හදිසි ආපදා තත්ත්වයක් හේතුවෙන් ලෝකයේ මොනම ආකාරයේ හෝ වගාවක් විනාශ වී ගියහොත්, නැවත වගා කිරීමට අවශ්‍ය වන බීජ ලබාගත හැකි රහසිගත Doomsday Vault එක ගැන ඔබ දන්නවා ද?

2020 වසර ලාංකිකයන් ඇතුළුව මුළුමහත් ලෝකයාටම එතරම් සුභ වසරක් නම් නොවන බව වසර ආරම්භයේ දී ම අපට දැකගන්න ලැබුණා. බොහෝ දෙනෙක් මේ වසර උදා නොවූවා නම්යැ යි සිතන මට්ටමට, මේ වසරේ සියලු ක්ෂේත්‍රයන් වෙත විශාල ගැටළු පැමිණියා. මේ වෙද්දී ලෝකයම කොරෝනා රෝග බියෙන් ඇළලී තිබෙන කාලයක, කවරදාකටත් වඩා පරිගණක ක්‍රීඩාවල වටිනාකම ලෝකය වෙත දැනෙමින් පවතිනවා. ස්වයං නිරෝධායනය වෙමින් නිවාස තුළට වී කාලය ගෙවන්නට සිදුව තිබෙන නිසා අනෙක් දිනවලට පරිගණක ක්‍රීඩා සඳහා එතරම් පෙළඹෙන්නේ නැති පුද්ගලයන් පවා ඒ වෙත යොමු වෙමින් සිටිනවා. කොහොම වුණත්, සියල්ලන්ටම මදි නොකියා ක්‍රීඩා කරන්නට හැකි තරමේ විවිධත්වයන්ගෙන් යුතු පරිගණක ක්‍රීඩාවන් රැසක් වසරේ පළමු කාර්තුව නිම වෙන්නත් පෙර නිකුත් වී අවසාන යි. මේ ලිපිය හරහා අපේ බලාපොරොත්තුව එවැනි ක්‍රීඩා කිහිපයක් පිළිබඳව ඔබට විස්තර ගෙන ඒමට යි.

ඔබ මීට පෙර Half-Life පරිගණක ක්‍රීඩා මාලාව පිළිබඳව අසා තිබෙනවා නම්, මුලින්ම මේ ඒ ක්‍රීඩාවේ තෙවැනි වෙළුම එහෙම නැතිනම්, Half-Life 3 නොවන බව කියන්නට ඕන. Half-Life විශ්වය පදනම් කරගෙනම නිර්මාණය වන වෙනස්ම ගණයේ පරිගණක ක්‍රීඩාවක් ලෙස යි මෙහි නිර්මාණකරුවන් එය හඳුන්වන්නේ. මෙය නිර්මාණය කරන Valve Corporation සමාගම නම් කියන්නේ, මේ ඔවුන්ගේ VR ආගමනය බව යි.

ෆ්‍රීමන් නම් පුද්ගලයෙක් වටා මේ කතාව දිවෙනවා. ඔහු අවදි වන්නේ වසර 20ක අසාමාන්‍ය නින්දකින් අනතුරුව යි. ඒ වෙද්දී පෘථිවිය Combine නම් පිටසක්වල අධිරාජයෙකු විසින් පාලනය කරමින් සිටිනවා. ඔහුට මේ ක්‍රීඩාව තුළ දී ඔහුගේ දුව (Alyx) ඇතුළු ඇගේ හිතවාදීන් පිරිසක් සමග ක්‍රීඩා කරන්න ලැබෙනවා. Half-Life 2 පරිගණක ක්‍රීඩාව හා සබැඳෙන ලෙසින් නිර්මාණය වී ඇති මේ ක්‍රීඩාව ඒ සිදුවීම්වලට වසර 5කට පෙර සිදුවීමක් ලෙස යි නිර්මාණය වී තිබෙන්නේ. ඔබ සතුවත් VR සහිත පරිගණක ක්‍රීඩා කන්සෝලයක් තිබේ නම් මේ ක්‍රීඩාව ඩොලර් 60ක් වැනි මිලකට ඔබට ලබාගන්න පුළුවන්. ඒ පරිගණක ක්‍රීඩාව වෙත සහාය දක්වන කන්සොල පිළිබඳව theverge සවිස්තරාත්මක ලිපියක් පළ කර තිබුණා. කොහොම වුණත්, 2007 සිට මේ ක්‍රීඩා මාලාව සමග එක්ව සිටින ක්‍රීඩකයන්ට මේ ඔස්සේ ඔවුන්ට තිබූ ගැටළු ගණනාවකට පිළිතුරු ලැබෙන බව නිර්මාපකයන් සඳහන් කර තිබුණා.

Doom 2016 පරිගණක ක්‍රීඩාවේ Reboot එකක් ලෙස මේ නව Doom Eternal පරිගණක ක්‍රීඩාව හඳුන්වන්න පුළුවන්. 2006 නිකුත් වූ Doom ක්‍රීඩාව අපූරු අත්දැකීමක් බව තමයි ක්‍රීඩකයන්ගේ නම් මතය. කිසිවිටක ක්‍රීඩාවෙන් ක්‍රීඩකයා ඉවතට නොයවා අපූර්ව පරිගණක ක්‍රීඩා අත්දැකීමක් ලබාදෙන්නට තරම් ඒ ක්‍රීඩාව සුවිශේෂී එකක් වුණා. පෙර ක්‍රීඩාවක අනුප්‍රාප්තික ක්‍රීඩාවක් වුවත්, සුවිශේෂී අන්දමෙන් එය ඉදිරිපත් කරන්නට නිර්මාපකයන්ට හැකිව තිබෙනවා. සාමාන්‍යයෙන් Reboot වන ක්‍රීඩාවක දකින්න ලැබෙන අංගයන්ට වඩා මේ ක්‍රීඩාව විශේෂ එකක් බවට පත් කරන්න ඔවුන්ට හැකිව තිබෙනවා. අමතර මෙහෙයුම්, වැඩි ග්‍රැෆික්ස් වගේම තවත් අංගයන් රාශියක් මෙයට එක් කිරීම නිසාවෙන්ම යි ඒ. මේ වසරේ බොහෝ දෙනෙක් මඟ බලා සිටි පරිගණක ක්‍රීඩාවක් බවට මෙය පත්ව එන්නේ නිතැතින්ම යි.

COD WAR ZONE එහෙම නැතිනම්, Call of Duty ක්‍රීඩාවේ Battle Royale ක්‍රීඩා ක්‍රමවේදයේ ආගමනය විදිහට මෙය හඳුන්වන්න පුළුවන්. Activision සමාගමේ නිර්මාණයක් ලෙස පසුගිය දිනෙක එළිදැක්ක මේ ක්‍රීඩාව සති කිහිපයක් ඇතුළත ක්‍රීඩකයන් සංඛ්‍යාවේ පෙරළිකාර වර්ධනයක් පෙන්නුම් කළා. Modern Warfare පරිගණක ක්‍රීඩාව මිල දී ගෙන සිටි ක්‍රීඩකයන්ට WAR ZONE ක්‍රීඩාව තරමක් කලින් අත්හදා බලන්නත් ඉඩ ලැබුණා. එලෙස ලබාදීම මේ ක්‍රීඩාව නිල වශයෙන් නිකුත් කරන්නටත් පෙර පරිශීලකයන් අතර ජනප්‍රිය වන්නට හේතුවක් වුණා. ඕනෑම අයෙකුට නොමිලයේ බාගත කරගෙන

ක්‍රීඩා කරන්න හැකි Free to play පරිගණක ක්‍රීඩාවක් ලෙස මෙය නිකුත් වුණා. ඒ වගේම, මෙහි තවත් විශේෂත්වයක් වන්නේ Cross Platform ක්‍රීඩාවක් ලෙස නිකුත් වීම යි. පරිගණකයක, Playstation එකක හෝ Xbox එකක වැනි ඕනෑම Platform එකක ක්‍රීඩකයන්ට එකට එක්ව මෙය ක්‍රීඩා කරන්න පුළුවන්.

Battle Royale සහ Plunder ක්‍රීඩා ක්‍රමවේදයන් මෙහි දී ඔබට ක්‍රීඩා කරන්න හැකි වෙනවා. එක ක්‍රීඩා තරගයකට Playersලා 150ක් ඇතුළත් වෙන අතරම, වෙන කිසිම BR ක්‍රීඩාවක නොමැති

නවතම අංගයන් ගණනාවක් WAR ZONE පරිගණක ක්‍රීඩාව වෙත ඇතුළත්. සති දෙකක් වැනි කාලයක් ඇතුළත මිලියන 30කට වැඩි ක්‍රීඩකයන් පිරිසක් මේ ක්‍රීඩාව වටා එක රොක් කරගන්නට මේ ක්‍රීඩාව සමත් වුණා. ඒ අතරට ලොව ජනප්‍රියම streamersලා පවා ඇතුළත්.

2019 වසරේ දෙසැම්බර් 12 වන දා සිට චීනයේ, වුහාන් නගරය මුල් කරගෙන පැතිරීම ආරම්භ වූයේයැ යි සැලකෙන කොරෝනා (COVID-19) වෛරසය පිළිබඳව අපි පෙර ලිපි ගණනාවකින් ඔබව දැනුවත් කර ඔබට මතක ඇති. මේ වෙද්දීත් ලෝකයේ ක්ෂේත්‍ර ගණනාවකට දැඩි බලපෑම් එල්ල කරන්නට මේ වෛරසයට හැකි වුණා. තාක්ෂණික ලෝකය වෙතත් මේ වෛරසයේ බලපෑම ඉතා තදින් දැනුණා. “තාක්ෂණික ලෝකයට වැළඳුණ කොරෝනා වෛරසය” නම් ලිපිය ඔස්සේ ලෝකය පුරා අතිශය ප්‍රචලිත සහ සුප්‍රකට සමාගම් / සන්නාමයන් වෙත දැඩි පාඩු සිදුකළ ආකාරය ගැන විග්‍රහ කෙරුණා. ඊට අමතරව මේ වසර පුරා පැවැත්වීමට නියමිතව තිබූ Google I/O, F8, Mobile World Congress වැනි සමුළු නවතා දමන්නට සිදුවීම ගැනත් එහි දී කතාබහ කෙරුණා.

මේ වෛරසයට එරෙහිව තවමත් නිසි ප්‍රතිකර්මයක් සොයාගන්නට ලෝකය අසමත්ව තිබෙනවා. මේ වෙද්දී රෝගය පැතිරීම ආරම්භ වූ බව සැලකෙන චීනය, මේ රෝගය ව්‍යාප්තිය තවදුරටත් අවම කරන්නට මිනිස් සේවකයන් වෙනුවට රොබෝවරුන්ගේ සහාය ලබා ගන්නවා.

තාක්ෂණය අතින් ලෝකයේ ප්‍රබලයෙකු ලෙස අවිවාදයෙන් සැලකෙන චීනය, මේ වෙද්දී මහජනතාවගේ සෞඛ්‍ය මට්ටම ශ්‍රේණිගත කිරීමට වර්ණ කේත ක්‍රමවේදයක් නිර්මාණය කර තිබෙනවා. මේ වෙත චීන රජය සමග අත්වැල් බැඳගන්නේ තාක්‍ෂණ දැවැන්තයින් වන අලිබබා සහ ටෙන්සෙන්ට් සමාගම් දෙක යි. කාර්මික කේන්ද්‍රස්ථාන නගරයක් ලෙස සැලකෙන Hangzhou හි දී පසුගිය දිනෙක අත්හදා බැලුණා. මෙහි දී පුද්ගලයන්ගේ වෛද්‍ය වාර්තාවන්, ගමන් මාර්ගයන්, වයස වැනි දත්ත ලබාගෙන ඔවුන් වෙත කොළ, කහ හෝ රතු යන වර්ණ තුනෙන් එකක් ලබාදීම සිදුකරනවා. මෙහි දී ඔවුන් ගමන් කළ ස්ථානයන් සහ සෞඛ්‍ය මට්ටම අනුව වෛරසයට නිරාවරණය වීමේ සම්භාවිතාව තීරණය කෙරෙනවා. වර්ණ කේතය මත පදනම්ව පුද්ගලයෙකු නිරෝධායනය කළ යුතු ද, නැති ද යන්න තීරණය කෙරෙනවා. Alibaba’s Alipay, Ant’s wallet වැනි වෝලට් සේවාවන් ඔස්සේ මේ වෙත ලියාපදිංචි වන්නට චීන ජාතිකයන් වෙත අවස්ථාව තිබෙනවා. බොහොමයක් metro stations, offices, stations වැනි පොදු ස්ථානයන් වන මෙම කේතයන් Scan කිරීමට පහසුකම් සලසා තිබෙනවා. සාමාන්‍යය ස්ථානයන්වල ගැවසීමට ඉඩ ලැබෙන්නේ මෙම දුරකතන යෙදුම මඟින් ලබාදෙන කේතය කොළ පැහැති වුණොත් පමණයි. ඒ වගේම ජනතාවගේ ශරීර උෂ්ණත්වය මැනීමට checkpoints විවිධ ස්ථානයන්වල සකස් කොට තිබෙනවා. මේ වන විටත් චීනයේ නගර 200කට වැඩියෙන් මෙම පද්ධතිය භාවිතා කරනවා. ඉතා ඉක්මනින් අනෙක් නගර වෙතත් මෙය අනිවාර්ය වේවි.

චීනයේ රෝහල්වල ආපනශාලාවන්ගේ ආහාර පිළියෙල කිරීමේ සිට වේටර්වරුන්, විෂබීජ නාශක ඉසීම සහ පිරිසිදු කිරීම, සහල් විකිණීම සහ අනෙකුත් සනීපාරක්ෂක ද්‍රව්‍ය බෙදාහැරීම දක්වා කොරෝනාවෛරසය පැතිරීම වැළැක්වීම සඳහා ගන්නා ක්‍රියාමාර්ග බොහොමයක රොබෝවරු පෙරමුණ ගෙන ඉන්නවා. ඊට අමතරව බොහොමයක් රෝහල්වල රෝග විනිශ්චය කිරීම, වෛද්‍ය සාම්පල ප්‍රවාහනය වැනි කටයුතු සඳහා පවා රොබෝ තාක්ෂණය භාවිතා කරනවා. ඊට අමතරව, චීනය වෙත ගුවන් යානයක ගමන් කළ මඟීන් පිරිසක් මේ වෙද්දී තාවකාලික නිරෝධායන මධ්‍යස්ථානයක රැඳී ඉන්නවා. ඔවුන් වෙත ආහාර සැපයීමට Little Peanut නම් රෝබෝවරයෙකු භාවිත කළ අවස්ථාවක් ගැන රොයිටර් වෙබ් අඩවිය වාර්තා කරනවා.

චීනයේ මේ වෛරසය හේතුවෙන් දැඩි ලෙස පීඩාවට පත් සමහර ප්‍රදේශ වෙත වෛද්‍ය උපකරණ වැනි දෑ ඉතා ඉක්මනින් ප්‍රවාහනය කිරීම සහ එම ප්‍රදේශවලින් රෝගීන්ගේ සාම්පල ගෙන ඒමේ පහසුම ක්‍රමවේදය Drone යානා භාවිතය බවට පත්ව තිබෙනවා. මේ යානා භාවිතය නිසාවෙන් කාලය විශාල වශයන් ඉතිරි කර ගැනීමට වගේම විවිධ සාම්පල අපවිත්‍ර වීමත් අවම කරගැනීමට හැකියාව ලැබී තිබෙනවා. මේ විශේෂ යානා සමග සෞඛ්‍ය තොරතුරු ගබඩා කර තිබෙන QR කෝඩ් ක්‍රමවේදයක් භාවිතා වෙනවා.

ඊට අමතරව, ගම්බද ප්‍රදේශවල විෂබීජ නාශක ඉසීම වෙනුවෙන් විශේෂිත කෘෂිකාර්මික Drone යානා භාවිත වෙනවා. තවත් විශේෂිත කාර්යයක් වෙත මේ වෙද්දී චීනයේ Drone භාවිත වෙනවා. ඒ මිනිසුන්ට නිවෙස්වලින් එළියට පැමිණෙන විට මුහුණු ආවරණ පළඳින ලෙස මතක් කිරීම වෙනුවෙනුයි.

සබැඳි ලිප:

තාක්ෂණික ලෝකයට වැළඳුණ කොරෝනා වෛරසය

චීනයේ පැතිරී යන නව කොරෝනාවෛරසය, ලෝකයම ගිල ගනීවි ද?

වූහාන් කොරෝනා වෛරස් වසංගතය- සිද්ධි මාලාව (මෙය යාවත්කාලීන කෙරෙන ලිපියකි)

COVID-19 රෝගයේ ඉරණම මෙන්න

කොරෝනා වැළඳුණු මවකට, තම දරුවාට මව්කිරි දෙනු හැකි ද?

COVID-19යෙන් ගැලවිමට ගව මුත්‍රා පානය කරන ඉන්දියානුවෝ

උතුරු කොරියාව කොරෝනා වෛරස් ආසාදිතයන්ට වෙඩි තැබුවා ද?

ලොව භීතියෙන් අවුලන්න සමත් වූ කොරෝනාවෛරසයය ගැන සත්‍ය තොරතුරු සේ ම, අසත්‍ය පුවත් ද ඉතා ඉක්මනින් සමාජගත වෙනවා. මෙය නවතන්න Facebook, Google සහ Microsoft සමාගම් නව සේවාවන් හඳුන්වා දුන්නා.

2019 වසරේ දෙසැම්බර් 12 වන දා සිට චීනයේ වුහාන් නගරය මුල් කරගෙන පැතිරීම ආරම්භ වූයේයැ යි සැලකෙන COVID-19 එසේ නොමැති නම්, කොරෝනා වෛරසය අද වෙද්දී ලෝකය තුළ විශාල කලබගෑනියක් නිර්මාණය කරන්නට සමත්ව තිබෙනවා. මෙයින් තාක්ෂණික ලෝකයට සිදු වූ බලපෑම් ගැන පෙර ලිපියකින් අප ඔබව දැනුවත් කළා. ලෝකයේ දැවැන්ත සමාගම් ගණනාවකට දැවැන්ත පාඩු සිදුකරන්නටත් මෙය සමත් වුණා. “තාක්ෂණික ලෝකයට වැළඳුණ කොරෝනා වෛරසය” ලිපිය වෙන්වුණේ ඒ වෙනුවෙන්ම යි. කොරෝනා රෝගයට එරෙහිව සටන් කරන්නට ලෝකයේ ප්‍රභල සන්නාමයන් රාශියක් සහ ලොව ප්‍රබල ව්‍යාපාරිකයන් එක්ව තිබෙනවා. මේ ලිපිය ඔස්සේ දිගහැරෙන්නේ ඔවුන් මේ වෛරසයට එරෙහිව ගෙන යන සටන පිළිබඳව යි.

Alibaba සමාගම ලොව සුප්‍රකට වන්නේ වෙළඳ සමාගමක් ලෙස යි. නමුත්, Alibaba සන්නාමය යටතේ විවිධ ක්ෂේත්‍රයන් ගණනාවක් පිළිබඳව පර්යේෂණ පැවැත්වෙනවා. කොහොම නමුත්, Alibaba සමාගමේ නිර්මාතෘ Jack Ma, කොරෝනා වෛරසයට එරෙහිව ගෙන යන සටන වෙනුවෙන් ඇමරිකානු ඩොලර් මිලියන 14.5ක් පරිත්‍යාග කොට තිබෙනවා. අදාළ මුදල කොරෝනා වෛරසයට එරෙහි ප්‍රතිශක්තිකරණ එන්නතක් නිපදවීම වෙනුවෙන් සහ රෝගීන් වෙනුවෙන් අවශ්‍ය කරන අනෙක් අත්‍යවශ්‍ය ද්‍රව්‍ය මිල දී ගැනීමට වෙන් වේවි. ලංකාව ඇතුළු ආසියානු රටවල් වෙත මේ වෙද්දීත් රෝගීන්ට අත්‍යවශ්‍ය ද්‍රව්‍ය ලබාදීමට ඔහු කටයුතු කරමින් සිටිනවා. ඒ පිළිබඳව වැඩි විස්තර ඔහුගේ twitter ගිණුමේ ඔහු සඳහන් කොට තිබෙනවා. ඒ වගේම, ඔහු යටතේ පවතින ආයතනයක් කොරෝනා වෛරසය හඳුනාගැනීමට හැකි කෘත්‍රීම බුද්ධි වැඩසටහනක් නිර්මාණය කර තිබුණා. Damo Academy සිදුකළ මේ සොයාගැනීම දැන් ලොව පුරා සෞඛ්‍ය ආයතන රාශියක භාවිත වෙනවා.

Apple CEO වන Tim Cook, පසුගිය දිනෙක ඔහුගේ නිල ට්විටර් ගිණුමේ සටහනක් තබමින් කියා සිටියේ, ඔවුන් මේ වෙද්දී ඇමරිකානු සෞඛ්‍ය ක්ෂේත්‍රයේ නියැලී සිටින්නන් වෙත මිලියන ගණනක ආරක්ෂක මුහුණු ආවරණ ලබා දී ඇති බව යි. ඒ වගේම, ඔවුන් කොරෝනාවට එරෙහි සටනේ සැබෑ විරුවන් බවත් ඔහු සඳහන් කර තිබෙනවා. පසුගිය දිනෙක ධවල මන්දිරයේ පැවති මාධ්‍ය හමුවක දී ඇමරිකානු උප ජනාධිපති Mike Pence ඉහත ප්‍රකාශය සනාත කළා. ඇපල් සමාගමෙන් මිලියන දෙකක පමණ මුහුණු ආවරණ ලැබුණු බවත්, ඒවා හැකි ඉක්මනින් බෙදාහරින බවත් එහි දී සඳහන් කෙරුණා.

ලොව පුරා මුහුණු ආවරණ හිඟයක් පවතින බව Amazon සමාගමේ CEO සහ නිර්මාතෘ Jeff Bezos සේවකයන් වෙත සටහනක් මඟින් දන්වා තිබුණා. නිවසේ සිට රාජකාරි කළ නොහැකි කොන්ත්‍රාත්කරුවන් වැනි සේවකයන්ට අත්‍යවශ්‍ය මුහුණු ආවරණ සඳහා මේ වන විටත් ඇනවුම් ලබා දී ඇතත්, එයින් ඔවුන් වෙත ලැබුණේ ඉතාම සුළු ප්‍රමාණයක් බව යි ඔහු සඳහන් කරන්නේ. මෙලෙස ඇණවුම් ලබා දී ඇත්තේ N95 වර්ගයේ මුහුණු ආවරණ සඳහා බව යි දැනගන්නට ලැබෙන්නේ. කොහොම නමුත්, තම සේවකයන්ගේ ප්‍රවේශම ගැන ඔහු ඇතුළු සමාගම් ගණනාවක ප්‍රධානීන් සැලකිලිමත් වන බව නම් පෙනෙන්නට තිබෙනවා.

Peyton Reed නම් රූපවාහිනී අධ්‍යක්ෂකවරයා Tesla සමාගමේ නිර්මාතෘ Elon Musk වෙත ස්තුතිය පළ කරමින් ට්විටර් සටහනක් පළ කර තිබුණා. ඒ, විශාල වටිනාකමකින් යුතු මුහුණු ආවරණ ඇතුළු උපකරණ රාශියක් UCLA Health facility එකක් වෙනුවෙන් පරිත්‍යාග කර තිබූ නිසාවෙනුයි. එවන්ම සටහනක් එක් කරමින් Facebook සමාගමේ නිර්මාතෘ සහ CEO Mark Zuckerberg කියා සිටියේ, තම සමාගමෙන් මුහුණු ආවරණ 720,000ක් පමණ මේ වෙද්දීත් පරිත්‍යාග කොට ඇති බව යි. ඊට අමතරව තවත් ආධාර එකතු කිරීමේ වැඩසටහන් ක්‍රියාත්මක කිරීමට ඔවුන් බලාපොරොත්තු වන බවත් සඳහන් කර තිබුණා. ඔහු සහ ඔහුගේ බිරිඳගේ (Chan Zuckerberg) යටතේ ක්‍රියාත්මක වෙන philanthropic groups හරහා San Francisco Bay Area හි සිදුවන කොරෝනා පර්යේෂණ මට්ටම ඉහළ නංවන්නට කටයුතු කරන බව ඔහු සඳහන් කර තිබුණා. එම කණ්ඩායම් මේ පර්යේෂණ සඳහා ඇමරිකාවේ California විශ්වවිද්‍යාලය සමග එකාබද්ධව ක්‍රියාකරන බව theverge.com වාර්තා කර තිබුණා.

සබැඳි ලිපි:

තාක්ෂණික ලෝකයට වැළඳුණ කොරෝනා වෛරසය

චීනයේ පැතිරී යන නව කොරෝනාවෛරසය, ලෝකයම ගිල ගනීවි ද?

වූහාන් කොරෝනා වෛරස් වසංගතය- සිද්ධි මාලාව (මෙය යාවත්කාලීන කෙරෙන ලිපියකි)

පසුගිය දිනෙක කාන්තා දිනය සැමරුණා ඔබට මතක ඇති. කාන්තාවන්ගේ නිදහස, අයිතීන් ගැන එදින වැඩි වශයෙන් කතාබහට ලක් වුණා. නමුත්, ඔබත් මමත් දවසේ වැඩි හරියක් ගෙවන තාක්ෂණික ලෝකයේ අතිශය ප්‍රබල කාන්තා චරිත ගණනාවක් ඉන්න බව ඔබ දැන සිටියා ද? මේ ලිපිය හරහා අප බලාපොරොත්තු වන්නේ ඒ කාන්තාවන් අතුරින් කිහිපදෙනෙක් පිළිබඳව ඔබව දැනුවත් කරන්නට යි.

Facebook සමාගම ලෝකයේ වගේම, මේ ලිපිය කියවන ඔබ කා අතරත් අතිශය ජනප්‍රිය සමාගමක් බවට නම් සැකයක් නැහැ. 2012 වසරේ එක් කාන්තාවක් මෙම සමාගමේ සුවිශේෂී තනතුරකට පත් වුණා. ඒ, සමාගම තුළ එවැනි තනතුරක් හෙබ වූ පළමු කාන්තාව බවට පත් වෙමින්. නමින් ෂෙරිල් සැන්ඩ්බර්ග් වන ඇය 2012 ජුනි මාසයේ දී, ෆේස්බුක් හි අධ්‍යක්ෂ මණ්ඩලයේ සේවය කළ පළමු කාන්තාව බවට පත් වුණා. (ෆේස්බුක් හි ප්‍රධාන මෙහෙයුම් නිලධාරී- Chief Operating Officer of Facebook) ඒ වගේම, එම වසරේම ඇය ටයිම්ස් සඟරාව නම් කරන ලොව බලගතුම පුද්ගලයින් 100 දෙනා අතරටත් එක් වෙන්නට සමත් වුණා. facebook සමාගම සමග සම්බන්ධ වීමට පෙර ඇය එක්සත් ජනපද භාණ්ඩාගාර ලේකම්ගේ කාර්යය මණ්ඩල ප්‍රධානියා ලෙස කටයුතු කළා. ඊට අමතරව තවත් සුප්‍රකට සමාගමක් වන ගූගල් සමාගමෙහි ගෝලීය ඔන්ලයින් විකුණුම් හා මෙහෙයුම් බාර උප සභාපති ලෙස සේවය කළා. තාක්ෂණයට සම්බන්ධ රැකියාවන්වල නිරත වූ ඇය, "Lean In: Women, Work, and the Will to Lead," නමින් කෘතියක් පවා රචනා කොට තිබෙනවා. මේ කෘතිය ඔස්සේ ස්ත්‍රීවාදය, රැකියා ස්ථානයේ ලිංගිකත්වය සහ වෘත්තීය ලෝකයේ ස්ත්‍රී පුරුෂ සමානාත්මතාවයට ඇති සමාජ/ පෞද්ගලික බාධක වැනි තේමාවන් සාකච්ඡා කෙරෙනවා. ඇයගේ වෘත්තීය ජිවිතයේ වසර ගණනක අත්දැකීම් අලලා ලියැවුණු මේ කෘතිය පිටපත් මිලියනයකට වඩා අලෙවී වූ කෘතියක්. ඇයගේ වත්කම් ප්‍රමාණය ඇමරිකානු ඩොලර් බිලියනයක් පමණ වන බව තමයි දැනගන්නට ලැබෙන්නේ.

ඔබත් මමත් හොඳින්ම දන්නා ලොව සුප්‍රකටම සමාජ ජාලයක් බවට පත්ව තිබෙන YouTube හි ප්‍රධාන විධායක නිලධාරිනිය ලෙස වර්තමානයේ කටයුතු කරන්නේ මැය යි. 1999 වසරේ Google සමාගම වෙත අලෙවිකරණ කළමනාකාරියක ලෙස සම්බන්ධ වූ ඇය, නොබෝ කලෙකින්ම වෙළඳ ප්‍රචාරණ හා වාණිජ අංශයේ ජ්‍යෙෂ්ඨ උප සභාපති බවට පත් වුණා. Google Video සේවාවේ අධීක්ෂකවරියක් ලෙස කටයුතු කළ ඇය, එකල Startup එකක් ලෙස පැවති Youtube සමාගම Google යටතට ලබාගැනීම පිළිබඳව අදහස් ඉදිරිපත් කළා. 2006 වසරේ දී ඇමරිකානු ඩොලර් බිලියන 1.5කට ආසන්න මුදලකට youtube සමාගම  
Google වෙත පවරා ගැනීමේ සියලු කටයුතු පාහේ මැය යටතේ සිදුවුණා. 2007 DoubleClick සේවාව ඇමරිකානු ඩොලර් බිලියන 3.1කට මිල දී ගැනීම සිදුවුණෙත් මැය යටතේ යි. 2014 වසරේ පෙබරවාරි මාසයේ ඇයව YouTube හි ප්‍රධාන විධායක නිලධාරිනිය ලෙස පත් කෙරෙනවා. දරුවන් පස්දෙනෙකු සමග ඇගේ වෘත්තීය ජීවිතය ජයගත් ආකාරය ගැන ඇය, සමාජය සමග බොහෝ විට අදහස් හුවමාරු කරගන්න අමතක කරන්නේ නැහැ. ෂෙරිල් වගේම මැයත් ලොව බලවත්ම පුද්ගලයන් 100 දෙනා අතරට තේරී පත් වුණා. ඒ 2015 වසරේ දී යි.

ලොව ප්‍රකට සහ ප්‍රමුඛ පෙලේ පරිගණක සහ උපාංග නිපදවන සමාගමක් වන IBM සමාගමේ CEO බවට පත් වන්නට ඇයට හැකි වුණා. ඒ, එම සමාගමේ එවැනි තනතුරක් ලද පළමු කාන්තාව බවට පත් වෙමින්. මැය IBM සමාගම වෙත එක් වුණ වසර ලෙස වාර්තා වෙන්නේ 1991 වසරයි. ඇයට ප්‍රධාන විධායක නිලධාරි ලෙස පත්වීම ලැබෙන්නේ 2011 වසරේ දී යි. ඒ කාලය අතරතුර ඇය සමාගම තුළ විවිධ තනතුරු රැසක් දරා තිබෙනවා. ඒ අතරට සමාගමේ සභාපති තනතුරත් අයිතියි. 2012 සිට අඛණ්ඩව වසර 3ක් (2014 දක්වා) Fortune magazine එක තෝරාපත් කරන "50 Most Powerful Women in Business" (ලොව බලවත්ම ව්‍යාපාරික කාන්තාවන් 50) දෙනා අතර මුල් තැනක රැඳෙන්නට ඇයට හැකි වුණා. ඊට අමතරව, 2014 වසරේ දී ලොව බලවත්ම පුද්ගලයන් 100 දෙනා අතරටත් ඇගේ නම තෝරා පත් වුණා.

ඇමරිකානු බහුජාතික ව්‍යවසාය තොරතුරු තාක්ෂණ සමාගමක් වන Hewlett-Packard සමාගමේ ප්‍රධාන විධායක නිලධාරිනිය ලෙස කටයුතු කරන මැය, දේශපාලන ක්‍රියාකාරිනියක ලෙසත් සුප්‍රකට යි. ඉතාම කීර්තිමත් සමාගම් ගණනාවක් සමග විධායක තනතුරු හොබවා පළපුරුද්ද සහ අත්දැකීම් ඇති තැනැත්තියක ලෙස ඇයට විශාල පිළිගැනීමක් ලැබෙනවා. 1980 දශකය තුළ ඇය වෝල්ට් ඩිස්නි සමාගමේ උපායමාර්ගික සැලසුම්කරණයේ උප සභාපතිනිය ලෙසත්, 1990 දශකයේ DreamWorks, Procter & Gamble සහ Hasbro සමාගම් සමගත් කටයුතු කළා. ලොව ප්‍රකට වෙළඳ සමාගමක් වන eBay සමාගමේ 1998 සිට 2008 දක්වා සභාපති සහ ප්‍රධාන විධායක නිලධාරිනිය ලෙසත් ඇය සේවය කළා. Hewlett-Packard සමාගමේ සාර්ථකත්වය පසුපස සිටින ප්‍රධාන චරිතයක් වන ඇයව, 2014 වසරේ ලොව බලවත්ම පුද්ගලයන්ගේ ලැයිස්තුවට ෆොර්බ්ස් සඟරාව ඇතුළත් කළා.

ලොව ප්‍රකට සෙවුම් යන්ත්‍රයක් සහ වෙබ් ලිපින සපයන සමාගමක් ලෙස නම් දරා සිටින Yahoo සමාගමේ ප්‍රධාන විධායක නිලධාරිනිය ලෙස කටයුතු කරන්නට ඇය සමත් වුණා. 2012 වසරේ ඇයට මේ පත්වීම හිමි වන විට ඇය ලොව ප්‍රකට ව්‍යාපාරික කාන්තාවක් ලෙස හඳුනාගැනීමට ලක්ව සිටියා. Yahoo සමාගම සමග සම්බන්ධ වීමට පෙර දශකයකට වැඩි කාලයක් Google සමාගමේ ප්‍රකාශක තනතුරක් සහ විධායක තනතුරක් මැය විසින් හෙබවූවා. 2013 වසරේ දී ටයිම්ස් සඟරාව මඟින් ප්‍රකාශයට පත් කරන බලවත්ම කාන්තා ව්‍යාපාරිකයන් 100 දෙනා අතරටත්, 2014 Fortune‍ magazine මඟින් ප්‍රකාශයට පත් වන වයස අවුරුදු 40ට අඩු ලොව ප්‍රමුඛ ව්‍යාපාරිකයන් අතර 6 වෙනි තැනටත් පත් වෙන්නට ඇයට හැකි වුණා. අද වෙද්දී ඇය ප්‍රමුඛ පෙලේ ව්‍යාපාරිකාවක් ලෙස ලොවම හඳුනන තැනැත්තියක්.

ලොව ප්‍රකට තාක්ෂණික සන්නාමයක් ලෙස හැඳින්වෙන Apple සමාගමේ වෙළඳ අංශයේ ජ්‍යෙෂ්ඨ උප සභාපති ලෙස කටයුතු කරන Angela Ahrendts මේ ලයිස්තුවේ සිටිය යුතුම කෙනෙක්. තාක්ෂණික ලෝකය වෙත පිවිසීමට පෙර ඇය Burberry සමාගමේ ප්‍රධාන විධායක අධ්‍යක්ෂිකාව ලෙස කටයුතු කළා. ඒ ,2006 - 2014 කාලයේ දී යි. වසර ගණනාවක විධායක ක්ෂේත්‍රයේ ඇති පළ පුරුද්ද නිසාම Apple සමාගමේ වෙළඳ අංශයේ ජ්‍යෙෂ්ඨ උප සභාපති ලෙස කටයුතු කරන්නට ඇයට ඇරයුමක් ලැබෙනවා. 2014 වසරේ දී ඇය ඇපල් සමාගම තුළ නව වාර්තාවක් තබනවා. ඒ, වැඩිම වැටුප් ලබන විධායක නිලධාරිනිය ලෙස යි. ඇය වසරක් තුළ ඇමරිකානු ඩොලර් මිලියන 70කට අධික මුදලක් ඒ වෙද්දී උපයන බව තමයි දැනගන්න ලැබෙන්නේ. ෆෝබ්ස් සඟරාවේ හි 2015 වසරේ ලොව බලවත්ම කාන්තාවන්ගේ ලැයිස්තුවේ 25 වන ස්ථානය ලබාගැනීමට අයට හැකි වෙනවා. BBC Radioවේ 4 Woman’s Hour 100 Power List එකෙහි 9 වන ස්ථානයත්, 2009 ෆොර්බ්ස් සඟරාවේ වසරේ ලොව බලවත්ම ව්‍යාපාරික කාන්තාවන්ගේ ලයිස්තුවේ 29 වන තැනත් ඇයට හිමි වෙනවා. ඒ වගේම, එක්සත් රාජධානියේ අග්‍රාමාත්‍යවරයාගේ ව්‍යාපාරික උපදේශක මණ්ඩලයේ ද තනතුරක් ඇය හොබවනවා.

මේ වන විට ලෝකය පුරා කොරෝනා (COVID-19) වයිරසයක් පැතිරී යන බව ඔබ දන්නවා. මේ වෛරසය පසුගිය 2019 වසරේ දෙසැම්බර් 12 වන දා සිට චීනයේ වුහාන් නගරය මුල් කරගෙන පැතිරීම ආරම්භ වූයේයැ යි සැලකෙනවා. එම වෛරසය ක්ෂේත්‍රයන් ගණනාවක් වෙත බලපෑම් කරන්නට සමත් ව තිබෙනවා. තාක්ෂණික ලෝකයත් ඉන් එකක්. මේ වන විටත් ලෝකයේ ප්‍රබල, ප්‍රමුඛ තාක්ෂණික සන්නාමයන් වෙත සහ සමාගම් වෙත මිලියන ගණනින් පාඩු සිදුකරන්නට කොරෝනා වෛරසයට හැකි වුණා. ඒ වගේම, ලෝකයේ විශාලතම තාක්ෂණික සමුළු ගණනාවක් නවතා දමන්නටත් සමාගම් වෙත සිදුවුණා. මේ ලිපිය ඔස්සේ දිගහැරෙන්නේ තාක්ෂණික ලෝකය වෙත කොරෝනා දැඩිව බලපෑම් කළ ආකාරය පිළිබඳව යි.

එළඹෙන මැයි මාසයේ 12 වැනිදාත් 14 වැනිදාත් අතර කාලයේ California හි පැවැත්වීමට නියමිතව තිබුණු Google I/O 2020 සජීවී අංගය කොරෝනා වෛරසය නිසා නවතා දමන්නට තීරණය කර තිබෙනවා. Google සමාගමේ නවතම නිෂ්පාදන හඳුන්වාදීම වෙනුවෙන් වාර්ෂිකව පවත්වන මේ සමුළුවේ සජීවී අංගය වෙත පමණක් 7000කට වැඩි පිරිසක් සම්බන්ධ වෙනවා. ඊට අමතරව, ලංකාව ඇතුළු රටවල් ගණනාවක එයට සමගාමීව I/O events පැවැත්වෙනවා. Google I/O 2019 event එකත් ලංකාවේ අපට Live streamවලට සීමා කරන්නට සිදුවුණා. ඒ, එවකට රටේ පැවති ආරක්ෂක අවදානම් තත්ත්වය නිසා යි. මෙවරත් එය අහිමි වීම ගැන නම් බොහෝ දෙනෙක් පසුවෙන්නේ අසතුටින්. කොහොම වුණත්, මෙවර ප්‍රධාන Google I/O 2020 Event එක ප්‍රධාන සමාජ ජාලා හරහා Live stream එකක් ලෙසින් පමණක් විකාශය කිරීමට Google සමාගම තීරණය කර තිබෙනවා. 2020 වසරේ සජීවී event එක සඳහා ටිකට් මිලදී ගත් පිරිස වෙත 2021 වසරේ event එක සඳහා එය පරිවර්තනය කර ගැනීමේ හෝ සම්පුර්ණ මුදල නැවත ලබාගැනීමේ පහසුකම ලබාදෙන බව සමාගම සඳහන් කළා.

කොරෝනා වෛරසය නිසාවෙන් කල් දැමෙන තවත් අතිශය ජනප්‍රිය අංගයක් ලෙස Game Developers Conference - GDC හඳුන්වන්න පුළුවන්. ලෝකය පුරා සිටින Game Developerලා සහ ක්‍රීඩකයින් එකට එකතු වන GDC වාර්ෂික සමුළුව, එළඹෙන මාර්තු 16ත් 20ත් අතර කාලයේ පැවැත්වීමට නියමිතව තිබුණා. 1988 වසරේ සිට වාර්ෂිකව පැවැත්වෙන GDC අංගය ලෝකයේ බොහෝ දෙනෙක් සහභාගී වන සහ විශාල අවධානයක් දිනාගන්නා අංගයක්. සාමාන්‍යයෙන් මේ අංගය වෙත වාර්ෂිකව 29,000ක් පමණ පිරිසක් සහභාගී වෙනවා.

ඒ වගේම, PAX East පරිගණක ක්‍රීඩා සමුළුවටත් කොරෝනා වෛරසය හේතුවෙන් ගැටළු මතුව තිබෙනවා. PAX East වෙත පරිගණක ක්‍රීඩා නිර්මාණ ක්ෂේත්‍රයේ ප්‍රමුඛ sony ඇතුළු සමාගම් කිහිපයක්ම සහභාගී නොවන බව දන්වා තිබෙනවා. සේවකයන්ගේ ආරක්ෂාකාව පිළිබඳව ගන්නා පියවරක් ලෙසින් තමන් මේ සමුළුවට සම්බන්ධ නොවන බවත්, ඒ පිළිබඳව තම කණගාටුව පළ කරන බවත් Sony සමාගම දැනුම් දී තිබෙනවා.

අප කවුරුත් හොඳින් දන්නා Facebook සමාගම වෙතත් මෙම වෛරස තත්ත්වය නිසා විශාල පාඩු සිදුවන්නට පටන් ගෙන තිබෙනවා. ඔවුන් වාර්ෂිකව පවත්වන F8 සමුළුවත් නොපවත්වන්නට ඔවුන් තීරණය කර තිබෙනවා. සාමාන්‍යයෙන් F8 සමුළුවේ දී Facebook සමාගමේ නව නිර්මාණයන් සහ තාක්ෂණයන් ගැන එළිදැක්වීම සිදුවෙනවා. කොහොම වුණත්, 2020 වසරේ ප්‍රධාන අංගය නොපැවැත්වුවත් බොහෝ රටවල්වල Developersලා වෙනුවෙන් දේශීය හමු පවත්වන්නට ඔවුන් සුදානම් වන බව දන්වා සිටිනවා.

ඊට අමතරව, සමාගම මුහුණපාන ප්‍රධාන ගැටළුවක් බවට පත් වෙන්නේ කොරෝනා වෛරසය ගැන සහ එහි ආසාදිතයන් ගැන facebook සමාජ ජාලයේ පැතිරෙන අසත්‍ය ප්‍රවෘත්ති යි. Facebook fact-checking ටූල් එක විශාල වශයෙන් මෙවැනි පුවත්වල සත්‍ය අසත්‍යතාව පිළිබඳව හෙළි කරනවා. නමුත්, බොහෝ විට භාෂාමය ගැටළුව වැනි කරුණු නිසාවෙන් එය අසාර්ථක වන වාර ගණන විශාල යි. www.buzzfeednews.com වෙබ් අඩවිය මෙලෙස වාර්තා වන ප්‍රසිද්ධ අසත්‍ය පුවත් පිළිබඳව යාවත්කාලීන වන වාර්තාවක් ඉදිරිපත් කර තිබුණා.

ලෝකයේ බොහෝ පිරිසක් සහභාගී වෙන තවත් ජනප්‍රිය අංගයක් කල් දැමීමට එහි සංවිධායකයන්ට සිදුවුණා. ඒ, Mobile World Congress ප්‍රදර්ශනය යි. Barcelona හි පැවැත්වීමට නියමිතව තිබු මේ ප්‍රදර්ශනය වෙත ලෝකය පුරා දුරකතන නිෂ්පාදකයන් සහ යෙදුම් සංවර්ධකයින් සහභාගී වෙනවා. මේ අංගය සංවිධානය කරන GSMA (Global System for Mobile Communications Association) හි CEO John Hoffman සඳහන් කළේ ලෝකය පුරා පැතිර යන මේ වෛරසය හේතුවෙන් මෙවර Mobile World Congres පැවැත්වීම කළ නොහැක්කක් බව යි. ඔවුන් 2021 වසරේ සමුළුව පැවැත්වීමට අරමුණු කරන බවත්, චීනය ඇතුළු ලෝකය පුරා මේ වෛරසයෙන් පීඩාවට පත් වූ ජනතාව වෙත තම ශෝකය පළ කරන බවත් ඔවුන්ගේ නිල වෙබ් අඩවියේ සඳහන් කර තිබුණා.

ලෝකයේ ප්‍රමුඛතම සමාගමක් වන Amazon සමාගමේ, ඉතාලි ශාඛාවේ සේවකයන් දෙදෙනෙක් වෙත කොරෝනා වෛරසය වැළඳී ඇති බව Amazon සමාගම තහවුරු කර තිබෙනවා. මේ වන විටත් ඒ අදාළ සේවකයින් නිරෝධායන ක්‍රියාවලි වෙත යොමු කර ඇති අතර, ඒ සේවකයන් වෙත අවශ්‍ය වන සහාය සමාගම වෙතින් ලබාදෙන බව ඔවුන් සඳහන් කරනවා. මේ වෙද්දීත් ඔවුන් අසළ සේවය කළ අනෙක් සේවකයන් වෙත මේ පිළිබඳව දැනුවත් කර ඇති බව යි සමාගම සඳහන් කරන්නේ.

Alibaba සමාගම කොරෝනා වෛරසයට එරෙහිව ක්‍රියාත්මක වෙන තාක්ෂණික සමාගම් අතර පෙරමුණට පැමිණ තිබෙනවා. Alibaba සමාගමේ නිර්මාතෘ Jack Ma මේ වෛරසයට එරෙහිව සිදුකරන පර්යේෂණ වෙත යුආන් මිලියන 100ක්, එසේ නොමැති නම් ආසන්න වශයෙන් ඇමරිකානු ඩොලර් මිලියන 14.5ක් පරිත්‍යාග කර තිබෙනවා. ප්‍රධාන වශයෙන් මේ මුදලේ වැඩි කොටසක් කොරෝනා වෛරසයට එරෙහි ප්‍රතිශක්තිකරණ එන්නතක් නිපදවීම වෙනුවෙන් වෙන් වේවි. ඒ වගේම රෝගීන් වෙනුවෙන් අවශ්‍ය කරන අනෙක් අත්‍යවශ්‍ය ද්‍රව්‍ය මිල දී ගැනීමටත් එයින් කොටසක් වෙන් වෙන බව තමයි දැනගන්නට ලැබෙන්නේ.

මීට අමතරව කොරෝනා වෛරසය හඳුනාගැනීමට හැකි කෘත්‍රීම බුද්ධි වැඩසටහනක් නිර්මාණය කරන්න Alibaba සමාගමේ පර්යේශණ ආයතනයක් වන Damo Academy වෙත හැකි වී තිබෙනවා. AI මඟින් බලගැන්වෙන නව රෝග විනිශ්චය කළ හැකි පද්ධතියක් ඇසුරෙන් 96 %ක නිරවද්‍යතාවයක් සහිතව, රෝගය තප්පර 20ක් වැනි කෙටි කාලයක් ඇතුළත හඳුනාගැනීමට හැකියාව පවතිනවා. CT Scaning ක්‍රමවේදයක් ඔස්සේ රෝගය හඳුනාගන්නා මෙකී පද්ධතිය වෙත කොරෝනා රෝගීන් 5000කට අධික ප්‍රමාණයකගේ දත්ත ඇතුළත් කර තිබෙනවා. ඒ වගේ ම මේ වන විට චීනයේ රෝහල් ගණනාවක දී මෙය අත්හදා බලා තිබෙනවා. මේ වන විටත් ලෝකය පුරා රෝහල් 100කට අධික ප්‍රමාණයක මේ පද්ධතිය ක්‍රියාත්මක වෙනවා.

පසුගිය ජනවාරියේ coronavirus යෙදුම වෙත SOS Alert එකක් යෙදීමට Google සමාගම තීරණය කළා. මේ ඔස්සේ ඔබට අදාළ ප්‍රධාන පුවත් සහ මූලාශ්‍රයයන් ඉතා ඉකමනින් සොයාගැනීමට හැකියාව ලැබෙනවා. වෛරස තත්ත්වය එක පසෙකින් වැඩි වන අතරතුර දී coronavirus යෙදුම භාවිත කරමින් එය වළකන බවට සඳහන් වෙන Fake Apps විශාල ප්‍රමාණයක් Playstore වෙත ඇතුළත් වුණා. Playstore තුළින් මෙම යෙදුම වෙත යම් වාරණයක් පනවා තිබෙනවා. Coronavirus යන යෙදුම භාවිත වෙන කිසිඳු app එකක් දැන් වෙද්දී Playstore හි දර්ශනය වෙන්නේ නැහැ. මෙය ජනතාව අතරට අසත්‍ය පුවත් යාම වළකාලීමට ගත් ක්‍රියාමාර්ගයක් බව යි බොහෝ දෙනෙකුගේ මත ය.

මීට අමතරව තාක්ෂණික සමාගම් කොරෝනාවට එරෙහිව ගෙන යන වැඩසටහන් ගැන ඔබ දන්නවා නම්, ඒ ගැනත් අපිට කියන්න අමතක කරන්න එපා.

සබැඳි ලිපි:

චීනයේ පැතිරී යන නව කොරෝනාවෛරසය, ලෝකයම ගිල ගනීවි ද?

වූහාන් කොරෝනා වෛරස් වසංගතය- සිද්ධි මාලාව (මෙය යාවත්කාලීන කෙරෙන ලිපියකි)

Google I/O 2019 හි දී අලුතින්ම හඳුන්වාදුන් සිත්ගන්නාසුළු දේවල්

2020 වසර ආරම්භ වෙන්නෙම පෙරළිකාර ජංගම දුරකතන රැසක් වෙළඳපොළට නිකුත් වෙන ගමන්ම යි. ඔබ මේ වසරේ ජංගම දුරකතනයක් මිල දී ගන්නවා නම් හෝ ඔබ තාක්ෂණයට කැමති කෙනෙක් නම්, මේ ලිපිය ඔබට වඩාත් වැදගත් වන බව අපට විශ්වාස යි. 2020 වසරේ ජංගම දුරකතන වෙළඳපොළේ එළිදැක්වෙන පෙරළිකාර ජංගම දුරකතන ගැන යි මේ.

සාමාන්‍යයෙන් ඕනෑම පුද්ගලයෙක් ජංගම දුරකතනයක් මිල දී ගනිද්දී සලකා බලන වැදගත්ම කාරණයක් බවට පත් වෙන්නේ එහි කැමරාව යි. මේ වසරේ දුරකතන මාදිලි නිර්මාපකයන් කැමරාව සහ image Processing Algorithm කෙරෙහි වැඩි සැලකිල්ලක් යොමුකර තිබෙන බව පැහැදිලි යි. 2020 වසරේ මුල් කාර්තුව ඇතුළත නිකුත් වූ බොහොමයක් High End උපාංගයන්ගේ දක්නට ලැබුණු සුවිශේෂත්වයක් වුණේ, මෙගාපික්සල් 100කට වැඩි කැමරාව යි. කොහොම වුණත්, මේ විශාල sensor එක සමග සාර්ථක වූ වගේම අසාර්ථක වූ දුරකතනත් තිබෙනවා. ඒ ගැනත් මේ ලිපිය තුළ අන්තර්ගත යි.

පසුගිය 12 වැනි දා පැවති Galaxy UNPACKED 2020 Event එකේ දී කාගේත් අවධානය දිනාගත් Samsung සමාගමේ නවතම High End සහ Flagship දුරකතන මාදිලි වූයේ S20, S20+ සහ S20+ Ultra දුරකතන යි. මේ දුරකතන ත්‍රිත්වයම අධි බලැති කැමරා Setup එකකින් සමන්විත යි. මේ වසරේ දැනට නිකුත් වූ බලවත්ම දුරකතන ලෙස මේවා හඳුන්වන්නට පුළුවන්. Android 10.0 සහ One UI 2 සහිත නව දුරකතන Exynos 990 ප්‍රොසෙසරයක්, Mali-G77 ග්‍රැෆික් ප්‍රොසෙසරයක්, සහ UFS 3.0 ධාරිතාවකින් සමන්විත වෙනවා. මේ ගැන වැඩි විස්තර ඔබට අප පෙර පළ කළ “දැවැන්ත කැමරාවක් පෙරටු කරගත් Samsung Galaxy S20” ලිපියෙන් කියවන්නට පුළුවන්.

Xiaomi සමාගමේ නවතම දුරකතන දෙකක් ලෙස මෙම දෙවර්ගය හඳුන්වන්නට පුළුවන්. ඔවුන්ගේ නවතම Flagship දුරකතනය Mi 10 ලෙස නම් වෙනවා. Note 10 දුරකතනය mid-range දුරකතනයක්. කොහොම නමුත්, Xiaomi සමාගම එදා සිටම අඩු මිලට ඉතාම බලවත් දුරකතන නිකුත් කිරීම පිළිබඳව ප්‍රසිද්ධියක් උසුලන සමාගමක්.

Mid-range දුරකතනයක් වෙත මෙතෙක් පැමිණි බලගතුම කැමරා සෙටප් එක සහිත උපාංගය ලෙස අවිවාදයෙන් පිළිගැනෙන මෙය නිකුත් වන්නේ 2019 වසරේ නොවැම්බර් මාසයේ දී යි. ඔබ හොයන්නේ බලවත්ම කැමරා සහිත Mid-range දුරකතනයක් නම්, මෙය ඊට කදිම දුරකතනය බව අපට කියන්න පුළුවන්. අඟල් 6.47ක AMOLED තිරයක් සහිත මේ උපාංගය බල ගැන්වෙන්නේ Qualcomm snapdragon 730G Chipset එකකිනුයි. 128GB අභ්‍යන්තර මතක ධාරිතාවක් සහ 6GB RAM මතකයක් සහිත මෙහි 5260 mAh ධාරිතාවයක Li-Po බැටරියක් ඇතුළත්. මෙහි සුවිශේෂීම ගුණාංගය වෙන්නේ Penta-rear camera setup එක යි. 108 MPක ප්‍රධාන කැමරාව, 12 MP සහ 5 MP Telephoto Camera දෙක, 20 MP ultrawide කැමරාව සහ 2 MP macro කැමරාවක් මෙකී Penta-rear camera setup එකට ඇතුළත්. 108 MP ප්‍රධාන කැමරාව දරාගන්න snapdragon 730G සකසනයට හැකිදැ යි ප්‍රශ්නාර්ථයක් නමුත්, ගෙවන මුදලට සාපේක්ෂව ඉතාම සාධාරණ අනගි උපාංගයක් ලෙස එය හඳුන්වන්නට පුළුවන්.

Xiaomi සමාගමේ නවතම බලවත් දුරකතන දෙක ලෙස මේවා හඳුන්වන්න පුළුවන්. Snapdragon 865 සකසනයකින් බල ගැන්වෙන මේ දුරකතන දෙක බොහෝ සෙයින් සමාන යි. Mi 10 දුරකතනයේ මුලික මාදිලියේ රැම් ධාරිතාවය 8GBවලින් ආරම්භ වන අතර, අභ්‍යන්තර ප්‍රධාන මතකය 128 GBවලින් ආරම්භ වෙනවා. ඊට අමතරව 256GB 8GB RAM, 256GB 12GB RAM ආදී වශයෙන් මාදිලි දෙකකින් ඔබට මෙය මිල දී ගන්න පුළුවන්.

Mi 10 Pro හි මූලික මතක ධාරිතාවයත් 8 GBවලින් ආරම්භ වන අතර, එහි ප්‍රධාන මතකය 256GB ලෙස යි දැක්වෙන්නේ. ඊට අමතරව 256GB 12GB RAM, 512GB 12GB RAM ආදී වශයෙන් මාදිලි ද්විත්වයකින් ඔබට එය මිල දී ගන්න පුළුවන්. දුරකතන දෙකෙහිම ප්‍රධාන පිටුපස කැමරාව 108 MP. අනෙක් කැමරා පිළිබඳව පහත වගුවෙන් දැකගන්න පුළුවන්.

Tab එක සහ දුරකතනය යන උපාංග දෙකක් වෙනුවට එකී කාර්යයන් දෙකම ඉටුවන පරිදි එක් උපාංගයක් නිර්මාණය කිරීම මේ ට්‍රෙන්ඩ් එකේ දී සිදුවෙනවා. මෙලෙස නැවිය හැකි Foldable දුරකතන නිර්මාණය කිරීම තාක්ෂණික සමාගම් වෙත විශාල අභියෝගයක් වූ බව නම් අප කවුරුත් හොඳින්ම දන්නා කරුණක්. Samsung Galaxy Foldable දුරකතනය යම්තාක් දුරට අසාර්ථක වූ බව ඔබට මතක ඇති. හකුලා තබන විට අඟල් 4.6ක් වන ජංගම දුරකතනයක් මෙන්ම දිගහැරිය විට අඟල් 7.3ක tablet එකක් ලෙස ද භාවිතා කළ හැකි මෙම දුරකතනය, 12GB RAM එකකින් සහ 512GB Internal Storage එකකින් සමන්විත වනවා. එපමණක් නොවේ, පසුපස camera 3ක් මෙන්ම cover එක මත කැමරාවක් සහ ඉදිරිපස කැමරා 2ක් වශයෙන් camera 6කින් මෙය සමන්විත යි.

Huawei Mate X දුරකතනයත් Foldable දුරකතන පිළිබඳව සලකා බලද්දී අමතක කරන්නට බැහැ. පසුගිය වසරේ සාර්ථක වූ එකම Foldable දුරකතනය ලෙස Huawei Mate X අවිවාදයෙන් හඳුන්වන්න පුළුවන්. ඊට අමතරව Motorola RAZR, Royole Flexpai ,TCL foldable Phone වැනි දුරකතනත් මේ රැල්ලටම එකතු වෙනවා.

කොහොම නමුත්, මේ රැල්ලේ සාර්ථකම දුරකතනය ලෙස හඳුන්වන්නට හැකි දුරකතනයක් නිකුත් වුණේ පසුගිය දිනෙක samsung සමාගමෙනුයි. ඒ පිළිබඳව ප්‍රසිද්ධ Youtuber කෙනෙකු වූ JerryRigEverything පවා සඳහන් කළා. පසුගිය පෙබරවාරි 11 වෙනි දා නිකුත් වූ මේ foldable දුරකතනය සතුව Super AMOLED Display එකක් තිබෙනවා. Snapdragon 855+ සකසනයකින් බල ගැන්වෙන මෙය පැමිණෙන්නේ නවතම android 10 සමග යි. එමෙන්ම, මෙහි 8GB RAM ධාරිතාවයක් සහ 256 GB අභ්‍යන්තර මතක ධාරිතාවයක් ද සහිත යි.

මීට අමතරව Smart Phone Trends ගැන ඔබ දන්නා කරුණු අපි එක්ක බෙදාගන්න අමතක කරන්න එපා. තවත් බොහොමයක් දුරකතන ගැන සහ නව ට්‍රෙන්ඩ්ස් ගැන කතා කරන්නට තිබෙනවා. ඒ පිළිබඳව නව ලිපියකින් ගෙන එන්නම්.

සබැඳි ලිපි:

මසකට ලක්ෂයක් විකිණෙන Huawei Mate X

දැවැන්ත කැමරාවක් පෙරටු කරගත් Samsung Galaxy S20

මසකට ලක්ෂයක් විකිණෙන Huawei Mate X

S10 දුරකතනය ඇතුළු 2019 සැම්සන්ග් නිෂ්පාදන එළිදැක්ම

Galaxy Foldable අබිබවන්නට එන Motorola Razr 2019

Android සංස්කරණයක් හැඳින්වීම සඳහාම අතුරුපසක නමක්, එහෙම නැති නම් රසකැවිල්ලක නමක් භාවිතා වුණා ඔබට මතක ඇති. නමුත්, නවතම android සංස්කරණය වූ Android 10 සමග මේ සම්ප්‍රදාය වෙනස් වුණා. ඒ පිළිබඳව අපි ඔබව Qවලින් අවසන් වෙන Android අතුරුපස ලිපිය ඔස්සේ දැනුවත් කළා. හැබැයි ඉතින් මේ නව android මෙහෙයුම් පද්ධතිය ගැන පරිශීලකයන් එතරම් ප්‍රසාදයක් දැක්වූ බව නම් පෙනෙන්නට තිබුණේ නැහැ. එහි නැවුම් යමක් අඩංගු නොවුණු බව තමයි ඔවුන්ගේ මතය වුණේ.

Google සමාගමේ නව android මෙහෙයුම් පද්ධතියක් පිළිබඳව දැනුම් දෙන්නේ ලෝකයේ විශාලතම වගේම වැඩිම ආකර්ෂණයක් දිනාගත් තාක්ෂණික සමුළුව වන Google I/O හි දී යි. ඊට අමතරව නව මෙහෙයුම් පද්ධතියක Preview releases එකක් නිකුත් වෙන්නේ මාර්තු අවසන් සති කිහිපය තුළ තමයි. නමුත්, මෙවර තරමක් කලින් ඔවුන්ගේ නවතම මෙහෙයුම් පද්ධති සංස්කරණයේ “Preview releases” එකක් සිදුකරන්න ඔවුන් තීරණය කර තිබෙනවා. බොහෝ දෙනෙක් මේ මෙහෙයුම් පද්ධතිය හැඳින්වීමට “Android R” ලෙස භාවිත කළත්, මේ වෙත නම් යොදා ඇත්තේ Android 11 ලෙස යි. එහි Developer Preview එකක් මේ වෙද්දීත් android-developers.googleblog.com වෙත නිකුත් කර තිබෙනවා. 5G experience එක වැඩි දියුණු කිරීමත් මෙහි එක අරමුණක් බව තමයි දැනගන්නට ලැබෙන්නේ. UI හෝ UX (පරිශීලක අතුරු මුහුණතේ හෝ පරිශීලන අත්දැකීමේ) එතරම් වෙනසක් නොමැති බව තමයි දැකගන්නට ලැබුණේ. කොහොම නමුත්, මෙය තවම පරිශීලකයන් වෙත නිකුත් කළ එකක් නොවන නිසා මෙහි වෙනස්කම් සිදු විය හැකි බව තමයි තාක්ෂණික ලෝකයේ බහුතර මතය.

මෙම මෙහෙයුම් පද්ධතිය ස්ථාපනයට නම් full system එකම manually flash කිරීමට ඔබට සිදුවෙනවා. එම Developer Preview එක මේ වෙද්දී සහාය දක්වන්නේ Pixel 2, 3, 3A,සහ 4 දුරකතන වෙත පමණයි. මේ මෙහෙයුම් පද්ධතියේ මූලික අරමුණු බවට පත් වෙන්නේ 5G bandwidth එක සමග ක්‍රියාත්මක වීමේ හැකියාව සහ නව ට්‍රෙන්ඩ් එක බවට පත්ව තිබෙන foldable screens සහිත දුරකතන වඩාත් කාර්යක්ෂමව ක්‍රියා කිරීමට අවශ්‍ය පහසුකම් සැපයීම යි. ඊට අමතරව Developer Preview එකේ දී අත්හදා බැලෙන පහසුකම් අතරට low-latency video decoding පහසුකමත් ඇතුළත්. Google සමාගමේ ම නවතම Game Streaming සේවාව වන Stadia ඇතුළු Streaming සේවාවන් වෙත අවශ්‍ය කරන විශේෂ HEIF - High Efficiency Image File Format පහසුකමත් Android 11 වෙත ඇතුළත් වෙනවා. ඒ වගේම Google සමාගමේ නවතම නියුරෝනික ජාලයේ API එකත් (Application programming interface - යෙදුම් ක්‍රමලේඛ අතුරුමුහුණත) මෙයට අඩංගු යි. ඇපල් සමාගමේ iOS සමගින් එන “ iMessage” පහසුකමට සමාන ක්‍රමවේදයක් Android 11 වෙත ඇතුළත් වෙනවා. මෙය “Conversations” ලෙසින් දැනට නම් ව තිබෙනවා.

එකී ප්‍රධාන පහසුකම්වලට අමතරව Developer Preview එකෙහි දැකගන්නට ලැබෙන පහසුම් සැකවින් පහතින් ඉදිරිපත් කරන්නම්.

Facebook භාවිත කරන්නෙක් නම්, එහි Messaging Platform එකෙහි ඇති “chat heads” ඔබට මතක ඇති. ඒ පහසුකම අනුකරණය කරමින් මේ නව Bubbles පහසුකම නිර්මාණය වෙනවා. Apps කිහිපයක Conversation කිහිපයක් Chat Bubble ලෙස පෙන්වීමට හැකියාව මේ ඔස්සේ ලබා දෙනවා. දැනට නම් මෙම පහසුකම සහාය දක්වන්නේ Google Messaging සඳහා පමණයි. නමුත්, මෙහි අරමුණ වන්නේ අනෙක් Messaging apps සඳහාත් එම පහසුකම ලබාදීම යි.

මේ හරහා ඔබට Notifications පෙන්වන කොටසේ වෙනම චැට් කිරීමට හැකියාව ලබා දෙනවා. අනෙක් notificationsවලින් බාධාවක් නොවී Message කිරීමට මේ ඔස්සේ හැකියාව ලැබෙනවා.

සාමාන්‍යයෙන් අපි install කරන ඕනෑම app එකක් අපේ camera, microphone, සහ location data වැනි දෑ ලබා ගැනීමට අවශ්‍ය නම් Permission ඉල්ලීමක් තිරයේ දර්ශනය කරනවා. ඒ ඉල්ලීමට ප්‍රතිචාර ලෙස බහුතරයක් උපාංගවල පෙන්වන්නේ Permission ලබාදීම හෝ නොදීම යන තෝරාගැනීම් දෙක පමණයි. නමුත්, තාවකාලිකව පමණක් Permission ලබාදීමේ තෝරාගැනීමක් ඔබට මේ නව පහසුකම ඔස්සේ ලැබේවි.

Google සමාගමෙන්ම හඳුන්වාදීමට යන Screen recording පහසුකමකුත් මේ නව Android 11 වෙත ඇතුළත්.

මේ පහසුකම්වලට අමතරව;

කොහොම වුණත්, මේ හුදෙක් Developer Preview එකක් පමණක් බව අපි මතක තබා ගත යුතු යි. නව android 11 ගැන අපට එළඹෙන මැයි මාසයේ Google I/O හි දී දැනගන්නට ලැබේවි.

අද වෙද්දී ජංගම දුරකතන සන්නාමයන් රාශියක් වෙළඳපොළ තුළ දැකගන්නට ලැබෙනවා. ඔවුනොවුන් අතර ඇති දැඩි තරගකාරීත්වය නිසාවෙන් පරිශීලකයන් වෙත නව්‍යකරණය වූ උපාංග ලබාදෙන්නට සෑම ජංගම දුරකතන සන්නාමයක්ම උත්සහ කරනවා. නමුත්, මතුපිටින් පෙනෙන තරමටම අප දකින සන්නාමයන් අතර තරගකාරීත්වයක් නම් නැහැ. ඔවුන් එකිනෙකා තම වාසිය වෙනුවෙන් ප්‍රතිවාදීන් මත යැපෙන හැටි පිළිබඳව පෙර ලිපියකින් අපි ඔබට කරුණු ගෙන ආවා. නිෂ්පාදකයන් සහ ලොකු පුටු හැමවිටම එකිනෙකාගේ පැවැත්ම වෙනුවෙන් අත්වැල් බැඳගෙන සිටින ආකාරයත්, අපව ඔවුන් වටා තබා ගැනීම සඳහා බාහිර ලෝකයට ගැටුමක් මවා පාන ආකාරය ගැනත් එහි අන්තර්ගත වුණා. කොහොම නමුත්, අද වෙද්දී ලෝකයේ ප්‍රබල තාක්ෂණික සන්නාමයන් කිහිපයකට ප්‍රසිද්ධියේ අත්වැල් බැඳගන්නට සිදුව තිබෙනවා. මේ ලිපිය දිගහැරෙන්නේ ඒ පිළිබඳව යි.

ඔබට මතක ඇති; පසුගිය වසරක ඇමරිකානු වර්තමාන ජනාධිපති ඩොනල්ඩ් ට්‍රම්ප් විසින් Huawei Technologies Co Ltd ආයතනය අසාදුලේඛනගත කිරීම එහෙම නැති නම්, Blacklist කිරීමේ සිදුවීම. මේ සිදුවීමට මුල් වෙන්නේ ඇමරිකානු රජය, චීනය “විදේශික ප්‍රතිවාදියෙකු” ලෙස සලකමින් ඔවුන්ට විරුද්ධව ක්‍රියා කිරීම ආරම්භ කළ නිසාවෙනුයි. අවසානයේ Huawei සමාගම වෙත google සේවාවන් සියල්ලම පාහේ අහිමි වන්නට මේ ගැටළුව දුර දිග ගියා. කොහොම වුණත්, 2019 වසරේ මේ සියලු සම්බාධක හමුවේ නොසැලී Huawei වැඩිම විකිණුම් අතර දෙවැනි තැනට පැමිණි බව ඔබට මතක ඇති.

Huawei ආයතනය පසුගිය සැප්තැම්බරයේ හඳුන්වාදුන් නවතම උපාංග පෙළ අතර තිබූ Huawei Mate 30 (flagship) ජංගම දුරකතනයත් Google Apps කිසිවක් නොමැතිව යි එළිදැක්වුණේ. Play store සේවාවත් ඒ සමගම අහිමි වන නිසා තුන්වන පාර්ශවීය යෙදුම් ගබඩාවකින් (Third-party app store) එකකින් හෝ වෙබ් අඩවියකින් අවශ්‍ය පරිශීලකයන්ට යෙදුම් ලබාගන්නට සිදුවුණා. මේ ගැටළු සියල්ලන්ටම ලැබෙන විසඳුමක් ගැන අපට තාක්ෂණික ලෝකයෙන් වාර්තා වෙනවා.

ඒ Huawei, Xiaomi ඇතුළු BBK සමාගමේ උප සමාගම් වන Oppo සහ Vivo සමාගම්වල දුරකතන වෙතත් වෙනම App platform එකක් නිර්මාණය කිරීමට ගෙන ඇති තීරණයක් පිළිබඳව යි. Reuters වර්තාවක මේ පිළිබඳව සඳහන් වෙනවා. Google සමාගමේ Play store සේවාව Huawei වෙත අහිමි වීම සමග ඔවුන් Global Developer Service Alliance (GDSA) යටතේ සන්ධාන ගත වී තිබෙනවා. කවර හෝ දවසක සියලු චීන දුරකතන වෙත ඉහත සේවා අහිමි වීමක් හෝ සේවා කප්පාදුවක් සිදුවුවොත් එයට එරෙහිව මේ සන්ධානය නැගී සිටීවි. මේ වෙද්දී චීනයේ Play store තහනම් වීම නිසා මේ වෙද්දීත් වෙනත් තුන්වන පාර්ශවීය සේවාවන් භාවිත කරන්නට පරිශීලකයා පෙළඹෙන බව appinchina.co වාර්තා කර තිබුණා. කොහොම නමුත්, මේ තුන්වන පාර්ශවීය යෙදුම් ගබඩාවන් ප්‍රධාන වශයෙන් මුහුණ දෙන ගැටළුවක් වන්නේ යෙදුම් නිර්මාපකයන්ගේ සහාය ලබාගැනීම තරමක් අපහසු වීම යි. නමුත්, මේ GDSA යටතේ නිර්මාණය වන App platform එක සාර්ථක වූවොත්, ඒ සියලු ගැටළු වෙත පිළිතුරු ලැබෙන බව නම් හොඳටම විශ්වාස යි. මේ වෙද්දී මේ නව App platform එක India, Indonesia, Russia, සහ Malaysia ඇතුළු රටවල් 9ක් වෙත අත්හදා බැලීමට මේ සන්ධානය සුදානම් වෙනවා. මේ නව App platform එක හරහා App developer (යෙදුම් සංවර්ධකයින්) වෙත ජංගම දුරකතන සන්නාමයන් කිහිපයක් වෙත ම ගැළපෙන පරිදි එක්වර තම යෙදුම උඩුගත කිරීමේ හැකියාව ලැබෙනවා. සමස්ත ජංගම දුරකතන වෙළඳපොළ තුළින් 40% - 45% අතර ප්‍රමාණයක් මේ සමාගම් සතු වෙනවා. එනිසාවෙන් මේ සිදුවන සන්ධාන ගත වීම ඇමරිකාව ඇතුළු google සමාගම වෙත දැඩිව බලපාන බව නම් නොරහසක්. වැඩිකල් නොයා Huawei සමාගම ඔවුන්ගේ නවතම මෙහෙයුම් පද්ධතිය Harmony OS නිකුත් කිරීමට ඇති සුදානමක් පිළිබඳවත් දැනගන්නට ලැබෙනවා. කොහොම වුණත්, මේ නව මෙහෙයුම් පද්ධතිය වෙත Huawei සමාගම ඇමරිකානු ඩොලර් බිලියනයකට වඩා වෙන් කර ඇති බව theverge.com සඳහන් කරනවා. මේ සන්ධාන ගත වීම සිදුවන කාලය අතරතුර Huawei සමාගම ඔවුන්ගේ ඉදිරියට පැමිණීමට නියමිත උපාංග වෙත ඔවුන්ගේම AppGallary එකක් අන්තර්ගත කිරීමට සුදානම් වෙන බව අපට දැනගන්න ලැබුණා. ඒ පිළිබඳව වැඩි විස්තර ඉදිරි ලිපියකින් ඔබ වෙත ගෙන එන්නම්. මේ ගැන ඔබේ අදහස් අපට කියන්නත් අමතක කරන්න එපා.

Facebook සමාගම පසුගිය කාලය පුරාවටම විටින් විට විවිධ නඩු හබවලට පැටලුණු හැටි ඔබට මතක ඇති. පසුගිය දිනෙක ඔවුන්ට ඇමරිකානු ඩොලර් මිලියන 550ක වන්දි මුදලක් ගෙවන්නට එකඟවන්න සිදුවුණා. ඒ, කාලයක් තිස්සේ අධිකරණයේ විභාග වෙමින් පැවති class-action lawsuit (සාර්ව නියෝජන අධිකරණ ක්‍රියාමාර්ගය) එකක් සමථයකට පත් කරගැනීම සඳහා යි. 2015 වසරේ සිට විභාග වෙමින් පවතින මේ නඩුව සඳහා ඔවුන්ට මුහුණ දෙන්නට සිදුවුණේ, ඔබත් මමත් නිතර දෙවේලේ දකින facebook පහසුකමක් නිසාවෙන්ම යි. සාමාන්‍යයෙන් ඔබ පිරිසක් සමග හෝ තව පුද්ගලයෙක් සමග facebook වෙත upload කරන ඡායාරූපයක් වෙත බොහෝ විට ඔවුන්ව ඉබේම tag වෙනවා ඔබ දැකලා ඇති. ඔබට එය වටිනා පහසුකමක් වුණත්, එහි භයානක පැත්තක් තිබෙන බව ඔබට මොහොතකට හෝ සිතුණා ද? ඔබේ අවසරයකින් තොරව ඔබේ මුහුණේ අංගයන් පිළිබඳව scan කර දත්ත වාර්තාවක් ඔවුන් ළඟ ඉතිරි වන බව ඔබට සිතුණා ද? (biometric data) මේ නඩුවට මුලික වෙන්නේ ඒ කාරණය යි. මෙලෙස යම් අයෙකුගේ අවසරයකින් තොරව ජෛවමිතික දත්ත ගබඩා කරගැනීම ඔස්සේ Biometric Information Privacy Act උල්ලංඝනය වීම සිදුවෙනවා. මේ පනත මඟින් යම් ව්‍යාපාර ආයතනයක්, යම් පුද්ගලයෙකුගේ හෝ කොටසකගේ ජෛවමිතික දත්ත අවසරයකින් තොරව ගබඩා කරගැනීම වළක්වාලනවා. ඔවුන්ට එසේ ගබඩා කර තබා ගැනීමට අවශ්‍ය නම්, අදාළ පුද්ගලයාගේ අවසරය අත්‍යවශ්‍ය වෙනවා.

2018 වසර වන විටත් මේ නඩුව විභාග වී අවසානව තිබුණේ නම් නැහැ. නමුත්, ඒ වර්ෂයේ දී facebook සමාගම facial recognition වෙත පරිශීලකයන්ගේ අවධානය යම් තරමක් දුරට යොමු කරවන්නට සමත් වුණා. ඔවුන් විනිවිදභාවයකින් යුතුව තමන්ගේ ආයතනය ඔස්සේ facial recognition භාවිත කරන ආකාර සහ ඒ ඔස්සේ පරිශීලකයන් වෙත හිමි වන පහසුකම් පිළිබඳව විවෘතව සඳහන් කළා. ඊටත් අමතරව පරිශීලකයාට කැමති නම් මේ පහසුකම නවතා දමන්නටත් option එකක් ලබාදුන්නා. 2019 වසර වන විට facial recognitionව පරිශීලකයාට අවැසි නම් පමණක් සක්‍රීය කරගැනීමට ඔවුන් පහසුකම් සැලසුවා. ඒ අනුව තවදුරටත් පෙරනිමි සැකසුමක් ලෙස (default settings) ඔවුන් මේ පහසුකම නව පරිශීලකයන් වෙත ලබා දෙන්නේ නැහැ.

කොහොම වුණත්, මේ සිදුවීම මෙතරම් දුර රැගෙන ආ යුතු එකක් නොවන බව තමයි තාක්ෂණික ලෝකයේ බොහෝ දෙනෙකුගේ මත ය. 2019 වසරේ අග භාගයේ දී facebook සමාගම සිදුකළ ඉල්ලීම් සියල්ල අධිකරණයේ දී ප්‍රතික්ෂේප වීමත් සමගම, මේ නඩුව අවසන් කිරීමට තිබූ බව තමයි බොහෝ දෙනෙක් සඳහන් කරන්නේ. 2019 වසරේ අගෝස්තුව අවසානයේ පැවති නඩු විභාගයේ දී facebook සමාගම සිදුකළ ෆෙඩරල් අභියාචනයන් 3-0 ලෙස ප්‍රතික්ෂේප වුණා.

නිව්යෝර්ක් ටයිම්ස් පුවත්පතට අනුව මේ ඇමරිකානු ඩොලර් මිලියන 550 අතරට සමස්ත නඩුවේ නීති ගාස්තු පවා ඇතුළත් වෙනවා. ඒ වගේම මෙයින් ඉතිරි කොටස සුදුසු පරිශීලකයන් වෙත යොමු වේවි. මේ ඇමරිකානු ඩොලර් මිලියන 550 විශාල මුදලක් ලෙස ඔබට දැනුණත්, එය facebook සමාගමට එතරම් දැනෙන මුදලක් නොවන බව තමයි theverge.com වෙබ් අඩවිය සඳහන් කරන්නේ. පසුගිය වසරේ, එනම් 2019 වසරේ හතරවන කාර්තුව වෙද්දී ඔවුන්ගේ ආදායම ඇමරිකානු ඩොලර් බිලියන 21ක්. Biometric Information Privacy Act එක නිසාවෙන් සමාගම් වෙත නඩු පැවරුණු පළමු අවස්ථාව මෙය නොවේ. මීට පෙර ද ලෝකයේ අතිශය කතාබහට ලක් වූ Google සමාගම වෙත පැවරුණු නඩුව ඔබට මතක ඇති. 2016 google වෙත ජෛවමිතික දත්ත අනිසි භාවිතය පිළිබඳව නඩු පවරෙන්නට හේතු වුයේ පරිශීලකයන්ගේ ඡායාරූප අනිසි ලෙස උඩුගත කරමින්, ඔවුන්ගේ මුහුණුවල දත්තවලින් කෘතීම බුද්ධිමය වැඩසටහන් පුහුණු කිරීම යන චෝදනාව යටතේ යි. කොහොම නමුත්, මේ නඩුව 2018 වසරේ නිෂ්ප්‍රභා කිරීමට ඇමරිකානු අධිකරණය තීරණය කළා. ඒ පැමිණිලි කරුට සෘජුව හානියක් සිදුවන ලෙස කිසිවක් සිදුව නැති බව පවසමිනුයි. මීට අමතරව වරක් Snapchat වෙතත් මෙවැනි ජෛවමිතික දත්ත අනිසි භාවිතය පිළිබඳව චෝදනා එල්ල වී තිබෙන බව arstechnica.com වෙබ් අඩවියත් සඳහන් කර තිබුණා. නමුත්, ඒ නඩුවත් පසුකාලීනව සමථයකට පත් කරගන්නට පැමිණිලි පාර්ශවයට සහ සමාගමට හැකි වූ බව තමයි දැනගන්නට ලැබෙන්නේ.

