැලිය හැකියි

ඔබේ ෆෝන් එක හෝ ලැප්ටොප් එක වෙන කෙනෙක්ට දෙන්නට සිදුවුණොත්, එහි තිබෙන සියලුම පෞද්ගලික දත්ත backup කරගෙන, උපාංගයෙන් මකා දමන්න. ෆේස්බුක්, ජීමේල් ආදියෙන් logout වෙන්න.

ෆෝන් එකේ ඩිස්ප්ලේ එක අලුත්වැඩියා කිරීමට එය අන්ලොක් කිරීමක් කොහෙත්ම අවශ්‍ය වන්නේ නැහැ. එවන් දේවල් කියමින් ඔබ රවටා ඔබේම දත්ත ලබා ගන්නට දරන වෑයම්වලට හසු වෙන්න එපා.

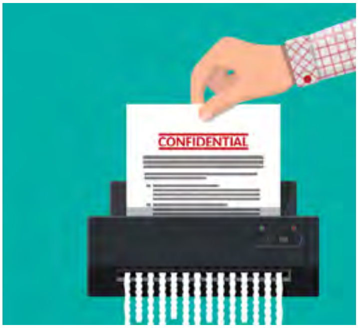
අස්ථාන ගත වුණොත් මොකද කරන්නේ?

ෆෝන් එකක් නැති වුණොත් එහි මොබයිල් ඩේටා සක්‍රියව තිබෙනවා නම් GPS භාවිතයෙන් එය තිබෙන තැන සොයා ගන්න පුළුවන්. ඇන්ඩ්‍රොයිඩ් සඳහා https://www.google.com/android/find මෙන්ම ඇපල් සඳහා https://www.apple.com/icloud/find-my/ වෙත පරිගණකයකින් පිවිස ස්ථානය සොයා ගන්න. දුරකථනය නැවත ලබා ගැනීම අපහසු නම් එම වෙබ් පිටුවල ඇති Erase විධානය භාවිතයෙන් උපාංගයේ සියළු දත්ත මකා දමන්න.

අනතුරුව, දුරකථන සේවා සම්පාදකයා (සිම්පත ලබා ගත් සමාගම) අමතා සිම්පත අක්‍රිය කරවාගන්න. එම අංකය ඔබට පසුව වෙනත් සිම්පතක් සමග ලබා ගත හැකියි. ගූගල්, ෆේස්බුක් ගිණුම්වල පාස්වර්ඩ්නුත් වෙනස් කරන්න. දැන්, https://www.ineed.police.lk/ වෙබ් අඩවිය හරහා දුරකථනයේ IMEI අංකය යොදා පැමිණිල්ලක් ගොනු කරන්න.

උපාංගයක් විකුණන්නට පෙර,

පැරණි ලැප්ටොප් එකක්, දුරකථනයක් වෙනත් කෙනෙක්ට දෙන්නට පෙර, ඔබේ දත්ත වෙනත් උපාංගයකට හෝ Google Drive වැනි සේවාවකට කොපි කරගෙන, ඔබ පිවිසී සිටින ගිණුම් සියල්ලෙන්ම Logout වී, ශ්‍රෙඩර් (Shredder) මෘදුකාංගයකින් දත්ත ශූන්‍ය කර දමන්න. නැත්නම්, ඔබ ඩිලීට් කළ දේවල් නැවතත් ලබා ගන්නට නව හිමිකරුවන්ට හැකියාව තිබෙනවා.



සියළු පුද්ගලික ගොනු Recycle Bin හෝ Trash එකෙනුත් ඉවත් කර දැමීමටත් මතක තබා ගන්න.

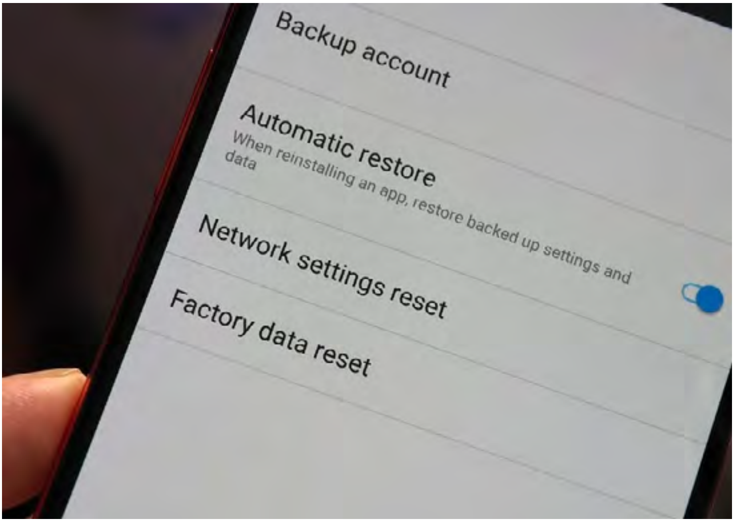
පහත දැක්වෙන්නේ එවන් ශ්‍රෙඩර් මෘදුකාංග කිහිපයක්.

- Blancco Drive Eraser - https://www.blancco.com/products/drive-eraser/
- DBAN - https://dban.org/
- BCWipe - https://www.jetico.com/data-wiping
- BleachBit - https://www.bleachbit.org/download

හාඩ් ඩිස්ක (Hard Disk - HDD) සහිත පරිගණක සඳහා ඉහත ලැයිස්තුවෙන් මෘදුකාංගය ස්ථාපනය කරගෙන, දත්ත ශූන්‍ය කර දමන්න.

ඇන්ඩ්‍රොයිඩ් සඳහා, පහත පියවර අනුගමනය කරමින් දුරකථනයේ ඇති සියලුම දත්ත එක්වරම මකා දමන්නට පුළුවන්.

Settings > Backup & Reset > Factory data reset > Reset phone



දුරකථනයේ Settings වෙත පිවිස ඉහත දක්වා ඇති පියවර හරහා Reset Phone යන විධානය තෝරන්න. මෙම පියවර දුරකථනය නිෂ්පාදිත ආයතනය අනුව වෙනස් වෙන්න පුළුවන්.

ඇපල් දුරකථන සඳහා පහත පියවර හරහා රීසෙට් (reset) කරන්න.

Settings > General > Reset > Erase All Content and Settings

4. අන්තර්ජාල වංචාවන්ට හසු නොවෙමු

මෙම කොටසින් ආවරණය වන කරුණු:

- වංචාවන් (Scams) ක්‍රියාත්මක වන ආකාර
- වංචාවන්ට භාවිතා කරන ක්‍රම, සහ ඒවායෙන් වැළකීම

ඉ-මේල්, ෆේස්බුක් මැසේජ් ආදිය හරහා අපේ මුදල්, තොරතුරු ආදිය සොරකම් කරගැනීමේ අරමුණින් වංචාවන් (Scams) ක්‍රියාත්මක වෙනවා. ඒවා පහත ආකාර වලින් සිදු විය හැකියි.

- ඔබ ඇණවුම් නොකළ, ඔබට අයත් බවට කියන භාණ්ඩයක් රේගුවේ ඇති බවත්, ඊට මුදල් ගෙවා ලබා ගත යුතු බවත් කීම.
- කරදරයකට පත්ව ඇතැයි කියමින් මුදල් ඉල්ලීම
- ව්‍යාජ මිතුරු හෝ විවාහ යෝජනා

ස්පෑම් (Spam) ලෙස එන වංචා (Scam)

ස්පෑම් කියන්නේ, අපිට අදාල නොවන, බොහෝ විට නොදන්නා පුද්ගලයින් එවන අනවශ්‍ය පණිවිඩ වලට යි.

වංචාකරුවන් මේවා හරහා අපේ අවධානය දිනා ගන්නට උත්සාහ කරනවා. මේ හරහා පහත දේවල් සිදු වෙන්න පුළුවන්.

