

# Cyber Guardian

Publication for your online safety



## සයිබර් ආරක්ෂාව පිළිබඳව රාජ්‍ය නිලධාරීන් පුහුණු කිරීම සඳහා පුද්ගලික අංශයේ සහාය

ශ්‍රී ලංකා සර්වි ආයතනය ශ්‍රී ලංකා තොරතුරු තාක්ෂණ කර්මාන්ත සම්මේලනය (FITIS) සහ ISE2 හි Colombo Chapter සමඟ වඩාත් ඵලදායී ගමනක් ආරම්භ කරමින් පසුගිය අප්‍රේල් 3 වන දින SLIDA හිදී අවබෝධතා ගිවිසුමක් අත්සන් කරන ලදී. මෙම ඉදිරිගාමී සහයෝගීතාව තුළින් ඉදිරි වසර දෙක තුළ රාජ්‍ය නිලධාරීන් 1000කට සයිබර් ආරක්ෂාව පිළිබඳ උපදේශනය සහ පුහුණු ලබාගැනීමේ අවශ්‍යතාව උදාවේ. එමගින් රාජ්‍ය ආයතන තුළ වඩාත් ආරක්ෂාකාරී දත්ත ක්‍රියාදාමයක් තුළින් සයිබර් ආරක්ෂණය උසස් මට්ටමට ගෙන ඒම අපේක්ෂාවයි.

දිනෙන් දින වර්ධනය වන සයිබර් ආරක්ෂණ අභියෝගයන් වළක්වා ගැනීමට මෙම සහයෝගීතාව වඩාත් ඵලදායී මාවතක් වනු ඇත. ශ්‍රී ලංකා තොරතුරු තාක්ෂණ කර්මාන්ත සම්මේලනය (FITIS) සහ ISE2 කොළඹ පරිච්ඡේදය සමඟ ඇතිකරගත් මෙම සහයෝගීතාව තුළින්, නවෝත්පාදන, දැනුම හුවමාරු කර ගැනීම සහ සාමූහික සවිබල ගැන්වීමේ සංස්කෘතියක් ඇති කිරීම ප්‍රවර්ධනය කරයි. මෙම අවබෝධතා ගිවිසුම සයිබර් ආරක්ෂණ අධ්‍යාපනය ප්‍රවර්ධනය කිරීම, දැනුවත්තාවය ඉහළ නැංවීම සහ වෘත්තීයමය භාවය පෝෂණය කිරීම සඳහා සර්වි ආයතනයේ කැපවීම අවධාරනය කරයි.

රාජ්‍ය නිලධාරීන්ට සහ සැපයුම්දාම පාර්ශවකරුවන්ට ඩිජිටල් අංශයේ මුහුණදෙන සංකීර්ණතා වලට විශ්වාසයෙන් සහ දරාගැනීමේ හැකියාවෙන් මුහුණදීමට ශක්තිය ලබාදෙනු ඇත. තාක්ෂණ රාජ්‍ය අමාත්‍ය කනක හේරත්, තාක්ෂණ අමාත්‍යාංශයේ ලේකම් ආචාර්ය ධර්මශ්‍රී කුමාරතුංග SLIDA හි අධ්‍යක්ෂ ජනරාල් නාලක කළුවැව, ශ්‍රී ලංකා එක්සත් ජනපද තානාපති කාර්යාලයේ ආර්ථික කටයුතු පිළිබඳ නිලධාරී ඇන්ඩ්‍රේ ජීන්, ශ්‍රී ලංකා සර්වි හි වැඩබලන සහාපති ජානක සම්පත්, එහි වැඩබලන ප්‍රධාන විධායක නිලධාරී ආචාර්ය. කනිෂ්ක කරුණාසේන, FITIS හි සහාපති ඉන්දික ද සොයිසා සහ ISE2 Colombo Chapter හි සහාපති සුජිත් ක්‍රිස්ටි සහ එහි ප්‍රධාන විධායක නිලධාරී ජයසිරි අමරසේන මහතා ඇතුළු පිරිසක් මේ අවස්ථාවට එක්වූහ.