කවර හෝ සමාජ ජාලයකට වඩ වඩාත් ඡායාරූප ඇතුළත් කිරීම අද වෙද්දී අතිශය භයානක දෙයක් බවට පත්ව තිබෙන බව ඔබ දන්නවා ද? ඒ පිළිබඳව අපි පසුගිය නව දශකය සහ Deep Fake භීතිකාව යන ලිපිය ඔස්සේ කතාබහ කළා. ඒ ලිපියත් ඔබ කියවිය යුතුම ලිපියක් ලෙසට අපි යෝජනා කරනවා. මේ ලිපිය ගැනත් ඔබේ අදහස් comment කරන්න අමතක කරන්න එපා!

අපි පෙර ඔබ වෙත ගෙන ආ හොඳම “wireless headphone ගැන ඔබ දන්නවා ද?” ලිපිය ඔස්සේ කතා කළේ මිලෙන් තරමක් වැඩි රැහැන් රහිත headphone පිළිබඳව යි. මේ ලිපිය ඔස්සේ දිගහැරෙන්නේ Budget කාණ්ඩයට අයත් වෙන Wireless Headphone ගැන යි. ඒවායේ දැනට පවතින මිල ගණන් වගේම, එම Headphoneවල ගුණාංග ගැනත් ඔබට මේ ඔස්සේ පැහැදිලි වේවි.

වසර ගණනාවක් ඇමසන් වෙබ් අඩවියේ වැඩිම විකිණුම් සහිත Headphone අතර පළමු තැන රැඳී සිටින Mpow 059 Bluetooth Headphone එක, අද වෙද්දී ලෝකය පුරා බොහෝ දෙනෙක් භාවිත කරන headphone එකක් බවට පත්ව තිබෙනවා. 40mm neodymium driver එකක් සහ CSR chip එකක් අන්තර්ගත මෙය, ඔබට ඉතා හොඳ සංගීතමය අත්දැකීමක් අඩු මුදලකට ලබාදෙන බව යි පරිශීලකයන් පවසන්නේ. සාමාන්‍යයෙන් මෙවැනි උපාංග මිලෙන් තරමක් අඩු නිසා වැඩි වෙලාවක් පැළඳ සිටීම යම් තරමක් අපහසු බව ඔබට සිතෙන්නට පුළුවන්. නමුත්, මෙහි ඇති around-ear cushion design එක එතරම් අපහසුවක් නොදැනෙන බැවින් දිගු වෙලාවක් එය පළඳින්නට ඔබට පහසුකම් සලසනවා. ඔබ Active Noise Cancellation පහසුකම සහිත හෙඩ්ෆෝන් එකක් නම් හොයන්නේ, මේ Mpow 059 ඔබට එතරම්ම ගැළපෙන එකක් නම් නෙවෙයි. Around-ear cushion design එක නිසාවෙන් passive noise isolating එකක් නම් සිද්ධ වෙනවා. කොහොම වුණත්, මේ හෙඩ්ෆෝන් එකේ බැටරිය වරක් සම්පූර්ණයෙන් ආරෝපණය කළ පසු පැය 20ක් පමණ ඔබට මෙය භාවිත කළ හැකි බව යි නිෂ්පාදකයන් සඳහන් කරන්නේ.

මෙහි දකින්න ලැබෙන ප්‍රධානම අඩුපාඩුවක් හැටියට Build Quality එක දක්වන්න පුළුවන්. තරමක් බාල වර්ගයේ ප්ලාස්ටික්වලින් නිමවා ඇති නිසා මෙහි Durability එක පිළිබඳව යම් යම් ගැටළු මතුවෙන්න ඉඩ තිබෙනවා. ඊට අමතරව මෙහි නිෂ්පාදකයන් පවසන්නේ, පැය දෙකකට වරක් වත් ඔබ හෙඩ්ෆෝන් එක ගලවා කන් දෙකට විවේකයක් ලබාදෙන ලෙසට යි. ඒ අතරතුර cushion සියල්ලම යළි යථා තත්ත්වයට පත් වීම සිදුවෙනවා. මෙහි මිල දැක්වෙන්නේ ඇමරිකානු ඩොලර් 29ත් 36ත් අතර යි.

සාමාන්‍යයෙන් තාක්ෂණයට ආස කරන ඔබ PANASONIC ErgoFit Earbud ගැන අසා නොතිබෙන්නට විදියක් නම් නැහැ. සාමාන්‍යයෙන් ඇමසන් වෙබ් අඩවිය ඇතුළු වෙබ් අඩවි ගණනාවක විකිණුම් අතර ඉහළම තැනක් ලබාගන්න PANASONIC ErgoFit Earbud වලට හැකියාව ලැබුණා. ඉතාම අඩු මුදලකට, සාමාන්‍ය ගුණාත්මක බවින් යුතු සංගීතමය අත්දැකීමක් ලබාදෙන්නට මේ උපාංගයට හැකි බව යි අපට දැනගන්නට ලැබුණේ. ඇමරිකානු ඩොලර් 11ත් 13ත් අතර මිලකට මෙය අන්තර්ජාලය ඔස්සේ මිලදී ගන්න ඔබට පුළුවනි. 5Hz සිට 24,000Hz දක්වා Frequency Response එකක් මෙහි තිබෙන බව නිෂ්පාදකයන් සඳහන් කරනවා. ඔබ මූලික අවශ්‍යතා සඳහා ඉතාම අඩු මුදලකට hands free එකක් හොයනවා නම්, මේ PANASONIC ErgoFit Earbud මාදිලිවලින් එකක් ඔබට හොඳටම ගැළපේවි.

ඔබත් අඩු මුදලට Sports මාදිලියක මුදලට හෙඩ්ෆෝන් එකක් හොයනවා නම්, මේ උපාංගය ඔබට අපූරුවට ගැළපේවි. Mpow Flame Bluetooth Headphone එක ඇමරිකානු ඩොලර් 19ත් 22ත් අතර මුදලකට අන්තර්ජාලය ඔස්සේ ඔබට මිල දී ගන්න පුළුවන්. ගෙවන ගානට උපරිම වටිනාකමකින් යුතු පහසුකම් සපයන මෙය, IPX7 Waterproof උපාංගයක් ලෙස තමයි වෙළඳපොළට නිකුත් වෙන්නේ. 11mm dynamic driversවලින් යුතු මේ Bluetooth Headphone එක, මෙම කාණ්ඩයේ වැඩිම විකිණුම් සහිත උපාංග මාදිලියක්. ඉතාම පහසුවෙන් කනේ රැඳෙන ලෙස බාහිර ආවරණයන් සැකසී ඇති මෙය, Unbox Therapy ඇතුළු ප්‍රසිද්ද youtube නාලිකා රාශියක ඇගයීමට ලක් වූ උපාංගයක් ලෙස හඳුන්වන්න පුළුවන්. මෙහි බැටරිය එකවරක් ආරෝපණය කළ පසු පැය 7-9ත් අතර කාලයක් ආයු කාලය රඳා පවත්වා ගන්නට සමත්. CVC 6.0 noise canceling microphone එකක් ඇතුළත් මේ උපාංගයට Active Noise Cancellation පහසුකම නම් නැහැ. ඉතාම හොඳ ගුණාත්මක මට්ටමක මෙහි sounds පවතින බව, පරිශීලකයන් බොහෝ දෙනෙක් සඳහන් කර තිබුණා.

Hi-Fi Sound සහිත ඉතාම හොඳ හෙඩ්ෆෝන් එකක් විදිහට මේය හඳුන්වන්නට හැකියි. එකවරක් ආරෝපණය කළ පසු පැය30කට ආසන්න කාලයක බැටරි ආයුකාලයක් සහිත මේ උපාංගය බජට් හෙඩ්ෆෝන් අතර ප්‍රධාන තැනක ඉන්නවා. Active Noise cancelling ඉතාම හොඳ මට්ටමින් ක්‍රියාත්මක වෙන මේ උපාංගය කිසිම අපහසුවකින් තොරව දවස පුරාම වුණත් පැළඳගෙන ඉන්න පුළුවන්. 40mm large-aperture driversවලින් සමන්විත මේ උපාංගය තුළින් ඔබට ඉතාම පැහැදිලිව ශබ්දයන්ට හා සංගීතයට සවන් දෙන්න හැකියාව සලසනවා. නවතම Bluetooth 5.0 තාක්ෂණයක් සමගින් නිකුත් වෙන මෙය සතුව cVc 8.0 noise-cancelling microphone එකක් පවතිනවා.

ඉහත මම සඳහන් කරපු හෙඩ්ෆෝන්වලට වඩා නම් මිලෙන් තරමක් වැඩි වුණත්, ඒ ගෙවන ගාණට උපරිම පහසුකම් ලැබෙන බව තමයි බොහෝ දෙනෙක් සඳහන් කරන්නේ. Build Quality එක අතින් ගත්තත්, ඉතාම ඉහළ තැනක තියෙන මෙකී උපාංගය ඇමරිකන් ඩොලර් 72.86ක් පමණ වෙනවා. හැබැයි ඉතින්, මේ හෙඩ්ෆෝන් එක ලංකාවට නම් මේ වෙද්දී අලෙවි නොකරන බව තමයි සමාගම සඳහන් කරන්නේ. ඒ නිසා වෙනත් විකිණුම්කරුවෙකුගෙන් හෝ තෙවන පාර්ශවයක් ලවා උපාංගය ලංකාවට ගෙන්වා ගන්න ඔබට සිදුවෙනවා.

දවසේ වැඩි කාලයක් අන්තර්ජාලය හා IoT සමග කාලය ගෙවන ඔබත්, මමත් පෞද්ගලිකත්වය ගැන මීට වඩා අතිශය සැලකිලිමත් විය යුතු බව අප මීට ටික දිනකට පෙර පළ කළ ලිපි ගණනාවක් ඔස්සේ පැහැදිලි කළා ඔබට මතක ඇති. තවද, අන්තර්ජාලයේ පළවන දෑ එකවර පිළිගැනීම හෝ එක් මූලාශ්‍රයකින් පමණක් තොරතුරු ලබාගැනීමත් ඉතාම භයානක දේවල් බවට අද වෙද්දී පත්ව තිබෙනවා. තාක්ෂණයේ දියුණුව සමග AI එසේ නොමැති නම්, කෘතීම බුද්ධි වැඩසටහන් භාවිතයෙන් විවිධ ඡායාරූප, වීඩියෝ පට අතිශය තාත්වික අන්දමෙන් නිර්මාණය වෙන්න පටන් ගැනීමත් සමග මේ තත්ත්වයන් තවත් භයානක වන්නට පටන් ගත්තා. මේ පිළිබඳව පෙර ලිපියක අපි ඔබව දැනුවත් කළා. ඔබ තොරතුරු තාක්ෂණය පිළිබඳව යම් දැනුමක් ඇත්තෙක් නම් අනිවාර්යෙන්ම Deepfake ගැන අසා ඇති. ප්‍රධාන වශයෙන් මේ තාක්ෂණයන් ඔස්සේ නිර්මාණය වෙන්නේ වීඩියෝ පට යි. භයානකත්වය වන්නේ; තවදුරටත් එවැනි වීඩියෝ පට සැබෑ ඒවා ද, නැති නම් කෘත්‍රීමව නිර්මාණය කරන ලද ඒවා ද යන්න සොයාගැනීම ඉතාම අපහසු වීම යි.

Deepfake පිළිබඳ කතිකාවතක් නිර්මාණය වෙන්නේ 2017 පමණ මෑතක වුවත්, මීට සමාන තාක්ෂණික ක්‍රමවේදයන් චිත්‍රපට නිර්මාණයන්වල දී සුලබ ව භාවිත කර තිබෙනවා. මුල් කාලයේ නිර්මාණය වූ මෙවැනි වීඩියෝවක දී පුද්ගලයෙකුගේ මුහුණේ ඉරියව්වල සිදුවන වෙනස්කම්, ආලෝකකරණයේ වෙනස්කම්, හිසකෙස් හෝ රැවුල වැනි දේවල් එහා මෙහා වීම ආදී තත්ත්වයන් බොහොමයක් ගැන සැලකිලිමත් වීම අත්‍යවශ්‍ය වුණා. ඒ නිසාවෙන් වීඩියෝවක තත්ත්පර කිහිපයක් වුවත්, මේ විදිහට එකෙන් එක සකසන්න වැය වන කාලය සහ මුදල් ප්‍රමාණය ඉතාම විශාල යි. එත් මේ වෙද්දී අතිශය සංකීර්ණ ක්‍රමවේදයන් භාවිත කරමින් AI වැඩසටහන් මඟින් මේවා ඉතා ඉක්මණින් නිර්මාණය කරනවා. ඔබට මතක නම් Fast Furious 7 චිත්‍රපටය නිෂ්පාදනය කරමින් සිටින අතරතුර එහි ප්‍රධාන චරිතයක් රඟපෑ Paul Walker මිය යනවා. ඉන් අනතුරුව රූගත කිරීම් සිදුවෙන්නේ ඔහුගේ සහෝදරයා සහ තවත් ඔහුගේ පෙනුමට ආසන්න සමානකමක් දක්වන සහාය නළුවන් යොදාගෙන යි. ඔවුන්ගේ ස්වරූපයන් Paul Walkerගේ රූපයට සමාන කරවන්නට භාවිත වෙන්නේ AI තාක්ෂණය ඔස්සේ Deepfake ක්‍රමවේදයන් සහ CGI ක්‍රමවේදයනුයි. පහළ Video වෙන් ඔබට ඒ පිළිබඳව යම් අදහසක් ලබාගන්නට පුළුවන්.

නමුත්, අද වෙද්දී ඔබත් දැනුවත්ව හෝ නොදැනුවත්වම හෝ එවැනි ක්‍රමවේදයන් භාවිත කරනවා. Deepfakeවල සිදුවෙන ක්‍රියාවලිය සරලව හැඳින්වුවොත්, එය කෘත්‍රීම බුද්ධිය සහ Machine Learning හෙවත් යාන්ත්‍රික ඉගෙනුම් ක්‍රමවේදයන් භාවිතයෙන් සිදුවන ක්‍රියාවලියක් ලෙස අර්ථ දක්වන්න පුළුවන්. දැනටමත් ඔබ Snapchat/ Instagram වැනි යෙදුම් ඔස්සේ මුහුණු වෙත විවිධ සජීවී Filters එකතු කරනවා නම්, නොදැනුවත්වම වගේ ඔබත් යම් දුරකට ඒ ක්‍රමවේදයන්ගේ අත්දැකීම ලැබූ පුද්ගලයෙක්.

AI ආශ්‍රිත Deepfake නිර්මාණය කරන වැඩසටහනකට සාර්ථක ප්‍රථිපල ලබාගන්නට නම් යම් පුද්ගලයෙකුගේ වීඩියෝ හෝ ඡායාරූප විශාල ප්‍රමාණයක් අවශ්‍ය වෙනවා. ඒ ඔස්සේ ඔහුගේ හෝ ඇයගේ මුහුණෙන් පෙන්වන බොහෝ ඉරියව් හඳුනාගන්නට මේ වැඩසටහන සමත් වෙනවා. මේ ඔස්සේ එසේ ඉගෙන ගත් ඉරියව් වෙනත් වීඩියෝවක පුද්ගලයෙකු වෙත ආදේශ කරෙනවා. පහතින් දැක්වෙන්නේ එවැනි වීඩියෝවක්.

බොහෝ දෙනෙක් හොඳින් හඳුනන ජනප්‍රිය පුද්ගලයන්ට මෙය විශාල ගැටළුවක්. දැන් පවතින Deepfake වැඩසටහන්වලට ස්වයංක්‍රීය ව සෙවුම් යන්ත්‍ර භාවිත කර ඡායාරූප සොයාගන්නට පවා හැකියාව තිබෙනවා. ඔබ අන්තර්ජාලය වෙත, සමාජ ජාලයන් වෙත ඡායාරූප වැඩි වශයෙන් එකතු කරන්නෙක් නම් මෙවැනි Deepfake වීඩියෝවක් ඔබේ රූපය සහිතව නිර්මාණය කිරීමත් එතරම්ම අපහසු නැහැ. ඔබට මතක නම සුරූපී නිළි ගල් ගඩෝට් යොදාගෙන සැකසූ අසභ්‍ය වීඩියෝව ඇතුළු ජනප්‍රිය තරු යොදාගෙන සකසන ලද Deepfake videos, ඔවුන්ගේ ජනප්‍රියත්වය නිසාම සමාජය තුළ ඉතා ඉක්මණින් මේවා ප්‍රචාරය වීම වළක්වන්නට බැහැ. මෙය අතිශය ගැටළුකාරී තත්ත්වයක් බවට අද වෙද්දී පත්ව තිබෙනවා. Twitter ඇතුළු සමාජ ජාලා ගණනාවක් මෙවැනි දේ ප්‍රචාරය කිරීම වැළැක්වීමට කටයුතු කර තිබෙනවා නමුත්, එය ප්‍රමාණවත් ද යන්න නම් තවමත් ගැටළුවක්.

2019 උණුසුම් කළ Faceapp භීතිකාව ඔබට මතක ඇති. මේ භීතිකාව සමග කරළියට පැමිණි ප්‍රධාන මතයක් වන්නේ මේ app එක හරහා අපේ මුහුණේ ඉරියව් සහ ඡායාරූප ලබාගෙන ඒ ඔස්සේ කෘත්‍රීම බුද්ධි වැඩසටහනක් පුහුණු කිරීම සිදුවෙනවා යන්න යි. කොහොම නමුත්, Faceapp එක හරහා එවැන්නක් සිදුනොවන බවත්, ඒ අවස්ථාවේ load කරවන image එකෙහි cache image එකක් පමණක් upload වීම සිදුවන බවත් Faceapp නිර්මාණකරුවන් සඳහන් කළා. මෙහි දී upload වෙන cache image එක අනුව නිර්මාණය වෙන overlay එක ඇප් එක වෙත පැමිණ එතන සිදුවන process එකක් මඟින් අවසාන ඡායාරූපය නිර්මාණය වෙන බවත් ඔවුන් වැඩිදුරටත් සඳහන් කළා.

ඔබ අනිසි බියක් ඇති කරගත යුතු නම් නැහැ. නමුත් එවැනි ක්‍රමවේදයන් තිබෙන බවත්, ඒ ඔස්සේ සිදුකළ හැකි දේ පිළිබඳවත් යම් අවබෝධයක් ලබාගැනීම වටිනවා. අන්තර්ජාලය තුළ Privacy කියන්නේ මිත්‍යාවක්. එනිසා යම් ලියවිල්ලක්, වීඩියෝවක් දුටු පමණින් කලබලයට පත් නොවී, ඒ පිළිබඳව නිර්පාක්ෂික සොයාබැලීමක් සිදුකර, එවැනි යෙදුම් භාවිතා කරනවා ද නැද්ද යන්න තීරණය කිරීම තමයි නුවණට හුරු.

චීනයේ තොරතුරු තාක්ෂණය හා සම්බන්ද සමාගම් වටා බිහි වූ රැල්ලක් මේ වෙද්දී ලෝකය පුරාම පැතිරෙන බවට දැනගන්නට ලැබෙනවා. මේ රැල්ල නම්; තමන්ගේ සේවකයන් දිරිමත් කිරීමට Cheerleadersලා බඳවා ගැනීම යි. බොහෝ විට මෙසේ බඳවා ගන්නේ පරිගණක වැඩසටහන් නිර්මාණය කරන සමාගම්. තමන්ගේ ක්‍රමලේඛකයන්ගේ කාර්යක්ෂමතාව අකණ්ඩව තබාගැනීම අරමුණු කරගෙන යි මෙය සිදුකරන්නේ. මෙලෙස බඳවා ගන්නා දිරිගන්වන්නියන් “programmer motivator”වරු එහෙම නැති නම්, 'programming cheerleaders'වරු විදිහට යි හැඳින්වෙන්නේ. මේ නවතම රැකියාව ජනප්‍රිය කරවීමට මුල් වූ බවට සැලකෙන්නේ සුරූපී නිළි ‘Shen Yue’ යි. කතා මාලාවන් ගණනාවක රඟපෑමේ යෙදුණ අතිශය ජනප්‍රිය නිළියක් වගේම, ඇය “programmer motivator”වරියක ලෙසත් සේවය කරන බව New York Times පුවත්පත සඳහන් කර තිබුණා. 26 හැවිරිදි ඇය, සිවිල් ඉංජිනේරු උපාධියක් හිමි තැනැත්තියක්.

මෙලෙස cheerleadersලා ලෙස බඳවාගන්නා යුවතියන්ට පැවරෙන රාජකාරී ගණනාවක් තිබෙනවා. ප්‍රධාන වශයෙන් ක්‍රමලේඛකයන් විටින් විට දිරිමත් කිරීම ප්‍රධාන රාජකාරිය වෙනවා. සාමාන්‍යයෙන් තොරතුරු තාක්ෂණය හා ඒ ආශ්‍රිත රැකියා කරන පුද්ගලයන් යම් තරමක් ඒකාකාරී ජීවිතයක් ගෙවන්නන්. දිගින් දිගටම පරිගණකය අසල වාඩි වී සිටීමෙන් යම් තරමක් දුරට ඔවුන්ගේ කාර්යක්ෂමතාව අවම විය හැකි බව ආයතන ප්‍රධානීන්ගේ මතය යි. මේ සුරූපී cheerleadersලා වෙත විටින් විට කතා කිරීමෙන් එය අවම කර ගැනීමට හැකිවනවා. ඒ වගේම අත්පොළසන් නාදයන් ලබාදීමත් මේ දිරිමත් කිරීම් යටතට ඇතුළත්. ක්‍රමලේඛනයක් නිවැරදිව කේතනය කිරීමෙන් අනතුරුව ඔවුන් වෙත cheerleadersලාගෙන් අත්පොළසන් නාදයක් වගේම, ඔබ හොඳින් එය කළා වගේ අගය කිරීමක් ලැබෙනවා. මෙයින් ක්‍රමලේඛකයන් දිරිමත් වෙන බව තමයි දැනට පවතින මත ය. ඊට අමතරව නිරතුරු සිනහා මුසු මුහුණින් සිටීම ඔවුන්ට අනිවාර්ය දෙයක්. විටින් විට සේවකයන්ට විඩාව දැනෙන විට ඔවුන්ගේ උරහිස් සම්භාහනය කිරීම, ඔවුන් අධෛර්යයට පත් වූ විට ඔවුන් ඇස වසාලීමත් මොවුන්ට කරන්න සිදුවන රාජකාරීන්ගෙන් කොටසක්. ඊට අමතරව ක්‍රමලේඛන සමග ටේබල් ටෙනිස් වැනි ක්‍රීඩාවක යෙදීමටත් සමහර විට ඔවුන්ට සිදුවනවා. ඒ සියල්ලෙහි අරමුණ ක්‍රමලේඛනගත කිරීම්වල ඇති ඒකාකාරී බව මඟහරවා ගැනීම යි.

මෙලෙස cheerleader කෙනෙක් ලෙස සේවයට යාම එතරම්ම පහසු කටයුත්තකුත් නොවන බව තමයි දැනගන්න ලැබෙන්නේ. එලෙස ආයතනයක් වෙත සම්බන්ධ වීමට ඔබට යම් මට්ටමක තාක්ෂණික දැනුමක් අවශ්‍ය වෙනවා. ඒ වගේම හොඳින් ඉංග්‍රීසි කතා කිරීමේ හැකියාව අමතර සුදුසුකමක් වන බව තමයි ආරංචි වෙන්නේ. පියකරු සිනහවක උරුම කාරියක් වීම, සාමාන්‍ය උස වගේ කරුණු ද, යම් යම් ක්‍රීඩාවන් කිරීමට ඇති හැකියාවනුත් මෙහි දී සලකා බැලෙනවා. ඊට අමතරව makeup දැමීමේ හා ඒ පිළිබඳ හැකියාවත් තිබිය යුතුම යි. බොහෝ විට මෙවැනි වෘත්තීන් සඳහා කාන්තාවන් තෝරාගන්නේ සමාජ ජාලා ඔස්සේ යි. නමුත්, දැන් දැන් මේ වෙනුවෙන් විවිධ දැන්වීම් අන්තර්ජාලය පුරාම වගේම පුවත්පත්වලත් පළ වනවා. මොවුන්ගේ රැකියාවේ අරමුණ ලෙස ඔවුන්ට හඳුන්වා දෙන්නේ; යම් මට්ටමකට සමාජයෙන් ඈත්ව කාලය ගෙවන ක්‍රමලේඛකයින් ඇතුළු පිරිස තරමක් දුරට හෝ සමාජය වෙත හුරු කර වීම යි. ඒ වගේම ඔවුන් මුහුණ දෙන අධික පීඩනයන් ඔස්සේ විෂාදය වැනි මානසික තත්ත්වයන් වෙත ඔවුන් යොමු වීම වළක්වාලීමත් cheerleadersලා අතින් ඉටු කෙරෙන කාර්යභාර්යයක්. ඔවුන්ව මේ වෙනුවෙන්ම පුහුණු කිරීමේ වැඩසටහන් පවා ක්‍රියාත්මක වෙනවා. සේවකයින්ගේ මානසික වාතාවරණයන් හඳුනාගැනීම, අවශ්‍ය නම් වෛද්‍ය ප්‍රතිකාර වෙත යොමු කිරීම වැනි කාරණා වෙනුවෙන් ඔවුන් දැනුවත් කෙරෙනවා.

කොහොම නමුත්, මෙලෙස cheerleadersලා බඳවා ගැනීම යම් යම් අවස්ථාවන්වල ඉතා දැඩිව විවේචනය වූ අවස්ථා අන්තර්ජාලයෙන් අපට හමුවුණා. චීනයේ ක්‍රමලේඛ අභිප්‍රේරකයින් විවිධ අක්‍රමික ලෙසින් සේවයේ යොදවන බවත්, වක්‍රාකාරයෙන් ඔවුන්ව ලිංගික සේවකයින් ලෙස ක්‍රියා කරන බවත් සමාජයේ යම් යම් පිරිස් චෝදනා නගනවා. ඒ චෝදනා කෙසේ වුවත්, චීනයේ ක්‍රමලේඛ අභිප්‍රේරකයින් බඳවා ගැනීමේ සංකල්පය අද වෙද්දී ලෝකය පුරා ව්‍යාප්ත වෙන්නට පටන් ගෙන. විශේෂයෙන් තම වෘත්තිය වශයෙන් පරිගණක ක්‍රීඩාවල නිරත වන්නන් දිරි ගැන්වීමට cheerleadersලා හෙවත් පරිගණක ක්‍රීඩක අභිප්‍රේරකයින් වෙත දැන් රැකියා වෙළඳපොල විවෘතව තිබෙනවා. පරිගණක ක්‍රීඩකයන් නිතරම දැඩි ලෙස කෝපයට පත් වීම අවම කිරීම වැනි දේ වෙනුවෙන් මේ අභිප්‍රේරකයින් යොදවා ගන්නවා. සේවය කරන පරිසරය සතුටු දායක එකක් කර වීම වෙනුවෙන් ඔවුන් කරන සේවය ප්‍රශංසනීය බව තමයි තාක්ෂණික ලෝකයෙන් වාර්තා වෙන්නේ. ලංකාව වැනි රටවල්වල මෙවැනි රැකියා සමාජීය වාතාවරණයන් හා සංස්කෘතික පසුබිම් මත එතරම්ම නොගැළපෙන බව පෙනුණත්, මේ මඟින් සමාජයෙන් කොන් වන විශාල පිරිසක් වෙත සහාය ලැබෙන බව nytimes.com පළ කර තිබූ වාර්තාවේ සඳහන්.

තාක්ෂණයේ දියුණුවත් සමග තොරතුරු සහ දත්ත සැනෙකින් ලෝකය පුරාවටම බෙදාහැරීමේ හැකියාව අද මිනිසා සතු යි. නමුත්, මෙලෙස බෙදාහැරෙන තොරතුරු, දත්ත අතර යහපත් දේ වගේම තව කෙනෙකුට හානියක් වෙන ඔවුන්ගේ අතිශය පෞද්ගලික දත්ත වැනි දේත් තියෙන්නට පුළුවන්. මෙලෙස සමාජගත වන තව කෙනෙකුගේ පෞද්ගලික දත්ත ලීක් වෙච්ච දෙයක් විදිහට සමාජයේ පැතිරෙන්නේ ඉතාම වේගයෙන්. එසේ වීම අවම කරගන්න ඔබත් කැමති ද? ලීක් වුණොත් කරන්න ඕනේ දේවල් දන්නවා ද? මේ ලිපිය හරහා දිගහැරෙන්නේ ඒ පිළිබඳව යි. ඒ වගේම ලීක් වෙන හැම දෙයක්ම ඇත්ත නොවන බවත් ලිපිය අවසන් වෙද්දී ඔබට වැටහේවී.

1996 පමණ සිට අන්තර්ජාලය තුළ මෙවැනි පෞද්ගලික දේ සහ අසැබි දේ ලීක් වීමට වැට බඳින්නට ලෝකය පුරා රජයයන් විවිධාකාර උත්සාහයන් දරා තිබෙනවා. අවාසනාවට ඒ කිසිවක් අද වෙනතුරුත් සම්පුර්ණයෙන්ම සාර්ථක වෙලා නැහැ. ඔබ මේ ලිපිය කියවන විටත්, සමාජයේ අතිශය කතාබහට ලක් වන ලීක් වූ හඬපට, වීඩියෝපට තිබෙන්නට පුළුවන්. විශේෂයෙන්ම, ඔබත් ටිකක් තරුණ වයසේ පසුවෙන්නෙක් නම් Whatsapp, Viber වැනි සේවා හරහා හෝ සමාජ ජාල හරහා ඔබේ ස්මාට්ෆෝන් එකට, පරිගණකයට මෙවැනි වීඩියෝවක්/ ලින්ක් එකක් නොපැමිණියා වෙන්න බෑ. මෙවැනි වීඩියෝ/ ඡායාරූප රූගත කිරීම කොතරම් දුරට නිවැරදි ද යන්න අපට තීරණය කරන්න හැකියාවක් නැහැ. ඒක පුද්ගලානුබද්ධ කාරණයක්. කොහොම වුණත්, ඒ වීඩියෝ/ඡායාරූප/හඬපට ලීක් වීම අවම කර ගන්නේ මෙහෙම යි.

වීඩියෝ/ඡායාරූප/හඬපට හෝ මොනයම් හෝ පෞද්ගලිකත්වයන්ට හානි වෙන දේ තලුමරමින් නරඹන පිරිසට අමතරව, ඒ ඔස්සේ මුදල් සොයන පිරිසකුත් අද වෙද්දී නිර්මාණය වෙලා සිටිනවා. කෙටි කරන ලද ලින්ක් එකක් (short link) ඔස්සේ බොහෝ විට මේ දේවල් හුවමාරු වීම සිදුවෙනවා. මේ ලින්ක් ඔස්සේ අදාළ වෙබ් පිටුව වෙත පිවිසීමේ දී වෙළඳ දැන්වීම් ගණනාවක් පසු කර යන්නට ඔබට සිදුවෙනවා. මේ වෙළඳ දැන්වීම් ඔස්සේ videoව upload කරන පුද්ගලයා වෙත මුදලක් ලැබෙනවා. ඒ වගේම අදාළ වීඩියෝව වැඩි පිරිසක් බාගත කර ගත්තොත්, මෙවැනි වීඩියෝ ගබඩා කර තබාගන්නා cloud සේවා මඟිනුත් (ඩවුන්ලෝඩ් කිරීම් ප්‍රමාණය අනුව) මුදල් ගෙවීම් සිදුකෙරෙනවා. ඉතාම ආකර්ශනීය මාතෘකාවක් සමග පළ වෙන මෙවැනි ලින්ක් හරහා පරිශීලකයන් විශාල ප්‍රමාණයක් අදාළ වෙබ් පිටු වෙත පිවිසීම සිදුවෙනවා. එහෙත්, මේ වෙද්දී නම් facebook වැනි සමහරක් සමාජ ජාල එවැනි වෙබ් අඩවිවල ලින්ක් පළ කිරීමට හෝ පණිවිඩ ලෙස යැවීමට ඉඩ ලබා දෙන්නේ නැහැ. Facebook Messenger, Telegram ,Whatsapp වැනි පණිවුඩ සහ බහුමාධ්‍ය හුවමාරු කිරීමට හැකි app හරහාත් මේවා හුවමාරු කිරීම දැන් දැන් තරමක් අපහසුවන්නට ඔවුන් ක්‍රියා කර තිබෙනවා. එනමුත්, ඒ කිසිවක් අතිසාර්ථක ක්‍රමවේදයන් නොවන බව ඔබත් මමත් හොඳින්ම දන්නා කරුණක්.

වීඩියෝ/ඡායාරූප/හඬපට හෝ ඕනෑම අයුරකින් ලීක් වී සමාජගත වන දෙයක සඳහන් වන හෝ අන්තර්ගත වන හෝ දකින්නට ලැබෙන පුද්ගලයන් හා ඔවුන්ගේ සමාජ තත්ත්වය, මුහුණු හෝ අනන්‍යතාව, දර්ශනවල හෝ හඬේ පැහැදිලි බව, වීඩියෝ පටවල නම් කාල පරාසය වගේම භාෂාව වැනි දේ අනුව බොහෝ විට මෙවන් දේවල් හි වටිනාකම තීරණය වෙනවා. එහි කථානායකයන් ප්‍රසිද්ධ පුද්ගලයන් නම් මෙහි වටිනාකම ඉතාම ඉහළ යි. ඒ නිසාවෙන් ලීක් විය හැකි එවැනි ඕනෑම දෙයක් ඔබ සතු නම්, එයින් ඔබට හෝ තවත් පුද්ගලයෙකුට, පිරිසකට අපහසුතාවයන් ඇති විය හැකි නම් ඔබ වඩාත් ප්‍රවේසම් විය යුතුම යි.

ලීක් වීමේ අවදානමක් තිබෙන දේ පටිගත හෝ චායාරූපගත නොකර සිටීමට ඔබට වගබලා ගත හැකි නම්, ලබාදෙන්නට හැකි හොඳම පුර්වාරක්ෂාව එය යි. ඔබ එලෙස නොකර සිටින තාක් කල්, ඔබේ කීර්ති නාමයට මෙවැනි දෙයකින් කැළලක් ඇති කිරීමට තව කෙනෙකුට ඇති ඉඩ ඉතාම අවම යි.

මේ වෙද්දීත් ඔබ සන්තකයේ ඇති එවැනි වීඩියෝ/ඡායාරූප/හඬපට හෝ ඕනෑම දෙයක් සදහටම මකා දමනවා නම් එය නිවැරදිව සිදුකරන්නේ මෙහෙම යි. mobile phones, memory cards, hard disks වැනි ගබඩා උපාංගයක ගබඩා කර ඇති දේ එක වර ඔබ delete කළ සැනින් මැකී යන්නේ නම් නැහැ. අදාළ ෆයිල් එක උපාංගය තුළ තිබෙන ස්ථානය හඳුනාගැනීමට අදාළ තොරතුරු මකා දැමීම පමණයි එවිට සිදුවෙන්නේ. මකා දැමූ දත්ත ස්ථාපනය කළ හැකි recovery software එකක් මඟින් එවැනි දත්ත නැවත ලබාගැනීමට හැකියාව තිබෙනවා. ඒ නිසාවෙන් මෙවැනි අතිශය වැදගත් දත්ත ගොනු මකා දැමීමේ දී zero filling tool එකක් හෝ file shredder tool එකක් භාවිතා කිරීම අතිශයයින්ම වැදගත් වෙනවා. මේ tool එකේ ක්‍රියාකාරිත්වය ඔස්සේ එවන් ගොනු නැවත යථාතත්ත්වයට පත් කළ නොහැකි ලෙසින් මකා දැමෙනවා.

සමහර විට ඔබ ළඟ ඇති ගොනු එකවර මකාදමන්න ඔබට නොහැකි වෙන්න පුළුවන්. එවිට කරන්න තිබෙන හොඳම විසඳුම වෙන්නේ encrypt මෘදුකාංගයක් භාවිත කිරීම යි. මෙහි මුරපදය නොදන්නා තාක් ඒ වෙත ඇතුළු වීම හෝ ගොනු භාවිත කිරීම ඉතාම අපහසු යි. පාස්වර්ඩ් එක සඳහා දීර්ඝ යමක් යොදන්නත් අමතක කරන්න එපා. වෙන කෙනෙකුට අනුමාන කිරීම් අපහසු දෙයක් නම් වඩාත් යහපත්. ශක්තිමත් මුරපද නිර්මාණය කරගන්න Lastpass වැනි සේවාවක් භාවිත කරන්න ඔබට පුළුවන්. නමුත්, මෙවැනි encrypt (ගුප්ත කේතනයන්) කිරීම් නැවත decrypt (විකේතනය) කිරීම කළ නොහැක්කක් නොවන බව ද ඔබ මතක තබාගත යුතුම යි.

ඔබේ පෞද්ගලික දත්ත වැඩිපුරම ලීක් වීමේ අවදානම පවතිනේ අලුත්වැඩියා කිරීමේ ස්ථානයන්ගෙන්. ඔබ සතුව එවැනි අතිශය පෞද්ගලික දත්ත තිබේ නම්, ඔබේ පරිගණකය හෝ ස්මාට්ෆෝන් එක අලුත්වැඩියාව සඳහා දින කිහිපයක් සේවා ස්ථානයක තබා තිබීම එතරම්ම නුවණට හුරු නැති බව මතක තබාගන්න. ඉලෙක්ට්‍රොනික උපාංග service සහ repairing ක්ෂේත්‍රයේ බහුතරයක් ඉතාම විශ්වාසවාසදායී සේවයක් සැපයුවත්, ඔබ සතුව ලීක් වීමේ වටිනාකම සහිත දේ පවතිනවා නම් අවදානමට පෙර සුදානම ඔබ සතු යි.

ඔබ ජංගම දුරකතනය විකිනීමක් සිදුකරනවානම් එහි දීත් සම්පුර්ණ දුරකතනයම encrypt කර format කර විකිණීමට වග බලාගන්න. එවිට දත්ත යලි ස්ථාපනය ඉතාම අපහසු යි. encrypt කරන ආකාරය ඔබට අන්තර්ජාලයෙන් ඉතාම පහසුවෙන් සොයාගන්න පුළුවන්.

1927 අසභ්‍ය ප්‍රකාශන සම්බන්ධ නීතිය අසභ්‍ය ප්‍රකාශන පනත ලෙස 2005 වර්ෂයේ දී සංශෝධනය කර ඇති අතර, එයට අනුව වගේම දණ්ඩ නීති සංග්‍රහයේ 285, 286 වගන්තිවලට අනුව පුද්ගලයන්ට හානි විය හැකි මුද්‍රිත චිත්‍ර, සිතුවම්, පෝස්ටර්, සංඥා ඡායාරූප, චිත්‍රපට, වීඩියෝ දර්ශන බෙදාහැරීම, ළඟ තබාගැනීම, නිපදවීම, ආනයනය කිරීම හෝ අපනයනය කිරීම, ප්‍රසිද්ධ කරවීම දඬුවම් ලැබිය හැකි වරදවල් බව සඳහන් වෙනවා. තවත් සරවල කිව්වොත්; ඔබ උඩුගත නොකළත් ඔබට ලැබෙන වීඩියෝවක් whatsapp වැනි සේවාවක් හරහා ලැබෙන වෙනත් කෙනෙකුට forward කිරීමත් සිර දඬුවමක් දක්වා දුරදිග යන්න ඉඩ තියනවා.

SLCERT නැත්නම්, පරිගණක හදිසි ප්‍රතිචාර අංශයට, අපරාධ පරීක්ෂණ දෙපාර්තමේන්තුවට එහෙමත් නැති නම් ළඟම තිබෙන පොලිස් ස්ථානයට වහාම සිදු වූ දෙය පිළිබඳව පැමිණිල්ලක් ඉදිරිපත් කරන්න. ඊට අමතරව ෆේස්බුක්, ගූගල් වැනි ආයතනවලට මේ ගැන පැමිණිලි කරන්න ඔබට පුළුවන්. ඔවුන්, සිය විශ්ලේෂණ මෘදුකාංග හරහා තවදුරටත් එවැනි දේ ප්‍රචාරණය වීම තරමක් දුරට අවම කරාවී. හිතන්න ඔබේ මේ අතිශය පුද්ගලික දේ වීඩියෝ පටයක් නම්, එය ප්‍රසිද්ධ කාමුක දර්ශන අඩංගු වෙබ් අඩවියක පළ වෙලා තිබෙනවා කියලා. ඔබට පුළුවන් ඔවුන්ව වහාම සම්බන්ධ කරගන්න. ඔවුන් ඔබේ පැමිණිලිවලට කන් දෙන්න බැඳී ඉන්නවා. email පණිවුඩයක් මඟින් ඔබ කරන දැනුම් දීමක් වෙනුවෙන් ඉතාම ඉක්මනින් අදාළ දේ වෙබ් අඩවිවලින් ඉවත් කරන්න ඔවුන් පියවර ගන්නවා. හැකි නම් කෙටි කලකට ඔබේ සමාජ ජාලා අක්‍රීය කරන්න කියලත් අපි ඔබට යෝජනා කරනවා. හිත ශක්තිමත් කරගන්න, අවශ්‍ය නම් මානසික වෛද්‍යවරයෙකුගේ සහාය පතන්න. ඔවුන් ඔබට ජීවියට මුහුණ දෙන්න අවශ්‍ය ශක්තිය සපයාවී.

අන්තර්ජාලය ඇතුළත පළ වන සියලු දේ සත්‍ය නොවන අතරම, ඔබ අන්තර්ජාලය සහ සමාජ ජාල භාවිත කරනවා නම් privacy කියන්නේ හුදෙක් වචනයක් පමණක් බවත් අපි ඔබට මතක් කරනවා. දෛනික තාක්ෂණික පරිශීලකයෙක් විදිහට මෙවැනි කෙනෙකුගේ පෞද්ගලික දර්ශන කෙසේ හෝ ඔබ වෙත ලැබුණොත් හැම විටම End user කෙනෙක් වෙන්න කියලා අපි ඔබෙන් ඉල්ලනවා. ඔබ රස විඳින්නේ හෝ බෙදාගන්නේ තව විශාල පිරිසකගේ ජීවිතවල ඉතා අමිහිරි දෙයක් බවත් ඔබ මතක තබාගන්න.

ඊට අමතරව Deep Fake වැනි ක්‍රමවේදයන් ඔස්සේ ඔබේ සමීපතමයන් වුවත්, අනුකරණය කළ හැකි බවත් ඔබට මතක් කරනවා. ඒ පහළ ඇති ‘සබැඳි ලිපි’ ඔස්සේ ඔබට දැනගන්නට හැකි වේවි. එනිසාවෙන් අන්තර්ජාලයේ පළ වෙන සියල්ල සත්‍ය නොවන බව ඔබ වටහාගත යුතුම යි.

මේ ගැන අදහස් පහළින් comment කරන්න අමතක කරන්න එපා.

ලංකාවේ බයිලා කලාව එම යුගයේ දී ජනප්‍රියත්වයට පත් කරන්නට කටයුතු කළ කපිරිඤ්ඤා වගේම කැලිප්සෝ තාලවලටත් සිංහල බයිලා සිංදු කියූ, බයිලා ලොවේ කිරුළු දැරූ රජු හෙවත් වොලී බැස්ටියන් පිළිබඳව යි මේ.

විද්‍යා ප්‍රබන්ධවල අපට සුලබ ව දැකගන්නට ලැබෙන ජීවී රොබෝවරු තවදුරටත් ප්‍රබන්ධයක් නොවන වග පසුගිය දිනෙක සනාථ වුණා. ඒ, පළමු "සජීවී මැෂීන්" එක නිර්මාණය කිරීම සමග යි. ඔබ 1990 දශකයේ සිට නිෂ්පාදනය වූ Jurassic Park වැනි චිත්‍රපට නරඹා තිබෙනවා නම් මේ සිදුවීමත් එවැන්නක් බව ඔබට සිතේවි. මිනිසා විසින් අලුතින් ජීවී විශේෂයක් මැවීම තමයි මෙහි දී සිදුවෙලා තිබෙන්නේ. සොබාදහමේ මෙතෙක් බිහි වූ කිසිවක් මෙයට සමාන කරන්නට හැකි වෙන්නේ නැහැ. මුළුමනින්ම පාහේ කාබනික ද්‍රව්‍යවලින් නිර්මාණය වී තිබෙන මේ රොබෝ පර්යේෂකයන් හඳුන්වන්නේ “ජීවමාන රොබෝවක්” එහෙම නැති නම්, “living robot” කෙනෙක් ලෙස යි. evolutionary algorithms එකක් (පරිණාමීය ඇල්ගොරිතමයක්) මත ක්‍රියාත්මක වෙන මොවුන්ව හඳුන්වන්නේ Xenobots ලෙස යි. Vermont විශ්වවිද්‍යාලයේ සුපිරි පරිගණකයක් භාවිතා කරමින් මෙහි සෛල වැඩසටහන් ගත කර (program the cells) තිබෙනවා. "ක්ලෝව්ඩ් ෆ්‍රොග්" හෙවත් "Xenopus laevis" කියන ගෙඹි විශේෂයේ ප්‍රාථමික සෛල (stem cells) කෘත්‍රිමව වර්ධනය කර, එමඟින් චලනය විය හැකි, ජලයේ පිහිනිය හැකි ලෙස මේ රොබෝ ජීවියා නිර්මාණය කර තිබෙනවා.

ඇමරිකාවේ "වර්මොන්ට්" සරසවිය සහ "ටෆ්ට්ස්" සරසවි ඒකාබද්ධව සිදුකරපු පර්යේෂණයන්ගේ ප්‍රතිඵලයක් විදිහට තමයි, මේ නව ජීවී කාණ්ඩය නිර්මාණය කරන්නට හැකි වෙලා තියෙන්නේ. සෛල පදනම ස්ටෙම් සෙල්ස් හරහා නිර්මාණයව තිබෙන නිසා මොවුන්ට තමන්ව ම සුව කර ගැනීමට (Self-healing) ඇති හැකියාව වැනි සුවිශේෂි හැකියාවන් පිහිටා තිබෙනවා. විද්‍යාත්මක පාරිභාෂික වදන් අතරට බයොලොජිකල් මැෂීන් වැනි නව වචන එකතු කරමින් නිර්මාණය වූ මේ රොබෝ ජීවියාට ලෝකයේ බොහෝ විද්‍යාවන් උඩුයටිකුරු කිරීමට අනාගතයේ හැකි වන බවට දැනටමත් අනාවැකි පළ වී තිබෙනවා.

කෘෂිකාර්මික යුගයේ සිටම මිනිසා විවිධ අවශ්‍යතාවන් සඳහා ජාන තාක්ෂණය හා ජාන සැකසීම වෙනස් කිරීම විවිධ මට්ටම්වලින් සිදුකර තිබෙනවා. ජාන විද්‍යාව භාවිත කරමින් අදටත් සත්ව හා ශාකවල ජාන සැකසුම් වෙනස් කරමින් විවිධ නිර්මාණයන් සිදුකරනවා. නමුත්, මෙහි දී සිදුවෙන්නේ ඊට හාත්පසින්ම වෙනස් ක්‍රියාවලියක් බව තමයි වර්මොන්ට් සරසවිය සඳහන් කරන්නේ. Xenobotsවරු පිළිබඳව සහ ඔවුන් තවදුරටත් වැඩි දියුණු කිරීම උදෙසා පර්යේෂණ සිදුකරන බවත් ඔවුන් සඳහන් කරනවා. කොහොම වුණත්, මේ වෙද්දීත් මේ ජීවී රොබෝවරු භාවිත කරමින් සිදුකළ හැකි ක්‍රියාවලින් පිළිබඳව හඳුනාගෙන තිබෙනවා. උදාහරණ ලෙස මුහුදේ එකතුව තිබෙන මයික්‍රො ප්ලාස්ටික් නිෂ්පාදන විඛාදනය කිරීම, ළදරු කලලවල විකෘතීන් නිවැරදි කිරීම, මිනිස් සිරුර අභ්‍යන්තරයේ හානි වූ ඉන්ද්‍රීයයන් අලුත්වැඩියා කිරීම, විකිරණශීලී අපද්‍රව්‍යවල විකිරණ හරණය වගේම, මිනිස් ශරීරයේ රුධිර නාල ඔස්සේ ඉන්ද්‍රියයන්ට අවශ්‍ය ඖෂධීය රසායන රැගෙන යෑම වැනි දේ සඳහන් කරන්න පුළුවන්.

කොහොම නමුත්, මේ නිර්මාණය සමග සමාජයේ යම් පිරිසක් තැති ගැනීමකට ලක් වෙනවා අපට දැකගන්න ලැබුණා. මිනිසුන් මේ කරන්නේ ස්වභාව ධර්මයට පිටින් යාමක් ලෙස යි ඔවුන් දකින්නේ. කොහොම වුණත්, මේ නිෂ්පාදනයේ වටිනාකම අදටත් වඩා අනාගතයේ අපට දැකගැනීමට හැකි වන බව නම් හොඳටම විශ්වාස යි.

සුපිරි නළු Keanu Reeves රඟපාන Fantasy සහ Sci-fi Genresවලට අයිති වන The Matrix, Matrix Reloaded, Matrix Revolutions නම් අතිශය ජනප්‍රිය චිත්‍රපට ත්‍රිත්වය පිළිබඳව වගේම එහි අන්තර්ගතයන් ගැනත් මේ දිනවල බොහෝ විට කතාබහ කෙරෙනවා. ඒ, 2021 වසරේ එළිදැක්වීමට නියමිත එහි සිව්වැනි චිත්‍රපටය නිසාවෙන් පමණක්ම නොවෙයි. ඔබට මතක නම් The Matrix පළමු චිත්‍රපටය, එහි ප්‍රධාන චරිතය වන Neoගේ මොළය යම් පරිගණක යන්ත්‍රයක් වෙත විවිධ සම්බන්ධ කර මෘදුකාංගයක් ඔස්සේ training programmes ගණනාවක් ඔහුගේ මොළය වෙත ඇතුළත් කරනවා. 1999 වසරේ තිරගත වූ මේ චිත්‍රපටයේ අඩංගු මොළය වෙත දත්ත ඇතුළත් කිරීමේ සංකල්පය, අද වෙද්දී සැබෑවක් බවට පත් වී තිබෙන බව ඔබ දන්නවා ද? මේ ලිපිය දිගහැරෙන්නේ ඒ පිළිබඳව යි. ලිපිය කියවන්න කලින් මේ කෙටි වීඩියෝ පටය බලලා ඔබේ මතකයන් අලුත් කරගන්න අපි ඔබට ආරාධනා කරනවා.

පර්යේෂකයන්ට අනුව පුද්ගල මොළය වෙත දැනුම පෝෂණය කිරීම ඉතාම පහසු කටයුත්තක් වන අතර, මේ වෙද්දීත් මොළය වෙත දැනුම ඇතුළත් කළ හැකි simulator එකක් නිර්මාණය කරමින් තිබෙන බව වාර්තා වෙනවා. මේ හරහා ඉතාම කෙටි කාලයක් තුළ පුද්ගලයින් වෙත යම් කුසලතාවයක් පුරුදු කිරීමට හැකියාව තිබෙන බව ඔවුන් telegraph.co.uk වෙත සඳහන් කර තිබුණා. මේ simulator එක Matrix චිත්‍රපටයේ මොළය වෙත දැනුම පෝෂණය කරන යන්ත්‍රය සහ මෘදුකාංගය වැනි උසස් මට්ටමේ පරිගණක මෘදුකාංගයක් සහ යන්ත්‍රයක් නිර්මාණය කිරීමේ පළමු පියවර බවට පත් වනු ඇතැ යි ඔවුන් විශ්වාස කරනවා.

චිත්‍රපටයේ Neo වෙත kung fu වැනි සටන් කලාවන් ඉගෙන ගන්නට ගත වුණේ තත්පර කිහිපයක් පමණයි. සාමාන්‍යයයෙන් එවනි සටන් කලාවක් ඉගෙන ගන්නට වසර ගණනාවක පුහුණුවක් වගේම කැපවීමක් අත්‍යවශ්‍ය යි. කැලිෆෝනියාවේ පිහිටි HRL Laboratories පර්යේෂණ කණ්ඩායම ඔවුන්ගේ simulator එක ඔස්සේ පුද්ගලයන්ගේ ඉගැනුම් හැකියාවන් පුළුල් කිරීමට හැකි බව අනාවරණය කරගෙන තිබෙනවා. ඔවුන් පවසන අන්දමට එය චිත්‍රපටයේ සංකල්පය තරම් තවමත් දියුණු මට්ටමක නැති අතර, මෙය හුදෙක් පළමු පියවරක් බව යි ඔවුන් සඳහන් කරන්නේ. ඔවුන් මේ ක්‍රමවේදය අත්හදා බැලීම සඳහා පුහුණුව ලැබූ ගුවන් නියමුවන් යොදාගෙන පර්යේෂණයක් සිදුකර තිබෙනවා. (මිනිස් මොළයේ දත්ත ගලාගෙන යාමට උපකාරී වන විද්‍යුත් සංඥාවන් පිළිබඳව අධ්‍යයනය කිරීමක් මෙහි දී සිදුව තිබෙනවා.) පුහුණුව ලැබූ ගුවන් නියමුවන් කිහිපදෙනෙකු පර්යේෂණ ආයතන තුළ ඇති realistic flight simulator එකක් වෙත යොමු කර, ඔවුන් එහි අතත්‍ය ගුවන් යානය පාලනය කිරීමේ දී ඔවුන්ගේ මොළය තුළ සංඥාවන් ගලා යන ආකාරය නිරීක්ෂණය කර, ඒ හා සමාන විද්‍යුත් සංඥාවන් වෙන වෙනම ඔවුන් තරම් පුහුණුවක් නොලැබූ ආධුනික කිහිපදෙනෙක්ගේ මොළය වෙත කෘත්‍රීම ව ලබාදෙමින් සම්පුර්ණ පර්යේෂණය සිදුකර තිබෙනවා. ආධුනික ගුවන් නියමුවන්ගේ පියාසර හැකියාවන් 33% පමණ ඉහළ දැමීමට මේ හරහා ඔවුන්ට හැකි වී තිබෙනවා. වැඩිදුරටත් අදහස් දක්වමින් HRL හි පර්යේෂකයන් සඳහන් කරන්නේ දැනට මෙවැනි simulator මඟින් පුද්ගල මනසේ ඉගැනුම් ක්‍රියාවලිය වෙත Boost එකක් පමණක් ලබාදිය හැකි බව යි.

වැඩිදුරටත් Dr. Matthew Phillips සඳහන් කරන්නේ ඔවුන්ගේ මේ simulator එක සාර්ථකව මොළය වෙත උත්තේජන සපයන පළමු යන්ත්‍රය බව යි. මේ ක්‍රමවේදය ඔස්සේ අනාගතයේ රිය පැදවීම වැනි ක්‍රියාවලි ඉතා ඉක්මනින් පුහුණු කරවීමට හැකියාව ලැබෙනු ඇතැ යි ඔහු විශ්වාස කරනවා. ඔවුන් මේ කරගෙන යන පර්යේෂණය වර්තමාන සමාජය වෙත අලුත් එකක් වුවත්, මෙහි මූලික සංකල්පයන් වසර 4000ක් තරම් අතීතයට දිවයන බව යි ඔහු සඳහන් කරන්නේ. පුරාණ ඊජිප්තුවේ විද්‍යුතය නිපදවන මාළුන් යොදාගෙන විවිධාකාර වේදනාවන් සමනය කිරීමේ ක්‍රමවේදයන් පැවතුණු බව ඔහු සඳහන් කරනවා.

ඔබට මතක නම් Tesla සමාගමේ නිර්මාතෘ වන Elon Muskගේ නවතම තාක්ෂණික ව්‍යාපෘතිය ලෙස ඔහු ආරම්භ කළ Neuralink ආයතනය සිදුකරන පර්යේෂණ පිළිබඳව අප පෙර ලිපියක ඔබ වෙත ගෙන ආවා. කෙසේ වෙතත්, උපාංග ඔස්සේ පුද්ගල මොළය පරිගණකය වෙත සම්බන්ධ කිරීම මඟින් මොළය Hackerවරුන් වෙත විවෘත කිරීමක් ලෙසත් ඇතැමුන්ගේ මතයක් පවතිනවා. එමෙන්ම මේවා ආශ්‍රයෙන් මිනිසුන් විවිධ දේ සඳහා යොමු කිරීමත් සිදුවිය හැකි බව යි ඔවුන්ගේ මත ය. මෙවැනි සමාජීය මත සමග මේ තාක්ෂණයන් කොයි ආකාරයෙන් පෑහේවි ද යන්න නුදුරු අනාගතයේ දී මේ පර්යේෂකයන් වෙත මතු වන ප්‍රධාන ගැටළුවක් බවට පත් වේවි.

Foldable Phone රැල්ල ආරම්භ වූ වසර විදිහට පසුගිය 2019 වසර හඳුන්වන්න අපට හැකියාව තිබෙනවා. නමුත්, මේ 2020 වසර ආරම්භ වෙන්නෙම Foldable Phone පෙරළියකින්. මේ ලිපිය හරහා දිගහැරෙන්නේ ඒ පිළිබඳව යි.

පසුගිය වසරේ Flexpai උපාංගයෙන් ඇරඹුණු Foldable රැල්ල Samsung සමාගමේ Galaxy Foldable වගේම, Huawei සමාගමේ Mate X ඇතුළු සමාගම් ගණනාවක් නැවිය හැකි දුරකතන නිර්මාණය කරන්නට පෙළඹවීමක් බවට පත් වුණා. කොහොම වුණත්, අවාසනාවකට වගේ මේ නැවිය හැකි දුරකතන නිෂ්පාදනය කළ සමාගම් ගණනාවක Foldable Phone අසාර්ථක උපාංග ලෙස තාක්ෂණික ලෝකයේ හැඳින්වෙන්නට ගත්තා. ඔබට මතක ඇති මිලෙන් තරමක් අධික Galaxy Foldable දුරකතනයේ durability එක පිළිබඳව ඇති වුණු මතභේදාත්මක වාතාවරණය. Samsung Galaxy Foldable දුරකතනය පරික්ෂා කිරීමේ සහ ජනප්‍රිය කරවීමේ අරමුණ ඇතිව social media influencersලා වෙත ලබා දුන්නා. නමුත්, ඔවුන්ගෙන් ලැබුණු ප්‍රතිචාර අයපත් වූ නිසාවෙන් දුරකතනය නිකුත් කිරීමට තිබූ දිනය කල් දමන්නට පවා සමාගමට සිදුවුණා. දෙවැනි වර දුරකතනය වෙළඳපොළ වෙත නිකුත් කළ විගසම මෙය තවමත් වෙළඳපොළ වෙත නිකුත් කිරීමට එතරම් සුදුසු නැති බව ජනප්‍රිය YouTube චැනලයක් වන JerryRigEverything වෙතින් සඳහන් කළා.

කෙසේවෙතත්, Foldable දුරකතන නිෂ්පාදනය කර සාර්ථක අලෙවියක් සිදුකළ සමාගමක් බවට පත් වෙන්නට පසුගිය දිනෙක Huawei සමාගමට හැකි වුණා. ඒ මාසයකට අලෙවි වන Huawei Mate X දුරකතන සංඛ්‍යාව 100,000ක් බවට ඔවුන් සිදුකළ ප්‍රකාශය සමග යි. Huawei සමාගම සමග Foldable දුරකතන නිෂ්පාදනයේ ප්‍රධාන ප්‍රතිවාදියා වන samsung සමාගම Galaxy Foldable දුරකතන මිලියනයක් විකුණා ඇති බව එහි විධායක නිලධාරියෙකු වන Young Sohn සඳහන් කර තිබුණත්, CES 2020 තාක්ෂණ ප්‍රදර්ශනයේ දී ඒ ප්‍රකාශය නිවැරදි කෙරුණා. ඒඅනුව විකුණා ඇති මුළු දුරකතන ප්‍රමාණය 400,000ත් 500,000ත් අතර බව තමයි වාර්තා වෙන්නේ. බැලූ බැල්මට වැඩිම විකිණුම් ප්‍රමාණය samsung සමාගම සතු වුණත්, Huawei Mate X තවමත් යුරෝපය වෙත හෝ චීනයෙන් පිට අලෙවිය අරඹා නැහැ. චීනය තුළ පමණක් මෙවැනි විකිණුමක් ලබන්නට Mate X වෙත හැකියාව තිබෙනවා නම්, Global Release එකෙන් අනතුරුව නව වාර්තාවක් තබන්නට මේ උපාංගයට හැකි වෙනු ඇතැ යි බොහෝ දෙනෙක් විශ්වාස කරනවා.

මේ දුරකතනය මෙතරම් ජනප්‍රිය වන්නට එහි දෘඩාංග මූලික හේතුවක් බවට පත් වෙලා තියෙනවා. HiSilicon Kirin 980 ප්‍රොසෙසරයක්, 8GB RAM එකක් වගේම 512GB Internal storage එකක් සහිත Huawei Mate X දුරකතනය පැමිණෙන්නේ ඇන්ඩ්‍රොයිඩ් 9 Pie මෙහෙයුම් පද්ධතිය සමග යි. මෙහි සිම් කාඩ් පත් දෙකක් දැමිය හැකි අතරම, එක සිම්පතක් වෙනුවට ඔබට අවශ්‍ය නම් නැනෝ මෙමරි card (NM) පතකින් Storage එක තවත් වැඩි කරගන්නට අවස්ථාව තිබෙනවා. ඊට අමතරව මෙහි Volume button එකට පහළින් fingerprint sensor එකක් (ඇඟිලි සලකුණු සංවේදකයක්), NFC, රිමෝට් එකක් ලෙස භාවිතයට IR port එකක් වගේම Huawei සමාගමේ නවතම ආරෝපණ තාක්ෂණයක් වන Huawei SuperCharge තාක්ෂණයෙනුත් මෙය සමන්විත යි. එනම්, විනාඩි 30ක Charging (ආරෝපණ) කාලයක දී 85%ක් දක්වා බැටරිය ආරෝපණය කරන්න හැකියාව තියෙනවා.

Falcon design එක සහිත අඟල් 8ක තිරය වගේම, Leica සමාගම විසින් නිපදවන ලද විශේෂ කැමරා 4කුත් මේ උපාංගය සතු වෙනවා. ප්‍රධාන කැමරාව මෙගාපික්සල් 40ක f/1.8 වූ wide කැමරාවක්. දෙවැනි කැමරාව මෙගා පික්සල් 16ක f/2.2 වූ ultrawide කැමරාවක්. තුන්වැන්න මෙගා පික්සල් 8ක telephoto lens සහිත කැමරාවක් වන අතරම හතරවැනි කැමරාව TOF (time-of-flight) නම් Depth එක හඳුනාගැනීමට ආලෝක පරාවර්තන වේගය භාවිතා කරන සංවේදකයක් ලෙස යි සඳහන් වෙන්නේ. මීට අමතරව නවතම 5G තාක්ෂණයටත් මේ උපාංගය සහාය දක්වනවා. චීනයේ මේ දුරකතනය අලෙවි වන මිල ලෙස දැක්වෙන්නේ yuan (යුආන්) 16,999ක් එහෙම නැති නම්, ඇමරිකානු ඩොලර් 2,400ක් ලෙස යි. බාර්සිලොනාවේ පැවැත්වීමට නියමිත MWC 2020 තාක්ෂණික ප්‍රදර්ශනයේ දී Huawei Mate X දුරකතනය ලෝකයේ අනෙක් රටවල් වෙතත් නිකුත් කෙරෙනු ඇතැ යි දැනට විශ්වාස කෙරෙනවා.

Halo පරිගණක ක්‍රීඩා මාලාවම පසුගිය දිනෙක පරිගණක වෙත නිකුත් වුණා. මේ ඔවුන් නිර්මාණය කරන්නේ ලබන වසරේ නිකුත් වීමට නියමිත Halo Infinite ක්‍රීඩාව වෙත Hype එකක් ද?

ලෝකයේ ජනප්‍රිය පුද්ගලයින් නිතර නිතර දෙස් විදෙස් පුවත් මැවීම සාමාන්‍යකරණය වී හමාරයි. මේ ලිපිය හරහා දිගහැරෙන්නේ ලෝකයේ අතිශය ජනප්‍රිය සංගීතඥයෙකු වන Akon නිර්මාණය කරන්නට සුදානම් වෙන අපූර්ව නගරය පිළිබඳව යි. පසුගිය වසර කිහිපය තුළ Akon පිළිබඳව විදෙස් මාධ්‍ය සහ සමාජ මාධ්‍ය තුළත් නිතර නිතර කතා බහට ලක් වුණා. විශේෂයෙන්ම ඔහු නිර්මාණය කරන්නට සුදානම් වන AKoin නම් cryptocurrency එක ඉන් ප්‍රධාන හේතුවක්. Cryptocurrency කියන්නේ භෞතිකව අපි පාවිච්චි කරන මුදල් වෙනුවට ඉලෙක්ට්‍රොනිකව සංසරණය වන ආකේතිත මුදල් වර්ගයක්. Akonගේ අරමුණ මේ Cryptocurrency එක ඔස්සේ අප්‍රිකාවේ ජිවන තත්ත්වය නගා සිටවීම යි. Cryptocurrency සහ blockchain ඉතාම නුදුරු අනාගතයේ දී අප්‍රිකාවේ ගැලවුම්කරුවා බවට පත් වන බව ඔහු විශ්වාස කරනවා. අප්‍රිකාවට බෙහෙවින් ආදරය කරන පුද්ගලයෙක් ලෙස සැලකෙන Akon, අප්‍රිකා මහාද්වීපයේ මිලියන 600ක් ජනතාවට විදුලිය ලබාදීමට දරන ප්‍රයත්නයන් ජාත්‍යන්තරයේ ඉහළින් පැසසුම් ලැබුවා.

ඔබ විද්‍යා ප්‍රබන්ධ චිත්‍රපට හෝ කතා මාලාවන් හි දැක ඇති අන්දමේ නගරයක් නුදුරු අනාගතයේ දී නිර්මාණය කිරීමට මේ සංගීතඥයා සුදානම් වෙනවා. මේ පිළිබඳව ඔහු පළමු අනාවරණය සිදුකළේ Nick Cannonගේ Power 106 Nick Cannon Mornings නම් රේඩියෝ වැඩසටහනට එක් වෙමිනුයි. සියයට සියයක් Cryptocurrency භාවිතයෙන් ගනුදෙනු කළ හැකි ලෙස මෙම නගරය සැලසුම් කරන බව තමයි ඔහු වැඩිදුරටත් සඳහන් කළේ. මේ නගරය නම් වෙන්නේ Akon City යන නමිනුයි. ඒ වගේම මේ නගරය සම්පුර්ණයෙන්ම පාහේ පුනර්ජනනීය බලශක්ති ක්‍රමවේදයන් භාවිත කර බල ගැන්වෙන ලෙස නිර්මාණය කරන්නට තමයි ඔහුගේ අදහස. (2014 වසරේ සිට ක්‍රියාත්මක වන Akon Lighting Africa ව්‍යාපෘතිය යටතේ මේ වෙද්දීත් ඔහු අප්‍රිකානු මහද්වීපයේ රටවල් 18කට සූර්ය බලයෙන් විදුලිය නිපදවා ගැනීමේ ක්‍රමවේදයන් හඳුන්වා දී තිබෙනවා.) ඔබ Marvel රසිකයෙකු හෝ Black Panther චිත්‍රපටය නරඹා තිබෙනවා නම් Wakanda රාජ්‍ය පිළිබඳව අසා ඇති. Akon මේ වෙර දරන්නේ සැබෑ ලෝකයේ Wakanda රාජ්‍යයක් නිර්මාණය කිරීමට බව තමයි බොහෝ මත පළ කරන්නේ.

අප්‍රිකානු ජනජීවිත නගා සිටවීමට බිහි වන අනාගතයේ නගරය- standard.co.uk

බටහිර අප්‍රිකාවේ පිහිටි Senegal ජනරජය පදනම් කරගෙන මේ Akon City එක නිර්මාණය වෙනවා. අදියර දෙකකින් ක්‍රියාත්මක වීමට නියමිත ක්‍රියාවලියේ පළමු අදියර එළඹෙන මාර්තු මාසයේ දී ආරම්භ වීමට නියමිත යි. වසර 10ක් ඇතුළත නගර ගොඩනැගීම අවසාන කිරීම අරමුණු කරගත් මේ ව්‍යාපෘතියේ දෙවන අදියර 2025 දී ආරම්භ කිරීමට ඔවුන් බලාපොරොත්තු වෙනවා. මේ නගරය ඉදිවෙන්නේ සෙනෙගල් හි ජනාධිපතිවරයා වන Macky Sall විසින් Akon වෙත තෑගී දුන් අක්කර 2,000ක භූමියක බව තමයි විදෙස් මාධ්‍ය වාර්තා කරන්නේ. මේ නගරයට ඉහළ මට්ටමේ ගුවන්තොටුපොළක් පවා අන්තර්ගත වන බව තමයි දැනගන්නට ලැබෙන්නේ.

AKoin අන්තර්ජාතික තලයකට පැමිණෙනු ඇතැ යි තමන් අපේක්ෂා කරන බවත්, ඔහුගේ නම සඳහන් නගරයක් ඉදිකරනවාට වඩා මේ හරහා අප්‍රිකානු ජන ජීවිත නගාසිටුවීම ඔහුගේ අරමුණ බව තමයි Akon සඳහන් කරන්නේ. මේ නගරය තුළ ඉතාම දියුණු තාක්ෂණික වෙනස්කම් දැකගන්නට හැකි වෙන බවට මේ වෙද්දීත් මත පළ වෙනවා.

අන්තර්ජාලය කියන්නේ අද වෙද්දී ඔබත්, මමත් ඇතුළු ලෝකයේ විශාල පිරිසක් වෙත පහසුකම් සපයන දෙයක්. කොටින්ම කිව්වොත් අන්තර්ජාලය තුළ සැරිසැරීම අද වෙද්දී බොහෝ දෙනෙකුගේ දෛනික දින චර්යාවේ කොටසක්. මේ 2019 වසරට අන්තර්ජාලය වෙත මූලාරම්භය වැටී වසර 50ක් සපිරෙනවා. මේ කියන්න යන්නේ ගත වුණු 50 වසර තුළ දී අන්තර්ජාලය පැමිණි ගමන් මඟෙහි සන්ධිස්ථාන කිහිපයක් පිළිබඳව යි.

පනස් වසරකට පෙර UCLA (University of California, Los Angeles) හි මහාචාර්යවරයෙක් සහ ඔහුගේ සිසුවෙකු අන්තර්ජාලය වෙත පුරෝගාමී වූ ARPANET තුළින් පණිවිඩයක් මුදාහැරියා. මේ ARPANET පසු කාලයක තොරතුරු තාක්ෂණ විප්ලවයේ මූලාරම්භය ලෙස හඳුන්වනු ලැබුවා. රොබර්ට් විලියම් ටේලර් නම් මේ මහාචාර්යවරයා අන්තර්ජාලය වගේම තවත් බොහොමයක් තාක්ෂණික නිර්මාණයන්ට දායක වුණා.

කොටින්ම ඉන්ටර්නෙට්හි ආරම්භය සඳහා අත්තිවාරම දැමුවේ රොබර්ට් ටේලර්ගේ පුරෝගාමීත්වයෙන් බව අපට එක හෙලා පිළිගන්නට හැකි කාරණාවක්. ඊට අමතරව පරිගණක ජාලකරණය (Computer Networking), මාර්ගගත තොරතුරු හා සන්නිවේදන පද්ධති (Online Information and Communication Systems) සහ නවීන පෞද්ගලික පරිගණක (Modern Personal Computing) සංවර්ධනය සඳහා ද ඔහු පුරෝගාමීව කටයුතු කර තිබෙනවා. මේ මොහොත තුළත් අන්තර්ජාලය තුළ මිලියන ගණනක් පිරිස සැරිසරන්නේ ඔහු ඇතුළු පිරිසකගේ දායකත්වය නිසාවෙනුයි.

ඔබ දන්නවා ද?  
ඔබ අන්තර්ජාලය භාවිත කරන මේ මොහොත වන විට ලෝකය පුරා අන්තර්ජාලය සහ ඒ ආශ්‍රිත සේවාවන් භාවිත කරන පිරිස පිළිබඳව internetlivestats.com වෙබ් අඩවියෙන් සජීවී ගණනය කිරීමක් දැකගන්න හැකි බව?

මුල් කාලයේ පරිගණක, පරිගණක ජාලයන් සහ අන්තර්ජාලය යනාදිය සියල්ලන්ටම විවෘත වූයේ නම් නැහැ. ඒ වගේම ඉතාම සරල ආරක්ෂණ ක්‍රමවේදයන් මුල්කාලීනව භාවිත වුණා. 1973 දී, උසස් පාසල් සිසුන් කණ්ඩායමක් පෙන්ටගනය විසින් කළමනාකරණය කරන ලද සංවෘත ජාලයක් ලෙස සැලකෙන ARPANET වෙත ප්‍රවේශය ලබාගත් බව වාර්තා අතර සඳහන් වෙනවා. මෙවැනි සිදුවීම් නිසාවෙන් අන්තර්ජාලය සම්බන්ධ පර්යේෂකයන් වන වින්ටන් සර්ෆ් සහ රොබර්ට් ඛාන්ගේ යෝජනාවන්ට අනුව අන්තර්ජාලයේ මූල ප්‍රොටෝකෝල (core protocols) වෙත ගුප්ත කේතන (Encryption) ක්‍රමවේදයන් හඳුන්වාදීම සිදුවුණා. මේ ඔස්සේ හැකර්වරු වැනි අනවසර පුද්ගලයන් වෙත පරිගණක පද්ධති වෙත ඇතුල්වීම ඉතා අපහසු වෙනවා.

මුල දී මේ වෙත ඇමරිකානු බුද්ධි නිලධාරීන් එතරම්ම කැමැත්තක් පළකර නොමැති බව තමයි දැනගන්නට ලැබෙන්නේ. කෙසේ නමුත්, එහි ප්‍රතිඵලයක් ලෙස අද වන විට අන්තර්ජාල පරිශීලකයන් වෙත ඉතා සංකීර්ණ මුරපද (passwords) සහ බහු-සාධක සත්‍යාපන පද්ධති (multi-factor authentication) හැසිරවීමට සිදුවෙනවා. වඩා වැඩි ආරක්ෂක අවශ්‍යතා සහිත පරිශීලකයන් වෙත ඔවුන්ගේ අන්තර්ජාල සම්බන්ධතා සහ ක්‍රියාකාරකම් ආරක්ෂා කරගැනීමට අතථ්‍ය පෞද්ගලික ජාල (virtual private networks) හෝ ටෝර් (Tor) වැනි විශේෂිත රහස්‍යතා මෘදුකාංග (specialized privacy software) භාවිතා කරන්නට සිදුවෙනවා.

‘The Internet’ යන්න නිල වශයෙන් බිහි වන්නේ 1983 ජනවාරි 1 වැනි දා යි. මෙලෙස උපත ලබන අන්තර්ජාලය තාක්ෂණය ඕනෑම කෙනෙකුට විවෘතව පිවිසීමට සහ භාවිතයට ගත හැකි ලෙස නිර්මාණය කිරීම ලෝකයේ බොහෝ දේ නව්‍යකරණය වීමට බලපෑ බව නම් නොරහසක්. අන්තර්ජාලය ඔස්සේ ලෝකය අද වන විට විශ්ව ගම්මානයක් බවට පත්ව තිබෙනවා. කොහොම වුණත්, මෙලෙස අන්තර්ජාලය ලෝකයේ සියල්ලන්ටම භාවිත කළ හැකි ලෙස එක මට්ටමකට ගෙන ඒමට ලෝකය පුරාම පර්යේෂකයන් විශාල වශයෙන් කැපවීම් සිදුකළ බව නම් සඳහන් කරන්නම ඕනේ. විවෘත පද්ධති අන්තර්-සම්බන්ධිත සම්මතයක් (Open Systems Interconnection standard) බිහි වෙන්නේ ඒ මහන්සියේ ප්‍රතිඵලයක් ලෙස යි.

TCP/ IP එසේ නැති නම්, Transmission Control Protocol/Internet Protocol ක්‍රමයන් පිළිබඳව යෝජනා වීමත් මේ සමගම සිදුවෙනවා. ඒ, සර්ෆ් සහ ඛාන් යන දෙනාගේ යෝජනාවක් මත යි. මේ ක්‍රමවේදය සාමාන්‍ය තැපැල් ක්‍රමවේදයන්ගේ ක්‍රියාවලියට සමාන යි. පැකේජය (දත්ත පැකට්ටුව) අදාළ ලිපිනය වෙත යැවීම සරලවම මෙහි සිදුවන ක්‍රියාවලිය ලෙස විස්තර කරන්න පුළුවන්. මේ ක්‍රමවේදය හරහා ජාලයේ අනෙක් පරිගණක සමග දත්ත හුවමාරු කරගැනීම ඉතාම පහසු වෙනවා.

1996 වර්ෂය වන විට අන්තර්ජාලය සර්වර් (සේවාදායක පරිගණක) 73,000ක පමණ පැතිරී ගියා. ඒ වගේම, සමීක්ෂණවලට භාජනය කළ ඇමරිකානු පුරවැසියන්ගෙන් 22%ක් පමණ නිතර අන්තර්ජාලය භාවිත කරන්නන් බව අනාවරණය වී තිබෙනවා. දිනෙන් දින වැඩි වෙන මේ අධික අන්තර්ජාල පරිශීලකයන් ප්‍රමාණයට සාපේක්ෂව ශීඝ්‍ර වශයෙන් ඉහළ යන කාමුක දර්ශන අඩංගු වෙබ් අඩවි ප්‍රමාණය සහ වීඩියෝ නරඹන පිරිසේ ඉහළ යාම පිළිබඳව ඇමරිකානු කොන්ග්‍රස් සභිකයන් නම් සුළු කොට තැකුවේ නැහැ. සයිබර් අවකාශයේ අශෝභන හා අසභ්‍ය දේ නියාමනය කිරීම සඳහා කොන්ග්‍රස් සභිකයන් විනීත සන්නිවේදන පනත (Communications Decency Act) පිහිටුවා ගත්තේ ඉන් අනතුරුව යි. එහෙත්, පසුව අධිකරණය මඟින් එහි විවිධ කොටස් අවලංගු කිරීමට කටයුතු කරනු ලැබුවා. නමුත් එහි 230 වන කොටස\* (Section 230) ක්‍රියාත්මක කිරීමට අධිකරණය අවසර ලබාදුන්නා. මෙමඟින් ෆේස්බුක් සහ ට්විටර් වැනි සමාජ මාධ්‍ය වෙබ් අඩවි නියාමනයකින් තොරව ක්‍රියාත්මක වීමට ඉඩ ලබාදෙන බව විචාරකයින්ගේ අදහස යි.

ඔබ දන්නවා ද?  
අන්තර්ජාලයේ පියා ලෙස සැලකෙන්නේ වින්ට් සර්ෆ් (Vint Cerf) බව.

TCP/ IP ක්‍රමවේදයන් භාවිත කර අන්තර්ජාලය වෙත සම්බන්ධ වීමට වෙන වෙනම එක් එක් උපාංගය වෙත ලිපිනයක් ලැබෙනවා. අන්තර්ජාලයේ අදාළ කොටස වෙත සම්බන්ධ වීමට එම ලිපිනය මතක තබාගත යුතුම යි. (උදාහණයක් ලෙස “104.25.161.117” වැනි සංඛ්‍යා මාලාවක් දක්වන්න පුළුවන්.) නමුත් මෙලෙස සංඛ්‍යා විශාල ප්‍රමාණයක් මතක තබාගැනීම ඉතාම අපහසු කාර්යයක්. පසුකලෙක ඒ වෙනුවට අද අපි වෙබ් අඩවි වෙත පිවිසෙන්න භාවිත කරන ඩොමේන් නාමයන් (උදාහරණයක් ලෙස, ඉහත IP එක වෙනුවට https://roar.media) භාවිතයට පැමිණෙනවා. IP ලිපින වෙනුවට මෙලෙස ඩොමේන් නාමයන් භාවිතා කිරීමෙන් අංක වැරදී වෙනත් වෙබ් අඩවි වෙත පිවිසීම අවම කිරීමට හැකියාව ලැබෙනවා.

මුළු අන්තර්ජාලයේම address book එකක් Floppy disk එකක ඇතුළත් කරන්නට Jon Postel වෙත පවරා තිබුණා. කෙසේ වෙතත්, ඔහු ද ඇතුළුව තවත් කිහිප දෙනෙකුගේ මතය වුණේ; එවැනි බලයක් එක් පුද්ගලයෙකු සතුව නොපැවතිය යුතු බව යි. 1960 වසර වන විට මුළු අන්තර්ජාලයේම සිටි බලවත්ම පුද්ගලයා ලෙස ඔහුව හඳුන්වනු ලැබුණා. 1998 වසරේ දී එක්සත් ජනපද වාණිජ්‍ය දෙපාර්තමේන්තුව විසින් ලොව පුරා අන්තර්ජාල ලිපිනයන් කළමනාකරණය කිරීම සඳහා නව පුද්ගලික ලාභ නොලබන සංවිධානයක් බලාත්මක කරන්නට පියවර ගත්තා.