- සහභාගී නොවූ තරගයකින් විශාල මුදලක් දිනූ බව කීම
- ව්‍යාජ අරමුදල් එක්රැස් කිරීම්
- ආයෝජනයක් සිදුකර ඉන් වැඩි මුදලක් ලද හැකි බව කීම
- අපේ ඡායාරූප ඔවුන් සතු බව කියමින් තර්ජනය කර කප්පම් ගැනීම

මේ ගැන වැඩි විස්තර දැනගන්න කැමති නම්, hithawathi.lk වෙබ් අඩවියේ ඇති ලිපිය බලන්න මේ QR Code එක ස්කෑන් කරන්න.
https://www.hithawathi.lk/si/help-center-si/knowledge-base-si/spam-vs-scam-si/

එක්තරා පාසලක නිවාසාන්තර ක්‍රීඩා උත්සවයේ ඡායාරූප පාසැල් පරිපාලන අංශය විසින් ෆෙස්බුක්හි පළ කර තිබුණා. ටික දවසකින් 10 වන ශ්‍රේණියේ ඉගෙනුම ලැබූ අනුරාධාගේ ෆේස්බුක් ගිණුමක ඒ ඡායාරූප පළව තිබෙන බව එයාගේ අම්මාගේ මිතුරියක් දැක්කත්, එම ගිණුම අනුරාධාගේ ගිණුමක් නොවන බවයි දැනගන්නට ලැබුණේ.

මැසේජ් කර මේ ව්‍යාජ ගිණුම ඉවත් කරවන්නට උත්සාහ කළත්, වංචාකරුවන් කිව්වේ, මුදලක් නොගෙව්වොත් තව තවත් ඡායාරූප පළ කරන බවයි. (සත්‍ය කතාවක් ඇසුරිණි. නම් ගම් මනඃකල්පිතයි.)

hithawathi.lk වෙබ් අඩවියේ ඇති තවත් සත්‍ය කථා සහ ගත යුතු පිළියම් ගැන දැනගන්න මේ QR Code එක ස්කෑන් කරන්න.
https://www.hithawathi.lk/si/help-center-si/real-time-cases-si/

වංචාවන්ගෙන් ගැලවෙන හැටි

- ඔබ නොදන්නා පුද්ගලයින්ගෙන් ලැබෙන පණිවිඩවලට ප්‍රතිචාර නොදැක්වීම
- ව්‍යාජ සමාජ ජාල ගිණුම් Report කිරීම
- සහභාගී නොවූ තරගයකින් ජය ලබන්නේ කෙසේදැයි විචක්ෂණශීලීව කල්පනා කිරීම
- ජීමේල් වැනි ස්වයංක්‍රීයව ස්පෑම් ඉ-මේල් වෙන් කරන සේවාවන් භාවිතය

නොදන්නා අය එවන ලින්ක් ක්ලික් නොකර සිටීම ද අත්‍යාවශ්‍ය වන්නේ ඒවායේ ෆිෂිං (Phishing) ක්‍රම තිබිය හැකි නිසා යි. ඒ ලින්ක් එකෙන් පිවිසුණාම ෆේස්බුක් login පිටුව වගේම ව්‍යාජ පිටුවක් පේනවා. එයට ඔබේ මුරපදය ටයිප් කළහොත් වංචාකරුවන්ට/හැකර්වරුන්ට ඔබේ මුරපදය ලැබෙනවා.

එනිසා වෙබ් අඩවියක සත්‍යතාව සැක හැර දැනගැනීම වැදගත්.

ව්‍යාජ/ෆිෂිං වෙබ් අඩවියක් හඳුනා ගන්නේ මෙහෙමයි

වෙබ් ලිපිනය වෙත අවධානය යොමු කරන්න. වෙබ් අඩවියකට පිවිසෙද්දී හෝ සබැඳියක් (Link) ක්ලික් කිරීමට පෙර අදාළ URL එක පරීක්ෂා කර බලා එය සැබෑ වෙබ් අඩවියක්ද යන්න තහවුරු කර ගන්න.

> https://transparencyreport.google.com/safe-browsing/search වෙත ගොස් Search by URL යන කොටුවට අදාල ලිපිනය ඇතුලත් කිරීමෙන් මෙය පහසුවෙන් කරගන්න පුළුවන්.

එසේම, ඔබට facebook.com වෙත පිවිසිය යුතු නම්, එහි එම අකුරුම ඇති බවත්, faecbook, facebok, facbook, facboook වැනි යමක් නොවන බවත් තහවුරු කරගන්න.

ව්‍යාජ වෙබ් අඩවි හඳුනාගත හැකි තවත් ආකාර දැනගන්න hithawathi.lk වෙබ් අඩවියේ ඇති ලිපි බලන්න මේ QR Code එක ස්කෑන් කරන්න.
https://www.hithawathi.lk/si/help-center-si/knowledge-base-si/you-decide-whether-it-is-a-fake-or-a-real-website/

නරඹන්නට යමක්

සාමාන්‍ය ජනතාව නොමග යවන වංචාකරුවන්ව රවටමින් ඔවුන්ගේ වංචාවන් ලොවට හෙළි කරන යූ ටියුබ් චැනල් තිබෙන බව දන්නවා ද?

- Kitboga
- IRLrosie
- Trilogy Media

ඉහත චැනල්වල නම් යූටියුබ් එකේ search කර නරඹන්න.

5. සමාජ ජාල දැනගෙන පාවිච්චි කරමු

මෙම කොටසින් ආවරණය වන කරුණු:

- සමාජ ජාල (Social Media) වල යහපත සහ අයහපත
- ගැටළු වලින් මිදෙන ආකාරය

සමාජ ජාල නිෂ්පාදකයන් විවිධ ආකාරයෙන් අපව ඊට ඇද බැඳ තබා ගන්නට උත්සාහ කරනවා. යමෙකු ආශා කරන දේවල් හඳුනාගෙන ඒවාම පෙන්වමින් වැඩි කාලයක් රඳවා ගැනීමත්, ඒ අතරතුර වෙළඳ දැන්වීම් පෙන්වීමත් ඒවායේ මූලික කාර්යයභාර්යය වෙනවා. මෙයට ඇබ්බැහි වුණොත් අධ්‍යාපනය පවා කඩාකප්පල් වෙන්න පුළුවන්. ඉතින් කළ යුත්තේ, ඒවායේ වාසි ලබමින්, ප්‍රවේශමෙන් භාවිතා කරන එකයි.

හොඳ සහ නරක තකට තක

බොහෝ දෙනෙක් සමාජ ජාල නරක දේවල් ලෙස නිර්වචනය කරන්නට උත්සාහ කළත්, ඒවායේ ප්‍රයෝජන බොහොමයි.

- දුර සිටින පැරණි මිතුරන් සමග කථා කිරීමට
- ඔබේ දක්ෂතා ප්‍රදර්ශනයට
- පොතපතින් ඔබ්බට සමාජයීය අවබෝධයක් ලබා ගැනීමට

සාමාන්‍ය ජීවිතය සහ සමාජ ජාල අතර කිසිම වෙනසක් නැහැ.

සත්‍ය සමාජයේ සිටින හොඳ මෙන්ම නරක අය ඒවායේත් ඉන්න නිසා පුද්ගලයන් තෝරා බේරා ගැනීම සාමාන්‍ය ජීවිතයේදී වගේම කළ යුතු වෙනවා.

අනවශ්‍ය දේවල්, සහ පුද්ගලයන් රිපෝට් / බ්ලොක් කරන්න

ෆේස්බුක් එකේ කිසිවකු සදාචාර විරෝධී යමක් පෝස්ට් කර තිබෙනවා නම්, පෝස්ට් එකේ දකුණු පස ඉහළ ඇති තිත් තුනක අයිකනය ක්ලික් කර, Find support or report post තෝරන්න. ලැබෙන කොටුවෙන් එම පෝස්ට් එක අසභ්‍ය (Nudity), ප්‍රචණ්ඩතාවයක් (Violence/Harassment), අසත්‍ය පුවතක් (Fake News) යනාදී ලෙස ගැලපෙන එක තෝරා යටින් ඇති Next බොත්තම ක්ලික් කරන්න.

