ISSUE NO 02

සැප්තැම්බර් 2023

# Cyber Guardian

Publication for your online safety

SRI LANKA CERT|CC
Sri Lanka Computer Emergency Readiness Team
Coordination Centre

DIGIECON SRI LANKA 2023-2030

**Warning**

## හැකර් වරුන්ගේ නවතම ඉලක්කය

# ජංගම දුරකථන

ජංගම දුරකථන, ටැබ් වැනි අතේ ගෙනයාහැකි උපාංග සයිබර් අපරාධ කරුවන්ගේ නවතම ඉලක්ක බවට පත්ව ඇති බව නවතම වාර්තා පෙන්වා දෙයි. ජංගම දුරකථන බුහුල වීම සහ බොහෝවිට පුද්ගලික දත්ත මුරපද ආයතනික තොරතුරු ඒවායේ අඩංගු කර තිබීම සයිබර් අපරාධකරුවන්ට මුරපද සොරකම් කිරීමට සහ පසුව සමාගම් ජාල වෙත ප්‍රවේශය ලබා ගැනීමට පහසු ප්‍රවේශයක් වී ඇති බව මෙම වතාවන් පෙන්වාදෙයි.

බොහෝ සමාගම් සේවකයන් තම ආයතනික ජාල වෙත ප්‍රවේශ වීම සඳහා තම ජංගම උපාංග භාවිතා කරයි. එය 39%ක් තරම් ඉහළ අගයක් ගෙන ඇතැයි ෆිනෑන්ස් ඔන්ලයින් සංඛ්‍යාලේඛන වාර්තාව පෙන්වාදෙයි. මෙම උපාංගයක් හැක් කිරීමෙන් සයිබර් අපරාධකරුවන්ට සමාගම් දත්ත වෙත ප්‍රවේශය ලබා ගැනීමට පහසුවෙන් ඉඩ සලසයි.

ජංගම උපාංග තුළ ඇති දත්ත බෙහෙවින් වැඩි බැවින් එය හැක් කළහොත් පරිශීලකයාට අයත් ක්‍රෙඩිට් කාඩ් තොරතුරු සමාජ මාධ්‍ය ගිණුම් ඇතුළු සංවේදී තොරතුරු වෙත ප්‍රවේශය ලබා ගැනීමට සහ එහි ඇති කැමරාවේ සහ මයික්‍රෆෝනයේ පාලනය අල්ලා ගැනීමෙන් රහස්‍ය සංවාදවලට ඇහුන්කන් දීමට හැකිවනු ඇත.

ජංගම උපාංග භාවිතා කරනන්ගෙන් සැලකිය යුතු ඉහළ ප්‍රමාණයක් අනාරක්ෂිත ජාල සහ ආයතනික ජාලයෙන් බැහැර අනාරක්ෂිත ස්ථාන හරහා (උදා: FreeWiFi) අන්තර්ජාලයට ප්‍රවේශවන අතර ඔවුන් ඉතා පහසුවෙන් හැකර්වරුන්ගේ ඉලක්ක බවට පත්වනු ඇත. ෆෝබ්ස් සඟරාව මෙම ප්‍රතිශතය 80% ලෙස සඳහන් කරයි.

එමෙන්ම අන්තර්ජාල වංචාවෙන් 70%කට ආසන්න ප්‍රමාණයක් ජංගම වේදිකාවන් හරහා සිදු වන බවයි ඔවුන් පවසන්නේ. බොහෝ ආයතන සමාගම් වැඩ සඳහා Bring your own device (BOYD) ප්‍රතිපත්තියක් තෝරා ගන්නා අතර හැකර්වරුන්ට පරිගණක උපාංගයට සහ එමඟින් සමාගම් ජාලයට ප්‍රවේශය ලබා ගැනීම ඇති ඉඩකඩ පහසුවී තිබේ.

