කලාපය 03

Cyber Guardian

2024

Publication for your online safety

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

ජංගම Apps ඔබටම තර්ජනයක් වෙන්නේ කොහොමද ?

විශ්වාස කළනොහැකි මූලාශ්‍ර මගින් ලැබෙන ජංගම දුරකථන සඳහා වූ Apps භාවිතා කිරීමේදී ඒවායේ මූලයන්, ක්‍රියාකාරිත්වය හා සත්‍යාපනය වැනි කරුණු ගැන සැලකිලිමත් නොවුන හොත් ආරක්ෂක අවදානමකට මුහුණදීමට ඔබට සිදුවණු ඇත. මෙම යෙදුම් පරිශීලකයින්ට හානි කිරීමට, පුද්ගලික දත්ත සොරකම් කිරීමට, හෝ උපාංගයේ ආරක්ෂාවට හානි කිරීමට නිර්මාණය කරණු ලැබේ. එමනිසා විශ්වාස කළනොහැකි ජංගම යෙදුම් මොනවාද සහ ඒවායින් ඇති වන අවදානම් මොනවාද යන්න පිළිබඳ දැනුමක් ලබාගැනීම වැදගත්.

ව්‍යාජ ජංගම Apps ලක්ෂණ

1. නොදන්නා හෝ තහවුරු නොකළ මූලාශ්‍ර

මෙවැනි Apps නිලවශයෙන් සපයන මූලාශ්‍ර **(Google play store,Apple app store)** මේවා බාගත කල නොහැකි අතර ඒ වෙනුවට තෙවන පාර්ශවීය වෙබ් අඩවිවල හෝ විකල්ප Apps ගබඩාවලින් සපයනු ලැබේ.

2. අවශ්‍ය ප්‍රමාණයට වඩා Permissions ඉල්ලීම්

සම්බන්ධතා, පණිවිඩ, ස්ථානය, කැමරාව සහ මයික්‍රෆෝනය වෙත ප්‍රවේශවීම වැනි ඒවායේ ක්‍රියාකාරිත්වය සඳහා අවශ්‍ය ප්‍රමාණයට වඩා ප්‍රවේශයන් මෙම Apps ඉල්ලා සිටිණු දක්නට පුළුවන් .

3. ද්වේෂ සහගත අරමුණු

මෙම Apps නිර්මාණයකර ඇත්තෙ අනිෂ්ට මෘදුකාංග, ඔත්තු මෘදුකාංග, ඇඩ්වෙයාර්, හෝ කප්පම් මෘදුකාංග පරිශීලකයාගේ උපාංගයට ඇතුල් කිරීමේ අරමුණෙනි.

4. පුද්ගලාරෝපණය හෝ ක්ලෝනකරණය

මෙම Apps නිත්‍යානුකූල Apps මෙන් ව්‍යාජ ලෙස පෙනිසිටිමින් පරිශීලකයන් රැවටීම සහ තොරතුරු සොරකම් කිරීම සිදුකරයි.

5. අනාරක්ෂිත කේතිකරණය (Insecure Coding)

අනාරක්ෂිත කේතනය කරන නිසා, මෙම Apps මගින් අනපේක්ෂිතව පරිශීලක දත්ත හෝ උපාංග දුර්වලතා හෙළිදරව් කරයි.මෙවැනි විශ්වාස කළනොහැකි ජංගම Apps භාවිතා කිරීම තුළින් බරපතල ආරක්ෂක අවදානම් ඇති කළ හැකිය. එවැනි යෙදුම් භාවිතා කිරීම හා සම්බන්ධ මූලික ආරක්ෂක ගැටළු හදුනා ගනිමු.

දත්ත සොරකම් කිරීම සහ රහස්‍ය තොරතුරු ආක්‍රමණය

පුද්ගලික තොරතුරු වෙත ප්‍රවේශය

මෙවැනි ව්‍යාජ Apps මගින් App සම්බන්ධතා, පණිවිඩ, ඡායාරූප, සහ ස්ථානය වැනි පුද්ගලික දත්ත වෙත ප්‍රවේශ වීමට අවසර ඉල්ලා සිටිය හැක.එමගින් එම දත්ත එකතු කර අනිසි ලෙස භාවිතා කළ හැකිය.

