කලාපය 05

2024

Cyber Guardian

Publication for your online safety

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

ශ්‍රී ලංකාවට ජාතික සයිබර් ආරක්ෂණ මධ්‍යස්ථානයක්

තීරණාත්මක ඩිජිටල් යටිතල පහසුකම් සපයන රජයේ ආයතනවල සයිබර් ආරක්ෂාව තහවුරු කිරීම සඳහා සයිබර් ආරක්ෂණ මධ්‍යස්ථානයක් ස්ථාපිත කිරීමට ශ්‍රී ලංකා සර්ට් ආයතනය පියවර ගනිමින් සිටියි. මෙම මධ්‍යස්ථානය පිහිටුවීමෙන් පසු තීරණාත්මක යටිතල පහසුකම් සපයන ආයතන වෙත එල්ලවන සයිබර් ප්‍රහාර එම මොහොතේම හඳුනා ගැනීම හා ඒවාට ප්‍රතිචාර දැක්වීමට හැකිවේ.

මෙම මධ්‍යස්ථානය සඳහා අවශ්‍යවන මෘදුකාංග සහ දෘඩාංග දැනටමත් මිලදීගෙන ඇති අතර මෙහි අවසන් පියවර ලෙස සයිබර් ආරක්ෂණ සිදුවීම් නිරීක්ෂණ මධ්‍යස්ථානය පිහිටුවීමේ කටයුතු සිදුවෙමින් පවතී. මෙවන් සයිබර් ආරක්ෂණ මධ්‍යස්ථානයකින් **(SOC)** සයිබර් තර්ජන හඳුනා ගැනීම, සිදුවීම් කළමනාකරණය කිරීම, විශ්ලේෂණය කිරීම, සන්නිවේදනය කිරීම සිදුකරනු ලබන අතර සිදුවිය හැකි සයිබර් ප්‍රහාරයක් කල්තිය හඳුනා ගැනීමත් එමගින් සිදුවිය හැකි බලපෑම තක්සේරු කිරීමටත් හැකියාව ලැබේ. ඉදිරි වසර කීපය තුළ තීරණාත්මක ඩිජිටල් යටිතල පහසුකම් සපයන රාජ්‍ය ආයතන සඳහා මෙම සේවාව ලබාදීමට ශ්‍රී ලංකා සර්ට් අයතනය කටයුතු කරනු ලැබේ. සීඝ්‍රයෙන් ඩිජිටල්කරණය වන ශ්‍රී ලංකාවේ අනාගත වර්ධනීය අපේක්ෂාවන් සපුරාලීම සඳහා සයිබර් ආරක්ෂණ අංශයේ අබණ්ඩ සහය ශ්‍රී ලංකා සර්ට් ආයතනය මෙමගින් තවදුරත් තහවුරු කරයි.

හිත මිතුරු වෙසින් එන සයිබර් වංචාකාරයෝ

මිතුරුවෙසින් පැමිණ අන්තර්ජාලය හරහා සිදුකෙරෙන විවිධ සයිබර් වංචාවන් මේදිනවල බහුලව දක්නට ලැබේ. පුද්ගලික ඉල්ලීම ව්‍යාපාරික හා රැකියා තෑගි හා මුදල් දිනුම් මේ අතර වේ. මෙම සයිබර් වංචා කුමන ආකාරයෙන් ඔබවෙත පැමිණේදැයි වටහා ගැනීම වැදගත්.