# රැන්සම්වෙයාර් කප්පම් කරුවන්ගෙන් ප්‍රවේශම් වන්න

**Security**


රැන්සම්වෙයාර් යනු ද්වේශසහගත මෘදුකාංගයක් වන අතර කප්පම් මුදලක් ගෙවන තුරු පුද්ගලයෙකුගේ හෝ ආයතනයක දත්ත ඇපයට තබා ගනී. මෙම සයිබර් අපරාධයේදී පරිගණක ජාල, ජංගම උපාංග සහ සේවාදායක පරිගණක වල තොරතුරු වෙත ප්‍රවේශය අවහිර කර එම දත්ත නිදහස් කිරීම සඳහා වින්දිතයින්ට ගෙවීමක් සිදු කරන ලෙස බලපෑම් කරනු ලබයි.

සාමාන්‍යයෙන් ගෙවීම ඉල්ලනු ලබන්නේ බිට්කොයින් හරහාය. එනම් හිමිකරු සොයා ගැනීමට දුෂ්කර වූ ගුප්තකේත මගිනි.

රැන්සම්වෙයාර් ආසාදනය වීමෙන් ඔබ ඔබගේ උපාංග ආරක්ෂා කර ගන්නේ කෙසේද?

අයාචිත email පණිවිඩ වල හෝ නොදන්නා වෙබ් අඩවි වල ඇති සබැඳි ක්ලික් කිරීමෙන් වලකින්න. ඔබ අනිෂ්ට සබැඳි ක්ලික් කළහොත් ස්වයංක්‍රීය බාගත වීමක් ආරම්භ කළ හැකි අතර එමඟින් ඔබේ පරිගණකය ආසාදනය වීමට ඉඩ ඇත.

පුද්ගලික තොරතුරු හෙළි කිරීමෙන් වලකින්න: පුද්ගලික තොරතුරක් ඉල්ලා විශ්වාස නොකළ හැකි මූලාශ්‍රයකින් ඔබට ඇමතුමක්, කෙටි පණිවිඩයක් හෝ විද්‍යුත් තැපෑලක් ලැබුනහොත් පිළිතුරු නොදෙන්න. සැක සහිත ඊමේල් ඇමුණුම් විවෘත නොකරන්න, සැක සහිත පෙනුමැති ඇමුණුම් කිසිවක් විවෘත කිරීමෙන් වලකින්න. අවිශ්වාසවන්ත ආකාරයකින් ඔබ අතට පත්වූ USB හෝ වෙනත් ගබඩා මාධ්‍ය ඔබේ පරිගණකයට සම්බන්ධ නොකරන්න.

විශ්වාසනීය ඇමුණුම් පමණක් විවෘත කර බාගැනීම් සඳහා සත්‍යාපිත සහ විශ්වාසදායී වෙබ් අඩවි පමණක් භාවිතා කරන්න.සියලුම වැදගත් තොරතුරු Backup කරන්න. නිතිපතා ඒවා ඒවා ක්‍රියාකාරී දැයි පරීක්ෂා කරන්න.

ඔබේ මෙහෙයුම් පද්ධතිය සහ මෘදුකාංග නවතම ස්වයන්ක්‍රීයව ක්‍රියාත්මකවන පැච් සමඟ යාවත්කාලීනව තබා ගන්න. යාවත්කාලීන වෛරස් විරෝධී මෘදුකාංගයක් පවත්වා ගෙන යන්න, ක්‍රියාත්මක කිරීමට පෙර අන්තර්ජාලයෙන් බාගත කල සියලුම මෘදුකාංග ස්කෑන් කරන්න.

විද්‍යුත් තැපැල් ඇමුණුම් වලින් මැක්‍රෝ සබල කිරීමෙන් වළකින්න. සයිබර් ආරක්ෂණ දැනුවත් කිරීමේ වැඩසටහන් සඳහා සහභාගී වීමට සේවකයින් දැනුවත් කිරීම සහ දිරිමත් කිරීම සිදු කරන්න.

Confidential

# PASSWORD
## පෞද්ගලිකයි රහසිගතයි

සමාජයේ සෑම පුරවැසියකුම ඩිජිටල් සමාජයේ සාමාජිකයන් ලෙස සයිබර් ආරක්ෂාව සඳහා අනුගමනය කලයුතු මූලික වර්යාවන් කිහිපයක් කෙරෙහි මෙවර සයිබර් ආරක්ෂණ මාසයේ බොහෝ රටවල අවධානය යොමුව තිබේ. ශක්තිමත් මුරපද password භාවිතය මූලික කරුණකි. විටින් විට මුර පද වෙනස් කිරීම එකම මුරපදයක් සෑමට භාවිතා නොකිරීම, මුරපදයක් ශක්තිමත් බව සඳහා අවම වශයෙන් අක්ෂර සංඛ්‍යා සංකේත දහයකින් වත් සමන්විත වීම. ද්වි සාධක සත්‍යාපන two-factor authentication වලින් සම්න්විත වීම මේ අතර වේ.