ICANN (Internet Corporation for Assigned Names and Numbers) බිහි වූයේ එලෙස යි. වසර 22කට ආසන්න කාලයක් ICANN විසින් වාණිජ්‍ය දෙපාර්තමේන්තුවේ කොන්ත්‍රාත්තුවක් යටතේ එම කාර්යය සිදුකළා. 2016 දී වාණිජ්‍ය දෙපාර්තමේන්තුවේ කොන්ත්‍රාත්තුව කල් ඉකුත් වූ අතර, ICANN හි පාලනය පුළුල් හා ගෝලීයකරණය වූ ව්‍යුහයක් කරා මාරුවීම සිදුවුණා.

2010 ජුනි මාසයේ දී සයිබර් ආරක්ෂණ පර්යේෂකයන් විසින් න්‍යෂ්ටික අවි නිපදවීම සඳහා ඉරානය භාවිතා කරන උපකරණ විනාශ කිරීම සඳහා විශේෂයෙන් නිර්මාණය කරන ලද Stuxnet නම් නවීන සයිබර් ආයුධයක් පිළිබඳව අනාවරණය කළා. නමුත්, අන්තර්ජාලය හරහා සැලකිය යුතු විනාශයක් ඇති කිරීමේ හැකියාව පිළිබඳව පාලකයන්ගේ අවධානය යොමු වන්නට තවත් දශකයක් පමණ ගත වුණා.

මිලියන ගණනක් දිනපතා සැරිසරන අන්තර්ජාලය කොතරම් ආරක්ෂිත ද යන්න පිළිබඳව දැන් දැන් ගැටළු මතුවෙමින් පවතිනවා. අපි අන්තර්ජාලයේ සැරිසැරීමේ දී ආරක්ෂාව පිළිබඳව වඩ වඩාත් සැලකිලිමත් විය යුතු දශකයක ආරම්භයක් ලෙස 2020 හඳුන්වන්න පුළුවන්.

මේ හරහා අන්තර්ජාල සේවා සපයන සමාගම්වලට ඒ හරහා ව්‍යාප්ත වෙන අන්තර්ගතයන් සම්බන්ධ කිසිදු නීතිමය වශයෙන් වගවීමට ලක් නොවී ඒ කන්ටෙන්ට් අන්තර්ජාලයෙන්, ඔවුන්ගේ ප්ලැට්ෆෝම්වලින් ඉවත් කිරීමට අවශ්‍ය ඉඩකඩ ඔවුන්ට ලබා දෙනවා. මෙවැනි වෙබ් අඩවිවල පළ වෙන ඒවායේ අන්තර්ගතය සම්බන්ධව එකී සේවා සපයන සමාගම් සහ අන්තර්ජාලයේ අන්තර්ක්‍රියා සහිත වෙබ් අඩවි තෙවැනි පාර්ශවයක් ලෙස හඳුනාගන්නවා මිස, නීතිමය වශයෙන් ඒවා "පළ කරන්නා" ලෙස සැලකෙන්නේ නැහැ.

ඒ නිසා කිසිවකු හෝ (වෙබ් අඩවි) හරහා පළ කරන දේවල්වල අඩංගු අන්තර්ගතයන්ට එරෙහිව නීතිමය පියවරක් නොහැකි වෙනවා සේ ම, ඔවුන් විසින් කවුරුන් හෝ තමන්ගේ වෙබ් අඩවිය හෝ සේවාව යොදාගෙන පළ කරන දේවල් ඉවත් කළහොත් හෝ සංස්කරණය කළහොත් එය පළ කරපු පාර්ශවයටත්, ඒ සමාගම්වලට එරෙහිව තමන් පළ කළ දේ ඉවත් කළා කියා නීතිමය පියවරක් ගන්නට තියෙන ඉඩ ඇහිරෙනවා.

2020 අලුත් දශකයක ආරම්භයක්, අලුත් කතාන්දරවල ආරම්භයක්, ඉතිහාසය නැවත ලියැවෙන-අලුත් වෙන අවුරුදුද්දක්. එහෙම වෙන්න හේතු ගණනාවක් තිබෙනවා. ඒ අතරට මේ වසර පුරාවට ක්‍රියාත්මක වීමට නියමිත අභ්‍යවකාශ ගමන් ගැනත් සඳහන් නොකරම බැහැ. මේ ලිපිය හරහා බලාපොරොත්තු වෙන්නේ ඉතිහාස පොතට අලුතින් එක් වීමට නියමිත සුවිශේෂී අභ්‍යවකාශ ගමන් පිළිබඳව ගෙන ඒමට යි. අපටත් වැඩි කලක් නොගොසින්ම අභ්‍යවකාශ ගත වෙන්න හැකි වෙන බව ලිපිය කියවන ඔබට වැටහේවි.

Elon Musk ගැන කියූ සැනින් ඔබට මතක් වෙන දේවල් අතර SpaceX (ස්පේස් එක්ස්) සමාගම සුවිශේෂී තැනක් ගන්නවා. SpaceX සමාගම 2020 වසර ආරම්භ කරන්නේ අතිශය කාර්යබහුල ලෙසිනුයි. ඔවුන් මේ වසරේ දී ලෝකයේ පළමු වරට සාමාන්‍ය මගීන් අභ්‍යවකාශය වෙත ගෙන යාමේ මෙහෙයුමක් වෙත සුදානම් වෙනවා. මෙම මෙහෙයුමට යොදාගන්නා යානය (කැප්සියුලය) SpaceX Dragon ලෙසින් හැඳින්වෙනවා. මෙහි පළමු ගමන වෙන්නේ NASA අභ්‍යවකාශගාමීන් ISS වෙත රැගෙන ගොස් නැවත පෘතුවිය බලා රැගෙන ඒම යි. පසුගිය දිනෙක Elon Musk මෙහි දී සිදුවන ක්‍රියාවලිය ගැන වගේම, ඉදිරියේ දී අභ්‍යවකාශය සාමාන්‍ය ජනයාට විවර වන ආකාරය පිළිබඳව Simulation Video එකක් අන්තර්ජාලය වෙත මුදාහැර තිබුණා. SpaceX Dragon යානය අභ්‍යවකාශය වෙත රැගෙන යන කාර්යය පැවරෙන්නේ Falcon 9 (Launch vehicle) යානය වෙත යි. ඊට අමතරව ස්පේස් එක්ස් ආයතනය මුළු ලොවටම පුළුල් අන්තර්ජාල සේවා ආවරණයක් ලබාදීම සඳහා සකස් කරන "ස්ටාලින්ක් චන්ද්‍රිකා" පන්තියට මේ වසරේ දී තවත් චන්ද්‍රිකා එක් කිරීමට නියමිත යි.

SpaceX සමාගම සමග 2020 වසරේ සාමාන්‍ය ජනයාට අභ්‍යවකාශය විවර කිරීමේ තරගයට එක්වෙන ප්‍රධානම තරගකරුවා වන්නේ, සුප්‍රකට ගුවන් යානා නිෂ්පාදන සමාගමක් වන Boeing සමාගම යි. මෙහි යානය වෙත (කැප්සියුලය) යොදා තිබෙන නම වෙන්නේ Boeing CST-100 Starliner යි. ස්ටාර්ලයිනර්, නාසා ආයතනයේ වාණිජ කාර්ය මණ්ඩල වෙත බෝයිං විසින් නිෂ්පාදනය කරන ලද කාර්ය මණ්ඩල කැප්සියුලයක්. මෙහි මූලික අරමුණ වන්නේ නාසා ආයතනයේ වාණිජ කාර්ය මණ්ඩලය ජාත්‍යන්තර අභ්‍යවකාශ මධ්‍යස්ථානයට සහ යෝජිත බිගෙලෝ වාණිජ අභ්‍යවකාශ මධ්‍යස්ථානය වැනි පුද්ගලික අභ්‍යවකාශ මධ්‍යස්ථාන වෙත ප්‍රවාහනය කිරීම යි. ඉතිහාසයේ පළමු වරට පුද්ගලික සමාගම්වල මැදිහත් වීමෙන් මිනිසුන් අභ්‍යවකාශයට ගෙන යෑම මේ වසර පමණක් නොව පුරා දශකයම සුවිශේෂ එකක් කිරීමට ප්‍රමාණවත්.

2020 වසරේ පෙබරවාරි මාසයේ දී සූර්යයා නිරීක්ෂණය සඳහා නිරීක්ෂණ යානයක් අභ්‍යවකාශගත කිරීමට යුරෝපා අභ්‍යවකාශ ආයතනය සහ නාසා ආයතනය එක්ව සුදානම් වෙනවා. ඇමරිකාවේ ෆ්ලොරිඩා ප්‍රාන්තයේ කේප් කැනෑවරල් (Cape Canaveral, Florida) සිට Atlas V 411 රොකට්ටුවෙන් මෙය අභ්‍යවකාශගත කිරීමටයි නියමිත. නිරීක්ෂණ යානය බුද ග්‍රහයාගේ කක්ෂය තුළ සිට (හිරුට ඇස්ට්‍රොනොමිකල් ඒකක 0.28ක් තරම් ආසන්නයට) සුර්යා නිරීක්ෂණය සිදුවෙනවා. මේ නිරීක්ෂණ මෙහෙයුම වෙත ගතවන කාලය වසර 7ක් බව තමයි වාර්තා වෙන්නේ. මේ කාලය පුරාවට හිරුගේ අධි දීප්ත ඡායාරූප ගැනීම සහ හිරු ආසන්නයේ සිට නිරීක්ෂණය කිරීම සිදුවේවි.

අඟහරු ග්‍රහයා සිය කක්ෂයේ පෘතුවියට ආසන්නතම ලක්ෂ්‍යයක ස්ථානගත වෙන වසරක් විදිහට ලැබූ 2020 වසර හඳුන්වන්නට පුළුවන්. උදාවන අවස්ථාවෙන් අඟහරු ග්‍රහයා නිරීක්ෂණය කිරීමට ලෝකයේ අභ්‍යවකාශ පර්යේෂණ ආයතන ගණනාවක් තමන්ගේ පර්යේෂණ රෝවර්, අඟහරු ග්‍රහයා වෙත පිටත් කිරීම 2020 වසර පුරාම සිදුවේවි. ප්‍රධාන වශයෙන් නාසා ආයතනය ඔවුන්ගේ අඟහරු රෝවරය ජූලී 17 වැනි දින ඇමරිකාවේ Cape Canaveral හි දී ගුවන්ගත කිරීමට සුදානම්. එය එළඹෙන 2021 වසරේ පෙබරවාරි 18 වැනි දා අඟහරු වෙත ගොඩබැස්වීම ඔවුන්ගේ අරමුණ යි. මෙය Atlas V රොකට්ටුවෙන් අභ්‍යවකාශ ගත වේවි.

https://mars.nasa.gov වෙබ් අඩවිය වෙත පිවිස මෙහි Countdown එක දැකබලාගන්න ඔබට පුළුවන්.

ඊට අමතරව යුරෝපා අභ්‍යවකාශ ආයතනය සහ රුසියාවේ රොස්කොස්මොස් ආයතනය එක්ව Rosalind Franklin (රොසලින්ඩ් ෆ්‍රෑන්ක්ලින්) නම් රෝවරයක් අඟහරු වෙත පිටත් කිරීමට සුදානම් වෙනවා. මේ රෝවරය මුලින් ExoMars rover ලෙස නම් කර තිබුණා. මෙය මේ වසරේ ජූලි මාසයේ 25 අභ්‍යවකාශගත කිරීමට සුදානම් වන අතර, එළඹෙන 2021 වසරේ මාර්තු මාසය වන විට අඟහරු වෙත ගොඩබැස්වීමට නියමිත යි.

මේ දෙකට අමතරව එක්සත් අරාබි එමීර් රාජ්‍යය "හෝප් මාර්ස් මිෂන්" යන තේමාව යටතේ අඟහරු නිරීක්ෂණ චන්ද්‍රිකාවක්, මෙම වසරේ කක්ෂගත කිරීමට තිබෙන සුදානමක් ගැනත් අපට දැනගන්න ලැබෙනවා. එය මේ වසරේ ජූලි මාසයේ අභ්‍යවකශගත කිරීමට සුදානම් වන අතර, නිශ්චිත දිනයක් පිළිබඳව තවමත් සැල වන්නේ නැහැ. ඒ කොහොම වුණත්, මේ යානයත් 2021 වෙද්දී අඟහරු වෙත ළඟා වීම සිදුවේවියැ යි අපේක්ෂා කෙරෙනවා.

ගුවන් යානා ටිකට්පතක් රැගෙන රටකින් රටකට පියාසර කරනවා සේ ම, අභ්‍යවකාශ ගමනත් සාමාන්‍යකරණය වන දවස වැඩි ඈතක නොවන බව දැන් අපට පැහැදිලි යි. මේ පිළිබඳව ඔබ දරන අදහස් පහළින් පළ කරන්නත් අමතක කරන්න එපා.

‘VIBES of Marketing’ හි නවවැන්න (09) 2020 ජනවාරි මස 9 වන දින සවස 06.00 සිට ශ්‍රී ජයවර්ධනපුර විශ්වවිද්‍යාල පරිශ්‍රයේ දී...

ඔබට මතක ඇති Huawei Technologies Co Ltd ආයතනය වෙත මේ වසර තුළ දී ගැටළු රාශියකට මුහුණ දෙන්නට සිදුවුණා. තම ආරක්ෂාවට Huawei උපාංග තර්ජනයක් බව ට්‍රම්ප් ආණ්ඩුව තීරණය කිරීමත් සමගම Huawei ආයතනය Blacklist (අසාදුලේඛනගත) කිරීම සිදුවුණා. ඊට අමතරව ඇමෙරිකාව සමග ව්‍යාපාර ගනුදෙනු කිරීම් සඳහා ඔවුන්ට සම්බාධක පැනවුණා. පසුගිය මැයි මාසයේ දී මෙසේ සිදුවුණත්, එයින් නොසැලී Huawei ආයතනය පසුගිය සැප්තැම්බරයේ ඔවුන්ගේ නවතම උපාංග පෙළ හඳුන්වා දුන්නා. ඒ අතරට Huawei Mate (flagship) ජංගම දුරකතන මාලාවේ නවතම මාදිලිය වන Huawei Mate 30 ජංගම දුරකතනයත් ඇතුළත්. එමෙන්ම Google Apps කිසිවක් නොමැතිව යි මෙය එළිදැක්වීමට ද කටයුතු කරනු ලැබුවේ. ඇන්ඩ්‍රොයිඩ් මෙහෙයුම් පද්ධතියට අදාළ Play Store, Google Play Services, Google Maps වැනි අත්‍යවශ්‍ය සේවාවන් ද Huawei දුරකතන වෙත අහිමි වුණා. මේ ගැන වැඩි දුර විස්තර Huaweiවලට ඇමරිකාවෙන් කුඩම්මාගේ සැලකිලි- එතකොට අපට මොනවා වෙයි ද? ලිපියෙන් කියවන්න ඔබට හැකියාව තිබෙනවා.

Gizchina.com වෙබ් අඩවිය සිදුකළ පර්යේෂණයක ප්‍රතිඵල අනුව ඇමරිකානු තහනම ද නොතකා ලොව වැඩිම විකිණුම් සහිත දුරකතන වෙළඳනාම අතර දෙවන තැනට පත් වෙන්න Huawei සමාගම සමත් වෙලා තියෙනවා. Counterpointresearch.com වෙබ් අඩවියට අනුව 2019 පළමු කාර්තුව අවසන් වන විටත් ඇපල් සමාගම අබිබවා ලොව ස්මාර්ට් දුරකතන වෙළඳ පොළෙහි ඉදිරියට පැමිණීමට Huawei සමත්ව සිටියා. Samsungවලට පමණක් දෙවැනි වූ එය වසරක් තුළ 50%ක වර්ධනයක් ලබා‍ගෙන තිබුණා. මේ වර්ධනය වසරේ ඉතිරි කාර්තු තුළත් රඳවා ගන්නට සමාගම සමත් වුණා. මේ වන විට ඔවුන් samsung සමාගමට පමණක් දෙවැනි ව තිබෙනවා. මේ සන්නාමයන් දෙක අතර තිබෙන පරතරය 3.6 %ක් පමණ බව තමයි Gizchina.com වෙබ් අඩවිය වාර්තා කරන්නේ.

මේ වසරේ දී පමණක් Huawei සමාගම අලෙවි කළ ජංගම දුරකතන ඒකක ප්‍රමාණය මිලියන 251ක්. එය සමස්ත ජංගම දුරකතන වෙළඳ පොළෙන් 17.7%ක ප්‍රමාණයක් ලෙස හඳුනාගන්න පුළුවන්. තවදුරටත් ජංගම දුරකතන වෙළඳ පොළ තම බලපරාක්‍රමය රඳවා ගන්න samsung සමාගම වෙත හැකි වෙලා තියෙනවා. ඔවුන් පසුගිය 2019 වසර තුළ ඒකක මිලියන 323ක් අලෙවි කරමින් 21.3%ක වෙළඳපල හිමිකාරත්වයක් ලබාගන්න සමත්ව තිබෙනවා. වසර මුල දුරකතන වෙළඳ පොළ දෙවැනි ස්ථානයට පත් ව සිටි ඇපල් සමාගම වසර අග වන විට තෙවැනි තැනට පත් වෙනවා. ඔවුන්ට 2019 වසර තුළ දී හිමි වෙන්නේ ජංගම දුරකතන වෙළඳ පොළෙන් 13.6%ක වෙළඳපළ කොටසක් පමණයි. ඔවුන් විකුණා ඇති iPhone ඒකක සංඛ්‍යාව මිලියන 193ක් ලෙසයි වාර්තා වෙන්නේ.

ඇමරිකාවෙන් පැමිණි දැඩි සම්බාධක හමුවේ වුවත් ස්ථාවරත්වය රැකගැනීමට Huawei සමත්ව තිබෙනවා. ඒ වගේම මේ වෙද්දී Huawei සමාගම Android පාදක නවතම මෙහෙයුම් පද්දතියක් (Harmony operating system) වෙත යොමු වෙමින් ඉන්නා බව ඔබ දන්නවා ඇති. එළඹෙන 2020 දී නිකුත් වන දුරකතන වෙත මේ මෙහෙයුම් පද්දතිය සහ ඒ වෙත ලැබෙන සේවාවන් සියල්ලම පාහේ Huawei වෙතම අනන්‍ය සේවාවන් බව ආරංචි මාර්ග සඳහන් කරනවා. අපි බලමු ඒ සේවාවන් සමග 2020 වසරේ Huawei ජංගම දුරකතන මොන වගේ පෙරළියක් සිදුකරයි ද කියලා. මේ ගැන ඔබේ අදහස් Comment Section එකේ පළ කරන්න අමතක කරන්න එපා.

පසුගිය 2018 වසර සහ මේ ගෙවෙන 2019 වසරේ මුල් භාගය ඇපල් සමාගම ඇතුළු ලෝකයේ අතිශය ප්‍රසිද්ද සමාගම් විශාල ප්‍රමාණයකයට එතරම්ම සුබ දායක වුණේ නැහැ. ඔබට මතක ඇති අපි ඇපල් සමාගමට උද්ගත වූ අපල කාලය ගැන පෙර ලිපියකින් කතා බහ කළා. ඒ ඔස්සේ අපි සවිස්තරාතමක්ව Qualcomm සමාගම සතු patent බලපත්‍රයන් තුනක කරුණු උල්ලංඝනය කිරීම නිසා ඔවුන් ඇපල් සමාගමට විරුද්ධව නඩු පැවරීම සහ Huawei සමාගම සම්බන්ධයෙන් පැවති ගැටළුකාරී තත්ත්වයන් ගැනත් වැඩි දුර කතාබහ කෙරුණා. 2019 වසර අවසන් වීමටත් මත්තෙන් තවත් ගැටළුකාරී තත්ත්වයන් රැසක් ඇපල් සමාගම වෙත උදා වුණා. මේ ලිපිය හරහා කතාබහ කෙරෙන්නේ ඒ පිළිබඳව යි.

පසුගිය දිනක ඇපල් සමාගම ඔවුන්ගේ සේවකයෙකු වෙත නඩු පැවරීමට කටයුතු කළා. ඒ ඔවුන් සමග පවත්වාගෙන ගිය ගිවිසුම් කඩ කරමින් වෙනත් සේවාදායකයන් කිහිපදෙනෙකු වෙත තමන්ගේ ව්‍යාපාරය පිළිබඳව සඳහන් කිරීම නිසා යි. කොහොම නමුත්, මේ සේවකයා ඊට බරපතල චෝදනාවක් ඇපල් සමාගම වෙත එල්ල කරනවා. ඒ, සමාගම තමන්ගේ අනුමැතියකින් තොරව පෞද්ගලික පණිවිඩ නිරීක්ෂණය කළ බව කියමිනුයි. Privacy කියන්නේ ඕනෑම මනුෂ්‍යයෙක් ඉතාම ඉහළින් අගය කරන දෙයක් බව ඔබට අමතුවෙන් කියන්නට අවශ්‍ය නැහැ. මේ චෝදනාව ඉතාම බරපතල වන්නේත් ඒ නිසාවෙනුයි.

මෙලෙස සමාගමේ බුද්ධිමය දේපළ පනත කඩ කළ බව සඳහන් කෙරෙන්නේ Gerard Williams III වෙත යි. ඔහු ඇපල් සමාගමේ mobile chips නිර්මාණය කිරීමේ ප්‍රධාන සැලසුම් නිලධාරියෙකු ලෙස කටයුතු කළා. මේ සිදුවීමට ඇපල් සමාගම වෙත චිප්ස් නිර්මාණය කරන Nuvia සමාගම සහ එහි වර්තමාන ප්‍රධානීන් දෙපළ වන Manu Gulati සහ John Brunoගේ නමුත් ඈඳෙන්නේ, Williams ඒ වෙත ඔහු සම්බන්ධ වීම නිසාවෙන් සහ ඔවුනුත් සමාගමේ හිටපු සේවකයන් නිසාවෙනුයි. ඊට අමතරව ඇපල් සමාගම චෝදනා කරන්නේ Williams ඇපල් සමාගමෙන් සේවකයන් සහ විවිධ ඉංජිනේරුවන් ඉවත් කරවා ගැනීමටත් කටයුතු කළ බව යි.

මේ වෙත පිළිතුරු දෙමින් Williams චෝදනා කරන්නේ ඔහු සහ සමාගමේ සේවකයන් අතර හුවමාරු වූ පණිවුඩ නීති විරෝධීව ඇපල් සමාගම නිරීක්ෂණය කර ඇති බවත්, එනිසාවෙන් Privacy violation එකක් සිදුව ඇති බව යි. ඒ වගේම ඇපල් සමාගමෙන් සේවකයන් ඉවත් වී යාම අඩපණ කිරීම අරමුණු කරගෙන මෙලෙස සේවකයන්ගේ පණිවිඩ ඔවුන් අධීක්ෂණය කරන බව යි. කොහොම වුණත් Williams වෙත තම සමාගමෙන් ඉවත් වී වෙනත් තරගකාරී සමාගමක් වෙත එකතුව වැඩ කිරීමට ඔවුන් අත්සන් කළ ගිවිසුම අනුව හැකියාව නොමැති බව තමයි ඇපල් සමාගම සඳහන් කරන්නේ. ඊට අමතරව තම සමාගම සමග වැඩ කළ කාලය තුළ ලද අත්දැකීම් සහ තාක්ෂණය භාවිත කරමින් ඇපල් සමග තරංග වැදීමට ඔහු කටයුතු කරන බව ඔවුන් සඳහන් කරනවා.

කෙසේවෙතත්, Williams එල්ල කරන චෝදනාවන් සත්‍ය බව තහවුරු වුණොත් තවදුරටත් පරිශීලක දත්ත ආරක්ෂාව ගැන ඇපල් තබා තිබෙන විශ්වාසය පළුදු වෙන බව නම් කියන්නට ඕනේ. ඔබට මතක නම් පසුගිය කාලය පුරාවට ඇපල් සමාගම ඔවුන්ගේ වෙළඳ දැන්වීම් ඔස්සේ කියා සිටියේ තම සමාගම අනෙක් තාක්ෂණික සමාගම්වලින් වෙනස් බවත්, පරිශීලක දත්ත කිසිවක් ඔවුන් එකරැස් නොකරන බව යි. ඒ වගේම ඔබට මතක ඇති, පසුගිය දිනයක ඇපල් දුරකතන පරිශීලක අවසරයකින් තොරව GPS දත්ත එක්රැස් කරන බවට චෝදනා එල්ල වුණා. “what happens on your iPhone, stays on your iPhone.” කියමන කොතරම් දුරට සත්‍යයක් වේදැ යි අපි බලා සිටිමු.

ඇපල් සන්නාමය ගැන වගේම ඒ හා බැඳුණු බොහෝ දේ ගැන ලිපි ගණනාවක් අපි මීට පෙර ඔබ වෙත ගෙන ආවා. ඔය පහතින් අමුණලා තියෙන්නෙ අන්න ඒ ලිපි.

2019 ඇපල් සමාගමට නපුරු වේවි ද?

ඇපල් සමාගමේ අපල කාලය අවසන් ද?  
Microsoft Laptop එකක් මිල දී ගන්න- “Mac Book” වෙතින් ඉල්ලීමක්

ඇපල් සමාගමට විරුද්ධව නැවතත් නඩු?

ඇපල් අලකලංචි

ලෝකය පුරා අතිශය ජනප්‍රිය Messaging App එකක් ලෙස WhatsApp හඳුන්වන්න පුළුවන්. මේ වසර පුරාවට WhatsApp, ලෝක මාධ්‍ය වගේම සමාජ මාධ්‍ය තුළත් විශාල වශයෙන් පුවත් මවන්නට සමත් වුණා. පසුගිය දිනෙක සිට ඉතාම දැඩි ලෙස සමාජ මාධ්‍ය තුළ කතාබහට ලක්වෙන මාතෘකාවක් ලෙස WhatsApp දුරකතන මිලිනය ගණනකට සහාය දැක්වීම නවත්වා දැමීමට එම සමාගම ගෙන ඇති තීරණය හඳුන්වන්න පුළුවන්. මේ ලිපිය හරහා අපේ බලාපොරොත්තුව ඒ කතාවේ ඇත්ත නැත්ත පිළිබඳව ඔබව දැනුවත් කිරීම යි. Facebook සමාගම සතුව පවතින ප්‍රධානතම messaging platform අතර WhatsApp ප්‍රධාන තැනක් ගන්නවා. ලෝකයේ බොහෝ රටවල මෙන්ම ලංකාවේත් ප්‍රධානතම පණිවිඩ හුවමාරු කරගන්නා ක්‍රමයක් ලෙස මෙය භාවිත වෙනවා. පසුගිය දිනෙක Facebook සමාගම ඔවුන්ගේ Support Page එක හරහා දන්වා සිටියේ 2020 පෙබරවාරි පළමු වෙනිදා සිට පැරණි මෙහෙයුම් පද්ධති ක්‍රියාත්මක වෙන දුරකථනවලට තවදුරටත් whatsapp සහාය නොදක්වනු ඇති බව යි.

මෙලෙස සහාය දීම නවත්වා දමන දුරකථන වෙන්නේ, 2014 වසරේ ඇපල් සමාගම හඳුන්වාදුන් iOS 8 හෝ ඊට පැරණි මෙහෙයුම් පද්ධති සංස්කරණයන් ක්‍රියාත්මක වෙන iPhone දුරකතන. 2010 වසරේ නිකුත් වූ Android 2.3.3 (Gingerbread) මෙහෙයුම් පද්දති ධාවනය වෙන දුරකථන වෙතත් WhatsApp සහාය දැක්වීම නවතා දමන්නට සමාගම තීරණය කර තිබෙනවා. ඒ වගේම පැරණි මෙහෙයුම් පද්ධති ධාවනය වෙන දුරකතනයකින් නව ගිණුම් නිර්මාණය කිරීමක් හෝ පවතින ගිණුමක් verify කිරීමක් සිදුකළහොත්, ඒ ගිණුම් block වීමට ද යම් ඉඩක් පවතින බව වාර්තා වෙනවා. මේ ආරංචිය සමග බොහෝ දෙනෙක් පළ කළ මතයක් වන්නේ; කෙමෙන් කෙමෙන් අභාවයට යන Microsoft සමාගමේ Winodws දුරකතන වෙත WhatsApp සහාය දීම නවතා දමනු ඇති බව යි. නමුත්, Windows 8.1 සහ නව සංස්කරණ ධානාවය වෙන දුරකතන වෙත මෙයින් බලපෑමක් නොවන බව තමයි දැනගන්නට ලැබෙන්නේ.

Dark Mode කියන්නේ දුරකතන භාවිත කරන ඕනෑම කෙනෙක් අත්විඳින්න කැමති පහසුකමක්. බොහොමයක් apps වෙත මේ වෙද්දීත් Dark Mode එකක් හඳුන්වා දී අවසන්. දුරකතනය රාත්‍රී කාලයේ දී පාවිච්චි කරද්දී සුදු තිරය තරමක් ඇසට අපහසුවක් බවට පත් වෙනවා. තිරය මතට Filters (Blue Light filters) එකතු කිරීම Reading Mode වැනි පහසුකම් බොහෝ නිෂ්පාදකයන් විසින් ලබා දෙන නමුත්, කළු පැහැති පසුබිම් යොදාගැනීම හෙවත් Dark mode එකක් සහිත Apps පාවිච්චි කිරීම ඊටත් වඩා සාර්ථක විසඳුමක්. විශේෂයෙන්ම Amoled / Oled / Super Amoled තිර සහිත දුරකතන පරිශීලකයන්ට විශාල වශයෙන් බැටරි ආයු කාලය ඉතිරි කර ගන්නත් හැකියාව Dark Mode ඔස්සේ ලැබෙනවා. WhatsApp පරිශීලකයන් මේ පහසුකම කාලයක් තිස්සේ බලාපොරොත්තුවෙන් පසුවන පහසුකමක්. පසුගිය දිනෙක අපූරු ප්‍රවෘත්තියක් සමාජ මාධ්‍ය ඔස්සේ ප්‍රචාරය වුණා. ඒ, Bug එකක් හේතුවෙන් WhatsApp Dark Mode එක enable වීමක් ගැන යි. මෙය සිදුව තිබෙන්නේ WhatsApp හි Beta සංස්කරණයන් භාවිත කරන පරිශීලකයන් කිහිප දෙනෙකුට යි.

YouTube link එකක් WhatsApp හරහා තවත් කෙනෙකුට යැවීමෙන් පසුව එහි thumbnail එක click කර picture-in-picture (PIP) ලෙස Video එක Play කළ විට ඉබේම WhatsApp Dark Mode එකක් enable වූ බව ඔවුන් සඳහන් කර තිබුණා. මේ අත්දැකීමට මුහුණ දී තිබුණේ android 10 මෙහෙයුම් පද්දතිය භාවිත කරන පරිශීලකයන් කිහිපදෙනෙකු යි. හැබැයි මේක ඉතාම සුළු පිරිසකට පමණක් සිදු වූ දෙයක් බව තමයි අපට නම් දැනගන්න ලැබුණේ. කොහොම වෙතත්, මේ වෙද්දී එම ගැටළුව නිරාකරණය කරන්නට පිළියම් යොදන්න සමාගම කටයුතු කර තිබෙනවා.

මේ පිළිබඳව independent.co.uk ඇතුළු වෙබ් අඩවි ගණනාවක් සිදුකළ විමසීම් වෙත WhatsApp සමාගම නිසි පිළිතුරු ලබා දී නැහැ. ඒ වගේම නිල වශයෙන් WhatsApp Dark Mode එක ලබාදෙන දිනයක් පිළිබඳවත් කසිම ආකාරයකට ප්‍රකාශයක් සමාගම නිකුත් කර නැහැ.

මෙම ලිපිය කියැවූ ඔබට WhatsApp ගැන අප මීට ඉහත දී පළ කළ ලිපි පෙළක්ම මෙන්න.

WhatsApp හරහා ඔබේ දුරකතනය හැක් වෙයි ද?

Whatsapp එකෙන් ඊශ්‍රායල සමාගමක් වෙත නඩු!

Whatsapp statusවල දී කළ හැකි අලුත්ම හෝඩුවාවන් සහ ප්‍රයෝග කීපයක්

නම් වෙනස් කරන Instagram සහ whatsapp

Facebook, Instagram, සහ WhatsApp බිඳ වැටීම hacking ප්‍රහාරයක් ද?

Google සමාගම ඔවුන්ගේ augmented reality platform එක වූ ARCore වැඩසටහන වෙත නව අංගයන් රැසක් එළිදැක්වීමට සුදානම් වෙනවා. පසුගිය වසරේ ඔවුන් නිල වශයෙන් ARCore හඳුන්වාදීමෙන් අනතුරුව ඒ වෙත අලුතෙන් බොහෝ දේ එකතු කරන්න Google සමාගම කටයුතු කළා. දැන් google සමාගම සඳහන් කරන්නේ ARCore වැඩසටහන වැඩසටහන නවමු මානයකට ගෙන යාමට මේ යාවත්කාලීනයන් සමග හැකි වනු ඇති බව යි. ඒ වගේම නුදුරු අනාගතයේ දී ම AR අත්දැකීම ඉතාම යථාර්ථවාදීව විඳගන්නට පරිශීලකයන් වෙත ඉඩ ලබා දිය යුතු බව යි. Chrome Dev Summit 2019 හි දීත් මේ ගැන යම් තරමක් දුරට අනාවරණය වුණා.

විශේෂයෙන්ම, ARCore වෙත හඳුන්වාදෙන නව Depth API එක පිළිබඳව බොහෝ දෙනකුගේ අවධානය යොමු වුණා. මේ නව Depth API එක නිසාවෙන් AR තාක්ෂණය භාවිතයෙන් නිර්මාණය වෙන අතත්‍ය වස්තු, සැබෑ ලෝකයේ objectsවලින් පිටුපස වුවත් නිර්මාණය කරන්නට හැකි වෙනවා. මේ නව Depth API එක පිළිබඳව උදාහරණ ලෙසින් Google සමාගම පෙන්වූ සැඟවීමට හැකියාව ඇති AR පූසා, දක්වන්න පුළුවන්. ඉතාම තාත්වික ලෙස භෞතිකව පවතින object එකක පිටුපස සිට ඉදිරියට ඒමටත්, සැඟ වී යාමටත් එම පූසාට හැකියාව තියෙනවා. මේ අනුව ඉදිරි වැඩිදියුණු කිරීම් ඔස්සේ ඔබේ ජංගම දුරකතනයට වස්තුන් දෙකක් අතර ඇති ඉඩ පිළිබඳව වඩාත් හොඳ අවබෝධයක් ලබාගන්නට හැකියාව ලැබෙනවා. මේ නවීකරණයන් සියල්ලම ලබාගන්න ඔබට නව දෘඩාංග සහිත දුරකතනයක් අවශ්‍ය වෙන්නේ නැහැ. පසුගිය වසර කිහිපය තුළ පැමිණි දුරකතන සියල්ලටම පාහේ සියලු නවීකරණයන් සහාය දක්වන බව සමාගම සඳහන් කරනවා. ඔබේ දුරකතනයත් ඒ අතර තිබෙනවා ද දැනගන්න developers.google.com වෙබ් අඩවිය ඔස්සේ පුළුවන්. මේ වෙද්දීත් AR තාක්ෂණය අත්හදා බලලා නැති නම්, අපි ඔබට ඒ අත්දැකීම විඳගන්න apps කිහිපයක් යෝජනා කරන්න කැමතියි. මේ සියල්ල install කරන්න කලින් Google ARCore app එක

Install කරගෙන ඉන්න කියලා අපි ඔබට මතක් කරනවා.

මේ දවස්වල ලංකාවේ Wall Art රැල්ලක් නිර්මාණය වෙමින් පවතිනවා. මෙය කරන්න විශාල මහන්සියක් වගේම විශාල මුදලකුත් වැය වෙනවා. මේ දේ අතථ්‍යව, එහෙම නැතිනම් virtually සිදුකරන්න හැකි වුණොත් ඒක අපූර්ව අත්දැකීමක් වේවි නේද? මේ ඒ වෙනුවෙන්ම නිර්මාණය වූ WallaMe. බිතිවල නිදහසේ කුරුටු ගාන්න මේ app එකත් එක්ක ඔබට පුළුවන්. Android සහ Apple යන දුරකතන වෙත මෙය සහාය දක්වනවා.

AR තාක්ෂණයට භාවිත කරමින් නිර්මාණය වූ තවත් අපුරු app එකක් ලෙස Just a Line හඳුන්වන්න පුළුවන්. තමන් වටේ තියෙන අවකාශයේ සරල චිත්‍ර නිර්මාණය කරන්න මේ app එක පහසුකම් සලසනවා. app එක ධාවනය කළ විට මඳ වෙලාවක් ගෙන, තමා වටේ වන අවකාශය calibrate කරගන්නවා. ඉන් අනතුරුව ඉතාම පහසුවෙන් ඔබට ඔබේ ජංගම දුරකතනය භාවිත කරමින් අවකාශයේ චිත්‍ර අඳින්න හැකියාව ලැබෙනවා. 3D ලෙසින් නිර්මාණය වෙන මේ චිත්‍ර සමග ඔබට විනෝද වන්නට අනිවාර්යෙන්ම හැකි වේවි.

ඉහත අපි සඳහන් කරපු app දෙකට අමතරව පෙර ලිපියක අපි කතා බහ කරපු MarkAR app එකත් මෙවැනිම තාක්ෂණයක් භාවිතා කරන app එකක් ලෙස හඳුන්වන්න පුළුවන්.කොහොම වුණත්, මේ චිත්‍ර ඇඳීම ඇතුළේ යම් අයහපත් පැතිකඩකුත් තිබෙනවා.

ඔබට හෝ වෙන අයෙකුට අපහාස වන අයුරින් ඕනෑම බිත්තියක Virtual Graffiti නිර්මාණය කිරීමේ හැකියාව ඉහත apps install කරගන්නා ඕනෑම අයෙකුට තිබෙනවා. ඒ ගැනත් මේ නිර්මාණකරුවන් සැලකිලිමත් විය යුතු යි. අපි මේ ගැන Virtual බිතුසිතුවම් පෙරළියක් අත ළඟ ලිපියෙන් වැඩිදුරටත් කතාබහ කළා.

සාමාන්‍යයෙන් TaToo එකක් ගහන්න බොහෝ දෙනෙක් කැමැත්තක් පළ කරනවා. නමුත් ටැටූව අපිට ගැළපෙනවද කියල එක බලාගන්න විදිහක් නම් තිබුණේ නැහැ. නමුත්, AR තාක්ෂණය ඔස්සේ එකී හැකියාවත් දැන් ඔබට ලැබෙනවා.

AR/VR තාක්ෂණය ගැන සහ එහි භාවිතාව ගැන වැඩිදුර සොයා දැනගන්න, අප මීට පෙර ලියූ ලිපි පෙළක්ම මෙන්න.

Virtual බිතුසිතුවම් පෙරළියක් අත ළඟ

Smart glass තාක්ෂණය සදහටම සිහිනයක් පමණක් වේවි ද?

යුධ පුහුණුවට ඇමරිකානුවන් HoloLens භාවිතා කරයි

මොබයිල් Appsවල මාවත වෙනස් කරන VR

කවරයේ පින්තූරය: vrscout.com

ලෝකයේ අතිශය ජනප්‍රිය සමාගම් රාශියක් ඉලක්ක කරගෙන සයිබර් ප්‍රහාර මාලාවක් මේ වසර පුරාවටම පාහේ එල්ල වුණා. විශේෂයෙන්ම මෙලෙස ප්‍රහාරයන්ට ලක් වුණේ තාක්ෂණික උපාංග හෝ සේවාවන්වලට සම්බන්ධ ආයතන යි. මේ වසර තාක්ෂණික ලෝකය වෙත නව නිපැයුම් ඉතා විශාල වශයෙන් නිකුත් වූ වසරක් වුණත් දිගින් දිගටම සයිබර් අවකාශය තුළ සිදුවන මේ ප්‍රහාර නිසා, එතරම්ම සුබදායි වසරක් ලෙස හඳුන්වන්න අපට හැකි වෙන්නේ නම් නැහැ. ආසන්නතම ප්‍රහාර සිදුවුණේ OnePlus සමාගම වෙත සහ TrueDialog සමාගම වෙත යි. මේ ප්‍රහාර දෙකෙන් පරිශීලක දත්ත විශාල ප්‍රමාණයක් හැකර්වරු වෙත නිරාවරණය වීම සිදුවුණා. ඒ උණුසුම යන්නටත් මත්තෙන් ලෝකයේ තවත් ප්‍රධාන පෙලේ සමාගම් දෙකක් වෙත එල්ල වූ සයිබර් ප්‍රහාරයන් ගැන ජර්මානු මාධ්‍ය ආයතන කිහිපයක්ම අනාවරණය කර තිබුණා. මෙලෙස ප්‍රහාරයට ලක් වූ සමාගම් ලෙස හඳුන්වෙන්නේ ප්‍රමුඛ පෙළේ මෝටර් රථ නිෂ්පාදන සමාගම් වන BMW සහ Hyundai සමාගම් දෙක යි.

අදාළ Computer Network අත්පත් කරගැනීම මොවුන්ගේ පළමු ඉලක්කය වී ඇති අතර, ඉන් අනතුරුව Cobalt Strike නම් ප්‍රසිද්ධ penetration testing toolkit එක ස්ථාපනය කර තිබෙනවා. ඉන් අනතුරුව එය නැවත ජලය තුළට පහසුවෙන් පිවිසිමට backdoor එකක් බවට පත් කර තිබෙනවා. කොහොම වුණත්, මේ උත්සාහය BMW සමාගමට ඉතා ඉක්මනින් හසුකර ගැනීමට හැකි වී තියෙනවා. නමුත් ඔවුන් එකවර ඒ වෙත ක්‍රියාත්මක නොවී හැකර්වරුන්ගේ අරමුණ සහ සමාගමේ පරිගණක ජාලයේ දුර්වලතාවයන් ගැන හැකර්වරුන්ගේ පියවර ඔස්සේ අධ්‍යයනය කර, ඉන් අනතුරුව හැකර්වරුන්ගේ Access අහිමි කිරීම සිදුකර තිබෙනවා. වහාම ක්‍රියාත්මකව, ඔවුන්ගේ ජාලයන් තුළ තිබූ vulnerability නිවැරදි කිරීමටත් ඔවුන් උත්සුකව කටයුතු කර තිබෙනවා. මේ ප්‍රහාරය එල්ල කළ කණ්ඩායම Ocean Lotus/ APT32 යන නම්වලින් පෙනී සිටින හැකර් කණ්ඩායමක් බව යි මේ වෙද්දී අනාවරණය වී තිබෙන්නේ. මේ සිදුවීම ගැන BMW සමාගම හෝ Hyundai සමාගම නිල ප්‍රකාශ නිකුත් කර නැහැ. ZDNet වෙබ් අඩවිය මේ පිළිබඳව සිදුකළ විමසීම් සඳහාත් ඔවුන් කිසිදු ප්‍රතිචාරයක් දක්වා නැති බව ඔවුන් වාර්තා කළා.

2014 වසරේ සිට ක්‍රියාකාරී සංගමයක් බවට සැලකෙන Ocean Lotus කණ්ඩායම රථවාහන නිෂ්පාදන සහ ඒ ආශ්‍රිත සමාගම් වෙත 2017 වසරේ සිට දිගින් දිගටම සයිබර් ප්‍රහාර එල්ල කරන බව වාර්තා වෙනවා. මේ හැකර්වරු වියට්නාම රජයේ අනුග්‍රහය ලබන පිරිසක් බව යි ආරංචි මාර්ග සඳහන් කරන්නේ. Toyota Australia වෙත එල්ල වූ මීට සමානම ප්‍රහාරයකටත් මේ කණ්ඩායම සැක කෙරෙනවා. ඒ වගේම, ඉන් සති කිහිපයකට පසුව Toyota Japan සහ Toyota Vietnam වෙතින් වාර්තා වූ Data Breach වෙතත් මේ කණ්ඩායම සම්බන්ධ බව යි සැක කෙරෙන්නේ. වියට්නාම් රජය විදේශ සමාගම්වලට එරෙහිව ආර්ථික ඔත්තු බැලීම, සමාගම් සතු බුද්ධිමය දේපළ සොරකම් කිරීම සහ පසුව, එය රාජ්‍ය අරමුදල් සපයන සමාගම් සඳහා භාවිතා කිරීම වැනි දේ සඳහා අනවසරයෙන් කණ්ඩායම් භාවිතා කරන බව යි ZDNet වෙබ් අඩවිය සඳහන් කරන්නේ. ඔවුන්ගේ මේ උත්සාහය අනෙක් සමාගම් පරදවා ඔවුන්ගේ නව රථවාහන සන්නාමය VinFast සන්නාමය ඉහළ නැන්වීම බව යි වැඩිදුරටත් කරුණු දක්වමින් zdnet.com සඳහන් කරන්නේ. VinFast සන්නාමය යටතේ නිකුත් වන නවතම වාහනය ඉතාම ඉක්මනින් වෙළඳපළ වෙත හඳුන්වාදීමට නියමිත යි.

මේ හා සබැඳි පහත ලිපිත් කියවන්න අපි ඔබට ඇරයුම් කරනවා.

OnePlus වෙත නැවතත් hacking ප්‍රහාරයක්

SMS පණිවුඩ මිලියන ගණනක් අන්තර්ජාලයට නිකුත් වෙයි!

සාමාන්‍යයෙන් බොහොමයක් සමාජ ජාලාවන් භාවිත කරන්න යම් ආකාරයක වයස් සීමාවක් තිබෙනවා. මෙයට ප්‍රධාන හේතුව වෙන්නේ අන්තර්ජාතික ළමා ආරක්ෂණ නීති පද්ධතිය යි. Child Online Privacy Protection Act එක එහෙම නැති නම්, COPPA එකට අනුව වයස අවුරුදු 13ට අඩු බාලවයස්කාරයින්ගේ දත්ත දෙමාපිය හෝ බාරකාර අනුමැතිය සහ අධීක්ෂණය නොමැතිව කිසිදු අන්තර්ජාල සේවාවක් ඔස්සේ එකතු කිරීම දඬුවම් ලැබිය හැකි වරදක්. ඇමරිකානු ඩොලර් 40,000ක් හෝ ඊට ඉහළ දඩයක් වුවත් COPPA පනත උල්ලංඝනය කිරීම වෙනුවෙන් නියම වෙන්න ඉඩ තිබෙනවා. නමුත්, ඔබත් මමත් කාලයක සිට භාවිත කරන සමහර සමාජ ජාලාවන් මේ නියාමනයන් නොසාලකා හරින බව ඔබ දන්නවා ද? සමාජ ජලා හෝ අන්තර්ජාල සේවාවන් වෙත ලියාපදිංචි වීමේ දී අවම වශයෙන් උපන්දිනයවත් ඒ ක්‍රියාවලියේ දී ඇතුළත් කිරීමට ඔබට සිදුවෙනවා. ලෝකයේ ජනප්‍රිය සමාජ ජාලයක් වූ instagram වෙතත් ලියාපදිංචි වීමට කිසිදු ආකාරයක වයස් සීමාවක් මෙතෙක් පැනවී තිබුණේ නම් නැහැ.

කොහොම වුණත් පරිශීලකයින් ප්‍රමාණය වැඩි වෙන නිසාවෙන්, විශේෂයෙන් ඇතැම් සමාජ ජාලා මේ පිළිබඳව එතරම්ම තැකීමක් කරන්නේ නැහැ. එනිසාවෙන්ම තවදුරටත් මේ ගැන නොසලකා ඉන්නට ඔවුන්ට හැකියාව ලැබෙන්නේ නැහැ. පසුගිය දිනෙක techcrunch.com වෙබ් අඩවිය මේ පිළිබඳව සවිස්තරාත්මක ලිපියක් පළ කරමින් මෙලෙසින් නිසි අධීක්ෂණයක් නොමැතිව කුඩා දරුවන්ට අන්තර්ජාලය සහ සමාජ ජාලා පරිශීලනය කිරීමට අවස්තාව ලබාදීම විශාල ගැටළු ප්‍රමාණයකට අත වැනීමක් බව කියා සිටියා. දිගින් දිගටම අන්තර්ජාලය හරහා සිදුවන අකටයුතුකම් වෙත දරුවන් ඉතා ඉක්මනින් හසුවීමට ඉඩ තිබෙන බවත් ඔවුන් පෙන්වා දෙනවා. අවම වශයෙන් Instagram මඟින්, ඒ වෙත ලියාපදිංචි වෙන පරිශීලකයන්ගෙන් වයස හා උපන්දිනය ඇතුළත් කරන ලෙස දැනුම් දිය යුතු අතර, තවත් ප්‍රයෝගික ක්‍රමවේදයන් ඔස්සේ ඒ පරිශීලකයන් ඇතුළත් කරන දත්ත තහවුරු කර ගැනීම සිදුකළ යුතු යි. Instagram සමාගමේ මව් සමාගම වන Facebook ආයතන, පරිශීලකයන්ගේ වයස් තහවුරු කර ගැනීමට විවිධ ක්‍රමවේදයන් භාවිතා කරනවා. තහවුරු කර ගත නොහැකි අවස්ථාවන්වල දී එවන් ගිණුම් තාවකාලිකව අත්හිටුවීමටත් Facebook සමාගම කටයුතු කරනවා. මේ සඳහා ඊටම වෙන් වූ වෙනම ඇල්ගොරිතමයන් පවා භාවිත වෙනවා. එලෙස තාවකාලිකව අත්හිටවනු ලබන ගිණුම් නැවත යථා තත්ත්වයට පත් කර ගැනීමට හැකි වෙන්නේ රජය මඟින් අනුමත කරන ලද පුද්ගල අනන්‍යතාව හඳුනාගැනීමේ ලියැවිල්ලක් ඉදිරිපත් කිරීමෙන් අනතුරුව යි.

මේ සියල්ල වෙනස් කරමින් පසුගිය දිනෙක Instagram වෙතත් Age Restriction හඳුන්වාදීමට යන බව දැනගන්න ලැබුණා. COPPA ඇතුළු ළමා ආරක්ෂණ පනත්වලට අවනත නොවී කටයුතු කළ සමාගම් ගණනාවකට ඉතා විශාල වන්දි මුදල් ගෙවන්නට සිදුවුණා. ලෝකයේ ශීඝ්‍රයෙන් වර්ධනය වෙන short video sharing platform එකක් වන TikTok වෙතත් මෙවැනි චෝදනා නිසා ඇමරිකානු ඩොලර් මිලියන 5.7ක් පමණ වන්දි ලෙස ගෙවන්නට සිදුවුණා. ඉන් අනතුරුව ඔවුන්, බාලවයස්කරුවන්ට තමන්ගේ සේවාව වෙත Register වෙන්න ඉඩ ලබා දුන්නත්, video පළ කිරීම හෝ comment කිරීමට හැකියාවක් ලැබෙන්නේ නම් නැහැ. ඔබට මතක ඇති අප මීට පෙර ලිපියකින් TikTok වාරණය කිරීමට රටවල් කිහිපයක් ගත් තීරණ සහ ඒවාට හේතු පිළිබඳව දැනුවත් දැනුවත් කළා. මේ නව Age Restriction එක බලපාන්නේ අලුතෙන් ඒ වෙත ලියාපදිංචි වෙන පරිශීලකයන්ට පමණයි.

අබිරහස් විසඳන Scooby-Doo සහ කණ්ඩායමේ නවතම සිනමාගමනය නුදුරේ දී ම සිදුවීමට නියමිත යි. එය නරඹන්න කලින් මේ කියන්න යන්නේ Scooby-Doo කතා මාලාවට පණ ලැබුණු විදිහ ගැන යි.

ලෝකයේ අතිශය ජනප්‍රිය සමාගම් රාශියක් ඉලක්ක කරගෙන සයිබර් ප්‍රහාර මාලාවක් මේ වසර පුරාවටම පාහේ එල්ල වුණා. ආසන්නතම සිදුවීම වාර්තා වුණේ OnePlus සමාගම වෙත යි. ඒ ගැන අපි ඔබව මීට ඉහත දී “OnePlus වෙත නැවතත් hacking ප්‍රහාරයක්” යන ලිපියෙන් දැනුවත් කළා. මේ කියන්න යන්නේ ලෝකයේ අතිශය ජනප්‍රිය තවත් සමාගමක් වෙත එල්ල වූ ප්‍රහාරයක් ගැන යි.

ඇමරිකානු TrueDialog, සමාගම ලෝකය පුරා අතිශය ජනප්‍රිය SMS පණිවිඩ හුවමාරු සේවාවක් ලෙස හඳුන්වන්න පුළුවන්. පසුගිය දිනෙක මේ සමාගම සපයන සේවාව ඔස්සේ හුවමාරු වුණ SMS (short message service) එහෙම නැතිනම්, කෙටි පණිවුඩ රැසක් අන්තර්ජාලය වෙත නිරාවරණය වී තිබුණා. මේ සේවාව වැඩි වශයෙන්ම භාවිත කරන උසස් අධ්‍යාපන ආයතන සහ ව්‍යාපාර ආයතන රැසක දත්ත මේ අතර තිබූ බව තමයි techcrunch.com වෙබ් අඩවිය අනාවරණය කරන්නේ. මෙලෙස දත්ත අන්තර්ජාලයට අනාවරණය වීමට ප්‍රධාන හේතුව ලෙස සඳහන් වෙන්නේ ඔවුන්ගේ දත්ත ගබඩා (Data Base)වල තිබූ ආරක්ෂණ උපක්‍රමයන්ගේ දෝෂයන් බව තමයි වාර්තා වෙන්නේ. මෙවැනි සේවා භාවිත කරමින් යවන bulk text සම්පුර්ණයෙන්ම පාහේ ඔවුන්ගේ සේවාදායක පරිගණකවල සහ දත්ත සමුදායන් තුළ ගබඩා වී තිබෙනවා. වසර ගණනාවක් තිස්සේ යැවූ පණිවිඩ මිලියන ගණනක් මෙලෙස අන්තර්ජාලය වෙත නිකුත්ව තිබෙන බව යි වාර්තා වෙන්නේ. මෙවැනි SMS සේවාවන් ගණනාවක් ලෝකය පුරා භාවිතයේ තිබුණත් මේ TrueDialog සේවාව, සේවාදායකයන් අතර ජනප්‍රිය වෙන්නේ ඔවුන්ගේ සේවාව ඔස්සේ two-way conversations පවත්වන්න හැකියාව තිබීම නිසා යි.

Noam Rotem සහ Ran Locar, ඇතුළු vpnMentor කණ්ඩායම විසින් පළමු වරට මේ breached database එක පිළිබඳව කරුණු අනාවරණය කරගෙන ඇති අතර, ඔවුන්ට අනුව මේ ඔස්සේ ඇමරිකාව ඇතුළු ලෝකයේ රටවල් ගණනාවක් TrueDialog පරිශීලකයන්ගේ දත්ත අති විශාල ප්‍රමාණයක් මේ දත්ත කාන්දුව වෙත හසුව තිබෙනවා. මෙසේ කාන්දු වූ දත්ත අතරට two-factor codes, security messages, usernames/ passwords, PII data වැනි දේවල් අඩංගු බව තමයි පරීක්ෂණ කණ්ඩායම සඳහන් කරන්නේ. ඊට අමතරව මේ breach එක නිසාවෙන් TrueDialog පරිශීලකයන්ගේ logins පවා ඉතාම අනාරක්ෂිත මට්ටමක පවතින බව vpnMentor කණ්ඩායම පෙන්වා දෙනවා. ඇමරිකාවේ ටෙක්සාස් ප්‍රාන්තයේ පවත්වාගෙන යන මේ සමාගම වසර 10ක් පමණ තිස්සේ පරිශීලකයන් වෙත සේවාවන් සපයන සමාගමක් ලෙස ඉතාම ප්‍රසිද්ධියක් උසුලනවා. ඒ වගේම, ලෝකය පුරා ජංගම දුරකතන සේවා සැපයුම්කරුවන් 990ක් පමණ මේ සමාගම සමග කටයුතු කරනවා. ඊට අමතරව මේ සමග රැඳී සිටින පරිශීලකයන් ප්‍රමාණය බිලියන 5කටත් අධික යි.

මේ පිළිබඳව vpnMentor කණ්ඩායම අනාවරණය කළ සැනින් TrueDialog සමාගම මේ වෙත පියවරක් ලෙස දත්ත සමුදායේ තිබූ ගැටළුව හඳුනාගනිමින් කටයුතු කර තිබුණත්, එය පමණක් ප්‍රමාණවත් නොවන බව යි vpnMentor කණ්ඩායමේ අදහස. සාමාන්‍යයෙන් මෙවැනි breach එකක් සිදු වූ වහාම පරිශීලකයන් තමන්ගේ සේවාදායකයන් වෙත නිල වශයෙන් දැනුම් දිය යුතු වුණත්, මේ වන තෙක් (2019.12.03) කිසිදු දැනුම් දීමක් හෝ නිල ප්‍රකාශයක් සිදුකර නොමැති බව ද ඔවුන් සදහන් කරනවා. ඒ වගේම මේ දත්ත breach එකේ සුලමුල සොයාගැනීම සඳහා තම කණ්ඩායමේ තාක්ෂණික දැනුම ලබාදෙන්න vpnMentor කණ්ඩායම ඉදිරිපත් වුණත්, ඒ පිළිබඳව TrueDialog සමාගම කිසිදු ප්‍රතිචාරයක් දක්වා තිබුණේ නැහැ. මෙම සමාගමේ නිහඬ පිළිවෙත ගැන techcrunch.com වෙබ් අඩවියත් තම අප්‍රසාදය පළ කරන්නේ ඔවුන් වෙතත් කිසිදු ප්‍රතිචාරයක් හෝ මේ සිදුවීම ගැන ප්‍රකාශයක් කිරීම අදාළ සමාගම ප්‍රතික්ෂේප කිරීම හේතුවෙනුයි.

මෙවැනි සිදුවීමක් පිළිබඳව සේවා ලාභියෙක් ලෙස ඔබට ගන්න පුළුවන් ක්‍රියාමාර්ග ගැන අපි පෙර ලිපියකින් ඔබව දැනුවත් කළා. ඒ, මෙතක් සිදු වූ ලොකුම Data breach එක ගැන යි.

Google සමාගම, ලෝකයේ වැඩිම දෙනෙක් භාවිත කරන සේවාවන් බොහොමයක් සපයන සමාගමක්. නමුත්, කාලයෙන් කාලයට විවිධ හේතු මත සමහර සේවාවන් නවතා දමන්නට Google සමාගමට සිදුවුණා. “2018 වසර සමග ම සමුගන්නා Google සේවාවන්” කිහිපයක් පිළිබඳව අප පෙර ලිපියකින් ඔබව දැනුවත් කළා. මේ කියන්න යන්නේ එවැනිම නවතා දැමෙන තවත් සේවාවන් කිහිපයක් ගැන වගේම, නවතා දැමුණු සේවාවන් වෙත ලබාදුන් සොහොන් කොත් පිළිබඳව යි.

Google Cloud Print සේවාව මේ වෙද්දීත් බොහෝ දෙනෙක් භාවිත කරන සේවාවක්. නමුත්, පසුගිය දිනෙක නිවේදනයක් නිකුත් කරමින් google සමාගම සඳහන් කළේ ඔවුන් මේ සේවාව නවතා දැමීමට සුදානම් වෙන බව යි. 2010 වසරේ google සමාගම හඳුන්වාදුන් මේ සේවාව, 2020 වර්ෂයේ දෙසැම්බර් මස 31 දින සිට නවතා දැමීමට ඔවුන් කටයුතු කරනු ඇති. Google Cloud Print සේවාව හරහා cloud-connected printerවලින් printout ලබාගැනීම සිදුකරන්න පුළුවන්. මේ සේවාව නිර්මාණය වෙන්නේ Chrome OS භාවිතා කරන්නන් වෙත යි. ඔබගේ Google account එක connect කර ඇති PC එකකට සම්බන්ධ වූ printer එකක් තිබෙන්නේ නම්, ඔබගේ ජංගම දුරකථනය මඟින් මේ සේවාව හරහා අදාළ PC එක සහ printer එක භාවිතා කරමින් printouts ලබාගැනීමේ හැකියාව තිබෙනවා.

Google Hangouts සේවාව Google සමාගමෙන් ලබාදුන් තවත් වටිනා සේවාවක්. messages, video chat, සහ VOIP වැනි පහසුකම් රැසක් සපිරි මේ සේවාව එළඹෙන වසරේ දී නවතා දැමීමට Google සමාගම තීරණය කර තිබෙනවා. වසර 8ක පමණ කාලයක් පරිශීලකයන් වෙත මේ සේවාව හිමි වුණා. මේ සේවාව වඩාත් ජනප්‍රිය වෙන්නේ Google Plus සමාග ජාලය ඔස්සේ යි. කොහොම වුණත්, G+ නවතා දැමීමෙන් පසුව මේ සේවාව හා රැඳුණු පිරිස ක්‍රමයෙන් අඩුව යන්නට පටන් ගත්තා. “ගූග්ල් ප්ලස්, පස් වන ලකුණු!” ලිපිය ඔබට මතක නම්, ඒ ඔස්සේ අපි වැඩිදුරටත් G+ නවතා දැමීම ගැන කතාබහ කළා.

Hire by Google සේවාව වසර දෙකකට පෙර එනම්, 2017 වසරේ ආරම්භ වෙන්නේ Google for Jobs ව්‍යාපෘතියට සමගාමීව යි. මෙහි අරමුණ බවට පත් වෙන්නේ නව/ කුඩා ව්‍යාපාර සඳහා අයදුම්කරුවන් සොයා දීම යි. කොහොම වුණත්, මෙය නිල වශයෙන් 2020 වසරේ සැප්තැම්බරයේ නවතා දමන බවට සමාගම පසුගිය දිනෙක නිවේදනය කළා.

මීට අමතරව Fabric, Hangouts on Air, Google Correlate, Google Translator Toolkit වැනි සේවා ගණනාවක් මේ වසරේ දී නවතා දමන්නට Google සමාගම කටයුතු කරනු ඇති. නවතා දැමූ අනෙක් සේවාවන් සමග ඔවුන් Google Graveyard එක එහෙම නැතිනම් killedbygoogle.com හි සඳහන් වේවි.

Sonic කියන්නේ ලෝකය පුරා ජනාදරයට පත් වූ චරිතයක්. මේ කියන්න යන්නේ ලබන වසරේ තිරගත වෙන්න නියමිත sonic චිත්‍රපටය ගැන සහ සොනික් sonicගේ ඉතිහාසයෙන් බිඳක්.

මේ වෙද්දී Facebook සාමාජජාලයේ හැසිරී හොඳින් අත්දැකීම් ඇති ඔබටත් මටත් Facebook Server Down එකක් කියන්නේ එතරම්ම නුපුරුදු දෙයක් නම් නෙමෙයි. විටින් විට සිදුවන තාක්ෂණික යාවත්කාලීනවීම් වැනි දේ නිසා බොහෝ විට තාවකාලිකව Facebook සමාජ ජාලය ඇතුළු Facebook සමාගම සතුව පවතින Whatsapp, Instagram වැනි සේවාත් බිඳ වැටීම සිදුවෙනවා. අලුතෙන්ම සිදුවුණු Server Maintenance එකක් නිසාවෙන් පසුගිය බ්‍රහස්පතින්දා දිනයේ (2019.11.28) ලෝකය පුරා විශාල පිරිසකට මේ සමාජජාලාවන් වෙත නිසි ආකාරයෙන් පිවිසෙන්න නොහැකි තත්ත්වයන් උද්ගත වුණා. ෆොටෝස් upload කිරීම, share කිරීම, සහ status update කිරීම වැනි ප්‍රධාන පහසුකම් අතුරුදන් වීම ලොව පුරාම මිලියන ගණනක් පරිශීලකයන් කලබලයට පත් කරන්නට සමත් වුණා. මේ බලපෑම ඉන් නොනැවතී WhatsApp එල්ල වුණා.

ඒ වගේම facebook හරහා sign වීමෙන් ගිණුම් වෙත ඇතුල් වීමට හැකියාව ලබාදුන් Spotify, Tinder වැනි සේවාවන් වෙතත් සම්බන්ධ විය නොහැකිවීම් පිළිබඳව ලෝකය වටෙන්ම වාර්තා වුණා. මේ බිඳවැටීම් මාලාව සිදුව ඇතැ යි සැලකෙන්නේ ඇමරිකානු නැගෙනහිර වෙරළබඩ වේලාවෙන් (Eastern Time (ET))

උදෑසන 6ට පමණ යි. ආරංචි මාර්ගවලට අනුව මෙය facebook සමාගමේ server යාවත්කාලීනවීමක් බව තමයි දැනගන්න ලැබෙන්නේ. මේ බිඳ වැටීම Thanksgiving Dayහි (තුති පිදීමේ දිනයේ) සිදුවීම නිසා ඒ පිළිබඳව සමාව අයදින්නත් සමාගම අමතක කළේ නම් නැහැ.

ඉතාම ඉක්මනින් අදාළ දෝෂයන් නිවැරදි කරන්න facebook සමාගම කටයුතු කළත් ඒ කාලය අතරතුර විවිධ facebook පිටු සහ පෞද්ගලික ගිණුම් (personal accounts) disable වීම් සහ report වීම් පිළිබඳව සඳහන් වෙන විවිධ post අපට දකින්නට ලැබුණා. මේ අතරින් බොහොමයක් තමන්ගේ ගිණුම්වල සහ pageවල reach වැඩි කරගන්නට දැරූ උත්සාහයන් බව තමයි අපට නම් පෙනී ගියේ. විශේෂයෙන් “අනේ මගේ page එක report වෙනවා sticker comments දාන්න” වැනි ප්‍රකාශයන් සුලභව අපට දකින්න ලැබුණා.

Post එකක්, පෞද්ගලික ගිණුමක් හෝ page එකක් වුණත් report වීමේ දී මූලික ක්‍රියාවලිය සිදුවන්නේ ඉහත සඳහන් කළ ආකාරයටම යි. උදාහරණයක් විදිහට ගත්තොත් ලංකාව තුළ සිදු වූ ත්‍රස්ත ක්‍රියාවන් සම්බන්ධව ලිපි සහ ඡායාරූප පළ කළ Facebook පිටු සහ ගිණුම් report වීම සහ disable වීම දෙයාකාරයකට සිදුවෙන්නට පුළුවන්. ඔවුන් දමන ලද postවල අන්තර්ගතය සමාජයට හානිදායක බව අනෙක් පරිශීලකයන් Facebook සමාගම වෙත report කිරීම නිසා හෝ මූලික පරීක්ෂාවන්වල දී හසු නොවුණු Facebook Community Standards සමග නොගැලපෙන යමක් facebook බොට්ස් වෙත හමු වූ නිසාවෙන් වෙන්නට පුළුවන්. මේ scan වීම සිදුවන්නේ බොට්ස් වෙත ලබා දුන් keywords වැනි දේවල් භාවිතයෙන්. මේ පරික්ෂාව වෙත ඔහුගේ post එකට ලැබෙන ප්‍රතිචාර (comments) පිළිබඳවත් සලකා බැලෙනවා. ඒ වගේම නිතරම facebook පිටුවක් හෝ ගිණුමක් පිළිබඳව අනෙක් පරිශීලකයන්ගෙන් report වීම් පැමිණෙනවා නම්, ඒ ගිණුම් හෝ පිටු පිළිබඳ ව සහ එහි අන්තර්ගතයන් ගැන සහ ඒවාට පුද්ගලයින් දක්වන ප්‍රතිචාර පිළිබඳවත් සලකා බැලීමක් සිදුකෙරෙනවා. විශේෂයෙන් අදාල report වීම් පැමිණෙන්නේ කුමන කාණ්ඩයක් යටතේ ද යන්න ගැනත්, ඒ අනුව ගත යුතු ක්‍රියාමාර්ග ගැනත් තීරණය කෙරෙනවා. බොහෝ විට මේ සියලු කටයුතු සඳහා ඒ එක් එක් කාර්යයන්ට විශේෂිත වූ බොට්වරුන් සිටිනවා.

සාමාන්‍යයෙන් තරමක් වැඩි reach එකක් තිබෙන, වැඩි පිරිසක් ගැවසෙන page සහ profile disable වීමට අනෙක් සාමාන්‍ය profileවලට සාපේක්ෂව යම් කාලයක් ගත වෙනවා. නමුත් likes හෝ reach වෙන ප්‍රමාණය වැඩිවීම ඔබේ facebook පිටුව ආරක්ෂා වෙන්නට විශේෂ හේතුවක් නොවන බව හොඳින් මතක තබාගත යුතු යි. එයට හොඳම උදාහරණය සපයන්නේ Sarcasm Facebook පිටුව යි. මිලියන ගණනක් likes තිබුණු ඒ පිටුවත් කාලයක් තිස්සේ disable වීමකට ලක් වී තිබුණා.

බොහෝ විට ඉහත Image එකේ දැක්වෙන අන්දමේ post බොහෝ විට profile එකට හෝ page එකට reach/ likes ලබා ගැනීමට දරන කූට ප්‍රයත්නයක් වීමට ලොකු ඉඩක් තිබෙනවා. කාගේ හෝ ඉල්ලීමකට, යම් කෙනෙකුට, හෝ පේජ් එකකට වැඩි වැඩියෙන් ස්ටිකර් කමෙන්ට්ස් ලබාදෙන විට ඔබ සියලු දෙනාගේ මිතුරු ලැයිස්තුවල සිටින යහළුවන්ට සහ ෆලෝවර්ස්ලට ඒක පේන්න තියෙන ඉඩ සෑහෙන වැඩි වෙනවා. එමඟින් අදාළ පුද්ගලයාගේ හෝ page එකේ reach වැඩි වීම පමණක් සිදුවෙනවා. reach වැඩි කරගැනීම වරදක් නොවුණත් ඔබ නොදැනුවත්ව හෝ මුලාවට පත් වී "වැහෙන්න යන්නේ....!", “අහවල් පිරිස මේ profile එක report කරනවා”, “මම අදාළ ලිපිය දාපු නිසා report වෙනවා, මෙච්චර ගාණක් comments දෙන්න” වැනි ප්‍රකාශයන් නිසා අනවශ්‍ය පුද්ගලයින්ට reach ලබා දෙන්න පෙර දෙවරක් නුවණින් සිතන්නයැ යි අපි ඔබට මතක් කරනවා.

පහත ලිපිත් කියවන්න අපි ඔබට ආරාධනා කරනවා

Facebook, Instagram, සහ WhatsApp බිඳ වැටීම hacking ප්‍රහාරයක් ද?

Facebook සහ Instagram like count එක ඉවත් කිරීමට සැරසෙයි

පෙර වැරදි නිසා facebook apps 10,000ක් අත්හිටුවයි!

නම් වෙනස් කරන Instagram සහ whatsapp

Profile එකක්, Page එකක් Report වුණොත් Comments දාලා ගොඩගන්න පුළුවන් ද?

2019 වසර ආරම්භයේ සිටම තාක්ෂණික ලෝකයට එතරම්ම සුබදායි නොවුණු බව කියන්න පුළුවන්. ලෝකය පුරා විවිධ සමාගම් ඉලක්ක කරගෙන විශාල සයිබර් ප්‍රහාර මාලාවක් වසර මුල සිටම එල්ලවුණා. අප ඒ පිළිබඳව ලිපි මාලාවකින් ඔබව දැනුවත් කළා. මෑතක සිදුවූ දරුණුතම ප්‍රහාරය ලෙස NordVPN වෙත එල්ලවූ ප්‍රහාරය ලෙස හඳුන්වන්න පුළුවන්. මේ කියන්න යන්නේ ලෝකයේ තවත් අතිශය ජනප්‍රිය සමාගමක් වෙත එල්ල වූ සයිබර් ප්‍රහාරයක් පිළිබඳව යි.

OnePlus කියන්නේ ප්‍රමුඛ පෙළේ smart phone නිශ්පාදනය කරන්නෙකු ලෙස ලෝකය පුරා ජනාදරයට පත්වුණු චීන ආයතනයක්. මේ සමාගම තමන්ගේ නිශ්පාදන කටයුතු ආරම්භ කළේ 2013 වසරේ දී යි. ලොව ප්‍රමුඛතම ඉලෙක්ට්‍රොනික් භාණ්ඩ නිපදවන සමාගමක් සහ ලෝකයේ දෙවන විශාලතම ජංගම දුරකථන නිපදවන සමාගම වන BBK සමාගමට අයත් අනු සමාගමක් තමයි OnePlus සමාගම. මේ සමාගම වෙත එල්ල වුණු දෙවන සයිබර් ප්‍රහාරය පසුගිය දා එල්ල වුණා. අවසාන ප්‍රහාරය එල්ලවී වසර දෙකකටත් අඩු කාලයක දී යි මේ.

ප්‍රහාරය ගැන නිල නිවේදනයක් නිකුත් කරමින් සමාගම සඳහන් කරන්නේ “unauthorized party” එකක්, එහෙම නැති නම් අවසර නොලත් පාර්ශවයක් විසින්, තම පාරිභෝගිකයන්ගේ දත්ත ලබාගෙන ඇති බව යි. පාරිභෝගිකයින්ගේ නම්, ලිපිනයන්, දුරකථන අංක, සහ විද්‍යුත් ලිපිනයන් වැනි දත්ත මෙලෙස හැකර්වරුන් අතට පත්වී ඇති බව තමයි සමාගම සඳහන් කරන්නේ.

FAQ එකක් ඔස්සේ සමාගම සඳහන් කරන්නේ තමන් මේ Data breach එක ගැන දැනුවත් වුණේ පසුගිය සතියේ බවත් සහ වහාම ඒ පිළිබඳව අදාල ආරක්ෂණ ක්‍රියාමාර්ග ගත් බව යි. OnePlus ප්‍රධාන වෙබ් අඩවියේ ඇති online store එකෙහි ඇති ආරක්ෂණ දුර්වලතාවයක් නිසාවෙන් මේ ප්‍රහාරය පැමිණෙන්නට ඇති බව තමයි මේ වෙද්දී සමාගම විශ්වාස කරන්නේ.

මේ ඔස්සේ පරිශීලකයන් වෙත Spam සහ Phishing ඇතුළත් email පණිවුඩ ලැබීමට ඉඩ තිබෙන බව සමාගම සඳහන් කරනවා. මේ ප්‍රහාරය මඟින් දත්ත අනාවරණය වූ පරිශීලකයන් ප්‍රමාණය ගැන නිල වශයෙන් සමාගම තවමත් සඳහන් කරන්නේ නැහැ. නමුත් මේ වන විට එම පරිශීලකයන් වෙත දැනුම්දීම් සිදු කිරීමට සමාගම කටයුතු කර තිබෙනවා. 2018 වසරේ ජනවාරියේ දීත් මෙලෙසම සිදුවූ ප්‍රහාරයෙන් පරිශීලකයන් 40,000කට පමණ බලපෑම් එල්ලවුණා.

Phishing සහ Spam පිළිබඳවත් යමක් ලිපිය වෙත එකතු කරන්න අප හිතුවා. අන්තර්ජාලයේ සැරිසරද්දී ඔබට ආරක්ෂා වෙන්නට ගත හැකි පියවර ගැන අපි පෙර ලිපි කිහිපයක කතාබහ කළා. ඇත්තටම phishing attacks කියන්නේ ඉතාම ප්‍රාථමික hacking/ attacking method එකක්. මේ හරහා සිදු වෙන්නේ ඔබ නිතර භාවිතා කරන වෙබ් අඩවියකට සමාන වෙබ් අඩවි ලිපිනයක් (URL) එකක් සහ පෙනුමක් සහිතව නිර්මාණය වෙන ව්‍යාජ වෙබ් අඩවියක් හරහා ඔබේ ගිණුම් දත්ත සහ පරිශීලක දත්ත සොරකම් කිරීමක්. Phishing කියන යෙදුම භාවිතයට එන්නේ, ආකර්ෂණීය උපායක් භාවිතා කරමින් පුද්ගලයන් ව්‍යාජ වෙබ් අඩවි වෙත ගෙන්වා ගැනීම නිසා (හරියට ඇමක් භාවිතා කර මාළු ඇල්ලීම වගේම) යි. හැකර්වරුන් අතර “f” වෙනුවට “ph” භාවිතා වන නිසාවෙන් fishing ලෙස භාවිතා නොවී phishing ලෙසින් යෙදුණා. Spam ලෙස හඳුන්වන්නේ හුදෙක් අන්තර්ජාලය ආශ්‍රිතව ක්‍රියාත්මක වෙන, විද්‍යුත් ලිපින භාවිතයේ දී අප වෙත ලැබෙන කරදරකාරී වෙළඳ දැන්වීම් හෝ කරදරකාරී ලිපි ලෙස හඳුන්වන්න පුළුවන්.

මේ ප්‍රහාරයන් සහ එවන් ගැලවෙන ආකාරය දැනගන්න අපි ඔබට පහත ලිපි කියවන්න ආරාධනා කරනවා

Phishing සහ Spamවලට එරෙහිව Google

Email ගොදුරු කරගන්නා “සේනා”වන්ගෙන් ප්‍රවේශම් වන්න!

Ransomwareවලින් පරෙස්සම් නොවුණොත්, කප්පම් ගෙවන්නත් වෙයි ඔන්න

පසුගිය මාර්තුවේ දී Google සමාගම Google Stadia සංකල්පය සහ එහි භාවිතාවන් ගැන හඳුන්වාදුන් විට තාක්ෂණික ලෝකය තුළ ඇති වූ hype එක ඔබට මතක ඇති. පසුගිය නොවැම්බර් 19 වැනි දින Stadia නිල වශයෙන් වෙළඳපොළ වෙත මුදා හැරීම සිදුවුණා. නමුත්, එදින පටන් මේ Platform එක ගැන අහන්න ලැබුණේ නම් එතරම් හොඳ කතා නෙමෙයි. Stadia Platform එක Google සමාගමේ අසාර්ථක උත්සාහයක් ද? මේ ලිපියෙන් අපි ඒ ගැන සොයා බලමු.

cross-platform game streaming සේවාවක් ලෙසින් ක්‍රියාත්මක වෙන Google Stadia හරහා ඔබට පරිගණක ක්‍රීඩාවන් ඔබේ ජංගම දුරකතනය තුළත් ක්‍රීඩා කරන්න පහසුකම් සලසනවා. ඊට අමතරව විවිධ වූ වෙනත් Gaming Platform තුළත් මෙලෙසින් මාරු වෙමින් ක්‍රීඩා කරන්න ඔබට පහසුකම් ලැබෙන බව තමයි googel සමාගම සඳහන් කළේ. සාමාන්‍යයෙන් Game download කිරීමට වැය වෙන අධික Data ප්‍රමාණය සහ ඉතාම ඉහළ පරිගණක පද්ධති අවශ්‍යතා (System Requirement) සහිත පරිගණක ක්‍රීඩා, ක්‍රීඩා කිරීමේ අපහසුතාවයන් මඟහරවා ගැනීමත් stadia සංකල්පයේ ප්‍රධාන අරමුණු අතර වුණා.

ඊට අමතරව Yotube,Twich,Mixer වැනි Platformවල පරිගණක ක්‍රීඩා Streaming කරන ක්‍රීඩකයන් සමග සජීවීව සම්බන්ධ වෙමින් ක්‍රීඩා කරන්නත් ඉඩ පහසුකම ලබා දෙන්න Stadia හරහා හැකියාව තිබෙනවා.

Stadia “Founder’s Edition” හි මිල ඇමරිකානු ඩොලර් 130ක් පමණ වන බව තමයි වාර්තා වුණේ. පසුගිය 19 වැනි දා මෙය නිල වශයෙන් නිකුත් වුවත්, එය මිලට ගත් බොහෝ දෙනෙකුට තවමත් මේ හරහා ක්‍රීඩා කරන්නට අවස්ථාව ලැබී නැහැ. ඒ ඔවුන්ගේ ඇතුළත් වීමේ කේතය රැගත් email පණිවුඩය තවමත් නොලැබීම නිසාවෙනුයි. කෙසේ වෙතත්, මේ මැසිවිලිවලට ප්‍රතිචාර දැක්වූ google සමාගම සඳහන් කරන්නේ; තමන් දිනක් හෝ දෙකක් ඇතුළත සියලුම email යවා අවසන් කරන බව යි. එනමුත්, තවමත් එය නොලැබුණු බව සඳහන් කරමින් Twitter සහ Reddit සමාග ජාලාවන්වල post පළ වෙන බව අපට දැකගන්න ලැබුණා.

තවත් පරිශීලකයන් කොටසක් මැසිවිලි නගන්නට පටන් ගත්තේ Stadia සමග සම්බන්ධ කළ පසු ඔවුන්ගේ Chromecasts උපාංගය අධික ලෙස රත් වීම සහ ඉන් අනතුරුව ක්‍රියා විරහිත වීම සිදුවන බව යි. විශේෂයෙන්ම මේ අකරතැබ්බයට මුහුණ දෙන්නට සිදුව තිබෙන්නේ Chromecast Ultra උපාංගය භාවිත කරන පරිශීලකයන් වෙත බව තමයි මේ වෙද්දී දැනගන්නට ලැබෙන්නේ. එමෙන්ම, මේ පිළිබඳව අප්‍රසාදය පළකරන තවත් පිරිසක් සඳහන් කරන්නේ; ඔවුන් මේ ගැන පුදුමයට පත් නොවන බව යි. වර්තමාන භාවිතයේ ඇති මීට සමාන අනෙක් උපාංග සමග සංසන්දනය කිරීමේ දී Chromecast Ultra එතරම්ම හොඳ උපාංගයක් නොවන බව යි ඔවුන්ගේ මතය. ක්‍රීඩාවන් කෙසේ වෙතත්, TV series එකක් බැලීමේ දී පවා එය අධික ලෙස රත් වීම් සිදුවන බව තමයි ඔවුන් ප්‍රකාශ කරන්නේ.