1. ව්‍යාජ පැතිකඩ: Fake Profiles

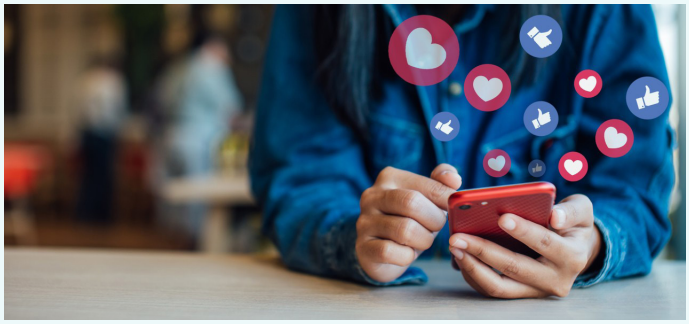
වංචාකරුවන් බොහෝ විට නීත්‍යානුකූලව පෙනී සිටීමට සොරකම් කරන ලද ඡායාරූප, නම් සහ වෙනත් විස්තර භාවිතා කරමින් සැබෑ පුද්ගලයන් ලෙස පෙනෙන ව්‍යාජ සමාජ මාධ්‍ය පැතිකඩ නිර්මාණය කරයි. මෙම පැතිකඩ සැබෑ පුද්ගලයින් හෝ සංවිධාන අනුකරණය කළ හැකිය නැතහොත් ඔවුන් හුදෙක් මිත්‍රශීලී ආගන්තුකයන් ලෙස පෙනෙන්නට පුළුවන.

2. මිතුරන්ගේ ඉල්ලීම්: Friend Request

ව්‍යාජ පැතිකඩ සැකසූ පසු මෙම වංචාකාරයන් විසාල වශයෙන් පරිශීලකයින් වෙත මිතුරු ඉල්ලීම් යවයි. ඉලක්කය වන්නේ ඔබේ පුද්ගලික තොරතුරු ලබාගැනීම සහ ඔබේ මිතුරන් ලැයිස්තුවට ඔවුන්ට ප්‍රවේශවීමට ඔබ මගින් අවස්ථාව උදාකර ගැනීමයි.

3. විශ්වාසය දිනාගැනීම: Gaining Trust

මිතුරු ඉල්ලීම පිළිගත් පසු වංචාකාරයා විශ්වාසය ගොඩනැගීම සඳහා ඔබ සමඟ අදහස් හුවමාරු කරගැනීමට පටන් ගනී. සම්බන්ධතාවය වඩාත් අව්‍යාජ බවක් පෙනෙන්නට ඔබේ ඡායාරූපවලට අදහස් දැක්වීම අගය කිරීම් වැනි දේවල් ඇතුළත් විය හැකිය.



4. තතුබෑම්: Phishing Attempt

විශ්වාසය තහවුරුවූ පසු ඔබට වැදගත් හෝ හදිසි දෙයක් යැයි කියමින් වංචාකාරයා ඔබට අනිෂ්ට සබැඳියක් malicious link සමඟ සෘජු පණිවිඩයක් එවිය හැකිය. පණිවිඩය "මෙම ඡායාරූප බලන්න!" වැනි දෙයක් විය හැක. හෝ "ඔබ ත්‍යාගයක් දිනාගෙන ඇත එයට හිමිකම් පෑමට මෙහි ක්ලික් කරන්න!"

එම සබැඳිය ෆෙස්බුක් වැනි ජනප්‍රිය සේවාවක ව්‍යාජ පිවිසුම් පිටුවකට සම්බන්ධ වන්නක් විය හැකිය. එහිදී ඔබේ පරිශීලක නාමය සහ මුරපදය ඇතුළත් කිරීමට ඔබෙන් අසනු ලැබේ. ඔබ එසේ කළහොත් වංචාකාරයා ඔබගේ සියලු තොරතුරු ග්‍රහනයට් ගනියි.

5. සූරාකෑම තවදුරත්

එම තොරතුරු හරහා ඔබේ පිවිසුම් විස්තර සමඟින් වංචාකාරයාට ඔබේ ගිණුමට ප්‍රවේශ වීමට වැඩි තොරතුරු සොරකම් කිරීමට සහ ඔබේ මිතුරන්ට තතුබෑම් පණිවිඩ phishing messages යැවීමට ඔබේ ගිණුම භාවිත කළ හැකි අතර වංචාව තවදුරටත් ව්‍යාප්ත කරයි.

මිතුරු වෙසින් එන තතුබෑම් වංචා වලින් (phishing) ඔබව ආරක්ෂා වෙන්නේ කෙසේද?

1. නොදන්නා ඉල්ලීම් ගැන ප්‍රවේශම් වන්න

ඔබ නොදන්නා කෙනෙකුගෙන් ඔබට මිතුරු ඉල්ලීමක් ලැබෙන්නේ නම් විශේෂයෙන් පැතිකඩ අලුත් නම් හෝ පළ කිරීම් පොස්ට් ඉතා අඩු නම් ප්‍රවේශම් වන්න. වංචාකරුවන් බොහෝ විට සැබෑ අන්තර්ගතයක් නොමැති ව්‍යාජ පැතිකඩ නිර්මාණය කරයි.