ෆේස්බුක් එකේ පෞද්ගලිකත්වය රැකගත හැකි තවත් ක්‍රම දැනගන්න hithawathi.lk වෙබ් අඩවියේ ඇති තොරතුරු බලන්න මේ QR Code එක ස්කෑන් කරන්න.
https://www.hithawathi.lk/si/help-center-si/social-media/facebook/

අසත්‍ය පුවත් හඳුනාගන්න

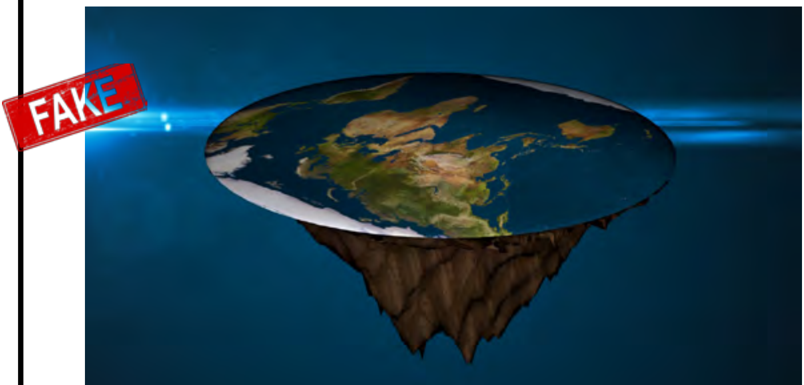
සමාජ ජාල හරහා විවිධ අයගේ යටි අරමුණු වෙනුවෙන් එහි සිටින අයගේ මනසට විවිධ අදහස් ඇතුලත් කරනවා. මේ නිසා ජනවාර්ගික ගැටුම් ඇමරිකාව, මියන්මාරය, පමණක් නොව ශ්‍රී ලංකාවේත් ඇති වුණා.

දේශපාලන අරමුණු, ව්‍යාපාරික අරමුණු ආදිය නිසා විවිධ ෆේස්බුක්/ ඉන්ස්ටග්‍රෑම් පිටු යොදාගෙන කාලයක් පුරාවට මේ අදහස් ක්‍රම ක්‍රමයෙන් පරිශීලකයන්ගේ හිසට ඇතුළු කරනවා.

එනිසා, යමක් දුටු වහා ශෙයා (Share) කරන්නේ නැතිව විචක්ෂණශීලීව ඇත්ත-නැත්ත සොයා බැලීම එය භාවිතා කරන අපි හැමෝගෙම වගකීමක්.

දුටු වහා කිසිවක් Share කරන්න එපා

ඇත්තම කතාව - ලෝකය පැතලියි!



ගුරුත්වාකර්ෂණය කියලා දෙයක් නෑ.

ලෝකය පැතලි නිසා තමයි හැමදේම බිමට වැටෙන්නේ. විද්‍යාව කියන්නේ බොරුවක්.

අනිත් අයටත් දැනගන්න Share කරන්න

අසත්‍ය පුවතක් සඳහා නිදර්ශනයක්

ඔබ දන්නවා ද?
මෙරට නීතිය අනුව, ඕනෑම මාධ්‍යයක් හරහා අසත්‍ය ප්‍රකාශ පළ කරන අයට දැඩි දඬුවම් පැනවිය හැකි වේ.

සම්ප්‍රචාරය හෙවත් ප්‍රොපගැන්ඩාවක් යනු තමාට අවශ්‍ය යටි අරමුණක් ක්‍රියාත්මක කර ගැනීමට යොදන සැලසුම් සහගත මොළ සේදීමකි.

එමගින් තමාගේ මතයට අනෙක් අයව අනුරූප කරගන්නට අවස්ථාව ලැබේ. සමාජ මාධ්‍ය හරහා මෙය කළ හැකි ක්‍රමය වන්නේ ප්‍රසිද්ධ පේජ් කිහිපයකට මුදල් ගෙවා ඔවුන් ලවා නිරන්තරයෙන් අදාල මතය සමාජ ගත කිරීම පමණි.

-තඹරු විජේසේකර ("සමාජ ජාල ජංජාලයේ කුප්‍රකට ඇබ්බැහිය" දිනමිණ - ද්වාර, 2020/10/05)

නීතිමය පියවර ගන්න

කරදරයකට මුහුණ දුන්නාම නිහඬව සිටීමෙන් සිදුවන්නේ අපරාධකරුවන්ට නිදැල්ලේ සිටීමට ඔබ අවසර දීමයි. ඉන් තවත් කෙනෙක් කරදරයේ වැටෙන්නට පුළුවන්. එනිසා බලධාරීන්ට ඒ ගැන දන්වන්න.

සමාජ ජාල (Facebook, Twitter, TikTok, Wiki වෙබ් අඩවි, Blog) හරහා කිසියම් හෝ පීඩාවකට මුහුණ දුන්නොත් ඔබේ පිහිටට හිතවත් ව්‍යාපෘතිය සිටිනවා.

ඒ සම්බන්ධ උපදේශනයන් ලබා ගැනීමට
011-421-6062 යන දුරකථන අංකය ඇමතිය හැකි අතර,
https://www.telligp.police.lk/ යන ලිපිනයට ගොස් එහි ඇති ආකෘති පත්‍රයෙන් Cybercrime තෝරා සාක්ෂි සහිතව පොලීසියට පැමිණිලි කිරීමට ද හැකියාව තිබෙනවා.

6. සයිබර් හිරිහැරවලට බිය වෙන්න එපා

මෙම කොටසින් ආවරණය වන කරුණු:

- මාර්ගගත හිරිහැර උදාහරණ සමග හැඳින්වීම
- බලපෑම සහ ඉන් මිදීමට කළ යුතු දේ

මාර්ගගත හිරිහැර (Cyberbullying) ලෝකයේ සෑම රටකම සිදුවන, වයස් භේදයකින් තොරව වැඩි පිරිසක් මුහුණ දෙන දෙයක්. තමන් කෙතරම් හොඳින් කටයුතු කළත්, එය වෛරී සහගතව විවේචනය කිරීම, තර්ජනය කිරීම, හෝ ගරුත්වයට හානි කිරීම වැනි දේ මේ හරහා සිදුවිය හැකියි.

2018 වසරේදී ෆාතිමා සහ තවත් පිරිමි ළමයෙකු තම විශ්ව විද්‍යාලයේ පැවති සාදයකදී ක්‍රීඩාවක් කරන අතරතුර ඒට පැමිණ සිටි නිල ඡායාරූප ශිල්පියකු විසින් කැමරා කාචයේ සටහන් කරගනු ලැබුවා.

මෙය අනෙකුත් ඡායාරූප සමග අන්තර්ජාලයේ පළ කෙරුණු අතර, අන්තවාදී ආගමික හස්තයන් මෙය දැඩිව විවේචනය කරමින් කියා සිටියේ දැරිවියක් එලෙස පිරිමි ළමුන් සමග ඡායාරූප නොගත යුතු බව යි. වාචික පරිභවයන්, හිරිහැර කිරීම් මෙන්ම මරණ තර්ජනයන් ද ඇයට එල්ල වුණු නිසා නිවසින් බැහැරව යාමත් ඇයට බිය දනවන්නක් වුණා.

2017 වසරේ කොමික්-කොන් නමින් පැවැත්වෙන සිනමාවේ වීර චරිත අනුව හැඩ ගැන්වෙන විවිධ ඇඳුම් තරගාවලියකදීත් මෙවැන්නක් සිදු වුණා. වොන්ඩර් වුමන් ලෙස හැඳ සිටි අමායා සහ ශෙහානිගේ ඡායාරූප පළවූ පසු වෙනත් ෆේස්බුක් පේජ්වලින් ඒවා ගෙන ඔවුන්ගේ ශාරීරික පෙනුම හාස්‍යයට ලක් කළා.