ලබන වසරේ සම්පුර්ණයෙන්ම cloud-based version එක හඳුන්වා දෙන තෙක්, Stadia උපාංගය ඔබට භාවිත කරන්නට හැකි වෙන්නේ Chromecast Ultra එකෙහිම පමණක් වීම නිසාවෙන් මේ ගැටළුව වඩාත් උග්‍ර අතට හැරෙන බව තමයි පරිශීලක මතය.

ඉහත ගැටළුව පැන නොනැගුණු පරිශීලකයන් වෙත තවත් ගැටළුකාරී වාතාවරණයන් වෙත මුහුණ දීමට සිදුව තිබුණා. විශේෂයෙන්ම අන්තර්ජාලය හරහා පරිගණක ක්‍රීඩා සිදුකරද්දී ඉතාම අවම latency එකක් තබා ගැනීම වැදගත්. නමුත්, මේ වෙන තෙක් Stadia පරිශීලකයන් වෙත google සමාගම සඳහන් කළ මට්ටමට latency අවම වීමක් නම් දැකගන්නට ලැබී නැහැ. එනිසාවෙන් ක්‍රීඩාවන් හි නිරත වීම සහ ජයග්‍රහණය තරමක් අපහසු බව යි ක්‍රීඩකයන් සඳහන් කරන්නේ.

ඉහත කිසිදු ගැටළුවකට Google සමාගම හෝ Stadia නිර්මාපකයින් නිල වශයෙන් පිළිතුරු ලබා දී නැහැ. පිළිතුරු කෙසේවෙතත්, තවමත් බොහෝ දෙනෙකුට ඔවුන් Order කළ Stadia උපාංග පවා නොලැබුණු බව යි තාක්ෂණික ලෝකය දෙසින් වාර්තා වෙන්නේ. ඇත්තටම මේ සංකල්පය අසාර්ථක ද? ලංකාව වගේ රටකට මෙය කොතරම් දුරකට ප්‍රායෝගික ද? මේ ගැන ඔබේ අදහස් පහළින් එකතු කරන්නත් අමතක කරන්න එපා.

තාක්ෂණයේ දියුණුවත් එක්ක අද වෙද්දී wireless headphone කියන්නේ අපට මේ වෙද්දී ඉතාම සුලබ ව දැකගන්න ලැබෙන දෙයක්. වඩා හොඳ Sound quality එකක්, noise cancellation වගේම, පැය ගණනාවක් වුණත් අපහසුවකින් තොරව headphone එක පැළඳගෙන ඉන්න හැකි මට්ටමට අද අපි කතා කරන headphone නිර්මාණය කරලා තියෙනවා. හැබැයි ඉතින්, සාමාන්‍යයෙන් තරමක් හොඳ wireless headphone එකක් මිල දී ගන්න ඔබට තරමක් වැඩි මුදලක් වැය කරන්න නම් සිදුවෙනවා. ඒ මුදල ඔබට වැය කරන්න හැකි නම්, ඔබට මිල දී ගන්න පුළුවන් උසස් මට්ටමේ wireless headphone කිහිපයක් පිළිබඳව යි මේ සටහන.

Bose සමාගම තමන්ගේ සමාගම් සන්නාම නාමය ගොඩනඟා ගන්නෙම noise-canceling headphones මත කිව්වොත් නිවැරදි යි. Bose සමග තරග වදින Sony සමාගම ඇතුළු headphones නිෂ්පාදනය කරන අනෙක් සමාගම් noise-canceling පිළිබඳව Bose සමාගම සිටින මට්ටම වෙත ළංවීමට දරන උත්සාහය අතිශය ප්‍රශංසනීය යි. නමුත්, අද වෙනතුරුත් Best overall headphones නම් බොහෝ විට ලබා දෙන්නේ Bose සමාගම බව නම් නොරහසක්. Bose Noise Cancelling Headphones 700 සහ Bose සමාගමේ QuietComfort 35 විදෙස් රටවල, නිතර ගුවන් යානා මඟින් ගමන් කරන්න හෝ උමං දුම්රිය මඟීන් අතර අතිශය ජනප්‍රිය headphone මාදිලි බවට පත්ව තිබෙනවා. අපහසුවකින් තොරව මුළු ගමන පුරාවටම පැළඳ ඉන්න හැකි මෙම මාදිලි දෙක අතුරින් Bose Noise Cancelling Headphones 700 මාදිලිය වඩාත් ආකර්ෂණීය ලෙසින් නිමවා ඇති බව යි භාවිත කරන්නන් සඳහන් කරන්නේ. ඒ වගේම සම්පුර්ණයෙන්ම නව්‍ය වූ හැඩයන්ගෙන් නිර්මාණය වී තිබෙන “Headphones 700” අනෙක් මාදිලියට වඩා තරුණයන් අතර ජනප්‍රියත්වයට පත්ව තිබෙනවා. මේ headphone එක සතුව පවතින විශිෂ්ට noise-canceling තාක්ෂණය මෙහි ජනප්‍රියත්වය වඩා වැඩි කරවන්නට එක් හේතුවක්. මෙහි තිබෙන සුවිශේෂී ගුණාංග අතරට එකවර device 2ක් connect (simultaneously) කිරීමේ හැකියාවත් සඳහන් නොකරම බැහැ.

සරල උදාහරණයකින් පැහැදිලි කරනවා නම්, හිතන්න ඔබ laptop පරිගණකය හා දුරකතනය සමග වැඩ කරමින් ඉන්නවා කියලා ඔබට හැකියාව තිබෙනවා. පරිගණකය ඔස්සේ යම් දෙයකට සවන් දෙන අතරේ ඔබේ headphone එකේ සම්බන්දතාවය පරිගණකයෙන් දුරකතනයට මාරු නොකර, එක්වරම ජංගම දුරකතනයට පැමිණෙන call එකක් answer කරන්නත් ඔබට පුළුවන්.

මීට අමතරව මෙහි තිබෙන Noise Cancelling level ඔබට කැමති පරිදි වෙනස් කරගන්නට ඔබට හැකියාව තිබෙනවා. සාමාන්‍ය භාවිතයන් හි දී පැය 20ක පමණ බැටරි ආයු කාලයක් රඳවාගන්න Bose Noise Cancelling Headphones (NCH700s) එකට පුළුවන්. සාමාන්‍යයෙන් රැහැන් රහිත Headphoneවල voice call quality එක තරමක් අඩු වීම සුලබ ව සිදුවන දෙයක්. නමුත්, bose සමාගමේ නිෂ්පාදකයින් NCH700s නිර්මාණයේ දී මේ පිළිබඳව වැඩි අවධානයක් යොමු කර තිබෙනවා. මෙහි මිල වෙන්නේ ඇමරිකානු ඩොලර් 399 වගේ මුදලක්.

Wireless Headphone එකක් තුළින් Sound Quality උපරිමයෙන් බලාපොරොත්තු වෙන කෙනෙක් නම්, මේ උපාංගය ඔබ වෙනුවෙන්ම යි. Sennheiser සමාගම කියන්නේ ශබ්ද පාලනය සහ ඒ හා සම්බන්ධ උපාංග නිෂ්පාදනය වෙනුවෙන් විශිෂ්ටතම නාමයක් හිමි කරගෙන සිටින සමාගමක්. ඔවුන්ගේ නිෂ්පාදනයක් ලෙසින් එළිදැක්වෙන Momentum 3 කියන්නේ Sound Quality එක අතින් උපරිම තලයේ තියන්න පුළුවන් Headphone එකක් කිව්වොත් නිවැරදි යි. Sennheiser සමාගමේ තුන්වන පරම්පරාවේ (third-gen) Momentum headphone කියන්නේ කනට කිසිදු අපහසුවකින් තොරව පැළඳ ඉන්න පුළුවන් leather ear pads දෙකක් සහිත උපාංගයක්. ඒ වගේම Sennheiser සමාගමේ අනන්‍යතාව බවට පත් වෙන සුපැහැදිලි, ගැඹුරු Sound Quality එකක් පවතින Momentum headphone එක දිගහැරිය විට ඉබේම බල ගැන්වීමට නිර්මාණය කර තිබෙනවා. මේ headphone එක සම්බන්ධ කර video නරඹන විට audio delay එකක් සිදුනොවන මට්ටමට මෙය නිර්මාණය කර තිබෙනවා. ඊට අමතරව SBC, AAC, AptX වැනි ඉතාම හොඳ codecs පරාසයක් වෙත මෙය සහාය දැක්වීම තවත් සුවිශේෂිත්වයක්. ඉහත සඳහන් කළ Bose headphone එක තරම් නොවුණත්, ඉතාම හොඳ noise cancellation, voice calls quality එකක් මෙය සතු යි.

Bose සමාගම සමග කරට කර තරග වදින Sony සමාගමේ ඉතාම හොඳ Sound quality එකක් noise cancellation එකක් සහිත wireless headphone එකක් ලෙස Sony WH-1000XM3 හඳුන්වන්න පුළුවන්. Techradar.com වැනි වෙබ් අඩවි ගණනාවක ජනප්‍රියම wireless headphone එකක් ලෙස මෙය හඳුන්වා දෙනවා. පසුගිය වසරවලට සාපේක්ෂව මේ වසරේ නිකුත් වූ wireless headphone මාදිලියේ විශේෂත්වයන් ලෙස බරින් තරමක් අඩු වීම, වඩාත් කාර්යක්ෂම ලෙස touch controls භාවිත කිරීමේ හැකියාව වැනි දේවල් හඳුවන්න පුළුවන්. aptX HD සහ Sony LDAC වැනි හොඳ codecs පරාසයක් වෙත මෙය සහාය දැක්වීමත් මෙහි ගුණාංගයන් වෙත ඇතුළත් වෙනවා. ඉහත සඳහන් කළ අනෙක් Headphone තරම් නොවුණත්, ඉතාම හොඳ noise cancellation/ voice calls quality එකක් මෙය සතු වන බව තමයි දැනගන්න ලැබෙන්නේ. එකවරක් charge කළ පසු පැය 30ක පමණ බැටරි ආයු කාලයක් රඳවාගන්න මෙයට හැකියාව තිබෙනවා. මීට අමතරව ඉතාම ඉක්මනින් බැටරිය ආරෝපණය කරගන්න Quick Charge mode එකකුත් මෙහි ඇතුළත් වෙනවා.

ඉහත දැක්වූ උපාංගවලට අමතරව Microsoft සමාගමේ Surface Headphone එකත් ඉතාම හොඳ මට්ටමේ wireless headphone එකක් ලෙස හඳුන්වන්න පුළුවන්. ඉහත අපි සඳහන් කරපු උපාංගයන්ට වඩා මිලෙන් තරමක් අඩුවීම නිසාත්, ආකර්ෂණීය ව නිමවා තිබීම නිසාත් තරුණයන් අතර මෙය ඉතා ඉක්මනින් ප්‍රචලිත වෙන්න අරන්. මේ කාණ්ඩයට අයත් වන තවත් උපාංගයක් ලෙස Bowers & Wilkins PX7 headphone එක හඳුන්වන්න පුළුවන්. පැය 30ක පමණ බැටරි ආයු කාලයක් දරන මෙහි, sound quality එක පිළිබඳව ප්‍රසිද්ධ තාක්ෂණික දැනුම බෙදා දෙන වෙබ් අඩවි ගණනාවකින් පැසසුම් හිමිව තිබෙනවා.

මේ ලිපිය හරහා ඔබව දැනුවත් කෙරෙන්නේ $300 - $400 කාණ්ඩයට අයත් wireless headphone කිහිපයක් පිළිබඳව යි. ඉදිරියේ දී එන උත්සව සමයේ තෑගී ලෙස හෝ ඔබේ පෞද්ගලික භාවිතය වෙනුවෙන් මේවා මිල දී ගන්නවා නම්, බොහොමයක් ආයතන මෙවැනි උපාංග වෙනුවෙන් විශාල වට්ටම් දෙසැම්බරයේ ලබාදෙන බව අපි ඔබට මතක් කරන්න කැමති. මීට අමතරව මේ කාණ්ඩවලට අයත් වන වෙනත් wireless headphone ගැන ඔබ දන්නවා නම් ඒ ගැන අදහස් පහළින් comments ඔස්සේ අපට කියන්න.

සාමාන්‍යයෙන් android භාවිතා කරන අප බොහෝ දෙනෙක්, අපට අවශ්‍ය apps download කර ගන්නේ google play store හරහා යි. ඒ, වෙනත් වෙබ් අඩවිවලින් ගන්නවාට වඩා ආරක්ෂාකාරී බව අතින් වැඩි නිසාවෙනුයි. නමුත්, පසුගිය දිනෙක හඳුනාගන්නා ලද ‘the Joker’ Malware එක සමග Google සමාගම තමන්ගේ යටතේ පවතින play store එක කෙතරම් ආරක්ෂාකාරීව තබා ගන්න උත්සාහ කළත්, හානිදායක apps කෙසේ හෝ එහි ක්‍රියාත්මක වීමට මාර්ගයන් සොයාගන්නා බව නැවතත් පැහැදිලි වුණා. Aleksejs Kuprins නම් පරිගණක ආරක්ෂණ පර්යේෂකයා සිදුකළ අනාවරණයත් සමග මේ මැල්වෙයාර් එක අඩංගු වූ සහ අඩංගු විය හැකි බවට සැක කළ දුරකතන යෙදුම් 24ක් පමණ වහාම ඉවත් කරන්න google සමාගම් තීරණය කළා. google සමාගම මෙම මැල්වෙයාර් එක හඳුනාගෙන playstore වෙතින් ඉවත් කරන විටත්, අදාළ apps downloads 472,000 පසු කර තිබුණු බව වාර්තා වෙනවා. මෙමඟින් සිදුවන්නේ දුරකතන පරිශීලකයාගේ අනුදැනුමකින් තොරව විවිධ සේවාවන් register කර, ඒවා වෙත මුදල් ලබාගන්න බව හඟවමින් ඔවුන්ගෙන් මුදල් ලබාගැනීම යි (පරිශීලකයෙකු ලියාපදිංචි වීමට සිදුවන ක්‍රියාවලිය අනුකරණය කිරීමයි). ඒ වගේම මීට ඔබේ දුරකතනයට එන ගෙවීම් තහවුරු කරන sms පණිවුඩ ඔබේ අවසරයකින් තොරව හඳුනාගනිමින් පිටපත් කර ගන්නට ද හැකියාව සතු වනවා. (මේ ගැන වැඩි විස්තර අපි ඔබට මීට ඉහත දී “Play store අරක්ගත් Joker Malware” ලිපියෙන් දැනුවත් කළා.) මේ සිදුවීම මෑතක සිදුවූවක් වුණත්, මීට පෙර මෙවැනි සිදුවීම් ඉතා විශාල වශයෙන් සිදුව තිබෙනවා. Google සමාගම Play protect හඳුන්වා දෙන්නෙත් මේ නිසාවෙන්ම යි. නමුත්, එය අතිසාර්ථක උපක්‍රමයක් නොවන බව කිහිපවිටෙකම සනාත වුණා.

Google සමාගම smart ජංගම දුරකතන වෙත පැමිණෙන malware සහ Bad apps හඳුනාගැනීමට හා ඒවාට විරුද්ධව සටන් කරන්න සමාගම් කිහිපයක් සමග එකඟතාවයකට පැමිණ තිබෙනවා. මේ අතරට ESET, Lookout, සහ Zimperium සමාගම් ඇතුළත් වෙනවා. මෙය හඳුන්වන්නේ “App Defense Alliance,” නමිනුයි. මේ එක්වීමේ මූලික අරමුණ බවට පත් වෙන්නේ, අනිටු මෘදුකාංග සහිත ජංගම දුරකතන යෙදුම් පරිශීලකයන් අතර ප්‍රචලිත වීමට පෙර ඉවත් කිරීම යි. බිලියන 2.5ක් පමණ සිටින android පරිශීලකයන් වෙත android මෙහෙයුම් පද්ධතිය සහ playstore එක ආරක්‍ෂිත platform එකක් බවට පත් කිරීම ඔවුන්ගේ ප්‍රධාන මෙහෙයුම බවට පත්ව තිබෙනවා.

Google Play Protect හා සමගාමීව app defense alliance එක ක්‍රියාත්මක වෙන බවට google සමාගම නිවේදනයක් නිකුත් කර තිබුණා. ඒ ඔස්සේ cloud based සේවාවක් ලෙසින් ක්‍රියා කරන Play Protect එක වඩාත් ආරක්ෂාකාරී තත්ත්වයකට පත් කරන්න හැකි වේවියැ යි ඔවුන් විශ්වාස කරනවා. කොහොම වුණත්, මේ සන්ධානගත වීමට පසුගිය මාස කිහිපයේ ව්‍යාප්ත වූ xHelper ඇතුළු මැල්වෙයාර් ප්‍රධාන හේතුවක් බව නම් නොරහසක්.

‘the Joker’ Malware එකෙන් අනතුරුව ඉතාම වේගයෙන් පැතිරී ගිය Trojan වෛරසයක් ලෙස xHelper හඳුන්වන්න පුළුවන්. එය ප්‍රධාන වශයෙන් ඉලක්ක කරගෙන තිබුණේ ඉන්දියාව, රුසියාව සහ ඇමරිකාව යි. තවමත් මෙහි මූලාශ්‍රයන් හෝ ආරම්භකයන් ගැන නිසි තොරතුරක් දැනගැනීමට, මේ පිළිබඳ පර්යේෂණ සිදුකරන MalwareBytes පර්යේෂක කණ්ඩායම ඇතුළු කණ්ඩායම්වලට නොහැකි වී තිබෙනවා.

මේ සන්ධානගත වීම යහපත් ලෙසින් android platform පරිශීලකයන් වෙත බලපානු ඇති බව තමයි, තාක්ෂණික ලෝකයේ බොහෝ දෙනෙක්ගේ මතය බවට පත් වන්නේ. මේ වෙද්දීත් තරමක් අනාරක්ෂිත මට්ටමක Play store පවතින බව ESET සමාගමේ ප්‍රකට ආරක්ෂක පර්යේෂකයෙක් වන Lukas Stefanko වාර්තාවක් දක්වමින් සඳහන් කර තිබුණා. පසුගිය මාසයේ පමණක් පරිශීලක දත්ත අවභාවිතා කරන හා මූල්‍යමය වංචාවන් සිදුකෙරෙන apps 172ක් පමණ හඳුනාගෙන තිබෙන බවත්, මේවා හඳුනාගෙන ඉවත් කරන විටත් Download countsවල එකතුව මිලියන 335ක් පමණ වූ බවත් ඔහු සඳහන් කර තිබුණා. ඊට අමතරව පසුගිය 2018 වසරේ “Android Security & Privacy Year in Review” එක දක්වමින් ඔවුන් සඳහන් කරන්නේ, Android ජංගම දුරකතන පරිශීලයකයන්ගෙන් 0.8ක පමණ උපාංගයන්හි PHA (Potentially Harmful Applications) අන්තර්ගත වන බව යි. ඒ අතරින් බොහෝ දෙනෙක් apps බාගත කර ගන්නේ playstore එක මඟින් බවත් ඔවුන් සඳහන් කරනවා. අදාළ apps playstore එකෙන් ඉවත් කිරීමට google සමාගම කටයුතු කළත්, ඒ වෙද්දීත් දුරකතනවල ඒවා භාව්ත කරන පරිශීලකයන් සිටින්නේ දැඩි අවදානමක බව යි Stefanko ප්‍රකාශ කරන්නේ.

තවද, මේ නව සන්ධානගත වීමත් සමග මෙවැනි සිදුවීම් සඳහා ඇති ඉඩකඩ අවම කරීමට හැකිවේයැ යි google සමාගම අපේක්ෂා කරනවා. හානිදායක app එකක් play store වෙත දැමීමෙන් අනතුරුව එය approve වී පරිශීලකයන් වෙත මුදාහැරීමට පෙර, එය නවත්වා ගැනීමට නව ‘app defense alliance’ ඔස්සේ හැකි වේවි. මේ ගැන ඔබේ අදහස් පහළින් comment කරන්න අමතක කරන්න එපා. ඒ වගේම “Phishing සහ Spamවලට එරෙහිව Google” ලිපියත් කියෙව්වට පාඩුවක් වෙන එකක් නෑ.

IGI පරිගණක ක්‍රීඩාව ලෝකය පුරා අතිශය ජනප්‍රිය වූවක්. මෙහි නවතම පරිගණක ක්‍රීඩාව 2021 දී නිකුත් වීමට නියමිත යි. මේ ක්‍රීඩාව නිර්මාණය කිරීමට ඔබටත් දායක වෙන්න පුළුවන්. මේ ඒ පිළිබඳව යි.

වේගයෙන් දියුණු වන තාක්ෂණික ලෝකය සමග ඉතාම වේගයෙන් වෙනස් වෙන නව්‍යකරණය වෙන තාක්ෂණයක් විදිහට සන්නිවේදන තාක්ෂණය හඳුන්වන්න පුළුවන්. පසුගිය දිනෙක චීනය සිදුකළ නිවේදනයකින් තාක්ෂණික ලෝකය තුළ විශාල කැළඹීමක් ඇති වුණා කිව්වොත් නිවැරදි යි. මේ වෙද්දී ලෝකය තුළ 5G තාක්ෂණය ප්‍රචලිත වෙන්න අරගෙන එතරම් කාලයක් ගිහින් නැති නමුත්, චීනය තමන් 6G තාක්ෂණය ගැන පර්යේෂණ ආරම්භ කළ බවට පසුගිය දිනෙක නිවේදනයක් නිකුත් කළා.

මේ තාක්ෂණය සැබෑවක් බවට පත් කරන්න හැකි ද? නැතිනම්, මේ තමන් අනෙක් රටවල්වලට පියවරක් ඉදිරියෙන් සිටින බව කියන්න චීනය දරන උත්සහයක් ද? මේ ගැන විස්තර ඔබ එක්ක බෙදාගන්න අපි හිතුවා.

සන්නිවේදනයේ දියුණුවත් එක්ක ඇති වන අලුත් සන්නිවේදන තාක්ෂණයන් හඳුන්වන්න අලුත් පරම්පරාවක් (Generation) කියන වචනය හඳුන්වා දුන්නේ, කලින් තියෙන තාක්ෂණයට වඩා පරම්පරාවක්ම ඉදිරියෙන් ඉන්නවා කියන දේ හැඟවීම අරමුණු කරගෙන යි. 4G තාක්ෂණය හඳුන්වාදීම සමග බොහෝ දෙනෙකුගේ මතය වුණේ මේ තාක්ෂණය සහ වේගය ප්‍රමාණවත් බව යි. කොහොම වුණත්, 5G තාක්ෂණය කරළියට ඒම සමග මේ මතය සම්පූර්ණයෙන්ම වගේ වෙනස් වුණා.

2019 අප්‍රේල් මාසයේ ලොව මුල් වරට දකුණු කොරියාවේ 5G තාක්ෂණය එරට ප්‍රධාන නගර 6න් 85%ක් පමණ ආවරණය කළා. එරට 5G බාගත කිරීමේ උපරිම වේගය තත්පරයට මෙගාබිට් 430ක් පමණ වුණා.

දකුණු ආසියාවේ මුල්වරට ශ්‍රී ලංකාව ද, 5G අත්හදා බැලීම් සහ සුළු ආවරණ කලාපයන් ලබන්නට සමත් වූ අතර 3.5-3.6GHz රේඩියෝ සංඥා පරාසය තුළ තත්පරයට ගිගාබිට් 1.4 - 1.5 පමණ ප්‍රමාණයක් ලැබිය හැකි බව මෙරට දුරකතන සමාගම් පෙන්වා දුන්නා.

1980 වර්ෂයට ආසන්න කාලයේ භාවිතා වූ analog (ප්‍රතිසම) cellular systems මේ ලෙස හැඳින්වෙනවා. මේ තාක්ෂණය එකල භාවිතා වුණේ radio telephone systems වෙනුවෙන් වන අතර, 1G කියන්නේ සම්පූර්ණයෙන්ම voice call සඳහා පමණක් ම භාවිතා වූ තාක්ෂණයක්.

1G තාක්ෂණයට වඩා, පරම්පරාවට වඩා හොඳ sound quality එකක් වගේම ආරක්ෂාව අතිනුත් ඉතාම ඉහළ වීම මේ පරම්පරාවේ විශේෂ ලක්ෂණයක්. මෙය එකල භාවිතා වූ පළමු digital cellular system එක බවට පත් වූ අතර, 2.5G යනු 2Gවලම වැඩි දියුණු කරන ලද සංස්කරණයක් ලෙස මෙය හඳුන්වනවා. මෙහි දී දත්ත හුවමාරු වේගය වේගය 144kbit/s සිට ඉහළට ගණන් ගැනෙනවා.

මේ පරම්පරාවේ දී Ip Data Networks භාවිතය සහ දත්ත හුවමාරු වේගය 384k bit/s තරම් වේගයක සිට ඉහළට පවත්වා ගන්නා පරම්පරාවක් වන අතර ම, මේ තාක්ෂණය අදටත් භාවිතයේ පවතින තාක්ෂණයක්.

4G සන්නිවේදන ජාලයක දී, තත්පරයක දී මෙගාබිට් 100ක පමණ වේගයක් දක්වා වේගයක් පවත්වා ගත හැකි වන අතර LTE සහ WiMAX යනු මේ පරම්පරාවේ කොටස් ලෙස හඳුන්වන්න පුළුවන්. වර්තමානය වන විට බහුලව භාවිතා කරන තාක්ෂණික පරම්පරාව යි මේ.

චීනයේ විද්‍යාව හා තාක්ෂණවේදය පිළිබඳව අමාත්‍යාංශය නිවේදනයක් නිකුත් කරමින් පසුගිය නොවැම්බර් 6 වෙනිදා සඳහන් කළේ, තමන් නිල වශයෙන් සන්නිවේදන තාක්ෂණයේ 6 වෙනි පරම්පරාව පිළිබඳව (6G) පරීක්ෂණ ආරම්භ කරන බව යි. මේ වෙනුවෙන් කණ්ඩායම් දෙකක් පත් කරන බව යි ඔවුන් සඳහන් කළේ. ඉන් එක කණ්ඩායමක් වෙත මේ තාක්ෂණයේ ප්‍රවර්ධනය සහ සංවර්ධනය පිළිබඳව වගකීම් පැවරෙනු ඇති. මේ කණ්ඩායම වෙත රජයේ නිලධාරීන් ඇතුළු පිරිසක් ඇතුළත් වෙන අතර අනෙක් කණ්ඩායම වෙත විශ්වවිද්‍යාල 37කින් තෝරාගත් පිරිසක්, විවිධ ව්‍යවසායකයන්, පර්යේෂණ ආයතනවල නියෝජිතයන් ඇතුළු පිරිසක් ඇතුළත් වෙනවා. ඔවුන් විසින් මෙහි තාක්ෂණික පැත්ත පිළිබඳව උපදෙස් ලබාදීම සිදුකෙරෙනු ඇති.

4G තාක්ෂණය හඳුන්වාදීම සිදුවූයේ 2009 වසරේ දී වුණත්, මේ වෙද්දීත් එම තාක්ෂණය භාවිත නොවෙන රටවල් සහ ප්‍රදේශ ඕනා තරම් තිබෙන බව අප හොඳින්ම දන්නවා. 2018 අවසාන කාර්තුවත් 2019ත් අතර හඳුන්වාදුන් 5G තාක්ෂණයට යාන්තමින් ලෝකය හුරුවෙමින් පවතින සමයක, 6G පිළිබඳව කතාබහ කිරීම ම කොයිතරම් දුරට ප්‍රායෝගික ද යන්න ගැටළුවක්. කොහොම වුණත්, ආසන්න වශයෙන් වසර 10ක කාලයක් තුළ පරම්පරාවකින් තව පරම්පරාවක් වෙත මාරු වීම සාමාන්‍යයෙන් සිදුවන්නක්. 4G තාක්ෂණයට වඩා 10 ගුණයකින් වේගවත්ව දත්ත හුවමාරු කරන්න 5G තාක්ෂණයට හැකියාව තිබෙනවා. 6 වෙනි පරම්පරාවේ වේගය ගැන අනුමානයන් ඉදිරිපත් කිරීම පමණයි, දැනට අපට සිදුකළ හැක්කේ.

පසුගිය සැප්තැම්බර් මාසයේ Huawei ප්‍රධාන විධායක නිලධාරි Ren Zhengfei ප්‍රකාශයක් නිකුත් කරමින් මේ නව පරම්පරාව ගැන තම සමාගම පර්යේෂණ ආරම්භ කරන බවත්, තවමත් ප්‍රාරම්භක අවදියේ 6G පර්යේෂණ පවතින බවත් ප්‍රකාශ කර තිබුණා. ඊට අමතරව මේ තාක්ෂණය මහජනතාව වෙත ලබාදීමට පෙර එසේ නොමැති නම්, වාණිජකරණය කිරීමට තවත් බොහෝ කලක් ගතවන බවත් දක්වා තිබුණා. කෙසේ වෙතත්, චීනයේ සහ හුවාවේ සමාගමේ මේ ප්‍රකාශයන් ඔස්සේ ඇමරිකාව ඇතුළු රටවල් පරදවා ඊළඟ පරම්පරාව වෙත යෑමට ඔවුන් දරන උත්සාහය ගැන සඳහන් කිරීම ම, තාක්ෂණික ලෝකයේ යුද්ධයකට අත වැනීමක් බව නම් කියන්නම ඕනේ.

මේ වෙද්දීත් ඇමරිකාව ඇතුළු රටවල් වෙතින් නිල වශයෙන් නොවුණත් මේ අභියෝගය තමන් බාරගන්න බවට, සහ චීනයේ මේ උත්සාහය අසාර්ථක එකක් වනු ඇති බවටත් ප්‍රකාශ නිකුත් කොට තිබෙනවා.

කිංග්ස්ටන් හි ක්වීන්ස් විශ්ව විද්‍යාලයේ පරිගණක පාසලේ මහාචාර්යවරයෙකු වන David Skillicorn ප්‍රකාශ කරන්නේ; මෙය චීනය හුදෙක් තමන්ගේ හැකියාවන් පිළිබඳව පාරම්බාන්න යොදාගත් ව්‍යාපාර සංකල්පයක් පමණක් බව යි. මෙය හුදෙක් සිහිනක් පමණක් බවත්, ඒ වෙත අවධානය යොමු කිරීමට තරම්වත් වැදගත්කමක් නොමැති බව යි ඔහු nationalpost.com වෙත අදහස් දක්වමින් සඳහන් කරන්නේ.

තොරතුරු තාක්ෂණයේ දියුණුව සහ රැහැන් රහිත තාක්ෂණයන් කරළියට පැමිණීමත් සමග මේ කිරණවලින් අහිතකර බලපෑම් හටගන්නා බවට පළ වන මතයන් හිස ඔසවන්නට පටන් ගත්තා. රූපවාහිනී සහ රේඩියෝ කිරණ, WiFi පිළිබඳව මෙන්ම මීට පෙර තිබුණු 3G වැනි කිරණවල බලපෑම ගැන ලොව පුරා කතාබහ ඇති වුණා. ඒ විතරක් නෙමෙයි, චන්ද්‍රිකා මඟින් පෘථිවියට එවන සංඥාවලින්, නිවසේ මයික්‍රෝවේව් උඳුනෙන්, රූපවාහිනිය හෝ CRT මොනිටර් ඉදිරියේ සිටීමෙනුත් කිරණ බලපෑම් ඇති වන බවට කටකතා සහ භීතිකාවන් පැතිරෙනවා. මෙය ඉතාම දුරදිග යන්නට පටන් ගන්නේ විද්‍යුත්-චුම්බක අධිසංවේදීතාව (Electromagnetic hypersensitivity) නමින් මනඃකල්පිත රෝග තත්ත්වයක් ද කරළියට පැමිණීමත් සමග යි. මේ ගැන වැඩි විස්තර “5G විකිරණ ශරීරයට අහිතකර ද?” ලිපියෙන් ඔබට දැනගන්න පුළුවන්. පසුගිය දිනෙක චීනය සිදුකළ නිවේදනයෙන් පසුව ආයෙත් මෙම භිතිකාවන් ගැන කතාබහ ආරම්භ වෙලා තියෙනවා. කොහොම වුණත්, දැන් චීනයට ඔවුන්ගේ ප්‍රකාශය සැබෑවක් කරන්නට වසර 10ක කාලයක් ලැබෙනවා. අපි බලමු කුමන රට ද මුලින්ම 6 වෙනි පරම්පරාවේ තාක්ෂණයේ පෙරමුණ ගන්නෙ කියලා.

චිත්‍ර සහ කතන්දර හරහා සුවහසක් දරුවන්ගේ ආදරය දිනාගත් ආදරණීය අත්තම්මා; සිබිල් වෙත්තසිංහ මැතිනිය පසුගිය 31 වනදා සිය 92 වන උපන්දිනය සැමරුවා. මේ ඇය ගැන සැකවින්.

සාමාන්‍යයෙන් භාණ්ඩයක් මිලට ගන්න ගියහම අඩුම මිල තියෙන තැනින් භාණ්ඩය මිලට ගන්න එක අපි කවුරුත් කරන දෙයක්. අන්තර්ජාලයෙන් බඩු මිල දී ගැනීමෙ දීත් මේ කාරණාව මේ විදිහටම සිදුවෙනවා. වෙබ් පිටු සිය ගණනක් පීරමින් අඩුම මිල තියෙන ඔන්ලයින් වෙළඳ සාප්පු අතර සැරිසරන එක දැන් trend එකක් බවට පත් වෙලා හමාරයි. මේ කියන්න යන්නේ එළඹෙන නිවාඩු සමයට අඩුම මිලට බඩු ගන්න ඔබට ලැබෙන අවස්ථාවන් ගැන යි.

කළු සිකුරාදා එහෙම නැති නම්, බ්ලැක් ෆ්‍රයිඩේ කියන්නේ ලංකාවට තරමක් ආධුනික සංකල්පයක්. මෙහි ආරම්භය සිදුවෙන්නේ 1952 දී පමණ ඇමෙරිකා එක්සත් ජනපදයේ දී යි. මෙය සෑම විටම යෙදෙන්නේ තෑන්ක්ස්ගිවින් ඩේ (Thanksgiving) එකට පසුව එන සිකුරාදා දිනයේ දී යි. තෑන්ක්ස්ගිවින් ඩේ එක සැමරීමේ අරමුණ වෙන්නේ ගොවියන් තමන්ගේ අස්වැන්න නෙලා ගැනීමේ සතුට සැමරීම යි. මෙය සෑම වසරකම නොවැම්බර් 4 වන සතියේ බ්‍රහස්පතින්දා දිනයේ සමරනු ලබනවා. ඊට පසුව එළඹෙන සිකුරාදා දිනය බ්ලැක් ෆ්‍රයිඩේ නමින් නම් වෙනවා. තෑන්ක්ස්ගිවින් ඩේ එක ඇමරිකානු නිල නිවාඩු දිනයක් වුවත්, මේ කළු සිකුරාදාව එලෙස ගණන් ගැනෙන්නේ නැහැ. නමුත්, එරට ප්‍රාන්ත කිහිපයක රජයන් එම ප්‍රාන්තවල නිවාඩු දිනයක් ලෙස මෙදින නම් කර තිබෙනවා. කළු සිකුරාදා හෙවත් බ්ලැක් ෆ්‍රයිඩේ කියලා මේ දවසට නම වැටුණේ ඇමෙරිකා එක්සත් ජනපදයේ ෆිලඩෙල්ෆියා ප්‍රාන්තයේ මේ දිනයට මාර්ග තදබදය, ඝෝෂාකාරී බව, මෝටර් රථ නැවත්වීමට ඉඩකඩ නොමැති වීම, මාර්ග අනතුරු, බැණ වැදීම්, හා එකිනෙකා රණ්ඩු කරගැනීම ඉතා ඉහළ ප්‍රමාණයක් වාර්තා වෙන නිසා යි.

මෙදිනට බොහොමයක් Online වෙළඳ සාප්පුවලිනුත් ඉතා ඉහළ වට්ටම් ලබාදීම සිදුවෙනවා. එනිසා එදාට ඔබ සාමාන්‍යයෙන් online shopping කරන වෙබ් අඩවිවලට පිවිසුණොත් ඉතාම ආකර්ශනීය වට්ටම් ලබා ගන්නට ඔබට හැකියාව තිබෙනවා. විශේෂයෙන්ම Ebay, aliexpress, amazon වගේ වෙබ් අඩවිවල කළු සිකුරාදා කියන්නේ විශාල වශයෙන් භාණ්ඩ අලෙවි වන දවසක්. ඔබත් ඔන්ලයින් සාප්පු සවාරි යන්න කැමති කෙනෙක් නම් එදා හොඳම දවසක්. මෙවර කළු සිකුරාදා යෙදෙන්නේ නොවැම්බර් 29 වෙනිදා යි. මේ ගැන වැඩි විස්තර “කළු සිකුරාදා’ හෙවත් ‘බ්ලැක් ෆ්‍රයිඩේ’ කියන්නේ ඇත්තට ම මොකක් ද?” යන ලිපියෙන් ඔබට කියවන්න පුළුවන්.

මිනිසුන්ව online shopping කිරිමට පෙළඹවීම අරමුණු කරගෙන (වාණිජමය පරමාර්ථ) වෙළඳ සමාගම් නිර්මාණය කළ නිවාඩු දවසක් ලෙස මේ දිනය ප්‍රකට යි. Thanksgiving දවසට දින 4කට පසු ව එන සඳුදා දිනයේ මෙය යෙදෙනවා. බොහෝ විට නොවැම්බර් මස අවසාන දින කිහිපය තුළ Cyber Monday යෙදුණත්, කලාතුරකින් මෙය දෙසැම්බර් මස මුල් සතියේ යෙදෙන අවස්ථා ද තිබෙනවා. මෙවර මේ සයිබර් සඳුදා දිනය යෙදෙන්නේ දෙසැම්බර් දෙවනිදා යි. Cyber Monday යන යෙදුම ඇලන් ඩේවිස් (Ellen Davis) සහ ස්කොට් සිල්වර්මෙන් (Scott Silverman) යන දෙදෙනාගේ සංකල්පයන් මත භාවිතයට පැමිණ තිබෙන්නක් බව යි දැනගන්න ලැබෙන්නේ. 2005 වසරේ නොවැම්බර් මාසයේ 28 වන දින එම යෙදුම නිල වශයෙන් ප්‍රකාශයට පත් කර ඇති අතර, ඉතාම ඉක්මනින් වසරේ වැඩිපුරම Online Shopping සිදුවන දිනයක් බවට සයිබර් සඳුදාව පත් වුණා. සමස්ථයක් ලෙස ගත් විට, සාමාන්‍ය දිනෙක Online Shopping සිදුවන ප්‍රමාණයට වඩා 85%ක පමණ මට්ටමකින් විකුණුම් වැඩි කර ගැනිමටත් වෙළඳුන්ට හැකියාව ලැබෙන දිනයක් ලෙස මෙය සැලකෙනවා. මේ සංකල්පය ආසියානු රටවල් වෙත 2012 වසරේ දී පමණ හඳුන්වාදීම සිදුවෙන්නේ ඉන්දියාවෙන්. ඒ google සමාගම සමග එක්ව යි. Black Friday දවසේ වට්ටම් මඟ හැරුණු බොහෝ දෙනෙකුට මේ දිනයේ දී එළඹෙන නත්තල් සමය වෙනුවෙන් අන්තර්ජාලය ඔස්සේ 70%ක පමණ විශාල වට්ටම්/ මිල අඩු කිරිම් සමග භාණ්ඩ මිල දී ගැනීමට හැකියාව තිබෙනවා. මේ දවසත් ඔබ අමතක නොකර ඔබේ ප්‍රියතම අන්තර්ජාල වෙළඳසැල් වෙත පිවිසෙන්නම ඕනේ දවසක්. විශේෂයෙන් අන්තර්ජාලයෙන් විවිධ මෘදුකාංග මිලට ගන්න ඉන්න ඔබට මේ දවස බොහොම වටීවි.

මේ දිනයත් ලෝකයේ බොහොමයක් රටවල්වල වෙළඳාම් සරුවන දිනයක් වගේම තවත් සුවිශේෂිත්වයක් සහිත දිනයක්. ලෝකයේ තනිකඩයන්ගේ දිනය ලෙස හඳුන්වන්නේ මේ දිනය යි. ලෝකය පුරා වෙසෙන සහකාරියක්/ සහකරුවෙක් නොමැති තනිකඩයන් වෙනුවෙන් නිර්මාණය වූ මේ දිනය Guanggun Jie (GU案g古NJ IE) එහෙම නැති නම් Singles' Day ලෙස හැඳින්වෙනවා. මෙය සැමරීම චීනයෙන් පැමිණි සම්ප්‍රදායයක්. තනිකඩව විසීමේ සතුට එසේ නොමැති නම්, තමන් තනිකඩ වීමේ අභිමානය සමරන දිනයක් ලෙස මෙය සැලකෙනවා. මේ දිනය සෑම වසරකම නොවැම්බර් මාසයේ 11 වෙනි දිනයේ සමරනු ලබනවා. ඔවුන්ට අනුව අංක “1” තනිකඩ බව විදහාපාන අංකයක්. හැබැයි, මේ වෙද්දී නම් මෙය සම්පුර්ණයෙන්ම පාහේ වානිජකරණය වී අවසාන යි. චීනය ඇතුළු රටවල් බොහොමයක සුවිශාල වට්ටම් සමග භාණ්ඩ විකිණීම සිදුවෙනවා. මේ දිනයට සමගාමිව ලංකාවෙත් විවිධ සමාගම් සහ අන්තර්ජාල භාණ්ඩ විකිණුම් සේවාවන් සුවිශේෂී වට්ටම් ලබාදෙනවා. හැබැයි ඉතින් බොහෝ දෙනෙක් මේ දිනය සමරන්නේ නම් තනිකඩ වීමේ සතුට සමරන්නම නෙමෙයි. කොහොම වුණත්, අන්තර්ජාලයෙන් බඩු ගෙන්වන, මිල දී ගන්න ඔබට මේ දිනයට සමගාමීව ආකර්ශනීය වට්ටම් ලබාගන්න පුළුවන්. විශේෂයෙන් AliExpress, gearbest.com වැනි වෙබ් අඩවි වෙත පිවිසෙන්න මේ දිනයේ අමතක කරන්නම එපා.

මේ හැර විශාල වට්ටම් සමග අන්තර්ජාලයෙන් භාණ්ඩ මිල දී ගන්න පුළුවන් දවස් ගැන ඔබ දන්නවා නම්, ඒ ගැනත් අප සමග අදහස් බෙදාගන්න අමතක කරන්න එපා.

2001 වසරේ තිරගත වූ Harry Potter and the Philosopher's Stone චිත්‍රපටය ඔබට මතක ද? මේ චිත්‍රපටය වගේම, ඉන් ඇරඹුණු Harry Potter චිත්‍රපට මාලාව ලෝකය පුරා අතිශය ජනප්‍රියත්වයට පත් වුණා. මේ චිත්‍රපට මාලාවේ පළමු චිත්‍රපටයේ Hogwarts මායා පාසල වෙත සිසුන් ඇතුළත් කරගන්නා දර්ශනය ඔබට මතක ඇති. එහි දී සිසුන්ව නිවාස සඳහා වෙන් කරන Sorting Hat (සෝටින් හැට්) එක එම කාර්යය කරන්නේ ඔවුන්ගේ ගතිගුණ පරික්ෂා කිරීමෙන් පසුව යි. මේ සෝටින් හැට් එක සැබෑවටම නිර්මාණය කරන්න ලංකාවේ විශ්වවිද්‍යාල සිසුන් පිරිසකට හැකිවෙලා තියෙනවා. ඔබ අයිති වෙන නිවාසය කියන්න විතරක්ම නෙමෙයි, තවත් දේ කරන්න මේ ලංකාවේ නිර්මාණය වූ හැට් එකට පුළුවන්.

මේ අපූරු කටයුත්ත කරලා තියෙන්නේ ශ්‍රී ජයවර්ධනපුර විශ්වවිද්‍යාලයේ විද්‍යාර්ථීන් පිරිසක්. ඔවුන් සියලු දෙනාම ශ්‍රී ජයවර්ධනපුර විශ්වවිද්‍යාලයේ ව්‍යවහාරික විද්‍යාපීඨයේ සිව්වන වසරේ ඉගෙනුම ලබන සිසුන්. මේ අපූර්ව නිමැවුම බිහි වෙන්නේ ව්‍යවහාරික විද්‍යාපීඨයට අයත් RIC රොබෝ විද්‍යාගාරයේ දී යි. ඔවුන්, චිත්‍රපටයේ සෝටින් හැට් සංකල්පය භාවිතා කරමින් නිර්මාණය කරන ලද මේ උපාංගයට පුද්ගල මනස කියවීමේ හැකියාවක් නම් නැහැ. නමුත්, මේ මායාකාරී තොප්පියට වෛද්‍ය සහ විද්‍යාත්මක අරමුණු සඳහා මොළයේ ක්‍රියාකාරිත්වය විශ්ලේෂණය කරන්න හැකි තාක්ෂණයක් ඔවුන් ඇතුළත් කර තිබෙනවා. මේ අපූර්ව නිර්මාණය නිසාවෙන් 2019 සෝෂල් රොබෝටික්ස් කොන්ෆරන්ස් (International Conference on Social Robotics 2019) වෙනුවෙන් ලංකාව නියෝජනය කරන්න ඔවුන්ව තෝරාගෙන තිබෙනවා. ස්පාඤ්ඤයේ මැඩ්‍රිඩ් නුවර දී එළඹෙන නොවැම්බර් 26 වෙනිදා මේ සමුළුව සහ තරගාවලිය පැවැත්වීමට නියමිත යි.

මීට අමතරව ශ්‍රී ජයවර්ධනපුර විශ්වවිද්‍යාලයේ Invention and Venture Creation Council (IIVCC) මඟින් සංවිධානය කරන ලද Innovate Sri Lanka 2019 ප්‍රදර්ශනය පසුගිය දිනෙක බණ්ඩාරනායක සම්මන්ත්‍රණ ශාලාවේ දී පැවැත්වුවා. එහි දීත් සෝටින් හැට් එක නැරඹීමට සහ එහි ක්‍රියාකාරිත්වය දැකබලා ගැනීමට විශාල ජනකායක් එක්රැස් වුණා. විශේෂයෙන්ම, කුඩා දාරුවන් මෙහි ක්‍රියාකාරිත්වය ඔස්සේ තමන් අයිති මායා පාසලේ කුමන නිවාසයටදැ යි දැනගන්නට උත්සුක වුණා.

Artificial Intelligence (AI- කෘතීම බුද්ධිය), Machine Learning වගේම අධිබලැති පරිගණක පද්ධතිවල සිදුවන පෙරළිකාර වෙනස්වීම් සහ යාවත්කාලීන වීම් සමග Social Robotics වෙත ප්‍රධාන කාර්යභාරයක් පැවරෙනවා. ඒ, ඉහත තාක්ෂණයන් සියල්ල එකතු කර ගනිමින්, මානව හිතකාමී රොබෝ යන්ත්‍ර නිර්මාණය කරමින් මිනිසුන්ගේ වැඩ කටයුතු පහසු කිරීම යි. සමාජ රොබෝ විද්‍යාව පිළිබඳ අන්තර්ජාතික සමුළුව කියන්නෙ; එවැනි නව සොයාගැනීම්, පර්යේෂණ ක්ෂේත්‍රයන්හි වර්ධනයන් පිළිබඳව ලෝකය වෙත ගෙන හැර පාන සමුළුවක්. ඊට අමතරව හොඳම මානව හිතකාමී රොබෝ යන්ත්‍ර සහ සංකල්ප නිර්මාණකරුවන් වෙත ඇගයුම් ලබාදෙන, වාර්ෂිකව පවත්වනු ලබන සුවිශේෂී සම්මන්ත්‍රණයක් ලෙසත් මෙය සලකන්න පුළුවන්.

ලෝකයේ ඉහළම පෙළේ විශ්වවිද්‍යාල රාශියක් තරග වදින “Best Robot Design Award” තරගාවලියේ අවසන් තරගකරුවන් අතරට පැමිණෙන්නට, ශ්‍රී ජයවර්ධනපුර විශ්වවිද්‍යාලයේ මේ විද්‍යාර්ථීන් හට හැකියාව ලැබී තිබෙනවා. මේ වෙත ලංකාව නියෝජනය කරමින් පිටත් වෙන කණ්ඩායමට අධීෂ ගම්මන්පිළ, අසේල විජේසිංහ, ටෙහානි වන්නිආරච්චි, දෝවිනි ජයසිංහ, විරාජි අමරජීව සහ ආචාර්ය රවින්ද්‍ර දී සිල්වා ජ්‍යෙෂ්ඨ කථීකාචාර්යතුමත් ඇතුළත් වෙනවා.

මේ නිර්මාණය සිදුකිරීමට ඔවුන්ට සහාය ලබාදුන් RIC රොබෝ විද්‍යාගාරයේ අධ්‍යක්ෂක, ආචාර්ය රවින්ද්‍ර දී සිල්වා ජ්‍යෙෂ්ඨ කථීකාචාර්යතුමා, විද්‍යාගාරයේ පර්යේෂණ සහකාර උදක මානවඩු මහතාට, විශ්වවිද්‍යාලයේ උපකුලපති මහාචාර්ය සම්පත් අමරතුංග, ව්‍යවහාරික විද්‍යාපීඨයේ පීඨාධිපති මහාචාර්ය ලලිත් කරුණානායක වගේම පරිගණක අධ්‍යනාංශයේ අංශාධිපති ආචාර්ය ආනන්ද ගාමිණි මහතා ඇතුළු සියලුම ගුරුවරුන්ටත්, ඔවුන්ට සහාය ලබාදුන් සියලු මිතුරු මිතුරියන්ටත් ස්තුතිවන්ත විය යුතු බව යි ඔවුන් අප සමග ප්‍රකාශ කළේ. 2019 සෝෂල් රොබෝටික්ස් කොන්ෆරන්ස් හි දී ලංකාවට කීර්තියක් අත්කර දෙන්නට හැකි වේවා යි Roar සිංහල අපි සුභ පතනවා.

ඔබ Potterhead කෙනෙක් විදිහට කැමතිම නිවාසය මොකද්ද? ඒ ගැන අපට කියන්න පහළ comment section එක භාවිතා කරන්න අමතක කරන්න එපා. ඊට අමතරව Harry Potter කතා මාලාවේ තිබෙන මන්තර වර්ග ගැන ලියූ ලිපිය සහ ගින්නෙන් උපන් ෆීනික්ස් ගැන ලියූ ලිපියත් කියවන්න අප ඔබට ආරාධනා කරනවා.

Smartphone අද වෙද්දී ඉතාම වේගයෙන් නූතන තාක්ෂණය සමග දියුණු වෙමින් පවතිනවා. විවිධ සමාගම් විවිධාකාරයෙන් ඔවුන්ගේ දුරකතන ආකර්ෂණීය මෙන්ම නවමු එළඹුමකින් නිමවන්නට පෙළඹෙන්නේ පාරිභෝගික ඉල්ලීම්, අපේක්ෂාවන් සහ ඔවුන්ගේ අවශ්‍යතාවයන් හඳුනාගනිමිනුයි. Foldable දුරකතන නිර්මාණය වෙන්නෙත් මෙවන් හේතු සාධක පදනම් කරගෙන යි. Tab එක සහ දුරකතනය යන උපාංග දෙකක් වෙනුවට, කාර්යයන් දෙකම ඉටුවන පරිදි එක් උපාංගයක් නිර්මාණය කිරීම මෙහි අරමුණ යි. 2019, Foldable වර්ෂය ලෙස හැඳින්වීමට හැකි වෙන්නෙත් සමාගම් රාශියකින්ම ෆෝල්ඩබල් තාක්ෂණික සංකල්පය යටතේ ජංගම දුරකතන නිර්මාණය කළ නිසා යි. Royole Flexpai උපාංගයේ සිට Samsung Galaxy Foldable, Huawei Huawei Mate X, Motorola Razr v4, TCL foldable Phone වගේ ජංගම දුරකතන මාදිලි ගණනාවක් පිළිබඳ මේ වසර තුළ දී කතා බහට ලක් වුණා.

වෙළඳපොළ වෙත නිකුත් වෙන Foldable දුරකතනයන්ගේ durability එක පිළිබඳව පවතින්නේ මතභේදාත්මක වාතාවරණයක්. ඊට ප්‍රමුඛතම හේතුව බවට පත් වෙන්නේ, මිලෙන් තරමක් වැඩි Samsung Galaxy Foldable දුරකතනය යි. පරික්ෂා කිරීමේ අරමුණැතිව දුරකතන ලබාදුන් social media influencersලාගෙන් එයට එතරම් යහපත් ප්‍රතිචාරයක් ලැබුණේ නම් නැහැ. භාවිතයට ගැනීමෙන් අනතුරුව දිනකින් හෝ දෙකකින් දුරකතනයේ විවිධ හානී වීම් සහ ගැටළුකාරී තත්ත්වයන් මතු වීම දැකගන්න ලැබීම මීට හේතුව යි. Review කරන්නන් අතරින් බොහෝ දෙනෙකු, Samsung සමාගම විසින් එම device එක සබැඳිව සඳහන් කර තිබූ සටහනක් කියවා නොමැති හෙයින් මෙකී අකරතැබ්බයට මුහුණපෑමට වූ බව පසුව අනාවරණය වුණා.

Galaxy Fold device එකේ Screen එක මත තිබෙන තුනී screen protector එකක් වැනි plastic layer එක ඉවත් කිරීම නිසාවෙන් මෙම තත්ත්වය උද්ගත වූ බව වාර්තා වන අතර, මෙය ඉවත් නොකරන ලෙස Samsung සමාගම විසින් අවධාරණය කොට තිබෙනවා. නමුත්, සාමාන්‍යයෙන් අලුතින් ජංගම දුරකතනයක් මිල දී ගත් විට දකින්නට ලැබෙන screen protection එක සඳහා අලවා තිබෙන පොලිතින් layer එකක් වැනි පෙනුමක් මීට ඇතුළත් හෙයින්, නිතැතින්ම එය ඉවත් කිරීමට පරිශීලකයා පෙළඹෙන බව මොවුන් පෙන්වා දෙනවා. ඉහත සිදුවීම් මාලාවෙන් අනතුරුව 2019 අප්‍රේල් මාසයේ නිකුත් කිරීමට නියමිතව තිබූ Galaxy Fold device එක, වෙළඳපොල වෙත නිකුත් කිරීම නැවත වරක් කල් දමන්නට සමාගමට සිදුවුණා.

ඉන්පසුව, Galaxy Fold device දුරකතනය යළිත් වෙළඳපොල වෙත නිකුත් කරන බව පසුගිය දිනෙක samsung සමාගම නිවේදනය කළා. අකුළා තිබෙන විට අඟල් 4.6ක් වන ජංගම දුරකතනයක් ද, දිගහැරිය විට අඟල් 7.3ක tablet එකක් ලෙස ද භාවිතා කළ හැකි මෙම දුරකතනය, 12GB RAM එකකින් සහ 512GB Internal Storage එකකින් සමන්විත වනවා. එපමණක් නොවේ, පසුපස camera 3ක් මෙන්ම cover එක මත කැමරාවක් සහ ඉදිරිපස කැමරා 2ක් වශයෙන් camera 6කින් මෙය සමන්විත යි. Samsung Unpacked 2019 Event හි දී Galaxy Fold device නැවත වෙළඳපොල වෙත පැමිණීම නිවේදනය කෙරුණා. කෙසේවෙතත්, මෙසේ වැඩිදියුණු කරන ලද උපාංගය භාවිතයේ දී අතිශය ප්‍රවේසම් විය යුතු බව සමාගම සඳහන් කර තිබුණා. Foldable දුරකතන තිරය පීඩනයට ඔරොත්තු නොදෙන බවත්, Galaxy Fold දුරකතනය දෙකට හැකිලීමේ දී තිර දෙක අතර කුණු දූවිලි අංශු එක්රැස් නොවන නමුත්, දෙපස තිර දෙකෙහි ඇති චුම්බක වෙත වෛද්‍ය උපකරණ, Credit Card, යතුරු වැනි උපකරණවලින් බාධා එල්ල විය හැකි බවත් එම නිවේදනයේ වැඩිදුරටත් සඳහන් වෙනවා.

මෙය තවමත් වෙළඳපොල වෙත නිකුත් කිරීමට එතරම් සුදුසු නැති බව ජනප්‍රිය YouTube චැනලයක් වන JerryRigEverything වෙතින් පසුගිය දිනෙක පෙන්වා දුන්නා.

මේ හේතුවෙන් Fold device, Foldable Phones වෙත යම් ආකාරයක කළු පැල්ලමක් එක් වූ බව කිව යුතු යි. මේ අලකලංචි අතරමැද Motorola සමාගම ඔවුන්ගේ නවතම දුරකතනය එළිදැක්වීමට සුදානම් වෙනවා. මෙය ඔවුන්ගේ වැඩිම විකුණුම් ප්‍රමාණයක් සිදු වූ Motorola RAZR දුරකතනයේ 2019 සංස්කරණය ලෙස යි ඔවුන් හඳුන්වන්නේ. මේ වසර අවසානයට පෙර නිකුත් වීමට නියමිත මෙකී RAZR දුරකතනයේ leaked images මේ වෙද්දීත් අන්තර්ජාලය පුරා සැරිසරන්නට පටන්ගෙන. මෙය Qualcomm Snapdragon 710 Chipset එකකින් සහ 2730mAh බැටරියක් මඟින් බල ගැන්වෙනු ඇති අතර, මිල ඇමෙරිකානු ඩොලර් 1,500ක් පමණ වන බවට අනුමාන කෙරෙනවා. මේ පිළිබඳව හටගත් කතාබහ තව තවත් උත්සන්න වෙන්නේ Lew Later youtube නාලිකාවේ පසුගිය දිනෙක පළ වූ වීඩියෝවක් සමග යි. කොහොම වුණත්, Foldable Phone වෙනුවෙන් බලා සිටින රසිකයින් නම් නවතම තොරතුරු නිසා අමන්දානන්දයට පත්ව තිබෙන බව අපට දැකගන්න පුළුවන්. theverge.com වෙබ් අඩවියේ මේ හා සම්බන්ධ තවත් leaked images ගණනාවක් පළ කර තිබුණා.

Facebook සමාගම සතුව පවතින ප්‍රධානතම messaging platform අතර WhatsApp ප්‍රධාන තැනක් ගන්නවා. ලෝකයේ බොහෝ රටවල මෙන්ම ලංකාවේත් ප්‍රධානතම පණිවිඩ හුවමාරු කරගන්නා ක්‍රමයක් ලෙස මෙය භාවිත වෙනවා. WhatsApp හරහා පැමිණි ඔබේ දත්ත සොරකම් කිරීමට හැකි බවට සැලකෙන වයිරස කාණ්ඩයේ අනිසි මෘදුකාංගයක් ගැන හෙළිදරව් වීමත් සමග බොහෝදෙනෙක් ඒ පිළිබඳව කතාබහ කරන්නට පටන් ගත්තා. අපි ඒ පිළිබඳව ඔබට පෙර ලියු “WhatsApp හරහා ඔබේ දුරකතනය හැක් වෙයි ද?” යන ලිපිය ඔස්සේ තොරතුරු ගෙන ආවා.

NSO Group නම් ඊශ්‍රායල සමාගමක් විසින් නිර්මාණය කරන ලද බව සැලකෙන Spyware එක හරහා ඔබේ දුරකතනයේ camera, microphone, emails, සහ messages වගේම, location වැනි තොරතුරු වෙත අනිසි ලෙස ප්‍රවේශ වීමට සහ භාවිත කිරීමට හැකියාව ලැබෙනවා. ඒ ඔස්සේ ඔබව අනිසි ලෙස නිරීක්ෂණය කරන්න (surveillance) ඔවුන්ට හැකියාව ලැබෙනවා. WhatsApp ඇමතුම් ලබාගැනීමට භාවිතා කරන protocol එක වන VOIP stack එක හරහා remote code execution (දුරස්ථව අවශ්‍ය code එකක් execute කිරීමේ හැකියාව) කිරීමේ හැකියාව තිබී ඇති අතර, එම ආරක්ෂණ දුර්වලතාවය භාවිත කරමින් hacking ප්‍රහාරය එල්ල කර තිබෙනවා. එංගලන්ත මානව හිමිකම් නීතිඥයෙකු තමාට පසුගිය මාසයේ ලැබුණු සැක සහිත WhatsApp ඇමතුම් ගණනාවක් නිසාවෙන් මේ පිළිබඳව Citizen Lab ආයතනය වෙත දැනුම් දී තිබෙනවා. ඒ සම්බන්ධව ඔවුන් සිදුකරන ලද පර්යේෂණයකින් අනතුරුව මේ සිදුවීම පිටුපස NSO Group නම් ඊශ්‍රායල සමාගම සිටින බවට සාක්ෂ්‍ය හමුව තිබුණා.

WhatsApp මිල දී ගැනීමට Facebook ආයතනය වෙත ඇමරිකානු ඩොලර් බිලියන 19.3ට ආසන්න මුදලක් වැය වී ඇති බව. එය facebook සමාගමේ විශාලතම මිල දී ගැනීම බවටත් පත්ව තිබෙනවා. නමුත්, ඔවුන් අපේක්ෂා කළ අන්දමේ ලාභයක් ලබා ගැනීමට නම් ඔවුන් අපොහොසත් වෙලා තිබෙනවා.

පසුව ආරක්ෂණ දුර්වලතාව වෙත ඉතා ඉක්මනින් පිළියම් යොදන්නට Facebook සමාගම කටයුතු සංවිධානය කළා. (facebook සමාගම සතුව whatsapp පවතින බව ඔබ දන්නවා ඇති නෙහ්.) ඒ whatsapp හි නව සංස්කරණයක් වූ WhatsApp- v2.18.15 ලබාදීමත් සමග යි.

the NSO Group නම් ආයතනය වෙත Facebook සමාගම වෙතින් නඩු පවරා තිබෙනවා. මෙහි ප්‍රධාන චෝදනාව ලෙස ඔවුන් ගොනු කර තිබෙන්නේ; උපාංග 1,400කට අධික ප්‍රමාණයක් වෙත අනිෂ්ට මෘදුකාංග ඇතුල් කිරීම සම්බන්ධව යි. ලොව වටා සිටින මානව හිමිකම් ආරක්ෂා කරන්නන්, මාධ්‍යවේදීන් ඇතුළු විශේෂිත පිරිසක් ඉලක්ක කරගෙන මෙම මැල්වෙයාර් එක ඔස්සේ තොරතුරු එක්රැස් කොට ඇති බව Washington Post හි ලිපියකට Whatsapp ප්‍රධානි Will Cathcart ප්‍රකාශ කර තිබුණා.

මේ ඊශ්‍රායාලීය සමාගම වෙත මීට පෙරත් කිහිපවිටෙක කුප්‍රකට චෝදනා එල්ල වී තිබුණා. ඒ රජය වෙත සාමාන්‍ය පුරවැසියන්ගේ තොරතුරු අනිසි ලෙස ලබාගත හැකි අන්දමේ විවිධ මෘදුකාංග ලබාදීම සහ රජය වෙත අනිසි ලෙස පුද්ගලයන් නිරීක්ෂණය කිරීමට විවිධ ක්‍රමවේදයන් සලසා දීම පිළිබඳව යි. මීට අමතරව පසුගිය වසරේ දී ‘ජමාල් කෂෝගි’ නම් මාධ්‍යවේදියෙකු සෞදි අරාබියේ ඉස්තාන්බුල්හි දී වධහිංසාවට ලක් කර ඝාතනය කළ සිදුවීම ඔබට මතක ඇති. මේ මාධ්‍යවේදියාගේ දුරකථනය තුළත් අදාළ මැල්වෙයාර් එක ස්තාපිතව තිබූ බව gizmodo.com වාර්තාවක් එක කරමින් සඳහන් කර තිබුණා.

ජමාල් පිළිබඳව වැඩි විස්තර “2018 වසරේ මිනිසා”- සත්‍ය වෙනුවෙන් සටන් කරන මාධ්‍යවේදීන්” යන ලිපිය තුළින් ඔබට කියවන්නට හැකියි.

මේ ආයතනය Google Ads සහ විවිධ රූපවාහිනී හා සමාජ මාලා සම්මුඛ සාකච්චා සිදුකරමින්, තමන්ගේ නමට වැටුණු කළු කැළැල වසා ගන්නට අසාර්ථක උත්සාහයක යෙදමින් සිටින බව vice.com වෙබ් අඩවියේ Tech segment එක වූ Motherboard වෙබ් අඩවිය සඳහන් කරනවා.

whatsapp ඇතුළු සියලුම සන්නිවේදන මෘදුකාංග නිර්මාණය කරන ආයතන වෙත, ලෝකය පුරා විවිධ රජයන්ගෙන් අදාළ මෘදුකාංග වෙත Backdoor එකක් එහෙම නැති නම් රජය වෙත පරිශීලක පණිවිඩ වැනි දෑ minitor කළ හැකි ක්‍රමවේදයක් ඇතුල් කරන මෙන් බලපෑම් එල්ල වීම සුලභව සිදුවන්නක්. උදාහරණ ලෙස; පසුගිය මාස කිහිපයකට පෙර Whatsapp message, traceable කරන ලෙස (යැවූ පුද්ගලයා සොයාගත හැකි වන ලෙස) ක්‍රමවේදයක් සකස් කරන මෙන් ඉන්දීය රජය ඉල්ලීමක් සිදුකර තිබුණා. එපමණක් නොවේ, ජර්මනියේ දීත්, ඇමරිකාව දෙසිනුත් මෙවැනි සිදුවීම් වාර්තා වුණා.

ඔබ Cyborgsවරුන් ගැන අහලා තියෙනවා ද? ඔබ චිත්‍රපට විද්‍යා ප්‍රබන්ධ වැනි දේට ආස කරන නරඹන පුද්ගලයෙක් නම් මේ සංකල්පය එතරම් ඔබට නුහුරු නොවෙන්න පුළුවන්. හිතන්න මොළයෙන් විධානයක් ලබා දී විවිධ උපාංග වැනි දෑ ක්‍රියාත්මක කරවන්න ඔබට හැකි වුණොත් කොහොමද? මේ තාක්ෂණය තවදුරටත් විද්‍යා ප්‍රබන්ධවලට සීමා වෙන්නේ නැහැ.

Tesla සමාගමේ නිර්මාතෘ වන Elon Muskගේ නවතම තාක්ෂණික ව්‍යාපෘතිය ලෙස ඔහු ආරම්භ කළ Neuralink ආයතනය, පරිගණකය සහ මිනිසා අතර සම්බන්ධතාවන් ගොඩනගන්නට නවමු පියවරක් තබන්නට පසුගිය දිනෙක සමත් වුණා. කෙළින්ම Cyborgවරු නොවුණත්, එම සංකල්පය පාදක කරගෙන තමයි මේ නව පියවර ගොඩනැගෙන්නේ. Brain Machine Interfaces (BMI)/ Brain computer Interface (BCI) එහෙම නැති නම්, පරිගණකය සහ මිනිසා අතරට අතුරු මුහුණතක් එක් කරමින් සම්බන්ධතාවයන් ගොඩනැගීම මේ සංකල්පයේ මුලික පදනම බවට පත්වෙනවා. මෙහි දී සිදුවන්නේ; electrodes (ඉලෙක්ට්‍රොඩ) භාවිතයෙන් මිනිස් මොළයේ ස්නායු ලබාදෙන විවිධ සංවේදනයන් විදානයන් බවට පරිවර්තනය කරමින් බාහිර උපකරණය හෝ උපාංගය ක්‍රියාත්මක කර වීම යි. මෙලෙසින් පාලනය කිරීමට හැකි උපාංග ලෙස පරිගණක හෝ රොබෝ අත් වැනි දෑ සලකන්න පුළුවන්. එවැනි සංකීර්ණ කාර්යයන් වෙත යොමු වීම කාලය ගත වන කටයුත්තක් බැවින්, 2020 දී ඔවුන් ඒ වෙනුවෙන් මිනිසුන් යොදාගෙන පර්යේෂණ සිදුකරන්න බලාපොරොත්තු වෙනවා.

මේ තාක්ෂණ සංකල්පය යම් කාලයක සිට විවිධ පර්යේෂණ සඳහා භාවිත වුණා. කොහොම වුණත්, Neuralink සමාගම BMI තාක්ෂණය (Brain Machine Interfaces) තවත් පියවරක් ඉදිරියට ගෙන යන්නට සමත් වුණා. මේ BMI devices ස්නායු ආබාධ සහිත පුද්ගලයන් වෙත පිහිට වීමට භාවිත වේවි. ඒ ඔස්සේ ඔවුන්ගේ රෝගවල නවතම තත්ත්වයන් සහ රෝග ලක්ෂණ ඉතාම සමීපව නිරීක්ෂණය කරන්නට වෛද්‍යවරුන් වෙත පහසුකම් සලසාවි. ඒ වගේම මේ මඟින් කෘතිමව ඔවුන් වෙත සම්බන්ධ කරන අත්-පා පාලනය කිරීමටත් ඔවුන්ට හැකි වේවි. මෙය තව දුරටත් වැඩි දියුණු කිරීම්වල දී මොළය සමග සෘජුවම සම්බන්ධ වෙමින් ක්‍රියාත්මක විය හැකි කෘත්‍රීම බුද්ධි වැඩසටහන් පවා නිර්මාණය වෙනු ඇති බව විද්වතුන්ගේ මතය යි. ඒ ඔස්සේ වඩාත් ඉක්මනින් මොළයේ ස්නායු මඟින් ලබාදෙන විධානයන් නිවැරදිවත්, කාර්යක්ෂමවත් සිදුකිරීමට හැකියාව ද ඒ ඔස්සේම ලැබේවි. මේ වන විටත් මේ හා සමාන තාක්ෂණයන් ලෝකයේ භාවිතා වෙනවා. නමුත්, මේ වෙද්දී භාවිතයේ තිබෙන උපාංග සම්බන්ධ කිරීමේ දී සහ පාලනය කිරීමේ දී මතු වන ප්‍රධාන ගැටළු රාශියක් තිබෙනවා. මේ වෙද්දී භාවිතයේ තිබෙන BMI උපාංග නිර්මාණය වෙන ප්‍රධාන අමුද්‍රව්‍ය බවට පත් වෙන්නේ සිලිකන්. සාමාන්‍ය භාවිතයේ තිබෙන BMI උපාංග සැබෑ මොළයේ පටකවලට වඩා විශාලත්වයෙන් වැඩි වීම නිසා, ඒවා මොළයේ තැන්පත් කිරීම් කොතරම් සුක්ෂමව සිදුකළත් අවට පටක වෙත හානි සිදුවීම හා ඒ ඔස්සේ ලබාගන්නා දත්ත අස්ථායි වීමට ලොකු ඉඩකඩක් තිබෙනවා. ඒ වගේම මේ උපාංග මොළය තුළ ප්‍රතිශක්තිකරණ ක්‍රියාවලි ආරම්භ කර වීම නිසා මොළය මඟින් ප්‍රතික්ෂේප වෙන්නටත් ඉඩ තිබෙනවා.

මේ වන විට භාවිතයේ පවතින BMI හෝ BCI උපාංගයන්ගේ පවතින දෝෂ සහ ගැටළු මතු නොවන ලෙස, නව උපාංග මාලාවක් නිර්මාණය කරීමට Neuralink ආයතනය සමත් ව තිබෙනවා. ඔවුන් ඒ වෙත නම යොදා තිබෙන්නේ “flexible BMI” ලෙසිනුයි. මේ නව flexible BMI උපාංග තැන්පත් කිරීම්වලට මොළයේ ප්‍රතිශක්තිකරණ පද්ධතිය එරෙහි වීම අවම කිරීමට ඔවුන් යොදාගන්නා රැහැන් ආදිය ඉතාම සියුම්ව නිර්මාණය කොට තියෙනවා. ඒ වගේම වර්තමානයේ භාවිතයේ තිබෙන උපාංගවලට වඩා කුඩා ලෙස මෙය නිර්මාණිත යි. මෙම උපාංග මොළය තුළ තැන්පත් කිරීම සිදුවෙන්නෙත් ඒ වෙනුවෙන්ම විශේෂයෙන් නිර්මාණය වූ රොබෝවරු මඟිනුයි.

මේ රොබෝවරු මොළයේ ස්නායුවලට සහ පටකවලට හානි නොවන ලෙස අදාළ උපාංග තැන්පත් කිරීම සඳහා සුවිශේෂී අන්වීක්ෂ භාවිත කරනවා. තාමත් පර්යේෂණ මට්ටමේ තිබෙන මේ flexible BMI සමග 2020 දී මිනිසුන් යොදාගෙන සායනික පර්යේෂණ සිදුකිරීමට බලාපොරොත්තු වන බව Musk සඳහන් කර සිටියා. Neuralink ආයතනය සමග ඔහු මේ සොයාගැනීම පිළිබඳව හෙළිදරව් කළේ San Francisco හි දී පැවැත්වූ උත්සවයක දී යි. මේ නව උපාංගය කන පිටුපස පළඳිනු හැකි ලෙසින් සකසා ඇති අතර, මෙහි ක්‍රියාකාරිත්වය වැනි දේ ඔබේ ජංගම දුරකතනයේ app එකක් මඟින් දැකගන්නට හැකි වෙන බව ඔහු වැඩිදුරටත් සඳහන් කළා. අනාගතයේ කිසිදු ක්‍රියාකාරකමකින් තොරව මොළයෙන් ලබාදෙන විධානයකින් විවිධ උපාංග ක්‍රියාත්මක කර වන මට්ටමට මේ තාක්ෂණය පත් වන බව යි, ඔහුගේ අදහස.

කෙසේ වෙතත්, මෙහි අයහපත් බලපෑම් තිබෙන බවට අද වෙද්දී යම් යම් මත පළ වෙමින් තිබෙනවා. මෙම උපාංග භාවිත කරන්නන්ගේ පෞද්ගලිකත්වය සම්බන්ධව ගැටළු මතු විය හැකි බව තමයි, වඩාත් ප්‍රබල මතය බවට පත් වෙන්නේ. මොළය කෙළින්ම පරිගණකය සමග සම්බන්ධ වීම සිදුවන නිසා විවිධ දත්ත කෙළින්ම මෙතුළින්ම ලබාගැනීමට අදාළ ආයතනවලට හැකි වනු ඇති බව යි, මොවුන්ගේ මතය. Neuralink ආයතනය Facebook ආයතනය සමග එකාබද්ධව තමයි මෙකී කටයුත්ත සිදුකරන්නේ. ඔබට මතක නම් Facebook ආයතනය, පරිශීලක දත්ත අවභාවිතාව ගැන කිහිපවිටෙක දී ම චෝදනා ලැබූ ආයතනයක්. මේ අපි ඒ පිළිබඳව පළ කළ ලිපියක්.

මීට අමතරව එකී උපාංග ඔස්සේ පුද්ගල මොළය පරිගණකය වෙත සම්බන්ධ කිරීම මඟින්, මොළය Hackerවරුන් වෙත විවෘත කිරීමක් ලෙසත් ඇතැමුන්ගේ මතයක් පවතිනවා. එමෙන්ම මේවා ආශ්‍රයෙන් මිනිසුන් විවිධ දේ සඳහා යොමු කිරීමත් සිදුවිය හැකි බව යි, ඔවුන්ගේ මතය.

මේ ගැන මොකද ඔබ හිතන්නේ? ඔබේ මොළයෙන් විධානයන් නිකුත් කරමින් විවිධ උපාංග ක්‍රියාත්මක කර වීම කොයි වගේ අත්දැකීමක් වේවි ද? ඒ ගැන ඔබේ අදහස් පහළින් comment කරන්න අමතක කරන්න එපා.

හිතන්න, ඔබ යන එන අතරමඟ දකින ඕනෑම බිත්තියක චිත්‍ර අඳින්න ඔබට අවස්ථාව ලැබුණොත් කොහොමට තියේවි ද? දැනටත් ඇතැම් පුද්ගලයන් එවැනි දේ සිදුකරනවා ඔබ දැකලා ඇති. සමහරක් ස්ථානවල නම් මෙවැනි දේ කිරීම නීතියෙන් තහනම්. හැබැයි ඔබට පුළුවන් වුණොත් මේ දේ අතථ්‍යව, එහෙම නැතිනම් virtually සිදුකරන්න ඒක අපූර්ව අත්දැකීමක් වේවි. ඔබේ අතේ තියෙන smart ජංගම දුරකතනය හරහා ඕනෑම බිත්තියක් ඔබේ චිත්‍ර අඳින කැන්වසයක් කරගන්න, ඒ වගේම ඔබේ ජංගම දුරකතනයේ app එකක් මඟින් එවැනි විවිධ චිත්‍ර නරඹන්න පුළුවන් වුණොත් කෙතරම් අපුරු වේවි ද? මේ අපූරු තාක්ෂණය සැබෑ වන්නට ගත වනු ඇත්තේ තවත් බොහොම සුළු කාලයක්. මේක app එකක්. ඒ වෙත නම දාල තියෙන්නේ “Mark AR” ලෙස යි.

මේ තාක්ෂණය සමග කොතරම් නම් දේ කරන්න පුළුවන් වේවි ද? සමහර විට ඉදිරියේ දී පෝස්ටර් වෙනුවට මෙවැනි app හරහා විවිධ දැන්වීම් සටහන් කිරීමත් සිදුකරන්න පුළුවන් වේවි. ඒ මඟින් පරිසර හානියත් අවම කරගන්න පුළුවන්. තව, ඔබට ඔබේ මිතුරන් සමග විවිධ ක්‍රීඩා වෙනුවෙනුත් මේ තාක්ෂණය යොදාගන්න හැකියාව තියෙනවා. උදාහරණයක් විදිහට treasure hunting වගේ ක්‍රීඩා කරන්න ඔබට නොයෙක් රහසිගත සලකුණු තබා යන්න පුළුවන්. ඔබේ මිතුරන්ට ඒවා සොයා ගනිමින් ක්‍රීඩාවේ නියැලෙන්න හැකියාව තියෙනවා.

මිනිසුන් සීගිරියේ කුරුටු ගීත ලියන්න පෙළඹුණේ, ඔවුන් ඒ තැනට පැමිණි බව සහ ඒ අවට ඔවුන් දුටු ලස්සන ගැන කියන්න. හැබැයි, අපට ඉතින් කැටපත් පවුරක් අයිති නැහැනේ. නමුත්, ඉතාම ඉක්මනින් ඔබටත් අතථ්‍ය කුරුටු ලිපි (Virtual Graffiti) ලියන්න, අඳින්න Mark AR හරහා අවස්ථාව ලැබෙනවා. මේ සියල්ල permanently ඔවුන්ගේ දත්ත ගොනු අතර තැන්පත් වෙනවා. ඔබ ගබඩා කරන නිර්මාණය සමග ඒ ස්ථානයේ පිහිටුමත් ඔවුන් ගබඩා කරගැනීම මේ Mark AR app එක හරහා සිදුවෙනවා. එහෙයින් එම ස්ථානයට පැමිණෙන ඕනෑම කෙනෙකුට app හරහා ඔබේ නිර්මාණය රසවිඳින්න සහ ඔබ ඒ ස්ථානයට පැමිණි බව දැකගන්න හැකියාව ලැබෙන බව තමයි මෙහි නිර්මාණකරුවන් කියන්නේ. මේ යෙදුම (app) ක්‍රියාත්මක වෙන්න අවශ්‍ය වෙන්නේ ඔබේ දුරකතනයේ cameraව සහ දුරකතනය AR තාක්ෂණය වෙත සහාය දැක්වීම පමණයි.

ඔබ දන්නවා ද; සියවස් 5ක් පුරාවට සීගිරියේ සුන්දරත්වය දුටු සංචාරකයන් ඒ මත විවිධ කවි, ගී ලියා ඇති බව?

මෙහි අඳුරු පැතිකඩකුත් නැතුවාම නෙමෙයි. හිතන්න, ඔබේ බිත්තියක හෝ ඔබට අයිති ස්ථානයක ඔබට හෝ වෙන අයෙකුට අපහාස වන අයුරින් Virtual Graffiti නිර්මාණය කිරීමේ හැකියාව මේ app එක ස්ථාපනය කර ඇති ඕනෑම අයෙකුට තියෙනවා. තවත් උදාහරණයක් කිව්වොත්; තරගකාරී විශාල වෙළඳ ආයතනයක් කුඩා කඩයක හෝ එවැනි ස්ථානයක තමන්ව ප්‍රචාරණය කිරීම වෙනුවෙන් Graffiti නිර්මාණයක් සිදුකළොත් ඒ හරහා අදාළ ආයතනය ප්‍රචාරය වෙනවා වගේම, කුඩා වෙළඳ ව්‍යාපාරිකයා බංකොලොත් වෙන්නත් ඉඩ තියෙනවා. හැබැයි, මේ දේවල් සිදුනොවෙන්න අදාළ app එක නිර්මාණය කරන බව තමයි මෙහි නිර්මාණකරුවන් නම් කියන්නේ.