අනවසර දත්ත එකතු කිරීම

මෙම යෙදුම් පරිශීලක අනුමැතියකින් තොරව සංවේදී තොරතුරු රැස් කර ඒවා තෙවන පාර්ශවයන් සමඟ බෙදා ගත හැකි අතර, එය රහස්‍යතා කඩ කිරීම්වලට තුඩු දෙයි.

අනිෂ්ට මෘදුකාංග සහ ඔත්තු මෘදුකාංග

අනිෂ්ට මෘදුකාංග (Malicious Software)

මෙම ව්‍යාජ Apps වල වෛරස්, ට්‍රෝජන් සහ ඔත්තු මෘදුකාංග ඇතුළු අනිෂ්ට මෘදුකාංග අඩංගු විය හැකි අතර, ඒවා ඔබේ දුරකතනයට හානි කළ හැකි අතර දත්ත සොරකම් කිරීමට හෝ හානි කිරීමට හේතු විය හැක.

Keyloggers

මෙවැනි අනිෂ්ට යෙදුම් මඟින් මුරපද සහ අනෙකුත් සංවේදී තොරතුරු ඇතුළුව ඔබ ටයිප් කරන සෑම දෙයක්ම ග්‍රහණය කරගත හැකි keyloggers ස්ථාපනය කරනු ඇත.

මූල්‍ය අවදානම්

තතුබෑම් ප්‍රහාර (Phishing Attacks)

මෙවැන Apps මගින්, ක්‍රෙඩිට් කාඩ් විස්තර සහ බැංකු ශේසපත්‍ර වැනි මූල්‍ය තොරතුරු ලබාගැනීමට පරිශීලකයන් රවටා තතුබෑම් ප්‍රහාරවලට පහසුකම් සැලසිය හැක.

අනුමත නොකළ ගනුදෙනු

මෙම යෙදුම්වලට අනවසර ගනුදෙනු ආරම්භ කළ හැකි අතර, එමගින් ඔබගේ බැංකු තැම්පතු පැහැරගනු ඇත.

උපාංගය සහ ජාල සම්මුතිය

උපාන්ග සහ ජාල පද්ධති වෙත අනවසර ප්‍රවේශ

සමහර Apps ඔබගේ පරිගණක උපාංගයනට අනවසර ප්‍රවේශ ලබා ගැනීමෙන්, ප්‍රහාරකයන්ට ඔබේ උපාංගයේ පූර්ණ පාලනය ලබා දෙයි.

ජාල ප්‍රහාර

ව්‍යාජ Apps වලට ජාල සැකසීම් හැසිරවීමට හෝ ඔබේ ජාලයට ප්‍රහාර විල්ල කිරීමට, අනෙකුත් සම්බන්ධිත උපාංගවලට හානි කිරීමට හැකිය.

Ransomware

Data Encryption:

Ransomware යෙදුම්වලට ඔබේ දත්ත සංකේතනය කළ හැකි අතර එය මුදා හැරීම සඳහා කප්පම් මුදලක් ඉල්ලා සිටිය හැක, කප්පම් මුදල නොගෙවන්නේ නම් දත්ත අහිමි වීමට හේතු විය හැක.

අනන්‍යතා සොරකම

අනන්‍යතා ප්‍රයෝජනයට ගැනීම

මෙම Apps විවිධ සේවාවන් සඳහා අවශ්‍ය අනන්‍යතා සොරකම් කළ හැකි අතර, අනන්‍යතා සොරකම් කිරීමට සහ ඔබගේ හිණුම් වෙත අනවසරයෙන් ප්‍රවේශ වීමට එමගින් හැකිවේ. → Page 02

ආක්‍රමශීලී සහ අනවශ්‍ය දැන්වීම්

ආක්‍රමණශීලී දැන්වීම්

සමහර Apps මගින් අනිෂ්ට වෙබ් අඩවිවල ඇති කරදරකාරී සහ හානිකර විය හැකි ආක්‍රමණශීලී වෙළඳ දැන්වීම් යොමුකිරීමෙන් අනවශ්‍ය කරදර ඇතිවේ.

