කලාපය 06

2024

Cyber Guardian

Publication for your online safety

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

දත්ත සොරකම් නිසා වන පිරිවැය පාඩුවත් පාරිභෝගිකයන්ට දැරීමට සිදුවන බව IBM වාර්තාවක් කියයි.

ජූලි මාසයේදී IBM ආයතනය නිකුත් කරන ලද 2024 නවතම දත්ත කඩකිරීමේ වාර්තාවට අනුව සිදුවී ඇති පිරිවැය පාඩුව ඩොලර් මිලියන 4.88 කි. එය පෙර වසරට වඩා 10% ක විශාල වැඩිවීමකි. මෙම අධ්‍යයනය Ponemon අන්තර්ජාතික ආයතනය විසින් සිදු කරන ලද අතර IBM විසින් විශ්ලේෂණය කරන ලදී. එය ලොව පුරා ආයතන 604ක දත්ත කඩකිරීම්,සොරාගැනීම් පිළිබඳව පුළුල් අධ්‍යනයකි. ඔවුන් අභ්‍යන්තර තොරතුරු ලබා ගැනීම සඳහා මෙම දත්ත කඩකිරීම් වලට සොරාගැනීම් වලට මුහුණදුන් 3,500 කට අධික ආරක්ෂක සහ ව්‍යාපාරික ප්‍රජාවක් සමඟ සාකච්චාකර ඇත. මෙමගින් හෙළිවන වැදගත් කරුණක් වන්නේ මෙම අභිමිවූ පිරිවැය පාඩුව එම ආයතනවල භාණ්ඩ හා සේවා වෙත පැවරීමෙන් එහි පීඩනය පාරිභෝගිකයන්ට දැරීමට සිදුව ඇති බවයි. මේ වසරේ ව්‍යාපාරවලින් 63% ක් කියා සිටියේ දත්ත කඩකිරීම් හේතුවෙන් සිදුවූ පාඩුව පිරිමසා ගැනීමට මිල ඉහළ දැමීමට සිදුවන බවයි. පසුගිය වසරේ 57% ක වැඩිවීමට සාපේක්ෂව නිෂ්පාදන මිල අධික වීමට මෙම දත්ත අහිමිවීමේ පාඩුව හෙතුවිතිබේ. පද්දති අක්‍රිය කාලය වැඩිවීම සහ පාරිභෝගිකයින් වෙනත් ආයතන වෙත මාරුවීම වැනි හේතු නිසා සිදුවන පාඩුව මෙම මිල වැඩිකිරීම් වලට බලපා තිබේ. මෙම දත්ත පැහැරගැනීම් වලින් අඩකට ආසන්න (46%) ප්‍රමාණයක් සමාජ ආරක්ෂණ අංක Email දුරකථන අංක සහ නිවසේ ලිපින වැනි පාරිභෝගික පුද්ගලික තොරතුරු ඇතුළත් බව වාර්තාව අනාවරණය කරයි. බුද්ධිමය දේපල, වෙළඳ රහස් වැනි, සංවේදී දත්ත උල්ලංඝනය කිරීම් 43% කි.

මෙසේ දත්ත පහර ගැනීම්වලට එක් විශාල හේතුවක් වන්නේ ප්‍රමාණවත් සයිබර් ආරක්ෂණ කණ්ඩායම් නොමැති කමයි. සමීක්ෂණයට ලක් කරන ලද සමාගම්වලින් අඩකට වඩා කියා සිටියේ ඔවුන් තම ආරක්ෂක දෙපාර්තමේන්තුවල දැඩි කාර්ය මණ්ඩල හිඟයක් සමඟ පොරබදමින් සිටින බවයි. මෙම සමාගම් නව AI තාක්ෂණයන් අනුගමනය කිරීම අරඹා ඇති නමුත් දැනටමත් මෙම කණ්ඩායම් මත මත පැටවී ඇති පීඩනය දරාගත නොහැකි බවයි.

ඔබගේ Facebook ගිණුම Hack වෙලාද ?

ඔබගේ Facebook ගිණුම හැක් කර ඇත්නම්, ඔබගේ ගිණුම සුරක්ෂිත කිරීමට සහ ඔබගේ පුද්ගලික තොරතුරු ආරක්ෂා කිරීමට ඉක්මනින් ක්‍රියා කිරීම වැදගත් වේ. ඔබ අනුගමනය කලයුතු මූලික කරුණු මෙසේ සඳහන් කල හැකියි.

1. ඔබට තවමත් ඔබේ ගිණුමට ප්‍රවේශ විය හැකිදැයි පරීක්ෂා කරන්න.