දැනට මෙවැනි Virtual Graffiti නිර්මාණය කරන්නට ඔබට හැකි වෙන්නේ VR Box එකක් වැනි උපාංගයක් තුළ නිර්මාණය වෙන අතත්‍ය පරිසරයක පමණයි.

Mark AR app එක වඩාත් සුවිශේෂී වෙන්නේ අන්න ඒ නිසාම යි. iDreamSky සමාගමේ නිර්මාණයක් ලෙසින් එළිදක්වෙන මේ app එකේ භාවිත වෙන්නේ, google සමාගමේ ARCore තාක්ෂණය යි. New York Comic-Con හි දී මෙහි අත්හදා බැලීම් සිදුවුණා. පැමිණි පිරිසට ජංගම දුරකතන රැගෙන එහෙ මෙහෙ යමින් Virtual Graffiti නිර්මාණය කිරීමට අවස්ථාව ලැබුණා.

iDreamSky සමාගමේ මීළඟ උත්සාහය එක නගරයක් තෝරාගෙන එහි දෙවන අත්හදා බැලීමේ වටය ක්‍රියාත්මක කිරීමට යි. ඒ ඔස්සේ ඔවුන් අදාළ app එක පරිශීලකයන් භාවිත කරන ආකාර වගේම, පරිශීලකයන් මෙය අවභාවිත කළහොත් ඒවාට ගත යුතු ක්‍රියාමාර්ග ගැන දත්ත එකතු කරගැනීමට නියමිත යි. එමෙන්ම “Mark AR” Street Artistලාට නව තෝතැන්නක් වගේම, සාමාන්‍ය පරිශීලකයන්ට විනෝදාස්වාදය වැඩි කරවන අංගයක් බවට ද මෙය පත් වේවි. මේ යෙදුම සඳහා විශේෂ comics-themed stencils එකතු කිරීමට නියමිත බවත් theverge වෙබ් අඩවිය සඳහන් කර තිබුණා. ඒවා භාවිත කරමින් ඔබටම අනන්‍ය වූ නිර්මාණයන් සිදුකිරීමට ආධුනිකයන්ට හැකි වේවි. ඉදිරියේ දී ඔබ සංචාරය කරන ස්ථානවල පා සටහන් පමණක් නොව, එම ස්ථානයන් වෙත හානි නොවන ලෙස ඔබ එතනට පැමිණි බවත් සටහන් කර යාමට හැකියාව ලැබේවි. අනාගතයේ facebook වෙනුවට AR social media එකක් නිර්මාණය වේවි. මේ තාක්ෂණය සාර්ථක වුවහොත්, එය අනාගත පෙරළියක මුල් පියවර වනවාට කිසිදු සැකයක් නම් නෑ. මේ ගැන වැඩි විස්තර mark.app වෙබ් අඩවියෙන් දැනගන්නට ඔබට හැකියාව තියෙනවා.

ඔබ දන්නවා ද; iDreamSky සමාගම කියන්නෙ Temple Run සහ subway surfers ඇතුළු ක්‍රීඩා රාශියක් නිර්මාණය කර ඇති සමාගමක් බව.

මේ තාක්ෂණය ගැන ඔබ මොකද හිතන්නේ? ලංකාවට මෙහි ආගමනය සිදු වූ විට, මොනයම් දේවල් සිදුවේවි ද? ඒ දේවල් ගැන කතා කරන්න පහළ තියෙන comment section එක විවෘත යි.

AR/VR තාක්ෂණය ගැන සහ එහි භාවිතාව ගැන වැඩිදුර දැනගන්න, අප මීට පෙර ලියූ ලිපි පෙළක්ම තියෙනවා ඔබට කියවන්න.

Google සමාගම Quantum computing තාක්ෂණය ප්‍රායෝගික භාවිතයට ගත හැකි මට්ටමට ගෙන එමින්, එම තාක්ෂණයේ තවත් පියවරක් ඉදිරියට තබන්නට සමත් වී ඇති බව වාර්තා වෙනවා.බොහෝ කාලයක් තිස්සේ quantum computing ගැන පරීක්ෂණ පැවැත්වීමට ලොව පුරා විශ්වවිද්‍යාල මෙන්ම Google, Intel, IBM වැනි විශාල සමාගම් රාශියක් කටයුතු කළා. ඒ සියලු දෙනාටම පෙර තමන් ඒ කඩයිම ජයගත් බව Google සමාගම පසුගිය සැප්තැම්බර් 27 වෙනි දා නිවේදනය කළා. මේ නිවේදනය මුලින්ම සිදු කරන්නේ සමාගමට 21 වසරක් පිරෙන දිනයේ වීමත් සුවිශේෂත්වයක්.

දැනට භාවිතයේ පවතින ඉහළම පෙලේ සුපිරි පරිගණකයක් හෙවත් ඉතාම බලගතු ක්‍රියාකාරීත්වයක් සහිත බහුකාර්ය (Multi Tasking) මේන්ෆ්‍රේම් පරිගණකයක පවා එය විසඳන්නට වසර 10,000ක පමණ කාලයක් ගනු ඇතැ යි සැලකෙන ගැටළුවක්, මේ ක්වන්ටම් ප්‍රොසෙසරය විනාඩි තුනකුත් තත්පර විස්සකින් විසඳා ඇති බව තමයි වාර්තා වන්නේ. මේ සඳහා භාවිතා වී ඇති ප්‍රොසෙසරය වන්නේ "සිකමෝ" ප්‍රොසෙසරය යි. මෙම ප්‍රොසෙසරයේ, ක්වන්ටම් තොරතුරු ක්‍රමවේදයේ තිබෙන සුවිශේෂීම ලක්ෂණය වන කිවුබිට්ස් (Qubits) 54ක් තිබීම තවත් විශේෂත්වයක්. ඉහත සඳහන් කළ තප්පර 200ක පමණ ගණනය කිරීමේ ක්‍රියාවලියේ දී මෙම ප්‍රෝසෙසරයේ කියුබිට් 54න් සක්‍රීය වී තිබෙන්නේ 53ක් පමණයි.

සාමාන්‍ය පරිගණකවල දත්ත ගබඩා කරන්නේ සහ පරිසැකසුම් කරන්නේ "1" සහ "0" ලෙසින්. අප මෙය "බයිනරි" ක්‍රමවේදය ලෙස හඳුන්වනවා. නමුත් ක්වන්ටම් භෞතික විද්‍යාවේ ඉලෙක්ට්‍රෝනයක භ්‍රමණය, අංශුමය ස්වභාවයේ හැසිරීම, සහ ප්‍රෝටෝනයක් ධ්‍රැවීකරණය යන අවස්ථාවන්වල දී හමුවන අවස්ථාවන් දෙකක අතර මැද පොදුවේ පවතින "අධිස්ථානය හෝ අධිස්ථාපිත (superposed) අවස්ථාව" දැන් පරිගණක සඳහා යොදා ගැනෙනවා.

ක්වන්ටම් අධිස්ථාපනය (Quantum Superposition) යනු යාන්ත්‍ර විද්‍යාවේ මූලධර්මයක්. භෞතික විද්‍යාවේ තරංග දෙකක් එක් කළ හැකිවාක් මෙන් ක්වන්ටම් විද්‍යාවේදී ක්වන්ටම් මට්ටම් (position) දෙකක් (හෝ වැඩි ගණනක්) එක් කළ හැකියි. එවිට එය තවත් මට්ටමක් ලෙස සැලකෙනවා. ගණිතමය වශයෙන් ගතහොත්, එය ෂ්‍රෝඩිංගර් ගේ බළලා (Schrodinger’s Cat) පරීක්ෂණයට සමානයි.

ඒ අනුව, ක්වන්ටම් පරිගණකවලට "0" සහ "1" ට අමතරව මේ අවස්ථා දෙකට ම පත්වීමේ අධිස්ථාපනය (Quantum Superposition) යොදා ගන්නවා. අන්න ඒ නිසා, මේ ක්වන්ටම් පරිගණකවලට පිරිසැකසිය (processing) යුතු තොරතුරු ලබාදුන් පසුව, එහි දත්ත පිරිසැකසුම් සහ ඒ පිරිසැකසුම්වලින් ලැබෙන ප්‍රතිඵල ඉතාම වේගවත්. සංකීර්ණ දත්තයක් පවා ඊට කෙටි කාලයකින් පිරිසකන්න පුළුවන්. තවත් සරලව සඳහන් කළොත්, Quantum computer එකක දී parallel processing, එහෙමත් නැතිනම් එකම අවස්ථාවක දී ගණනය කිරීම් විශාල සංඛ්‍යාවක් සිදු කළ හැකි වෙනවා. මෙතෙක් කල් සාමාන්‍ය පරිගණකයක දී සිදුවූයේ එකක් පිටුපස එකක්, එහෙමත් නැතිනම් serial processing ලෙස ගණනය කිරීම් සිදු කිරීම යි.

නමුත් ගූග්ල් සමාගමේ ක්වන්ටම් කම්පියුටරය "ක්වන්ටම් සුප්‍රිමසි" ක්‍රියාකාරීත්වයට පත්වීම ගැන වෙනත් සමාගම් නොයෙකුත් ආන්දෝලනාත්මක මත පල කරනවා. උදාහරණයක් ලෙස IBM සමාගම විසින් Google සමාගමේ මේ නිල නිවේදනය සම්බන්ධයෙන් නිවේදනයක් නිකුත් කරමින් කියා සිටින්නේ, Google සමාගමේ ගණනය කිරීම් නිවැරදි නොවන බවත්, සාමාන්‍ය supercomputer එකක් හරහා අදාල ගණනය කිරීම් සිදු කිරීමට වසර 10,000ක් ගත නොවන බවත්, එම කටයුත්ත දින 2.5කින් පමණ සිදු කළ හැකි බවත්.

කොහොම වුනත් IBM ආදී වූ අනෙකුත් සමාගම් සහ තරගකරුවන් පවසන අන්දමට ගූග්ල් සමාගම මේ ජයග්‍රහණය ලැබූ බවට පල කෙරුණු එකම පිළිගත හැකි තොරතුර වන්නේ 2019 වසරේ අගෝස්තු මාසයේ නාසා ආයතනයට යවා, එම ආයතනය මඟින් පල කරන ලද පර්යේෂණ පත්‍රිකාවක්. නමුත් මේ පත්‍රිකාව පළ කර කෙටි කාලයකින් එය එම ආයතනයේ වෙබ් අඩවියෙන් ඉවත් කෙරුණු බවත්, නාසා ආයතනයට එබඳු පර්යේෂණ පත්‍රිකාවක් ලබාදීමේ දී අනුගමනය කළ යුතු පටිපාටිය ඔවුන් අනුගමනය කර නැති බවත් තමයි දැන ගන්නට ලැබී තිබෙන්නෙ.

කොහොම නමුත් මේ පර්යේෂණ පත්‍රිකාව ඉවත් කරන්නට පෙර එය ඩවුන්ලෝඩ් කරගත් පිරිස් දැන් එය ලෝකය පුරා සංසරණය කරමින් සිටිනවා. මේ පිළිබඳව මධ්‍යස්ථ අදහස් දක්වන විශේෂඥයන් පවසන්නේ "ගූග්ල්.ඒ.අයි" හෙවත් ගූගල් සමාගමේ කෘත්‍රිම බුද්ධි ගවේෂණ උප සමාගම විසින් සුවිශාල ජයක් ලබාගෙන තිබෙන නමුත්, මෙහි නියම භාවිතාව ඉතා සුලභව මිනිස් වර්ගයාට ලැබෙන්නට තව යම් කාලයක් ගතවනු ඇති බව යි.

කෙසේ වෙතත් මේ වන විට ප්‍රායෝගිකව භාවිතා කළ හැකි මට්ටමේ chip එකක් ආකාරයෙන් මෙය නිෂ්පාදනය කිරීමට සමත්වීම හරහා Google සමාගම අනෙකුත් සමාගම් අභිබවා ගොස් ඇති අතර මෙය computing තාක්ෂණයේ විශාල පියවරක් ඉදිරියට තැබීමක් ලෙස අපට හඳුන්වන්න පුළුවන්.

NordVPN පසුගිය කාලය තුළ විශාල ප්‍රසිද්ධියක් ලබපු VPN සේවාවක් ලෙස හැඳින්වීම වරදක් නැහැ. ප්‍රධාන වශයෙන්ම ඔවුන් ප්‍රවර්ධන කටයුතු වෙනුවෙන් වැය කළ ඉතාම විශාල මුදල එයට එක හේතුවක්. සාමාන්‍යයෙන් VPN එකක් භාවිත කරන පුද්ගලයින් බලාපොරොත්තු වෙන ආරක්ෂාව තවදුරටත් මේ සේවාව මඟින් ලැබෙනවා ද යන්න ගැන ගැටළුකාරී වාතාවරණයක් පසුගිය දිනෙක මතු වුණා. ඒ පසුගිය වසරේ මේ සේවාව වෙත එල්ල වූ හැකර් ප්‍රහාරයක් ගැන සහ ඒ ඔස්සේ සිදු වූ බව කියවෙන Data Breach එකක් පිළිබඳව කරුණු අනාවරණය වීම සමග යි.

ඒ සියල්ලටම පෙර අපි කතා කරමු VPN ගැන.

අන්තර්ජාලයට සම්බන්ධ වන සියලු දෙනාටම IP ලිපිනයක් ලැබෙනවා. මේ IP ලිපිනය ගෙදරකට ලැබෙන ලිපිනයක් වගේම යි, අපිව අනන්‍යතාව අන්තර්ජාලය තුළ හඳුනාගන්නට සහ අදාළ දත්ත හුවමාරු කරගන්නට මෙය උදව් වෙනවා. ISP (Internet Service Provider) එහෙම නැති නම්, ඔබේ අන්ත්ර්ජාල සේවා සපයන්නා සතුව ඔබේ දත්ත සියල්ල තිබෙනවා. ඔබට තරමක් දුරට හෝ අන්තර්ජාලය තුළ ඔබේ අනන්‍යතාව සඟවාගන්න තිබෙන හොඳම විකල්පයක් වෙන්නේ VPN එකක් භාවිතා කිරීම යි. VPN හරහා සිදුවන්නේ අපේ දත්ත ආකේතනය (encrypt) ISP හෝ අදාළ වෙබ් අඩවියටවත් අපේ අනන්‍යතාවය එනම්, අපේ IP ලිපිනය, පිවිසෙන වෙබ් අඩවි, හුවමාරු කරන දත්ත ආදිය දැනගැනීමට නොහැකි ආකාරයට ආවරණය කිරීම යි. ඊට අමතරව Geo-spoof, එහෙමත් නැතිනම් තමන් සිටින ස්ථානය සඟවා වෙනත් ස්ථානයකින් අන්තර්ජාලයට සම්බන්ධ වන බව පෙන්වීම, අවහිර කරන ලද වෙබ් අඩවි වෙත පිවිසීමට ඉඩ ලබාදීම වගේ බොහොම සේවාවන් VPN එකක් මඟින් ලබාගන්න පුළුවනි. මේ කටයුත්තම අපට අවශ්‍ය නම් Proxy සේවාවක් මඟිනුත් ලබාගන්න පුළුවන්. තවත් වැඩිදුර කියවන්න ඔබ කැමති නම්, අප පෙර පළ කළ TOR ජාලය ක්‍රියාත්මක වන ආකාරය පිළිබඳ ලිපිය කියවන්න අප ඔබට ආරාධනා කරනවා.

සාමාන්‍යයෙන් VPN එකක් භාවිතා කරන්න හේතු ගණනාවක් තිබෙනවා. ප්‍රධාන වශයෙන් ඔබේ දත්ත ආරක්ෂාව වැඩි වීම සහ ඔබව කිසිවෙකුට track කිරීමේ ඉඩ බොහෝ දුරට ඇහිරීම පෙන්වා දෙන්න පුළුවන්. නමුත්, බොහෝ දෙනෙක් තමාගේ තියෙන දත්ත ගැන සහ අන්තර්ජාලය තුළ ආරක්ෂා වීම ගැන එතරම් සැලකිල්ලක් දක්වන බවක් අපට පෙනෙන්නේ නම් නැහැ.

අන්තර්ජාය තුළ ඔබේ දත්තවලට ඉතාම ඉහළ මිලක් නියම වෙන බව ඔබ දන්නවා ද? මේ වටිනාකම නියම වෙන්නේ මෙහෙම යි. උදාහරණයක් විදිහට; Facebook ආයතනය සහ එහි වෙළඳ දැන්වීම් පිළිබඳව සලකමු. වෙළඳ දැන්වීම් ප්‍රචාරණයේ දී ඒවාට වැඩිම වටිනාකමක් ලැබෙන්නේ වඩාත්ම උචිත පාර්ශවයන්ට එම දැන්වීම් පෙන්වීමට හැකි වීමෙනුයි. ෆේස්බුක් සමාගම අපේ රුචි අරුචිකම් (ඔවුන් සතුව ඇති ඔබේ දත්ත) හොඳින් දන්නා නිසා මේ වාසිය හොඳින්ම අත්විඳිනවා. අද වන විට වෙළඳ දැන්වීමක් ප්‍රචාරණය කරමින් තමන්ගේ නිෂ්පාදන වැඩිපුර විකුණාගන්නට රූපවාහිනී දැන්වීමකටත් වඩා ෆේස්බුක් හි කරන ඉලක්කගත දැන්වීමක් සාර්ථක වන්නේ මේ නිසා යි. එවන් තත්ත්වයක් යටතේ ‘දත්ත’ කියන්නෙත් දැන්වීම ප්‍රචාරය කරන්නා සහ පාරිභෝගිකයා අතර සබඳතාව ඇති කරන තවත් නිෂ්පාදන භාණ්ඩයක්.

ජනතාවගෙන් ඍජුව විස්තර ගන්නවාට වඩා, නොමිලේ අන්තර්ජාලයට පිවිසෙන්නට ඉඩ ලබා දී පිවිසෙන අයගේ දත්ත පහසුවෙන්ම, නොදැනීම ලබාගෙන තමන්ගේ ව්‍යාපාරය කරගෙන යාම ඔවුන්ට පහසුවක්. එය win-win හෙවත් අපට සේවාවක් නොමිලේ ලැබෙනවා සේ ම ලබා දෙන්නාට අපේ දත්ත ලබාගැනීමට හැකි වන නිසා දෙපාර්ශවයම ජයගන්නා අවස්ථාවක්. හැබැයි, අපිට පාඩුව සිදුවන්නේ පසුකාලීනව යි. එය හුදෙක් අපි හොරන් ගිය අසභ්‍ය වෙබ් අඩවියක දැන්වීමක් තිරය මත දිස්වීමේ සිට අපේ වටිනා පෞද්ගලික දත්තයක් ඔවුන් සතු කරගෙන ඉන් කප්පම් ගැනීමක් දක්වා දිවෙන්නට පුළුවන්. මේ අනවශ්‍ය කර්තව්‍යය කරන්නේ “අහිංසක” ලෙස දත්ත ලබාගත් VPN සමාගම නොවේ. ඔවුන්ට මුදල් ගෙවා අපේ දත්ත ලබාගන්නා අපවත් නොදන්නා තෙවන පාර්ශවයකින්. මතක තබාගන්න නොමිලයේ කිසිදු සේවාවක් ඔබට නොලැබෙන බව.

NordVPN ආයතනයට අනුව 2018 වසරේ ඔවුන්ගේ ෆින්ලන්තයේ පිහිටි Server එක වෙත හැකර් ප්‍රහාරයක් එල්ලව තිබෙනවා. නමුත්, මේ server එක තුළ ඔවුන් කිසිදු පරිශීලකයෙකුගේ activity logs, usernames, හෝ passwords රඳවා තබාගන්නේ නැති බව සමාගම සඳහන් කළා. කොහොම නමුත්, මේ ප්‍රහාරයෙන් හැකර්වරුන් වෙත පරිශීලකයන් යොමු වුණු වෙබ් අඩවි ගැන දත්ත පමණක් අනාවරණය වූ බව සමාගම උපදේශකවරයෙකු theverge.com වෙත සඳහන් කර තිබුණා. Encryption හේතුවෙන් වෙබ් අඩවිවල අන්තර්ගතයන් හෙළි නොවූ බවත් ඔහු වැඩිදුරටත් සඳහන් කර තිබුණා.

පසුගිය වසර කිහිපය පුරාවට NordVPN ආයතනය තම සේවාව අන්තර්ජාල පරිශීලකයන් වෙත හුරු කරවීමට විශාල ප්‍රයත්නයක් දරුවා. විශේෂයෙන්ම විවිධ youtube නාලිකා ගණනාවකම content අතරේ වගේ ම, podcast අතරතුරත් NordVPN තුළින් ලැබුණු අනුග්‍රාහකත්වයන් ගැනත් සඳහන් වුණා. මේ විශාල ප්‍රචාරණය නිසාම ඒ වෙත ලැබුණු පරිශීලකයන් ප්‍රමාණය ඉතාම විශාල බව තමයි වාර්තා වෙන්නේ.

NordVPN හි තාක්ෂණ උපදේශන මණ්ඩලයේ සාමාජිකයෙකු වන ටොම් ඔක්මන් (Tom Okman) theverge.com වෙත ප්‍රකාශයක් ලබාදෙමින් සඳහන් කර තිබුණේ, ඔවුන්ගේ පරිශීලකයන් සම්බන්ධ වී සිටින vpn servers සෑම විනාඩි 5ක් හෝ ඒ ආසන්න කාලයක් තුළ දී මාරු වෙන බව යි. අදාළ ප්‍රහාරය සිදුකළ හකර්වරුන් හට ඔවුන්ගේ server ඇතුළත දත්ත ලබාගන්නට ලැබුණේ ඉතාම කෙටි කාලයක් බවත් ඔහු වැඩි දුරටත් සඳහන් කර තිබුණා.

සිදු වූ Data Breach එක පිළිබඳව blog අඩවියක තිබූ වාර්තාවකින් මේ පිළිබඳව සමාජය වෙත කරුණු අනාවරණය වී තිබෙනවා. මේ Breach එක ගැන තම සමාගම මාස කිහිපයකට පෙර දැනගත් බවත්, ඒ පිළිබඳව කිසිදු කරුණක් සමාජගත නොකළේ NordVPN ආයතනයට ඔවුන්ගේ අනෙක් servers ගැනත් පරීක්ෂණ පැවැත්වීමට කාලය අවශ්‍ය වූ නිසා බවත් Okman සඳහන් කරනවා. හැකර්වරුන් ලබාගත් දත්ත අවභාවිත වූ අවස්තාවක් ගැන කිසිදු සිදුවීමක් වාර්තා වී නොමැති අතර, මේ ගැන ඉතාම ඉක්මනින් පරිශීලකයන් වෙත දැනුවත් කිරීමක් සිදුකරන බව ඔවුන් සඳහන් කරනවා. වෙන කිසිදු data center එකකට මෙයින් හානියක් වී නොමැති අතර, මෙය hack වීමක් ලෙසින් හැඳින්වීමට තරම් දෙයක් නොවන බව යි ඔහු සඳහන් කරන්නේ.

පසුගිය දිනෙක Google සමාගම ඔවුන්ගේ දෘඩාංග හඳුන්වාදීමේ අවස්ථාවේ දී නවතම උපාංගයන් ගණනාවක් හඳුන්වා දුන්නා. ඒ අතරට බොහෝ දෙනෙකු බලා සිටි Pixel 4 සහ Pixel 4 XL දුරකතනයන් දෙකත් ඇතළත් වුණා. බොහෝ දෙනෙක් පුදුමයට පත් වුනේ මේ දුරකථනය සතුව Fingerprint sensor එකක් නොමැති වීම නිසාවෙනුයි.

විශාල sensors ප්‍රමාණයක් භාවිත කරමින් ඔවුන් වඩාත් ආරක්‍ෂිත face unlock තාක්ෂණයක් මේ දුරකතනයට ඇතුළත් කිරීම තාක්ෂණික ලෝකයේ කතාබහක් ඇති කරවන මාතෘකාවක් වුණා. විශේෂයෙන්ම Motion Sense පහසුකමක් මේ වෙත ඇතුළත් වන අතර, Pixel 4 ජංගම දුරකථනය අතට ගන්නා විට මේ Motion Sense හරහා Camera එක සහ Face unlock සඳහා වන අනෙකුත් sensors සූදානම් කරනු ලබනවා.

කොහොම නමුත් BBC හි වාර්තාකරුවෙකු වූ Chris Fox සිදුකළ අනාවරණයක් සමගින් මේ ආරක්ෂණ ක්‍රමවේදයේ තිබෙන දුර්වලතාවයන් ගැන විශාල කතාබහක් ගොඩනැගුනා. මොහු සිදු කළ අනාවරණයෙන් පසුව හෙළි වුනේ පරිශීලකයා ඇස් වසාගෙන සිටිය ද දුරකථනය unlock කර ගැනීමට හැකියාව තිබෙන බව යි. එම නිසා පරිශීලක දත්ත ආරක්ෂාව පිළිබඳව මතු වෙන්නේ විශාල ගැටළුවක්. උදාහරණයක් ලෙස දුරකතනයේ හිමිකරු නින්දේ සිටින විට දී වුවත් ඉතාම පහසුවෙන් දුරකථනය ඕනෑම අයෙකුට unlock කරගැනීමට හැකියාව මේ දුර්වලතාවය හරහා ලැබෙනවා. මේ පිළිබඳව google support page එකෙත් දැකගන්න පුළුවන්. ඔවුන්ට අනුව ඔබේ දුරකථනය ඕනෑම කෙනෙකුට ඔබේ මුහුණ වෙත ඇල්ලීමෙන් unlock කර ගැනීමට හැකියාව තිබෙනවා.එයින් ආරක්ෂා වීමට ඔබේ දුරකථනය ආරක්ෂිත ස්ථානයක, එනම් සාක්කුවක හෝ handbag එකක වැනි තැනක තබාගත යුතු වෙනවා.

මෙය තරමක් හාස්‍යජනක සිදුවීමක් වෙන්නේ මෙතරම් දියුණු තාක්ෂණයක් හෝ sensors ගණනාවක් භාවිත නොවුනත් Face unlock පහසුකම සහිත දුරකථන ගණනාවක් වෙත මෙවැනි ගැටළුවක් පැන නොනැගීම යි (Retinal scanner වැනි තාක්ෂණික ක්‍රමවේද ඒ වෙත භාවිත වීම ඊට ප්‍රධාන හේතුව යි). මේ තාක්ෂණයම භාවිතා කරන නව iPhopne මාදිලි වෙතත් මෙවැනි ගැටළුවක් නොපැමිණීම මේ තත්ත්වය තවත් ප්‍රශ්නකාරී කරවනවා. iPhopne මාදිලි භාවිත කරන FaceID තාක්ෂණය ඔස්සේ දුරකථනය unlock වීමට නම් අදාළ පරිශීලකයා ගේ ඇස් විවරව තිබිය යුතුම යි.

මෙවැනි දුර්වලතාවයක් තිබිය දී face unlock එක ප්‍රධාන unlock method එක බවට අපත් කර තිබීම, සහ එමඟින් බැංකු කටයුතු පවා approve කිරීමේ පහසුකම් ලබාදීම කොතරම් ආරක්ෂිත ද යන්න ගැටළු සහගත යි. මේ වෙද්දීත් Google සමාගම මේ වෙත විසඳුම් ලබාදීමට කටයුතු කරමින් සිටින බව වාර්තා වෙනවා. ඉදිරියේ දී Pixel 4 පරිශීලකයන්ට “Require eyes to be open” යනුවෙන් සටහනක් ඔවුන්ගේ සෑම ෆේස් අන්ලොක් කිරීමක දීම දැකගන්නට ලැබේවි. නමුත් මේ software fix එක ලබන මාසය තෙක් ලබාදීමට ඔවුන්ට නොහැකි වනු ඇති බව යි දැනගන්නට ලැබෙන්නේ. එතෙක් පරිශීලක කැමැත්ත පරිදි Pin එකක් හෝ Pattern එකක් භාවිත කරන ලෙස ඔවුන් දැනුම් දෙනවා.

මේ මාසය තුළ ආරක්ෂණ ක්‍රමවේදයන් අසාර්ථකවීම් පිළිබඳව වාර්තා වූ තවත් දුරකථන මාදිලියක් ලෙස Samsung හඳුන්වන්න පුළුවන්. Samsung නවතම දුරකතනවල ආරක්ෂණ දුර්වලතාවයක් පසුගිය දිනෙක හඳුනාගනු ලැබුණා. On screen fingerprint sensor ඇතුලත් දුරකතන වෙත “gel cover”- tempered glass භාවිත කරන පරිශීලකයන්ගේ දුරකතන ඉතාම පහසුවෙන් ඕනෑම කෙනෙකුට finger print එක අසල swip කිරිමක් මඟින් unlock කිරීමේ හැකියාවක් පවතින බව thesun.co.uk වෙබ් අඩවිය අනාවරණය කළා. මේ ගැන අදහස් දක්වමින් Samsung සමාගම සඳහන් කර තිබුණේ ultrasonic fingerprint sensor එකට ඇඟිලි සලකුණු හඳුනාගැනීම සඳහා භාවිත කරන 3D patterns නිවැරදිව rednder කිරීමට gel cover එක නිසා නොහැකිවන බව යි. මේ සඳහා පිලියමක් ලෙස security update එකක් ඉතාම ඉක්මනින් ලබාදෙන බවත්, එතෙක් Galaxy S10, S10 Plus, and S10 5G වැනි දුරකථන භාවිත කරන පරිශීලකයන් “gel cover”- tempered glass ඉවත් කර නැවත fingerprint setup කරගන්නා ලෙස දැනුම් දෙනවා.

මේ ගැටලුව On screen fingerprint තාක්ෂණය භාවිත වෙන අනෙක් දුරකතන වෙතත් බලපාන්න ඉඩ තිබෙනවා. මේ තාක්ෂණය ගැන වගේම, ඔබ පෞද්ගලිකව ඔබේ දුරකතනය unlock කරන්න භාවිත කරන ක්‍රමවේදයත්, ඊට විශේෂ හේතුවක් තිබේ නම එයත් පහළ comment section එකේ කියන්න අමතක කරන්න එපා.

ගල්කිස්ස හෝටල් පරිශ්‍රයේ දී පැවැත්වෙන්නට නියමිත අපුර්ව සාහිත්‍ය උළෙලක් තමයි, අන්නාසි සහ කඩලගොටු සාහිත උළෙල කියන්නේ. ඒ සඳහා ඔබටත් සම්බන්ධ වෙන්න පුළුවන්. ඒ කොහොමද කියලා අපි මේ ලිපියෙන් දැනගනිමු.

Epic Games සමාගමේ නිර්මාණයක් ලෙස 2017 වසරේ දී එළිදැක්වුණ Fortnite පරිගණක ක්‍රීඩාව ලෝකයේ විශාලම prize pool එකක් සහිත පරිගණක ක්‍රීඩාවක් ලෙස අතිශය ජනප්‍රිය යි. Survival සහ Battle Royale කියන Game Genresවලට මේ ක්‍රීඩාව අයිති වෙනවා. 2018 වසරේ දී පමණක්

ඇමරිකානු ඩොලර් බිලියන 2.4ක ආදායමක් ලැබූ Fortnite ක්‍රීඩාව සමග ලොව පුරා මිලියන 125ක් පමණ ක්‍රීඩකයින් රැඳී සිටිනවා. පසුගිය දිනෙක Fortnite mobile version එකත් ඔවුන් තමන්ගේ ක්‍රීඩා ලෝලීන් වෙත හඳුන්වා දුන්නා. කොහොම වුණත්, පසුගිය 13 වෙනිදා සිට මේ ක්‍රීඩාව ක්‍රීඩා කිරීමට නොහැකි තත්ත්වයක් උදා වුණා.

බොහෝ දෙනෙකුට මතු වුණ ගැටළුව තමයි; මේ Fortnite අවසානය ද? කියන එක. හදිසියේම Fortnite ක්‍රීඩාවේ තිබෙන දූපත වෙත යම් ආකාරයක උල්කාපාතයක් කඩා වැටෙනවා. කඩා වැටෙන මේ උල්කාෂ්මය හේතුවෙන් දූපත විනාශ වී යන්න පටන් ගන්නවා. ක්‍රීඩකයන්ට මෙම සිදුවීම දෙස බලා සෙවීම හැර කිසිවක් කරන්නට හැකියාවක් තිබුණේ නැහැ. ඉන් අනතුරුව නිර්මාණය වෙන කළු සිදුරක් තුළට සියලුම දේ ඇදී යනවා.

කළු සිදුර කියන දේ ඔබට යම් නුහුරු සංකල්පයක් නම් පහළ video එක නරඹන්න අපි ඔබට ආරාධනා කරනවා.

මේ ක්‍රීඩාව තුළ සිදුවුණු එකී සිදුවීම.

මේ සිදුවීම පිළිබඳව ක්‍රීඩකයන් වගේම තාක්ෂණික ලෝකයේත් බොහෝ කතාබහට ලක් වෙන්න පටන් අරගෙන යි තියෙන්නේ. මේ සිදුවීම වටා පවතින උණුසුම වඩාත් තීව්‍ර වෙන්නේ Fortnite ක්‍රීඩාව වෙනුවෙන් පවත්වා ගෙන ගිය Twitter account එක සියලුම tweet මකා දැමීම නිසාවෙනුයි. මේ වෙද්දි එහි blackhole එකෙහි live video එකක් පමණක් දැකගන්න හැකියාව තියෙනවා. Fortnite වෙනුවෙන් වෙන්ව තිබූ නිල facebook පිටුවත් අක්‍රීයව යි පවතින්නේ. ක්‍රීඩාව සහ එහි bugs වැනි දෑ පිළිබඳව සටහන් වන Epic සමාගමේ Public Trello Board එකත් අක්‍රීය තත්ත්වයට පත්ව තිබෙනවා.

Twitch, YouTube සහ Twitter ඇතුළු සමාජ මාධ්‍ය සියල්ලේම පාහේ, මේ ක්‍රීඩාව වෙනුවෙන් නිර්මාණය වී තිබූ නිල ගිණුම් තුළ blakhole එක පමණක් දැකගන්න පුළුවන් වෙනවා. මිලියන ගණනක් ක්‍රීඩකයන් බලාපොරොත්තු දල්වා බලා සිටින්නේ මීළඟට සිදුවන දෙය පිළිබඳව යි.

“the end is near “this is the end වැනි twitter පණිවිඩ කිහිපයක්ම නිල twitter ගිණුමේ පළ වී තිබුණත්, මේ වෙද්දී ඒ සියල්ල ඉවත් කර ඇති බව අපිට දැකගන්න පුළුවන්.

කොහොම නමුත්, twitter පණිවිඩයක් නිකුත් කරමින් PlayStation සමාගම සඳහන් කරන්නේ; ක්‍රීඩකයන් මෙය ක්‍රීඩා කිරීමේ දී භාවිතා කළ V-bucks (ක්‍රීඩාව තුළ විවිධ දේ මිල දී ගැනීම සඳහා භාවිත කරන ඒකකයක්) සියල්ල ගැන බිය විය යුතු නැති බව යි. වැඩි විස්තර දැනගන්න epicgames.helpshift.com වෙබ් අඩවිය හරහා පුළුවන් බවත් ඔවුන් මතක් කරනවා.

ක්‍රීඩාවට දැන් ඇතුල් වෙන්න උත්සාහ දරන ක්‍රීඩකයන් වෙත විවිධ error පණිවිඩ දර්ශනය වීම් දැකගන්න ලැබිලා තියෙනවා.

බොහෝ දෙනෙක් මේ සිදුවීම ගැන වගේම ඊළඟට සිදුවන දේ පිළිබඳව විවිධ අනුමානයන් ගණනාවක් ඉදිරිපත් කර අවසන්. ඔවුන්ගේ විශ්වාසය නව මුහුණුවරකින් ක්‍රීඩාව යළි නිකුත් වනු ඇති බව යි.

COD කියූ සැනින් ඔබේ මතකයට එන අතිශය ජනප්‍රිය පරිගණක ක්‍රීඩාවේ mobile සංස්කරණය පසුගිය දිනෙක නිකුත් කෙරුණා.

TikTok App එක අද වෙද්දී ලෝකයේ ශීඝ්‍රයෙන් වර්ධනය වෙන short video sharing platform එකක් බවට පත් වී අවසන්. මේ වෙද්දී මෙහි download count එක මිලියන 660ක් පමණ වෙන බව තමයි වාර්තා වෙන්නේ. කොහොම වුණත් tiktok ගැන කතා කරද්දී Musical.ly ගැන කතා නොකරම බැහැ. Musical.ly කියන්නෙ 2014 වසරේ Alex Zhu, Luyu Yang යන දෙදෙනා අතින් නිර්මාණය වුනු කෙටි lip-sync videos නිර්මාණය කළ හැකි app එකක්. ආරම්භයේ සිටම මේ app එක තරුණ තරුණියන් අතර අතිශය ජනප්‍රිය වෙනවා. 2017 වසර වන විට එහි පරිශීලකයන් සංඛ්‍යාව මිලියන 200ත් ඉක්මවූවා. කොහොම වුණත්, 2017 වසරේ මේ Musical.ly App එකෙහි අයිතිය ByteDance සමාගම විසින් ඇමරිකානු ඩොලර් මිලියනයකට මිල දී ගන්නවා. ඉන් අනතුරුව ඔවුන්ගේ යටතේ පැවති TikTok App එක සමග merge කිරීම සිදුකරනවා. අද වෙද්දී මේ app එක භාෂා 75කින් ලෝකය පුරාම භාවිත වෙනවා.

ඉන්දියාවෙන්, ඉන්දුනීසියාවෙන් සහ බංගලාදේශයෙන් තහනම් වූ TikTok

ඉන්දියාව තුළ මිලියන 120කට වැඩි පරිශීලකයන් පිරිසක් හිමි ‘TikTok’ හි නුසුදුසු අසැබි දේ අන්තර්ගත වන බවත්, ඒ මඟින් ඉන්දීය සංස්කෘතියට හානී වීම සිදු වේයැ යි ගොඩනැඟුණු චෝදනා සැලකිල්ලට ගනිමින් පසුගිය අප්‍රේල් 16 වෙනිදා මදුරාසි මහාධිකරණය ඉන්දියාවෙන් TikTok app එක ඉවත් කරන ලෙස google සමාගමට සහ apple සමාගමට දැන්වූවා. කෙසේ වෙතත්, මේ තහනම පැවතුණේ සතියක් වැනි ඉතාම කෙටි කාලයක් පමණයි. TikTok හිමිකාරිත්වය දරන ByteDance සමාගම මේ තහනම හේතුවෙන් ඔවුන් $500,000 පමණ පාඩුවක් ලබන බවත්, එවැනි නුසුදුසු දේ upload කිරීම නැවැත්වීම සඳහා අවශ්‍ය කරන තාක්ෂණික පහසුකම් TikTok සතු බවත් අධිකරණයට දන්වා සිටියා. අවසානයේ සතියක් වැනි කාලයක් ඇතුළත TikTok තහනම ඉවත් කරගන්නට ByteDance සමාගමේ නීතීඥන් හට හැකි වුණා.

පසුගිය මාසයක දී නැවතත් ඉන්දීය අමාත්‍යවරුන් කිහිපදෙනෙක්ම, ඉන්දීය සංස්කෘතියට එරෙහි දේ අන්තර්ගත වීම නිසා ඉන්දියාවෙන් tiktok තහනමක් පිළිබඳව කතිකාවතක් ගොඩනගන්නට සමත් වුණා. මෙයට හේතුව ලෙස ඔවුන් සඳහන් කරන්නේ sexually explicit content, cyberbullying වැනි දේ අඩංගු වීම යි. ඊට deepfakes වැනි ක්‍රමවේද ඔස්සේ විවිධ පුද්ගලයන් සහ චරිත සඳහා අපහාස වන අයුරින් නිර්මාණය වන videos පවා මෙහි අඩංගු බව ඔවුන් ප්‍රකාශ කළා.

2018 වසරේ ජූලි මාසයේ 3 වෙනිදා කාමුක දර්ශන, අසභ්‍ය දේ, සහ විවිධ පුද්ගලයන්ට අපහාස වෙන දේ අන්තර්ගතයැ යි කියමින් ඉන්දුනීසියානු රජය TikTok වෙත චෝදනා එල්ල කරා. එවැනි දේ නැවත්වීමට සහ අදාළ content වාරණය කිරීමට 20 දෙනෙකුගෙන් යුතු කාර්යමණ්ඩලයක් ඉන්දුනීසියාව වෙත අනියුක්ත කිරීමට ByteDance සමාගම පොරොන්දු වුණා. ඉන් අනතුරුව 2018 ජූලි 11 වෙනිදා මේ තහනම ඉවත් කෙරුණා.

කාමුක සහ අසභ්‍ය දර්ශන ඇතුළත් video පට සහ වෙබ් අඩවි තහනම් කිරීමට බංගලාදේශය ගෙන යන 'anti-porn war' සංකල්පය සමග විවිධ වෙබ් අඩවි සහ apps 20,000කට අධික සංඛ්‍යාවක් තහනම් කිරීමට බංග්ලාදේශ රජය පසුගිය පෙබරවාරියේ දී කටයුතු කළා. මේ අතරට TikTok app එකත් ඇතුළත් වුණා. දීර්ඝ පැහැදිලි කිරීම්වලින් අනතුරුව මේ තහනමත් ඉවත් කරවා ගැනීමට ByteDance සමාගම සමත් වුණා.

2018 වසරේ සහ 2019 වසර දී දෙවතාවක්ම නව යොවුන් වියේ ගැබ් ගැනීම් නිරූපණය කරන වීඩියෝ වැනි “පිළිගත නොහැකි” content අන්තර්ගත වීම සම්බන්ධයෙන් Douyin (චීනයේ TikTok හඳුන්වන නාමය) වැනි apps ගණනාවකට චීන මාධ්‍යවලින් සහ රජයෙන් දැඩි අවලාද නැගුණා. මෙවැනි දෑ දිගින් දිගටම පළ වෙන්නේ නිර්මාණ developerවරුන්ගේ නොසැලකිල්ල නිසා බව යි රජය චෝදනා නගන්නේ. මේ චෝදනාව ඉතාම දැඩි ලෙස සැලකිල්ලට ගන්න ByteDance සමාගමට සිදුවෙනවා. ඒ ඔවුන්ගේ ප්‍රධාන සමාගම පිහිටියේත් චීනයේ නිසාම යි. මේ නිසා චීනයට නොගැළපෙන ඉතාම විශාල TikTok content ප්‍රමාණයක් filter කිරීම සිදුකරන බව යි දැනගන්නට ලැබුණේ. නමුත්, මේ filter කිරීම් නිසාම තවත් විශාල ප්‍රශ්නයකට මුහුණ දෙන්න ByteDance සමාගම ඇතුළු TikTok කාර්යමණ්ඩලයට සිදුවෙනවා.

Theguardian.com වෙබ් අඩවියේ පසුගිය දිනෙක TikTok විවිධ content චීන රජයට පක්ෂපාතීව ඉවත් කිරීම පිළිබඳව ලිපියක් පළ වුණා. චීන රජයට විරුද්ධව කෙරෙන කතාබහ අඩංගු video වාරණය කරන බවට TikTok වෙත චෝදනා එල්ල වුණා. මේ තහනම් කරන video අතරට Tiananmen Square, Tibetan independence සහ Falun Gong වැනි සිදුවීම් වගේම, Hong Kong protests එක පිළිබඳව කෙරෙන ප්‍රකාශයන් පවා ඇතුළත් වුණ බව යි වාර්තා වන්නේ. මෙසේ චීන රජයට පක්ෂපාතීව සිදුකෙරෙන මෙම content ඉවත් කිරීම පිළිබඳව සමාලෝචනයක් සිදුකරමින් පර්යේෂණයක් පැවැත්විය යුතු බව, ඇමරිකානු සෙනෙට් සභික Marco Rubio එක්සත් ජනපදයේ භාණ්ඩාගාර දෙපාර්තමේන්තුවේ විදේශ ආයෝජන කමිටුව (Treasury Department’s Committee on Foreign Investment in the United States - CFIUS) වෙත ලිපියක් යවමින් ඉල්ලීමක් කර තිබෙනවා.

මේ ගැන theverge.com වෙබ් අඩවිය වෙත අදහස් දක්වමින් TikTok හි නියෝජිතයෙකු ප්‍රකාශ කර තිබෙන්නේ; ඔවුන්ගේ content ඉවත් කිරීම පිළිබඳව කිසිම රජයක මැදිහත් වීමක් නොවන බව යි. කෙසේ නමුත්, මේ ගැන තවමත් CFIUS වෙතින් ප්‍රතිචාරයක් දක්වා නැහැ.

මේ TikTok තහනම ගැන ඔබ මොකද හිතන්නේ?

සිසුන් ගණනාවකට තමාගේ වියදමින් උගන්වන සුපිරි ගුරුවරයෙක් පිළිබඳව ඉන්දියාවෙන් චිත්‍රපටයක් නිර්මාණය වුණා. එම චිත්‍රපටයට පාදක වූ සැබෑ ගුරු තරුව පිළිබඳව යි මේ.

පසුගිය වසරට සාපේක්ෂව පරිශීලකයන්ගේ messages, call information, සහ GPS locations වැනි දත්ත සොරකම් කරන apps ප්‍රමාණය මේ 2019 වසරේ මුල් මාස 8 තුළ දී පමණක් සියයට 373ක පමණ ප්‍රතිශතයකින් වැඩි වී ඇති බව Senior Malware Intelligence Analyst කෙනෙක් වන Nathan Collier malwarebytes.com වෙත සටහනක් ඉදිරිපත් කරමින් සඳහන් කරනවා.

ඔහුට අනුව පසුගිය මාසය තුළ පමණක් malwarebytes ආයතනය අනවසර monitoring/ tracking apps, spyware, හෝ stalkerware algorithms අඩංගුයැ යි සැක කෙරෙන වැඩසටහන් 2,500කට අධික සංඛ්‍යාවක් Scan කිරීමට සිදුව තිබෙනවා. ඊට අමතරව මේ වන විටත් නීතිය ක්‍රියාත්මක කරවන විවිධ කණ්ඩායම් සහ ලෝකය පුරා සිටින ආරක්ෂක පර්යේෂකයන් සමග ඒකාබද්ධව ගෘහස්තව සිදුවන අන්තර්ජාල අපයෝජනයන් අනවසර දත්ත සොරකම් වැනි දේට විරුද්ධවත් ඔවුන් ක්‍රියාමාර්ග සැලසුම් කරමින් සිටින බව ඔහු සඳහන් කරනවා.

සාමාන්‍යයෙන් stalkerware ලෙස හඳුන්වන්නේ අප තව කෙනෙක් ගැන යම් උපාංගයක් ගැන තොරතුරු ලබාගන්නා මෘදුකාංගයක් වැනි දෙයක්. මේවා සාමාන්‍ය ජීවිතයේ දී භාවිත වෙන අවස්ථාවන් බොහොමයක් තිබෙනවා. උදාහරණයක් විදිහට, තමන්ගේ ආදරණීයයන් ඉන්න තැන් දැක බලාගන්නට විවිධ ආයතන apps වර්ග හඳුන්වා දී තිබෙනවා. අදාළ දෙපාර්ශවයේම හෝ උපාංග දෙකේම අවසර සහිතව ඔවුන් සිටිනා ස්ථාන එකිනෙක වෙත පෙන්වනවා. තමන්ගේ දරුවන් ගැන, ආදරණීයන් ගැන තොරතුරු ලබාගන්න භාවිත වෙන මේ apps අද වෙද්දී ඉතාම සුලභ යි. තවදුරටත්, මේ වැනි වැඩසටහන් අස්ථානගත වුණ විවිධ උපාංග සොයාගන්නත් භාවිතා කරනවා. කෙසේ වෙතත්, මේ වැඩසටහන් අවභාවිතා වන අවස්ථා නම් ඕනෑ තරම් අද වෙද්දී දැකගන්නට හැකියාව තිබෙනවා. මේ තාක්ෂණයන් අනිසි ලෙස භාවිත කරන්නන්ට ඔවුන්ගේ වින්දිතයින්ට අහිතකර ලෙස ඔවුන්ව track කිරමට හැකියාව ලැබෙනවා. සුලභව මෙවැනි පුද්ගලයන් ඔවුන්ගේ වින්දිතයින්ගෙන් ලබා ගන්නා දත්ත වර්ග කිහිපයක් මේ විදිහට දක්වන්න පුළුවන්.

ඒ වගේම ඔබට Mobile Menace Monday: beware of monitoring apps කියන ලිපිය කියවන්න කියලා ඔබට ආරාධනා කරනවා.

කොහොම වුණත් මෙවැනි වැඩසටහන් අවභාවිතා කිරීම සහ අදාළ පුද්ගලයාගේ අවසරයකින් තොරව දත්ත භාවිත කිරීම සයිබර් අපරාධයක් ලෙසින් සැලකෙනවා. (Android 10 මෙහෙයුම් පද්ධතිය සමග එන්නට නියමිත, තාවකාලිකව අදාළ app එක වෙත permission allow කිරීමේ හැකියාවත් මෙවැනි අපරාධ අවම කිරීමට ගත් එක ක්‍රියාමාර්ගයක්)

රුසියාව, ඉන්දියාව, බ්‍රසීලය සහ එක්සත් ජනපදය ගෝලීය වශයෙන් ඇන්ඩ්‍රොයිඩ් ස්ටෝකර්වෙයාර් නිර්මාණය සහ භාවිතය වැඩිම කලාපයන් බවට පත්ව තිබෙනවා. ලෝකයේ ජනප්‍රිය ආරක්ෂක පර්යේෂණ ආයතයනක් වන Kaspersky ආයතනය මේ වසර තුළ දී පමණක් පරිශීලකයාගේ අවසරයකින් තොරව මේ අනිෂ්ට මෘදුකාංග ස්ථාපනය හෝ එසේ කිරීමට උත්සාහ දැරීම් පිළිබඳව පැමිණිලි 518,223 තමන් වෙත ලැබී තිබෙන බව සඳහන් කරනවා.

මෙලෙසින් අන්තර්ජාලයේ සැරිසරන පරිශීලකයන් බිලිගන්නටම නිර්මාණය වූ spams/ phishing sites වගේ දේවල් අද වෙද්දී සුලභ කරනු බවට පත් වී හමාර යි. මේවා අපට හඳුනාගන්න සහ ගැලවෙන්න ඉතාම අපහසු මට්ටමට ඉතා සූක්ෂමව සහ තාත්විකව නිර්මාණය කරන්න හැකර්වරුන් පියවර ගන්නවා. බොහෝ විට මෙවැනි stalkerware ස්ථාපනය කිරීමත් එවැනි web අඩවි හෝ phishing email හරහා සිදුවෙනවා.

Whatsapp, facebook ඇතුළු instant messaging apps බොහොමයකුත් මේ ලෙසින් stalkerware ග්‍රහණයට නතු වෙන්නට පුළුවන්. WhatsApp is end-to-end encrypted (E2EE) භාවිතා වුණත් දත්ත ලබාගන්නා පුද්ගලයාගේ හෝ යවන පුද්ගලයාගේ දුරකථනය හෝ පරිගණකය මෙවැනි මෘදුකාංගයක ග්‍රහණයට නැතුව තිබෙනවා නම් E2EE තාක්ෂණයෙන් ඵලක් නැති බව ඔබට පැහැදිලි ඇති.

මේ ලිපිය සමග සබැඳෙන අන්තර්ජාලයේ සැරිසරද්දී ඔබට ආරක්ෂා වෙන්නට ගත හැකි පියවර ගැන අප පළ කළ ලිපිය වගේම, phishing පිළිබඳව පළ කල ලිපියත් කියවන්න ඔබට ආරාධනා කරනවා. මේ ගැන ඔබේ අදහස් පහළින් comment කරන්නත් අමතක කරන්න එපා.

2004 වසරේ පෙබරවාරි 4 වෙනි දා මාර්ක් සකර්බර්ග් ඇතුළු හාවර්ඩ් විශ්වවිද්‍යාලයේ සිසුන් කිහිපදෙනෙකු වන Eduardo Saverin, Andrew McCollum, Dustin Moskovitz සහ Chris Hughes කියන කිහිපදෙනාගේ මූලිකත්වයෙන් තමයි facebook සමාජ ජාල වෙබ් අඩවිය ආරම්භ වෙන්නේ. කොහොම වුණත් මේ වන විට සිය 15 වෙනි සංවත්සරය සමරන facebook ජාලයට පසුගිය වසර ගණනාවම එතරම් සුභ වුණේ නම් නැහැ. පසුගිය වසරේ සිදුවුණු Facebook-Cambridge Analytica data scandal සිදුවීමත් එක්ක බොහෝ පරිශීලකයන් ප්‍රමාණයක් Facebook කෙරෙහි තබා තිබූ විශ්වාසය බිඳ වැටුණා කිව්වොත් නිවැරදි යි. කේම්බ්‍රිජ් ඇනලිටිකා නැමති ෆේස්බුක් පාරිභෝගිකයන්ගේ දත්ත අවභාවිතය පිළිබඳ සොයාබැලීමට පත් කළ විශේෂ කොමිසම සඳහා සාක්ෂ්‍ය ලබා දෙන්නත් මෙහි දී සකර්බර්ග්ට සිදුවුණා. ඒ වගේ ම ඇමරිකානු කොන්ග්‍රස් සභිකයන් ඉදිරිපිට ඔවුන්ට තාක්‍ෂණය පිළිබඳවත් අවබෝධ කර දෙන්නට ද සිදුවුණා. ඉතින්, මේ සිදුවීම ලෝකයේ සමාජ ජාලයන් භාවිතා කරන සියල්ලන් අතරම පාහේ අතිශය කතා බහට ලක් වූ මාතෘකාවක් බවට පත් වුණා.

මේ සිදුවීමේ උණුසුම හරියාකාරයෙන් බැස යන්නටත් කලින් facebook ගිණුම් මිලියන 50කට පමණ එල්ල වුණු දැවැන්ත සයිබර් ප්‍රහාරය ඔබට මතක ඇති. ප්‍රහාරයට ලක්වූ බවට සැක කෙරුණු ගිණුම්වල access token reset කරමින් ඔවුන් ඒ Vulnerability නිවැරදි කළ බව සමාගම ප්‍රකාශයක් නිකුත් කළා.

Facebook හි ගැටළු එතනින් නැවතුණේ නැහැ. පසුගිය 2018 වසරේ දෙසැම්බර් 18 වෙනි දා New York Times හෙළිදරව් කළ කරුණුවල ප්‍රතිඵලයක් ලෙස තවත් සිද්ධි දාමයක් නිරාවරණය වුණා. ඔවුන් වාර්තා කර තිබුණේ; ෆේස්බුක් සමාගම තම ව්‍යාපාරික සගයන් ලෙස කටයුතු කරන netflix සහ spotify වෙත වගේ ම, Royal Bank of Canada ලබාදීමට කටයුතු කර තිබේ ද යන්න යි. ඔවුන්ට පරිශීලකයන්ගේ පෞද්ගලික පණිවිඩ පවා බැලීමේ සහ මැකීමේ හැකියාව තිබූ බවත් එහිදී හෙළිදරව් වුණා. nytimes.com, businessinsider.com මේ පිළිබඳව දීර්ඝ හෙළිදරව්වක් කළා. මිට අමතර ව පසුගිය දිනෙක Facebook ජාලයේ තිබූ bug එක නිසාවෙන් මිලියන 6.8 පරිශීලකයින්ගේ privacy දමා ඇති පින්තූර පවා නැරඹීමේ හැකියාව බාහිර app developresලාට ලැබී තිබුණේ, Facebook පිළිබඳ පරිශීලක විශ්වාසය තව තවත් අඩු කරමිනුයි.

කොහොම වුණත් මේ සියලු ගැටළු නිරාකරණය කරගන්නා අතරතුර එයින් තමන් පාඩමක් ද ඉගෙන ගත් බව ද ඔවුන් දන්වා සිටියා. ඒ, ඔවුන් සිදුකළ පර්යේෂණයක ප්‍රතිඵල ලෙසින් facebook සමාජ ජාලයේ ක්‍රියාත්මක වෙන තුන්වන පාර්ශවයේ apps දසදහසකට අධික ප්‍රමාණයක් ඉවත් කරමිනුයි. මෙයට හේතුව ලෙස දැක්වෙන්නේ එකී apps විසින් පරිශීලක දත්ත අවභාවිතා කිරීම යි. එමෙන්ම, තහනම් කළ apps දසදහසකට ආසන්න ප්‍රමාණයක් නිර්මාණය කර ඇත්තේ developersලා 400 දෙනෙක් පමණ සුළු පිරිසක් වීම පුදුමයට කාරණයක්. ආසන්න වශයෙන් ගත කල, එක developer කෙනෙක් apps 25ක් පමණ නිර්මාණය කර ඇති බව වාර්තා වෙනවා. මෙහි අරමුණ සංවිධානාත්මකව apps භාවිත කරමින් පරිශීලක දත්ත සොරාගැනීම යි. කොහොම වුණත්, ඔවුන්ගේ මේ පර්යේෂණයේ ප්‍රතිඵල ලෙසින් තාවකාලිකව අත්හිට වූ apps ප්‍රමාණය 60,000කට ආසන්න වන අතර, ඉන් බහුතරයක් සුළු සුළු කාරණා මත තාවකාලිකව අත්හිට වූ බවයි වැඩිදුරටත් වාර්තා වන්නේ.

Facebook apps භාවිත කරන්න කලින් ඔබත් දෙවතාවක් ඒ ගැන හිතනවා නම් හොඳයි කියන එකයි, අපේ යෝජනාව!

2019 වසර, අනෙක් වසරවලට සාපේක්ෂව smartphone ලෝකයට වැඩි විවිධත්වයක් එකතු කළ වසරක් ලෙස හඳුන්වන්න පුළුවන්. පසුගිය වසරවලට සාපේක්ෂව දුරකථන සමාගම් අතර තරගකාරීත්වය වඩ වඩාත් වැඩි දියුණු වුණු වසරක් විදිහටත් මේ වසර හඳුන්වන්න පුළුවන්. එහි ප්‍රතිඵල ලෙස ලෝකයට හඳුන්වා දුන් දුරකථන ගැන යි මේ ලිපිය හරහා සාකච්ඡා කෙරෙන්නේ.

Nokia වෙළඳ නාමය පිළිබඳව ඔබ හොඳින්ම දන්නවා. නොකියා සන්නාමය යටතේ නිකුත් වූ දුරකථන අතර අතිශය ජනප්‍රියත්වයට පත් වූ Nokia 3310 දුරකථනය, 2017 වසරේ HMD Global සමාගම යටතේ නැවත වෙළඳපොලට නිකුත් වූ බව ඔබට මතක ඇති. ඒ සමාගම Nokia 2720 දුරකථනයත් නව මාදිලියකින් නිකුත් කිරීමට පසුගිය දිනෙක කටයුතු කළා. Nokia 2720 Flip ජංගම දුරකථනය 2019 සැප්තැම්බර් මස නිල වශයෙන් announce කෙරුණු අතර, මෙහි විශේෂත්වයක් වන්නේ පළමු මාදිලිය නිකුත් කිරීමෙන් වසර 10කට පසුව මෙම වැඩිදියුණු කළ මාදිලිය නිකුත්වීම යි. Linux මත පදනම් වූ KaiOS මෙහෙයුම පද්ධතියෙන් සමන්විත මේ දුරකථනය සතුව WhatsApp, Google Assistant, Facebook, YouTube, සහ Google Maps වැනි apps භාවිත කිරීමේ හැකියාව පවතිනවා. දුරකථනය ශක්තිමත් වීම සහ දින 28ක් පවතින battery ආයු කාලය නිසා මෙය ඉතා ඉක්මනින් ජනප්‍රිය වන බව සමාගමේ විශ්වාසය යි.

දුරකථන සමාගමක් වශයෙන් වගේම තවත් විවිධාකාර උපාංගයනුත් නිපදවන පෙරළිකාර සමාගමක් ලෙස ප්‍රසිද්ධ MI සමාගම, ඔවුන්ගේ නවතම උපාංගය ලෙසින් Mi Mix Alpha හඳුන්වා දුන්නා. මෙහි විශේෂත්වය වන්නේ ජංගම දුරකථනය වටා පැතිරුණු display එක යි. මෙම ජංගම දුරකථනයේ screen to body ratio අගය 180%ක් නිසාම මෙය පිළිබඳ ලෝකයේ විශාල කතාබහක් ඇති වුණා. ඒ වගේම screen to body ratio අගය 180% වන ලොව පළමු දුරකථනය ලෙසත් මෙය ඉතිහාසගත වෙනවා.

නවතම 5G තාක්ෂණය සහිත මෙම දුරකථනය සතුව Qualcomm Snapdragon 855+ Chipset පවතිනවා. ඒ වගේම samsung සමාගමේ නවතම camera sensor එක සහිත දුරකථනය වෙන්නෙත් මෙය යි. මෙගාපික්සල් 108කින් සමන්විත කැමරාව මෙහි තවත් සුවිශේෂී අංගයක්. 12GB RAM එකක් සහ 512GB internal memory එකකින් මේ දුරකථනය සමන්විත යි. කැමරාව විශාල 1/1.33 වර්ගයේ සංවේදකයක් සහ ටෙට්‍රසෙල් තාක්‍ෂණයෙන් සමන්විත යි. Ultra-wide කැමරාවට අංශක 117ක පරාසයක් ආවරණය කළ හැකි අතර තෙවන කැමරාව 12MP Telephoto කාචයකින් සමන්විත වෙනවා. 2800$ වැනි ඉහළ මිලක් මෙයට තීරණය වී තිබෙනවා.

Foldable දුරකථනයක්, එසේ නොමැති නම් නැවිය හැකි දුරකථනයක්, කියන්නේ බොහෝ දෙනෙකුගේ සිහිනයක්. මේ සිහිනය ජය ගැනීම දුරකථන සමාගම් රාශියක ඉලක්කය බවට පත් වෙන්නේ ඒ නිසාවෙන්. Samsung සමාගම Samsung Unpacked 2019 Event එකේ දී ඔවුන්ගේ පළමු Galaxy Fold දුරකථනය හඳුන්වා දුන්නා. නමුත් එය මහජනතාවට නිකුත් කිරීමට පෙරම ඒ දුරකථනවල යම් යම් දෝෂයන් හටගත් බව එහි අත්හදාබැලීමේ උපාංග භාවිතා කළ කිහිප දෙනෙකුම සඳහන් කළා. විශේෂයෙන් ඒ අතරට අතිශය ජනප්‍රිය youtubersලා පවා ඇතුලත් වුණා. ඒ ගැටළු තරමක් දුරට නිරාකරණය කරමින් ඔවුන්ගේ දුරකථනය නැවතත් වෙළඳපොළට නිකුත් කිරීමට samsung සමාගම තීරණය කර තිබුනා. නමුත් එය තවමත් එතරම් සාර්ථක නොමැති බව පසුගිය දිනෙක නැවතත් සනාත වුණා. ඒ, JerryRigEverything සිදු කළ videoවක් නිසාවෙන්.

කොහොම වුණත් පසුගිය සැප්තැම්බර් 27 වැනි දින ඇමෙරිකාවේ වෙළඳපොලට මෙම device එක නිකුත් කිරීමට Samsung සමාගම තීරණය කළ අතර, එහි මිළ ඇමෙරිකානු ඩොලර් 1,980ක් වන බව වාර්තා වෙනවා.

Motorola RAZR කියන්නේ Motorola සමාගමේ ජනප්‍රියම ජංගම දුරකථනයක් කිව්වොත් නිවැරදි යි. ඒ එය නිෂ්පාදනය කළ කාලය තුළ ඒකක මිලියන 130කට වඩා අලෙවි කිරීමට මොවුන් සමත් වී තිබුණ නිසාවෙන්. Cnet.com වෙබ් අඩවියට අනුව මේ වසරේ අග නම්‍යශීලි දුරකථනයක් ලෙසින් නවතම Motorola RAZR දුරකථනයක් නිකුත් කිරීමට මෝටරෝලා සමාගම සූදානම් වෙනවා. මේ දුරකථනය වෙත Blutooth certification ලැබුනේ පසුගිය පෙබරවාරියේ වුණත්, මෙය නිකුත් වීම තරමක් ප්‍රමාද වීමට බොහෝ දෙනෙකු චෝදනා කරන්නේ නම්‍යශීලි තිරයේ ප්‍රයෝගිකත්වය හා ඇතිවූ ගැටළුවලට යි. Qualcomm Snapdragon 710 Chipset එකකින් සහ 2730mAh බැටරියකින් සමන්විත මේ දුරකථනය ඇමරිකානු ඩොලර් 1500ක පමණ මිලකට අලෙවි වේයැ යි විශ්වාස කෙරෙනවා.

මේ දුරකථනවලට අමතරව පසුගිය මාස කිහිපය ඇතුළත නිකුත් වූ සහ නිකුත් වීමට තිබෙන දුරකථන ගණනාවක් තිබෙනවා. ලබන 15 වෙනි දින නිකුත් වෙන Pixel 4 දුරකථනය ගැන වගේම තවත් සුවිශේෂී දුරකථන ගණනාවක් ගැන විස්තර ඉදිරි ලිපිවලින් ඔබට දැන ගන්න පුළුවන්. මේ ගැන ඔබේ අදහස් පහළින් සඳහන් කරන්නත් අමතක කරන්න එපා.

Smart ජංගම දුරකථනය කරළියට ඒමත් සමග මිනිසුන්ගේ එදිනෙදා කටයුතු වගේම තවත් බොහෝ දේවල් සිදු කර ගැනීමට ඔවුන්ට පහසු වුණා. තැන තැන ගෙනයාමට හැකි වීම වගේම බරින් අඩු වීමත්, වැඩකටයුතු රාශියක් කරගැනීමට හැකිවීමත් නිසා අද වෙද්දී smartphone එකක් බොහෝ දෙනෙකුගේ ළඟ අපට දකින්න ලැබෙනවා. මීටත් වඩා දුරට වැඩ පහසු කරගන්න තමයි smart glass සංකල්ප බිහි වෙන්නේ.

VR, AR වැනි සංකල්ප සහ තාක්ෂණයන් භාවිතා කරමින්, සම්ප්‍රදායික ස්මාට් ජංගම දුරකථනය වෙනුවට, අතට නොගෙන ඇසේ පළඳින කන්නාඩියක් වැනි උපාංගයක් හරහා විවිධ කටයුතු සිදු කර ගැනීම තමයි මේ smart glass සංකල්පයේ සරල අරමුණ. එහිදී ඔබේ ඇසේ චලනයන් හරහා ග්ලාස් එක මඟින් මේ විධානයන් හඳුනාගැනීම සිදු වෙනවා. ඔබ බොහෝ විට මෙවැනි තාක්ෂණයක් විද්‍යා ප්‍රබන්ධයන්වල දැක තිබෙන්නට පුළුවන්. අද වෙද්දී ඒ සංකල්පයන් චිත්‍රපටවලට සීමා නොවී, ඒ හා සමාන තාක්ෂණයන් සැබෑ ලෝකයේත් භාවිතා වෙනවා.

තාක්ෂණික ලෝකයේ ජිවත්වන, තාක්ෂණය සමග නිතර ගැටෙන බොහෝ දෙනෙක් සිහින මවපු දෙයක් තමයි තමාගේ ජංගම දුරකථනය smart glass එකක් බවට පත්කර ගැනීම. මේ අදහසට පක්ෂ පිරිස වගේම අකමැති පිරිසකුත් අපට දකින්න ලැබුණා. උදාහරණයක් විදිහට Google Glass පිළිබඳව ඇතිවුණු කතාබහ ඔබට මතක ඇති.

අද වන විට බොහෝ දෙනෙකු සිතන අන්දමට Google Glass අසාර්ථක, සමාගම විසින් අතහැර දමන ලද නිෂ්පාදනයක්. නමුත් Google සමාගම Google Glass පිළිබඳ පර්යේෂණයන් අතහැර දමා නැහැ. Google සමාගමේ මව් සමාගම ලෙසින් හැඳින්වෙන Alphabet සමාගම මේ වසරේ මුල් භාගයේ Google lens ව්‍යාපෘතියට නැවත පණ දුන්නා. දැන් එය හුදෙක් අත්හදා බැලීමේ පවතින උපාංගයක් නම් නොවෙයි. ඒ වගේම Facebook සමාගම සහ apple සමාගම AR glass නිපදවීම පිළිබඳව සලකා බලමින් සිටින බවත්, මේ වෙද්දී දැනගන්න ලැබනවා. ඒ වගේම මෙවැනි ව්‍යාපෘති සඳහා මිලියන ගණනක මුදල් ආයෝජනයන් පවා යෙදවෙනවා. නමුත් මේවා 2019 වසර වෙද්දීත් මිනිසුන්ගේ එදිනෙදා ජිවිතය වෙත පැමිණ නැත්තේ ඇයි ද යන වග ඔබට ප්‍රශ්නයක් ඇති.

මෙයට මූලිකම හේතුව වන්නේ තාක්ෂණයේ සීමාවන්. අප හුදෙක් විද්‍යා ප්‍රබන්ධවල දකින මට්ටම වෙත smart glass කියන සංකල්පය ගෙන ඒමට තවත් බොහෝ කාලයක් ගත වේවි. ඒ වගේම මේ උපාංග සාමාන්‍ය පොදු ජනතාවට භාවිත කළ නොහැකි වීමට තවත් එක හේතුවක් වන්නේ එහි අධික මිල යි. බොහොමයක් මෙවැනි glass පැළඳ සිටීමේ ප්‍රයෝගික අපහසුතාවන්, අවහිරතාවන් ද තිබෙනවා. ඒ වගේම මේ smart glass පිළිබඳව කතා බහ කරද්දී, එය මිනිසුන්ගේ පෞද්ගලිකත්වයට හානියක් වෙන බව තමයි බහුතරයක ගේ පිළිගැනීම.

VR තාක්ෂණය, එහෙම නැති නම් Virtual Reality (අතථ්‍ය-තථ්‍යතාව), කියන්නේ මේ සියවසේ ජිවත් වන අප බොහෝ දෙනෙකුට සුලබව හමුවන, අහන්න ලැබෙන තාක්ෂණයක්. මේ තාක්ෂණික වචනය අපට අහන්න ලැබෙන්නේ 1982 වර්ෂයේ ඩේමියන් බ්‍රොඩරික් විසින් රචිත ජුදාස් මැන්ඩලා නම් විද්‍යා ප්‍රබන්ධය හරහා යි. මේ තාක්ෂණික සංකල්පයේ වඩා වැඩිදියුණු මට්ටමක් ලෙසින් miscrosoft සමාගම නිෂ්පාදනය කරන HoloLens උපාංග හඳුන්වන්න පුළුවන්.

සාමාන්‍යයෙන් VR තාක්ෂණය හරහා ඔබට තිරයක් ඔස්සේ ත්‍රිමාන රූප හරහා වෙනස්ම පරිසරයක හිඳ කටයුතු කරනවා සේ අත්දැකීමක් ලබාගන්න පුළුවන්. එම තාක්ෂණය අද වන විට බොහොමයක් වෙබ් අඩවි සහ පරිගණක ක්‍රීඩා නිර්මාණකරුවන් බහුලව භාවිතා කරන තාක්ෂණයක්. නමුත් HoloLens උපාංග මිට හාත්පසින්ම වෙනස් තාක්ෂණයක් භාවිතා කරන්නේ. ඒ හරහා ඔබට සැබෑ පරිසරය තුළම ත්‍රිමාන රූප මවා ගැනීමේ හැකියාව සහ ඒවා සමග කටයුතු කිරීමේ හැකියාව ලබා දෙනවා. මේ තාක්ෂණයේ නිර්මාතෘ වන බ්‍රසීල ජාතික ඇලෙක්ස් කිප්මන් කියන්නේ, මේ වන තෙක් විද්‍යා ප්‍රබන්ධ චිත්‍රපට සහ කතාවල පමණක් දක්නට ලැබුණු තාක්ෂණය මේ හරහා සැබෑ වන බව යි.

අතථ්‍ය ලෝකය සැබෑ ලෝකය සමග මුහු වන HoloLensහි තාක්ෂණයට miscrosoft සමාගම දෙන නාමය වෙන්නේ Mixed Reality යන්න යි. මේ හරහා ඔබට විවිධ objects (වස්තූන්) තමන් සිටිනා පරිසරය තුළ දී ම නිර්මාණය කරමින්, වෙනස් කරමින් කටයුතු කළ හැකි අවකාශයන් ලබා දෙනවා. HoloLens උපකරණය මේ සියල්ල සිදුකිරීමට විශේෂ උපාංග භාවිතා කරනවා. මෙහි භාවිත වන සංවේදක මඟින් මේ උපකරණය භාවිත කරන පුද්ගලයා සිටින පරිසරය, ඔහු සිදුකරන චලනයන් පිළිබඳව ගණනය කිරීම් සහ හඳුනාගැනීම් සිදුකරනවා. Light Source හතරක් සහ විශේෂ ලේසර් තාක්ෂණයක් සහිත Depth Camera ඇතුළු මෙම කොටස, මෙම උපකරණයේ ඇස ලෙස හඳුන්වන්න පුළුවන්. ඒ වගේම, එමඟින් ලබා දෙන ටෙරා බයිට් ගණනක දත්තයන් process කරමින් භාවිත කරන්නාට අවශ්‍ය වස්තුන් නිර්මාණය කිරීම සිදුවෙනවා. ඒ සඳහාම විශේෂිත HPU (Holographic Processing Unit) නම් චිපයක් ඔවුන් එයට ඇතුළත් කර තිබෙනවා. ඒ වගේම මේ උපකරණය විශේෂිත speakers පද්ධතියකින් ද සමන්විත යි.

මේ උපකරණය සහිත විශේෂිතම අංගයක් වන්නේ මෙහි දර්ශන තලය ලෙසින් භාවිත වන විදුරු තීරය යි. සාමාන්‍යයෙන් ඇසට ඉතා සමීපයේ ඇති යමක් නිරීක්ෂණය කිරීමේ හැකියාව මිනිස් ඇසට නැහැ. ඒ නිසාවෙන් මේ උපකරණයට, හුදෙක් මේ තිරය වෙත ප්‍රක්ෂේපනයන් පමණක් සිදුකිරීම ප්‍රමාණවත් වෙන්නේ නැහැ. නමුත් ඔවුන් භාවිත කරන විශේෂ තාක්ෂණය ඔස්සේ සාමාන්‍ය අවස්ථාවන්හි මිනිස් ඇස ක්‍රියාත්මක වන ලෙසින්ම ඇස තුළ ම ආලෝක කිරණ මඟින් මේ රූප මැවීම සිදුකරනවා. මේ තාක්ෂණය නිසාවෙන් භාවිත කරන්නාට සත්‍ය බාහිර ලෝකය තුළ ම තමන්ට අවශ්‍ය දේ නිර්මාණය සහ භාවිතයට අවස්ථාව ලැබෙනවා.

මේ තාක්ෂණය භාවිත කිරීමට පෙර සිට ම VR/ AR තාක්ෂණයන් භාවිතයෙන් ඇමරිකානු සෙබළුන් පුහුණු කිරීම සඳහා විශේෂිත වැඩසටහන් ක්‍රියාත්මක වුණා. නමුත් මේ නව තාක්ෂණය හරහා වඩාත් ඵලදායී ලෙසින් ඒ කටයුත්ත සිදුකිරීමට හැකියාව පවතිනවා. ඒ වගේම, මේ යුධ කටයුතු සඳහා නිර්මාණය වන (military-grade) HoloLens සාමාන්‍ය භාවිතය සඳහා ඇති උපාංගවලට වඩා වෙනස්කම්වලින් යුක්ත යි. බාහිර පෙනුමෙන් මෙන්ම විශේෂිත තාප සංවේදක හා night vision වැනි පහසුකම්වලින් සමන්විත විශේෂිත උපාංග 2500ක් පමණ ඉදිරි වසර කිහිපය තුළ ඇමරිකානු හමුදාවට ලබාදීමට කටයුතු කරන බව යි ඔවුන් සඳහන් කරන්නේ.

Mac පරිගණක භාවිතා කරන බොහෝ දෙනෙකු බලා සිටි ඔවුන්ගේ නවතම මෙහෙයුම් පද්ධතිය, macOS Catalina ලබන ඔක්තෝම්බර් මාසයේ දී එළිදැක්වීමට Apple සමාගම සූදානමින් සිටිනවා. දීර්ඝ කාලයක් beta testings කිරීමෙන් අනතුරුව යි මෙය නිකුත් කිරීමට ඔවුන් තීරණය කර තිබෙන්නේ. පරිශීලකයන්ට මේ මෙහෙයුම් පද්ධතිය සමග නව්‍යකරණය වූ විශේෂාංගයන් රාශියක් ලැබෙනවා. Mac App Store හරහා සුපුරුදු පරිදි මෙය download කර ගැනීමට පරිශීලකයින්ට ඉඩ ලැබෙනවා.

WWDC 2019 event එක අතරතුර දී හෙළි කළ පරිදි Project Catalyst නම් වූ framework එකක් හරහා iPad apps mac පරිගණකවල භාවිතා කළ හැකි ලෙස නිර්මාණය කිරීමේ හැකියාව ලබාදීමට Apple සමාගම සූදානම් වෙනවා.

mac OS Catalina සංස්කරණය ලැබීමට නියමිත පරිගණක

ඔවුන්ගේ beta තත්ත්වයේ තිබු IOS 13 දුරකථන මෙහෙයුම් පද්ධතිය පසුගිය සැප්තැම්බර් 19 වැනි දින නිල වශයෙන් නිකුත් කළා. මෙහි සුවිශේෂීම පහසුකම ලෙස system-wide dark mode එක පෙන්වා දෙන්න පුළුවන්. ඒ වගේම Apple Maps, Photos, Reminders, Memoji, Music යන appවල වැඩිදියුණු කිරීම්, Swipable typing පහසුකම keyboard එකට එකතු කිරීම, අලුතින් හඳුන්වාදුන් Privacy feature වැනි තවත් පහසුකම් කිහිපයක්ම මෙයට ඇතුලත් වෙනවා. ඒ වගේම මේ update එක සමග iOS Keyboard එක වෙත නව භාෂා 38ක් හඳුන්වා දී තිබෙනවා. ඒ අතරට සිංහලත් ඇතුලත්. මේ මෙහෙයුම් පද්ධතිය iPhone 11, iPhone 11 Pro, iPhone 11 Pro Max, iPhone XS, iPhone XS Max, iPhone XR, iPhone X, iPhone 8, iPhone 8 Plus, iPhone 7, iPhone 7 Plus, iPhone 6S, iPhone 6S Plus, iPhone SE, iPod touch (seventh generation) යන devices සඳහා මේ වන විටත් ලබා දී අවසාන යි. එහි තිබු bugs කිහිපයක් පසුව හඳුනා ගත් අතර ඒවා නිරවුල් කර 13.1 සංස්කරණය පසුගිය 24 වෙනිදා ලබාදීමට ඔවුන් කටයුතු කර තිබුණා.

MacOS සහ iOS භාවිතා කරන පරිශිලකයන් වෙත safari web browser එකෙහි නවතම සංස්කරණය Safari version 13.0 පසුගිය දිනෙක නිකුත් කරනු ලැබුණා. මේ හරහා iOS භාවිතා කරන පරිශිලකයන් හටත් mac පරිගණකයකදී Safari web browser හරහා සිදු කළ හැකි සියළුම පහසුකම් ඇතුලත් වන අන්දමේ web browsing අත්දැකීමක් ලබාදීමට Apple සමාගම කටයුතු කර තිබනවා. මේ නව update එක තුළ privacy සහ security පිළිබඳව වැඩි අවධානයක් යොමු කර ඇති අතර ලබාදෙන නව පහසුකම් යටතට Download manager පහසුකමකුත් ඇතුලත් වෙනවා.

කොහොම නමුත් මේ සංස්කරණය සමගින් පැරණි Safari Extension සියල්ල නවතා දැමීමට Apple සමාගම තීරණය කර ඇති බැවින් Safari App Extension API එක හරහා නිර්මාණය කරනු ලැබූ Extensions පමණක් ක්‍රියාත්මක වනු ලබනවා.

බොහෝ දෙනා ප්‍රකාශ කරන පරිදි VPN extension සහ Ad Blocking extension බොහෝමයක් මේ අනුව අකර්මන්‍යය වී ගොස් ඇති බව වාර්තා වෙනවා.

පසුගිය සැප්තැම්බර් 3 වෙනිදා google සමාගමේ නවතම android මෙහෙයුම් පද්ධතිය, Android 10 නිකුත්වුණා. Essential Phone එක සහ Xiaomi සමාගමේ Redmi K20 Pro දුරකථනය වෙතත් මේ මෙහෙයුම් පද්ධතිය ලබාදෙන්න එම සමාගම කටයුතු කර තිබුණා.

