ISSUE NO 04

NOVEMBER 2023

Cyber Guardian

A Publication on Online Safety

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

SECURITY

Online සාප්පු යන්න පෙර මේ ගැනත් හිතන්න.

අද අපේ රටෙත් වැඩිපුර ම තරුණ අය අතර online ක්‍රමයට භාණ්ඩ මිලදී ගැනීම ජනප්‍රියයි. මේ උත්සව සමයේ විවිධ මිල අඩුකිරීම් වැනි වෙළෙඳ උපක්‍රම වැඩිවන නිසා සයිබර් අපරාධකරුවන් බොහෝ විට ඔන්ලයින් සාප්පු යන්නන් ඉලක්ක කර ඔවුන්ගේ මුදල් හෝ ඔවුන්ගේ පුද්ගලික තොරතුරු සොරකම් කිරීම වැඩිවිය හැකියි. ඔවුන් මෙය කරන්නේ ව්‍යාජ සරල වෙබ් අඩවි පිහිටුවීම, නොපවතින නිෂ්පාදන විකිණීම, ඔවුන්ට අවශ්‍ය නොවන පුද්ගලික සහ ගෙවීම් තොරතුරු ඉල්ලා සිටීම සහ ඔබේ උපාංගයේ අනිෂ්ට මෘදුකාංග malawar ස්ථාපනය කිරීම ඇතුළු විවිධ ක්‍රම හරහා ය. මේ නිසා ඔබ අන්තර්ජාලය හරහා සාප්පු සවාරි යාමේදී අවදියෙන් සිටීම සහ ආරක්ෂිතව සිටීම වැදගත් වේ.

සයිබර් අපරාධකරුවෙකුට ඔබේ මූල්‍ය තොරතුරු සහ මුදල් ලැබුණු පසු ඔබට ඔබේ මුදල් ආපසු ලබා ගැනීමට අපහසුය. ඔබේ භාණ්ඩ කිසිදා නොපැමිණීම ගැන ඔබ කලකිරීමට පත්වනවා පමණක් නොව, ඔබ භාණ්ඩ සඳහා ගෙවූ මුදල්ද ඔබට අහිමි වනු ඇත.

අන්තර්ජාල සාප්පු සවාරි සඳහා පුද්ගලික උපාංග (උදා: ස්මාර්ට් ෆෝන්, ටැබ්ලට්, පරිගණක සහ ලැප්ටොප්) භාවිතා කරන විට සිතිය යුතු බොහෝ දේ ඇත. ඔබගේ සබැඳි සාප්පු සවාරි අත්දැකීම සුරක්ෂිත බව සහතික

කර ගැනීමට පහත ආරක්ෂක ඉඟි අනුගමනය කරන්න.

ආරක්ෂිත උපාංග භාවිතයෙන් භාණ්ඩ මිලදී ගැනීම් කරන්න. ඔබ සබැඳි සාප්පු සවාරි සඳහා භාවිත කරන උපාංගවල නවතම යාවත්කාලීන ස්ථාපනය කර ඇති බවත් විශ්වාසදායී ජාලයකට සම්බන්ධ වී ඇති බවත් සහතික කර ගන්න. උදාහරණයක් ලෙස, පොදු Wi-Fi වෙනුවට ඔබේ නිවසේ Wi-Fi හෝ (4G / 5G) සෙලියුලර් භාවිතා කරන්න. ඔබගේ ගෙවීම් තොරතුරු සහ ගිණුම් ආරක්ෂා කරන්න. විශ්වාසවන්ත විකුණුම්කරුවන් භාවිතා කරන්න.

අනතුරු ඇඟවීමේ සංඥා දැන ගන්න.

ඉතා අඩු මිල ගණන්, සෘජු බැංකු තැන්පතු හරහා ගෙවීම්, සහ ඉතා අලුත් හෝ බෙදාහැරීම්, ආපසු පැමිණීම සහ පෞද්ගලිකත්ව ප්‍රතිපත්ති පිළිබඳ සීමිත තොරතුරු ඇති අන්තර්ජාල වෙළඳසැල් සියල්ල වංචාවක සලකුණු විය හැකි බව සිහිතබා ගන්න.