2. පැතිකඩ සත්‍යාපනය කරන්න Verify the Profile

ඉල්ලීම ඔබ දන්නා කෙනෙකුගේ සේ පෙනේ නම් එය නීත්‍යානුකූල බව සහතික කිරීමට ඔවුන්ගේ පැතිකඩ දෙවරක් පරීක්ෂා කරන්න. එහි ඇති වෙනත් ක්‍රියා කාරකම් සැබෑ වීවා දැයි පරීක්ෂා කරන්න. වෙනත් ක්‍රමයකින් මිතුරන් අමතා තහවුරු කරගන්න.

3. සැක සහිත සබැඳි ක්ලික් කිරීමෙන් වළකින්න

ඉල්ලීම ඔබ දන්නා කෙනෙකුගෙන් වුවද සබැඳි අඩංගු ඕනෑම අනපේක්ෂිත පණිවිඩයක් ගැන ප්‍රවේශම් වන්න විශේෂයෙන් පණිවිඩය අසාමාන්‍ය හෝ එම පුද්ගලයාට සබැඳියාවක් නොපෙනේනම් ඉවත්වන්න.

4. සැක සහිත ක්‍රියාකාරකම් වාර්තා කරන්න

මිතුරු ඉල්ලීමක් තතුබෑම් වංචාවක කොටසක් යැයි ඔබ සැක කරන්නේ නම් එම පැතිකඩ පිළිබඳව සමාජ මාධ්‍ය වේදිකා වට වාර්තා කරන්න. ඒමඟින් වංචාකාරයා යට තවදුරටත් අන් අය ඉලක්ක කිරීම වැළැක්වීමට උපකාරී වේ.

ශාරීරික ආරක්ෂාව වගේම සයිබර් ආරක්ෂාවත් වැදගත්

SCAM

අපි අපගේ ශාරීරික සෞඛ්‍යය ගැන සිතනවාසේම සයිබර් ආරක්ෂාව ගැන සිතීමද වැදගත්බව අන්තර්ජාතික සයිබර් ආරක්ෂණ සන්ධානය (The National Cybersecurity Alliance) පෙන්වාදෙයි. සයිබර් අවකාශයේ නිරෝගිබව ඔබේ සබැඳි හොඳින් පවතින බවට තවත් සහතිකයක් වනු ඇත.මිනිසුන් අත් සේදීම විටමින් ගැනීම හෝ ව්‍යායාම කිරීම වැනි පූර්වාරක්ෂාවන් ලබාගෙන සිටියදී පවා අසනීප විය හැකි සේම ඔබ සයිබර් ආරක්ෂණ හොඳම භාවිතයන් අනුගමනය කළත් ඔබේ සබැඳි පද්ධතිවලට පහර එල්ලවිය හැකියි. සයිබර් ඔරොත්තු දීමේ හැකියාව යනු ඔබ වඩාත් සුදුසු ක්‍රමෝපායන් ක්‍රියාත්මක කිරීමයි. එයට අමතර වෙළුම් පටියක් හෝ ශල්‍යකර්මයක් අවශ්‍ය විය හැකිය නමුත් ඔබට සුවය ලැබීමට එය හේතුවක් වනු ඇත. ඔබට සැලසුමක් තිබිය යුත්තේ එබැවිනි.

අද සයිබර් ආරක්ෂාව යනු සයිබර් ප්‍රහාරවලට ඔරොත්තු දීමේ සහ ප්‍රකෘතිමත් වීමේ හැකියාව මෙන්ම නව තර්ජනවලට අනුවර්තනය වීමේ හැකියාව අවධාරණය කරන තීරණාත්මක සංකල්පයකි. පුද්ගලයන්ට ව්‍යාපාරවලට සහ වෙනත් සංවිධානවලට ඔවුන්ගේම ඔරොත්තු දීමේ හැකියාව තක්සේරු කර ඔවුන්ගේ සයිබර් ඔරොත්තු දීමේ උපාය මාර්ග ශක්තිමත් කළ හැකිය.

