ISSUE NO 01

AUGUST 2023

Cyber Guardian

Publication for your online safety

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

Policies

රාජ්‍ය ආයතන සඳහා ශක්තිමත් තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්තියක්

ඩිජිටල් ආරක්ෂාව වැඩි දියුණු කිරීම සහ සංවේදී තොරතුරු ආරක්ෂා කිරීම සඳහා ක්‍රියාකාරී ඉදිරි පියවරක් තබමින්, ශ්‍රී ලංකාවේ පරිගණක හදිසි ප්‍රතිචාර සංසදය (CERT) රාජ්‍ය ආයතන සඳහා පුළුල් තොරතුරු සහ සයිබර් ආරක්ෂණ ප්‍රතිපත්තියක් ඉදිරිපත්කොට තිබේ. රාජ්‍ය ආයතන සඳහා වූ තොරතුරු හා සයිබර් ආරක්ෂණ ප්‍රතිපත්තියට 2022 වසරේ අගෝස්තු මාසයේදී අමාත්‍ය මණ්ඩල අනුමැතිය ලැබුන අතර එය මේ වසරේ සිට ක්‍රියාත්මක කිරීමට තාක්ෂණ අමාත්‍යාංශය පියවරගෙන ඇත. ශ්‍රී ලංකා සර්ට් CERT මෙරට සයිබර් ආරක්ෂණ සිද්ධි සඳහා ප්‍රතිචාර දක්වන ආයතනය වන අතර සයිබර් ආරක්ෂාව සම්බන්දයෙන් වූ ප්‍රතිපත්ති නිර්මාණය හා සම්බන්ද සේවාවන් සපයන රාජ්‍ය ආයතනය ද වේ. මෙම සයිබර් ආරක්ෂණ ප්‍රතිපත්තිය සියලුම රාජ්‍ය ආයතන සඳහා බලපැවැත්වේ.

මූලික අරමුණු

සයිබර් තර්ජන සඳහා සූදානම
ශ්‍රී ලංකා CERT තාක්ෂණ අමාත්‍යාංශයේ සහයෝගීතාවයෙන්, සයිබර් තර්ජනවලට එරෙහිව රජයේ ආයතන සූදානම් කිරීමේ වැඩසටහනක් ක්‍රියාත්මක කරන අතර ඊට සයිබර් තර්ජන විශ්ලේෂණය, අවදානම් තක්සේරු කිරීම් සහ ක්‍රියාශීලී ආරක්ෂක පියවර ඇතුළත් වේ.

ප්‍රතිපත්ති රාමුව
රාජ්‍ය අංශ හරහා තොරතුරු සුරක්ෂිතතාව සඳහා පැහැදිලි මාර්ගෝපදේශ, ප්‍රමිතීන් සහ හොඳම භාවිතයන් ස්ථාපිත කිරීමට ශක්තිමත් ප්‍රතිපත්ති රාමුවක් සංවර්ධනය කොට ඇත. මෙම ප්‍රතිපත්ති රාමුව දත්ත ආරක්ෂාව, සිද්ධි සඳහා ප්‍රතිචාරය සහ ඊට ගන්නා ක්‍රියාමාර්ග ඇතුලත්වේ.

කුසලතා වර්ධනය
සයිබර් තර්ජන ඵලදායී ලෙස හඳුනා ගැනීමට සහ අවම කිරීමට අවශ්‍ය කුසලතා වලින් රාජ්‍ය සේවකයින් සන්නද්ධ කිරීම සඳහා පුහුණු සහ කුසලතා වර්ධනය කිරීමේ වැඩසටහන් ක්‍රියාත්මක කෙරේ. මෙම ක්‍රියාවලිය සයිබර් ආරක්ෂණ පිලිබඳ දැනුවත් කිරීමේ සංස්කෘතියක් බිහිකිරීම අපේක්ෂිතයි.

රාජ්‍ය-පෞද්ගලික අංශයේ සහයෝගීතාව
පුද්ගලික අංශය සහ ජාත්‍යන්තර සයිබර් ආරක්ෂණ ආයතන සමඟ සහයෝගීතාවය ශ්‍රී ලංකාවේ සයිබර් ආරක්ෂණ ක්‍රියාවලිය ශක්තිමත් කිරීමට යොදා ගැනේ. එය දැණුම හුවමාරුව, සයිබර් තර්ජන පිළිබඳ දැණුම බෙදා ගැනීම සහ දැනුවත්භාවය වර්ධනය කරනු ඇත.