OnePlus ආයතනය විසින් ඔවුන්ගේ OnePlus 7 සහ OnePlus 7 Pro දුරකතන වෙතත් ඔවුන්ගේ නව මෙහෙයුම් පද්ධතිය වන OxygenOS 10හි stable සංස්කරණයක් නිකුත් කරනු ලැබුණා. මේ සංස්කරණය OTA update වැඩසටහන හරහා අනෙක් දුරකථන වෙතත් ඉතා ඉක්මනින් download කර ගැනීමට හැකි වේවි. අනෙක් දුරකථන වෙත මෙය තවමත් නිකුත් කර නොමැති නිසා ඒවා වෙත මෙය ලැබෙන දිනය සැප්තැම්බර් 26 වැනි දින ලන්ඩනයේ පැවැත්වීමට නියමිත OnePlus event එකේ දී ප්‍රකාශයට පත් කෙරෙනු ඇතැ යි බලාපොරොත්තු වෙනවා.

කෙසේ වෙතත් මේ update එක OnePlus 7 සහ 7 Pro ජංගම දුරකථනවලට අමතරව OnePlus 5/5T, OnePlus 6/6T වෙතත් ලබාදෙනු ඇති බව බොහෝ දෙනෙකුගේ විශ්වාසය යි.

Google සමාගම නිකුත් කරන Pixel ජංගම දුරකථන මාලාව ලෝකය පුරා අතිශය ජනප්‍රිය බවට පත්වූවක්. විශේෂයෙන්ම මේ දුරකථන මාලාවේ කැමරා පද්ධතිය කාගේත් සිත් ඇදගන්නට සමත්ව තිබෙනවා. ඉදිරියේ දී නිකුත් කරන්නට ඇති Pixel 4 දුරකථනය පිළිබඳව මේ වෙද්දීත් විශාල කතාබහක් තාක්ෂණික ලෝකයේ ඇතිව තිබෙන බව ඔබ දන්නවා ඇති.

සාමාන්‍යයෙන් ජංගම දුරකතනයක් නිකුත් වෙන්නට කලින් එහි පෙනුම සහ එහි විස්තර අන්තර්ජාලයට නිකුත් වීම පුරුද්දක් ලෙස සිදුවන්නක්. සමහර අවස්තාවන්වල දුරකතන සමාගම් හිතා මතාම මේ දත්ත අන්තර්ජාලයට කාන්දු කිරීමත් සිදු කරනවා. ඒ ඔවුන්ගේ දුරකතනය ප්‍රචාරණයන් සිදු කර ගැනීම අරමුණු කර ගෙන යි.

පසුගිය දිනෙක google සමාගම pixel 4 දුරකථනය සඳහා නිර්මාණය කළ බවට සැලකෙන ප්‍රචාරණ වෙළඳ පටයක් (promotional video එකක්) අන්තර්ජාලයට එකතු කිරීමට ස්පාඤ්ඤ ජාතික Proandroid වෙබ් අඩවිය සමත් වුණා.

මේ අනුව ඉදිරියට එන Pixel 4 දුරකතනයේ night sight mode එකෙහි නව සංස්කරණයන් අහස/තරු ආදිය ඡායාරූපගත කළ හැකි astrophotography mood එකක් හඳුන්වාදීමට නියමිත බව වගේම වැඩි දියුණු වූ air gestures, සහ Google Assistant භාවිතා කර voice මඟින් පමණක් Google Photos app එකේ වැඩ කර ගැනීමට හැකියාව ලැබෙන බවත් මෙහි සඳහන්.

ඒ වගේම Pixel ජංගම දුරකථනයේ unlocking mechanism එක Face unlock තාක්ෂණය මත පදනම් වන අතර, iPhone Xවල සිට භාවිතා වන ආකාරයේ advanced sensors ගණනාවක් භාවිතා කරමින් ඉතාමත් ආරක්ෂිත ආකාරයේ Face unlocking ක්‍රමයක් හඳුන්වාදීමට Google සමාගම කටයුතු කර තිබෙන බවක් කියවෙනවා. Face unlock කිරීම සඳහා භාවිතා වන ඡායාරූප හෝ කිසිදු රූපමය තොරතුරක් ජංගම දුරකථනයෙන් පිටතට ගෙන නොයන බවත්, සියළු processing කටයුතු ජංගම දුරකථනය තුළම සිදු කරනු ලබන බවත්, කිසිදු අවස්ථාවක දී Google හෝ වෙනත් සේවාවකට මේ දත්ත භාවිතා කළ නොහැකි බවත් ඔවුන් වැඩිදුරටත් පෙන්වා දෙනවා.

මීට අමතරව මෙහි අන්තර්ගත වන විශේෂිතම තාක්ෂණය වන්නේ Google සමාගමේ Advanced Technology and Projects (ATAP) team එක විසින් සිදු කරගෙන ගිය Project Soli නමින් හැඳින්වූ ව්‍යාපෘතියේ ප්‍රතිඵලයක් ලෙස නිර්මාණය කළ Soli chips භාවිතා කරමින්, හස්ත සංඥා භාවිතා කිරීමේ හැකියාව ලැබීම යි. ගීතයක් skip කිරීම, alarm එකක් නැවැත්වීම හෝ call එකක් ලැබෙන විට එය silent කිරීම වැනි කටයුතු මූලිකව මේ හරහා සිදු කිරීමේ හැකියාව ලබා දෙන බවත්, ඉදිරියේ දී මෙය භාවිතා කරමින් තවත් පහසුකම් භාවිතා කිරීමේ හැකියාව ලබාදීමටත් Google සමාගම බලාපොරොත්තුවෙන් සිටින බව වාර්තා වෙනවා.

සම්පුර්ණ Pixel 4 ජංගම දුරකතනයේයැ යි සැලකිය හැකි ඡායාරූප පෙළක් theverge.com වෙබ් අඩවිය වෙත යම් පුද්ගලයෙකු විසින් ඒවා තිබුණා.

තවමත් Pixel 4 ජංගම දුරකථනය නිල වශයෙන් නිකුත් කරන දිනයක් සඳහන් කර නොමැති නමුත් බොහෝ විට ඔක්තෝම්බර් මාසයේ මෙය සිදු වේවියැ යි බොහෝ දෙනෙක් විශ්වාස කරනවා. කෙසේ වෙතත් අන්තර්ජාලය වෙත කාන්දුවුණු මේ images පිළිබඳව බොහෝ දෙනෙකු විවිධ මතයන් පල කරනවා. පසුපස තනි කැමරාවකින් පමණක් මෙතෙක් සමන්විත වුනු pixel දුරකතන මෙවර එය වෙනස් කිරීම පිළිබඳව වගේම එහි නිමාව සහ මුහුණත ගැනත් මේ වෙද්දී කතා බහක් ගොඩ නැගෙමින් පවතිනවා. මේ ගැන ඔබේ අදහස අපට පහළින් comment කරන්න මතක කරන්න එපා.

Update: Pixel 4 ජංගම දුරකථනය එළැඹෙන ඔක්තෝබර් 15 වන දා නිල වශයෙන් නිකුත් කෙරෙන බව Google ආයතනය විසින් මීට සුළු මොහොතකට පෙර ප්‍රකාශයට පත් කෙරුනා.

Apple උපාංග භාවිතා කරන Apple සන්නාමයට ආදරය කරන බොහෝ දෙනෙකු වගේම, තාක්ෂණයට කැමැත්තක් දක්වන බොහෝ දෙනෙකු මඟ බලා සිටි, 2019 වසරේ apple සමාගමේ විශාලම hardware event එක (දෘඩාංග එළිදක්වන උත්සවය) පසුගිය 10 වෙනිදා පැවැත්වුණා. ඉතිහාසයේ ප්‍රථම වතාවට twitter සහ apple වෙබ් අඩවියට සීමා නොවී youtube හරහාත් මේ event එක සජීවීව නැරඹීමේ හැකියාව ලබා දෙන්නට ඇපල් සමාගම කටයුතු කර තිබුණා. පුරා පැය දෙකක් පමණ වේලාවක් පැවැත්වුණු මෙහිදී නව උපාංග ගණනාවක් එළිදක්වනු ලැබුවා.

බොහෝ දෙනෙක් බලාපොරොත්තු වූ පරිදිම iPhone 11, iPhone 11 Pro, සහ iPhone 11 Pro Max දුරකථන කාගේත් අවධානය දිනාගත් බව අපට දැකගන්න ලැබුණා. ඒ වගේම තවත් සුවිශේෂී උපාංග ගණනාවක් මෙහිදී හඳුන්වාදෙනු ලැබුණා. මේ ඒ පිළිබඳව යි.

මේ උත්සවය අතරතුර, ඇපල් සමාගම ඔවුන්ගේම streaming සේවාවක් ආරම්භ කරන බව නිවේදනය කළා. Apple TV Plus ලෙසින් මේ සේවාව ඔවුන් නම් කර තිබෙනවා. මේ සේවාව මාසයකට $4.99 පමණ මුදලකට ලබාදෙන්න ඔවුන් තීරණය කර තිබෙනවා. ඒ වගේම ඔබ අලුතින් නිකුත් වූ ඇපල් උපාංගයක් මිල දී ගත් විට වසරක් පුරාවට නොමිලයේ ඇපල් ටීවී සේවාව ඔබට ලැබෙනවා.

මේ Event එක අතරතුර දී හඳුන්වාදුන් තවත් වැදගත් උපාංගයක් ලෙස නව iPad එක හඳුන්වන්න පුළුවන්. මේ නව iPad එක අඟල් 10.2ක screen එකක් සහිතව යි එළිදැක්වෙන්නේ. පැරණි iPad එක සතුවුණේ අඟල් 9.7ක පමණ screen එකක් පමණ යි. මෙහි විකිණුම් මිල ආරම්භ වෙන්නේ පැරණි ipad එකෙහි මිලට සමාන මිලක් වූ $329කින් වුණත් මෙහි වැඩි දියුණුවූ අංගයන් කිහිපයක්ම සහිත යි. A10 Bionic processor එකකින් සමන්විත Seventh Gen iPad එක සතුව Smart Connector එකක් ද සහිත යි. මේ හරහා ඉතාම පහසුවෙන් ඇපල් සන්නාමය යටතේ අලෙවිවන Smart Keyboards ඔබට සවි කර ගැනීමට හැකි වෙනවා. ඔවුන්ට අනුව වේගය අතිනුත් විශාල වශයෙන් වැඩි දියුණුවීම් මෙහි දැකගන්න පුළුවන්.

2.හත්වන පරම්පරාවේ iPad - iphoneincanada.ca

Apple Watch Series 5 කියන්නෙත් බොහෝ දෙනෙක් බලා සිටි උපාංගයක්. බාහිර පෙනුමෙන් පසුගිය Apple Watch එකෙන් එතරම් වෙනසක් නොවුණත්, අලුත් පහසුකම් ගණනාවකින් මෙය සමන්විත යි. බොහෝ දෙනෙකුගේ අවදානය දිනාගත්තේ always-on display function එක සඳහා මෙය සහාය දැක්වීම යි. එක්වරක් charge කිරීමෙන් පසුව පැය 18ක් පමණ ක්‍රියාත්මක වීමට මෙයට හැකියාව තිබෙනවා. මෙහි GPS model එක $399 ලෙසිනුත් GPS + LTE model $499 ලෙසත් වාර්තා වෙනවා.

Apple Watch series 3 හි මිල ඩොලර් 279 සිට 199 දක්වා අඩු කිරීමටත් මොවුන් තීරණය කර තිබෙනවා.

පසුගිය වසරේ ඇපල් සමාගම නිවේදනය කළ iPhone XRහි අනුප්‍රාප්තිකයා ලෙසින් මේ iPhone 11 හඳුන්වන්න පුළුවන්. අඟල් 6.1ක ප්‍රමාණයේ LCD display එකක් සමගින් නිෂ්පාදනය කර ඇති අතර Apple සමාගමේ අලුත්ම chipset එක වන A13 Bionic chipset එක මෙයට අන්තර්ගත වෙනවා. ඒ වගේම දැනට smart ජංගම දුරකතනයක අඩංගු වේගවත්ම චිප් එක එය බව යි ඔවුන් සඳහන් කළේ. මෙය 12MP wide-angle සහ 12 MP ultra-wide dual camera පද්ධතියකින් සමන්විත වන අතර, night mode එක සහ flasher වැඩි දියුණු කර තිබෙන බව ඔවුන් සඳහන් කළා.

iPhone 11 ජංගම දුරකථනය පැරණි iPhone XR එකට වඩා ඩොලර් 50ක් මිළ අඩුවෙන්, ඩොලර් 699ක මුදලකට අලෙවි කිරීමට Apple සමාගම තීරණය කර තිබෙනවා.

iPhone 11 Pro සහ Pro Max යන මාදිලි ද්විත්වයම camera 3කින් සමන්විත කැමරා පද්ධතියකින් (triple camera) සමන්විත යි. Deep Fusion සහ machine learning භාවිත කරමින් ඉතා පැහැදිලි ඡායරූප ලබා ගැනීමට හැකියාව මේ දුරකථන සතු යි. iPhone 11 Pro අඟල් 5.8ක display එකක් සහ Pro Max අඟල් 6.5ක display එකකින් සමන්විත වෙනවා. Pro දුරකතනය iPhone Xs Max ජංගම දුරකථනයට වඩා පැය 4ක කාලයක් භාවිතා කළ හැකි බවත්, iPhone 11 Pro Max ජංගම දුරකථනය Xs Max දුරකතනයට වඩා පැය 5ක කාලයක් භාවිතා කළ හැකි බවත් ඔවුන් ප්‍රකාශ කර සිටියා.

iPhone 11 Pro ජංගම දුරකථනය ඩොලර් 999කට, සහ iPhone 11 Pro Max ජංගම දුරකථනය ඩොලර් 1099ක මුදලකටත් සැප්තැම්බර් 20 වෙනිදා සිට බෙදාහැරීමට ඔවුන් සූදානම් බවත් සඳහන් කළා.

මේ වෙද්දීත් මේ event එක සහ අලුත් දුරකථන පිළිබඳව විශාල කතා බහක් ඇති වී තිබෙනවා. ඒ වගේම මේ දුරකථනවල ක්‍රියාකාරීත්වයත්, design එක පිළිබඳවත් හොඳ වගේම නරක ප්‍රතිචාරත් ලැබෙනවා. ඔබ මේ ගැන මොකද හිතන්නේ? පහළින් comment කරන්න අමතක කරන්න එපා.

Google සමාගම තමන්ගේ යටතේ පවතින play store එක කෙතරම් ආරක්ෂාකාරීව තබා ගන්න උත්සාහ කළත් හානිදායක apps කෙසේ හෝ එතුළ ක්‍රියාත්මක වීමට මාර්ගයන් සොයාගන්න බව නැවතත් පැහැදිලි වුණේ පසුගිය දිනෙක හඳුනාගන්නා ලද ‘the Joker’ Malware එක සමග යි. මේ malware එක පසුගිය දිනක් වෙනතුරුම හඳුනාගැනීමට හැකියාව ලැබී තිබුනේ නැහැ. apps 24ක් තුළ මෙය ක්‍රියාත්මක වෙමින් තිබුණු බවට Aleksejs Kuprins නම් පරිගණක ආරක්ෂණ පර්යේෂකයා අනාවරණය කර ගැනීමට සමත් වුණා. පහත සඳහන් වෙන්නේ දැනට මේ මැල්වෙයා එක අඩංගු වූ බවට හඳුනාගත් Android apps.

මේ applications ඔබේ ජංගම දුරකතනයෙත් අඩංගු වෙනවා නම් වහාම එය ඉවත් කර ප්‍රති වයිරස aplication එකක් install කරගන්න ලෙස අපි ඔබට මතක් කරනවා. කොහොම වුණත් google සමාගම මේ මැල්වෙයාර් එක හඳුනාගෙන playstore වෙතින් ඉවත් කරවන විටත් අදාළ apps downloads 472,000 පසු කර තිබුණු බව වාර්තා වෙනවා. මේ මැල්වෙයාර් එක මඟින් සිදු වෙන්නේ දුරකථන පරිශීලකයාගේ අනුදැනුමකින් තොරව විවිධ සේවාවන් register කර, ඒවා වෙත මුදල් ලබාගන්න බව හඟවමින් ඔවුන් ගෙන් මුදල් ලබා ගැනීම යි (පරිශීලකයෙකු ලියාපදිංචි වීමට සිදුවන ක්‍රියාවලිය අනුකරණය කිරීම යි). ඒ වගේම මේ malware එකට ඔබේ දුරකතනයට එන ගෙවීම් තහවුරු කරන sms පණිවුඩ ඔබේ අවසරයකින් තොරව හඳුනා ගනිමින් පිටපත් කර ගන්නට ද හැකියාව තියෙනවා.

Kuprinsට අනුව මේ මැල්වෙයාර් එක රටවල් 37ක පමණ දැඩිලෙස පැතිර තිබෙනවා. කෙසේ වෙතත් දැනට මේ මැල්වෙයාර් එක ආසාදනය වී ඇති බවට හඳුනාගත් apps සියල්ලම ඉවත් කිරීමට google සමාගම කටයුතු කර තිබෙනවා. ඔබ මේ apps ඔබේ දුරකතනයට install කර ඇති නම් ඔබේ online ගිණුම්වල සහ බැංකු ගිණුම්වල සැක කටයුතු subscription වැනි දේවල් පිළිබඳව අවධානයෙන් පසුවිය යුතු බව ඔහු සඳහන් කරනවා.

පෙරත් මෙවැනිම සිදු වීම් කිහිපයක්ම වාර්තා වුණා. ඔබට මතක ඇති, “Play Store එකෙන් apps ගන්නේ බලාගෙන යි” වැනි ලිපි හරහා අප ඒ පිළිබඳව ඔබට තොරතුරු ගෙන ආවා. තාක්ෂණික ලෝකයේ ජිවත් වෙන ඔබ හැමදේම පිළිබඳව අවධානයෙන් සිටීම ඉතාම වැදගත්.

2019 වසර වන විට අන්තර්ජාලයේ ඇති වෙබ් අඩවි සංඛ්‍යාව බිලියන 1.94ක් පමණ වන බව වාර්තා වෙනවා. මේ වෙබ් අඩවි අතරින් අපේ වැඩ පහසු කරගන්න හැකියාව ලබා දෙන වෙබ් අඩවි තියෙන්නේ බොහොම සුළු ප්‍රමාණයක්. අන්තර්ජාලයේ නිතර දෙවේලේ සැරිසරණ ඔබට අතිශයින් වැදගත් වෙන වෙබ් අඩවි 10ක් පිළිබඳව යි මේ ලිපිය හරහා දිගහැරෙන්නේ.

අන්තර්ජාලය තුළ විවිධ සේවාවන් භාවිතා කරද්දී ඒවා වෙත sign in වීමට සිදු වෙනවා. නමුත් මේ sign in වීම හරහා ඔබට ඒ සේවාවේ විවිධ email පණිවිඩ වැනි දේ වගේම විවිධ ප්‍රචාරණ email ආදිය පැමිණෙන්නට බොහෝ ඉඩ කඩ තියෙනවා. මේ සේවාව ඔබ භාවිතා කරන්නේ එක වරකට පමණක් නම් එවැනි email පණිවිඩ තමන්ගේ පෞද්ගලික හෝ රාජකාරී විද්‍යුත් ලිපිනයන් වෙත පැමිණීම කරදරයක්. මෙයට හොඳම විසඳුම නම් තාවකාලික විද්‍යුත් ලිපිනයක් භාවිතා කිරීම යි. මේ වගේ සේවාවන් සපයන වෙබ් අඩවි ගණනාවක් තියෙනවා. 10MinuteMail කියන්නේ එවැනි සේවාව සපයන එක් වෙබ් අඩවියක්. මේ වෙබ් අඩවිය හරහා විනාඩි 10කට පමණ තාවකාලික විද්‍යුත් ලිපිනයක් සකසා දෙනවා. එය කල් ඉකුත් වෙන තෙක් එය හරහා වැඩ කරගන්න ඔබට හැකියාව තියෙනවා.

මුදල් ගෙවා ලබා ගත යුතු මෘදුකාංග සහ සේවාවන් බොහොමයක් අප භාවිතා කරන්නේ cracked මෘදුකාංග (චෞර මෘදුකාංග) විදිහට යි. එය නීතියට අනුව දඬුවම ලැබිය හැකි වරදක්. ඉතින් එසේ එම සේවාවන් සහ මෘදුකාංග භාවිතා නොකර, ඒ වෙනුවට වෙනත් විකල්ප සේවාවක් භාවිතා කරන්නට ඔබට හැකියාව මේ වෙබ් අඩවිය හරහා ලැබෙනවා. alternativeto නමින් හැඳින්වෙන මේ වෙබ් අඩවිය හරහා ඔබට මුදල් ගෙවා ලබා ගන්න බොහොමයක් මෘදුකාංගවලට විකල්ප මෘදුකාංග සොයාගන්න වගේම බාගත කරගන්නත් මඟපෙන්වීම සිදු කරනවා. ඒ වගේම ඒ මෘදුකාංගය භාවිත කරන්නන්ගේ reviews පවා මේ වෙබ් අඩවිය හරහා බලාගන්න ඔබට පුළුවන්.

පන්ති කාමරයකට සීමා වී සිදු කරන ඉගෙනගැනීම් මේ වන විට අභාවයට යමින් පවතිනවා. ඔබට අවශ්‍ය සියලු දේ එසැනින් ඔබ අසලට ගෙන එන අන්තර්ජාලය හරහාම ඔබට ඉගෙනගැනීම් කටයුතු වඩාත් පලදායි ලෙසින් සිදු කරගන්නට දැන් අවස්තාව තියෙනවා. E- Learning / web learning / Web teaching වගේ සංකල්පයන් අද ලෝකයේ භෝ රටවල් භාවිතා කෙරෙනවා. මේ වෙද්දී ලංකාව තුලත් යම් මට්ටමකට ආන්තර්ජාලය භාවිතයෙන් දුරස්ථව සිදු කෙරෙන ඉගෙනගැනීම් සහ ඉගැන්වීම් පිළිබඳව ප්‍රචලිත වෙමින් පවතිනවා. නමුත් මෙවැනි සේවාවන් ලබා ගන්න ඔබට යම් මුදලක් ගෙවන්න සිදු වෙනවා උදාහරණයක් විදිහට udemy.com හඳුන්වන්න පුළුවන්. මෙහි ඉතා සීමිත cources ප්‍රමාණයක් නොමිලයේ ලබාගන්න හැකියාව තිබුණත් අනෙක් cource ඉගෙනීමට යම් මුදලක් ගෙවන්නට ඔබට සිදු වෙනවා. මිට වෙනස්ව ඉතාම අඩු මුදලකට සහ නොමිලයේ විවිධ අංශයන් යටතේ ඉගෙනීමට හැකි වෙබ් අඩවියක් khanacademy. ඕනෑම වයසක පුද්ගලයෙකුට මේ හරහා සිය ඉගෙනීමේ කටයුතු සිදු කරගන්නට හැකියාව තියෙනවා. මේ වෙබ් අඩවිය හරහා මාපියන්ට වුවත් parenting වැනි මාතෘකා පිළිබඳ දැනුම ලබාගත හැකියි.

අන්තර්ජාලය හරහා භාණ්ඩ හා සේවාවන් මිල දී ගන්න පුද්ගලයින්ගෙන් 95% දෙනා ඒවායේ ඇති Reviews මත තමයි මේ භාණ්ඩය මිල දී ගන්නවා ද නැද්ද යන්න තීරණය කරන්නේ. නමුත් අද වෙන විට යම් යම් වෙළෙඳුන් විසින් විවිධ bot වර්ග වැනි මෘදුකාංග භාවිත කරමින් ව්‍යාජ reviews නිර්මාණය කරමින්, තමන්ගේ භාණ්ඩ ප්‍රවර්ධනය කිරීමට උත්සාහ දරනවා. මෙවැනි ව්‍යාජ රිවිව්ස් හෙළි කරන වෙබ් සේවාවක් තමයි fakespot කියන්නේ. බොහෝ දෙනෙක් සුලභව භාවිතා කරන amazon, bestbuy, steam, sephora වැනි වෙබ් අඩවි ගණනාවකට මෙය සහාය දක්වනවා. ඔබට කරන්න තියෙන්නේ ඔබ මිල දී ගන්නා භාණ්ඩයේ link එක මෙහි search bar එක මත paste කිරීම පමණ යි. එවිට ඒ වෙබ් අඩවිය මඟින් භාණ්ඩය A සිට F දක්වා rate කිරීමකට ලක් කරනවා.

වෙබ් ලිපිනයක් හෝ file එකක ඇති වයිරසයන් ඉතාම පහසුවෙන් හඳුනාගන්නට පහසුකම් සලසන වෙබ් අඩවියක් ලෙසින් Virustotal වෙබ් අඩවිය හඳුන්වන්නට පුළුවන්. ඔබට අවශ්‍ය file එක වෙබ් අඩවිය වෙත upload කිරීම හරහා එහි වයිරස තිබේ ද යන්න සොයාගැනීමට හැකියි. ඒ වගේම විවිධ වෙබ් ලිපිනයන්වල වයිසරයන් ඇතිදැ යි සොයා ගන්නත් මේ වෙබ් අඩවිය ඔබට උපකාරී වෙනවා. වයිරස ඇති බව හෝ අනතුරුදායක බව virustotal මඟින් දැනුම් දුන්නොත්, අදාළ වෙබ් අඩවිය මඟහරින එක නුවණට හුරු යි.

90 දශකයේ සිටම ලෝකයේ අතිශය ජනප්‍රිය Westlife කණ්ඩායම ගැන ඔබ මේ කරුණු දන්නවා ද?

Facebook සහ instagram වලින් Like count එක පෙන්වීම ඉවත් කිරීමට facebook සමාගම කටයුතු කිරීම සම්බන්ධව පසුගිය කාලය පුරාවට යම් යම් මතයන් පළවුනා. මේ ආරංචි පිළිබඳව පක්ෂව වගේම එයට අකමැත්තක් දවන විශාල පිරිසකුත් සිටින නිසාවෙන් මේ පිළිබඳව විශාල කතාබහක් ගොඩ නැගුණා. කොහොම වෙතත් මේ ආරංචිය සනාත කරවන පුවතක් පසුගිය දෙවැනි දා දැනගන්නට ලැබුණා. මෙයට හේතුව ලෙසින් සඳහන් facebook සමාගම සඳහන් කරන්නේ ඔබව follow කරන පුද්ගලයින් හට ඔබට ලැබෙන likes ප්‍රමාණය වැදගත් නොවෙන නිසාත්, likes count එක මතම පමණක් යම් content එකක ගුණාත්මකභාවය මැනීම සිදු නොවිය යුතු නිසාත් මේ පියවර ගෙන ඇති බව යි.

මේ මෙය දැනට ක්‍රියාත්මක වීමට නියමිත instagram සඳහා පමණයි. නමුත් මෙය facebook සමාජ ජාලය වෙතත් සිදු වෙන්නට හැකි බව Facebook Android App එකේ Source Code එක පදනම් කරගෙන ප්‍රකාශයක් නිකුත් කරන ඉංජිනේරු විශේෂඥයෙකු වන ජේන් වොන්ග් සඳහන් කර තිබුණා.

TechCrunch ඇතුළු තාක්ෂණික ප්‍රවෘත්ති සපයන වෙබ් අඩවි කිහිපයක් කළ විමසීම්වල දි මේ තීරණය ගැන facebook ආයතනය තහවුරු කිරීමක් සිදු කර තිබෙනවා. නමුත් මෙය facebook සමාජ ජාලය වෙත පරික්ෂා කිරීම තවමත් අරඹා නැති බවත් ඔවුන් ප්‍රකාශ කර තිබුණා. මේ අනුව අදාල post එක share කළ, post එකේ හිමිකරුට පමණක් like count එක (ප්‍රමාණය) දැකගත හැකි වනු ඇති අතර, අනෙක් පුද්ගලයන් හට දැකගත හැකි වනුයේ අදාල post එකට like කරනු ලැබූ mutual friendsලා ගේ නම් පමණයි. තවමත් පර්යේෂණ මට්ටමේ පවතින නිසාවෙන් commentsවලට වැටෙන likes සහ reaction ප්‍රමාණය පෙන්වීම සිදු වෙනවා.

මෙය තාමත් නිල වශයෙන් ක්‍රියාත්මක වෙන දිනයක් නිශ්චිතව සඳහන් වෙන්නේ නැහැ. නමුත් මේ තීරණය පිළිබඳව යම් මට්ටමක අප්‍රසාදයක් ගොඩනැගෙමින් තිබෙන බවත් වාර්තා වෙනවා. මේ තීරණය පිළිබඳව ඔබ හිතන්නේ මොකක්ද? පහළ comment section එක ඒ වෙනුවෙන් විවෘත යි.

'Blu' macaw කියපුවම හැමෝටම මතක් වෙන්නෙ Rio Animation Film එකේ ඉන්න ගිරවාව. නමුත් මේ ගිරවා වඳ වී ගිය සත්ත්වයෙක් ලෙසින් නම් කෙරුණා.

දුක්ගැහැට පිරුණු ජීවිතය වසර ගණනාවක් ගෙවා හදිසියේම බොලිවුඩයේ තාරකාවක් වන්නට වරම් ලැබූ තැනැත්තියක්, රනූ මොන්ඩාල්.

ලෝකයේ බහුතරයක් දුරකථන, පරිගණක වැනි උපාංග භාවිතා කරන පිරිසට අතිශය වැදගත් වෙන පහසුකමක් තමයි Bluetooth කියන්නේ. නමුත් තවදුරටත් Bluetooth භාවිත කිරීම ඔබේ දුරකතනයට එතරම් ආරක්ෂාකාරී නොවන වග පසුගිය දිනෙක අනාවරණය වුණා. මේ ලිපිය හරහා මේ තත්ත්වය පිළිබඳව වගේම Bluetooth ඉතිහාසය පිළිබඳවත් තොරතුරු ඔබ වෙත ඉදිරිපත් වෙනවා.

මේ තාක්ෂණයෙ නිර්මාතෘ විදිහට සැලකෙන්නේ Jaap Haartsen. ඔහු 90 දශකයේ Ericsson සමාගමේ සේවය කළ අයෙක්. UHF radio wave භාවිතයෙන් උපාංගයන් දෙකක් අතර දත්ත හුවමාරු කර ගැනීමට හැකි බවට කළ සොයාගැනීම තාක්ෂණික ලෝකයේ පෙරලියක් බවට පත් වුණා. මුල් අවධියේ දී MC හෙවත් Multi Communicator link වැනි නාමයන් භාවිතා වුණත්, පසු කාලීනව මෙයට Bluetooth යන නාමය යෙදෙන්නේ ඓතිහාසික සිදුවීමක් පසුබිම් කරගෙන ය. ඒ දහවැනි සියවසේ විසූ බවට සැලකෙන Harald Bluetooth නම් රජ කෙනෙකුට ගෞරව කිරීම පිණිස යි. රූනික් හෝඩියේ අකුරු දෙකක් වූ (ᚼ, Hagall) and (ᛒ, Bjarkan) එකතු කර bluetooth ලෝගෝව නිර්මාණය කර තිබේ.

bluetooth පහසුකමේ තිබෙන දුර්වලතාවයක් පසුගිය දිනෙක අනාවරණය කර ගනු ලැබුවා. Bluetooth තාක්ෂණය භාවිතා කරමින් devices දෙකක් සම්බන්ධ වන අවස්ථාවේ දී පිටස්තර පුද්ගලයෙකු හට මෙම දුර්වලතාවය අදාල devicesවල දත්ත ලබාගැනීම සඳහා, සහ ඒවා පාලනය කිරීම සඳහා භාවිතා කළ හැකි වෙනවා. බ්ලූටූත් තාක්ෂණය භාවිත කරමින් උපාංග දෙකක් එකිනෙක සම්බන්ධ කිරීමේ දී connection එක ආරක්ෂා කරගැනීමට encryption keys භාවිතා වෙනවා. නමුත් මෙම දුර්වලතාවය නිසා ඒ keys වෙනුවට ඊට වඩා ආරක්ෂාවෙන් අඩු වෙනත් key එකක් එතන වෙත දැමීමට හැකියාව ලැබෙනවා. මේ attacking ක්‍රමවේදය Key Negotiation of Bluetooth (KNOB) ලෙසින් හඳුන්වනවා.

කෙසේ වෙතත් එම අවස්ථාවේ දීම උපාංගය hack වීමක් සිදු නොවුනත් brute-force මාදිලියේ ප්‍රහාරයකින් ඉතාම පහසුවෙන් උපාංගවල පාලනය ලබා ගැනීමට hacker වරයාට අවස්තාව ලැබෙනවා. Bluetooth Special Interest Group (Bluetooth තාක්ෂණය පිළිබඳ standards නිර්මාණය කරන ආයතනය) වෙත මෙය නිවැරදි කිරීමට හැකියාවක් නොමැති බවත් සඳහන් වෙනවා. කෙසේ වෙතත් මේ වන විට Microsoft සමාගම විසින් Windows වලටත්, Cisco සමාගම විසින් IP Phones සහ Webex වලටත්, Google සමාගම විසින් Android වලටත්, Apple සමාගම විසින් macOS, iOS සහ watchOSවලටත් මෙන්ම Blackberry සමාගම විසින් ඔවුන්ගේ ජංගම දුරකතනවලටත් මේ වෙනුවෙන් security updates නිකුත් කර අවසානයි. එනිසාවෙන් මේ අවධානමෙන් ගැලවෙන්න ඔබේ පරිගණකයේ හෝ ජංගම දුරකතනයේ මෙහෙයුම් පද්ධතියේ නවතම version එක වෙත යාවත්කාලින කර ගත යුතු යි.

Android මෙහෙයුම් පද්ධතිය smart ජංගම දුරකථන භාවිතා කරන බොහෝ දෙනා අතරේ අතිශය ජනප්‍රිය මෙහෙයුම පද්ධතියක්. මෙහි ආරම්භයේ සිටම ඉංග්‍රීසි හෝඩියේ අකුරු තිබෙන පිළිවෙලට සෑම Android සංස්කරණයක් හැඳින්වීම සඳහාම අතුරුපසක නමක්, එහෙම නැති නම් රසකැවිල්ලක නමක් භාවිතා වුණා. කොහොම වුණත් මේ කාරණය Android Qවල සිට වෙනස් වෙනවා. Android 10 ලෙසින් ඉදිරියට පැමිණෙන android සංස්කරණය හැඳින්වෙන අතරම ඉදිරියේ දීත් පහසුවෙන් අලුත්ම සංස්කරණය කුමක්දැ යි හඳුනාගත හැකි ආකාරයට නම් කිරීමටත් Google සමාගම තීරණය කර තිබෙනවා.

මේ පිළිබඳව නිල Blog අඩවිය හරහා නිවේදනයක් නිකුත් කරමින් ඔවුන් සඳහන් කරන්නේ android මෙහෙයුම් පද්ධතිය බිලියන 2.5ක පමණ active devicesහි භාවිතා වන global operating system එකක් නිසාවෙන් ලෝකයේ ඕනෑම අයෙකුට පහසුවෙන් තේරුම් ගත හැකි අන්දමින් මේ නාමකරණය වෙනස කිරීමට ඔවුන් තීරණය කළ බව යි. එසේම ඔවුන් භාවිතා කරන සමහර අතුරුපස වර්ග ලෝකය පුර එක ලෙසින් ජනප්‍රිය නොවන නිසා මෙන්ම අලුත්ම Android සංස්කරණය කුමක් ද යන්න සෘජුවම සොයාගත නොහැකි වීම වැනි ගැටළු මතුවීම මඟහරවා ගැනීමත් මේ නාමකරණය වෙනස් වීමට බලපා තිබෙනවා. මේ වෙනස්වීම සමග ඔවුන් ඔවුන්ගේ logo එකත් වෙනස් කිරීමට තීරණය කර තිබෙනවා. මෙලෙසින් සිදු වන්නේ 2014 වසරෙන් පසුව යි. කොළ වර්ණය, Android Robot ගේ හැඩය මෙන්ම අකුරුවල වර්ණය ද මේ අනුව වෙනස් වනු ඇති.

ඉදිරි සති කිහිපය තුළ දී නිකුත් වීමට නියමිත Android stable release එක සමගින් මේ අලුත් logo එක සහ color scheme භාවිතය ආරම්භවීමට නියමිත යි.

Facebook සමාගම Instagram සහ whatsapp මිල දී ගැනීමෙන් අනතරුව විශාල වෙනස්කම් රාශියක් සිදු කරනු ලැබුවා. මේ කියන්න යන්නේ ඔවුන් සිදු කරන්නට යන අලුත්ම වෙනස්කම පිළිබඳව යි. ලෝකයේ බොහෝ දෙනෙකු භාවිතා කරන Instagram සහ whatsapp සේවාවන් දෙක හඳුන්වන නාමයන් වෙනස් කිරීමට facebook සමාගම තීරණය කර තිබෙනවා.

Instagram 2012 අප්‍රේල් 9 වැනිදාත්, 2014 පෙබරවාරි 14 whatsapp සේවාවත් මිල දී ගැනීමෙන් අනතුරුව, එම සේවාවන් දෙකෙහි වර්ධනය විශාල වශයෙන් ඉහළ ගොස් තිබෙනවා. මේ වර්ධනයට ප්‍රමාණවත් තරමින් facebook ආයතනයට ගෞරවයක් හිමි නොවීම පිළිබඳව එහි CEO Mark Zuckerberg එතරම් සතුටට පත් නොවන බවයි දැනගන්නට ලැබෙන්නේ. ඒ නිසාවෙන් Facebook නාමය වඩාත් ප්‍රචලිත කිරීම අරමුණු කරගෙන යෝජිත වෙනස්කම සිදුවණු ඇත. Facebook නාමය අදාල සේවාවන් සමග සම්බන්ධ කිරීම ඉතාම ඉක්මනින් සිදු කිරීමට මේ වන විටත් තීරණය කර අවසන්. මේ අනුව Instagram සහ whatsappහි නාමයන් සමග facebook නාමය ද යෙදීමට ඔවුන් කටයුතු කරමින් සිටිනවා. දැනට Instagram ලෙස පවතින නම "Instagram from Facebook" ලෙසත්, WhatsApp, "WhatsApp from Facebook" ලෙසත් ඉදිරියේ දී හැඳින්වෙන බව The Information වෙබ් අඩවිය වාර්තා කර තිබුණා. එය facebookහි සේවය කරන්නන් විසිනුත් සනාත කර තිබූ බව වාර්තා වෙනවා.

නම් වෙනස් කිරීමෙන් අනතුරුව Google Play Store සහ Apple App Storeවල Instagram from Facebook සහ WhatsApp from Facebook ලෙස නම දර්ශනය කිරීමට කටයුතු කරනු ඇති අතර App එක open කරනු ලබන අවස්ථාවේ දී දර්ශනය වන splash screen එක මත ද මේ අලුත් නම් දර්ශනය කිරීමට නියමිත යි. කෙසේ වෙතත් device එකේ home screen එක හෝ app drawer එක මත සුපුරුදු පරිදි Instagram සහ whatsapp ලෙසින් දර්ශනය වේවි. මේ අලුත් වෙනස්කම තවත් සේවාවන් කිහිපයකටම සිදුවණු ඇති බව තමයි වාර්තා වෙන්නේ. මේ වන විටත් Facebook ආයතනය විසින් 2014 මිල දී ගැනුණු Oculus සඳහා මේ වෙනස්කම සිදු කර ඇති බව දැනගන්න ලැබෙනවා. එහි දර්ශනය වෙන්නේ Oculus from Facebook ලෙසිනුයි.

Microsoft සහ apple සමාගම් අතර ප්‍රචාරණ යුද්ධය නැවතත් ආරම්භ වී තිබෙනවා. මේ ප්‍රචාරණ යුද්ධය කාලයකට පෙරත් ඉතාම දීර්ඝ ලෙසින් පැවතුනා. මෙය නැවත ආරම්භ වීමට හේතුව බවට පත් වෙන්නේ Surface Laptop 2 එක වෙනුවෙන් microsoft සමාගම නිෂ්පාදනය කරන ලද වෙළඳ දැන්වීමක්.

මේ වෙළඳ දැන්වීමේ පෙනී සිටින පුද්ගලයාගේ සැබෑ නම වෙන්නේ Mackenzie Book නම් වන අතර, "Mac Book” යනුවෙන් ඔහුව මිතුරන් අතරේ හඳුන්වනු ලබනවා. මේ වන විටත් මේ Videoව හරහා ඔවුන්ගේ Surface Laptop 2 පරිගණකය වෙත විශාල ප්‍රසිද්ධියක් ලබා දීමට Microsoft ආයතනයට හැකි වී තිබෙනවා. ඕස්ට්‍රේලියානු ජාතිකයෙකු වූ මේ පුද්ගලයා Macbook පරිගණකය සමග Surface Laptop එක සංසන්දනය කරමින් මැක් පරිගණකයට වඩා Microsoft Surface Laptop 2 එක හොඳ බව පෙන්වා දෙනවා. අවසානයේ “You should get a Surface — trust me, I’m Mac Book,” ලෙසින් ද පවසනවා. මේ වෙළඳ ප්‍රචාරණ යුද්ධය අද ඊයේ ආරම්භ වූවක් නොවෙයි. අද කාලයක් පුරාවට පැවතුන එකක්.

මේ වැනි විවිධ මඩ ගසාගැනීම් ප්‍රමුඛ පෙළේ සමාගම් අතර සුලභව සිදුවන දෙයක්. එක එක සමාගම්වල අඩුපාඩු හෝ විවිධ උපාංගවල අඩු ලුහුඬුකම් පෙන්වා දෙමින් තමන්ගේ සන්නාමයේ උපාංග මිල දී ගන්නා ලෙස මූලික වශයෙන් මේ වෙළඳ දැන්වීම් බොහොමයක සඳහන් වෙනවා. මෑත කාලීනව විශාලව ප්‍රසිද්ධියට පත් වූ samsung ingenious campaign එක ඔබට මතක ඇති.

මෙවැනි වෙළඳ දැන්වීම්වලට අමතර තවත් විවිධ ප්‍රචාරණ උපක්‍රම භාවිත කරන්නට ලෝකයේ අතිශය ජනප්‍රිය සමාගම් පෙළඹෙනවා. වරෙක huawei සමාගම නවතම ඇපල් ජංගම දුරකථනය මිල දී ගැනීමට පෝලිමේ සිටි Apple fansලා හට power banks ලබා දී තිබුණා. ඒ “ Here's a power bank you'll need it” යන පාඨය සමග යි.

ඔබ දුරකතනයක් හෝ යම් උපාංගයක් මිල දී ගන්නවා නම් මෙවැනි ප්‍රචාරනයන් නිසාවෙන් පමණක් එය මිල දී ගැනීම එතරම් හොඳ දෙයක් නම් නෙවෙයි. ඔබ මිල දී ගන්නා භාණ්ඩයේ Reviews පිළිබඳව වගේම එය භාවිතා කර තිබෙන පුද්ගලයන්ගේ user reviews වැනි දේ පිළිබඳව යම් අධ්‍යයනයකින් අනතුරුව යම් මිල දී ගැනීමක් සිදු කිරීම නුවණට හුරු යි.

ලංකාවට ඇවිත් ඩොලර් 1000ක තේ බිව්ව Harald Baldr සුදු මහත්මයා ගැන ඔබ දන්නවද ?

බීඩි, ලංකාවේ අඩු ආදායම්ලාභීන් අතර ප්‍රසිද්ධියක් උසුලන දුම්වැටි වර්ගයක්. තරමක් දැඩි ගන්ධයක් සහිත වුවත් සාමාන්‍ය සිගරෙට්ටුවක මිලෙන් දහයෙන් පංගුවකටත් අඩුවෙන් මිලට ගත හැකි නිසා බීඩි ලංකාවේ උප සංස්කෘතියක් බවට පත්වී හමාර යි.

බීඩි සෑදීමේ හා ඒවායේ දුම් ඉරීමේ පුරුද්ද ආරම්භ වූ බවට සැලකෙන්නේ 17 වන සියවසේ අග භාගයේ දී යි. ඒ දුම්කොළ සහ ඒ ආශ්‍රිත නිෂ්පාදන සිදු කරන ඉන්දියාවේ ගුජරාටයේ කේදා සහ පන්ච්මැහැල් දිස්ත්‍රික්කයන් ආශ්‍රිතව යි. ඒ කාලයේ ජනප්‍රියව පැවති, භාවිතයට තරමක් කරදරකාරී හූකා වෙනුවට කම්කරුවන් ඉතිරිවන දුම්කොළ කුඩු “කඳුකර කළුවර” නම් ගසක කොළයක ඔතා පානය කිරීමට පුරුදු වුණා. 19 වන සියවස පමණ වන තෙක්ම මෙය poor man’s cigarette (දුප්පත් මිනිසුන්ගේ සිගරට්) ලෙසින් ඉන්දියාවේ ව්‍යාප්තව තිබුණා. විශේෂයෙන්ම ඉන්දියාවේ ගුජරාත් ප්‍රාන්තයේ මේ “දුප්පත් මිනිසුන්ගේ සිගරට්” වෙත තිබූ ජනප්‍රියත්වය දුටු සිගරට් නිෂ්පාදකයන්, සාමාන්‍ය සිගරට් මෙන්ම මේවා ද තනා අලෙවි කිරීම ආරම්භ කළා.

මෙම කර්මාන්තය විධිමත් කිරීමේ ගෞරවය හිමිවන්නේ ගුජරාත් ප්‍රාන්තයේ සොහොයුරන් වන මෝහන්ලාල් සහ හර්ගෝවින්දාස් පටෙල් (Mohanlal, Hargovindas Patel) වෙත යි. ඔවුන් මධ්‍යම ඉන්දියාවේ ජබල්පූර්හි බහුල වශයෙන් ලබා ගත හැකි දේශීය තෙන්දු (කළු තිඹිරි) කොළ භාවිතයෙන් බීඩි එතීමේ වාසි හඳුනාගත්තා. වියලි තෙන්දු කොළ මඟින් බීඩි එතීමේ දී සුරුට්ටුව ඉරිතැලීම හෝ කැඩී යාම සිදු නොවන අතර, එමඟින් බීඩි වෙත අපූර්ව රසයක් ද එකතු වෙන නිසාවෙන් පටෙල්වරුන්ගේ බීඩි ව්‍යාපාරය ඉතා ඉක්මණින් සාර්ථක වුණා. ඔවුන්ගේ සූත්‍රය ඉන්දියාව පුරා අනෙකුත් නිෂ්පාදකයින් විසින් ද අනුගමනය කෙරෙන්නට පටන් ගත්තා.

20 වෙනි සියවස පමණ වන විට මේ කර්මාන්තය ඉන්දියාවේ නැතිවම බැරි කර්මාන්තයක් බවට පත් වී අවසාන යි. හින්ද්මාතා (Hindmata) වැනි බීඩි සන්නාමයන් ඉන්දියානු ජාතිකත්වය උපයෝගයෙන් තමන්ගේ ව්‍යාපාරය ඉන්දියාව පුරාම ව්‍යාප්ත කළා. මේ අතරට Mother India, සිංහයන්, මහත්මා ගාන්ධි සංකේතයන්, සහ ජාතික ධජයේ වර්ණ භාවිතය සිදු වුණා

ලංකාවේ බීඩි ප්‍රචලිත වීම ආරම්භ වූ බව සැලකෙන්නේ ලංකාවේ තේ කර්මාන්තයට ඉන්දීය ද්‍රවිඩ ජනතාව පැමිණීමත් සමග යි. “සෙයියදුරාජා කඩප්පුලී” යන සන්නාමයක් යටතේ ලංකාවට මුලින් ආනයනය වූ බීඩි පසු කාලීනව ලංකාවේම නිෂ්පාදනය ආරම්භ වෙනවා.

බීඩි ලංකාවේ ජනප්‍රියත්වයට පත් වන්නේ ඈත කලෙක වුණත්, අද වෙද්දීත් බීඩි කර්මාන්තය තරමක් අවිධිමත්ව සිදු වෙනවා. Social Development Network (SDN) එකට අනුව වසරකට නිපදවෙන බීඩි ප්‍රමාණය බිලියන 2.5ක් පමණ. නමුත් 2018 වසරේ පමණක් බීඩි බිලියන 4.5ක් පමණ නිෂ්පාදනය වී ඇති බව Ceylon Tobacco Company (CTC)හි අවසාන කාර්තුමය වාර්තාව ඇස්තමේන්තුවේ සඳහන්. ඒ අනුව බීඩි බිලියන 2කට අධික ප්‍රමාණයක් හොරෙන් ආනයනය කර හෝ එසේ නොමැති නම් රහසිගතව නිෂ්පාදනය කර තිබෙනවා. මෙලෙසින් හොරෙන් ගෙන්වන බීඩි සහ තෙන්දු කොළ නිසාවෙන් ලංකාවේ බීඩි කර්මාන්තයට එල්ල වෙන්නේ විශාල බලපෑමක් බව නම් කිව යුතු යි.

මෙලෙසින් හොරෙන් ගෙන්වන බීඩි සහ අමුද්‍රව්‍ය ගුවන්තොටුපළවල් සහ වරාය රේගුව මඟින් අත් අඩංගුවට පත් වෙන වාර ගණන විශාල යි.

බීඩි නිසාවෙන් ඇතිවන සෞඛ්‍ය ගැටළු ප්‍රමාණය නම් අති විශාල බව මතක් කළ යුතු තවත් කරුණක්. බීඩි සුරුට්ටුවේ ෆිල්ටරයක් නොමැති නිසා සාමාන්‍ය සිගරට්ටුවකට සාපේක්ෂව ඉතා විශාල තාර සහ නිකොටීන් ප්‍රමාණයක් පානය කරන්නාගේ ශරීරගත වීම සිදු වෙනවා. ඒ වගේම මේ කර්මාන්තයේ නිරත වෙන පුද්ගලයන්ටත් එමඟින් විශාල බලපෑම් සහ සෞඛ්‍ය ගැටළු ඇති වන බව නම් නොරහසක්. කර්මාන්තයේ පවතින අවිධිමත් බව නිසාවෙන් වගේම, බීඩි එතීම බොහෝ විට ගෘහාශ්‍රිතව සිදුවන නිසාත් ප්‍රමාණවත් ආරක්ෂාවක් නොමැති වීම පුදුමයට කරුණක් නොවේ. දුම්කොළවලට දිගු කාලීනව නිරාවරණය වීමෙන් ශරීරයේ කෝටිනින් සහ සැලකිය යුතු මට්ටමකට නිකොටින් තැම්පත් වන අතර ඒවා ඇස් පෙනීමට, සම, සහ ශ්වසන පද්ධතියට දැඩි ලෙස බලපානවා.

කිසිදු ආකාරයක කොන්ත්‍රාත්තුවක් හෝ සෞඛ්‍ය සහ ආරක්ෂක ප්‍රමිතීන්ගෙන් ආවරණය නොවන බීඩි එතීමේ කර්මාන්තයේ යෙදී සිටින පවුල් 8,000කට ආසන්න ප්‍රමාණයෙන් 95%කට වඩා වැඩි ප්‍රමාණයක් කාන්තාවන් බවයි SDN සභාපති ජීව සිරිවර්ධන පැවසුවේ. ළමයින් ද බොහෝ විට වෙළඳාමට සම්බන්ධ වන අතර, ඔවුන්ගේ දෙමාපියන්ට බීඩි රෝල් කිරීමට සහාය වන බව සභාපති සිරිවර්ධන සඳහන් කළා.

සිගරට් සඳහා සිදුවන බදු ඉහළ නැංවීම් හේතුවෙන් සීඝ්‍රයෙන් ඉහළ යන සිගරට් මිල නිසාවෙන්, තරුණයන් බීඩි වෙත විශාල වශයෙන් නැවත යොමු වීමට ඉඩක් පවතිනවා. රුපියල් 70 - 90 අතර මිලකට සිගරට්ටුවක් මිල දී ගැනීමට වඩා, ඒ මිලට බීඩි මිටියක් මිලට ගැනීම ඔවුන්ට ලාභදායි යි. වෙන් වෙන්ව හෝ මිටි වශයෙන් විකිණෙන බීඩිවල කිසිදු ආකාරයක රූපමය අනතුරු ඇඟවීමක් දැකගන්නටත් ලැබෙන්නේ ද නැහැ.

සීඝ්‍රයෙන් ඉහළ යන පාරිභෝජනය සහ සෞඛ්‍ය ගැටළු ඇතිකිරීමේ අවදානම නිසා කර්මාන්තය කළමනාකරණය කිරීම සඳහා පැහැදිලි නියාමනයක් හඳුන්වා දීම සිදුවිය යුත්තක්. සිගරට් මිල ඉහළ දැමීමෙන් පමණක් වාර්ෂිකව බිලියන 7.5කට අධික ආදායමක් රජය උපයන අතර හුදෙක් සිගරට් මිල ඉහළ දැමීම මඟින් පමණක් දුම්පානයෙන් සිදුවන සෞඛ්‍ය ගැටළු සඳහා විසඳුම් සෙවිය හැකි ද යන්න පිළිබඳව ඇත්තේ නම් යම් ගැටළුකාරී තත්ත්වයක්.

Google maps කියන්නේ smart දුරකතනයක්/ පරිගණකයක් තියෙන ඕනෑම කෙනෙකුට නිතර දෙවේලේ සහාය වෙන සේවාවක්. දුර ගමනක් යන කෙනෙකුට මේ සේවාව හරහා ගමනාන්තය වෙත යන්න කෙටිම පාර වගේම, මාර්ගයේ තියෙන වාහන තදබදය සහ ගමනාන්තයට ළඟාවීමට ගතවන කාලයත් ආසන්න වශයෙන් දැනගන්න හැකියාව තියෙනවා. ඒ වගේම අවශ්‍ය නම් street view, සහ අවශ්‍ය නම් satellite තාක්ෂණය භාවිතා කරමින් satellite map එකක් වුණත් බලා ගන්න අපට හැකියාව තියෙනවා. මේ කියන්න යන්නේ google map වෙත අලුතින් හඳුන්වාදුන් පහසුකම් හිහිපයක් පිළිබඳව යි.

ඔබ ගමන් කිරීමට නියමිත බස් රථය හෝ දුම්රිය වැනි පොදු ප්‍රවාහන සේවාවන්වල එම මොහොතේ කෙතරම් සෙනඟ සිටීදැ යි යන්න පිළිබඳව prediction එකක් ලබාදීමේ පහසුකමක් හඳුන්වා දීමට Google සමාගම කටයුතු කර තිබෙනවා. පසුගිය මාස ගණනාවක් පුරාවට google Maps භාවිතා කරන විවිධ පුද්ගලයන්ගෙන් අදාල තොරතුරු එකතු කරගැනීමට Google ආයතනය කටයුතු කර තිබෙන අතර, මේ වන විට අදාල predictions ලබා දිය හැකි ප්‍රමාණයට දත්ත එකතු කර ඇති බව වාර්තා වෙනවා. දැනට නගර 200ක පමණ මේ පහසුකම ක්‍රියාත්මක වෙන බව දැනගන්නට ලැබෙනවා.

කෙසේවෙතත් මේ මඟින් බස් රථයේ සිටින සැබෑ මඟීන්ගේ සංඛ්‍යාව හරි ආකාරයෙන් ගණනය කිරීමක් නොවන අතර, පසුගිය කාලසීමාවක දත්ත පදනම් කරගනිමින් ඊට අදාල අනාවැකියක් පමණක් සපයන බව මතක තබාගත යුතු වෙනවා.

අපට අවශ්‍ය ස්ථානයට ගමන් කිරීමට සෘජුව භාවිතා කළ හැකි බස්/ දුම්රිය වාර ගැන, සහ ඊට අදාල ගත වන කාලසීමාවන් ගැන තොරතුරු ලබා දෙන Google Transit ලංකාව වෙතත් ලබාදෙන්න google සමාගම කටයුතු කළා. මෙහි විශේෂත්වය වන්නේ අදාල ස්ථානයට ගමන් කළ හැකි වෙනත් මාර්ග සහ ඒ සඳහා බස් කිහිපයක් භාවිතා කරමින් ඉතාමත් ඉක්මණින් ගමන් කළ හැකි ආකාරයන් පවා දැනගැනීමට හැකි වීම යි.

මෙහි තොරතුරු යාවත්කාලීන වීම් සිදු කරන්නේ බස්නාහිර පළාත් ප්‍රවාහන අධිකාරිය මඟින් සහ දුම්රිය දෙපාර්තමේන්තුව මඟින්. දැනට බස්නාහිර පළාතේ මේ පහසුකම ක්‍රියාත්මක වෙනවා. කෙසේ වෙතත් මේ සේවාව වඩාත් නිවැරදිව ක්‍රියාත්මක වීමට නම් ඒවා භාවිත කරන පිරිස වැඩි වීම අනිවාර්යය කාරණයක්.

Hacking කිව් විට බොහෝ විට මතකයට එන්නේ පරිගණක, සහ පරිගණක පද්ධති අශ්‍රිතව අවසර නොලත් පුද්ගලයෙකු සිදු කරන හානිකර ක්‍රියාකාරකමක් වන්නට පුළුවන්. නමුත් hacking එතනින් එහාට විහිදුණු බොහොම පුළුල් මාතෘකාවක්. ඇත්තටම හැකර් කෙනෙක් කියන්නේ නරක කෙනෙක් ද? Hacking කියන්නේ භයානක දෙයක් ද? මේ ගැන වගේම, හැකින්ග් ගැන දැනගන්න ආස ඕනෑම කෙනෙකුට ප්‍රයෝජනවත් වන්නට හැකි, 27 දා පැවැත්වෙන Omega CTF Event එක ගැන විස්තර මේ ලිපිය හරහා දැන ගන්න ඔබට පුළුවන් වේවි. මේ පිළිබඳව කතා බහ කරන්න එකතු වුනේ ඔසඳ මලිත් ජයතිස්ස (IT Security Consultant/ Security Researcher)

ඇත්තටම Hacking කියලා කියූ සැනින් ඔබේ මතකයට එන්නේ facebook hacking කියන කතාව. Hacking එතනින් එහාට විහිදුණු බොහොම පුළුල් මාතෘකාවක්. ඇත්තටම ලංකාවේ නොවුණත් ජාත්‍යන්තරය පිළිගත් වෘත්තියක් විදිහට හැකින් සලකනවා. යම් සමාගමක් හෝ ආයතනයක් ඕනෙම system එකක් නිර්මාණය කරන්ගෙන යද්දී ඕනෑම පද්ධතියක දෝෂ හටගන්න හැකියාව තියෙනවා. ඒ දෝෂ පසුකාලීනව පද්ධතියේ ආරක්ෂාවට පවා තර්ජනයක් වෙන්නට පුළුවන්. මේ දෝෂ හඳුනාගෙන ඒ පද්ධතිය ආරක්ෂාව පරික්ෂා කිරීමට ආයතනය විසින්ම හැකර්වරුන් සේවයට යොදවා ගන්නවා. Pentesting කියලත් මේ කටයුත්ත හඳුන්වනවා. මේ කටයුත්ත සිදු වෙන්නේ සමාගම සමග අදාළ හැකර්වරයා ඇති කරගන්න නීතියමය ගිවිසුමකින් අනතුරුව යි. සරලවම මොවුන් white hat hackers ලෙසින් හඳුන්වනවා.

කොහොමද හැකර් කෙනෙක් වෙන්නේ?

හැකර් කෙනෙක් කියන්නේත් සාමාන්‍ය පුද්ගලයෙක්. නමුත් ඔහු සතුව සුවිශේෂී හැකියාවන් පවතිනවා. සාමාන්‍යයෙන් හැකර් කෙනෙක් බවට පත් වෙන්න නම් බොහෝ අංශයන් පිළිබඳව දැනුමක් අවශ්‍ය වෙනවා. උදාහරණයක් විදිහට හැකර් කෙනෙක් වෙන්න තොරතුරු තාක්ෂණ අංශවල එක අංශයකින් පමණක් හැකි වෙන්නේ නැහැ. ඒත් ඔබ ඉගෙනගන්න පටන් ගන්නවා නම් පොඩි තැනකින් පටන් ගන්න. ඒ විෂයය කරුණු ඔබට ප්‍රායෝගික භාවිතයේ දී අනිවාර්යයෙන්ම වැදගත් වෙනවා. හැබැයි පොත් කියවලා, විභාග කරලා, උපාධි-ඩිප්ලෝමා සහතික අරගෙන විතරක් හැකර් කෙනෙක් වෙන්න බැහැ. මොකද, සාමාන්‍යයෙන් System එකක් හදද්දී ඒවායේ ආරක්ෂාව ගැන ඔවුන් විශේෂයෙන් සැලකිලිමත් නිසා, ඒ ආරක්ෂක උපායයන් මඟ හරිමින් system එකේ දුර්වල ස්ථානයන් හොයාගන්න ඔබට out of the box හිතන්නම වෙනවා. ඒක අධ්‍යාපනය හරහාම පමණක් ලබන්නට පුළුවන් හැකියාවක් නෙවෙයි.

කුඩා කාලයේ මට පාසල් අධ්‍යාපනයට එතරම් උනන්දුවක් තිබුණේ නැහැ. අපොස උසස් පෙළටත් එතරම් උනන්දුවක් තිබුනේ නැහැ. නමුත් අන්තර්ජාලය හරහා මම බොහෝ දේ ඉගෙනගත්තා. හැමදේම තනියම ඉගෙනගෙන අත්හදා බැලුවා. මේ තැනට එන්න හේතුවුණේ මගේ ඒ කැපවීම. අවසානයේ මට විදේශ රටවල් ගණනාවකින් රැකියා අවස්ථා සඳහා ආරාධනා ලැබුණා. දැන් මම ඉන්නේ ලන්ඩන්වල. ලෝකයේ අතිශය ප්‍රසිද්ධ සමාගම් රාශියක් සමග මම මේ වෙද්දීත් වැඩ කරලා තියෙනවා. මම මේ සියල්ලම කළේ තනියම ලබපු අධ්‍යාපනය එක්ක. ලංකාවේ ඒ වගේ ක්‍රමවේදයන් හදාරන අය ඉන්නේ හරිම ටික දෙනා යි. මම දැකලා තියෙනවා ලංකාවේ හැමදේම රජයෙන් දෙනකම් බලන් ඉන්නවා. ඒක ආකල්පමය ගැටළුවක්.

මේ event එකේ අරමුණ වෙන්නේ ලංකාවේ ඉන්න මේ තාක්ෂණයට ආස කරන අයට ඒ පිළිබඳව යම් හැඳින්වීමක් ලබා දෙන එක, සහ මේ ක්ෂේත්‍රය තුළ තිබෙන රැකියා අවස්ථා වගේ දේවල් පිළිබඳව දැනුවත් කරන එක. ඒ වගේම මේ Event එක කොටස් දෙකකින් සමන්විත වෙනවා. මුල කොටස වෙන් වෙන්නේ CTF challenge එකක් වෙනුවෙන්. දැනටමත් ඒ වෙනුවෙන් කණ්ඩායම් 48ක් පමණ ලියාපදිංචි වෙලා තියෙනවා. එදා දවසේ අනිත් කොටස වෙන් වෙන්නේ තොරතුරු තාක්ෂණයට ආස ඕනෑම කෙනෙක් වෙනුවෙන්, සහ මේ ක්ෂේත්‍රය ගැන දැනගන්න කැමති ඕනෑම කෙනෙක් වෙනුවෙන් වන meetup එකක් වගේ. එතැනදී මම බලාපොරොත්තු වෙනවා CTF challenge එක ගැන වැඩි දුර විස්තර කරන්න.

පහළ link එකෙන් ඔබට ඒ වෙත ලියාපදිංචි වෙන්න පුළුවන්.

https://www.meetup.com/sliit-cscs/events/263124284/

මේක පැවැත්වෙන්නේ ජූලි 27 වෙනි දා SLIIT ආයතනයේ යි.

දශක ගණනාවකට පෙර ලංකාවේ චිත්‍රකතා අතිශය ජනප්‍රියව පැවතුනා. එවකට චිත්‍රකතා වෙනුවෙන්ම පුවත්පත්වල විශාල ඉඩක් වෙන්වුණා. ඒ වගේම ඉතාම ජනප්‍රිය චිත්‍රකතා පොත් පවා පල වුණා. නමුත් කාලය සමග මේවායේ ජනප්‍රියත්වය ක්‍රමයෙන් අඩුවුණා. අද වෙද්දී චිත්‍රකතා බොහෝ විට මීම් විදිහට හෝ දේශපාලනික cartoon විදිහට පුවත්පත්වල දැකගන්නට පමණයි පුළුවන්.

‘Papadamn’ උත්සහ කරන්නේ මෙය වෙනස් කිරිමට යි. Papadamn නිර්මානය කළ Achinthya Amarakoon Roar වෙත අදහස් දක්වමින් සඳහන් කළේ මුල දී ඇගේ අදහස වුණේ චිත්‍රකතා මාලාවක් නිර්මාණය කිරීම නොවන බව යි. මුලින්ම චිත්‍රකතා පිටු 5ක් පමණක් නිර්මාණය කර තිබුණු බවත් ඇය සඳහන් කළා. නමුත් ඇය Elakiri අන්තර්ජාල ෆෝරමය වෙත upload කළ නිර්මාණ නැවත නැවත facebook වෙත upload වන්නට පටන්ගත්තායින් මේ පිළිබඳව සමාජයේ වූ කැමැත්ත ඇය වටහා ගත් බවත්, ඉන් අනතුරුව ඇය විසින්ම ඒවා facebook වෙත upload කිරීමට සිතූ බවත් ඇය සඳහන් කළා.

එලෙසින් ඇය ආරම්භ කළ facebook පිටුවේ නාමය “Papadamn” වූ අතර ශ්‍රී ලංකා සමාජය හා දේශපාලනය පිළිබඳ හාස්‍යජනක, එහෙත් විවේචනාත්මක විවරණයක් ඒ හරහා සිදු කිරීමට ඇය උත්සාහ දරනවා. සමාජ ජාලාවන් තුළ ඇගේ පිටුවට සහ චිත්‍රකතා වෙත ලැබුණු පිළිගැනීම හේතුවෙන් දීර්ඝ චිත්‍රකතා මාලාවක් ‘Sakkai-Muniyayi’ (සක්කයි මුනියයි) ලෙසින් ආරම්භ කරනවා. මේ කතාව ගෙතෙන්නේ වැරදි හැසිරීම් නිසාවෙන් දිව්‍යලෝකයෙන්, සහ අපායෙන් පිටුවහල් කළ දෙවියෙක් සහ යක්ෂයෙකු වටා යි. මීට වසරකට පෙර, 2018 ජූලි මාසයේ, ඇරඹුණු සක්කයි මුනියයි චිත්‍රකතා මාලාව මේ වන විට සමාජ ජාලාවන් තුළ අතිශය ජනප්‍රියත්වයක් ලබා තිබෙනවා. දැනට මෙහි එක කතා වාරයක් නිමාවට පත් වී තිබෙන (season) නමුත් ඉතාම ඉක්මනින් දෙවැනි Season එකත් ආරම්භ කිරීමට බලාපොරොත්තුවෙන් සිටින බව තමයි දැනගන්න ලැබෙන්නේ. මේ චිත්‍රකතා මාලාව හරහා ලංකාවේ සමාජයීය යතාර්ථයන් පිළිබඳව කතා බහ කෙරෙන නිසාවෙන්ම බොහෝ දෙනෙකු මේ කතා මාලාවට ඇලුම් කරන බව යි අපේ පෞද්ගලික අදහස.

Facebook වෙත මේ කතා මාලාව upload කිරීමත් සමගම අභියෝග ගණනාවකට මුහුණ දීමට තමන්ට සිදුවූ බව ඇය සඳහන් කරනවා. Facebook algorithm විටින් විට කතා මාලාවේ කොටස්වල reach අඩු වැඩි කිරීම ඉන් එකක්. එනිසාවෙන් සක්කයි මුනියයිට අමතරව විටින් විට gag-comics upload කිරීමට සිදු වුණු බව යි ඇය සඳහන් කළේ.

අචින්ත්‍යා වෘත්තියෙන් UX designer කෙනෙක් විදිහට කටයුතු කරනවා. නිවසේ සිටම වෘතියේ නියැලෙන නිසාවෙන් ඇයට ඇගේ නිදහස් කාලයේ මේ විනෝදාංශයෙන් ඔබ්බට ගිය චිත්‍රකතා නිර්මාණය වෙත යොදවන බව තමයි සඳහන් කළේ. චිත්‍රකතා යනු අමුතුම ආකාරයේ කතාන්දර කීමේ මාධ්‍යයක් බවත්, එය නැවත ලාංකිකයින් අතර ප්‍රචලිත වනු දැකීමෙන් ඇය විශාල සතුටක් ලබන බවත් අචින්ත්‍යා සඳහන් කළා. සක්කයි මුනියයි වෙත මේ වගේ පිළිගැනුමක් ලැබේවියැ යි ඇය නොසිතූ බව ද ඇය අප වෙත අදහස් දක්වමින් කියා සිටියා.

තාක්ෂණයේ දියුණුව සමග ලංකාවේ චිත්‍රකතා අභාවයට යන මොහොතක අන්තර්ජාලය හරහාම LankaComics වැනි සමාජ ජාල පිටු අතීත චිත්‍රකතා වර්තමානය තුළ ජීවමාන කිරීමට අත්වැල් සපයනවා. ‘Papadamn’, Sachi Ediriweera, සහ Isuri Dayaratne වැනි නිර්මාණකරුවන් නිසාවෙන් ලංකාවේ චිත්‍රකතාවල අනාගතය පිළිබඳව යම් බලාපොරොත්තු තබා ගත හැකි බව අපට හැඟෙනවා.

පසුගිය 22 දා අසල්වැසි ඉන්දියාවෙන් සඳෙහි පරික්ෂා නොකරන ලද කොටසක් ගවේශනය වෙනුවෙන් චන්ද්‍රයාන් 2 නම් රොකට්ටුව දියත් කළා.

මිනිසා සඳ ජයගෙන පසුගිය 21 වෙනි දාට අඩ සියවසක් සපිරුනා.

චිත්‍රපට/ වීඩියෝ පරිගණකයෙන් හෝ smart දුරකතනයෙන් නරඹන ඔබට VLC media player එක නුහුරු වෙන්නට හැකියාවක් නැහැ. නොමිලයේ ලබාදෙන නිසාත්, විවෘත කේත මුලාශ්‍ර වැඩසටහනක් (open source software) නිසාත් Formats ගණනාවක media files play කිරීමට හැකි වීම හේතුවෙන් පරිගණක භාවිත කරන ඕනෑම කෙනෙක් අතර VLC media player එක අතිශය ප්‍රසිද්ධ යි. අවාසනාවකට මෙන්, VLC හි ඉතා බරපතල ආරක්ෂක දෝෂයක් තිබෙන බව මේ වෙද්දී හඳුනාගෙන තියෙනවා. VLC media ව්‍යාපෘතියේ සිටින පුද්ගලයින් හට එය මඟහරවා ගැනීමට හැකියාව ලැබෙන තෙක් එය uninstall කිරීම නුවණට හුරු වැඩක් බව යි Roar අපේ යෝජනාව.

ජර්මානු ජාතික පරිගණක හදිසි ප්‍රතිචාර කණ්ඩායම [Germany’s national Computer Emergency Response Team (CERT-Bund)] කළ සොයා ගැනීමකට අනුව, මේ දුර්වලතාවය නිසා අපව හැකර්වරුන් වෙත නිරාවරණය වීමක් සිදුවෙනවා. මෙය නම් කරලා තියෙන්නේ CVE-2019-13615 යන නමින්. මෙය වෙත ලැබී තිබෙන vulnerability score එක 9.8 බව යි සඳහන් වෙන්නේ.

මේ ආරක්ෂක දුර්වලතාවය හේතුවෙන් RCE -remote code execution (දුරස්ථ කේත ක්‍රියාත්මක කිරීම) ක්‍රමවේද භාවිතය වෙත පහසුවෙන් ඉඩක් ලැබෙන අතර, පරිගණකයට ඇතුල්වීමට උත්සාහ දරන හැකර්වරුන් වෙත අවසරයකින් තොරව මෘදුකාංග ස්ථාපනය කිරීමට, වෙනස් කිරීමට හෝ ක්‍රියාත්මක කිරීමට ඉඩ සලසනවා. සරලවම කිව්වොත්, මේ හරහා හැකර්වරුන් හට ඔබේ පරිගණකය තුළ තිබෙන files (ගොනු) බැලීමට වගේම delete කිරීමටත් හැකියාව ලැබෙනවා.

වාසනාවකට මෙන් තවමත් මේ ආරක්ෂක දුර්වලතාවය භාවිතයෙන් සයිබර් ප්‍රහාරයන් ක්‍රියාත්මක වී නොමැති බව යි වාර්තා වෙන්නේ. WinFuture වෙබ් අඩවියට අනුව Windows, Linux, සහ Unix මෙහෙයුම් පද්ධති වෙත නිකුත් වී ඇති VLC Media Playersවල මෙම ආරක්ෂක දෝෂය හඳුනාගෙන ඇති අතර, mac පරිගණක වෙත නිකුත් ව ඇති සංස්කරණයන් හි මෙය දකින්නට නොමැති බව යි ඔවුන් සඳහන් කරන්නේ.

මේ වන විටත් VLC කණ්ඩායම මේ ආරක්ෂක දෝෂය වෙත patch එකක් නිර්මාණය කිරීම ආරම්භ කර තිබෙනවා. නමුත්, තවමත් ඔවුන්ට එහි 60%ක ප්‍රමාණයක් පමණයි අවසාන කරගැනීමට හැකියාව ලැබී තියෙන්නේ. ඒ නිසාවෙන් ඔවුන් සම්පුර්ණයෙන්ම මේ ආරක්ෂක දෝෂය වෙත පිළියම් යොදන තෙක් VLC Media Player එක ඔබේ පරිගණකයෙන් ඉවත් කර, ඒ වෙනුවට KM player/ MPC Player වැනි විකල්ප player එකක් වෙත යොමුවීම සුදුසු යි.

මේ සතිය පුරාවටම බොහෝ දෙනෙක් කතා බහ කරන මාතෘකා අතරට නැවත වරක් ප්‍රසිද්ධියට පත්වන faceapp ඉහළම තැනක් ගන්නවා. හැබැයි මේ faceapp හරහා ඔබේ දත්ත ලබා ගත හැකි බවට මතයන් පවතින බව ඔබ දන්නවා ද? ඇත්තටම මේ faceapp නිසාවෙන් ඔබේ පෞද්ගලික දත්ත අන්සතු වෙනවා ද? මේ පිළිබඳව යි මේ ලිපිය දිග හැරෙන්නේ.

faceapp කියන්නේ 2017 වසරේ රුසියානු Wireless Lab නම් සමාගමක මෘදුකාංග නිර්මාපකයින් පිරිසක් එක්ව නිර්මාණය කරනා ලද ජංගම දුරකථන යෙදුමක් (app එකක්). මේ යෙදුම හරහා සිදු වන්නේ ඔබේ රුව සහිත ඡායරුපයකට යම් ආකාරයක filters එකතු කිරීම මඟින් බාහිර පෙනුම වෙනස් කර පෙන්වීමක්. AI එකක් සහිත Alogrytham එකක් මඟින් මෙය ක්‍රියාත්මක වෙනවා. ඔබේ රුව සහිත ඡායාරුපය ඔවුන්ගේ server එකක් වෙත upload කිරීමෙන් අනතුරුව අදාළ Alogrytham එක මඟින් ඔබ නියම කළ filters එකතු වීම සිදු වෙනවා.

මෙය 2017 වසරේ ජනප්‍රියත්වයට පත් වෙන්නට ඇරඹි කාලයේම මෙයට යම් යම් ආකාරයේ චෝදනාවන් විවිධ පිරිස් මඟින් එල්ල වුණා. උදාහරණයක් විදිහට මෙහි භාවිතා කරන යම් යම් filters මඟින් කළු ජාතිකයන් ගේ හමේ පැහැය වෙනස් කරමින් ඔවුන්ට අගෞරව සිදු කරන බවට පරිශීලකයන් වෙතින් මැසිවිලි එල්ල වුණා. කොහොම වුණත් පසුගිය දින කිහිපය තුළ මේ faceapp හදිසියේම නැවතත් කරලියට පැමිණීම සහ ලෝකයේ අතිශය ජනප්‍රිය සහ ප්‍රසිද්ධ පුද්ගලයින් ගණනාවක් තමන්ගේ සමාජ ජාල ගිණුම් වෙත මේ යෙදුම භාවිතා කරමින් ඡායාරූප එකතු කිරීම බොහෝ දෙනෙකුගේ කතා බහට ලක්වුනා. ඒ වගේම මෙහි තිබිය හැකි පෞද්ගලික දත්ත අන්සතු වීමේ හැකියාව පිළිබඳත් කතා බහක් ගොඩ නැගෙන්න මේ හදිසි රැල්ල තෝතැන්නක් බවට පත්වුනා.

“FaceApp: Is The Russian Face-Aging App A Danger To Your Privacy?” යන සිරස්තලය සමගින් forbes වෙබ් අඩවිය පල කළ ලිපිය මේ කතා බහ යම් ආකාරයක සමාජ කතා බහක් ගොඩ නගන්නට හේතු වුණා. ඒ වගේම මේ පිළිබඳව theverge.com වෙබ් අඩවියට ඔවුන් ලබා දෙන ලද ප්‍රකාශයකට අනුව ඔවුන් තමන්ගේ servers වෙත upload කරන images ටික කලකින් ඉවත් කෙරෙනවා. මේ පිළිබඳව Guardian Firewallහි CEO සහ iOS researcher කෙනෙක් වන විල් ස්ට්‍රෆැක් twitter සටහනක් තබමින් කියා සිටියේ, තමන් traffic analyzer එකක් භාවිතා කරමින් මෙහි සිදු වන ක්‍රියාවලිය ප්‍රතිනිර්මාණය කළ බවත්, එහි අසාමාන්‍ය දත්ත භාවිතයක් තමා නොදුටු බවත්. කෙසේ වෙතත් මේ app එක හරහා අප තෝරාදෙන image එක පමණක් ඔවුන්ගේ server වෙත upload වීම පිළිබඳව වුවත් අප්‍රසාදය දක්වන්නන් සිටිය හැකි බව ඔහු තව දුරටත් සඳහන් කර තිබුනා. techcrunch.com වෙබ් අඩවිය වෙත ප්‍රකාශ කර තිබුණේ පරිශීලක ඉල්ලීම් පැමිණියහොත් ඔවුන් සතුව තාවකාලිකව ගබඩා කර ගන්නා cashe image පවා මකා දැමීමට ඔවුන් සුදානම් බව යි. ඔබටත් අවශ්‍ය නම් මේ පියවර මඟින් request කිරීමට හැකියාව තිබෙනවා.

Setting>Support>Report a bug වෙත පිවිස “privacy” යටතේ ඉල්ලීමක් සිදු කිරීමට ඔබට හැකියාව තිබෙනවා. පරිශීලකයන්ගේ ඡායාරූප රුසියාවට ගෙන යන බව පැවසුව ද මෙම සේවාව සඳහා භාවිතා කරන්නේ AWS සහ Google Cloud Platform සේවාවන්වල servers බැවින්, R&D team එක රුසියාවේ සිටිය ද මෙම ඡායාරූප ගබඩා කිරීම සිදුවන්නේ රුසියාවෙන් පිටත, එනම් Amazon සහ Google සමාගම්වල data centersවල බව එහි හිමිකරු වන Yaroslav Goncharov TechCrunch වෙබ් අඩවියට ප්‍රකාශ කර තිබෙනවා.

සාමාන්‍යයෙන් මිලියන 150කට වඩා පිරිසක් භාවිතා කරන මේ දුරකථන යෙදුම Android Play store සහ Apple App store දෙකේම පවතින app එකක්. සාමාන්‍යයෙන් මේ වගේ යෙදුමකින් එවැනි දත්ත සොරාගැනිමක් සිදු වෙනවා නම් මේ වෙන තෙක් අදාල යෙදුම playstore හෝ app storeහි රැඳී තිබෙන්නේ නැහැ. විශේෂයෙන්ම මේවා වෙත යම් යෙදුමක් එකතු කරද්දී යම් ආකාරයක review කිරීමක් සිදු කරනවා. එනිසාවෙන් එවැනි යමක් සිදු කිරීමට හැකියාවක් ලැබෙන්නේ නැති තරම්. විශේෂයෙන්ම සම්පූර්ණ ගැලරි එකම අප්ලෝඩ් කිරීමට බොහෝ විට අවසර තිබෙන්නේ cloud සේවාවන් සඳහා පමණ යි. Prisma වැනි image overlay කිරීම් සිදු කරන application වෙත ඒ අවස්ථාවේ load කරවන image එකෙහි cache image එකක් පමණක් upload වීම සිදු වෙනවා. Faceapp වෙතත් Neural Network එකක් හරහා භාවිතා වෙන්නේ එවැනිම තාක්ෂණයක්. මෙහිදී upload වෙන cache image එක අනුව නිර්මාණය වෙන overlay එක ඇප් එක වෙත පැමිණ එතන සිදු වන process එකක් මඟින් තමයි අවසාන ඡායාරුපය නිර්මාණය වෙන්නේ. එනිසාවෙන් අනිසි බියක් ඇති කර ගතයුතු නැහැ.