සයිබර් ආරක්ෂණ ඔරොත්තු දීමේ හැකියාව අවබෝධ කර ගැනීම

සාමාන්‍යයෙන් සයිබර් ආරක්ෂණ ඔරොත්තුදීමේ හැකියාව යනු අත්‍යවශ්‍ය ක්‍රියාකාරකම් ආරක්ෂිතව පවත්වා ගැනීමට සහ සයිබර් සිදුවීම්වලින් ඉක්මනින් ප්‍රකෘතිමත් වීමට සංවිධානයකට ඇති හැකියාවේ කොඳු නාරටියයි. එය ක්‍රියාකාරී පියවර සිද්ධි ප්‍රතිචාර සූදානම සහ යතාතත්වයට පත්වීමේ ප්‍රතිසාධන උපාය මාර්ග ඇතුළත් වේ.

එලදායී ඔරොත්තු දීමේ හැකියාව ප්‍රහාරවල බලපෑම අවම කිරීමට අක්‍රිය කාලය අඩු කිරීමට සංවේදී දත්ත ආරක්ෂා කිරීමට පාරිභෝගික විශ්වාසය පවත්වා ගැනීමට සහ නියාමන අවශ්‍යතාවලට අනුකූල වීමට උපකාරී වේ. එය සංවිධානයේ කීර්තිය සහ මූල්‍ය ස්ථාවරත්වය ආරක්ෂා කරයි.

ඔබේ ඔබේම සයිබර් ඔරොත්තු දීමේ හැකියාව තක්සේරු කරන්න. අපි සාමාන්‍යයෙන් සංවිධාන සඳහා සයිබර් ආරක්ෂාව පිළිබඳ උපාය මාර්ග ගැන කතාකරන අතර පුද්ගලයෙකු ලෙස ඔබේ සයිබර් ඔරොත්තු දීමේ හැකියාව පිළිබඳ ඔබම ඇගයීම හොඳ අභ්‍යාසයකි. මෙය ඔබේ ව්‍යාපාරය ලාභ නොලබන සංවිධානයක් හෝ කණ්ඩායමක් ශක්තිමත් කිරීමේ සැලැස්මක් ආරම්භ කිරීමට පෙර පළමු පියවර විය හැකිය. ඔබේම ඩිජිටල් පුරුදු ආරක්ෂක භාවිතයන් සහ ඇතිවිය හැකි තර්ජන පිළිබඳ දැනුවත්භාවය සලකා බලන්න. ඔබෙන්ම මෙසේ අසන්න.

මම දිගු සංකීර්ණ සහ අද්විතීය මුරපද භාවිතා කරනවාද?

මම සෑම ගිණුමක් සඳහාම MFA බහු සත්‍යාපන සක්‍රීය කර තිබේද?

මම නිතිපතා මෘදුකාංග යාවත්කාලීන කරනවාද?

මම සැක සහිත සබැඳි ක්ලික් කිරීම හෝ නොදන්නා ඇමුණුම් බාගත කිරීම ප්‍රතික්ෂේප කරනවාද?

මම වැදගත් දත්ත උපස්ථ (Backup) කර සයිබර් සිද්ධියකදී එය යථාතත්වයට ප්‍රතිසාධන කරන්නේ කෙසේදැයි දන්නේද?

@ The National Cybersecurity Alliance

Pictuer Story

දකුණු පළාත් සයිබර් ආරක්ෂණ වැඩමුළුවක්

දකුණු පළාත් රාජ්‍ය නිලධාරීන් හා තොරතුරු තාක්ෂණ නිලධාරීන් සඳහා සයිබර් ආරක්ෂාව පිළිබඳ දැනුවත් කිරීමේ වැඩිදින වැඩමුළුවක් ගාල්ල දකුණු පළාත් කළමනාකරන හා සංවර්ධන මධ්‍යස්ථානයේදී පසුගියදා පැවැත්විණි. ශ්‍රී ලංකා සර්ට් ආයතනය සහ දකුණු පළාත් ප්‍රධාන ලේකම් කාර්යාලය එක්ව සංවිධානය කල මෙම වැඩමුළුවට 150 කට ආසන්න පිරිසක් සහභාගිවුහ.