රාජ්‍ය සංවිධාන සවිබල ගැන්වීම
මෙම ප්‍රතිපත්තිය ක්‍රියාත්මක කිරීම රජයේ දත්ත, සේවා සහ පුරවැසි තොරතුරු සුරක්ෂිත කිරීම සඳහා අත්‍යවශ්‍ය පියවරකි. එය ශ්‍රී ලංකාවේ ඩිජිටල් සංවර්ධන ක්‍රියාවලිය ශක්තිමත් කරන අතරම සයිබර් සිදුවීම් සඳහා ප්‍රතිචාර දැක්වීමට ක්‍රියාශීලි සම්බන්ධීකරණ, වැඩපිළිවලක් සහතික කරයි.

පුරවැසියන් සමඟ සම්බන්ධ වීම
සයිබර් ආරක්ෂාව සම්බන්ධයෙන් ක්‍රියාකාරී භූමිකාවක් ඉටු කිරීමට ශ්‍රී ලංකා CERT පුරවැසියන් දිරිමත් කරයි. සැක සහිත සබැඳි ක්‍රියාකාරකම් වාර්තා කිරීම සහ ආරක්ෂිත ඩිජිටල් පුරුදු පුහුණු කිරීම ජාතික සයිබර් ආරක්ෂාව පවත්වා ගැනීම සඳහා අත්‍යවශ්‍ය වේ.

ශ්‍රී ලංකා CERT සහ තාක්ෂණ අමාත්‍යාංශය අතර ඒකා බද්ධ ප්‍රයත්නය තුලින් සයිබර් ආරක්ෂණය සඳහා රජයේ කැපවීම අවධාරනය කරයි. මෙම ප්‍රතිපත්ති ක්‍රියාත්මක කිරීමෙන් සහ සයිබර් සුපරීක්ෂාකාරී සංස්කෘතියක් පෝෂණය කිරීමෙන්, ශ්‍රී ලංකාව ආරක්ෂිත ඩිජිටල් රටක් ලෙස සහතික වනු ඇත.

Security

Virus Guards
පරිගණක ආරක්ෂාවට ඩිජිටල් මුරකරුවෙක්

සීඟ්‍රයෙන් ඉදිරියට යන තාක්ෂණික පරිවර්තන තුළ, ඔබේ ඩිජිටල් ජීවිතය සුරක්ෂිත කිරීම සඳහා පරිගණක වෛරස් ආරක්ෂකයින් අත්‍යාවශ්‍යව ඇත. බොහෝ විට ප්‍රති-වයිරස මෘදුකාංග හෝ ආරක්ෂක කට්ටල ලෙස හඳුන්වන මෙම වැඩසටහන් පරිගණක වෛරස්, හානිකර මෘදුකාංග සහ සයිබර් තර්ජන පැමිණීමට පෙර එරෙහිව පුර්වගාමී ආරක්ෂකයන් ලෙස සේවය කරයි.

වෛරස් ආරක්ෂකයින්, ඔබේ පරිගණකය අඛණ්ඩව අධීක්ෂණය කරයි, නිරන්තරයෙන් හානිකර මෘදුකාංග හඳුනා ගැනීම සහ ඒවා ක්‍රියාත්මක වීම වළක්වයි. නව තර්ජන පැමිණීම වැලැක්වීමට සහ හඳුනාගත් තර්ජන ඉවත් කිරීමට ආරක්ෂාව සැපයීම යාවත්කාලීන කරයි. වෛරස් ආරක්ෂක මෘදුකාංග පැවතියත්, පරිශීලකයන් සැක සහිත වෙබ් අඩවි සහ ඇමුණුම් මඟහරවා ගනිමින් ප්‍රවේශම්කාරීව අන්තර්ජාලය භාවිතා කිරීම වැදගත්වේ. විශේෂයෙන්ම ව්‍යාපාර රාජ්‍ය ආයතන, සංවේදී දත්ත ආරක්ෂා කර ගැනීම වැදගත්වන්නේ එය ඔවුන්ගේ කීර්තිය නාමය පවත්වා ගැනීමටද හේතුවක් වන බැවිනි.

කෙටියෙන් කියතොත් Virus Guards යනු ඩිජිටල් මුරකරුවන් වන අතර, දිනෙන් දින වර්ධනය වන ඩිජිටල් ලෝකයේ ඔබගේ උපාංග සහ දත්ත ආරක්ෂා කරයි.

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

Risk

අනාරක්ෂිත භාහිර දත්ත ගබඩා දෘඩාංග භාවිතයේ අවදානම

ඩිජිටල් පහසුකම් බුක්තිවිඳින ඔබ අනිවාර්යයෙන්ම, දත්ත හුවමාරු කිරීම සඳහා බාහිර දත්ත ගබඩා දෘඩාංග භාවිතා කරනු ඇති. කෙසේ වෙතත්, ඒ නිසා ම එහි ඇති අවදානම පිළිබඳවද ඔබගේ අවධානය යොමුකිරීම වැදගත්.