අන්තර්ජාලය තුළ Privacy කියන්නේ මිත්‍යාවක්. නොමිලයේ ලබා දෙන facebook සමාජ ජාලය වෙතත් පරිශීලක දත්ත අනිසි භාවිතය පිළිබඳව චෝදනා පල වුණා ඔබට මතක ඇති. ඇතැමුන් මේ චෝදනාව හඳුන්වන්නේ මේ යෙදුම රුසියානු එකක් නිසාවෙන් ඇමරිකානුවන් ගෙතූ අසත්‍ය ප්‍රචාරයක් ලෙස යි.

එනිසා යම් ලියවිල්ලක් දුටු පමණින් කලබලයට පත් නොවී, ඒ පිළිබඳව නිර්පාක්ෂික සොයා බැලීමක් සිදු කර, එවැනි යෙදුම් භාවිතා කරනවා ද නැද්ද යන්න තීරණය කිරීම තමයි නුවණට හුරු.

පසුගිය කාලය තුළ ලංකාවේ බොහොමයක් දෙනා අතර කතාබහට ලක්වූ මාතෘකාවක් බවට මිගමුව ප්‍රදේශයෙන් හමුවූ ජංගම දුරකතන 400ත්, sim card පත් 17,000කට අධික ප්‍රමාණයත්, routers 60ත් පත් වුණා. මෙය ත්‍රස්තවාදී ක්‍රියාවක් බවටත් බොහොමයක් දෙනා චෝදනාවන් එල්ල කළ අතර, තවෙකෙක් කියා සිටියේ මෙය Click Farm එකක් බව යි. මේ ලිපිය හරහා මේ පිළිබඳව සහ මෙහි භයානකත්වය පිළිබඳව ඔබ සමග තොරතුරු බෙදාගන්න බලාපොරොත්තු වෙනවා.

සාමානයෙන් Click Farm එකක්, එහෙම නැතිනම් Click Fraud Farm එකකට පරිගණක එකකට හෝ කීපයකට සම්බන්ධ කරගත් නවීන ජංගම දුරකථන විශාල ප්‍රමාණයක් අයත් වෙනවා. මේ හරහා බොහෝ දේ සිදු කිරීමට හැකියාව තියෙනවා. බොහො විට මෙවැනි Click Farm හරහා Social Media ගිණුම්වල reach සහ likes වැඩි කිරීම සිදු කරනවා. ඒ වගේම youtube views වැඩි කිරීම සහ trending list එක වෙත videos එකතුකිරිම පවා මේ මඟින් සිදු කරන්න පුළුවන්.

ඒ වගේම ලංකාව වැනි රටවල විවිධ ප්‍රවෘත්ති, ප්‍රකාශයන් සමාජය තුළ වයිරල් ලෙසින් ප්‍රචාරය කරවීම වැනි දේ සඳහාත් භාවිත කරගන්න හැකියාව තියෙනවා. මේ හරහා අසත්‍ය ප්‍රකාශයක් වුවත් ඉතාම කෙටි කාලයකින් සමාජයේ ප්‍රසිද්ධ කරන්න හැකියාව තියෙනවා. ඒ වගේම යම් ගිණුමක්, පිටුවක්, වීඩියෝවක් හෝ පොස්ට් එකක් දිගින් දිගටම report කිරීම මඟින් ඉවත් කරවන්නත් හැකියාව තියෙනවා. ඒ වගේම Ad clicks ප්‍රෝග්‍රෑම් වඩා සාර්ථකව කරගෙන යෑම, නීති විරෝධී ලෙස අන්තර්ජාතික ඇමතුම් ලබාගැනීම, SMS චන්ද විකිනීම නැත්නම් SMS කැම්පේන් කිරීම, වෙබ්සයිට් ට්‍රෆික් වැඩි කිරීම වගේ දේවල් සඳහාත් මේවා භාවිත කරන්න හැකියාව තියෙනවා. සමාජයක් තුළ අන්තර්ජාලය හරහා අර්බුදයන් නිර්මාණය කිරීම සඳහා මේවා භාවිත කරන අවස්ථාවන් නැතුවා නොවේ. එම නිසා මේවා troll farm නමිනුත් හඳුන්වනවා.

මෙවැනි ට්‍රොල් ෆාම් භාවිතයෙන් ඇමරිකානු ඡන්දයට බලපෑම් සිදු කළ බව සහ ඇමරිකාව තුළ අර්බුද නිර්මාණය කළ බවට රුසියාවට චෝදනා එල්ලවුණා.

කෙසේ වෙතත් මේ වන විට බොහොමයක් රටවල මෙවැනි ට්‍රොල් ෆාම් නීතියෙන් තහනම්. නමුත් ලංකාව වැනි ආසියාතික සහ තුන්වන කාණ්ඩයේ බොහෝ රටවල අදටත් මේ ගැන හරි ආකාරයෙන් නීති සම්පාදනය කර නැහැ.

මේ සිදුවීමෙන් පසුවවත් එවැනි දේ පිළිබඳව සොයා නීති සම්පාදනය කිරීම සිදු කළ යුත්තක්. කෙසේ වෙතත් මෙවැනි ෆාම් විශාල සමාගම් විසිනුත් භාවිත කළ අවස්ථා පිළිබඳව අන්තර්ජාලයෙන් තොරතුරු ඕනෑ තරම් සොයාගන්න හැකියාව තියෙනවා. උදාහරණයක් විදිහට aliexpress වැනි අන්තර්ජාලය හරහා භාණ්ඩ විකුණන වෙළඳුන්වල විවිධ භාණ්ඩ සඳහා ratings වැඩි කර ගැනීමට මෙවැනි උපක්‍රම භාවිතා කරනවා. සමාජ මාධ්‍ය භාවිතා කරන ඔබට හොඳින් මතක ඇති පසුගිය කාල වකවානුවේ දිගින් දිගටම සිදු වූ ප්‍රසිද්ධ facebook group සහ pages අහිමි වීම්. එවැනි දේ සඳහාත් මේ ෆාම්වල යම් බලපෑමක් ඇති බවට බොහෝ දෙනෙකු මත පල කරනවා. මෙවැනි ෆාම් ඔස්සේ විවිධ අන්තර්ජාල ක්‍රීඩාවන්වල නිරත වන පුද්ගලයන් පවා ඉන්නවා. ඒ වගේම playstore, apps storeවල විවිධ apps සඳහා download count එක වැඩි කර ගැනීම සඳහා වගේම reviews දමා ගැනීම වෙනුවෙනුත් මේවා භාවිත වෙන අවස්ථා එමට යි. මේ පිළිබඳව හරි ආකාරයෙන් නීති සම්පාදනයට බලධාරීන්ගේ ඇස් විවර විය යුතු යි. එසේ නැති නම් විශාල සමාජ කලබැගෑනියක් වුව ද ඇති විය හැක.

මිලියන ගණනක් භාවිතා කරන twitter සිය 13 වෙනි සංවත්සරය මේ වසරේ සැමරුවා. මේ කියන්න යන්නේ twitter ගැන ඔබ නොදන්නා දේවල් කිහිපයක්.

ඇපල් සමාගම සහ චීන රජය අතර මේ වන විට පවතින්නේ උග්‍ර මට්ටමකට පැමිණ තිබෙනවා. මෙවැනි අවස්ථාවක හදිසියේම ඇපල් සමාගම තමන්ගේ Mac Pro නිෂ්පාදනාගාර චීනය වෙත ගෙන යාමට තීරණය කර තිබෙන බව ආරංචි මාර්ගයන් පවසනවා. ඇපල් සමාගම වෙනුවෙන් Mac පරිගණක නිෂ්පාදනය කරන Quanta Computer ආයතන මේ වන විටත් මේ ස්ථාන මාරු සඳහා වැඩ කටයුතු සූදානම් කරමින් සිටින බව තමයි දැනගන්න ලැබෙන්නේ. ඇමෙරිකාවේ Austinවල පැවති Mac Pro නිෂ්පාදනාගාර, චීනයේ ශැන්ග්හායි වෙත ගෙනයනු ඇත. මෙයට ප්‍රධානතම හේතුව ලෙසින් වාර්තා වෙන්නේ Mac Pro නිෂ්පාදනයට අවශ්‍ය කරන අමුද්‍රව්‍ය, සැපයුම්කරුවන් චීනය ආශ්‍රිතව කටයුතු සිදු කිරීම යි. චීනය වෙත ආයතනය රැගෙන යාමෙන් අමුද්‍රව්‍ය ප්‍රවාහනයට ගත වන කාලය සහ මුදල් ඉතිරිකර ගනිමින් Mac Pro පරිගණකවල නිෂ්පාදන වියදම සැලකිය යුතු ප්‍රමාණයකින් අඩු කර ගැනීමට Apple සමාගමට හැකියාව ලැබෙනු ඇත. කෙසේ වෙතත් නිල වශයෙන් මේ පිළිබඳව තවමත් ඇපල් සමාගම නිවේදනයක් නිකුත් කර නැහැ.

2019 වසරේ ආරම්භය ඇපල් සමාගමට එතරම්ම සුභදායක වුණේ නැති බව ඔබට මතක ඇති. Qualcomm සමාගම, ඇපල් සමාගමට විරුද්ධව නඩු පැවරීම සහ තවත් හේතු ගණනාවක් බලපෑවා. ඒ පිළිබඳව අප ඔබව “2019 ඇපල් සමාගමට නපුරු වේවි ද?” ලිපියෙන් දැනුවත් කළා.

දශක තුකට අධික කාලයක් තිස්සේ ඇපල් සමාගමේ සේවයේ සිටි ඇපල් සමාගමේ ප්‍රධාන සැලසුම් නිලධාරීවරයා වන Jony Ive ඇපල් සමාගම හැරයන්නට තීරණය කර තිබෙනවා. විශාල වශයෙන් මාධ්‍ය ඉදිරියේ පෙනී නොසිටියත් ‘90 දශකයේ පමණ සිට අප භාවිතා කරන ඇපල් උපාංගවල නිර්මාණ කාර්යයභාරයට විශාල දායකත්වයක් ලබා දුන් පුද්ගලයෙක් ලෙසින් Jony Ive හඳුන්වන්න පුළුවන්. බොහෝ දෙනෙක් ඇපල් උපාංග සඳහා බොහෝ ඇලුම් කරන්නේ එහි තිබෙන පෙනුම හා දැනෙන premium හැඟීම නිසාවෙන්. ඒ පෙනුම පවත්වාගන්නට දායකත්වය ලබාදුන් පුද්ගලයෙක් ලෙසින් Jony Ive හඳුන්වන්න පුළුවන්.

මොහු සමාගම හැරයාමට හේතුව ලෙසින් ඔහු සඳහන් කරන්නේ ඔහුගේම design firm එකක් ආරම්භ කිරීමට බවයි වාර්තා වෙන්නේ. මෙලෙසින් ආරම්භ වෙන LoveFrom design firm එක ඉදිරියේ දීත් ඇපල් සමාගම සමග ඉතා සමීපව කටයුතු කිරීමට සැරසෙන බව යි දැනගන්නට ලැබෙන්නේ. Apple සමාගම LoveFrom ආයතනයේ පාරිභෝගිකයෙකු වුවහොත් බොහෝ විට ඉදිරියේ නිකුත් වන ඇපල් උපාංග සඳහාත් මොහුගේ නිර්මාණ දායකත්වය ලබෙන්නට ඉඩ තිබෙනවා. කෙසේ වෙතත් Jony Iveගේ මේ හැරයාම පිළිබඳව විවිධ මතයන් ඇපල් සමාගමේ නිෂ්පාදන අගයන පුද්ගලයන් අතර පවතිනවා. වසර 5කට පමණ පෙර The Guardian පුවත්පත සමග පැවති සාකච්ඡාවක දී ඔහු සිදු කළ යම් ප්‍රකාශයක් මේ කතාබහට තුඩු දී තිබෙනවා. Apple සමාගම විසින් නව්‍යකරණය (innovate) කිරීම නවතා දැමුවහොත් ඔහු Apple සමාගමෙන් ඉවත්ව යන බව තමයි ඒ ප්‍රකාශයේ අඩංගු වෙන්නේ. මේ සියල්ලෙහි ඇත්ත නැත්ත ඉදිරියේ දී ඉතා ඉක්මනින් අපිට දැක බලාගන්න හැකියාව ලැබෙයි.

පැරන්නන්ට අනුව ලෝකය නිර්මාණය වෙලා තියෙන්නේ මූලධාතු හතරක් එකට එකතු වීමෙන්. වාතය, පොළව, ගින්දර, සහ ජලය ඒ මූලධාතු හතර යි. වාතය, පොළව, සහ ජලය යන තුනම පදාර්ථයේ ස්වරූපයන් නමුත්, ගින්දර කියන්නේ පදාර්ථයේ ස්වරූපය වෙනස් කරන රසායනික ක්‍රියාවලියක්. ගින්දරේ විද්‍යාව කොහොම වුණත් ඒ පිළිබඳව අපේ පැරැන්නන් අතරේ විවිධ මිත්‍යා කතන්දර, විශ්වාසයන් වගේම ඇදහීම් සිරිත් විරිත් පවා ගොඩ නැගී තිබුණා. මේ 21 වෙනි සියවස වෙද්දීත් ඇතැම් රටවල සාම්ප්‍රදායිකව එවැනි චාරිත්‍රයන් වාරිත්‍රයන් පැවතෙනවා.

මේ ගින්දර මිනිසා සොයා ගැනුණු ආකාරය සහ භාවිතය ආරම්භ වීම පිළිබඳව වගේම කාලවකවානුවක් පිළිබඳව විවිධ මත ගැටුම් පවතිනවා. ග්‍රීක පුරවෘතයන්ට අනුව මෙලොව මුලින්ම ජීවත්ව ඇත්තේ යෝධ පුරුෂයන් කොට්ඨාශයක් වන ටයිටන්වරුන් පමණ යි. නිතරම දෙවි වුරුන් සමග යුධ වැදුණු මොවුන් අතරේ දූරදර්ශීභාවයේ ටයිටන්වරයා ලේසින් හඳුන්වන ප්‍රොමිතියස් ද වුණා. ඒ කාලයේ ගින්දර කියන්නේ දෙවිවරුන් සතුව පැවති වටිනාම සම්පතක්. මෙය මිනිසුන් මැවිමෙන් අනතරුව මිනිසුන් වෙත ලබා දිය යුතු ත්‍යාගයක් වුවත්, පොළොවේ ජීවත් වන මිනිසුන්ගේ ක්‍රියාකලාපය ගැන අපැහැදුණු දෙවිවරු මෙය මිනිසුන් වෙත ලබා නොදී සිටින්න තීරණය කළා. මේ මහඟු සම්පත මිනිසාගෙන් සඟවා තබාගැනීමට විරුද්ධ වුණු ප්‍රොමිතියස් දෙවියන්ගෙන් ගින්දර සොරාගෙන මිනිසුන්ගේ ප්‍රයෝජනය සඳහා මෙලොවට රැගෙන ආවා.

මෙයින් දැඩි ලෙස කිපුණු මහා දෙවි සීයුස් මිනිසුන්ට දඬුවම් කිරීමට තීරණය කළා. පොළොවේ පස් සහ වතුරවලින් තමන්ට මනුෂ්‍ය දියණියක් නිර්මාණය කර දෙන ලෙස ශිල්ප කර්මාන්තයන්ට අධිපති හෙෆීස්ටස්ට නියෝග කළා. ඇයට පැන්ඩෝරා යනුවෙන් නම් තැබුණා (ඇයගේ නමේ අරුත “සියළු තෑගි” ගෙනෙන්නා යනු යි). මේ පැන්ඩෝරාට එක එක දෙවිවරුන්ගෙන් විවිධාකාර ගුණාංග ලැබුණා. ආදරයට සහ රූපයට අධිපති ඇෆ්රොඩයිට් ඇයව ලස්සන කළා. කලාවට අධිපති ඇපොලෝ ඇයට සංගීතමය හැකියාව ලබා දුන්නා. ඒ වගේම දෙවියන්ගේ පණිවිඩකරුවා හර්මිස් ඇයට ඕනෑම කෙනෙකු තමන්ගේ මතයට නම්මා ගැනීමේ හැකියාව තිලිණ කළා. අනතුරුව දෙවිවරු හැමෝම එකතු වෙලා ඇයට 'කුතුහලය ' කියන ගුණාංගය උරුම කළා.

ප්‍රොමිතියස් පැන්ඩෝරාව විවාහ කරගන්නට සිහින දකින බව දැනගත් සියුස් කළේ, ඇයව ප්‍රොමිතියස්ගේ සහෝදරයා එපිමීතියස්ට විවාහ කරලා දුන්න එක යි. මේ දෙන්නව මහ පොළොවේ ජීවත් වෙන්න පිටත් කළා. එහෙම යද්දී මේ දෙන්නට අරන් යන්න රහසිගත පෙට්ටගමක් ලබා දුන්නා. හැබැයි එය කිසිම දවසක විවෘත කරලා බලන්න තහනම් වුණා. මාස ගණනක් යනතුරු පැන්ඩෝරා මෙම පෙට්ටිය ගැන සිතුවේ නැහැ. කාලයක් ගත වෙද්දී, පැන්ඩෝරාට උරුම වෙලා තිබුණ කුතුහලය කියන ගුණාංගය නිසාම, මේ පෙට්ටගම ඇරලා බලන්න ඇය පෙළඹුණා. ඇය පෙට්ටගම විවර කරද්දීම ජීවිතයේ නරක නපුරු දේවල් සියල්ලම - ඒ කියන්නේ ලෙඩ රෝග, අපරාධ, ඉරිසියාව, වෛරය, සහ දුක් දොම්නස් පෙට්ටගම තුළින් එළියට පැනලා මහ පොළොවට නිදහස් වුණා. ඇය පෙට්ටගම ආපසු වහද්දි ඉතිරි වෙලා තිබුනේ බලාපොරොත්තුව විතර යි. අදටත් ලෝකයේ සියලු කරදර මධ්‍යයේ ජිවත් වෙන්න ඔබට ශක්තිය ලෙසින් බලාපොරොත්තු ඉතිරිවන්නේ එනිස යි.

තාත්තා පෙට්ටගම ඇරලා බලන්න තහනම් කලේ ඇයි කියල ඇයට තේරුම් ගියා. තමන් මේ පෙට්ටගම විවර කළ බව තාත්තා දැන ගනීවි කියලා ඇය හොදටෝම බය වුණා. ඒ වුනත් මේක සියුස් කල් තියා සැලසුම් කළ උගුලක් බව ඇය දැනගෙන හිටියේ නැහැ. කොහොම වෙතත් දෙවියන්ගෙන් ගින්දර සොරාගත් ප්‍රොමිතියස්ට තවත් දඬුවමක් හිමිවුණා. ඔහුව පණපිටින් ගිජුලිහිණියන්ට ආහාරය පිණිස ලබා දුන්නා. ඔහුට මිය යාමත් තහනම් වුණා. මිය යන වාරක් පාසා නැවත පණ එන ලෙසත්, ඒ පණ එන හැම වාරයකම නැවතත් පෙර ලෙසම ලිහිණියන්ගේ ආහාරය වන ලෙසත් ඒ දඬුවම ක්‍රියාත්මක වුණා.

කෙසේ වෙතත් ගින්දර සොරාගත් ප්‍රොමිතියස් මානව ශිෂ්ටාචාරයේ ආරම්භකයා ලෙසින් පැරැන්නන් සලකනවා. දෙවියන් මිනිසාට ගින්දර ලබා නොදුන්නේ මිනිසා ගින්දරෙන් කුමක් කරාවි ද යන්නට තිබූ බිය නිසා බවයි කියවෙන්නේ. මිනිසුන් අද වෙද්දී ඒ බිය සාධාරණ බව ඔප්පු කරලා හමාර යි. ගින්දර කියන්නෙ මානව ශිෂ්ඨාචාරය හැඩගස්වපු “දෙවියන්ගේ හස්තය” යි. මිනිස් අවි ආයුධ සියල්ලම පාහේ උපන්නේ ගින්නෙන්. තාක්ෂණය උපදින්නේ ගින්නෙන්.

ගින්දර මිනිසා වෙත ලැබුණු ආකාරය පිළිබඳව විවිධ ශිෂ්ටාචාරයන් සහ විවිධ සංස්කෘතිවල බොහෝ කතාන්දර නිර්මාණය වී තිබෙනවා. ඒ පිළිබඳව අප ඉදිරි ලිපිවලදී ඔබව දැනුවත් කරන්න බලාපොරොත්තු වෙනවා. ඒ වගේම ඉදිරියේ දී ලියවෙන්න ඕනේ පුරාවෘත්තයන් ගැනත් ඔබේ අදහස් අපට කියන්න අමතක කරන්න එපා.

පෙරේදා රාත්‍රියේ (ජූලි 02) හදිසියේම ලෝකය පුරා වෙබ් අඩවි මිලියන ගණනක සහ වෙබ් ආශ්‍රිත සේවාවන් විශාල ප්‍රමාණයක් හදිසියේම අකර්මණ්‍ය වීමක් සිදුවුණා. මෙයට හේතුව ලෙසින් සඳහන් වුණේ Cloudflare සේවාවේ සිදු වූ බිඳවැටීමක් බව යි වාර්තා වෙන්නේ. ලෝකයේ වෙබ් අඩවි නිර්මාණකරුවන්ගේ සහ ඒ ආශ්‍රිතව සේවාවන් සපයන ආයතන අතර අතිශයින් ජනප්‍රිය Content Delivery Network (CDN) සේවාවක් බවට Cloudflare පත්ව තිබෙනවා. මේ සේවාව භාවිත කරන්නන්ගේ වෙබ් අඩවි සහ වෙබ් සේවාවන් තුළ අඩංගු content ඔවුන්ගේ servers තුළ තැන්පත් කරගනිමින් අදාළ වෙබ් අඩවි පරිශීලනය කරන්නන් හට වේගවත්ම server එක හරහා ඉතාමත් ඉක්මණින් අදාළ content ලබාදෙන ආකාරයේ සේවාවක්. ඊට අමතරව SSL certificate ලබාදීම, වෙබ් අඩවිවල වේගය හා ගුණාත්මක බව ඉහළ දැමීම සඳහා අවශ්‍ය වන කටයුතු සහ සේවාවන් රාශියක් Cloudflare මඟින් සපයනු ලබනවා. මිලියන 16කට අධික internet property සමග සම්බන්ධව කටයුතු කරන ලෝකයේ විශාලතම cloud ආශ්‍රිත සේවාවක් ලෙසින් Cloudflare හඳුන්වන්නට පුළුවන්.

සාමාන්‍යයෙන් මෙවැනි අකර්මණ්‍යවීම් පිළිබඳව තොරතුරු ලබාදෙන downdetector.com වෙබ් අඩවියත් මේ නිසාවෙන් අකර්මණ්‍ය තත්ත්වයකට පත්වුණා. පැයකට ආසන්න කාලයක් තිස්සේ පැවති මේ බිඳවැටීම නිසාවෙන් Discord, Shopify, Fiverr, Coinbase වැනි ප්‍රසිද්ධ සේවාවන් පවා අකර්මණ්‍යය වී තිබූ නමුත්, බිඳවැටීම සාර්ථකව අවසන් කරමින් නැවත වරක් තම සේවාව යථා තත්ත්වයට පත් කර ඇති බව Cloudflare ආයතනය විසින් මේ වන විට නිල වශයෙන් ප්‍රකාශයක් නිකුත් කර තිබෙනවා.

මේ බිඳවැටීමට හේතු ලෙසින් ඔවුන් සඳහන් කරන්නේ, Cloudflare serversවල CPU භාවිතාව හදිසියේ ඉහළ යාම බව තමයි ඔවුන් සඳහන් කරන්නේ. Primary සහ secondary පද්ධති ද්විත්වයේම මෙම තත්ත්වය හටගත් බවත්, බිඳවැටීම සිදුවීම සඳහා මූලික වූ හේතුව පිළිබඳව මේ වන විට සොයා බලමින් සිටින බවත් ඔවුන් වැඩිදුරටත් ප්‍රකාශ කර සිටිනවා.

ඊයේ දිනයේ හදිසියේම Facebook, Whatsapp සහ Instagram බිඳවැටීමක් සිදුවුණා. මේ බිඳවැටීමේ දී images සහ videos හුවමාරු කරගැනීමේ දී අදාළ images හරි හැටි දිස් නොවන බව වැඩි වශයෙන් වාර්තා වී ඇති අතර, ඇතැම් ප්‍රදේශවල සිටින්නන් හට WhatsApp හරහා messages යැවීමේ දී ද ගැටලු මතු වී තිබෙනවා. විශේෂයෙන්ම යුරෝපීය රටවල්, ඇමරිකාව, දකුණු ඇමෙරිකානු රටවල් සහ ජපානය යන රටවල්වලට මෙම තත්ත්වය තදින් බලපා ඇති නමුත් ඇතැම් පරිශීලකයන් හට කිසිඳු ගැටලුවකින් තොරව සේවාව භාවිතා කළ හැකි බව ද දැනගන්නට ලැබෙනවා. මේ පිළිබඳව විවිධ මත පළ වූ අතර, මෙය සහ පෙරේදා (දෙවැනිදා ජූලි 02) සිදු වූ cloudflare බිඳවැටීම අතර සම්බන්ධයක් ඇති බවට විවිධ ප්‍රචාරයන් පවා පැතිර ගියා. Facebook සිදුකිරීමට යන major update වෙත සිදුවන පෙර සැකසුම් ක්‍රියාවලියක් නිසාවෙන් ඔවුන්ගේ Content Delivery Network (CDN) එක වෙත යම් බලපෑමක් සිදුවන්නට ඇති බව බොහෝ දෙනා මත පළ කරනවා. කෙසේ වෙතත්, මේ වන විට සියල්ල යථා තත්ත්වයට පත් කිරීමට හැකි වූ බව facebook සමාගම twitter පණිවිඩයක් මඟින් දන්වා තිබෙනවා.

මේ බිඳවැටීමත් සමග බලපෑ අනෙක් සේවාවන් ගැන වගේම, බොහෝ වෙබ් අඩවි බිඳවැටීම් පිළිබඳ live map සපයන down detector වෙබ් අඩවිය හරහා අදාළ සේවාවන් අක්‍රීය වී ඇති ප්‍රදේශයන් සහ කාලය ගැනත්, යථා ස්වරූපය පිළිබඳවත් විස්තර දැනගැනීමට හැකියාව පවතිනවා.

ලංකාවේ නිර්මාණය වූ සුපිරි ගණයේ Multi-Player ක්‍රීඩාව“Extraction Valley™ Devil’s Curse” පසුගිය දිනෙක එළිදැක්වුණා.

අසාධ්‍ය මට්ටමේ රෝගීන්ට ජීවිත බේරා ගන්නට රුධිරය අත්‍යවශ්‍ය යි. මේ, එයට සහායක් ලෙස Roar අප සංවිධානය කළ වැඩසටහන යි.

දිනෙන් දින දියුණු වන තාක්ෂණයත් සමග අද වෙද්දී ශ්‍රී ලංකාවත් ඉතා සීග්‍රයෙන් දියුණු වෙමින් පවතිනවා. තාක්ෂණික ලෝකය එසේ වෙනස් වෙද්දී මිනිසුන් තම නිදහස් කාලය ගෙවන ආකාරයේත් යම් පෙරළියක් සිදුවුණා. බොහෝ නිවෙස්වල ‘පරිගණකය’ අනිවාර්ය අංගයක් බවට පත් වීමත් සමග ම, පරිගණක ක්‍රීඩා කරළියට ආවා. පරිගණක ක්‍රීඩා එක්ක අද වෙද්දී සමාජය මුහුවෙමින්, වෙනස් වෙමින් යන ආකාරය ගැන ගේම්වලින් ගේමක් දෙන්න යන, ලංකාවේ ගේමර්ස්ලා යන ලිපියෙන් මීට පෙර අප විමසුමක් කළා ඔබට මතක ඇති. ක්‍රීඩකයන් ගැන එසේ කතා කරද්දී, එවැනි පරිගණක ක්‍රීඩා නිර්මාණය කරන නිර්මාණකරුවන් පිළිබඳවත් අමතක කරන්නට බැහැ. මේ කියන්න යන්නේ, ලංකාවේ නිර්මාණය වෙමින් පැවති සුපිරි ගණයේ Multi-Player පරිගණක ක්‍රීඩාවක නිල එළිදැක්වීම පිළිබඳව යි.

ලංකාවේ නිර්මාණය වෙමින් පවතින තවත් විශිෂ්ට ගණයේ පරිගණක ක්‍රීඩාවක් ලෙස RAM Studios කණ්ඩායම නිර්මාණය කරන Extraction Valley නම් යුධමය ක්‍රීඩාව හඳුන්වන්න පුළුවන්. ඔවුන් පවසන අන්දමට මේ තරම් සවිස්තරාත්මක සහ දියුණු graphics ලක්ෂණ සහිතව ලංකාවේ නිර්මාණය වන පළමු Multi-Player පරිගණක ක්‍රීඩාව මෙය යි. 2018 වසරේ ඇරඹුණු මෙම ක්‍රීඩාවේ නිර්මාණ කටයුතු මේ වෙද්දී අවසන් වෙලා තිබෙනවා. Pre-alpha මට්ටමෙන් මේ ක්‍රීඩාව නොමිලයේ අත්හදා බැලීමටත් පසුගිය කාලයේ ඔවුන් ලාංකිකයන් වෙත අවස්ථාව ලබා දුන්නා. “Extraction Valley™ Devil’s Curse” මේ මස 23 වෙනි දා නිල වශයෙන් එළිදැක්විමට සියලුම කටයුතු මේ වෙනකොට සූදානම්. එදාට Roar-සිංහල කණ්ඩායමත් Online Media Partner වශයෙන් ඔවුන්ට සහයෝගය ලබාදෙන්නේ ඉතාමත් සතුටින් මෙන්ම ආඩම්බරයෙන්.

දැන් අපි බලමු මේ ක්‍රීඩාව ක්‍රීඩා කරන්න නම් ඔබේ පරිගණකයේ පැවතිය යුතු System Requirement මොනවාද කියලා.

කෙසේවෙතත්, මේ ක්‍රිඩාව ඔබට බාගත කරගන්න නම් තව ටික දවසක් බලන් ඉන්න සිද්ධ වෙනවා. සාමාන්‍ය ජනතාව වෙත මෙය නිකුත් කරන්න ලබන මාසේ පළවෙනි සතිය පමණ ගතවේවි. Unreal Engine 4 මඟින් නිර්මාණය වෙන මෙම ක්‍රීඩාව first වගේ ම third person යන දෙයාකාරයට ම ක්‍රීඩා කරමින්, ඒ අත්දැකීම් අත්විඳින්න ඔබට හැකියාව ලැබෙනවා. පළමු නිකුත් කිරීම වෙත ලංකාවේ අතිශය ප්‍රසිද්ධ youtubersලා ගණනාවක් සම්බන්ධ වීමටත් නියමිත යි.

Pre-alpha මට්ටමේ දී සිදුකළ අත්හදා බැලීමක් පහත වීඩියෝව හරහා දැක බලා ගන්න ඔබට පුළුවන්.

මේ Extraction Valley පරිගණක ක්‍රීඩාව නිර්මාණය කරන RAM Studios කණ්ඩායම සම්මාන උළෙලවල් කිහිපයක දී ඇගයුමට ද ලක්වුණා.

ඔය පහත තියෙන්නේ Extraction Valley ක්‍රීඩාවේ Screen Captures කිහිපයක්.

RAM Studios කණ්ඩායම පහත සබැඳිවලින් සම්බන්ද කරගන්න ඔබට පුළුවන්.

ශ්‍රී ලාංකික නාමය ජාත්‍යන්තර තලයට රැගෙන යන්නට වෙර දරන RAM Studios කණ්ඩායමට Roar-සිංහල අපෙන් උණුසුම් සුභ පැතුම්!

අප හොඳින් දන්නා වගේම, අපේ කනට හුරු ගීත නිර්මාණ විශාල සංඛ්‍යාවක් ගායනා කරපු, ලෝක ප්‍රසිද්ධ එකිනෙකට වෙනස් ගීත රැසක් නිර්මාණය කරපු සංගීත කණ්ඩායමක් වන Backstreet Boys ගැන මේ තොරතුරු ඔබ දැන සිටියා ද?

පරිගක ක්‍රීඩාවලින් මනසට අහිතකර බලපෑමක් සිදුවන බවට ලෝකයේ ප්‍රසිද්ධ මතයක් පවතිනවා. පසුගිය වසරේ වාර්තා වුණු සිදුවීමක් නිසාවෙන් මේ කතාබහ තවත් දුරටත් පැතිරෙන්නට හේතු වුණා. Call of Duty ක්‍රීඩාවෙන් පරාජයට පත් තරුණයෙකු, තමන්ගේ මිතුරාට උල් ආයුධයකින් ඇන තුවාල සිදුකිරීම මෙම සිදුවීම යි. මේ එක සිදුවීමක් පමණ යි. ලංකාවේ එතරම් සුලබ නොවුණත්, අනෙක් රටවල මෙවැනි සිදුවීම් වාර්තා වෙද්දී විශේෂයෙන්ම ඒ හා සබැඳි පරිගණක ක්‍රීඩා පිළිබඳව සඳහන් වූ අවස්ථා එමට යි. 2018 වසරේ මෙවැනි සිදුවීම් බහුල ව සිදුවුණු වසරක් ලෙසින් සඳහන් වෙනවා.

සමහර ක්‍රීඩාවන්වල ඇති ප්‍රචණ්ඩකාරී තත්ත්වයන් ඔස්සේ කෙනෙකුගේ මනස විකෘති කර, ප්‍රචණ්ඩත්වය සාමාන්‍ය දෙයක් බවට පත් කරන්න හේතු වෙන බව මේ මතය දරන පිරිසේ අදහස යි. ඒ වගේම මේ ක්‍රීඩාවන් හරහා සංවේදී බව අඩු වීමටත්, ඉක්මනින් තරහ යාමේ තත්ත්වයන් ඇති වන්නට පුළුවන් බවත් ඔවුන් අතර තවත් මතයක්. කෙසේ වෙතත්, එය එසේ නොවන බවට මතයන් හුවා දක්වන්නන් සඳහන් කරන්නේ එලෙසින් මනස විකෘති වේ නම් මීට වඩා අතිශය ප්‍රචණ්ඩකාරී තත්ත්වයන් ඇති විය හැකි බව යි.

පසුගිය දිනෙක ලෝක සෞඛ්‍ය සංවිධානය (WHO) විසින් video game ක්‍රීඩා කිරීම තුළින් ඇතිවන කැළඹිලි සහගත තත්ත්වය මානසික රෝගයක් ලෙස නම් කිරීමට කටයුතු කර තිබෙන බව වාර්තා වුණා.රෝග පිළිබඳ ජාත්‍යන්තර වර්ගීකරණයේ (International Classification of Diseases) 11 වන සංස්කරණය අනුව (ICD 11) මෙම තත්ත්වය ද රෝගයක් ලෙස ගණන් ගැනෙනවා. මෙය ක්‍රියාත්මක වෙන්නේ 2022 සිට යි.

මෙහි රෝග ලක්ෂණ ලෙසින් ඔවුන් හඳුන්වන්නේ සිය දෛනික කටයුතුවලින් බැහැරව පරිගණක ක්‍රීඩාවල නිරත වීම, දැඩි ලෙස ඇබ්බැහි වීම නිසාවෙන් ක්‍රීඩා නොකර සිටිය නොහැකි වීම ආදී ලෙසින්. කෙසේ නමුත් Entertainment Software Association මේ තීරණය වෙත දැඩි ලෙස විරෝධතාවය පලකරනවා. ඔවුන්ගේ නිල වෙබ් අඩවිය හරහා නිවේදනයක් නිකුත් කරමින් ඔවුන් සඳහන් කරන්නේ ලෝක සෞඛ්‍ය සංවිධානය මේ තීරණය වහාම අවලංගු කළ යුතු බව යි. නමුත් මෙම වර්ගීකරණයට gaming disorders ඇතුළත් කිරීමට පෙර ඔවුන් විවිධ රටවල් ගණනාවක් ඇසුරෙන් ද ජන කණ්ඩායම් අතර ද පර්යේෂණ සිදු කර, ඒ මඟින් ලැබුණු තොරතුරු අනුව එම වර්ගීකරණයට මෙය ඇතුළත් කර ඇති බව WHO පෙන්වා දෙනවා.

මේ හා සමානවම සමහර රටවල් ඇතැම් පරිගණක ක්‍රීඩා තහනම් කිරීම, සහ ක්‍රීඩා කිරීමට කාල සීමාවන් පැනවීම් පසුගිය මාස කිහිපය පුරාවටම වාර්තා වුණා. උදාහරණයක් ලෙස ඉන්දියාවේ ගුජරාට් ප්‍රාන්තයේ PUBG ක්‍රීඩාව තහනම් කිරීම සහ එය නොතකා ක්‍රීඩාවේ යෙදුනු පිරිසක් ගුජරාට් පොලිසිය අත්අඩංගුවට ගෙන, පසුව ඇප මත නිදහස් කිරීම හඳුන්වන්න පුළුවන්. Hindustan times වෙබ් අඩවියේ මේ පුවත පල වී තිබුනේ ‘Demon in every house’: 10 arrested in Gujarat for playing PUBG යන සිරස්තලයත් සමග යි. ගුජරාට් ප්‍රාන්තයේ රජය මේ තීරණය ගෙන තිබුනේ ළමයින් පාඩම් වැඩ පසෙක ලා මේ ක්‍රීඩාවේ නිරත වන බව දෙමව්පියන් සහ අධ්‍යාපන බලධාරීන් නැගු මැසිවිලි නිසාවෙන්.

මේ වර්ගීකරණය යටතේ video game play කරන සියළුදෙනා මෙම වර්ගීකරණය යටතේ මානසික රෝගීන් ලෙස නොසැළකෙන බවත්, මේ අතරින් ඉතාමත් සුළු පිරිසක් පමණක් මානසික රෝගී තත්ත්වයන්ගෙන් පෙළෙන බවත් ලෝක සෞඛ්‍යය සංවිධානය වැඩිදුරටත් පෙන්වා දෙනවා. වෘත්තියක් ලෙසින් දියුණු වන මේ ක්‍රීඩාවන්, අනාගත ඔලිම්පික් තරග සඳහාත් එකතු වීමට නියමිත නමුත්, මේ වර්ගීකරණයට එකතු වීම පරිගණක ක්‍රීඩාවන්වල දිශානතියට යම් බලපෑමක් එල්ල කරනු ඇති බව නම් නොරහසක්.

මේ වසර පුරාවට අන්තර්ජාලයේ අඳුරු පැතිකඩ පිළිබඳ බොහොම කතාබහට ලක්වුණා. එය තවත් ඉහළ දමමින්, පසුගිය දිනෙක Database Server 50,000 ගණනකට Nansh0u නමින් හඳුන්වන චීන හැකර්කරුවන් පිරිසක් ප්‍රහාරයක් එල්ල කළා. APT ගණයේ සයිබර් ප්‍රහාර එල්ල කරන පිරිසක් ලෙසින් මොවුන් ප්‍රසිද්ධ යි. Advanced persistent threat (APT) නමින් හඳුන්වන මේ ප්‍රහාරයන් සාමාන්‍යයෙන් එල්ල වෙන්නේ යම් රටක රාජ්‍ය ආයතන, සමාගම්, හමුදාවන් හෝ දේශපාලන බලාධිකාරය ඉලක්ක කරගෙන යි.

සාමාන්‍ය සයිබර් ප්‍රහාරයකුත්, ඇඩ්වාන්ස්ඩ් ප’සිස්ටන්ට් ත්‍රෙට් සයිබර් ප්‍රහාරයක් අතරත් විශාල වෙනසක් තිබෙනවා. සාමාන්‍යයෙන් මෙවැනි දැවැන්ත ප්‍රහාර පිටුපස බොහෝ විට එක පුද්ගලයෙකු නොව විශාල වශයෙන් සංවිධානය වූ, විශාල මූල්‍ය බලයක් සහිත රාජ්‍යක් හෝ ඉතා බලවත් පාර්ශවයක් සිටිනවා. බොහොමයක් සයිබර් හැකින් ප්‍රහාරවල අරමුණක් බවට පත්වෙන, ප්‍රසිද්ධිය ලබා ගැනීමේ අරමුණෙන් හෝ තම හැකියාව පෙන්වීමේ අරමුණෙන් මෙවැනි ප්‍රහරයක් සිදු වන්නේ නැහැ. මාස ගණනාවක සැලසුම් සහ දත්ත, තොරතුරු එකතුවක් මත ක්‍රියාත්මක වන අතිශයින් සූක්ෂම ප්‍රහාරයක් ලෙස මෙය හඳුන්වන්න. පුළුවන්. ප්‍රහාරයට ලක් වෙන පාර්ශවය ඒ පිළිබඳව දැනගන්නා තෙක් වසර ගණනාවක් තිස්සේ වුව ද මෙවැනි ප්‍රහාරයන් ක්‍රියාත්මක වීමට ඉඩ තිබෙනවා. චීනයේ සහාය ලබන APT කණ්ඩායම් ඇමරිකාවෙන් යුධ රහස් සොරකම් කරන බවට කලකට පෙර චෝදනා නැගුනා.

APT ප්‍රහාරකයන්ගේ ප්‍රධාන අරමුණු තුනක් අපට හඳුනාගන්න පුළුවන්

බහුතරයක් ප්‍රහාරකයින් මේ සඳහා යොදාගන්නේ ඊමේල් ඔස්සේ කරන ෆිෂින් ප්‍රහාර සහ සීරෝ ඩේ එක්ස්ප්ලොයිට් /zero-day exploit (මෘදුකාංග සහ මෙහෙයුම් පද්ධතිවල ඇති දෝෂ හරහා මෙවලමක් ආධාරයෙන් සිදු කරන සයිබර් පහරදීම් ). APT ප්‍රහාරකයින් කණ්ඩායමක් මෙවැනි සීරෝ ඩේ එක්ස්ප්ලොයිට් 4ක් යොදාගෙන ඉරානයේ න්‍යෂ්ඨික බලාගාරවලට සිදුකළ පහරදීම ඔබට මතක ඇති. මේ සීරෝ ඩේ එක්ස්ප්ලොයිට් හඳුනාගනිමින් විකිණීම අද වන විට විශාල ව්‍යාපාරයක් බවට පත්වී තිබෙනවා.

Nansh0u කණ්ඩායම පසුගිය දිනක එල්ල කළ ප්‍රහාරය මඟින් වෙබ් අඩවි 50,000ක පමණ MS-SQL සහ PHPMyAdmin යෙදවුම්වල username සහ passwords සොරාගෙන ඇති බව අනාවරණය වුණා. Hosting සපයන සමාගම් ගණනාවකින් ලබාගත්, එකකට එකක් වෙනස් payloads 20 පමණ භාවිත කරමින් මෙය සිදු කර ඇති බව සඳහන් වෙනවා. සාමාන්‍ය port scanner එකක් හරහා එළියට විවෘතව පවතින Servers හඳුනාගනිමින් ඒවාට brute force attacking එල්ලකිරීම මඟින් අදාළ මුරපද සොයාගෙන තිබෙනවා. දැනට අනාවරණය වී ඇති ආකාරයට cryptocurrency mine කිරීම මේ ප්‍රහාරයේ මූලික අරමුණ බවට පත්වී තිබෙනවා. TurtleCoin නැමැති cryptocurrency නිපදවීම සඳහා මෙය දැනට භාවිත කර තිබෙනවා. මේ ප්‍රහාරයට මූලික හේතුව බවට සැක පල කරන්නේ server සඳහා සුලභ මුරපද (common passwords) භාවිතා කර තිබීම බවයි සයිබර් ආරක්ෂක පර්යේෂකයන් සඳහන් කරන්නේ.

ලෝකයේ සුප්‍රසිද්ධ වෙබ් අඩවියක් වන flipboard.com වෙබ් අඩවිය වෙතත් මේ හා සමාන ප්‍රහාරයක් එල්ල වී තිබුණා. 2018 වර්ෂයේ ජුනි මස 2 වැනි දින සිට 2019 වර්ෂයේ මාර්තු 23 වැනි දින දක්වා, සහ 2019 වර්ෂයේ අප්‍රේල් මස 21 සහ 22 ඇතුළු මාස 10ක පමණ කාලසීමාව ඇතුළත හඳුනා නොගත් හැකර්වරුන් පිරිසක් විසින් Database access කර තිබුණා. User Name, Password ඇතුළු තවත් දත්ත විශාල ප්‍රමාණයක් ඔවුන්ට ලබාගත හැකිව තිබී ඇති බව නිල වෙබ් අඩවියේ සටහනක් තබමින් ඔවුන් සඳහන් කළා. තම මිලියන 150කට අධික පරිශීලකයන්ගේ bank details, credit card numbers වැනි දේ එම වෙබ් අඩවිය මඟින් ගබඩාකර නොගන්නා නිසාවෙන් ඒ කිසිවක් ඔවුන් අතට පත් නොවූ අතර, flipboard ගිණුම වෙත භාවිතා කරන මුර පද වෙනත් ගිණුම් සඳහා භාවිතා කරන්නේ නම් ඒවා වෙනස් කර ගන්නා ලෙස ඔවුන් දැනුම් දෙනවා.

ශ්‍රී ලාංකීය ඩිජිටල් නව්‍යකරණයේ පෙරගමන්කරු හෙළකුරු සමාගම පසුගිය දා ජාත්‍යන්තර ප්‍රමිතියේ අති නවීන කාර්යයාලීය නිවහනකක් වෙත පියනැගුවා. 2011 වර්ෂයේ දී තරුණ ව්‍යාවසායක ඉංජිනේරු ධනික පෙරේරා ආරම්භ කළ හෙළකුරු සමාගම (භාෂා ලංකා පුද්ගලික සමාගම) මෙතෙක් ආ ගමනේ සුවිශේෂීම සංධිස්ථානයක් ලෙස මෙය හඳුන්වන්න පුළුවන්.

තොරතුරු තාක්ෂණ ක්ෂේත්‍රයේ දැවැයින්තයින් රාශියකගේ සහභාගීත්වයෙන් පැවති මෙම නව කාර්යයාල සමාරම්භක උළෙල සඳහා ඩිජිටල් යටිතල පහසුකම් අමාත්‍යාංශයේ හිටපු ලේකම් වසන්ත දේශප්‍රිය ප්‍රධාන ආරාධිත වශයෙන් සහභාගී වූ අතර, මොරටුව විශ්වවිද්‍යාලයයේ පරිගණක විද්‍යා ඉංජිනේරු, හිටපු අධ්‍යයනාංශ ප්‍රධානී විශාඛා නානායක්කාර, LK වසම් ලේඛණාධිකාරියේ ප්‍රධානී ගිහාන් ඩයස්, ශ්‍රී ජයවර්ධනපුර විශ්වවිද්‍යාලයයේ ව්‍යවසායකත්ව අධ්‍යයනාංශ ප්‍රධානී ශාමන් උදයංග ඇතුළු විද්වතුන් ද, හෙළකුරු සමාගමේ සේවාලාභී හා හවුල්කාර ආයතනයන් වන ශ්‍රී ලංකාවේ ප්‍රධාන පෙළේ බැංකු, ටෙල්කො, සහ මාධ්‍ය ආයතන නියෝජිතය කරමින් විශේෂ ආරාධිතයින් රාශියක් ද, ආරම්භක-සමාගම් දිරිගැන්වීමේ ආයතන නියෝජනය කරමින් තවත් ආරාධිතයින් රාශියක් ද එක් වී සිටියා.

ශ්‍රී ලාංකීකයින්ගේ එදිනෙදා ඩිජිටල් ජීවිතයට අත්‍යාවශ්‍ය, සිංහල යතුරුකරණය ඇතුළු දෛනික ඩිජිටල් සේවාවන් රැසක් තම ඩිජිටල් නිපැයුම් හරහා පිරිනමන හෙළකුරු සමාගම, මේ වන විට මිලියන 5කට අධික වැඩිම ඩවුන්ලෝඩ් ගණනක් සහිත ශ්‍රී ලාංකීය ජංගම දුරකථන යෙදුම නිපදවා තිබෙන අතර, ශ්‍රී ලංකීකයින්ගේ හදවතේ රැඳි අංක 1 ඩිජිටල් සන්නාමය බවටත් පත් වී තිබෙනවා. ජාත්‍යන්තර ප්‍රමිතියෙන් සහ උසස් ගුණාත්මයෙන් යුත් නව්‍ය ඩිජිටල් නිපැයුම් දේශීය වෙළඳපොළට ගැළපෙන ලෙසින් දේශීය හැඩයකින් හඳුන්වාදීම සහ නව්‍ය ව්‍යාපාර ආකෘතීන් යටතේ ප්‍රචලිත කිරීම හෙළකුරු සමාගමේ මේ සාර්ථකත්වයට හේතු වුණා.

මේ වන විට "හෙළකුරු" සන්නාමයෙන් නොනැවතී, ශ්‍රී ලාංකීය ව්‍යාපාර සඳහා නව්‍ය අන්තර්ජාල ගෙවීම් සේවා හඳුන්වා දෙමින් පෙරට ආ නව "PayHere" ඩිජිටල් සන්නාමයත්, රටේ අනාගත පරපුරට නව්‍ය ඩිජිටල් අධ්‍යාපන ක්‍රමවේද හඳුන්වා දෙමින් පෙරට ආ "හපන්" ඩිජිටල් සන්නාමයත් හෙළකුරේ සහෝදර සන්නාමයන් ලෙස දේශීය වෙළඳපොළට එක් වී ඇති අතර, ඒවා මඟින් ද ශ්‍රී ලාංකීකයින්ට පෙර අත් නොවිඳි නව්‍ය ඩිජිටල් සේවාවන් රැසක් සැපයෙනවා.

මෙතෙක් කල් නිපැයුම් මූලික කරගනිමින් ආරම්භක සමාගමක් ලෙස කටයුතු කළ හෙළකුරු සමාගමේ මේ නව සමාගම් කාර්යයාලීය සම්ප්‍රාප්තිය, මින් ඉදිරියට "ඩිජිටල් තාක්ෂණයන් හරහා මහජනයා සවිබල ගැන්වීම" යන සමාගමික දැක්ම පෙරදැරි කරගනිමින් සමාජ අවශ්‍යතාවයන් සපුරාලීමට කැප වූ පරිණත සමාගමක් වීමේ සංකේතාමක ප්‍රවිශ්ටයක් ලෙස දැක්විය හැකි බව, මෙම උත්සවයේ ප්‍රධාන කථාව අතරතුර අදහස් දැක් වූ සමාගමේ නිර්මාතෘ ධනික පෙරේරා සඳහන් කළා. එමෙන්ම මෙවන් ජාත්‍යන්තර ප්‍රමිතියෙන් යුත් අති නවීන කාර්යයාලයක් තම කාර්යයමණ්ඩලයට තිළිණ කිරීම ව්‍යවසායකත්ව ජීවිතයේ ආරම්භයේ පටන් පැවති සිහිනයක් බවත්, වසර 8කට පසු මෙදින කිසිඳු බාහිර ප්‍රාග්ධන ආයෝජනයකින් තොරව එම සිහිනය සැබෑ කරගත හැකි වූයේ තම කාර්යයමණ්ඩලයේ කැපවීම සහ තම ඩිජිටල් සේවාවන් ගැන දේශීය පාරිභෝගිකයින් තැබූ අඛණ්ඩ විශ්වාසය නිසා පමණක්ම බවත් විශේෂයෙන් සඳහන් කළා. හෙළකුරේ ආයතනයේ නව ලිපිනය නො.46, ගාලු පාර, කළුතර වන අතර Google Maps ඔස්සේ ද ඔබට එම ස්ථානය සොයාගත හැකිය. ශ්‍රී ලාංකීය ඩිජිටල් නව්‍යකරණයේ පෙරගමන්කරු භාෂා ආයතනයට roar සිංහල අපෙන් සුබපැතුම්.

මීට ටික කලකට පෙර roar සිංහල අපත් ධනික පෙරේරා සමග ලංකාවේ ව්‍යවසායකත්වය සහ තාක්ෂණික භාවිතය පිළිබඳව කතා බහකට යොමුවුණා.

දේශගුණික වෙනස්වීම් සාමාන්‍ය මිනිස් ජිවිතය විවිධ සංකීර්ණ ආකාරයන් ඔස්සේ වෙනස් කිරීමට, සහ හැඩ ගැස්සවීම් සිදු කිරීමට සමත්. මිනිස් ජිවිතයේ බොහෝ පැතිකඩ මෙන්ම ලිංගික සාඑල්‍යතා අනුපාතිකය සඳහා ද දේශගුණික තත්ත්වයන් බලපෑම් සිදු කරන බව විවිධ නව විශ්ලේෂණයන් ඔස්සේ හෙළි වී තිබෙනවා. විශේෂයෙන් නිවර්තන දේශගුණයක් සහිත රටවල ලිංගික සරුබව අනෙක් රටවලට සාපේක්ෂව ගත්කල තරමක් වැඩි බව මේ විශ්ලේෂණයන් ඔස්සේ හෙළි වී තිබෙනවා. සමකය ආසන්නයේ පවතින නිවර්තන දේශගුණයක් සහිත බොහෝ රටවල් ආර්ථිකමය වශයෙන් යම් තරමකට දුර්වල වීමට මේ කාරණය හේතු වී තිබෙනවා. වක්‍රාකාරව දුප්පත් රටවල් සහ පොහොසත් රටවල් අතර ආර්ථික තත්ත්වයන්හි විශාල පරතරයන් ඇති වන්නේ මේ දේශගුණික වාතාවරණයන් නිසාවෙන් බව විශ්ලේෂණයෙන් හෙළිවුණු කරුණක්.

මෙම අධ්‍යයනය සිදු කිරීමේ දී විශ්ලේෂකයන් සම්මත ආර්ථික න්‍යායන් සංයුක්ත කරමින් ආර්ථිකයේ විවිධ අංශවලට දේශගුණික විපර්යාසයන් ඔස්සේ බලපෑම් ඇතිවිය හැකි ආකාරය පිළිබඳ ආකෘතියක් ගොඩනගා තිබෙනවා. ආර්ථිකයේ අනෙක් කොටස් කාලගුණයට එතරම් සංවේදී නොවුන ද දේශගුණික විපර්යාස හේතුවෙන් කෘෂිකර්මාන්තය නිසාවෙන් ආර්ථිකයට සිදු වන බලපෑම් ඉහළ මට්ටමක තිබෙනවා. කොලොම්බියාව මත පදනම් වූ උපකල්පිත ආර්ථික මොඩියුලයක් ආශ්‍රයෙන් දේශගුණික විපර්යාසවල ආර්ථිකමය බලපෑම පිළිබඳව ඔවුන් විශ්ලේෂණය සිදු කළා. දිගින් දිගටම වැඩිවන ජනගහනය සහ අධික කාබන් විමෝචනය දිගටම පැවතුනහොත්, දේශගුණික විපර්යාස නිසාවෙන් කෘෂිකාර්මික ඵලදායිතාව වෙත දැඩි ලෙස බලපෑම් ඇතිවන බව ඔවුන් නිරීක්ෂණය කළා. මේ හරහා කෘෂිකාර්මික ක්ෂේත්‍රය වෙත ශ්‍රම වෙළඳපොළෙන් වැඩි කොටසක් යොමු වීම සිදු වන්නට පුළුවන්.

සාමාන්‍යයෙන් සමකය ආසන්නයේ පවතින, බොහොමයක් නිවර්තන දේශගුණික තත්ත්වයන් පවතින රටවල ප්‍රධාන ජීවනෝපාය සහ ප්‍රධාන ආර්ථික පෝෂකයක් ලෙසින් කෘෂිකර්මාන්තය හඳුන්වන්න පුළුවන්. මේ ක්ෂේත්‍රයේ යෙදීම සඳහා අධ්‍යාපන සුදුසුකම් අවශ්‍ය නොවීම, සහ පවුලේ දරුවන් සියල්ලන් වෙත අධ්‍යාපනය ලබා දීමට තරම් ආර්ථිකමය හැකියාව නොමැති වීම නිසාවෙන් තමන්ගේ කෘෂිකර්මාන්ත රැකියාව වෙත තම දරුවන් යොමු කිරීම බහුලව සිදුවන්නක්. මෙලෙසින් අඩු අධ්‍යාපනයක් යටතේ ඉදිරි සමාජයක් වෙත දරුවන් යොමු කිරීම හරහා රටෙහි සාක්ෂරතාව පහළ බසිනවා වගේම උද්ධමනය වැනි ගැටළු රැසකට මේ හේතුව මුල පුරනවා. උදාහරණයක් විදිහට කොලොම්බියාව වැනි රටක ලිංගික සරුබව හා අඩු අධ්‍යාපන මට්ටමක් සහිත බව නිසාවෙන් ආර්ථිකය දැඩි ගැටලුකාරී තත්ත්වයන් වෙත පත්ව තිබේ. මෙය චක්‍රයක් ලෙසින් සිතුවහොත් ආර්ථික අවපාතයන් වෙත ලිංගික සාපල්‍යතා මට්ටම ඉහළ බව බලපෑම් එල්ල කර තිබෙනවා.

අවසානයේ පර්යේෂකයන් ඔවුන්ගේ මොඩුලයන් සහ පර්යේෂණ ස්විස්ටර්ලන්තය වෙත ආදේශ කළ විට එක හා සමාන රටාවන් දැකගන්නට ලැබී තිබුණා. ඔවුන් පැමිණි නිගමනය බවට පත් වුණේ නිවර්තන දේශගුණයක් පවතින රටවල කාලගුණික වෙනස්කම් හේතුවෙන් ලිංගික සාපල්‍යතා අගයන් ඉහළ අතර සාපේක්ෂව අඩු අධ්‍යාපනික මට්ටමක් පවතින අතර, ඉහළ අක්ෂාංශවල පවතින රටවල මෙහි ප්‍රතිවිරුද්ධ රටාවන් දැකගන්නට ලැබෙනවා.

දේශගුණික, කාලගුණ විපර්යාසයන් වගේම සරු භාවය කෙරෙහි බලපාන වෙනත් යාන්ත්‍රණ විශාල ප්‍රමාණයක් පවතිනවා. අනෙක් ආර්ථික සාධක, සංස්කෘතික වෙනස්කම්, සහ ස්වාභාවික විපත් හා යුද්ධ වැනි සිදුවීම් ඒ යටතට ගැනෙනවා. විශ්ලේෂණයන්ට අනුව සරු භාවය පිළිබඳ බලපෑම "ධනවත් ඉහළ-අක්ෂාංශික රටවල් සහ දුප්පත් සමක ආසන්න රටවල් අතර ආදායම් පරතරය වැඩි කළ හැකි බව” ඔවුන්ගේ මතය යි. මේ මතයන්වලට වඩා වෙනස් මතධාරින් ද සිටින බව කිව යුතුම යි.

ඉන්දියාවේ සහ ලංකාවේ අතිශය ජනප්‍රියත්වයට පත්වූ #PrayForNeasamani කියන ටැග් එක ගැන කුතුහලෙන් ද ඉන්නේ?

Roar ටෙක් විදිහට අප ගේම්වලින් ගේමක් දෙන්න යන, ලංකාවේ ගේමර්ස්ලා ගැන වගේම ජාත්‍යන්තරය ජය ගන්න සූදානම් වෙන ලංකාවේ නිර්මාණය වූ games ගැනත් ලිපි පල කළා ඔබට මතක ඇති. මේ කියන්න යන්නේ ලංකාවේ පිරිසක් ටිකක් වෙනස් ආකාරයකට ලංකාවේ සම්ප්‍රදායික උත්සවයක් සමරපු ආකාරය ගැන. Multi Theft Auto San Andreas එහෙමත් නැත්නම් MTA San Andreas කියන්නේ ලෝකයේ බොහෝ දෙනෙක් ක්‍රීඩා කරන multiplayer video game එකක්. මේ ක්‍රීඩාව ගැන කතා කරද්දී OnlineLK team එක කියන්නේ අමතක කරන්නම බැරි පිරිසක්. මේ ක්‍රීඩාව ලාංකිකයන්ට සමීප කිරීමට පෙරමුණ ගත පිරිසක් ලෙසින් මොවුන් හඳුන්වන්න පුළුවන්. 2011 වසරේ සිට මේ පිරිස මේ කටයුත්තේ නිරත වෙනවා.

පසුගිය කාලයේ සිදු වූ කණගාටුදායක සිදුවීම් මාලාව නිසාවෙන් පුරුදු පරිදි වෙසක් උත්සවය සැමරීම තරමක් අපහසු දායක කටයුත්තක් බවට පත්වුණා. නමුත් OnlineLK Team එකට හැකි වුණා තරමක් වෙනස් විදිහට වෙසක් සමරන්න තාක්ෂණයත් එක්ක නිතර ගැටෙන තරුණ ප්‍රජාවට අවස්ථාවක් ලබා දෙන්න. ඒ ඔවුන් ගේ වෙසක් කලාපය හරහා. මේ වෙසක් කලාපය පැවැත්වෙන්නේ online වීම තමයි මෙහි තියෙන සුවිශේෂීත්වය වෙන්නේ. පසුගිය වසරේ ඔවුන් පැවැත්වූ වෙසක් කලාපයට වඩා මේ වසරේ ඇති උත්කර්ෂවත් අන්දමින් එය නිර්මාණය කරමින් පවත්වන්නට ඔවුන් කටයුතු කර තිබුණා. සාමාන්‍ය වෙසක් සැමරුමක් සේම දන්සැල්, වෙසක් තොරණත්, රුවන්වැලි මහා සෑ ආකෘතියක් පවා මෙහි නිර්මාණය කර තිබීම විශේෂී වුණා. වෙසක් අසිරිය විඳගන්න වගේම අලුත් මිතුරන් හඳුනගන්නත් මේක හොඳ අවස්ථාවක්. ඒ වගේම OnlineLK Team එක ඔවුන්ගේ server එකේ වෙසක් බලන්න එන අයට විශේෂ තෑගි කිහිපයක් ද ලෑස්ති කර තිබෙන බව අපට දැනගන්න ලැබුණා. ඔබත් මේ වෙසක් කලාපය හා එක්වෙන්න කැමැත්තක් දක්වනවා නම් පහත link එක හරහා San Andreas game එක download කරගෙන ඔබගේ PC එකේ ස්ථාපනය කළ යුතු වන අතර, ඊට අමතරව MTA Client Application එක ද install කරගත යුතු වෙනවා.

මේ Game එක සහ Supporting software එක install කළ පසුව පහත server address එක ඇතුළත් කර OnlineLK MTA San Andreas Freeroam Server එකට connect වෙලා ඔබටත් MTA Online වෙසක් අසිරිය විඳගන්න අවස්ථාව ලැබෙනවා.

Server Address: mtasa://mta.onlinelk.net:22003

Game එක install කිරීම හෝ මේ පිළිබඳව යම්කිසි ගැටළුවක් ඇත්නම් Messenger සේවාව හරහා ඔවුන්ව සම්බන්ධ කරගැනීමේ හැකියාව ද පවතිනවා.

මීට අමතරව තවත් පරිසක් විසින් රටේ වෙසක් අසිරිය ලොවට පෙන්වීම සඳහා vesak.ceyentra.lk නම් වෙබ් අඩවියක් මුදාහැර තිබුණා මේ හරහා, ලෝකයාට අපේ හදවත් තුළ නොනැසී පැවතුන වෙසක් ආලෝකය රැගෙන යාම අරමුණු වුණා.

පසුගිය 2018 වසරේ "Tamil Eelam Cyber Force" ලෙස හඳුන්වාගන්නා පිරිසක් විසින් ශ්‍රී ලංකා රජයේ වෙබ් අඩවි දිගින් දිගටම hack කරමින්, රජයේ හමුදාවන් යුද්ධයේ අවසාන කාලවකවානුව තුළ දී සැලසුම් සහගතව දෙමළ වැසියන් මරා දැමූ බවත්, විශාල කාලතුවක්කු සහ රසායනික අවි භාවිතා කරමින් ප්‍රහාර එල්ල කළ බවත්, දමිළ කාන්තාවන් ලිංගික සිරකාරියන් ලෙස තබාගෙන කටයුතු කළ බවත්, තවමත් ශ්‍රී ලංකාව තුළ මෙම සංහාරය සිදුවෙමින් පවතින බවටත් මත පල කළ බව ඔබට මතක ඇති. එම ප්‍රහාරය එල්ලවූයෙත් මැයි 18 (විජයග්‍රහණ සැමරුම් දිනය) ආසන්න දිනයක බව ඔබට මතක ඇති. මේ වසරේත් පසුගිය 19 වෙනි දා ශ්‍රී ලංකා රජයේ වෙබ් අඩවි ඇතුළු ලංකික වෙබ් අඩවි 13කට අධික සංඛ්‍යාවක් වෙත සයිබර් ප්‍රහාරයක් එල්ල කරන්නට ඔවුන් සමත් වුණා. මේ වෙබ් අඩවි අතරට රාජ්‍ය ආයතන, විශ්වවිද්‍යයයාල හා පෞද්ගලික ආයතන ද ඇතුළුව පහත සඳහන් වෙබ් අඩවිත් මේ ආකාරයෙන් hacking ප්‍රහාරවලට ලක් වී තිබෙන බව සනාථ වී තිබෙනවා.

TechCERT ආයතනය වැඩිදුරටත් ප්‍රකාශ කරන අන්දමට මෙවර සිදුවූ ප්‍රහාරවලට හේතුව ‍පිළිබඳව නිල තොරතුරක් තවමත් වාර්තා නොවන අතර, දේශපාලනික හේතූන් මෙයට බලපාන්නට ඇති බවට ඔවුන් සැක පල කරනවා. එසේම මේ වෙබ් අඩවි බොහොමයක් පැවතුනේ එකම වෙබ් server එකක නිසාවෙන් මෙය mass defense එකක් විය හැකි බවටත් බොහෝ දෙනෙකු මත පල කරනවා. මේ වන විට ප්‍රහාරයට ලක්වූ වෙබ් අඩවි යථා තත්ත්වයට පත් කර තිබෙන බව TechCERT ආයතනයේ ප්‍රධාන විධායක නිලධාරී (CEO) දිලීප ලත්සර, newsfirst වෙත සඳහන් කර තිබුණා.

ප්‍රහාරයට ලක්වූ වෙබ් අඩවි ගණනාවක්ම නිසි අයුරින් යාවත්කාලින කිරීම් සිදු නොවීම නිසා මෙලෙස ප්‍රහාරයට ලක්ව ඇති අතර, ඔබ වෙබ් අඩවියක් පවත්වාගෙන යන්නේ නම් හා ඒ සඳහා Wordpress, Joomla වැනි CMS එකක් භාවිතා කරන්නේ නම් ප්‍රධාන CMS එක සහ අදාළ සියලු plugins සහ security tweak යාවත්කාලින කර ගැනීම සිදු කළ යුතු බව TechCERT ආයතනය දැනුම් දී තිබෙනවා.

\*ඉහත යාවත්කාලින වීම් සිදු නොවුණු වෙබ් අඩවි ලෙස සඳහන් වන්නේ plugins, security tweak, CMS යාවත්කාලින නොවීම පිළිබඳ මිසෙක, වෙබ් අඩවිය වෙත ලිපි ඡායාරුප වැනි දෑ එක නොවුණු බව නොවේ.

සාමාන්‍යයෙන් ආදරවන්තියක්, ආදරවන්තයෙක් හොයා ගන්නකොට අප බොහෝවිට තෝරාගන්නේ සමාන ආශාවන් ඇති සහෘද හදවත් ඇති පුද්ගලයින්. එය තරමක් අපහසු කටයුත්තක් වෙන්න පුළුවන්. අද වෙද්දී එහෙම කෙනෙක් ගැන හිත ගිය ගමන් මුලින්ම කරන දේ වෙන්නේ facebook ඉන්නවා ද කියලා හොයාගෙන, ඔහුව හෝ ඇයව තමන්ගේ මිතුරු ලැයිස්තුවට එකතුකර ගන්න එක. ඒ වගේ කෙනෙක් හොයා ගත්තත් කැමැත්ත ප්‍රකාශ කරන්න ඊට වඩා අපහසු වෙන්න ඉඩ තියෙනවා. පසුගිය අප්‍රේල් මාසේ 30 වෙනි දා පැවති, facebook සමාගමේ F8 2019 developers conference එකේ දී මේ ගැටළුවට ඔවුන් ලබා දෙන්න හිතාගෙන ඉන්න විසඳුම පිළිබඳව පැහැදිළි කළා. මේ විසඳුම ඔවුන් හඳුන්වන්නේ “Secret Crush” යන නමින්. මේ පහසුකම අයත් වෙන්නේ මීට වසරකට පමණ පෙර facebook සමාගම නිවේදනය කළ “facebook Dating” කියන සංකල්පය යටතට යි.

මේ හරහා තමන්ගේ මිතුරු ලැයිස්තුවේ කෙනෙකු පිළිබඳ කැමැත්තක් තියෙනවා නම්, ඒ ගැන දැන්වීමේ හැකියාව ලබා දෙනවා. මේ සේවාවට ඔබේ මිතුරු ලයිස්තුවෙන් නව දෙනෙකු එකතු කරගන්න හැකියාව ලබා දෙනවා. ඒ හරහා ඔහුට හෝ ඇයට ඔබේ Secret Crush list එකේ ඔවුන් සිටිනා බව දන්වනවා. ඒ වගේම ඔබේ Secret Crush list එකට ඇතුළත් කර ගන්නට හැකි පුද්ගලයින් පිළිබඳ suggestions ලබා දීමත් සිදු කෙරෙනවා. මේ සේවාව ලබාගන්නට නම් ඔබ වයස 18ට වැඩි විය යුතු අතර, මේ සේවාව දෙපාර්ශයටම ක්‍රියාත්මක වීමට නම් ඒ දෙදෙනාම අනෙක් කෙනාගේ secret Crush list වල රැඳී සිටිය යුතු යි. Crush එක මේ Dating සේවාව සමගින් එකතු වී නැති නම්, ඔහුගේ හෝ ඇයගේ Secret Crush list එකේ ඔබේ නම නොමැති නම්, මේ පිළිබඳ ඔහුට හෝ ඇයට දැනුම් දීමක් සිදු වන්නේ නම් නැහැ.

මේ සේවාව මෙතෙක් ක්‍රියාත්මක වුණේ කොලොම්බියාව, තායිලන්තය, කැනඩාව, ආජන්ටිනාව, සහ මෙක්සිකෝ යන රටවල පමණ යි. නමුත් මේ වසරේ සිට ෆිලිපිනය, වියෙට්නාමය, සිංගප්පූරුව, මලේශියාව, ලාඕසය, බ්‍රසීලය, පීරු, චිලී, බොලිවියා, එක්වදෝරය, උරුගුවේ, පැරගුවේ, ගයනා, සහ සුරිනාම් යන රටවලට මේ සේවාව ක්‍රියාත්මක වෙනවා. මේ සේවාව ලංකාව වෙත ලබා දීමට නම් තව වසර කිහිපයක් ගතවේවි. facebook සමාගමේ අතුරුමුහුණතේ සිට එක දිගට සිදුවන මේ වෙනස්කම් පිළිබඳ මේ වෙද්දී විශාල කතාබහක් ඇතිව තිබෙන බව නම් නොරහසක්.

මේ දිනවල WhatsApp හරහා ඔබේ ජංගම දුරකතනයට පැමිණිය හැකියැ යි සැලකෙන වයිරසය බොහෝ දෙනෙකුගේ අවධානය දිනාගත් මාතෘකාවක් බවට පත්වෙලා තිබෙනවා. මෙහි ඇත්ත නැත්ත සහ භයානකත්වය පිළිබඳව ඔබ දැනුවත් කරන්න තමයි මේ ලිපිය හරහා බලාපොරොත්තු වෙන්නේ. Facebook සමාගම සතුව පවතින ප්‍රධානතම messaging platform අතර WhatsApp ප්‍රධාන තැනක් ගන්නවා. ලෝකයේ බොහෝ රටවල මෙන්ම ලංකාවේත් ප්‍රධානතම පණිවිඩ හුවමාරු කරගන්නා ක්‍රමයක් ලෙස භාවිත වෙන WhatsApp පසුගිය දින කිහිපයේ විශාල වශයෙන් කතාබහට ලක්වෙන්නට පටන් ගත්තේ, ඒ හරහා පැමිණි ඔබේ දත්ත සොරකම් කිරීමට හැකි බවට සැලකෙන වයිරස කාණ්ඩයේ අනිසි මෘදුකාංගයක් ගැන හෙළිදරව් වීමත් සමග යි.

NSO Group නම් ඊශ්‍රායල සමාගමක් විසින් නිර්මාණය කරන ලද බව සැලකෙන මෙම Spyware එක හරහා ඔබේ දුරකතනයේ camera, microphone, emails, සහ messages වගේම, location වැනි තොරතුරු වෙත අනිසි ලෙස ප්‍රවේශ වීමට සහ භාවිත කිරීමට හැකියාව ලැබෙනවා. WhatsApp ඇමතුම් ලබාගැනීමට භාවිතා කරන protocol එක වන VOIP stack එක හරහා remote code execution (දුරස්ථව අවශ්‍ය code එකක් execute කිරීමේ හැකියාව) කිරීමේ හැකියාව තිබී ඇති අතර, මේ ආරක්ෂණ දුර්වලතාවය භාවිත කරමින් hacking ප්‍රහාරය එල්ලකර තිබෙනවා. එංගලන්ත මානව හිමිකම් නීතිඥයෙකු තමාට පසුගිය මාසයේ ලැබුණු සැක සහිත WhatsApp ඇමතුම් ගණනාවක් නිසාවෙන් මේ පිළිබඳව Citizen Lab ආයතනය වෙත දැනුම් දී තිබෙනවා. ඒ සම්බන්ධව ඔවුන් සිදු කරන ලද පර්යේෂණයකින් අනතුරුව මේ සිදුවීම පිටුපස NSO Group නම් ඊශ්‍රායල සමාගම සිටින බවට සාක්ෂ්‍ය හමුවී තිබෙනවා.

මේ දුර්වලතාවය පවතින බවට හඳුනාගෙන ඇත්තේ පහත WhatsApp සංස්කරණයන් තුළ යි:

WhatsApp - v2.19.134 සංස්කරණයට පෙර සංස්කරණයන්

WhatsApp Business - v2.19.44 සංස්කරණයට පෙර සංස්කරණයන්

WhatsApp - v2.19.51 සංස්කරණයට පෙර සංස්කරණයන්

WhatsApp Business - v2.19.51 සංස්කරණයට පෙර සංස්කරණයන්

WhatsApp - v2.18.348 සංස්කරණයට පෙර සංස්කරණයන්

WhatsApp - v2.18.15 සංස්කරණයට පෙර සංස්කරණයන්

WhatsApp විසින් මේ වන විටත් මේ දුර්වලතාවය නිවැරදි කරමින් නව සංස්කරණයක් නිකුත් කර තිබෙනවා. ඔබේ WhatsApp මෘදුකාංගය තවමත් පවතින්නේ පෙර සඳහන් කළ සංස්කරණවලින් එකක නම් හැකි ඉක්මනින් එය යාවත්කාලින කර ගන්නා ලෙස WhatsApp සමාගම දන්වා සිටිනවා.

කෙසේ නමුත් තවමත් මෙම ප්‍රහාරයේ අරමුණ හෝ, සිදුවූ දත්ත සොරකම් පිළිබඳව සොයාගෙන නැහැ.

මුල් කාලයේ youtube වෙත video upload කිරීම සිදුවුණේ විනෝදයට නමුත්, අද වන විට ඒ හරහා විශාල වශයෙන් මුදල් සොයන පුද්ගලයින් සංඛ්‍යාව අතිවිශාල යි. කෙලින්ම youtube හරහා නොවුණත් විවිධ අනුග්‍රහකත්වයන් සහ විවිධ දේ අලෙවි කිරීම් වැනි දේ ඔස්සේ ආදායම් ලැබීම සිදුවෙනවා. මේ කියන්න යන්නේ 2018 වසර වෙද්දී youtube හරහා ජනප්‍රියත්වය ලබා ගනිමින් වැඩිම ආදායම් ලැබූ පුද්ගලයින් කිහිපදෙනෙකු ගැන යි.

වයස අවුරුදු 23ක් වූ මොහු මේ වසරේ ලැබූ ආදායම ආසන්න වශයෙන් ඇමරිකානු ඩොලර් මිලියන 14.5 පමණ වෙනවා. උපතින් ඇමරිකානු ජාතිකයෙක්. Logan Paul රංගන ශිල්පියෙක්, ක්‍රීඩකයෙක්, වගේ ම ගායකයෙකු ලෙසත් කටයුතු කර තිබෙනවා. වරක් සියදිවි නසා ගැනීමේ සිදුවීමක් පිළිබඳ වීඩියෝවක් ඉදිරිපත් කිරීම නිසා මොහුට ප්‍රේක්ෂකයන්ගේ බලවත් අප්‍රසාදයටත් පත් වෙන්න වුණා .කෙසේ වෙතත්, ඔහුගේ youtube නාලිකාව වන Loagan Paul Vlogs වෙත මිලියන 22ක subscribersලා සිටිනවා.

මේ දවස්වල වැඩිපුරම කතා බහට ලක්වන youtuber ලෙසින් PewDiePie හඳුන්වන එක වරදක් නෑ. 2018 වසර වෙන්න කලින් වැඩිම subscribers ප්‍රමාණයක් හිමි කර ගැනීමට Tseries නාලිකාව සමග විශාල තරගයක් ලබා දෙන පුද්ගලයෙකු ලෙස හඳුන්වන්න පුළුවන්. PewDiePie නාලිකාව හා සම්බන්ධ මුද්‍රණ යන්ත්‍ර හැක් කිරීමේ සිදුවීම ඔබට මතක ඇති. මේ වන විට ඔහුට සිටින subscribers ප්‍රමාණය මිලියන 77 පමණ වෙනවා. වසරකට මොහු ලබන ආදායම ඇමරිකානු ඩොලර් මිලියන 15.5ක් පමණ වෙනවා. වයස 29 හැවිරිදි ස්වීඩන් ජාතිකයෙකු වන මොහුගේ සැබෑ නම Felix Arvid Ulf Kjellberg වෙනවා.

කාන්තාවන් බොහොමයක් අතර අතිශය ජනප්‍රිය youtube නාලිකාවක් වන Jeffree Star රුපලාවන්‍ය ද්‍රවය වැනි දෑ review (සමාලෝචනය) සිදුකරන නාලිකාවක්. මිලියන 11කට අධික subscribers ප්‍රමාණයක් ඇති මේ නාලිකාව, වසරකට ලබන සමස්ත ආදායම ඇමරිකානු ඩොලර් මිලියන 18 පමණ වෙනවා. Jeffree Star වෘත්තිය වශයෙන් සිදුකර ඇත්තේ ද වේශ නිරූපණ ශිල්පියෙකු ලෙස කටයුතු කිරීම යි. ඇමරිකානු ජාතික මොහුගේ වයස අවුරුදු 33ක් වෙනවා.

Tyler Toney, Coby Cotton, Cory Cotton, Cody Jones, Garrett Hilbert කියන පස්දෙනාගෙන් සැදුම්ලත් කණ්ඩායම් තමයි Dude Perfect කියන්නේ. මේ වන විට ඔවුන්ගේ youtube නාලිකාව මිලියන 37ක් subscribe කර තිබෙනවා. ඔවුන්ගේ මුළු ආදායම ලෙස ඇමරිකානු ඩොලර් මිලියන 20ක් වාර්තා වෙනවා. මීට සති කිහිපයකට පෙර ඔවුන් ලෝක වාර්තාවකටත් හිමිකම් කියන්න උත්සාහ දරුවා.

Jake Paul කියන්නෙත් ප්‍රසිද්ධ youtube තරුවක් 2018 වසරේ මොහුගේ ආදායම ඇමරිකානු ඩොලර් මිලියන 21.5ක් ලෙස තමයි වාර්තා වෙන්නේ. මොහුගේ youtube නාලිකාව මිලියන 17 subscribe කර තිබෙනවා. ඇමරිකානු ජාතික Jake Paul 21 හැවිරිදි ඇමරිකානු ජාතිකයෙක්. මේ නාලිකාව විනෝදාස්වාදය වෙනුවෙන් වෙන්වුණු එකක්.

Ryan ToysReview නාලිකාව කුඩාම දරුවන්ගේ සිට වැඩිහිටි ඕනෑම කෙනෙක් ආසාවෙන් නරඹන නාලිකාවක්. එයට හේතුව වන්නේ Ryan නම් 8 හැවිරිදි දරුවා සහ ඔහුගේ පවුලේ පිරිස විසින් මේ නාලිකාව පවත්වා ගෙන යාම යි. සෙල්ලම් බඩු වර්ග සමාලෝචනය කිරීම් මේ නාලිකාව හරහා සිදුකෙරෙනවා. මේ නාලිකාව සතුව සිටින subscribers ප්‍රමාණය මිලියන 17කට අධික යි. 2018 වසරේ මේ නාලිකාව සතු ආදායම ඇමරිකානු ඩොලර් මිලියන 22 පමණ වෙනවා. රයන් ලෝකයේ වයසින් කුඩාම youtube තරු අතරින් කෙනෙක්.