එමෙන්ම තම මෘදුකාංග විටින්විට යාවත්කාලීන කිරීම Regular Software Updates හා ස්වයන්ක්‍රීයව යාවත්කිරීම් බලගැන්වීම, ආරක්ෂණ Firewalls and Network Security වලින් සන්නද්ධ වීම, ආරක්ෂිත වෙබ් අඩවි පමණක් පරිහරණය Secure Web Browsing සඳහා HTTPS සහිත වෙබ් අඩවියක් දැයි සැලකිලිමත් වීම, ඊමේල් භාවිතයේදී නන්නාදුනන ගොනු attachment, link වෙත පිවිසීමෙන් වැලකීම, නිරන්තරයෙන් Regular Backups තබාගැනීම වැනි කරුණු සාමාන්‍ය ජනතාවගේ සයිබර් ආරක්ෂාවට අතිශයෙන්ම වැදගත්වේ.

Risk

## සමාජ මාධ්‍ය - ඔබේ චරිත සහතිකයක්

අද බෙහෙවින් ජනප්‍රිය Facebook වැනි සමාජ මාධ්‍ය ඔබ භාවිතා කරන්නෙක් නම් අනිවාර්යයෙන්ම අවධානය යොමුකළයුතු කරුණු කීපයක් ඇත. Email ලිපිනය දුරකථන අංකය, ඡායාරූප වැනි ඔබගේ පීවිදත්ත තොරතුරු, බැලීමට හැක්කේ කාටද යන්න ඔබ විසින්ම තීරණය කළයුතුව තිබේ. එය මිතුරන් සඳහා පමණක් සකසා තිබීම වැදගත්වේ. ප්‍රසිද්ධියේ බෙදා ගැනීමට අකමැති ඡායාරූප හෝ වෙනත් අන්තර්ගතයන් ගැන විශේෂයෙන් සැලකිලිමත් විය යුතුවේ. සමාජ මාධ්‍ය තුළ ඔබ බෙදා ගන්නා තොරතුරු මගින් සමාජය ඔබ කුමන ආකාරයේ කෙනෙක් දැයි තීරණය කරනු ඇත. එය ඔබගැන ඔබවිසින්ම දෙන චරිත සහතිකයකි. ඔබට ලැබෙන ඔබ හිතන හැමදෙයක්ම එකතු කිරීමට පෙර දෙපාරක් හිතන්න

ඔබගේ තොරතුරු ප්‍රකාශ ඔබගේ ප්‍රතිරූපය පෙන්වන කැඩපතක් බැවින් අනාගතයේදී ඒවා ඔබට අවාසි ලෙස භාවිතා වීමට ඉඩ ඇතිබව සිතන්න. නව රැකියාවක් සොයන විට, අනාගත සේවා යෝජකයා ඔබ ගැන තොරතුරු සොයා ගන්නා පළමු ස්ථානය

Beware

# කාන්තාවන් සඳහා පමණයි

විශේෂයෙන්ම, ඔබ කාන්තාවක් ලෙස අන්තර්ජාලයේ සැරිසරන විට පුරුෂයෙකු නොවිඳින ආරක්ෂක ගැටළු සහ බාධක වලට මුහුණ පෑමට සිදු වේ. සයිබර් අවකාශය හරහා සිදුවන ලිංගික හිරිහැර කිරීම්, තර්ජනය කිරීම, අනවසරයෙන් පුද්ගලික ඡායාරූප සහ වීඩියෝ බෙදා හැරීම් ආදිය සයිබර් අවකාශයේ කාන්තාවන් මුහුණ දෙන ගැටළු කිහිපයකි. මේවා සයිබර් අවකාශයේ ස්ත්‍රී පුරුෂ සමාජභාවය මත පදනම් වූ අපයෝජනයන් ය.