බාහිර දත්ත ගබඩා දෘඩාංග ධාවකයන්, තොරතුරු දත්ත එහා මෙහා ගෙනයාමට පහසුවක් වුවත් එමගින්ම ඔබගේ මෘදුකාංග සහ දත්ත වලට හානි සිදුවීමට ඇති ඉඩකඩද වැඩිවී ඇත. මෙම බාහිර දත්ත ගබඩා දෘඩාංග ධාවක සමග විනාසකාරී වෛරස් ගමන් කිරීමෙන් ආරක්ෂිතව පැවති ඔබගේ පරිගණකවලට සම්බන්ධ කළ විට, එහි ඇති ඔබේ ගොනු සහ සංවේදී තොරතුරු අනතුරට ලක්වේ.

පොදු අවදානම්

අහිතකර Malware මෘදුකාංග මගින් හානියට ලක්වූ බාහිර දත්ත ගබඩා දෘඩාංග ධාවක භාවිතාවෙන් වෛරස්, Ransomware හෝ ඔත්තු මෘදුකාංග Spyware එක් උපාංගයකින් තවත් උපාංගයකට පැතිර යා හැකි අතර එමගින් සැලකිය යුතු හානියක් සිදු වේ.

දත්ත සොරකම් කිරීම

ඔබගේ බාහිර දත්ත ගබඩා දෘඩාංග ධාවකයක් නැතිවීම හෝ සොරකම් කිරීම මගින් ලෙහෙසියෙන්ම ඔබසතු රහස්‍ය දත්ත වෙනත් කෙනෙකු අතට පත්විය හැකි අතර, එමගින් ඔබගේ පුද්ගලික තොරතුරු හෝ ආයතනික තොරතුරුවල රහස්‍ය භාවය නැතිවිය හැකියි.

අවදානම් අවම කිරීම

අවදානම් අවම කිරීම සඳහා ඔබට විශ්වාසනීය සහ ප්‍රමිතියෙන් යුතු බාහිර දත්ත ගබඩා දෘඩාංග පමණක් භාවිත කරන්න. සැමවිටම අහිතකර වෛරස සහ පැරණි වයිරස් ඉවත්කිරීම සඳහා ස්කෑන් කරන්න. බාහිර දත්ත ගබඩා දෘඩාංග තුළ ඇති සංවේදී දත්ත ආරක්ෂිතව තබා ගැනීමට ඒවා සංකේතනය Encrypt කිරීම සලකා බලන්න. සේවකයින් හෝ පවුලේ අය අතර මේවායේ ආරක්ෂාව පිළිබඳ දැනුවත් කිරීම ප්‍රවර්ධනය කරන්න. සුපරීක්ෂාකාරීව සහ ආරක්ෂිත භාවිත පිළිවෙත් අනුගමනය කිරීමෙන්, ඔබට ඔබගේ ඩිජිටල් උපාංග හා සම්බන්ධ අවදානම් අවම කර ගත හැකියි.

Protect

සයිබර් අවකාශයේ ඔබගේ පෞද්ගලිකත්වය ආරක්ෂා කරගන්නේ කොහොමද?

ඔබගේ විද්‍යුත් තැපෑල සහ අනෙකුත් සම්බන්ධතා තොරතුරු ප්‍රසිද්ධියේ බෙදා නොගන්න.

ඔබගේ සමාජ මාධ්‍ය ගිණුම්වල සෙටින් පරීක්ෂා කරන්න; දුරකථන අංකය, බෙදා ගත් තොරතුරු, ඡායා රූප වැනි ඔබගේ පීවදත්ත තොරතුරු බැලිය හැක්කේ කාටද? එය මිතුරන්ට පමණක් බලා ගත හැකි ලෙස සැකසීමට වගබලා ගන්න.

සෑම කෙනෙකුටම බලා ගැනීමට අවශ්‍ය නොවන ඡායා රූප හෝ වෙනත් අන්තර්ගතයන් සම්බන්ධයෙන් විශේෂයෙන් ප්‍රවේශම් වන්න. අන් අය සම්බන්ධ තොරතුරු බෙදා ගැනීමේදීද ප්‍රවේශම් වන්න. ඔබ ඔබේ මිතුරන්ගේ සහ පවුලේ ඡායා රූප සම්පූර්ණයෙන්ම නාඳුනන අය සමඟ බෙදා ගන්නේ නම් ඔවුන්ට මේ ගැන කුමන ආකාරයේ අදහසක් ඇති වේදැයි සිතා බලන්න.