ඔවුන්ට එල්ල වූ හිංසනයන්ට එරෙහිව වොන්ඩර් වුමන් චරිතය රඟපෑ නිළිය ද තම ට්විටර් ගිණුම හරහා මුළු ලොවම ඉදිරියේ අමායා සහ ශෙහානිව ප්‍රශංසාවට ලක් කළා.

ඔබත් මෙවන් අවස්ථාවකට මුහුණ දුන්නොත්, අපරාධ පරීක්ෂණ දෙපාර්තමේන්තුවේ (CID) සමාජ ජාල අංශය වෙත dir.cid@police.lk හෝ 011 233 7432 හරහා දැනුම් දෙන්න.

මාර්ගගත හිරිහැරවල (Cyberbullying) බලපෑම

අශෝභන අදහස් දැක්වීම හෝ පොදුවේ හිරිහැර කිරීම කෙනෙකුට වේදනාවක්, දුකක් හෝ කෝපයක් ඇති වෙන්න පුළුවන්. ඒ හරහා මානසික අවපීඩනය, කාංසාව හෝ ආත්ම අභිමානය පිළිබඳ ගැටළු ඇති වෙනවා.

බොහෝ දෙනෙක් ෆෝන් එක පාවිච්චි කරන්නේ ගෙදර ඉන්න වෙලාවට යි. ගෙදර කියන්නේ තමන්ට ආරක්ෂිත, හිතට සතුටක් ගෙනෙන තැනක් වුණත්, එතැනදී පවා අශෝභන අදහස් හෝ හිරිහැර කිරීම්වලට (අන්තර්ජාලය හරහා) මුහුණ දීමෙන් තත්ත්වය භයානක වෙන්න තිබෙන ඉඩකඩ වැඩියි.

කෙනෙක් බණිද්දී එතනින් ඉවත්ව යන්න පුළුවන් වුණත්, වචනයෙන් කියපු දෙයක් ටිකකින් අමතක වුණත්, සමාජ ජාලවල ලියා පළ කළ දෙයක් නැවත නැවතත් කියවන්නට හැකි නිසා තමන්ගේ හිත දිගින් දිගට ම පීඩාවට පත් වෙනවා.

හිරිහැර කරන පුද්ගලයා එයට මුහුණ දෙන කෙනාගේ (වින්දිතයාගේ) සිතුවිලි/හැඟීම් දුරකථන තිරය හරහා නොදකින නිසා තව තවත් පරිභව කරන්නට පෙළඹෙනවා. ඉන් වින්දිතයාට ඇතිවන පීඩනය තවත් වැඩි වෙනවා.

එවැනි අවස්ථාවක කළ යුතු දේ

අදාල පුද්ගලයාව බ්ලොක් (block) කරන්න

- දුරදිග යන්නට පෙර, ස්ක්‍රීන්ශොට් (Screenshots) අරගෙන, ඔවුන්ව අවහිර (Block) කරන්න.

ඔවුන් කියන දේවල් ගණන් ගන්න එපා

- ඔබ නිවැරදි බව ඔබ දන්නවා නම්, ඔවුන්ගේ වචන වලින් පෙනෙන්නේ ඔවුන්ගේ නොහැදියාව බව තේරුම් ගන්න.

ඔවුන් පළ කළ දේවල් නැවත නැවතත් කියවන්න එපා

- ඉන් ඔබේ තරහා ඇවිස්සීම මිස සිදුවන හොඳක් නැහැ. සිදුවීම report කරන්න.

හැමෝටම එකම සිතීමේ විලාශයක් නැති බව තේරුම් ගන්න.

- බණින බවක් පෙනුනත්, සමහර විට ඒ ඔවුන් තම අදහස ප්‍රකාශ කරන ආකාරය වෙන්න පුළුවන්.

උපකාර සපයන ආයතන දැනුවත් කරන්න

- හිතවතී, පොලිස් ළමා හා කාන්තා කාර්යාංශය, ජාතික ළමා ආරක්ෂණ අධිකාරිය වැනි ආයතන වෙත දන්වන්න.

7. නීති පද්ධතිය ඔබ වෙනුවෙන් සූදානම්

මෙම කොටසින් ආවරණය වන කරුණු

- දේශීය පරිගණකාශ්‍රිත අණපනත්

හොර මෘදුකාංග පාවිච්චි කරන්න එපා

2003 අංක 36 දරණ බුද්ධිමය දේපළ පනතේ 6(1) (අ) වගන්තිය යටතේ පරිගණක වැඩසටහන් සඳහා ප්‍රකාශන හිමිකම් ලැබෙනවා. මේ නිසා ඔයා හදපු මෘදුකාංගයක් හොරෙන් ගන්න අනෙක් අයට බැරි වෙනවා.

ඒ වගේම, මයික්‍රොසොෆ්ට්, ඇඩෝබ් වැනි සමාගම්වල මෘදුකාංග ක්‍රැක් කරලා ව්‍යාපාරික ආයතනයක පාවිච්චි කළොත් ඉහළ ආයතන නිලධාරීන්ට පවා එයට වගකියන්නට සිදු වෙනවා. කඩෙන් ගන්නා අඩු මිල සීඩී පවා මෙයට අයත් වෙනවා.

අසභ්‍ය දර්ශන වලින් වැළකීමට අයිතිය ඔබට තිබෙනවා

සශේන්ට එයාගේ අයියාගේ යාළුවෙක් ෆෝන් එකේ තිබිලා වීඩියෝ ටිකක් පෙන්නුවා. ඒවායේ තිබුණු දේවල් අසභ්‍ය බව සශේන්ට තේරෙන්න වැඩි වෙලාවක් ගියේ නැහැ.

"මල්ලි කැමති නැද්ද මේ වගේ එකක් කරලා ගාණක් හොයාගන්න? හොඳට ගෙවන්නම් ඔයාට." ඒ අයියා ඇඟට පතට නොදැනී කිව්වා.

ශ්‍රී ලංකාවේ දණ්ඩ නීති සංග්‍රහය ගැන අවබෝධයක් තිබුණු සශේන් ඒකට තදින්ම විරුද්ධ වුණා. අවු. 18ට අඩු තමන්ට මේ වගේ වීඩියෝ පෙන්වන එක වගේම, ඒවාට සහභාගී වීමට කෙනෙක් කතා කරනවා නම් ඒ අයට වසර 2කට නොඅඩු සිර දඬුවම් පවා ලැබිය හැකි බව එයා පැහැදිලි කළා.

කිසිම විටෙක නිරුවත් හෝ අති පෞද්ගලික ඡායාරූප ගන්න එපා. වෙනත් අයට ගන්නට අවසර නොදීමත් ඔබේ අයිතියක්.

ඉන්ටර්නෙට් කැෆේ වලදී අපයෝජනයට ඉඩ නැහැ

2006 දී ශ්‍රී ලංකාවේ දණ්ඩ නීති සංග්‍රහයට එක් වුණු සංශෝධනය (2006 අංක 16 දරන දණ්ඩ නීති සංග්‍රහ (සංශෝධන සහිත) පනත) මගින් පරිගණක සේවා සපයන පුද්ගලයන් (උදා: සයිබර් කැෆේ) දරුවන්ව ලිංගික අපයෝජනයට ලක් වීමෙන් වැළැක්වීමේ යුතුකම ඇති අය ලෙස හඳුනාගෙන තිබෙනවා.

තමන්ගේ පරිගණක හරහා දරුවකු ලිංගික අපයෝජනයට ලක් වෙනවා නම් එයාලා ඒ බව ළඟම තිබෙන පොලීසියට දැනුම් දෙන්න ඕන. නැත්නම් එයාලාට වසර 2ක සිර දඬුවමක් සහ/හෝ දඩයක් නියම වෙනවා.

අන් අයගේ පරිගණක/දුරකථනවලට අත නොතබමු

ඉස්කෝලෙ ඇරිලා තාත්තා වැඩ ඉවර වෙනකම්, තාත්තා වැඩ කරන රජයේ ඔෆිස් එකේ ඉන්න සුපුන්ට එතන කම්පියුටර්වල තියෙන දේවල් බලන්න ආසා හිතුණා.