ලොගින් වන්න: ඔබට සුපුරුදු ආකාරයට ලොග් වීමට උත්සාහ කරන්න. සාර්ථක නම්, වහාම ඔබගේ මුරපදය වෙනස් කිරීමට සහ ඔබගේ ගිණුම් සැකසීම් සමාලෝචනය කිරීමට ඉදිරියට යන්න. ඔබට ලොග් විය නොහැකි නම්, ඔබේ විද්‍යුත් තැපෑලෙන් හෝ දුරකථන අංකයෙන් ඔබේ මුරපදය යළි පිහිටුවීමට Facebook පිවිසුම් පිටුවේ ඇති “Forgot Password” විකල්පය භාවිතා කරන්න.

2. ඔබේ මුරපදය වෙනස් කරන්න.

ඔබට ඔබගේ ගිණුමට ප්‍රවේශ විය හැකි නම්, ඔබගේ මුරපදය ශක්තිමත් සහ ඔබටම ආවේනික ආකාරයකට වෙනස් කරන්න. පොදු මුරපද හෝ ඔබ වෙනත් වේදිකාවල භාවිතා කර ඇති ඕනෑම දෙයක් භාවිතා කිරීමෙන් වළකින්න.

ද්වි-සාධක සත්‍යාපනය සක්‍රීය කරන්න:

අමතර ආරක්ෂිත උපායක්ත ලෙස ද්වි-සාධක සත්‍යාපනය (2FA) සකසන්න. මේ සඳහා ඔබ නව උපාංගයකින් ලොග් වන සෑම අවස්ථාවකම ඔබගේ දුරකථනයට හෝ විද්‍යුත් තැපෑලට පණිවුඩයක් ලබාගැනීමට පොදු කේතයක් අවශ්‍ය වේ.

3. ඔබගේ Email ගිණුම පරීක්ෂා කර සුරක්ෂිත කරන්න.

Facebook හා සම්බන්ධ ඔබගේ Email Access ආරක්ෂිත බව සහතික කරගන්න. හැකර්වරුන් ඔබගේ විද්‍යුත් තැපෑලට ප්‍රවේශය ලබා ගතහොත් ඔවුන්ට ඔබගේ Facebook ගිණුම පාලනය කළ හැක. අවශ්‍ය නම්, ඔබේ විද්‍යුත් තැපැල් මුරපදය ද වෙනස් කර එහි ද්වි-සාධක සත්‍යාපනය සක්‍රීය කරන්න.

4. හැක් කිරීම ෆෙස්බුක් වෙත වාර්තා කරන්න.

Facebook හි Help Center හරහා වාර්තා කරන්න.එහි ඇති “hacked account.” මෙනුව සොයන්න. ඔබගේ ගිණුම අවදානමට ලක්ව ඇති බව වාර්තා කිරීමට එහි ඇති උපදෙස් අනුගමනය කරන්න.

ඔබට ඔබගේ ගිණුමට කිසිසේත්ම ප්‍රවේශ විය නොහැකි නම් හැක් කරන ලද ගිණුම් සඳහා Facebook හි support option සහාය විකල්ප භාවිතා කරන්න. හැඳුනුම්පතක් ඉදිරිපත් කිරීමෙන් ඔබේ අනන්‍යතාවය තහවුරු කරන ලෙස ඔවුන් ඔබෙන් ඉල්ලා සිටිය හැක.

5.ගිණුම් ක්‍රියාකාරකම් සමාලෝචනය කරන්න.

මෑත කාලීන login locations and devices බලන්න. ඔබ කිසියම් සැක කටයුතු ක්‍රියාකාරකමක් දුටුවහොත්, අනෙකුත් සියලුම සැසිවලින් ඉවත් වන්න (ඔබට මෙය security and Login settings හරහා කළ හැක). ඔබගේ Facebook ගිණුමට සම්බන්ධ කර ඇති නොදන්නා apps or services තිබේදැයි පරීක්ෂා කර ඒවා ඉවත් කරන්න.

6. ඔබේ සම්බන්ධතා වලට දන්වන්න.

ඔබේ ගිණුම හැක් කර ඇති බව ඔබේ සම්බන්ධතාවලට දන්වන්න. එමගින් හැකර් විසින් කරන ඕනෑම පණිවිඩයකට හෝ පෝස්ට් වලට ගොදුරු වීම වළක්වයි.

7.සැක සහිත ක්‍රියාකාරකම් සඳහා නිරීක්ෂණය.

පුද්ගලික තොරතුරු ඉල්ලා සිටින ඊමේල් හෝ පණිවිඩ Facebook වෙතින් එන බව පෙනුනත් ඒවා ගැන ප්‍රවේශම් වන්න. කිසියම් අසාමාන්‍ය ක්‍රියාකාරකමක් සිදුවනවාදැයි නිරන්තරයෙන් පරීක්ෂාකාරීව සිටින්න.