ඔබ සමාජ මාධ්‍ය වල පළ කරන සහ බෙදා ගන්නා දේ තුළින් ඔබේ පොදු ප්‍රතිරූපය නිරූපනය වන බව සිතන්න. නව රැකියාවක් සොයන විට, යම් සේවා යෝජකයකු ඔබ ගැන තොරතුරු සොයා ගන්නා පළමු ස්ථානය මෙය බව සිතන්න.

ඔන්ලයින් ප්‍රශ්නාවලිය සහ තරඟ පැවැත්වීම ගැන සැලකිලිමත් වන්න. මේවා හානිකර නොවන විනෝදයක් ලෙස පෙනෙන්නට පුළුවන. නමුත් ඔවුන් ඔබ ගැන, ඔබේ රුචිකත්වයන් ආදී දේවල් ලබාගෙන අලෙවිකරණ සමාගම්වලට විකුණන බව දැනගන්න. ඔවුන්ගේ අරමුණ මුදල් ඉපයීමයි.

ඔබගේ නොවන පරිගණක උපාංගයක් භාවිතා කරන්නේ නම්, incognito ප්‍රවේශයකින් එය භාවිතා කිරීම ප්‍රවෙසම්කාරී වේ.

යෙදුම් බා ගැනීමේදී, ස්ථාන සේවා, ලිපින (දුරකථන ලැයිස්තුව), ඡායාරූප සහ වීඩියෝ ආදිය වෙත ප්‍රවේශය ලබා දෙන ලෙස ඔබෙන් නිතර අසනු ඇත. ප්‍රවේශය ලබා දීමට පෙර මොහොතක් සිතා බලන්න - මෙම යෙදුමට ප්‍රවේශය තිබීම ඇත්තෙන්ම අවශ්‍යද?

යම් අවස්තාවක ඔබට හිංසාකාරී පණිවිඩවල ඡායා රූප ලැබෙන්නේනම් ඒවායේ ස්ක්‍රීන් ෂොට් එකක් ගෙන වාර්තා කරන්න.

Global

ඇමෙරිකාවේ සයිබර් ආරක්ෂාව පිළබඳ දැනුවත් කරන්න මාසයක විශේෂ වැඩසටහන්

2004 වසරේ සිට ඔක්තෝම්බර් සයිබර් ආරක්ෂාව පිළිබඳ මාසය ලෙස අමෙරිකානු කොන්ග්‍රසය විසින් ප්‍රකාශයට පත්කොට තිබේ. ඒ අනුව මෙම මාසය තුළ ඩිජිටල් ආරක්ෂාව පිළිබඳ දැනුවත් කිරීම සහ පුද්ගලික දත්ත ඩිජිටල් ආකාරයේ අපරාධ වලින් ආරක්ෂා කර ගැනීමේ වැදගත්කම දැනුවත්කිරීම සඳහා ඇමෙරිකානු රාජ්‍ය සහ පෞද්ගලික අංශ එක්ව සිටියි.

දත්ත නීති කඩකිරීම් මෙන්ම හැකර්ප්‍රහාර පිළිබඳව බොහෝ පුවත් ඇමෙරිකාව තුළ පළවනු දක්නට ඇති නමුත් දත්ත ආරක්ෂා කර ගැනීමට අවශ්‍ය සියලුම ආකාරයේ ක්‍රමවේදයන් ඇති බැවින් ඉන් පසුබට නොවන ලෙස ඔවුහු ඉල්ලා සිටිති. මේ නිසා වැදගත්ම දෙය සයිබර් ආරක්ෂාව පිළිබඳ වූ දැනුවත් භාවය බව ඇමෙරිකානු සයිබර් ආරක්ෂාව හා ඒ පිළබඳ වූ යටිතල පහසුකම් ඒජන්සිය CISA අවධාරණය කරයි.

මේ වසරේ මහජන දැනුවත් කිරීමේදී පහත කරුණු කෙරෙහි අවධානය යොමුකිරීමට ඔවුන් තීරණය කර ඇත.

- ශක්තිමත් මුරපද සහ මුරපද කළමනාකරණය (Use strong passwords and a password manager)
- බහු සාධක සත්‍යාපනය ක්‍රියාත්මක කිරීම (Turn on multifactor authentication)
- තතුබෑම් හඳුනාගෙන වාර්තා කිරීම (Recognize and report phishing)
- මෘදුකාංග යාවත්කාලීන කිරීම වැදගත්කම (Update software)

published By CERT Media