ඒවායේ තිබුණු මිළ ග්‍රාහක තොරතුරු, ට්‍රැෆික් දත්ත වගේ හැම දෙයක්ම බලන්න සුපුන් උත්සාහ කරද්දි එයාගෙ තාත්තා මේක දැකලා අවවාද කළා.

පුතේ, පරිගණකයකට හෝ පරිගණකයක ඇති තොරතුරු වලට ප්‍රවේශ වෙන්න තමන්ට නීත්‍යානුකූල අයිතියක් නැති බව හොඳින් දැන දැනම ඒවාට අනවසරයෙන් ප්‍රවේශ වීම 2007 අංක 24 දරණ ශ්‍රී ලංකා පරිගණක අපරාධ පනත අනුව ලොකු වැරැද්දක්. ඒවායේ අනවසර වෙනස් කිරීමක්, හානියක්, මුරපද වෙනත් අයට දෙන එක වගේ ගොඩක් දේවල් ඒකෙන් ආවරණය වෙනවා. ඒ නිසා කවදාවත් ඔයාට අයිති නැති කම්පියුටර්වල මොනවත් කරන්න යන්න එපා. හොඳ ද?

තාත්තා පැහැදිලි කළ දේ සුපුන් පිළිගත්තා. ඒ නිසා සිර දඬුවම් සහ දඩ මුදලකින් බේරෙන්න එයාට පුළුවන් වුණා.

වෙනත් කෙනෙක් පාස්වර්ඩ් එකක් ටයිප් කරද්දි වුණත් අපි අහක බලාගන්න පුරුදු වෙන්න ඕන. ඒක යහපත් පුද්ගල ගුණාංගයක්.

8. මානසික ගැටළු වලට මුල පුරන සයිබර් අපරාධ

මෙම කොටසින් ආවරණය වන කරුණු

- ඇති විය හැකි මානසික අපහසුතාවයන් හා විසඳා ගැනීමට කළ හැකි දේ

සහන් දවසක් ඉන්ටර්නෙට් යද්දී වෙබ් සයිට් එකක තිබුණා, එයා අන්තර්ජාලයට ආපු 1,000,000,000 පුද්ගලයා නිසා ඇමරිකානු පුරවැසිභාවය ලැබෙන බව. හැබැයි ඒකට පොඩි ගෙවීමක් කරන්න ඕන කියලත් තිබුණා. සතුටින් ඉපිල ගිය සහන්, ඒ ගාණ තමන්ගේ ක්‍රෙඩිට් කාඩ් පතින් ගෙව්වා.

"මං දැන් ඇමරිකාවට යන්න ඉන්නේ. දැන් මම ගොඩ!" සහන් යාළුවො හැමෝටම කිව්වා. ගමේ අයත් එයාට සුබ පැතුම් එක් කළා.

ඒත් එතනින් පස්සේ ඒ ගැන කිසිම තොරතුරක් එයාට දැනගන්න ලැබුණේ නැහැ. බැංකුවෙන් ආපු ඇමතුමකින් කිව්වේ එයාගේ කාඩ්පතින් ගෙවපු ගාණට අමතරව කිහිප වරක දී රු. ලක්ෂයකට ආසන්න මුදලක් ස්වයංක්‍රීයව කැපී ඇති බවයි.

සහන්ට සමාජයට මුහුණ දෙන එක ගැටළුවක් වුණා. යාළුවොන්ගෙන් විහිළු තහළු රැසකට මුහුණ දෙන්නත් සිද්ධ වුණා.

කෝපය, වංචාවට ලක් වූ බව, ඉච්ඡාභංගත්වය, කළකිරීම, අගෞරවයට පත් වීම, අසරණ වීම වගේ හැඟීම් සමුදායක් සහන්ගේ සිත පුරා පැතිර ගියා.

වංචනික ක්‍රියා, සහ අපහාස කිරීම් වලට බය වෙන්න එපා!

සමාජ ජාල ආශ්‍රිතව

- ව්‍යාජ ආදර සම්බන්ධතා
- අපයෝජනයන්
- රවටා හෝ කප්පම් වශයෙන් මුදල් ලබා ගැනීම්
- බැණ වැදීම් (Hate speech)
- අපහාස කිරීම් (Cyber bullying)

සම්බන්ධ සිද්ධි බොහොමයක් සිදු වෙනවා. මේවාට මුහුණ දුන්නාම නිසි මානසික උපදේශනයක් ලැබුණේ නැත්නම් ජීවිත අහිමි කරගැනීම් පවා ඇති වෙන්න පුළුවන්.

ඉතින් ඒ වගේ දේකට මුහුණ දුන්නොත් කිසිම වේලාවක ඒකට බය වෙන්න එපා. අවශ්‍ය නීතිමය පියවර අරගෙන, ඒ ප්‍රශ්නයට ඍජුව මුහුණ දෙන්න.

නිහඬව සිටීම වංචාකරුවන්ට උල්පන්දම් දීමක්

සමාජ මාධ්‍ය ආශ්‍රිත සත්‍ය සිද්ධි ගැන hithawathi.lk වෙබ් අඩවියේ ඇති තොරතුරු බලන්න මේ QR Code එක ස්කෑන් කරන්න.
https://www.hithawathi.lk/si/help-center-si/news-papers/

වැඩිහිටියෙකුට දැනුම් දෙන්න

ඔබ මේ වගේ ගැටළුවකට මුහුණ දුන්නොත් වහාම ගුරුවරයෙකුට, වැඩිහිටියෙකුට මේ ගැන දැනුම් දෙන්න. මේ අත්පොත අවසානයේ ඔබට පිහිට පැතිය හැකි ආයතන/සංවිධානවල දුරකථන අංක තිබෙනවා.

සමාජ මාධ්‍ය නිසා දැනුම, සමාජ කුසලතා, නිර්මාණශීලීත්වය, අධ්‍යාපනික සාධනය, විවිධ සංස්කෘතීන්, ආගම් පිළිබඳ දැනුම දියුණුවීම, ආත්ම අභිමානය ගොඩනැගීම වගේ වාසි රැසක් ලැබෙනවා. ඒ නිසා අවබෝධයෙන් යුතුව සමාජ මාධ්‍ය සහ අන්තර්ජාල භාවිතයට හැමවිටම හුරු වෙන්න.

රන්දිමාගේ ෆේස්බුක් ගිණුමේ හිටපු යාළුවෙක් එයාගේ නිතර දුක සැප අහමින් බොහොම සමීප වුණා. කතා කරන්න යාළුවෙක් හමුවුණු එක ගැන සතුටින් හිටපු එයා ඉගෙනීමත් අමතක කරලා මේ කිසිදා නොදුටු යාළුවාත් එක්ක චැට් කරන්න පෙළඹුණා. තමන්ගේ ප්‍රශ්න බෙදාහදා ගන්න කෙනෙක් ලැබුණු එක ගැන එයා ගොඩක් සතුටින් හිටියේ. ක්‍රම ක්‍රමයෙන් මේ දෙදෙනා අතර ආදරයක් ඇතිවුණා.

ඒත්, ඒ ආදරේ ඔප්පු කරන්න නම් සිනමාහල් වැනි විවිධ තැන්වලට ඇවිත් නිතර හම්බවෙන්න ඕන කියලා ඒ අයියා කිව්වා.

මේ ගැන සැක හිතුණු එයා ඉක්මනින්ම එයාගේ අම්මලාට සම්පූර්ණ විස්තරේ කිව්වා. හිතවතී වැනි වෙබ් අඩවිවලින් අන්තර්ජාලයේ සිදුවන වංචාවන් ගැන හොඳ දැනුමක් ලබාගෙන හිටපු ඒ බුද්ධිමත් දෙමව්පියන් රන්දිමාට ඒ ගැන මෙහෙම පැහැදිලි කළා.