පරිගණක උපාංගවල ක්‍රියාකාරිත්වය අඩපනකිරීම.

සම්පත් ගලායම් අනිෂ්ට අප්ප්ස් මගින් ඔබගේ ජංගම

දුරකතනයේ ධාරිතාවන් විශාල ලෙස පරිහරණය කිරීම නිසා, ඔබේ උපාංගය මන්දගාමී කරයි සහ බැටරිය ඉක්මනින් බැසයයි.

ඔබව ආරක්ෂා වන්නේ කෙසේද

1. **නිල Apps බාගතකරගන්න**. Google Play Store සහ Apple Apps Store වැනි විශ්වාසදායක මූලාශ්‍රවලින් පමණක් යෙදුම් බාගතකරගන්න.
2. **Apps ප්‍රවේශයන් ගැන පරීක්ෂාකාරිවන්න**. Apps ඉල්ලා සිටින ප්‍රවේශයන් එහි ක්‍රියාකාරිත්වය සඳහා අවශ්‍යමද යන්න ගැන පරීක්ෂා කාරිවන්න.
3. **ප්‍රතිචාර සහ ශ්‍රේණිගත කිරීම් කියවන්න**. Apps එකේ විශ්වාසනීයත්වය මැන බැලීමට පරිශීලක සමාලෝචන සහ ශ්‍රේණිගත කිරීම් පරීක්ෂා කරන්න.
4. **ආරක්ෂක මෘදුකාංග ස්ථාපනය කරන්න**. ඔබගේ දුරකථනය, උපාංගය ස්කෑන් කිරීමට සහ ආරක්ෂා කිරීමට පිළිගත් ප්‍රති වයිරස සහ ප්‍රති-අනිෂ්ට මෘදුකාංග Apps යෙදුම් භාවිතා කරන්න.
5. **ඔබගේ ජංගම දුරකථනය යාවත්කාලීනව තබාගන්න**. අනාරක්ෂිතතා හඳුනා ගැනීමට ඔබගේ මෙහෙයුම් පද්ධතිය සහ Apps නිතිපතා යාවත්කාලීන කරන්න.
6. **සබැඳි සහ බාගත කිරීම් ගැන ප්‍රවේශම් වන්න**. සැක සහිත සබැඳි (Links) ක්ලික් කිරීමෙන් හෝ සත්‍යාපනය නොකළ මූලාශ්‍රවලින් යෙදුම් බාගතකිරීමෙන් වළකින්න.

සුපරීක්ෂාකාරිව සිටීමෙන් සහ ආරක්ෂක පියවර ගැනීමෙන්, ඔබට ව්‍යාජ ජංගම Apps හා සම්බන්ධ ආරක්ෂක ගැටළු සැලකිය යුතු ලෙස අඩු කළ හැකිය.

ETF නිලධාරීන්ට සයිබර් ආරක්ෂාව ගැන දැනුවත් කිරීමක්.

සේවා නියුක්තිකයන්ගේ භාර අරමුදල් මණ්ඩලයේ (ETF) **තෝරාගත් රාජ්‍ය නිලධාරීන් සඳහා සයිබර් ආරක්ෂාව පිලිබඳ දැනුවත්කිරීමේ වැඩසටහනක් පසුගියදා පැවැත්විණි. ශ්‍රී ලංකා තොරතුරු හා සන්නිවේදන තාක්ෂණ නියෝජිතායතනය** (ICTA) **මගින්, සංවිධානය කළ එකාබද්ධ ධාරිතා ප්‍රවර්ධන වැඩසටහන** (ICBA) **යටතේ** NextGenGov **ධාරිතා ප්‍රවර්ධානය කිරීමේ පදනම් වැඩසටහන** (NextGenGov Foundation Capacity Building Program) **සමග එක්ව මෙම දැනුවත්කිරීම සිදුකෙරිණ.**