ආරක්ෂිත ගෙවීම් ක්‍රම භාවිතා කරන්න

සෘජු බැංකු තැන්පතු, මුදල් මාරු කිරීම් හෝ බිට්කොයින් වැනි ඩිජිටල් මුදල් වලින්

කිසි විටෙකත් නොගෙවන්න. මන්ද මේ ආකාරයෙන් යවන ලද මුදල් නැවත ලබා ගැනීම දුස්කරවුවකි. ඔබ PayPal මගින් හෝ ඔබේ ක්‍රෙඩිට් කාඩ්පතෙන් ගෙවිය යුතුය.

වංචනිකයන්ට හසු නොවන්න. සැක සහිත සම්බන්ධතා වාර්තා කරන්න

සබැඳි ඇණවුම් ගැන ඔබට ලැබෙන අමුතු දුරකථන ඇමතුම්, පණිවිඩ හෝ ඊමේල් ගැන දැනුවත් වන්න. එය ඔබගේ පුද්ගලික හෝ මූල්‍ය තොරතුරු බෙදා ගැනීමට ඔබව පොළඹවා ගැනීමට උත්සාහ කරන කෙනෙකු විය හැකිය. ඔබට මතක නැති ඇණවුමක් ගැන යමෙකු ඔබව සම්බන්ධ කර ගන්නේ නම්, එය වංචාවක් විය හැකිය. සම්බන්ධතාව නවත්වා පරීක්ෂා කිරීමට ඔවුන්ගේ නිල වෙබ් අඩවියේ විස්තර භාවිතා කරමින් ගබඩාව වෙත ළඟා වන්න.

ව්‍යාජ බෙදාහැරීම් වංචා ගැන විමසිල්ලෙන් සිටින්න

ඔබේ භාණ්ඩ පැමිණෙන තෙක් ඔබ බලා සිටින අතරතුර ඔබේ ආරක්ෂාව අඩු නොකරන්න. සයිබර් අපරාධකරුවන්ට අනිෂ්ට මෘදුකාංග බාගත කිරීමට හෝ ඔබේ පුද්ගලික තොරතුරු ලබා දීමට ඔබව රැවටිය හැකි සබැඳි සමඟ ව්‍යාජ පාර්සල් බෙදා හැරීමේ දැනුම් දීම් යැවිය හැක. ඔබට එවැනි පණිවිඩයක් ලැබෙන්නේ නම්, සබැඳිය ක්ලික් නොකරන්න. පණිවිඩය වහාම මකන්න.

Services

ඩිජිටල් ෆොරෙන්සික්ස් DIGITAL FORENSICS

අධිකරණ කටයුතුවලදී අවශ්‍ය ඩිජිටල් සාක්ෂි අනාවරණය කර ගැනීමට සහ විශ්ලේෂණය කිරීමට සහාය වීම ශ්‍රී ලංකා CERT ආයතනය සතු තවත් වැදගත් කරය භාරයකි. ඒ සඳහා විශේෂඥ දැනුමැති පිරිසක් අති නවීන ක්‍රම අනුව විමර්ශන සේවා සැපයීමට සුදානම්ව සිටිති.

සංකීර්ණ සයිබර් සිද්ධීන්, දත්ත කඩකිරීම් සහ අනවසර ප්‍රවේශයන් පිළිබඳ සිද්ධි විසඳීමේදී පුද්ගලයන්ට සහ සංවිධානවලට ශ්‍රීලංකා CERT සහාය වෙයි. අපගේ අධිකරණ වෝහාරික විශේෂඥයින් විවිධ මූලාශ්‍රවලින් ඩිජිටල් දත්ත ලබා ගැනීමට, සංරක්ෂණය කිරීමට සහ විශ්ලේෂණය කිරීමට අති නවීන මෙවලම් සහ ක්‍රමවේද භාවිතා කරයි. එය සයිබර් ප්‍රහාරයක මූලාශ්‍රය හඳුනා ගැනීම, මකා දැමූ ගොනු ප්‍රතිසාධනය කිරීම හෝ නීතිමය ක්‍රියාදාමයන්හිදී විශේෂඥ සාක්ෂි ඉදිරිපත් කිරීම සඳහාවූ විශ්වාසදායක සේවාවකි.