දුවේ, හිතේ තියෙන දේවල් කියන්න යාළුවෙක් ඉන්න එක හොඳ දෙයක්. අනික අවු. 20ක් වුණු ඔයාගෙ වයසත් එක්ක පිරිමි ළමයින්ට ආකර්ෂණය වෙන එකත් සාමාන්‍ය දෙයක්.

ඒත් ඒවායෙන් අයුතු ප්‍රයෝජන අරගෙන ජීවිතේම විනාශ කරලා දාන්න බලාගෙන ලොකු පිරිසක් ඉන්නවා. දුක අහන මුවාවෙන් එයාලා තවත් දුක් ගොඩක් දීලා තමයි අන්තිමට දාලා යන්නේ.

ඔයා මේ ගැන අපිට කලින්ම කියපු එක ගැන බොහොම සතුටුයි. මෙයාගේ ප්‍රොෆයිල් එක ගැන අපි පොලීසියට පැමිණිලි කරමු. ඔයා එක්ක චැට් කරපු ඒවත් ස්ක්‍රීන්ෂොට් (Screenshot) අරගෙන සාක්ෂි විදියට යවන්න ඕන. එතකොට ආයෙ ඔයා වගේ අහිංසක දරුවෙක්ව බිලි ගන්න එයාලාට අවස්ථාවක් ලැබෙන්නෙත් නැහැ. අපි කටවහගෙන හිටියොත් තව මේ වගේ ගොඩක් භයානක දේවල් සිද්ධ වෙන්න පුළුවන්.

9. තාක්ෂණය කියන්නේ හරිම වටිනා දෙයක්

> මෙම කොටසින් ආවරණය වන කරුණු:
>
> - අන්තර්ජාලය යනු බියවිය යුත්තක් නොවන බව
> - නිසි දැනුම ඇති විට ඕනෑම ගැටළුවක් විසඳා ගත හැකි බව

අම්මාත් එක්ක ඉරිදා පොළට ගියපු සසඳිට සෙනඟ අතරේ අම්මාව මඟ හැරුණා. එහා මෙහා ඇවිදිමින් හැම මුහුණක්ම අම්මාගේ මුහුණදැයි බලමින් යද්දී ක්‍රමයෙන් ඇස් දෙක කඳුළින් තෙත් වන්නටත් පටන් ගත්තා.

වාසනාවකට එයාගේ ගුරුතුමියත් පොළට ඇවිත් හිටපු නිසා අහම්බයකින් සසඳිව දැක්කා.

ගුරුතුමිය- දුවේ ඇයි ඔයා මේ තනියම?

සසඳි- අනේ ටීච මට අම්මාව මඟ හැරුණා. හොයාගන්න බෑනේ.

ගුරුතුමිය- ඔයා අම්මාට කෝල් එකක් දීලා බැලුවේ නැද්ද දුවේ?

සසඳි- මට ෆෝන් එකක් නෑනේ ටීච. අම්මා කියනවා ඒවා ළමයින්ට හොඳ නැහැ කියලා.

ගුරුතුමිය- ඒක වැරදි අදහසක් දුවේ. ප්‍රවේශමෙන් පාවිච්චි කරන හැටි ඔයාට උගන්වනවා මිසක් තාක්ෂණයෙන් ඔයාව ඈත් කරන එක හොඳ දෙයක් නෙවෙයි. ඉන්නකො, මම කෝල් එකක් දෙන්නම්. දුව පොඩ්ඩක්වත් බය වෙන්න එපා හොඳ ද?

පැන්සලක් කියන්නේ අපි හැමෝම ලියන්න ඉගෙන ගන්න පාවිච්චි කළ දෙයක්. ඒත්, John Wick චිත්‍රපටය බලපු කෙනෙක් පැන්සල කියන්නේ මිනීමරු උපකරණයක් කියලා අර්ථ දැක්වුවොත් මෙලොව කිසිම දරුවෙක්ට අකුරු ලියන්න බැරි වේවි.

බොහෝ වැඩිහිටියන් ඔවුන්ට තාක්ෂණය ගැන ඇති දැනුමේ අඩු බවත්, ඇතැම් මාධ්‍ය විසින් සංවේදනවාදීව වාර්තා කරන කරුණු නිසාත් අන්තර්ජාලය, පරිගණක, සහ සමස්තයක් වශයෙන් තාක්ෂණය කියන්නේ භයානක දෙයක් බවට සමාජ දුර්මතයක් ගොඩනගාගෙන තිබෙනවා.

ඒත්, හිතවතී ව්‍යාපෘතිය ගෙන එන මේ අත්පොත කියවපු ඔයාට දැන් ඕනෑම ගැටළුවකට මුහුණ දෙන්නට අවශ්‍ය දැනුම තිබෙනවා. මෙහි තිබෙන ඉංග්‍රීසි වචන සර්ච් කරමින් තවත් දැනුම එකතු කරගන්නටත්, ඕනෑම දෙයක් අන්තර්ජාලය තුළින්ම සර්ච් කරමින් අනාගතයේ බිහිවන තාක්ෂණය ගැන තමන්ගේ දැනුම වැඩි කරගන්නට පුරුද්දකුත් ඔබට ලැබෙනවා.

වගකීමෙන් පාවිච්චි කරමු

අන්තර්ජාලය භාවිතා කරද්දී තමන්ගේ ආරක්ෂාව වගේම අනෙක් අයගේ ආරක්ෂාව ගැනත් අපි හිතන්න ඕනෑ. අපේ හිත රිදෙන්න කතා කරන කෙනෙක්ගෙන් පෙර පරිච්ඡේදවල විස්තර කළා වගේ මිදෙනවා හැර, පෙරළා ඔවුන් සමග ගැටෙන්නට ගියහොත් ඔබත් ඔවුන්ට සයිබර් හිරිහැර (Cyberbullying) කරන්නෙක් බවට පත් වෙනවා.

යහපුරුදු උගනිමු

තමන්ගේ දත්ත වගේම අනිත් අයගේ දත්ත, මුරපද ආදියට උපරිම ආරක්ෂාවක් දෙන්නටත්, වෙනත් කෙනෙක් පාස්වර්ඩ් එකක් ටයිප් කරද්දී ඉවත බලා ගැනීමත් වගේ යහපුරුදු ඇති කර ගනිමු.

ඔබට පුහුණු කළ හැකි එවන් පුරුදු කිහිපයක් පහත දැක්වෙනවා.

මම අන්තර්ජාලය හරහා කවදාවත් අනෙක් අයට හිරිහැර කරන්නේ නැහැ

මම අන්තර්ජාලය හරහා වෙනත් අයගේ නිර්මාණ සොරකම් කරන්නේ නැහැ

මම වෙනත් කෙනෙක්ගේ උපාංගයකින් පෞද්ගලික තොරතුරු, ඡායාරූප ආදිය සොරකම් කරන්නේ නැහැ

මම අන්තර්ජාලය හරහා යමක් කරන්නට පෙර ඉන් ඇතිවිය හැකි ප්‍රතිඵල ගැන දෙවරක් හිතනවා

මම අන්තර්ජාලය තුළින් ගත හැකි උපරිම යහපත් ප්‍රයෝජන ගනිමින් දැනුම දියුණු කරගන්නවා

අන්තර්ජාලය තුළ යහපත් පුරවැසියෙක් වෙමු

අපි සමාජයේ ජීවත් වෙද්දී පරාර්ථකාමීව, කල්පනාකාරීව කටයුතු කරමින් අධ්‍යාපනයෙන් ඉහළටම ගිහින් රටට සේවයක් කරනවා වගේම, අන්තර්ජාලය තුළත් යහපත් පුරවැසියෙක් බවට පත් වුණොත් හැමෝටම එය යහ ප්‍රයෝජන ලද හැකි දැනුම් පාරාදීසයක් බවට පත් වේවි.