Our Services

සයිබර් ප්‍රහාරවළින් මෘදුකාංග යෙදුම් ආරක්ෂා කර ගැනීම

පුළුල් ආරක්ෂක ක්‍රමවේද සහ අති නවීන තාක්ෂණය ඔස්සේ සයිබර් තර්ජනවළින් මෘදුකාංග යෙදුම් ආරක්ෂා කිරීම පිළිබඳව විශේෂඥ දැනුමෙන් අපි සන්නද්ධව සිටින්නෙමු. ඔබගේ යෙදුම්වලට විල්ලවිය හැකි අනතුරු හඳුනා ගැනීම සඳහා අප විසින් පුළුල් අවදානම් තක්සේරු, කේත සමාලෝචන සහ විනිවිදයෑම් පරීක්ෂණ පවත්වනු ලැබේ ඔබේ මෘදුකාංගය සයිබර් ප්‍රහාරවලට ඔරොත්තු දෙන බව සහතික කිරීම සඳහා ක්‍රියාකාරී ආරක්ෂාව කෙරෙහි අවධානය යොමු කරමින්, ශක්තිමත් ෆයර්වෝල්, ආක්‍රමණ හඳුනාගැනීමේ පද්ධති සහ සංකේතාංකන ප්‍රොටෝකෝල අප විසින් ක්‍රියාත්මක කරනු ලැබේ. අපගේ ප්‍රවීණයන් නවතම ආරක්ෂණ ප්‍රවණතා පිළිබඳව යාවත්කාලීන දැනුමෙන් සන්නද්ධව සිටින අතර, අඛණ්ඩ අධීක්ෂණ සහ සිදුවීම් සඳහා ක්ෂණික ප්‍රතිචාර සැපයීමේ හැකියාව අප සතු වේ. අප සමඟ ගොඩනගා

ගන්නා හවුල්කාරිත්වය තුළින්, පරිණාමය වන සයිබර් තර්ජනවළින් ඔබේ මෘදුකාංග යෙදුම් ආරක්ෂා වී ඇති බව සහ ඔබේ වටිනා දත්තවල අඛණ්ඩතාව සහ රහස්‍යභාවය ආරක්ෂා වී ඇති බව තහවුරු කරගත හැකියි.

- ජංගම යෙදුම් සඳහා අවදානම් තක්සේරුව -ඇන්ඩ්‍රොයිඩ් (Android), අයිඕඑස් (IOS), සහ හාමනි (Harmony)
- මෘදුකාංග යෙදුම්, වෙබ් යෙදුම් සහ ගෙවීම් ද්වාර සඳහා අවදානම් තක්සේරුව
- CBSL මාර්ගෝපදේශ යටතේ ගෙවීම් සම්බන්ධ ජංගමයෙදුම් සඳහා VAPT
- ආරක්ෂණය පිළිබඳ පුහුණුව සහ දැනුවත් කිරීම
- ආරක්ෂණ සිදුවීම්වලට ප්‍රතිචාර දැක්වීම

රාජ්‍ය නිලධාරීන් සඳහා ISC2 CC පුහුණු වැඩසටහනක්.

ශ්‍රී ලංකා සර්ට් CERT ආයතනය සහ ISC2 Colombo Chapter එක්ව, රජයේ නිලධාරීන් සඳහා පවත්වණු ලබන සයිබර් ආරක්ෂාව පිලිබඳ ISC2 CC පුහුණු වැඩසටහන පසුගියදා ශ්‍රී ලංකා සංවර්ධන පරිපාලන ආයතනයේදී ආරම්භ කරන ලදි.

මෙමගින් තෝරාගත් රාජ්‍ය නිලධාරීන් ISC2 CCසහතිකය ලැබීමට අවශ්‍ය පුහුණුව ලබනු ඇත. රාජ්‍ය අංශයේ සයිබර් ආරක්ෂාව වඩාත් විධිමත්ව පවත්වාගන යාමට අවශ්‍ය සහාය ලබාදීම මෙහි අරමුනයි. මේසඳහා ISC2 සහ ISC2 හි Colombo Chapter සහායවේ.

මෙම වැඩසටහන මගින් තෝරාගත් රාජ්‍ය නිලධාරීන් 1000ක් පුහුණු කිරීම හා ISC2 CC සුදුසුකම ලබා දීමට අවශ්‍ය කටයුතු සැලසුම් කර ඇත.