8. අමතර ආරක්ෂක පියවරයන් සලකා බලන්න.

සංවේදී තොරතුරු හෙළිදරව් වී ඇත්නම්, identity theft protection services සේවා භාවිතා කිරීම සලකා බලන්න.ඔබේ ගිණුම සුරක්ෂිතව තබා ගැනීමට ඔබේ ආරක්ෂක පියවර වරින් වර සමාලෝචනය කර යාවත්කාලීන කරන්න.

9. අනාගත හැක් කිරීම් වලක්වන්න.

සයිබර් භාවිතයේදී සෑමවිටම ශක්තිමත් මුරපද භාවිතාය, එකම මුරපදය අනෙකුත් වේදිකා සඳහා භාවිතා නොකිරීම, පුරුද්දක් ලෙස පවත්වාගනයාම වැදගත්වේ එමෙන්ම සැක සහිත සබැඳි ගැන ප්‍රවේශම් වන්න. ඊමේල් හෝ පණිවිඩවල ඇති සබැඳි නීත්‍යානුකූල බව ඔබට විශ්වාස නම් මිස ඒවා click නොකරන්න.මෙම පියවර ගැනීමෙන් ඔබට ඔබේ Facebook ගිණුමේ පාලනය නැවත ලබා ගැනීමට සහ අනාගත අනවසරයෙන් ඇතුළුවීමේ උත්සාහයන්ගෙන් එය ආරක්ෂා කර ගැනීමට උපකාරී වේ.

ඔබ සයිබර් අපරාධකරුවන්ගේ ඇමක් විය යුතු නැත.

තුබෑම්(Phishing)යනු වැරදි සබැඳියක් link ක්ලික් කිරීමට හෝ අනිෂ්ට ඇමුණුමක් බාගත කිරීමට ඔබව පොළඹවා ගැනීමේ අරමුණින් අපරාධකරුවන් ව්‍යාජ ඊමේල් සමාජ මාධ්‍ය පළ කිරීම් හෝ සෘජු පණිවිඩ භාවිතා කරමින් සිදුකරන සයිබර් වංචාවකි. ඔබ වැරදි තුබෑම් සබැඳියක් හෝ ගොනුවක් ක්ලික් කළහොත් ඔබ ඔබේ පුද්ගලික තොරතුරු සයිබර් අපරාධකරුවන්ට විවරකර දීමක් වනු ඇත. එමගින් තුබෑම් (Phishing) ක්‍රමයකට ඔබේ උපාංගයට අනිෂ්ට මෘදුකාංග ඇතුලත්විය හැකිය.

කෙසේ වෙතත් ඔබට ලැබෙන Email ලිපි වලට බිය විය යුතු නැත. වාසනාවකට මෙන් වංචනික විද්‍යුත් තැපෑලක් වළක්වා ගැනීම මේවනවිට පහසු වී ඇත. නමුත් එය රදාපවතින්නේ ඔබට ඒ පිලිබඳ ඇති අවබෝදය අනුවයි. යම් දැනුමක් ඔබට ඇත්නම් ඔබ මෙම සයිබර් වංචාකරුවන්ට (phishers) බියවීමට අවශ්‍ය නොවනු ඇත.

ඔබ එය Click ක්ලික් නොකල යුත්තේ ඇයිදැයි සිතන්න.

ඔවුන්ගේ උපක්‍රම සියුම් විය හැක නමුත් ඔබ තුබෑම් phishing උත්සාහයක් හඳුනාගත් පසු ඔබට එයට හසුනොවී සිටිය හැකිය. කිසියම් සබැඳියක් ක්ලික් කිරීමට හෝ ඇමුණුම් බාගත කිරීමට පෙර තත්පර කිහිපයක් ගත කර ඊමේල් නීත්‍යානුකූල එකක් දැයි සහතික කර ගන්න. එවැනි තුබෑම් විද්‍යුත් තැපෑලක් පැහැදිලිව හඳුනා ගන්නේ කෙසේද යන්න පිළිබඳ පහත උපදෙස් සැලකිල්කිලට ගන්න. එහි සඳහන් කරුණු කොතරම සත්‍ය දැයි සිතා බලන්න. එයට හදිස තැතිගන්වන හෝ තර්ජනාත්මක භාෂාවක් ඇතුළත් වේද?

එය වැරදි අක්ෂර විනයාසයන් සහ වැරදි ව්‍යාකරණ වළින් පිරී ඇති දුර්වල ලෙස සකස් කර ඇති ලියවිල්ලක්ද ?
සුබපැතුම් අපැහැදිලිදැ නැතහොත් ඉතා සාමාන්‍යද?