ඔබත් දැන් වගකීමෙන් යුතු
යහපත් අන්තර්ජාල වැසියෙක්

10. සයිබර් හිරිහැරයකට මුහුණ දුන්නොත් අමතන්න

හිතවතී ව්‍යාපෘතිය

තොරතුරු තාක්ෂණය හා අන්තර්ජාලය ආශ්‍රිත ක්‍රියාකාරකම් හේතුවෙන් අපහසුතාවට පත්වූ හෝ හිංසන හෝ කරදර වලට ගොදුරු වූවන් සඳහා උපකාරක සේවාවන් ක්‍රියාත්මක කිරීම සඳහා හිතවතී ව්‍යාපෘතිය කැපවී ඉන්නවා. ලංකා වසම් ලේඛකාධිකාරිය (LK Domain Registry) මගින් මෙම ව්‍යාපෘතිය ක්‍රියාත්මක කරගෙන යනු ලබනවා. ප්‍රධාන වශයෙන් ළමයින්, නව යොවුන් වියේ දරුවන්, තරුණියන් සහ කාන්තාවන් මෙහි අරමුණු වූවත්, ඕනෑම කෙනෙක්ට මිත් හෘදයාංගම සහයෝගයක් ලබාගන්න අවස්ථාව තිබීම විශේෂත්වයක්.

දුරකථන අංකය - 011-421-6062
ඉ-මේල් - help@hithawathi.lk
වට්ස්ඇප් සහ වයිබර්: +94 77 771 1199

ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර සංසදය (SL CERT)

කාමර අංක 4-112, බණ්ඩාරනායක අනුස්මරණ ජාත්‍යන්තර
සම්මන්ත්‍රණ ශාලාව, බෞද්ධාලෝක මාවත, කොළඹ 07.

දුරකථන +94 11 2691 692 / +94 11 2679 888
ෆැක්ස් +94 11 2691 064
ඉ-මේල් slcert@cert.gov.lk
වෙබ් අඩවිය www.cert.gov.lk

ජාතික ළමා ආරක්ෂණ අධිකාරිය

ජාතික ළමාරක්ෂක අධිකාරිය,
අංක 330, තලවතුගොඩ පාර, මාදිවෙල,
ශ්‍රී ජයවර්ධනපුර,
ශ්‍රී ලංකාව.

දුරකථන: +94 11 2 778 911 - 4 හදිසි ඇමතුම් අංකය: 1929
ඉ-මේල්: ncpa@childprotection.gov.lk
වෙබ් අඩවිය: www.childprotection.gov.lk

ශ්‍රී ලංකා පොලිස් අන්තර්ජාල අපරාධ පැමිණිලි මධ්‍යස්ථානය

දුරකථන: 011-285-4931
ඉ-මේල්: dir.cid@police.lk
වෙබ් අඩවිය: www.telligp.police.lk

කාන්තා හා ළමා කටයුතු අමාත්‍යාංශය

5 වැනි මහල, සෙත්සිරිපාය අදියර II, බත්තරමුල්ල, ශ්‍රී ලංකාව.
දුරකථන: +94 11 2186055 / හදිසි ඇමතුම් අංකය: 1938
ෆැක්ස්: +94 11 2187249
ඉ-මේල්: secycdwa@gmail.com
වෙබ් අඩවිය: www.childwomenmin.gov.lk

අපරාධ පරීක්ෂණ දෙපාර්තමේන්තුවේ සමාජ ජාල අංශය

ඉ-මේල් ලිපිනය: dir.cid@police.lk
දුරකථන අංකය: 011 233 7432

පාරිභාෂික වචන මාලාව

Privacy Policy - ප්‍රයිවසි පොලිසි

රහස්‍යතා ප්‍රතිපත්තියක් යනු, කිසියම් පාර්ශවයක් විසින් තම ගනුදෙනුකරුවකුගේ හෝ සේවාදායකයෙකුගෙන් දත්ත රැස් කරගෙන, ඒවා භාවිතා කරන ආකාරය, සහ කළමනාකරණය කරන ක්‍රම අනාවරණය කරන ප්‍රකාශයක් හෝ නෛතික ලේඛනයකි.

Malicious software / Malware - මැල්වෙයා

අනිෂ්ට මෘදුකාංග යනු, පරිගණක පද්ධතියකට අනවසරයෙන් පිවිසීමට, පද්ධතියක් කඩාකප්පල් කිරීමට, හානි කිරීමට හෝ දත්ත ලබා ගැනීමට විශේෂයෙන් නිර්මාණය කර ඇති මෘදුකාංග වේ.

Spam - ස්පෑම්

ස්පෑම් හෙවත් අයාචිත තැපැල් යනු, වෙළඳ දැන්වීම් යැවීමට, අනිෂ්ට මෘදුකාංග පැතිරීමට වැනි දේවල් සඳහා සාමාන්‍යයෙන් විශාල පරිශීලකයින් සංඛ්‍යාවක් වෙත එක වර අන්තර්ජාලය හරහා යවන ලද අනවශ්‍ය ඉ-මේල් පණිවිඩ වේ.

Botnet - බොට්නෙට්

අනිෂ්ට මෘදුකාංගවලින් ආසාදනය වූ සහ අයිතිකරුවන්ගේ අනුදැනුමකින් තොරව කණ්ඩායමක් ලෙස පාලනය වන පුද්ගලික පරිගණක ජාලයකි. උදා: අයාචිත තැපැල් යැවීමට.

Ransomware - රැන්සම්වෙයා

මුදල් ගෙවන තුරු පරිගණක පද්ධතියකට ප්‍රවේශ වීම අවහිර කිරීම සඳහා නිර්මාණය කර ඇති අනිෂ්ට මෘදුකාංග වර්ගයකි. මේවා ගොනු ආකේතනය කර, භාවිතා කිරීමට නොහැකි තත්වයට පත් කර දමන අනිෂ්ට මෘදුකාංග විශේෂයකි.

Hate speech - හේට් ස්පීච්

කිසියම් කණ්ඩායමකට, විශේෂයෙන් ජාතිය, ආගම හෝ ලිංගික දිශානතිය මත පදනම්ව අගතිය ප්‍රකාශ කරන අසභ්‍ය හෝ තර්ජනාත්මක කථාවක් / ලියා දැක්වීමකි.

Cyberbullying - සයිබර් බුලීං

පුද්ගලයෙකුට හිරිහැර කිරීම සඳහා විද්‍යුත් සන්නිවේදනය භාවිතා කරමින් බිය ගැන්වීමේ හෝ තර්ජනාත්මක ස්වභාවයේ පණිවිඩ යැවීම.

IMEI number - ඉමි අංකය

දුරකථන උපාංග වෙන්කර හඳුනා ගැනීම සඳහා ලබා දී ඇති අද්විතීය (unique) අංකයකි. දැමිය හැකි සිම්පත් ගණන අනුව උපාංගයකට ඇති ඉමි අංක සංඛ්‍යාව තීරණය විය හැක.

QR code - කිව්-ආර් කේත

ස්මාර්ට් ජංගම දුරකතනයක කැමරාවෙන් කියවීම සඳහා වෙබ් ලිපින හෝ වෙනත් තොරතුරු ගබඩා කළ හැකි යාන්ත්‍රික කේතයකි. Play Store හෝ App Store වෙත ගොස් "QR code scanner" ලෙස සර්ච් කර එවන් ඇප්ස් ස්ථාපනය කර ගත හැකි වේ.

යොමුව

මෙම ග්‍රන්ථය සම්පාදනයේදී පහත මූලාශ්‍ර භාවිතා කෙරිණි.

- ඵලදායී හා ආරක්ෂාකාරී ඩිජිටල් තාක්ෂණයේ භාවිතය තුළින් සුරක්ෂිත පාසල් අධ්‍යාපනයක් - පුහුණු අත්පොත
- දිනමිණ පුවත්පත
- හිතවතී වෙබ් අඩවිය (www.hithawathi.lk)
- www.stopbullying.gov
- www.freepik.com

ඔබේ දැනුම උරගා බලන්න

මේ අත්පොතෙන් ලද දැනුමත්, සහ ඔබට එදිනෙදා ඇතිවන ගැටළු සම්බන්ධයෙන් සර්ච් කර ලබා ගන්නා අමතර දැනුමත් භාවිතයෙන් හිතවතී වෙබ් අඩවියේ තිබෙන ප්‍රශ්නාවලියට පිළිතුරු සපයා සයිබර් ආරක්ෂණය ගැන ඔබේ දැනුම් මට්ටම පරීක්ෂා කරගන්න.