අපගේ ඩිජිටල් අධිකරණ වෛද්‍ය සේවා සමඟින්, ඔබට ඩිජිටල් සිදුවීම් පිළිබඳ තීරණාත්මක අවබෝධයක් ලබා ගැනීමට, සුදුසු ක්‍රියාමාර්ග ගැනීමට, සහ ඔබේ සමස්ත සයිබර් ආරක්ෂණ ක්‍රියාවන් වැඩිදියුණු කිරීමට හැකිය. payment device fraud act හා සම්බන්ධ විමර්ශන වලදී ඩිජිටල් වෝහාරික පරීක්ෂණ සඳහා සහබාගිවීම, විද්‍යුත් තැපෑල සම්බන්ධ ඩිජිටල් අධිකරණ වෝහාරික, විමර්ශන, CCTV වීඩියෝ දර්ශන වැඩිදියුණු කිරීම්, දත්ත ප්‍රතිසාධනය, හා දත්ත විනාස කිරීම වැනි අවස්ථාවල සාක්ෂි විමර්ශනයට සහායවීම මෙමගින් සිදුකෙරේ.

Hot Line -101

report@cert.gov.lk

www.cert.gov.lk
www.onlinesafety.lk

අන්තර්ජාලයේ අතරමන් නොවන්න

ව්‍යාප පණිවුඩවලින් ආරක්ෂා වන්න.

ව්‍යාප පණිවිඩ ගැන අවදියෙන් සිටීම අන්තර්ජාලය තුල ඔබව ආරක්ෂා කර ගැනීමට හොඳ ක්‍රමයකි. පණිවිඩය නීත්‍යානුකූල නොවිය හැකි යැයි ඔබ සිතන්නේ නම් එවැනි සබැඳි මත ක්ලික් නොකරන්න. බොහෝ විට, වංචාකරුවන් ඔබ විශ්වාස කරන පුද්ගලයෙකු හෝ සංවිධානයක් ලෙස පෙනී සිටියි.

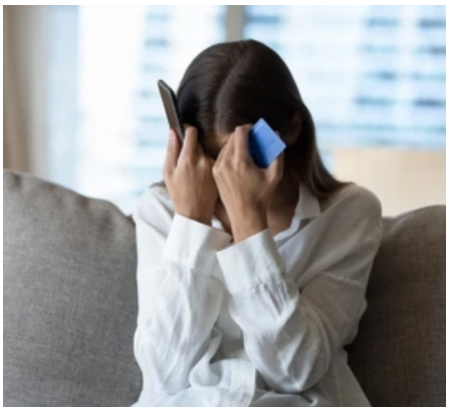
ඔබ බලාපොරොත්තු වූ දෙයට වඩා වෙනස් link to folder දිගුවක් තිබේ නම් ගොනු බාගත නොකරන්න (උදාහරණයක් ලෙස, ඔබ PDF හෝ ඉමේජ් එකක් අපේක්ෂා කරන විට exe හෝ .msi වලින් අවසන් වන ගොනුවක්).

විශ්වාසදායක නොවන මූලාශ්‍රවලින් ඔබේ ඊමේල්වල එන ඉමේජ් වෙත පිවිසීමෙන් වලකින්න. වයිරස් වලට එම පින්තූර හරහා සම්බන්ධ විය හැකිය. ඔබ භාවිතා කරන වැඩසටහනේ සැකසුම් හෝ විකල්ප වලදී මෙය අක්‍රිය කළ හැක.

නීත්‍යානුකූල යැයි පුළුල් ලෙස නොදන්නා තෙවන පාර්ශවීය බාගැනීම් අඩවි වලින් යෙදුම් බාගත නොකරන්න. ඒ වෙනුවට ඔබගේ උපාංගය සඳහා නිල බාගතකිරීම් ගබඩාව භාවිතා කරන්න. උදාහරණයක් ලෙස, Apple App Store, Google Play Store හෝ Microsoft Store යෙදුම් බාගත කිරීම සඳහා සබැඳි දැන්වීම් මත ක්ලික් නොකරන්න, සහ දැන්වීම් අවහිර කිරීමේ මෘදුකාංග භාවිතා කරන්න.

peer-to-peer ජාල වලින් යෙදුම් බාගත කර ස්ථාපනය නොකරන්න; ගොනු වෙනස් කළේ කවුදැයි ඔබට කිසිදා දැනගත නොහැක. ඊමේල් හෝ ක්ෂණික පණිවිඩවල ඇති සබැඳි ක්ලික් නොකරන්න, හෝ ඇමුණුම් නීත්‍යානුකූල බව ඔබට විශ්වාස නම් මිස ඒවා ක්‍රියාත්මක නොකරන්න.