### Policy// රාජකාරී කටයුතු සඳහා ඔබේ පෞද්ගලික පරිගණකය භාවිතා කළහැකිද?



රජයේ ආයතනයක් සිය සේවකයින්ට නිල රාජකාරී ඉටු කිරීම සඳහා ඔවුන්ගේ පෞද්ගලික ජංගම පරිගණක, ස්මාර්ට් දුරකථන සහ වැඩිලට් පරිගණක

යනාදී මෙවලම් භාවිතා කිරීමට අවසර ලබා නොදිය යුතු බව රාජ්‍ය ආයතන සඳහා තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය 4.3.22, තහවුරු කර ඇත. කෙසේ වෙතත්, ආයතනයේ තොරතුරු ආරක්ෂණ කමිටුව විසින් තීරණය කරනු ලබන විශේෂිත තත්වයන් යටතේ, තොරතුරු ආරක්ෂණ නිලධාරීන්ගේ අධීක්ෂණය යටතේ නිල රාජකාරී ඉටු කිරීම සඳහා තෝරාගත් සේවකයින්ට ඔවුන්ගේ පුද්ගලික මෙවලම් භාවිතා කිරීමට අවසර දිය හැකිය. එවැනි අවස්ථාවන්හිදී එම මෙවලම් ආයතනය තුළ ක්‍රමවත්ව ලියාපදිංචි කර ඒවා තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තියට අනුගත වන ලෙස ක්‍රියාවේ යෙදවීම අත්‍යවශ්‍යවේ. එනමුදු, කිසිදු තත්වයක් යටතේ ඉතා රහසිගත සහ රහසිගත ලෙස වර්ගීකරණය කර ඇති තොරතුරු සැකසීමට හෝ ගබඩා කිරීමට සේවකයින්ගේ පෞද්ගලික මෙවලම් භාවිතා කිරීමට අවසර නොදිය යුතුය.

නිල රාජකාරී ඉටු කිරීම සඳහා සේවකයින්ගේ පෞද්ගලික මෙවලම් භාවිතා කිරීමට අවසර දී ඇතිවිට, ඔවුන්ගේ පරිශීලක ගිණුම් සඳහා සීමිත වරප්‍රසාද ඇති බවටත්, ගිණුම් ශක්තිමත් මුරපද සහ බහු සාධක සත්‍යාපනයෙන් ආරක්ෂා කර ඇති බවටත්, ප්‍රති-අනිෂ්ට මෘදුකාංග ස්ථාපනය කර ඒවායේ ස්වයංකාරීය යාවත්කාලීන කිරීම් සක්‍රීය කර ඇති බවටත්, මෙහෙයුම් පද්ධති, උපයෝගීතා මෘදුකාංග සහ භාවිතා කරන අනෙකුත් යෙදුම් මෘදුකාංග වලටද බලපත් සහිත බවට සහ ඒවා යාවත්කාලීන කර ඇති බවටත් ආයතනය සහතික විය යුතුය.

වෝහාරික පරීක්ෂණයක් සිදු වන අවස්ථාවකදී, රාජකාරී කටයුතු සඳහා භාවිත වන පෞද්ගලික උපාංගවල ඇති පුද්ගලික සහ ආයතනික තොරතුරු විමර්ශනය කිරීමට හෝ පරීක්ෂණ කටයුතු සඳහා එම මෙවලම් රඳවා තබා ගැනීමට සහ නීතිමය අවශ්‍යතා මත රාජ්‍ය ආයතන හෝ පාර්ශවයන් වෙත නිකුත් කිරීමට ආයතනයට අයිතිය ඇත.

සිය පෞද්ගලික මෙවලම්වල ආරක්ෂාව මෙවලම් හිමිකරුගේ වගකීමක් විය යුතුය. උපාංගය භාවිතා කිරීම හේතුවෙන් පෞද්ගලික දත්ත හැකිවීම ඇතුළුව මෙවලම්වලට සිදුවන හානියක් හෝ අස්ථානගත වීමක් සඳහා ආයතනය වගකිව යුතු නොවේ.