1. ඔබේ දුරකථනය විකිණීමට පෙර දත්ත ආරක්ෂාව වෙනුවෙන් ගත යුතු නිවැරදි ක්‍රියාමාර්ගය තෝරන්න.

    a. දුරකථනයේ මුරපදය වෙනස් කිරීම

    b. සියලුම දත්ත මකා දැමීමට Factory reset කිරීම

    c. වෝල්පේපර් එක මාරු කිරීම

    d. සිම්පත ඉවත් කිරීම

2. අන්තර්ජාලය හරහා කෙනෙක් ඔබට බැණ වැදුණොත් ඔබ එයට වහාම ප්‍රති පිළිතුරු යැවිය යුතුද?

    a. ඔව්

    b. නැත

3. හිතවතී ව්‍යාපෘතියෙන් ඉටු නොවන්නේ පහත සඳහන් දේවල් අතුරින් කුමක්ද?

    a. ගැහැණු ළමුන්ට පමණක් සහාය වීම

    b. උපදේශන සේවා සැපයීම

    c. නීතිමය ක්‍රියාමාර්ග ගැනීමට අවශ්‍ය තොරතුරු ලබා දීම

    d. ඇමතුම් සේවාවක් පවත්වාගෙන යාම

4. ද්වි-සාධක සත්‍යාපනය (Two-factor Authentication / 2FA) යනු කුමක්ද?

    a. අනිෂ්ට මෘදුකාංගයකි

    b. SMS පණිවිඩයකි

    c. ෆිෂිං සඳහා එවන පණිවිඩයකි

    d. මුරපදයට අමතරව අනන්‍යතාවය සහතික කරන ක්‍රමවේදයකි.

5. ඔබේ ඡායාරූපයක් අනවසරයෙන් පළ කර තිබුණහොත් එයට ගත හැකි හොඳම ක්‍රියාමාර්ගය කුමක්ද?

    a. කමෙන්ට් කර බැණ වැදීම

    b. මැසේජ් කර එය ඉවත් කරන ලෙස කීම

    c. රිපෝට් කර, හිතවතී ව්‍යාපෘතිය වෙත දැනුම් දීම

    d. සමාජ ජාල භාවිතයෙන් සදහටම වැළකීම

6. ශක්තිමත් පාස්වර්ඩ් එකක් වන්නේ?

   a. ඔබේ දුරකථන අංකය

   b. ඔබේ උපන්දිනය

   c. වැකියක මුල් අකුරු සංකේත ඉලක්කම් මිශ්‍රව

   d. නමට ඉදිරියෙන් 123

7. ළමා හා තරුණ පරපුර මුහුණ දෙන ඔන්ලයින් අවදානමක් නොවන්නේ

   a. සයිබර් හිංසනයට ලක් වීම

   b. අන්තර්ජාලයට ඇබ්බැහි වීම

   c. සයිබර් අපරාධවලට හසු වීම

   d. අන්තර්ජාලය හරහා ඉගෙනුම් කටයුතු කිරීම

8. අන්තර්ජාලයේ සැරිසැරීම හා බැඳි අසත්‍ය ප්‍රකාශය වන්නේ

   a. අපරාධවල නියැළෙන ව්‍යාජ ගිණුමක් පිටුපස සිටින තැනැත්තා කිසිසේත් සොයා ගත නොහැක

   b. අප නොදන්නා බොහෝ දේ අන්තර්ජාලය හරහා ඉගෙන ගත හැක

   c. සමහරු අන්තර්ජාලය අවභාවිත කර අන් අයට වංචා, හිංසා පීඩා කරයි

   d. හිතවතී, සයිබර් අවකාශයේ සුරක්ෂිතව සිටිය යුතු ආකාරය ගැන ඔබව දැනුවත් කරයි

9. අන්තර්ජාලයට / සමාජ මාධ්‍යන්ට ඇබ්බැහි වීම පිළිබඳ අසත්‍ය ප්‍රකාශය තෝරන්න.

   a. කුකීස් හරහා වෙළඳුන් අන්තර්ජාලයේ ඔබ සැරිසරන වෙබ් අඩවි, රුචි අරුචිකම් හඳුනා ගනී.

   b. සමාජ මාධ්‍ය / අන්තර්ජාලය මඟින් සෑම විටම ඔබව පොළඹවන්නේ යහපත් දේ කිරීමටයි.

   c. අතීතයේ ඔබ සෙවූ යමකට අදාළව ආකර්ෂණීය දැන්වීම් / යෝජනා තවමත් දිස් විය හැක.

   d. සමාජ ජාල, අපේ මොළයේ ක්‍රියාකාරීත්වය අවබෝධ කර ගෙන අවධානය ගැනීමට තැත් කරයි.

10. සබැඳි (ලින්ක්ස්) ක්ලික් කිරීමේදී හෝ ඇමුණුම් (ඇටෑච්මන්ට්ස්) ඩවුන්ලෝඩ් කිරීමේදී ඔබ සැලකිලිමත් විය යුත්තේ ඇයි?

   a. ඔබේ පරිගණකයට හානි කරන වෛරස් ඒවායේ තිබිය හැක.

   b. ඒවායේ නුසුදුසු දේවල් අන්තර්ගත විය හැක.

   c. ඒ හරහා ඔබේ පරිගණකයෙන් තොරතුරු සොරකම් කිරීමට ඉඩ ඇත.

   d. ඉහත සියල්ලම.

පිළිතුරු

(1-b, 2-b, 3-a, 4-d, 5-c, 6-c, 7-d, 8-a, 9-b, 10-d)

දේශ සීමා බාධක අවහිරතා මැඩ, ලෝකය තනි යායක් කිරීමට තොරතුරු තාක්ෂණය ඉටු කර ඇති කාර්යභාරය සුළුපටු නොවේ. විශ්ව ගම්මාන සංකල්පය, විශ්වීය පවුල් සංකල්පය අද දැස් අභිමුව යථාර්ථයක් බවට පත් වෙමින් පවතී. බැලූ බැල්මට විශ්ව ගම්මානය සුන්දර සංකල්පයකි.

ඒ අනුව ලෝකය තනි ගමකි. ගැටලුව එය නොවේ. ලංවෙන්ට, ලංවෙන්ට යහපත් දේ මෙන් ම අයහපත් දේත් සැණෙකින් බෝ වීමයි. විනාශකාරී වෛරසයක් වුව, සැණෙකින් පැතිරේ. ලෝකය තනි යායක් කරන සයිබර් අවකාශය ඔස්සේ නවීන දැනුම, ආදරය, කරුණාව, දයාව, මිත්‍රත්වය, මනුෂ්‍යත්වය වැනි උත්තරීතර දේ මෙන් ම මානසික වෛරස ද පැතිර යා හැකි ය. කොටින්ම ලෝක විනාශයට පාර කැපිය හැකි ය.

තොරතුරු තාක්ෂණික පහසුකම් පුළුල් කරන අතරේ ඒ පිළිබඳ විද්‍යානුකූල දැනුම මෙන් ම, එම පහසුකම් ආරක්ෂිතව පරිහරණය කිරීම පිළිබඳ දැනුම ද වැඩි වැඩියෙන් ලබා දීම ඉතා වැදගත් වේ. ඒ අනුව බලන විට 'හිතවතී' පළ කරන 'සයිබර් සුරැකුම්' ඉටු කරන්නේ මිල කළ නොහැකි කාර්යභාරයකි.

ආචාර්ය හසන්ත හෙට්ටිආරච්චි
විධායක අධ්‍යක්ෂ
ස්වාධීන රූපවාහිනී මාධ්‍ය ජාලය

HITHAWATHI
www.hithawathi.lk
ISBN 978-624-5622-00-9
9 786245 622009