පුද්ගලික තොරතුරු ඉල්ලීම් එයට ඇතුළත්ද?

නුහුරු නුපුරුදු හයිපර්ලින්ක් (hyperlink) හෝ ඇමුණුමක් මත ක්ලික් කිරීමේ හදිසි අවශ්‍යතාවක් අවධාරණය කරයිද?

එය අමුතු හෝ හදිසි ව්‍යාපාරික ඉල්ලීමක්ද?

එවන්නාගේ විද්‍යුත් තැපැල් ලිපිනය සහ එහි සඳහන් සමාගමට ගැළපේ දැයි එකවිට හදුනාගත නොහැකි සරල අක්ෂර විනයාසයන් සමග සසඳන්න.

එවැනි ඊමේල් පණිවිඩයක් ව්‍යාප එකක් සහ අපරාධකරුවෙකුගේ තතුබෑම් ගවේෂණයේ කොටසක් බව හඳුනාගත් පසු ඔබ කළයුත්තේ කුමක්ද?.

ඔබ කාර්යාලයේ සිටී නම් සහ ඔබගේ කාර්යාල ඊමේල් ලිපිනයට විද්‍යුත් තැපෑල පැමිණියේ නම් හැකි ඉක්මනින් එය ඔබගේ තොරතුරු තාක්ෂණ කළමනාකරුට හෝ සයිබර් ආරක්ෂක නිලධාරියාට වාර්තා කරන්න.

විද්‍යුත් තැපෑල ඔබේ පුද්ගලික විද්‍යුත් තැපැල් ලිපිනයට පැමිණියේ නම් එය කියන දේ නොකරන්න. කිසිදු සබැඳියක් ක්ලික් නොකරන්න දායකත්වයෙන් ඉවත් වීමේ සබැඳිය (unsubscribe link) හෝ ඊමේල් වෙත ආපසු පිළිතුරු දීම හෝ නොකරන්න. එම මකන Delete බොත්තම භාවිතා කරන්න. මතක තබා ගන්න සබැඳි මත ක්ලික් නොකරන්න, Delete කරන්න.

ඔබට ඔබේ ආරක්ෂාව තවත් පියවරක් ඉදිරියට ගෙන ගොස් ඔබේ ඊමේල් වැඩසටහනෙන් යැවීමේ ලිපිනය අවහිර කළ හැක. Outlook ,Gmail ,Mac Mail,Yahoo හි ඇති sending address අවහිර කරන්න.

සමහර ඊමේල් වේදිකා ඔබට ඔබේ phishing තතුබෑම් උත්සාහයන් වාර්තා කිරීමට ඉඩ දෙයි. විද්‍යුත් තැපෑලක් ඔබේ තතුබෑමට උත්සාහ කරන බවට ඔබ සැක කරන්නේ නම් එය ඉක්මනින් වාර්තා කිරීම (report phishing attempts) වඩාත් සුදුසුය. තතුබෑම් පණිවිඩය ඔබේ කාර්යාල විද්‍යුත් තැපෑලට පැමිණියේ නම් ඔබේ තොරතුරු තාක්ෂණ දෙපාර්තමේන්තුවට හැකි ඉක්මනින් තත්ත්වය පිළිබඳව දන්වන්න.?@The National Cybersecurity Alliance

Picture Story

සයිබර් ආරක්ෂක පද්ධති පිළිබඳ ධාරිතා සංවර්ධන වැඩසටහනක් ගම්පහදී

රාජ්‍ය ආයතන සඳහා වන සයිබර් ආරක්ෂක පද්ධති පිළිබඳ ධාරිතා සංවර්ධන වැඩසටහනක් ගම්පහ දිස්ත්‍රික් ලේකම්/ දිසාපති ලලින්ද ගමගේ මහතාගේ ප්‍රධානත්වයෙන් පසුගියදා ගම්පහ දිස්ත්‍රික් ලේකම් කාර්යාලයීය ශ්‍රවණාගාරයේදී පැවැත්විණි.

ශ්‍රී ලංකා පරිගණක හදිසි ප්‍රතිචාර සංසදය (Sri Lanka CERT) ස්වදේශ කටයුතු අමාත්‍යංශය හා ඒකාබද්ධව සිදු කරනු ලබන මෙම වැඩසටහන සඳහා ගම්පහ දිස්ත්‍රික්කයේ ප්‍රාදේශීය ලේකම්වරුන් ඇතුලු තොරතුරු තාක්ෂණය හා සම්බන්ධ නිලධාරීන් පිරිසක් ඒක්ව සිටියහ.