# සයිබර් ආරක්ෂාව පිළිබඳ පුහුණුව ලැබූ රාජ්‍ය නිලධාරීන් හා මාධ්‍යවේදීන්ට සහතික පත් ප්‍රදානය කෙරේ.



සහතිකපත් ප්‍රදානය කිරීමේ උත්සවය SLIDA හි දී පැවැත්විණ. තාක්ෂණ රාජ්‍ය අමාත්‍ය කනක හේරත් මහතා මෙම උත්සවයේ ප්‍රධාන ආරාධිතයා ලෙස සහභාගිවිය. තාක්ෂණ අමාත්‍යාංශයේ ලේකම් ආචාර්ය. ධර්ම ශ්‍රී කුමාරතුංග. SLID හි අධ්‍යක්ෂ ජනරාල් නාලක කළුවැව, ශ්‍රී ලංකාවේ එක්සත් ජනපද තානාපති කාර්යාලයේ ඇන්ඩ්‍යා ෂීන්, -ශ්‍රී ලංකා සර්වි හි වැඩබලන සභාපති ජානක සමීපත්, එහි වැඩබලන ප්‍රධාන විධායක නිලධාරී ආචාර්ය. කනිෂ්ක කරුණාසේන, FITIS හි සභාපති ඉන්දික ද සොයිසා සහ ISC2 Colombo Chapter හි සභාපති සුජිත් ක්‍රිස්ටි මහතා ඇතුළු සම්භාවනීය පිරිසක් මෙම අවස්ථාවට එක්වූහ.



රාජ්‍ය ආයතනවල ප්‍රධාන තොරතුරු තාක්ෂණ නිලධාරීන්, සහකාර තොරතුරු තාක්ෂණ නිලධාරීන් ISO / AISO සඳහා ශ්‍රී ලංකා සර්වි ආයතනය සංවිධානය කළ සයිබර් ආරක්ෂණ පුහුණු පාඨමාලාවට සහභාගිවූ නිලධාරීන් සඳහා සහතිකපත් පිරිනැමීම පසුගියදා සිදුකෙරිණ. රාජ්‍ය ආයතන 37 ක නිලධාරීන් 60ක් මීට සහභාගිවූහ. මීට අමතරව, සයිබර් ආරක්ෂාව සහ සයිබර් ආරක්ෂාව සම්බන්ධ සිද්ධීන් මහජනතාවට එලදායි ලෙස වාර්තා කරන්නේ කෙසේද යන්න පිළිබඳව මාධ්‍යවේදීන් දැනුවත් කිරීමේ වැඩසටහනක් ද පැවති අතර ඊට එක්වූ මාධ්‍ය වේදීන් 40 දෙනෙකුට ද ඒ සඳහා මෙහිදී සහතික ප්‍රදානය කෙරිණ.

## AI සයිබර් ආරක්ෂාවට තර්ජනයක්ද?



ක්‍රියාකාරකම් සඳහා විවැනි දත්ත සයිබර් අපරාධකරුවන්ට ඉතා අගනා පසුබිමක් සකස්කරයි.

එපමණක් නොව, පුද්ගලයන්ගෙන් 42%ක් සංවේදී දත්තවල ආරක්ෂාව අවදානමට ලක් කරමින් ව්‍යාපාරික අරමුණු සඳහා AI මෙවලම්වලට රැකියා සම්බන්ධ තොරතුරු ඇතුළත් කරති. මෙමගින් ආයතනික ආරක්ෂාවට AI තර්ජනයක් වීමේ අවදානම මෙමගින් අවධාරනය කරයි.