අනිෂ්ට පණිවිඩ වලින් ඔබව ආරක්ෂා කර ගැනීමට අයාචිත තැපැල් spam filter පෙරහන භාවිතා කරන්න. ඔබට සේවාවකට හෝ ගිණුමකට ලොග් වීමට අවශ්‍ය නම්, නීත්‍යානුකූල නොවන සබැඳියක් ක්ලික් කරනවාට වඩා කෙලින්ම ඔවුන්ගේ වෙබ් අඩවියට පිවිසෙන්න. සම්බන්ධතා වලින් ලැබෙන යෙදුම්, ඊමේල් හෝ USB ස්ටික් හරහා ලබාගන්නා දේවල් පළමුව ඔබේ ප්‍රති-වයිරස යෙදුමෙන් ඒවා පරිලෝකනය නොකර ස්ථාපනය නොකරන්න.



පුද්ගලික දත්ත (Data) කියන්නේ මොනවද?

අද බොහෝ දෙනෙක් පුද්ගලික දත්ත ආරක්ෂාව ගැන කතා කරනවා. ඇත්තටම මේ ගැන ඔබ දන්නවද?

එය ව්‍යවහාර බසින් වඩාත් සරලව මෙසේ ප්‍රකාශ කළ හැකියි. යම් පුද්ගලයෙකු හඳුනාගත හැකි ඕනෑම දෙයක් දත්තයක් ලෙස වන අතර එයට නම, හඳුනා ගැනීමේ අංකය, ස්ථාන දත්ත ඇතුළත් වන අතර භෞතික, කායික, ජානමය, මනෝවිද්‍යාත්මක, ආර්ථික, සංස්කෘතික හෝ සමාජ හඳුනා ගැනීම සඳහාවූ විශේෂිත සාධක ද ඇතුළත් වේ. දත්ත ආරක්ෂාව යනු පුද්ගලයෙකුගේ පුද්ගලික දත්ත නොදැන භාවිතා කිරීම, හුවමාරු කිරීම හෝ නඩත්තු නොකිරීම සහතික කිරීමේ අයිතියකි. මේ සඳහා වන සියලුම නීතිමය රැකවරණ 2022 අංක 09 දරණ පුද්ගලික දත්ත ආරක්ෂණ පනත මගින් සපයනු ලබයි.

මොකද්ද මේ VPN

විශ්වාසනීය නොවන ජාල හරහා අන්තර්ජාලයට සම්බන්ධවීමේදී සංවේදී තොරතුරු ආරක්ෂා කිරීම සඳහා ගුප්ත කේතනය cryptography කරන ලද VPN සම්බන්ධතා භාවිතා කරයි. මෙහිදී සැරිසරන දත්ත වල රහස්‍යභාවය හැකර්වරුන්ගේ පමණක් නොව, ඔබේ අන්තර්ජාල සේවා සැපයුම්කරුගේද ආරක්ෂා කිරීමට VPN මගින් ඔබේ තොරතුරු cryptography ගුප්තකේතනය කරයි.

මෙමගින් ඔබ මාර්ගගතව කරන සන්නිවේදන පිළිබඳ තොරතුරු නිරීක්ෂණය කිරීම සහ රැස් කිරීම අන් අයට අපහසු වන අතර පොදු ජාල Public Wi-Fi භාවිතා කරන විට ඔබේ ආරක්ෂාව වැඩි කරයි. VPN virtual private network එකක් භාවිතා කරන අතරම ඔබ සියලු ආරක්ෂක පැච් ලබා ගෙන ඇතිබව සහතික කිරීම සඳහා නවතම යාවත්කාලීන කිරීම් කාලීනව ස්ථාපනය කළ යුතු අතර ද්වි-සාධක සත්‍යාපනය දිගටම භාවිතා කල යුතුය.