ඔබ නැණවත් කාන්තාවක් ලෙස, සෑම විටම සයිබර් අවකාශයේ පවතින අන්තරායන් පිළිබඳව දැනුවත්ව සිටිය යුතු වන අතර, ස්ත්‍රී පුරුෂ සමාජභාවය මත පදනම් වූ සයිබර් අපයෝජනයන්ගෙන් ඔබව ආරක්ෂා කර ගැනීමට ඔබේ කුසලතා වර්ධනය කර ගත යුතුය. කාන්තාවක් ලෙස ඔබට මුහුණ පෑමට සිදු විය හැකි සයිබර් තර්ජන කිහිපයක් පහත දැක්වේ.

සයිබර් හිරිහැර කිරීම (Cyber bullying Cyber) යනු පුද්ගලයෙකු අපහසුතාවයට පත් කිරීමට, අපහාසයට පත් කිරීමට, තර්ජනය කිරීමට හෝ නිහඬ කිරීමට සමාජ මාධ්‍ය, ඊමේල් හෝ ජංගම දුරකථන භාවිතා කිරීමයි. ඔබට ෆේස්බුක්, වට්ස්ඇප්, වයිබර්, ඉන්ස්ටග්රෑම් සහ වෙනත් සමාජ මාධ්‍යක් හරහා පහත සඳහන් ගැටළු ඇතිවිය හැකිය.

ඩොක්සිං (Doxing)

ඩොක්සිං යනු ඔබේ නිවසේ ලිපිනය, දුරකථන අංකය, ඊමේල් ලිපිනය හෝ සේවා ස්ථානය වැනි ඔබේ පුද්ගලික තොරතුරු ඔබේ අවසරයකින් තොරව බෙදා හැරීමයි. එවැනි ඔබගේ පෞද්ගලික තොරතුරු අපරාධකරුවකුට ඔබව බිලැක්මේල් කිරීමට හෝ ඔබ මෙන් පෙනී සිටීමට භාවිතා කළ හැකිය.

සයිබර් ස්ටොකින් (Cyber-stalking)

සයිබර් ස්ටොකින් යනු ඔබට හිරිහැර කිරීමට හෝ ඔබ සමඟ සම්බන්ධතාවයක් ඇති කර ගැනීමට අන්තර්ජාලය හරහා ලබා ගත හැකි ඔබේ පෞද්ගලික දත්ත (ඔබේ මූල්‍ය කටයුතු, සමාජ සම්බන්ධතා තොරතුරු, පෞද්ගලික සහ වෘත්තීය ජීවිතය පිලිබඳ දත්ත, ඔබේ ගමන්බිමන් පිලිබඳ තොරතුරු ආදිය) රැස් කිරීමයි.

පළිගැනීම සඳහා අසභ්‍ය දර්ශන භාවිතය (Revenge porn)

Revenge Porn යනුවෙන් යනුවෙන් හඳුන්වන්නේ යම් කාන්තාවකගේ නිරුවත් හෝ අසභ්‍ය දර්ශන අන්තර්ජාලය හරහා බෙදා හැරීමයි. බොහෝවිට මෙවැනි සිදුවීම් වාර්තා වන්නේ හිටපු පෙම්වතුන් විසින් පළිගැනීමේ හෝ අපහාහ කිරීමේ චේතනාවෙන් මෙවැනි දෑ සිදුකරන බවයි.

මෙවැනි තර්ජනයන්ට මුහුණ දෙන්නේනම් එය සයිබර් හිරිහැරයකි. එවිට එම පුගලයන් බ්ලොක් කිරීම, අදාළ සමාජ මාධ්‍යට පැමිණිලිකිරීම, ඊටත් එහා ක්‍රියා මාර්ග වෙත පිවිසීමට නීතියේ පිළිසරණ පැතිය හැකිය.

---

මෙය බව සිතිය යුතුව තිබේ. මෙම අංශ වෙත දක්වන උනන්දුව සැලකිල්ල දැනුවත්භාවය මෙරට ඩිජිටල් සංවර්ධනය වඩාත් ආරක්ෂිතව ඉදිරියට යාමේ ඇති හැකියාව තීරණය කරනු ඇත.