ඌර්නෝග්‍රිකයින් ඔවුන්ගේ දෛනික ජීවිතයේ, ආහාර කළමනාකරණයේ සිට වෛද්‍ය උපදෙස් ලබා ගැනීම දක්වා, වැඩි වැඩියෙන් AI මෙවලම් භාවිතයට එක්කරගන්නා විට සයිබර් ආරක්ෂාව සහ වංචා අවදානම් පිළිබඳ අභියෝගයට ද මුහුණදීමට සිදුවිය හැකි බව. KPMG සමීක්ෂණ වාර්තාවක් මත පදනම් කරගනිමින් "Info security සඟරාව" පෙන්වා දෙයි. මේ අනාවරණය තුළින් AI යෙදුම්වල පවා ඇති විය හැකි දුර්වලතා ඉස්මතු කරයි. පාරිභෝගිකයින් මෙම පද්ධතිවලට සංවේදී තොරතුරු කැමැත්තෙන්ම ඇතුළත් කිරීමෙන් තමන් විසින්ම මේ සයිබර් තර්ජනයන්ට නිරාවරණය විය හැකිය. මෙය පුද්ගලයන් අනතුරට පත් කරනවා පමණක් නොව ව්‍යාපාරවලට සහ සමස්ත සයිබර් ආරක්ෂණ ක්‍රමවේදයටම බලපාන්නකි.

සයිබර් අපරාධකරුවන් දැනටමත් ඔවුන්ගේ ප්‍රහාරක ක්‍රම වැඩි දියුණු කිරීම සඳහා AI මෙවලම් භාවිතා කරයි. රහස්‍ය තොරතුරු බෙදා ගැනීමට පාරිභෝගික කැමැත්තෙන්ම ඉදිරිපත්වීම ඇවිලෙන ගිණිමහට පිදුරු දැමීමක් බව මෙම සඟරාව පෙන්වාදෙයි. Deepfake AI අනුකරණයන් වැනි වර්ධනය වෙමින් පවතින තර්ජන සමග සම්බන්ධ වූ විට සමාජයේ ඉදිරි සංවර්ධනයට වඩාත් පලදායීවූ තාක්ෂණයක් පිළිබඳ බලාපොරොත්තු බොදවී යනු ඇති බව වැඩිදුරටත් අවධාරණය කරයි.

මෙම සමීක්ෂණයෙන් පෙන්නුම් කරන ආකාරයට පාරිභෝගිකයින්ගෙන් සැලකිය යුතු කොටසක් AI මෙවලම් භාවිතා කරන විට, බොහෝ විට ප්‍රතිවිපාක ගැන නොසිතා අවදානම් හැසිරීම් වල යෙදෙන බවයි. තුනෙන් එකකට වඩා (38%) පිරිසක් මූල්‍ය තොරතුරු ඇතුළත් කරන බව පිළිගන්නා අතර 27% ක් ලිපිනයන් හෝ උපන් දින වැනි පුද්ගලික තොරතුරු පමණක් හෙළිකර ඇති බව පිළිගනී. අනන්‍යතා සොරකම්, මූල්‍ය වංචා සහ වෙනත් අපරාධකාරී

පරිශීලකයින් (59%) තාක්ෂණය පිළිබඳ දැනුමක් ඇති බව පැවසුවත්, බොහෝ දෙනෙක් තවමත් භයානක වංචාවලට ගොදුරු වෙති. විවැනි සිදුවීම් සඳහා පාරිභෝගිකයින්ට දොස් පැවරීම සාමාන්‍ය දෙයක් වී ඇත, නමුත් මූල්‍ය සේවා (25%), සෞඛ්‍ය සේවා (18%) සහ රාජ්‍ය (15%) වැනි අංශ සඳහා දැඩි නියාමනයක් සඳහා ඔවුහු පෙණී සිටිති. 20% ක් පමණ විශ්වාස කරන්නේ සියලුම අංශ එකම ප්‍රමිතියකට අනුකූල විය යුතු බවයි. කෙසේ වෙතත්, අවදානම් අවම කිරීම සඳහා දැනුවත්භාවයෙන් යුතුව ඩිජිටල් තාක්ෂණයන් භාවිතා කිරීමේ වගකීම පාරිභෝගිකයන්ද දරයි.