DanTDM නාලිකාව වෙන් වෙන්නේ බොහෝ දුරට minecraft වීඩියෝ ක්‍රීඩාව වෙනුවෙන්. daniel robert middleton තමයි මේ නාලිකාවේ හිමිකරු .ඔහු වෘතියෙන් පරිගණක ක්‍රීඩාවෙහි නියැලෙන්නෙක්. මේ වෙන කොට ඔහුගේ youtube නාලිකාව සතුව subscribersලා මිලියන 20ක් පමණ ඉන්නවා. ඒ වගේ ම මේ වසරේ ආදායම ඇමරිකානු ඩොලර් මිලියන 20.7ක් පමණ වන බව තමයි වර්තා වෙන්නේ. මොහු 27 හැවිරිදි බ්‍රිතාන්‍ය ජාතිකයෙක්.

මේ වෙන කොට මේ අගයන් වෙනස් වෙන්න හැකියාව තියෙනවා. මේ ආසන්න වශයෙන් ඔවුන් ලබන පිළිබඳව විස්තරයක් පමණයි.

ලංකාවේ පසුගිය දිනවල ඇති වූ වාතාවරණයන් නිසාවෙන් ලංකාවේ සමාජ ජාල මාධ්‍යයන් තාවකාලික තහනමකට ලක්වුණා. මේ තහනම ශ්‍රී ලංකා රජයෙන් පනවන්නට හේතු වුණේ අසත්‍ය ප්‍රචාරයන් සහ ප්‍රවෘත්ති ප්‍රචාරය වීම සහ සමාජය තුළ අනවශ්‍ය භීතියක් ඇති වීම වළක්වාලීම අරමුණු කරගෙන යි. මේ සමාජ මාධ්‍ය ජාලයන් වරණය සිදුවූවත් බොහෝ දෙනෙක් මේ වන විට VPN භාවිත කරමින් සමාජ මාධ්‍ය භාවිත කරනවා අපට දකින්න ලැබුණා. මේ වාරණය අතරතුර විවිධ facebook පිටු සහ පෞද්ගලික ගිණුම් (personal accounts) disable වීම් සහ report වීම් පිළිබඳ ව විවිධ post අපට දකින්නට ලැබුණා. මේ අතරතුරේ තමන්ගේ ගිණුම්වල සහ pageවල reach වැඩි කරගන්නට උත්සහ දැරීම් ගණනාවක් අපට දකින්න ලැබුණා. විශේෂයෙන් “අනේ මගේ page එක report වෙනවා sticker comments දාන්න” වැනි ප්‍රකාශයන් සුලභව අපට දකින්න ලැබුණා. profile එකක් හෝ page එකක් report වීමක් සිදුවුණොත් comments දැමීම පමණක් ප්‍රමාණවත් ද? කොහොමද profile එකක් report හෝ disable වෙන්නේ? මේ ලිපිය හරහා අපි කතාබහ කරන්න යන්නෙ ඒ ගැන.

සාමාන්‍යයෙන් අපි facebook post එකක් දැම්මහම ඉබේම යම් මුලික අදියරේ පරික්ෂා කිරීමකට ලක්වෙනවා. එය සිදුවෙන්නේ Facebook botsලා මඟින්. මේ බෝට්ස්ලා එහෙම නැති නම් මේ ස්වයංක්‍රිය වැඩසටහන් මඟින් අපි පළ කරන ලිපි, ඡායාරූප scan කිරීමක් සිදුවෙනවා. එහි අඩංගු වචන හෝ සංකේත Facebook Community Standardsවලට එරෙහිව නොයන්නේ නම් එය පළවෙනවා. නමුත්, එය යම් අකාරයකින් ඊට එරෙහිව යන්නක් නම්, එය ඉවත් කරගන්නා ලෙස දැනුම් දීමක් හෝ දෙවන වර review එකක් සඳහා ඉල්ලීමක් කිරීමට වගේ ම, මේ ලිපිය හෝ ඡායාරූපය අඩංගු post එක පරිශීලකයා පළ නොකරන ලද එකක් නම් (ගිණුම් හැක් වීමක් වැනි දෙයක් හෝ වෙන අයෙකු විසින් පරිශීලක අනුදැනුම නොමැතිව පළ කරන ලද්දක් නම්) එය ඉවත් කර, ගිණුමේ ආරක්ෂාව වැඩි කර ගැනීමට පරිශීලකයා වෙත විවිධ options ලබා දෙනවා. එතෙක් එය draft එකක් ලෙසින් ඔවුන් රඳවා ගන්නවා. දෙවන වර review කිරීමේ දී එය Facebook Community Standards සඳහා නොගැලපෙන්නේ නම් එය ඉවත් කළ බවත් ඔබට දැනුම් දෙනවා. මේ සඳහා සාමාන්‍යයෙන් දිනක් හෝ දෙකක් පමණ කාලයක් ගත වෙන්නට ඉඩ තියෙනවා.

Post එකක්, පෞද්ගලික ගිණුමක් හෝ page එකක් වුණත් report වීමේ දී මුලික ක්‍රියාවලිය සිදුවන්නේ ඉහත සඳහන් කළ ආකාරයටම යි. උදාහරණයක් විදිහට ගත්තොත් ලංකාව තුළ සිදු වූ ත්‍රස්ත ක්‍රියාවන් සම්බන්ධව ලිපි සහ ඡායාරූප පළ කළ Facebook පිටු සහ ගිණුම් report වීම සහ disable වීම දෙයාකාරයකට සිදුවෙන්නට පුළුවන්. ඔවුන් දමන ලද postවල අන්තර්ගතය සමාජයට හානි දායක බව අනෙක් පරිශීලකයන් Facebook සමාගම වෙත report කිරීම නිසා හෝ මුලික පරීක්ෂාවන්වල දී හසු නොවුණු Facebook Community Standards සමග නොගැලපෙන යමක් facebook බොට්ස් වෙත හමු වූ නිසාවෙන් වෙන්නට පුළුවන්. මේ scan වීම සිදුවන්නේ බොට්ස් වෙත ලබා දුන් keywords වැනි දේවල් භාවිතයෙන්. මේ පරික්ෂාව වෙත ඔහුගේ post එකට ලැබෙන ප්‍රතිචාර (comments) පිළිබඳවත් සලකා බැලෙනවා. ඒ වගේ ම නිතරම facebook පිටුවක් හෝ ගිණුමක් පිළිබඳ ව අනෙක් පරිශීලකයන්ගෙන් report වීම් පැමිණෙනවා නම්, ඒ ගිණුම් හෝ පිටු පිළිබඳ ව සහ එහි අන්තර්ගතයන් ගැන සහ ඒවාට පුද්ගලයින් දක්වන ප්‍රතිචාර පිළිබඳවත් සලකා බැලීමක් සිදුකෙරෙනවා. විශේෂයෙන් අදාළ report වීම් පැමිණෙන්නේ කුමන කාණ්ඩයක් යටතේ ද යන්න ගැනත් ඒ අනුව ගත යුතු ක්‍රියාමාර්ග ගැනත් තීරණය කෙරෙනවා. බෝහෝ විට මේ සියලු කටයුතු සඳහා ඒ එක් එක් කාර්යයන්ට විශේෂිත වූ බොට්වරුන් සිටිනවා.

මේ, facebook භාවිතා කරන බොහෝ දෙනෙකු අතර තිබෙන මිත්‍යා විශ්වාසයක්. සාමාන්‍යයෙන් තරමක් වැඩි reach එකක් තිබෙන වැඩි පිරිසක් ගැවසෙන page සහ profile, disable වීම අනෙක් සාමාන්‍ය profileවලට සාපේක්ෂව යම් කාලයක් ගත වෙනවා. නමුත්, මෙවැනි වාතාවරණයන් හි දී ඒ පිළිබඳ ව විශේෂයෙන් සොයාබැලීමක් සිදුවෙනවා. likes හෝ reach වෙන ප්‍රමාණය ඔබේ facebook පිටුව ආරක්ෂා වෙන්නට විශේෂ හේතුවක් නොවන බව හොඳින් මතක තබාගත යුතු යි. එයට හොඳම උදාහරණය සපයන්නේ Sarcasm Facebook පිටුව යි. මිලියන ගණනක් likes තිබුණු ඒ පිටුවත් කාලයක් තිස්සේ disable වීමකට ලක් වී තිබුණා.

Stickers හෝ comments දැමීමෙන් disable වීමෙන් වැළකෙන්න හැකියාවක් නම් නැහැ. එය එක්කෝ බොහෝ දෙනෙක් මිත්‍යාවක් ලෙසින් විශ්වාස කරන යමක් හෝ තමන්ගේ profile එකට හෝ page එකට reach/ likes ලබා ගැනීමට දරන කූට ප්‍රයත්නයක් වීමට ලොකු ඉඩක් තිබෙනවා. කාගේ හෝ ඉල්ලීමකට, යම් කෙනෙකුට, හෝ පේජ් එකකට වැඩි වැඩියෙන් ස්ටිකර් කමෙන්ට්ස් ලබාදෙන විට ඔබ සියලු දෙනාගේ මිතුරු ලැයිස්තුවල සිටින යහළුවන්ට සහ ෆලෝවර්ස්ලට ඒක පේන්න තියෙන ඉඩ සෑහෙන වැඩි වෙනවා. එමඟින් අදාළ පුද්ගලයාගේ හෝ page එකේ reach වැඩි වීම පමණක් සිදුවෙනවා. reach වැඩි කරගැනීම වරදක් නොවුණත් ඔබ නොදැනුවත්ව හෝ මුලාවට පත් වී "වැහෙන්න යන්නේ....!", “අහවල් ආගමෙන් මේ profile එක report කරනවා”, “මම අදාළ ලිපිය දාපු නිසා report වෙනවා, මෙච්චර ගාණක් comments දෙන්න” වැනි ප්‍රකාශයන් නිසා අනවශ්‍ය පුද්ගලයින්ට reach ලබා නොදෙන්න.

පසුගිය සතියේ ඇතුළත දී ඔබේ ගිණුම block වෙන්න බලපාන්න පුළුවන් ප්‍රධාන සාධයක් ලෙසින් VPN හඳුන්වන්න පුළුවන්. සමාජ මාධ්‍ය වාරණය තිබු සමයේ ඔබ විටින් විට facebook වෙත පැමිණෙද්දී VPN හරහා රට විටින් විට මාරු කිරීම සිදුකළා නම් facebook එක හරහා එය ඔබේ ගිණුමට වෙනත් රටවල පුද්ගලයින් ඇතුළු වෙනවා ලෙසින් හඳුනාගැනීමට ලොකු ඉඩක් තිබෙනවා. එවිට ඔබේ ගිණුමේ ආරක්ෂාව තර කිරීමට security checking වැනි option එකක් භාවිතා වෙන්නට ලොකු ඉඩක් තිබෙනවා.

\* මේ සඳහා facebook ආයතනය භාවිතා කරන වැඩසටහන් අංගසම්පුර්ණ නැහැ. එනිසා වැඩි දෙනෙකු ඔබේ post එකක් report කිරීමක් සිදුකළොත් දින කිහිපයකට හෝ (temporarily) ඔබේ ගිණුම block වෙන්නට යම් ඉඩක් තිබෙනවා.

2017 WannaCry ransomware පරිගණක වයිරස නැවැත්වීමට මූලිකත්වය ගෙන කටයුතු කළ මාකස් හචින්ස් නමැති පරිගණක ආරක්ෂක පර්යේෂකයා computer hacking සහ conspiracy පිළිබඳ චෝදනා දෙකක් සඳහා වැරදිකරු බවට පත්ව තිබෙනවා.

ප්‍රකට බ්‍රිතාන්‍ය ජාතික පරිගණක ආරක්ෂක පර්යේෂකයෙකු වූ හචින්ස් ලෝකය පුරා අතිශය ජනප්‍රියත්වයට පත්වුණේ, රටවල් 150 පරිගණක 75,000කට පමණ පැතිර පැවති භයානක WannaCry ransomware පරිගණක වයිරසයට killswitch එකක් සොයා ගැනීමට ස්වාධින පරිගණක ආරක්ෂක පර්යේෂකයෙකු ලෙස ලබාදුන් දායකත්වය, සහ එය අඩපණ කිරීමට ප්‍රමුඛත්වය ගෙන කටයුතු කළ පුද්ගලයෙකු නිසාවෙනුයි. නමුත් පසුගිය දිනෙක ඔහු වෙත එල්ල වූ චෝදනා 8න් දෙකකට ඔහු වැරදිකරු බවට පත්වූ අතර, අනෙක් චෝදනා නිෂ්ප්‍රභා කෙරුණා. මේ චෝදනා අතර, Malware සහ ආරක්ෂණ පර්යේෂකයෙකු ලෙස තම නාමය රඳවා ගනිමින් කටයුතු කිරීම අරමුණු කරගෙන හානිදායක Malware නිර්මාණය කිරීමත් ඇතුළත්. කෙසේ වෙතත් මේ පිළිබඳ විශේෂ ප්‍රකාශයක් සිය නිල වෙබ් අඩවියේ තබමින් හචින්ස් සඳහන් කළේ තමා අතින් වූ වැරදි පිළිබඳව පසුතැවෙන බවත්, ඒ සඳහා පුර්ණ වගකීම බාරගන්නා අතර තමාගේ හැකියාවන් භාවිතා කරමින් පෙර පරිදිම malware attacksවලින් පොදු ජනතාවගේ ආරක්ෂාවට කැපවෙන බව යි.

ZDNet වෙබ් අඩවිය ලබාගත් උසාවි ලේඛන අනුව ඔහු වෙත වූ චෝදනා අටෙන් වැරදිකරු වූ චෝදනා දෙක සඳහා වසර 5ක් දක්වා සිර දඬුවමක්, ඇමරිකානු ඩොලර් 250,000ක දඩ මුදලක් හෝ දෙකටම යටත්වීමට ඔහුට සිදුවේවි. Kronos සහ UPAS-Kit නම් බැංකුවලට ප්‍රහාර එල්ලවෙන malware නිර්මාණය කිරීම, සහ 2015 වසරේ තවත් දෙදෙනෙකු සමග එක්ව හානිදායක malware එකක් නිර්මාණය කිරීම සහ ඒ පිළිබඳව ප්‍රචාරණය ඔහුට විරුද්ධව ඇති ප්‍රබලම චෝදනා වෙනවා.

අත්අඩංගුවට පත්වූ හචින්ස් ඇප මත නිදහස් කර ඇති අතර, මේ වන විට ඔහු නඩු විභාගය තෙක් ලොස් ඇන්ජලිස්හි වාසය කරන බව තමයි වාර්තා වෙන්නේ. පසුගිය කාලය පුරාවට ඔහු පරිගණක ආරක්ෂණය වෙනුවෙන් සිදු කළ මෙහෙය නඩු විභාගයේ තීන්දුවට වක්‍රව හෝ බලපෑම් කරනු ඇති බව යි බොහෝ දෙනෙකුගේ මතය. මේ වන විට ඔහුට කිසිදු සේවා දායකයෙකු සමග කටයුතු කිරීම තහනම් කර තිබෙනවා.

මේ ගෙවෙන්නේ ලෝකය තාක්ෂණය අතින් ඉතාම දියුණු වෙමින් පවතින යුගයක්. තාක්ෂණය දියුණු වෙද්දී විශාල වශයෙන් දියුණු වෙන අංශයක් තමයි ප්‍රවාහන අංශය කියන්නේ. අපි එදිනදා ගමනක් යන්න පෞද්ගලික වහනයක් නැති නම්, බොහෝ විට taxi සේවාවක් භාවිත කීරීම සුලබ යි. ඒ සේවාවන් අතරින් ලෝකය පුරාම ජනප්‍රිය සේවාවක් විදිහට uber සේවාව හඳුන්වන්න හැකියාව තියෙනවා. සාපේක්ෂව මිල තරමක් අඩු වීම සහ ගුණාත්මක සේවාව නිසා අද වෙද්දී ලංකාවෙත් smartphone භාවිතා කරන බොහෝ දෙනෙක් uber app එක තමන්ගේ දුරකථනයේ අනිවාර්යය app එකක් ලෙසින් තබා ගන්නවා. පසු ගිය දිනවල uber සමාගම තාක්ෂණිකව නව මානයකය තමන්ගේ සේවාව රැගෙන යන බව නිවේදනය කළා. ඒ පිළිබඳව යි මේ කියන්න යන්නේ.

Google සමාගම සහ එහි තාක්ෂණික පෙරළිය පිළිබඳ අප ඔබව පෙර ලිපි මඟින් දැනුවත් කළා. සුවිශාල සමාගමක් වුණ google සමාගම 2016 වසරේ අප්‍රේල් 1 වෙනි දා (April Fool's Day එක, එහෙමත් නැතිනම් මෝඩයාගේ දිනය) සමරන්නට Self-driving bicycle පිළිබඳ videoවක් නිකුත් කළා,

එය සත්‍යයක් නොවුණත්, මේ වෙද්දී ඌබර් සමාගම ඒ තාක්ෂණය සැබවින්ම නිර්මාණය කිරීමේ කටයුත්තට මුලපුරලා තියෙනවා. මේ වෙද්දී scooter, bike වෙත මේ autonomous තාක්ෂණය යොදාගැනීම අත්හදා බැලෙමින් පවතින බව 3D Robotics ආයතනයේ CEO වන Chris Anderson තම twitter ගිණුමේ නිවේදනයක් පළකරමින් ප්‍රකාශ කර තිබුණා.

දැනටමත් යුරෝපයේ රටවල් කිහිපයක uber jump සේවාව පවත්වාගෙන යනවා. ඒ හරහා ඔබට bikes හුවමාරුව මඟින් ගමනාගමනයේ යෙදෙන්න හැකියාව ලැබෙනවා. මේ ක්‍රමවේදයේම නව පිම්මක් ලෙසින් තමයි ඔවුන් Autonomous තාක්ෂණය යොදා ගන්නට අදහස් කරන්නේ. ඊට අමතරව පසුගිය දිනෙක යුරෝපයේ ධාවනය වන uber electronic වාහන වෙත swap කළ හැකි බැටරි තාක්ෂණය හඳුන්වා දුන්නා. මේ හරහා ධාවනයේ යෙදෙමින් සිටින රථයකට හදිසියේ අතරමඟ නවත්වා charge කර ගැනීමට අවශ්‍ය වන්නේ නැහැ.

CES 2019 අන්තර්ජාතික තාක්ෂණික පාරිභෝගික ඉලෙක්ට්‍රොනික ප්‍රදර්ශනය පිළිබඳවත්, එහිදී ඉදිරිපත් වුණු නව නිර්මාණයන් පිළිබඳවත් පෙර ලිපියකින් ඔබව දැනුවත් කළා. Uber සමාගමත් මේ ප්‍රදර්ශනයේ දී තමන්ගේ අනාගත නිර්මාණයන් සහ සංකල්පයන් පිළිබඳව ඉදිරිපත් කිරීමක් සිදු කළා. මේ නව නිර්මාණය කාගේත් අවධානය දිනා ගන්නට සමත්වුණා. හෙලිකොප්ටර ඇතුළු ගුවන් යානා නිෂ්පාදනය කරන ලෝක ප්‍රකට සමාගමක් වන Bell සමාගම සමග එක්ව ගුවන් taxi සේවයක් ආරම්භ කිරීමට සූදානමින් සිටින බව ඔවුන් එහිදී නිවේදනය කළා. අප පෙර ලිපියක Drone තාක්ෂණය පිළිබඳව කතාබහ කළා මතක ඇති නේ? මේ නිර්මාණය වෙන air taxiත් තරමක් ඒ හා සමාන යි. ඔවුන් එය හඳුන්වන්නේ Nexus Bell යන නමින්.

තෙල් මිල ඉහළයාම නිසා හෙලිකොප්ටර භාවිතයට ඇති ආර්ථික ගැටළු, නිර්මාණය වන්නට නියමිත hybrid යානය නිසාවෙන් විසඳෙනු ඇතැයි ඔවුන් අපේක්ෂා කරනවා. මේ යානයට එක වර මිනිසුන් 5 දෙනෙකු පමණ (කිලෝග්රෑම් 272ක් පමණ) රැගෙන යා හැකි අතර ඔවුන් මෙය ලබන 2012 වසර මැද භාගය වන විට වෙළඳපොළ වෙත හඳුන්වා දීමට සුදානමින් සිටිනවා. මේ යානයෙන් ආරක්ෂාකාරීව, පවුලේ සාමාජිකයන් සමග පවා වුව ගමන් කළ හැකි වනු ඇතැ යි Bell සමාගම The Verge වෙබ් අඩවිය වෙත සඳහන් කර තිබුණා. Bell සමාගම හැරුණු විට ලෝකයේ අතිශයින් ජනප්‍රිය තවත් තරගකාරී වෙළඳ නාමයන් වන Boeing, Airbus, Kitty Hawk වැනි සමාගම් මේ වන විටත් air taxi නිර්මාණය කිරීමේ තරගයට පිවිස අවසාන යි. කෙසේ වෙතත් 2017 වසරේ ඔවුන් ඇරඹි මේ ව්‍යාපෘතිය මේ වෙද්දී අවසන් භාගය කරා පැමිණ තිබෙන බව තමයි පෙනෙන්නනට තිබෙන්නේ. නමුත් මෙවැනි තාක්ෂණයක් ලංකාවට පැමිණෙන්න නම් තවත් ටික කාලයක් ගත වෙනවා නොඅනුමාන යි.

Hacking කිව්වහම බොහෝ විට ඔබට මතකයට එන්නේ පරිගණක, සහ පරිගණක පද්ධති අශ්‍රිතව අවසර නොලත් පුද්ගලයෙකු සිදු කරන හානිකර ක්‍රියාවලියක් වන්නට පුළුවන්. නමුත් hacking එතනින් එහාට විහිදුණු බොහොම පුළුල් මාතෘකාවක්.විශේෂයෙන්ම Social Engineering වගේ skill එකක් හැකර්වරුන් භාවිතයට ගන්නේ කොහොමද කියන එක පිළිබඳව අපි පෙර ලිපියක සඳහන් කළා.

ලෝකයේ ජිවත් වන මිලියනයකට ආසන්න හදවත් රෝගීන් පිරිසකගේ ජීවිතය අවදානමේ හෙලන vulnerability (ආරක්ෂක දුර්වලතාවන්) දෙකක් සොයා ගැනීමට පසුගිය දිනෙක හැකියාව ලැබුණා. සමහර හදවත් රෝගීන්ගේ හදවතේ ක්‍රියාකාරිත්වය සාමාන්‍ය මට්ටමට ගෙන ඒමටත්, හදිසි අකර්මන්‍යවීම් නවතා ලීමටත් Cardioverter Defibrillator එසේ නැති නම් පොදුවේ pacemakers නමින් හඳුන්වන උපකරණ භාවිතා කිරීම ලෝකයේ සුලභව සිදු වන දෙයක්. පොදුවේ මේ උපකරණ හරහා ලබා දෙන විද්‍යුත් කම්පනයන් මඟින් හදවත් රෝගීන්ගේ හදවත් ස්පන්දනයන් සහ වේගයන් සාමාන්‍ය මට්ටමට පාලනය කිරීම සිදු වෙනවා.

.

Medtronic නම් ලෝකයේ ප්‍රමුඛතම උපාංග නිර්මාණය කරන සමාගම විසින් නිෂ්පාදනය කරන ලද, සිරුර තුළ තැම්පත් කළ හැකි Cardioverter Defibrillator උපකරණයක මේ දුර්වලතාවයන් හඳුනාගෙන තිබෙනවා. CVE-2019-6538 සහ CVE-2019-6540 යන නම් දැනට මෙම දුර්වලතාවය නම් කොට තිබෙනවා. මේ දුර්වලතාවයන් නිසාවෙන් කිසිදු ආරක්ෂිත මුරපද භාවිතා කිරීමකින් තොරව උපාංගයට පිවිසීමේ හැකියාව සහ මේ device එකට සම්බන්ධ වීමට භාවිතා කරන telemetry protocol එක හරහා ගමන් කරන දත්ත කිසිදු encryption එකකින් තොරව ගමන් කරන බැවින්, මීටර් 6ක පමණ දුරක සිටින attacker කෙනෙකුට වුවත් මෙය පහසුවෙන් hack කරගැනීමේ හැකියාව ඇති බව තමයි වාර්තා වෙන්නේ. අදාළ ආයතය මේ දුර්වලතාවයන් සඳහා patches නිර්මාණය කරන බව එම ආයතන සඳහන් කර තිබෙන්නේ එතෙක් එම ආයතනයෙන් නිර්මාණය කරන ලද සහ නිෂ්පාදනය කරන ලද Implantable Cardioverter Defibrillator භාවිත කරන්නන්ට වෛද්‍ය උපදෙස් අනුව මේ උපාංගය භාවිතා කරන ලෙසත් එම සමාගම දන්වා තිබෙනවා.

Hacking කිව්වහම බොහෝ විට ඔබට මතකයට එන්නේ පරිගණක, සහ පරිගණක පද්ධති අශ්‍රිතව අවසර නොලත් පුද්ගලයෙකු සිදු කරන හානිකර ක්‍රියාවලියක් වන්නට පුළුවන්. නමුත් hacking එතනින් එහාට විහිදුණු බොහොම පුළුල් මාතෘකාවක්. ඔබ දන්නවා ද hacking උපක්‍රම භාවිතා කරමින් පරිගණක පමණක් නොව පුද්ගලයින් ද hack කරන්න පුළුවන් බව?

බොහෝ විට hacking ප්‍රහාරයකට ලක් වෙන්නේ පද්ධතියක්. මිනිසා කියන්නෙත් එවැනිම පද්ධතියක් ලෙසින් හිතන්නට ඔබට පුළුවන් නම්, එහි දුර්වලතා, bugs වගේ දේවල් හොයාගන්න එක එතරම්ම අපහසු නැහැ. සාමාන්‍යයෙන් එවැනි hacking උපක්‍රම හඳුන්වන්නේ social engineering කියලා. මේක එක්තරා විදියක hacking Category( ප්‍රවර්ගයක්) එකක් විදිහට හඳුන්වන්න පුළුවන්. හැකර්වරු බොහෝ විට භාවිතා කරන ප්‍රසිද්ධ attacking strategies/methods ගණනාවක් මේ යටතට තමයි ගණන් ගැනෙන්නේ.

සරලවම කිව්වොත් යම්කිසි පුද්ගලයන් කණ්ඩායමකගෙන් හෝ පුද්ගලයෙකුගෙන් අවශ්‍ය යම් දෙයක් ලබා ගැනීම සදහා ඔවුන්ව/ ඔහුව/ ඇයට මනෝවිද්‍යාත්මකව බලපෑම් කිරීම. හරිම සරලව මෙහෙම විග්‍රහ කළාට hacker කෙනෙකු සතුව තියෙන බලගතුම අවියක් විදිහට මෙය හඳුන්වන්න පුළුවන්. සරල උදාහරණයකින් පැහැදිලි කළොත්;

A සහ B කියලා පුද්ගලයින් දෙන්නෙක් ඉන්නවා. දෙදෙනාගෙන් A කියන්නේ හැකර්. එතකොට B තමා ගොදුර (victim), එහෙමත් නැත්නම් හැක්-වෙන කෙනා. Aට Bගේ facebook ගිණුමේ Email සහ Password ලබාගන්න අවශ්‍ය යි. A විසින් Bව එක්තරා විදිහකට රැවටීමට ලක්කරනවා. Bගේ විශ්වාසය දිනාගෙන එයාටත් නොදැනෙන්න තමන්ට ඕන කරන විස්තර ටික ලබාගන්නවා. සමහරක් විට Aට කෙළින්ම තමන්ට අවශ්‍ය කරන තොරතුරු ලැබෙන්නත් පුළුවන්, නොලැබෙන්නත් පුළුවන්. මොකද ඒක තීරණය වෙන්නේ A කියන පුද්ගලයා බොරු කියලා රැවටීමෙහි කොච්චර දක්ෂ ද යන්න වගේම B කියන පුද්ගලයා අපරික්ෂාකාරී ද කියන එක මත.

තරමක් බරපතල මට්ටමේ ක්‍රියාවලියකට (hack කිරීමකට) සූදානම් වෙන පුද්ගලයෙක් සාමාන්‍යයෙන් දින ගාණක්/ මාස ගණනක් තමාට අවශ්‍ය පුද්ගලයා නිරීක්ෂණය කරමින්, ඔහුව හොඳින් අධ්‍යයනය කිරීමක් සිදු කරනවා. පෞද්ගලික දත්තවල සිට භාවිතා කරන සුවඳ විලවුන්, ආශ්‍රය කරන පුද්ගලයින්, විශේෂයින්ම කාන්තාවන් ගැන නිරීක්ෂණයක් සිදු කරනවා. ඒ වගේම මේ Social Engineering ප්‍රහාරයන් පුද්ගලමූලික සහ පරිගණක පද්ධතිමූලික වශයෙන් ප්‍රධාන ක්‍රමවේදයන් දෙකකට සිදු වෙනවා. කොයි ක්‍රමවේදය අනුව සිදු වුණත් ප්‍රධාන ඉලක්කය වෙන්නේ ඒ පද්ධතියේ ඉන්න දුර්වලම පුද්ගලයා. මේ දුර්වලතාව ඔවුන් මනින්න භාවිතා කරන ප්‍රධාන සාධක කිහිපයක් තියෙනවා.

මේ සියල්ලම මිනිසුන් සතු පොදු දුර්වලතාවයන්. ඔවුන් පරිගණක පද්ධතියක සතුව තියෙන vulnerabilities, bugs නිරීක්ෂණය කරන ලෙසින්ම තමයි මේවා නිරීක්ෂණය කරන්නේ. ඒ වගේම මේ පොඩි ලක්ෂණත් පුද්ගලානුබද්ධව වෙනස් වෙනවා. උදාහරණයක් විදිහට කෑදරබව ගත්තොත්, එක් පුද්ගලයෙක් කෑමට කෑදර වෙද්දී තවෙකෙක් මුදලට කෑදර වෙන්න පුළුවන්. ඒවා තේරුම් ගැනීම, සහ ප්‍රහාරය එල්ල කළ යුතු ආකාරය තීරණය වෙන්නේ හැකර් සතු දත්ත වගේම ඔහුගේ නිර්මාණශිලිත්වය මත යි.

පහත සඳහන් ක්‍රමවේදයන් සමහරකට සෘජුවම Social Engineering භාවිතා නොවුණත්, ඉහත සඳහන් කර ඇති පොඩි පොඩි පුද්ගල දුර්වලතාවයන් අවභාවිතා කරමින් ක්‍රියාත්මක වෙන කුප්‍රකට hacking methods කීපයක් මේ.

ඔබ සාමාන්‍යයෙන් තොරතුරු තාක්ෂණයට උනන්දු පුද්ගලයෙක් නම් මේ නම නුහුරු වන්නට විදිහක් නැහැ. Social Engineering භාවිතයෙන් සිදුවුණු කුප්‍රකටම සහ පැරණිතම ප්‍රහාරය පිළිබඳ තොරතුරු වාර්තා වෙන්නේ මේ ප්‍රවර්ගයෙන්.

වසර 3000කට පමණ පෙර ග්‍රීකයින් ට්‍රෝයි නගරයට විරුද්ධව සිදුකළ බව කියන ට්‍රෝජන් යුද්ධය පිළිබඳ ඔබ අසා තිබෙනවා ද? අවුරුදු දහයක් පුරා ට්‍රෝයි නගරය වැටලීමට ග්‍රීකවරුන් උත්සහ කළත් ඒවා අසාර්ථක වුණා. අවසානයේ ග්‍රීකයින් ට්‍රෝයිවරුන් පූජනිය ලෙස සැලකූ සත්ත්වයෙකු වන අශ්වයෙකුගේ ඉතා විශාල දැවමය පිළිමයක් නිර්මාණය කරනු ලබනවා. රහසේ එය තුළට තෝරාගත් විශේෂ බලකායක් පුරවා, මෙය ග්‍රීක ත්‍යාගයක් ලෙස නගරයට පිවිසෙන ප්‍රධාන දොරටුව ඉදිරිපස තබනවා. ග්‍රීකවරුන් පසුබැස ගොස් ඇතැ යි සිතූ ට්‍රෝයි ජනතාව මෙම දැවමය අශ්වයා ට්‍රෝයි නගරය තුළට රැගෙන යන්නේ ඔවුන්ගේ ජයග්‍රහණයේ සංකේතයක් ලෙස යි. නමුත් දවස අවසානයේ අශ්වයා තුළ සිටි ග්‍රීක සොල්දාදුවන් අඳුර වැටෙනවාත් සමග එය පිටතට පැමිණ, ප්‍රධාන දොරටුවේ ආරක්ෂාවට යොදවා සිටි මුරකරුවන් මරා, අවසානයේ ට්‍රෝයි නගරය යටත් කරගනු ලැබුවා.

අප දැන් කතාකරන මාතෘකාවේ දී භාවිතා කරන්නෙත් මෙවැනිම ක්‍රමවේදයක්. තෝරාගත් තැනැත්තා රැවටීමකට ලක්කර, ඔහුට malicious file එකක් download කරගන්න සැලැස්වීම එහිදී සිදු වෙනවා. එම තැනැත්තා මේ file එක open කළ විට ඔහුගේ පරිගණකයේ/ උපාංගයේ backdoor එකක් හැකර් වෙත විවෘත වෙනවා. ඒ හරහා අවශ්‍ය විටක දී ඔහුගේ පරිගණකය පාලනය කරන්න hackerට හැකියාව ලැබෙනවා.

මෙහිදී කරන්නේ තමාට අවශ්‍ය කරන target එක කෙළින්ම නිරීක්ෂණය කරන එක. මේ සඳහා එතරම් තාක්ෂණික දැනීමක් අවශ්‍ය නෑ. මේ ක්‍රමය භාවිතා කරලා hackersලට PIN අංකයන්, passwords වගේ ගොඩක් රහසිගත තොරතුරු හොයාගන්න පුළුවන්. මේ ක්‍රමය බොහෝ වෙලාවට ගොඩක් සෙනග ගැවසෙන ස්ථානවල තමයි ඔවුන් සිදුකෙරෙන්නේ. මොකද එතකොට යි තමාගේ ඉලක්කයට නොදැනෙන්න මෙය සිදුකරන්නට හැකියාව ලැබෙන්නේ. Credit/ debit card වංචාවෙන් ගැලවෙන්නේ මෙහෙම යි! ලිපියේ දීත් මේ ගැන සාකච්ඡා කෙරුනා.

Social Engineeringවල ප්‍රධාන technique එකක් විදිහට මෙය හඳුන්වන්න පුළුවන්. තෝරාගත් ඉලක්කය සමාජය හා සම්බන්ධකම් පවත්වන online chat session, emails, phone වගේ දේවල්වලින් හැකර්ට අවශ්‍ය තොරතුරු හොයාගන්න එක තමයි සරලවම මේ වෙන්නේ.

බොහොමයක් විශාල ආයතනවල වැරදීම් සිදුවුණු ගමන් ලිපි ගොනු ඉවත් කිරීමක් සිදු කරනවා. ඒ වගේම බොහොමයක් සමාගම් කිසිම විදිහකට ලිපිගොනු විනාශ කිරීමේ ක්‍රමයක් භාවිතා කරන්නෙත් නැහැ. මේ විදිහට ඉවතලන phone books, system manuals, රැස්වීම් කැලැන්ඩර, මුද්‍රිත login නාම සහ passwords, මුද්‍රිත source codes වගේ ගොඩක් වටිනා රහසිගත දත්ත hackersලට කුණුගොඩවලින් හොයාගන්න පුළුවන්.

බැංකුවක් වැනි නීත්‍යානුකූල ආයතනයක් ලෙස පෙනී සිටිමින්, තමන්ගේ ඉලක්කයට දුරකථන ඇමතුමක් ලබා දී තමාට අවශ්‍ය තොරතුරු ලබාදීමට පෙළඹවීම Vishing / Voice phishing/ phone phishing විදියට හඳුන්වන්න පුළුවන්. දුරකථනයකින් ඔබ අමතන SCAM ලිපිය හරහාත් අපි මේ ගැන කතා කළා. Phishing සහ Spam පිළිබඳවත් ඊට පෙර ලිපි මඟින් දීර්ඝව කතාබහ කළා.

Reverse Social Engineeringවල ප්‍රධාන කොටස් 3 දැකගන්න පුළුවන්. Sabotage, Marketing, Support විදිහට. Sabotage කියන පියවරේ දී වෙන්නේ hackerට තමාගේ ඉලක්කය සමග සම්බන්ධ වෙන්න ලැබුණු පොඩි ඉඩක දී එම ඉලක්කයට යම් වරදක් සිදු කිරීම හෝ එවැනි දෙයක් සිදුවුණු ලෙස හඟවනවා. එය විසඳන්නට ඉලක්කය විසින් යමෙකු හොයන මට්ටමට පත් කරනවා. දෙවැනි පියවර ආරම්භ වෙන්නේ එතකොට. Marketing පියවරේ දී වෙන්නේ අර ගැටළුව විසඳාගන්නට උත්සාහ කරන ඉලක්කයට, එයට ඉහළම සුදුස්සා තමා බව ඒත්තු ගැන්වීම. තුන්වන පියවර විදිහට Supportවල දී ඉලක්කයේ විශ්වාසය දිනාගෙන, උදව් කරන මුවාවෙන් hackerට අවශ්‍ය සංවේදී දත්ත ඔහු ලබා ගන්නවා.

මේ හැරෙන්නට තවත් විවිධ ක්‍රමවේදයන් ගණනාවක් තිබෙනවා.

දැනුවත්ව හෝ නොදැනුවත්ව ඔබත් Social Engineering පිළිබඳ විශේෂඥයෙක් කියලා හිතිලා තියෙනවා ද? නොදැනුවත්වම වුණත් Social Engineering භාවිතා කරලා ඔබේ වැඩකටයුතු බොහෝ සිදු කරලා ඇති. උදාහරණයක් විදිහට පොළෙන් බඩු මිල දී ගන්න ගියාම මුදලාලිලා එක්ක දිගින් දිගටම හෙට්ටු කිරීම් කරන්නේ මේ ක්‍රමවේදය භාවිතයෙන් තමයි. අවසානයේ ඔබ අවශ්‍ය මුදලට ආසන්න ගාණකට භාණ්ඩය මිලට ගන්නවා. සුපිරි වෙළඳසැලක තත්ත්වය මීට තරමක් වෙනස්. ඔවුන්ගේ පාරිභෝගික සහායකයින් ඔබට භාණ්ඩ තෝරාගැනීමට සහය වෙන මුවාවෙන් පැමිණ, ඔවුන්ගේ භාණ්ඩ සහ සන්නාමයන් ඔබේ බඩු ලැයිස්තුවට ඇතුල් කරන්නේ ඔබටත් නොදැනීම යි.

Social Engineering සමාජයට අහිතකර යමක් නොවෙයි. භාවිතයේ ගැටළුවක් තමයි පවතින්නේ. මේ ලිපියේ අරමුණ එවැනි අවභාවිත කිරීම් පිළිබඳ ඔබව දැනුවත් කිරීම යි. ඒ වගේම The Circle (2017), Snowden (2016), Algorithm (2014), Fifth Estate (2013), Darknet 2018, Mr. Robot, Searching, Cam(2018),Who Am I(2014), TheCircle(2017), Nerve(2016), Blackhat(2015), Transcendence(2014), Friend Request(2016) වැනි චිත්‍රපට සහ ටෙලිකතා මාලා නරඹන ලෙස අප ඔබට යෝජනා කරනවා.

අතීතයේ රූපවාහිනිය සහ ගුවන් විදුලිය අතිශය ජනප්‍රිය සන්නිවේදන මාධ්‍යයන්. නමුත් තොරතුරු තාක්ෂණ පෙරළිය සමග නිර්මාණය වුණු අන්තර්ජාලය සහ smart උපාංග නිසාවෙන් අද වෙනකොට රුපවාහිනී සහ ගුවන් විදුලි තරමක් දුරට අභාවයට යමින් තියෙනවා කිව්වොත් නිවැරදි. එකට මූලික හේතුව බවට online streaming services. පසුගිය ලිපිවල දී අපි online streaming සේවාවන් කිහිපයක් පිළිබඳව කතාකළා ඔබට මතක ඇති. Netflix කියන්නෙත් ලෝකයේ අතිශයින් සුප්‍රසිද්ධ video streaming සේවාවක්. Netflix සමාගම ඔවුන්ගේ නවතම subscription plan එක මසකට ඇමරිකානු ඩොලර් 3ක පමණ මුදලකට ($3.63) තෝරාගත් රටවල් කිහිපයකට ලබාදෙන්න පසුගිය දවසක තීරණය කළා. ඉන්දියාව කියන්නෙත් තෝරාගත් එක රටක්.

මේ වෙනකොට ඉන්දියාවට Netflix මාසික සැලසුම සඳහා වැයවෙන මුදල ඇමරිකානු ඩොලර් $7.27 පමණ වෙනවා. මෙයින් හරි අඩකට පමණ මුදලකට තමයි මේ හඳුන්වා දීමට නියමිත නව සැලසුම ක්‍රියාත්මක වෙන්නේ. මෙය mobile plan එකක් ලෙසින් තමයි ඔවුන් හඳුන්වාදීමට තීරණය කර තිබෙන්නේ. The Verge වෙබ් අඩවියට ඔවුන් ප්‍රකාශයක් නිකුත් කරමින් සඳහන් කර තිබුනේ Netflix සේවාව සමාජය තුළ වඩාත් ප්‍රචලිත කරමින්, පරිශීලකයන් වැඩි ප්‍රමානයකට සේවාව ලබාගත හැකි වන පරිදි විවිධ ජනමට්ටම් සහ විවිධ තෝරාගත් කලාපයන් ආශ්‍රිතව මෙවැනි කෙටිකාලින සැලසුම් හඳුන්වාදීම ඔවුන්ගේ අරමුණ බව යි. මේ හරහා ජනතාව වෙත මෙවැනි සේවාවන් හඳුන්වාදීම ඔවුන්ගේ එක අරමුණක් බවට පත්ව තිබෙනවා. බොහෝවිට ඉදිරි කාලය තුළ දී නෙට්ෆ්ලික්ස් සමාගම මඟින් සතිපතා ගෙවීම් සිදු කළ හැකි weekly හෝ දෙසතියකට වරක් ගෙවීම් කළ හැකි biweekly subscriptions හඳුන්වා දේවි. ඉන්දියාවේ අන්තර්ජාලය සඳහා වැයවෙන මුදල ඉතාම අඩු නිසාවෙන් ඉන්දියාවේ අන්තර්ජාල පහසුකම් ඇති ජනතාව online content කෙරෙහි වැඩි අවධානයක් යොමු කරන බව variety.com වෙබ් අඩවිය සඳහන් කර තිබුණා. මේ නිසාවෙන් බොහෝවිට මෙවැනි සැලසුම් අත්හදාබැලිමට බොහොමයක් සමාගම් තෝරාගන්නා රටක් බවට ඉන්දියාව පත්ව තිබෙනවා.

මෙය පරීක්ෂණයක් පමණක් නිසාවෙන් දීර්ඝකාලීන සැලසුමක් නොවන වගත් සඳහන් කළ යුතු යි. ඉන්දියාව හැරුණු විට මේ ගෙවීම් සැලසුම ක්‍රියාත්මක වෙන අනෙක් රටවල් පිළිබඳව නෙට්ෆ්ලික්ස් සමාගම නිල වශයෙන් කිසිදු සඳහනක් කර නැහැ.

Netflix උපසභාපතිවරයෙකු වන ටොඩ් යෙලින් පසුගිය දිනෙක ඉන්දියාවේ මුම්බායි නුවර පැවැත්වූ ප්‍රධාන දේශනයක් අතරතුර දී ඔවුන් සතුව streaming සේවාවන්වල අනාගතය පිළිබඳ සැලසුම් වගේම, ඉන්දියාව ආශ්‍රිත කරගෙන නිර්මාණය කිරීමට බලාපොරොත්තු වන නෙට්ෆ්ලික්ස් කතාමාලාවන් පිළිබඳවත් සඳහන් කළා. ඉන්දියාව ආශ්‍රිතව නිර්මාණය වූ Sacred Games නම් කතා මාලාවේ සාර්ථකත්වය පිළිබඳව වගේම ඒ වෙත ලෝකය පුරාම රසිකයන් ආකර්ෂණය කර ගන්න හැකි වීම පිළිබඳවත් සඳහන් කළා.

මේ හා සමානවම ඉන්දියාව ආශ්‍රිතව Hotstar සමාගමත් $5.30 වැනි අඩු මිලකට ඔවුන්ගේ සේවාව ලබා ගැනීමේ හැකියාව පසුගිය දිනෙක ලබා දීමට තීරණය කළා. ඒ වගේම Spotify සමාගමත් පසුගිය දිනෙක ඔවුන්ගේ සේවාව ඉන්දියාව වෙත නිකුත් කළා. නමුත් ලංකාවේ අන්තර්ජාල සඳහා වැයවෙන අධික මුදල නිසාවෙන් මෙවැනි සේවා ලබා දුන්නත් අප බොහෝ දෙනෙකුට ඒවා සිත්සේ භාවිතා කරන්නට හැකිවේ ද යන්න සැකසහිත යි.

PUBG (PlayerUnknown's Battlegrounds) ක්‍රීඩාව අද වන විට ලෝකයේ බොහෝ දෙනෙක් ක්‍රීඩා කරන ක්‍රීඩාවක් බවට පත්වෙලා තියෙනවා. විශේෂයෙන්ම ආසියාතික රටවල් අතර මේ ක්‍රීඩාව අතිශයින්ම ජනප්‍රියත්වයට පත්වුණා. මේ ක්‍රීඩාව සඳහා බොහෝ විට යොමු වෙන්නේ තරුණයින් සහ පාසල් ළමුන්. 2017 වසරේ නිකුත් වුණු මේ ක්‍රීඩාව අයිති වෙන්නේ Battle Royale Game Genre එකට. පසුගිය වසර තුළ දී පමණක් මෙම ක්‍රීඩාව ඇ. ඩො. බිලියන 1.035ක ආදායමක් උපයාගෙන තියෙනවා.

PUBG නිසාවෙන් පසුගිය දිනක ඉන්දියාවේ කිහිප දෙනෙකු අත්අඩංගුවටත් පත්වුණා. මේ ක්‍රීඩාව දැඩි ලෙසින් දරුවන් ඇබ්බැහි කර ගන්නා නිසාවෙන් ඉන්දියාවේ ගුජරාට් ප්‍රාන්තයේ මේ ක්‍රීඩාව තහනම් කර තිබුණා. ඒ තහනම නොතකා ක්‍රීඩාවේ නිරත වූ කිහිප දෙනෙකු ගුජරාට් පොලිසිය අත්අඩංගුවට ගෙන, පසුව ඇප මත නිදහස් කර තිබුණා. Hindustan times වෙබ් අඩවියේ මේ පුවත පල වී තිබුනේ ‘Demon in every house’: 10 arrested in Gujarat for playing PUBG යන සිරස්තලයත් සමග යි. ගුජරාට් ප්‍රාන්තයේ රජය මේ තීරණය ගෙන තිබුනේ ළමයින් පාඩම් වැඩ පසෙක ලා මේ ක්‍රීඩාවේ නිරත වන බව දෙමව්පියන් සහ අධ්‍යාපන බලධාරීන් නැගු මැසිවිලි නිසාවෙන්. කෙසේ වෙතත් ඉන්දියාවෙන් අනෙක් ප්‍රදේශ සඳහා තවමත් මේ ක්‍රීඩාව විවෘත යි.

දරුවන්ගේ මේ අධික ඇබ්බැහි වීම නිසාවෙන් PUBG ක්‍රීඩාවේ නිර්මාණකරුවන් එක දවසකට මේ ක්‍රීඩාව ක්‍රීඩා කළ හැකි උපරිම පැය ගණන සම්බන්ධයෙන් සීමාවක් පනවන්නට තීරණය කර තිබෙනවා. මේ වන විටත් ඉන්දියාවේ Tier 1 සහ Tier 2 මට්ටමේ නගරවලට (නගර වර්ගීකරණය සඳහා, එහි ජීවත්වීමට වැය වන ජීවන වියදම, දියුණුව මත පදනම් වූ වර්ගීකරණ මට්ටම් 3න් දෙකකි. මේ මට්ටම් දෙක යටතට ඉන්දියාවේ මහා නගර 16ක් පමණ අයත් වන අතර ඉතිරි සියලු ප්‍රදේශ Tier 3 ලෙසින් වර්ග වේ) අදාළ ප්‍රදේශයන් සඳහා මෙය අත්හදා බැලෙමින් පවතිනවා. මේ හරහා, PUBG ක්‍රීඩා කරන කාලය අනුව Health reminders එවීමටත් කටයුතු කෙරෙනවා. ක්‍රීඩා කාලය පැය 2 දී සහ පැය 4ක් වන විට reminders එවීම, සහ පැය 6ක් වූ විට පසු දින වන තෙක් ක්‍රීඩා කිරීමට නොහැකි වන ලෙසින් මේ ක්‍රියාවලිය ක්‍රියාත්මක වෙනවා. මේ ක්‍රියාවලිය ලෝකයේ අනෙක් රටවලට භාවිතා කිරීම පිළිබඳව නිල වශයෙන් කිසිදු සඳහනක් සමාගම විසින් සිදු කර නැහැ.

Facebook පරිශීලකයන් මිලියන සිය ගණනකගේ passwords (පරිශීලක මුරපද) සාමාන්‍ය අයෙකුට කියවිය හැකි (plain text) ලෙසින් ගුප්ත කේතනයකින් තොරව (no encryption) ගබඩා කරගෙන සිටින බවත්, ඒ ගොනුවලට අභ්‍යන්තර ප්‍රවේශයන් ඇති සේවකයන් ඕනෑම කෙනෙකුට ඒවා සොයා ගත හැකි බවත්, පසුගිය දා පරිගණක ආරක්ෂණයන් සහ බිඳ වැටීම් පිළිබඳ විමර්ශනය කරන Krebs on Security වෙබ් අඩවිය හෙළි කළා.

සාමාන්‍යයෙන් පරිශීලකයන්ගේ මුරපද hashing නම් විශේෂිත ක්‍රමවේදයක් භාවිතා කරමින් ගබඩා කිරීම සිදු වෙනවා. නමුත් විවිධ errors නිසාවෙන් මේ නිරාවරණයන් සිදුව ඇති බව විශ්වාස කෙරෙනවා. Krebs on Security වෙබ් අඩවියේ නිර්මාතෘ බ්‍රයන් ක්රෙබ්ස්ට අනුව මෙලෙස නිරාවරණය වී ඇති පරිශීලක මුරපද සංඛ්‍යාව මිලියන 200ත් 600ත් අතර වෙනවා. මේ බව facebook ආයතනය සිය නිල blog අඩවියෙ “Keeping Passwords Secure,” යන මාතෘකාව යටතේ සටහනක් තබමින් තහවුරු කළා. මෙහිදී සමාගම වැඩිදුරටත් සඳහන් කර සිටියේ පසුගිය ජනවාරියේ සිදු කළ security review එකේ දී මේ ගැටලුව හඳුනාගත් බව යි. මේ ගැටලුව නිරාකරණය කර ඇති බවත්, මෙයින් මුරපද නිරාවරණය වූ පරිශීලකයින් ඒ පිළිබඳව දැනුවත් කරන බවත් ඔවුන් ප්‍රකාශය මඟින් සඳහන් කර තිබුණා.

Facebook සමාගමට අනුව මේ මුර පද සමාගමේ අභ්‍යන්තර server එකක තැම්පත්ව තිබූ නිසාවෙන් සමාගමෙන් පිටත කිසිවෙකුට මෙය නිරාවරණය නොවී ඇති අතර, සමාගමේ අභ්‍යන්තර සේවකයින් ඒවා අනිසි ලෙසින් භාවිතයට ගත බවට තවමත් කිසිදු සාක්ෂ්‍යයක් නැහැ. මේ නිරාවරණය වුණු මුරපද මිලියන 100ක් පමණ facebook lite භාවිත කරන්නන් වන අතර, මිලියන 10ක් පමණ අනෙක් පරිශීලකයන්, සහ 10,000ක් පමණ Instagram පරිශීලකයින් ද වෙනවා. මේ ලෙසින් පරිශීලක මුරපද සටහන්ව තිබූ ගොනු තුළින් facebook සමාගමේ සේවකයින් 2000ක් පමණ විවිධ සෙවීම් සිදු කර ඇති අතර, මේ ගොනු වෙත සිදුවුණු පළමු ඇතුළුවීම 2012 වසර දක්වා දිවෙන බව සඳහන් වෙනවා.

මීට පෙර සිදුවුණු මෙවැනි සිදුවීමක් පිළිබඳව පෙර ලිපියකින් අප ඔබ වෙත තොරතුරු ගෙන ආවා. මෑතක ලොව පුරා පරිශීලකයන් විශාල ප්‍රමාණයකට සිදුවුණු facebook බිඳ වැටීම ගැනත් ඔබට මතක ඇති.

වැඩි ආරක්ෂාව සඳහා මුර පද වෙනස් කර, security key එකක් හෝ two-factor authentication on කර ගන්න කියලා Roar අපි යෝජනා කරනවා.

පසුගිය 2018 වසර සහ මේ ගෙවෙන 2019 වසරේ මුල් භාගය ලෝකයේ ප්‍රසිද්ධ සහ ජනප්‍රිය සමාගම් ගණනාවකට එතරම් සුභදායි වුණේ නම් නැහැ. විශේෂයෙන්ම ඇපල් සමාගමට මේ ලැබූ වසර අරඹන්නට සිදු වුණේ විශාල ගැටළු රාශියකට මුහුණ දෙන ගමන්. විටින් විට විවිධ ක්‍රමවේදයන් භාවිතා කරමින් නැවතත් තම ස්ථාවරත්වය ගොඩ නගා ගැනීමට, සහ තමන් වෙත පැවරුණු නඩුවලින් නිදහස් වෙන්නට ඇපල් සමාගම දැරූ බොහෝ ප්‍රයත්නයන් අපට දැකගන්නට ලැබුණා. විශේෂයෙන්ම Qualcomm සමාගම සමග පවතින ගැටළුව ඉතාම උග්‍ර මට්ටමකට පසුගිය දින කිහිපය තුළ ළඟා වුණා. Qualcomm සමාගම ලෝ වටා රටවල් ගණනාවක අධිකරණයන්වල ඇපල් සමාගමට විරුද්ධව නඩු පැවරුවා.

පසුගිය දිනක සැන් ඩියේගෝ නගරයේ අධිකරණයක පැවති නඩු විභාගයක දී ඇමරිකානු ඩොලර් මිලියන 31ක මුදලක් Qualcomm සමාගම වෙත ගෙවන ලෙස අධිකරණය ඇපල් සමාගමට නියෝගයක් නිකුත් කළා. ඒ, ඔවුන් සතුව හිමිකම් පවතින පේටන්ට් බලපත්‍ර 3කට අදාල තාක්ෂණයන් ඇපල් සමාගම විසින් භාවිත කර ඇති බව හෙළි වීම නිසාවෙන්. මේ නඩුව Qualcomm සමාගම විසින් 2017 වසරේ ගොනු කරන ලද්දක් වන අතර, එය ඔවුන් අධිකරණය වෙත ගොනු කළ අනෙකුත් නඩුවලට සාපේක්ෂව කුඩා එකක් වීමත් බොහෝ දෙනෙකුගේ අවධානය දිනා ගත්තා. මේ අනුව,

මේ තාක්ෂණයන් පේටන්ට් බලපත්‍ර අනුව Qualcomm සමාගම සතු තාක්ෂණයන් බවත්, ඇපල් සමාගම iPhone වෙත ඒ තාක්ෂණයන් අවසරයකින් තොරව භාවිත කර ඇති බවත් නඩු විභාගයන් අතරේ දී අනාවරණය වුණා. මෙහි පළමු තාක්ෂණය ඇපල් සමාගමේ සේවකයෙක් විසින් නිර්මාණය කර ඇති බව ඔවුන් පැවසුවත් ජූරිය විසින් එය ප්‍රතික්ෂේප කර ඇති බව සඳහන් වෙනවා. බොහෝ විට ලබන මාසයේ පැවැත්වීමට නියමිත නඩු විභාගයේත් වැඩි වාසිය Qualcomm සමාගම සතු වනු ඇති බව බොහෝ දෙනෙකු විශ්වාස කරනවා.

ඇපල් සමාගම ඔවුන්ගේ store එක හරහා සිදු කරන සියලු මිල දී ගැනීම් සඳහා 30%ක කොමිස් මුදලක් අය කරගන්නවා. අදාළ නිර්මාණකරු හෝ නිෂ්පාදකයාට ලැබෙන්නේ 70% මුදලක් පමණ යි. මාසිකව ගෙවීම් සිදු කළ යුතු Spotify වැනි monthly subscriptionවලිනුත් මේ මුදල අයවීම සිදු වෙනවා. මෙය බලපානු ලබන්නේ App Store එක හරහා සිදු කරනු ලබන ගණුදෙනුවලට පමණක් වන බැවින්, Spotify සමාගම විසින් ඒ වෙනුවට වෙනත් Payment method එකක් භාවිතා කිරීමට උත්සාහ කර තිබෙන අතර, Apple සමාගමේ නීති අනුව එයට ද ඉඩක් නොමැති බව මොවුන් ප්‍රකාශ කරනවා.

මීට අමතරව Spotify වැනි සේවාවන්වල promotions ආදිය ද වලක්වාලීමට Apple සමාගම කටයුතු කර තිබෙන බව ඔවුන් සඳහන් කරනවා. Apple Music ප්‍රචාරණය කිරීම අරමුණු කරගෙන Spotify ඇතුළු අනෙක් online streaming සේවාවන් වෙත Siri වැනි පහසුකම් ලබා නොදෙන්නටත්, Apple music වෙත පමණක් ඒ පහසුකම් ලබා දෙන්නට සමාගම කටයුතු කර තිබෙනවා. මේ නිසාවෙන් තව දුරටත් අඩු මුදලට තම සේවාව පාරිභෝගිකයන්ට ලබා දෙන්නට නොහැකි බව Spotify සමාගම සඳහන් කර තිබුණා. මේ ආකාරයේ විවිධ ක්‍රියාකලාපයන් කිහිපයක් සම්බන්ධ කරමින් යුරෝපා කොමිසම ඉදිරියේ නඩුවක් පැවරීමට Spotify සමාගම කටයුතු කර තිබෙන අතර, මීට අදාල කටයුතු සිදු කරමින් පවතින බව යුරෝපා කොමිසමේ නිළධාරියෙකු විසින් The Wall Street Journal වෙබ් අඩවියට ප්‍රකාශ කර තිබුණා.

ඊයේ දිනයේ සිට Facebook, Instagram යන ප්‍රධානම සමාජ ජාලයන්ගේ බිඳවැටීමක් ලෝකයේ විවිධ ප්‍රදේශවලින් වාර්තා වුණා. මේ බිඳවැටීම සියලු දෙනාට බල නොපෑ අතර පිරිසකට මේ හරහා දැඩි ලෙසින් බලපෑම් එල්ල වුණා. Photos upload කිරීම share කිරීම, සහ status update කිරීම වැනි ප්‍රධාන පහසුකම් ලොව පුරාම මිලියන ගණනක් පරිශීලකයන් කලබලයට පත් කරන්නට සමත් වුණා. මේ බලපෑම ඉන් නොනැවතී Whats App වෙතත් බලපෑම් එල්ල කරනට සමත් වුණා. group call පහසුකම අඩපණ වීම සහ WhatsApp status දැමීමට නොහැකි වීම වැනි දේ සිදුවුණා. මෙය බලපෑ තවත් සේවාවක් ලෙසින් facebook සමාගම් ජාලය යටතේම පවතින Oculus store එක හරහා games මිල දී ගැනීමට නොහැකි වීම් පිළිබඳවත් ලෝකය පුරාම පරිශීලකයන්ගෙන් පැමිණිලි වාර්තා වෙනවා.

ඒ වගේම facebook හරහා sign වීමෙන් ගිණුම් වෙත ඇතුල් වීමට හැකියාව ලබාදුන් Spotify, Tinder වැනි සේවාවන් වෙතත් සම්බන්ධ විය නොහැකි වීම් පිළිබඳව TechCrunch වෙබ් අඩවිය වාර්තා කර තිබුණා. මේ බිඳවැටීම් මාලාව සිදුව ඇතැ යි සැලකෙන්නේ ඇමරිකානු නැගෙනහිර වෙරළබඩ වේලාවෙන් (Eastern Time (ET)) 13 වෙනි බදාදා දහවල් 12.53 පමණයි (ලංකාවේ වේලාවෙන් රාත්‍රී 10.22ට පමණ).

මේ වන විට තත්ත්වය බොහෝ සෙයින් යථා තත්ත්වයට පත්ව ඇති අතර, මෙම බිඳවැටීමට හේතුව “DDOS ප්‍රහාරයක්” නොවන බව නිල වශයෙන් ඔවුන්ගේ twitter ගිණුම් හරහා ෆේස්බුක් සමාගම මේ වන විට නිවේදනය කොට තිබෙනවා. ඒ නිසාවෙන්, මේ සිදුවීම මුලික කරගෙන පැතිරෙන අසත්‍ය කතාවන්ට නොරැවටෙන ලෙස අපි දැනුවත් කරන්න කැමතියි.

මේ බිඳවැටීම සහ බලපෑ අනෙක් සේවාවන් ගැන වගේම ඕනෑම බොහෝ විට වෙබ් අඩවි බිඳවැටීම් පිළිබඳ live map සපයන down detector වෙබ් අඩවිය හරහා මේ ආකාරයෙන් අදාළසේවාවන් අක්‍රීය වී ඇති ප්‍රදේශයන් සහ කාලය පිළිබඳව දැනට පවතින තත්ත්වය පිළිබඳව විස්තර දැනගැනීමේ හැකියාව තිබෙනවා. ඒ වගේම මේ සිදුවීමට නිල හේතුවක් තවමත් facebook සමාගම ප්‍රකාශ කර නැහැ. ආරංචි මාර්ගවලට අනුව මෙය facebook සමාගමේ server යාවත්කාලීන වීමක් බව තමයි දැනගන්න ලැබෙන්නේ.

මීට දින කිහිපයකට පෙර තමයි facebook ඇතුළු සමාගම් කිහිපයක් එක්ව බල ගැන්වෙන marea cable එකෙහි වේගය පිළිබඳව අපි ඔබට තොරතුරු ගෙන ආවේ.

Facebook සමාගම, Microsoft සමාගම, සහ යුරෝපයේ විදුලි සංදේශ සේවා සහ යටිතල පහසුකම් සපයන සමාගමක් වන Telxius විසින් 2017 වසරේ ඔවුන්ගේ දැවැන්තම ක්‍රියාවලියේ සාර්ථක නිමාව පිළිබඳව ලෝකය දැනුවත් කළා. ඒ Marea නම් මුහුද යටින් දිවෙන දීර්ඝ Cable එක සාර්ථකව එලා අවසන් කිරීම සම්බන්ධයෙනුයි. මේ subsea cable එකේ දිග කිලෝමීටර 6,600ක් පමණ (සැතපුම් 4100 පමණ) වෙනවා. මෙය පිහිටා තිබෙන්නේ ආදී 17,000 පමණ ගැඹුරු මුහුදේ. සාමාන්‍යයෙන් මුහුදු යටින් දිවෙන මෙවැනි කේබලයක් එළිම සඳහා වසර 5කට ආසන්න කාලයක් ගත වෙනවා. නමුත්, මෙය සම්පුර්ණ කිරීමට ඔවුන්ට ගත වෙන්නේ වසර 2කට ආසන්න කාලයක් පමණයි. මේ කේබලය මඟින් ස්පාඤ්ඤ සහ ඇමරිකාව අතර සම්බන්ධතාවය ගොඩනගනවා. මෙම කේබලය තුළින් දත්ත ගමන් කරන වේගය (න්‍යායයික දත්ත හුවමාරු වේගය) 160Tbps වුවත්, ප්‍රායෝගිකව ලබාගත හැකි සාමාන්‍යය දත්ත හුවමාරු වේගය 9.5Tbps පමණ වුණා. ඔවුන් මේ පවතින තත්ත්වයන් සහ තාක්ෂණයන් යටතේ බලාපොරොත්තු වන උපරිම වේගය වූ 20Tbps වෙත යාමට හැකියාව ලැබුණෙත් නැහැ.

Marea කේබලය සහ එහි භූගෝලීය පිහිටීම් ඔස්සේ වඩාත් කාර්යක්ෂමව අන්තර්ජාල සම්බන්ධතාවයන් ලබා ගන්නට පහසුකම් ප්‍රධානව සැලසුණේ යුරෝපයට වුණත් ආසියා මහද්වීපය, අප්‍රිකා මහද්වීපය, ඇතුළු ප්‍රදේශ ගණනාවකට මෙහි වක්‍ර පහසුකම් සැලසුණා. මෙහි බර නිල් තල්මසුන් 34 දෙනෙකුට සමාන කරනවා. එනම්, කිලෝග්‍රෑම් මිලියන 4.65ක් පමණ වෙන බව තමයි වාර්තා වෙන්නේ. මේ ක්‍රියාන්විතය අතිශයින් වැදගත් වෙන්නේ ඒ වන විටත් ලෝකයේ ආර්ථිකය සම්පුර්ණයෙන්ම වාගේ රඳා පැවතුණේ අන්තර්ජාලය සහ cloud සේවාවන් මත වීම නිසයි. මේ කේබල් එක හරහා මයික්‍රොසොෆ්ට් සමාගමේ Azure cloud platform එක Microsoft’s Office 365, Xbox Live, Facebook, Instagram සහ Whatsapp ඇතුළු සේවාවන් රාශියක් වෙනම තලයකට ඔසවා තබන්නට ඔවුන්ට හැකියාව ලැබුණා. වඩාත් ඉක්මනින් නොබිඳෙන සම්බන්දතාවයන් සහිතව සන්නිවේදනයේ නිම්වළලු පුළුල් කිරීමේ විශාල පියවරක් ලෙසින් එවකට මෙය හැඳින්වුණා.

පසුගිය දිනක 16QAM modulation භාවිත කරමින් ඔවුන් සිදුකරන ලද අත්හදා බැලීමක ප්‍රතිඵලයක් ලෙසින් ඔවුන් බලාපොරෝත්තු වූ වේගයට වඩා වැඩි වේගයක් ලබා ගත හැකි බව ඔවුන් සොයා ගත්තා. 26.2Tbps තරම් වේගයක් කරා යන්නට ඔවුන්ට මේ හරහා හැකියාව තිබෙන බව තමයි දත්ත සටහන්වල වාර්තා වුණේ. මෙය ඉතාම වැදගත් ආරංචියක් බවට පත් වෙන්නේ, තවත් ඇමරිකානු ඩොලර් මිලියන ගණනක් වියදම් කර නව කේබල් එකක් එළීමට වඩා පවතින කේබල් එකම ආධාරයෙන් data transferring speed එක වැඩි කර ගැනීමට ඔවුන්ට හැකියාව ලැබීමයි.

ගෙවුණු 2018 වසර සහ උදාවුණු 2019 වසර facebook ඇතුළු විශාල සමාගම් රාශියකට එතරම් සුභදායී වසරක් නම් නෙවෙයි. ලෝකයේ ප්‍රමුඛතම සමාගමක් වූ ඇපල් සමාගමටත් මේ අපල කාලයට මුහුණ දෙන්නට සිදු වුණු ආකාරය ගැන අප පෙර ලිපියකින් ඔබව දැනුවත් කළා. Qualcomm සමාගමේ patent බලපත්‍ර කිහිපයක් උල්ලංඝනය කිරීමේ සිදුවීමක් මුල්කරගෙන ජර්මනිය තුළ iPhone 7 සහ 8 ජංගම දුරකතන මාදිලි විකිනීමට තහනම් පැනවුණා. නමුත් පසුගිය සතිය තුළ සිදුවුණු දීර්ඝ සාකච්ඡා අතරතුර දී ඇතිකරගත් එකඟතාවයන් නිසාවෙන් මේ අවහිරතා මඳක් ලිහිල් කරන්නට Qualcomm සමාගම තීරණය කර තිබෙනවා. Apple සමාගමට Qualcomm chips භාවිතා කළ iPhone 7 සහ 8 ජංගම දුරකතන පමණක් ජර්මනිය තුළ අලෙවි කිරීමටත්, Intel chips සහිත iPhone 7 සහ 8 ජංගම දුරකතන විකිණීම තව දුරටත් අවහිර කරන්නටත් ඔවුන් තීරණය කළා. මේ අනුව ඔවුන් ජර්මනිය තුළ අලෙවි කරන සියලුම ඇපල් ජංගම දුරකතන සඳහා Qualcomm chips පමණක් භාවිතා කරන්නට තීරණය කළ බව ඇපල් සමාගම නිවේදනය කළා.

නමුත් ඇපල් සමාගමට චීනය තුළ පැවති තහනම තව දුරටත් ක්‍රියාත්මක යි. ඇපල් සමාගමට පැනවූ මේ තහනමට බලපෑ හේතුව මෘදුකාංග යාවත්කාලීන කිරීමක් මඟින් නිවැරදි කිරීමට කටයුතු කර ඇති බවට වාර්තා වෙනවා.

මිනිසාගේ එදිනෙදා වැඩ කටයුතු පහසු කර ගන්නට සහාය දක්වන කෘත්‍රිම බුද්ධි සහායකයින් පිළිබඳව අප පෙර ලිපියකින් ඔබව දැනුවත් කළා. Smart Home කියන සංකල්පය තුළ දී Google home සහ google assistant තරමට තෙවන පාර්ශවීය යෙදුම් නොමැති බව ඔබ සමහර විට දන්නවා ඇති. මේ නිසාවෙන්ම apple සමාගම පසුගිය දිනෙක PullString නම් ආයතනයක් මිල දී ගත්තා. ඇපල් දුරකතනයෙන් ඔබ්බට ගොසින් අනෙක් smart device සමගත් ක්‍රියාත්මක වීමට නම් ඇපල් කෘත්‍රිම බුද්ධි සහායකයා වන siri වැඩසටහන අනෙක් යෙදුම් නිර්මාණ ශිල්පීන්ට සමීප කරවිය යුතු බව ඔවුන් තීරණය කරන්නට ඇති. ඒ නිසාවෙනුයි Alexa හා Google Assistant වෙනුවෙන් apps නිර්මාණයට සහාය දැක්වූ ප්‍රධාන සමාගමක් වූ PullString සමාගම ඔවුන් මිල දී ගැනීමට කටයුතු කළේ. මෙනිසා Apple Siriට අඩුවක්ව පැවතුණු 3rd party integrationsවල විශාල වර්ධනයක් ඉදිරියේ දී බලාගන්නට හැකි වේවි. නිල වශයෙන් මිල ගණන් හෙළිදරව් වී නොතිබුණත්, 2011 වසරේ ඇරඹි මෙම සමාගම ඇමරිකානු ඩොලර් මිලියන 44ත් 100ත් අතර මිලකට මිල දී ගන්නට ඇති බවට නිල නොලත් වාර්තාවල සඳහන්.

Android භාවිත කරන්නන්ට play store තිබෙනවා වගේම, Apple උපාංග භාවිත කරන්නන්ට App Store හරහා තමාගේ උපකරණ වෙත apps download කර ගන්න හැකියාව තිබෙනවා. මෙලෙසින් App Store හරහා apps download කරන සහ මිල දී ගන්නා පරිශීලකයන් වෙත credit cards ලබා දෙන්නට Apple සමාගම තීරණය කර තිබෙනවා. මේ කටයුත්ත සිදු කරන්නේ ලෝකයේ අතිශය සුප්‍රකට ගෝල්ඩ්මන් සැක්ස් නම් බැංකු ජාලයක් සමග යි. Apple devicesවල දැනටමත් තිබෙන Wallet app එකට අලුතෙන් මේ පහසුකම එකතු වීමට නියමිත යි. මේ හරහා ආරක්ෂාව අතින් දියුණුවක් වගේම, පරිශීලකයාට සහන ගණනාවක් ලබාදීමට ඔවුන් සූදානම්.

ආරම්භයක් ලෙසින් මේ පහසුකම හරහා සිදු කරන මිල දී ගැනීම් සඳහා 2%ක cash back කිරීමක් ඔවුන් සිදු කරන බව තමයි වාර්තා වෙන්නේ. තවමත් මේ පහසුකම නිල වශයෙන් පරිශීලකයන්ට ලබා දෙන දිනයක් ගැන ඔවුන් ප්‍රකාශයක් නිකුත් කර නැහැ. බොහෝ දෙනෙකු අපේක්ෂා කරන්නේ ඇපල් සමාගමේ මීළඟ එළිදැක්වීමේ උතසවයේ දී, එනම් එළඹෙන ජූනි මාසයේ පැවැත්වීමට නියමිත WWDC 2019 event එකේ දී, මෙය නිල වශයෙන් පරිශීලකයන් වෙත ලබා දෙනු ඇති බව යි. ඒ වගේම මෙම event එකේ දී ඇපල් සමාගමේ නව නිර්මාණයන් පිළිබඳව ඉඟි ලබාගැනීමට හැකි වේවියැ යි බොහෝ දෙනෙක් විශ්වාසය පල කරනවා.

අන්තර්ජාලයේ සැරිසරන ඕනෑම කෙනෙකුට ඩොමේන් නාමයන් කියන්නේ නුහුරු දෙයක් නෙවෙයි. සෑම ගෙදරකටම ලිපියක් තියෙනවා වගේම, හැම වෙබ් අඩවියකටම IP (Internet Protocol) එකක් තියෙනවා. ඒක මතක තබා ගැනීම අපහසු නිසා තමයි වසම් නාමයක්, එහෙම නැත්නම් ඩොමේන් නාමයක් භාවිතා කරන්නේ. ඒ හරහා තමයි අනෙක් අයට වෙබ් අඩවිය වෙත පැමිණෙන්න මඟ සැලසෙන්නේ. මේ ඩොමේන් නාමයන් විවිධ මිල ගණන් යටතේ මිල දී ගැනීමට තියෙනවා. සාමන්‍යයෙන් namecheap.com/ godaddy.com වැනි වෙබ් අඩවියකින් ඉතාම පහසුවෙන් සහ අඩු මුදලකින් ඔබට ඩොමේන් නාමයන් මිල දී ගැනීමට පුළුවන්. ආකර්ශනීය සහ මතකයේ රැඳෙන ඩොමේන් නාමයක් හරහා තමන්ගේ වෙබ් අඩවිය ප්‍රචාරය කිරීම, සහ ජනප්‍රිය කරවීම වඩා පහසු යි. මේ කියන්න යන්නේ ඔබට අදහා ගත නොහැකි මට්ටමේ මිල ගණන්වලින් අලෙවි වුණු ඩොමේන් නාමයන් පිළිබඳව යි.

මිනිස් ආශාවන් සහ ඇබ්බැහිවීම් කියන්නේ ව්‍යාපාරිකයන්ට විශාල වශයෙන් මුදල් උපයන්න හැකියාව සලසන කාරණා දෙකක්. ඒ අතරිනුත් සූදුව කියන්නේ ලොව පුරා විශාල වශයෙන් පිරිස් ඇබ්බැහිවෙන කුප්‍රකට අංශයක්. ඉක්මනින් මුදල් උපයන අරමුණින් බොහෝ දෙනෙක් සූදු ක්‍රීඩාවල නිරත වෙනවා. අද වෙනකොට ලෝකයේ හැමදේම ඩිජිටල්කරණය වෙමින් පවතින යුගයක සූදුවත් එලෙස වීම පුදුමයක් නෙවෙයි.

https://www.casino.com කියන්නේ සූදු ක්‍රීඩාව සඳහාම අතිශය ප්‍රසිද්ධ වෙබ් අඩවියක්. මෙහි ඩොමේන් නාමය 2003 වසරේ අළෙවි වෙලා තියෙන්නේ ඇමරිකානු ඩොලර් මිලියන 5ක් වැනි මුදලකට.

2007 වසරේ මේ ඩොමේන් නාමය අලෙවි ඇත්තේ ඩොලර් මිලියන 9.5ක මුදලකට. ලෝකයේ සමස්ත internet traffic එකෙන් 36% පමණ මෙවැනි adults movie වෙබ් අඩවි වෙත යැවෙනවා. විශේෂයෙන්ම ඇමරිකාවේ වැනි රටවල විශාල වශයෙන් ලාභ ලැබිය හැකි කර්මාන්තයක් මේ. ලෝකයේ වැඩිම traffic ඇති පෝර්නොග්‍රැෆි වෙබ් අඩවියක් ලෙසත් මේ වෙබ් අඩවිය සලකන්න පුළුවන්. ඒ, බොහෝ දෙනෙක් “porn” යන වචනය භාවිතා කරමින් සෙවුම් සිදු කරන නිසාවෙන්.

2009 වසරේ ඩොලර් මිලියන 11ක පමණ මුදලකට අලෙවි වූ ඩොමේන් නාමයක් තමයි මේ. ලෝකයේ වැඩිම ආකර්ශනයක් සහ විශාල ලාභයක් ලැබිය හැකි ක්ෂේත්‍රයක් ලෙස සැලකෙන හොටෙල් ක්ෂේත්‍රයට පමණක් නෙවෙයි, මෙම වෙබ් අඩවිය හරහා ඔබට නිවාඩුවක් ගත කිරීම සඳහා යා හැකි ගමනාන්තයන්, එයට වැයවෙන මුදල් වගේ විස්තර පහසුවෙන් ලබාගන්න පුළුවන්.

ලෝකයේ තවත් අතිශය කුප්‍රකට වෙබ් අඩවියක් ලෙස හඳුන්වන්න පුළුවන් මේ වෙබ් අඩවි ඩොමේන් නාමය 2006 වසරේ දී ඇමරිකානු ඩොලර් මිලියන 13ක පමණ මුදලකට අලෙවි වුණා. මේ වෙබ් අඩවියට වැඩිම traffic පැමිණෙන්නේ ඉන්දියාව, එක්සත් ජනපදය, ඉතාලිය වැනි රටවලින්. ඒ වගෙම ලෝකයේ ජනප්‍රියම වෙබ් අඩවි අතර මෙයත් රැඳී තිබෙනවා.

මේ වෙබ් අඩවිය 2008 වසරේ ඩොලර් මිලියන 15ක පමණ මුදලකට අලෙවි වූ වෙබ් ඩොමේන් නාමයක්. මූල්‍යමය කටයුතු පිළිබඳ වෙබ් අඩවියක් ලෙස ප්‍රචලිත මෙය 2008/2009 කාලයේ දී ponzi scheme එකකට (පිරමිඩ මුදල් වංචා වැනි) චෝදනා ලබනවා. එම සිදුවීම මේ සමාගමට එතරම් හොඳ වාතාවරණයක් ඇති කළේ නම් නැහැ.

මේ වෙබ් අඩවිය චීන ජාතික සමාගමකට අයත් වෙබ් ඩොමේන් නාමයක්. අන්තර්ජාලය හරහා ඩිජිටල් නිෂ්පාදන අලෙවි කරන වෙබ් අඩවියක් ලෙසින් ලෝකයේ ප්‍රසිද්ධියක් උසුලනවා. විශේෂයෙන්ම සයිබර් ආරක්ෂාව පිළිබඳ නිෂ්පාදන මේ හරහා අලෙවි වෙනවා. මෙය මිලියන 17කට 2015 වසරේ මිල දී ගැනුණ වෙබ් ඩොමේන් නාමයක්.

ඔබට පෞද්ගලික ජෙට් යානයන් මඟින් ගමනක් යන්නට අවශ්‍ය නම්, මේ වෙබ් අඩවිය හරහා එය සිදු කර ගන්න පුළුවන්. 2012 වසරේ ඩොලර් මිලියන 30කට මේ වෙබ් ඩොමේන් නාමය අලෙවි වෙලා තියෙනවා. අද වෙද්දි ඔවුන් www.evojets.com වෙබ් අඩවිය හරහා ක්‍රියාත්මක වෙනවා.

Privatejet.com, එහෙම නැති නම් evojets.com

Vacationrentals.com කියන්නේ 2007 වසරේ ඩොලර් මිලියන 35කට අලෙවි වුණ වෙබ් ඩොමේන් නාමයක්. මේ වෙබ් අඩවිය හරහාත් ඔබට ඔබේ නිවාඩු කාලයන් ගත කරන්නට සුදුසු ස්ථානයන් වගේම, ඒ ඒ තැන්වලට ලැබුණු reviews පවා බලාගන්න බලාගන්න පුළුවන්.

2010 වසරේ අලෙවි වූ Insurance.com ඩොමේන් නාමය ඩොලර් මිලියන 35.6ක මුදලකට තමයි අලෙවි වුණේ. ඒ වගේම carinsurance.com ඩොමේන් නාමය අළෙවි වුණේත් 2010 වසරේ යි. හැබැයි ඒ ඩොලර් මිලියන 49.7ක මුදලකට. මේ ඩොමේන් නාමයන් දෙකටම හිමිකම් කියන්නේ quinstreet.com සමාගම යි.

ලෝකයේ අද වෙද්දී රක්ෂණයන් කියන්නේ අතිශය වැදගත්කමක් දරන්නක් බවට නිතැතින්ම පත්වෙලා. අවදානම් කළමනාකරණය කියන්නේ මිනිසා අනිවාර්යයෙන්ම සිතිය යුතු කරුණක්. එයට පිලියමක් ලෙස රක්ෂනාවරණයක් ලබා ගැනීම බොහොම වැදගත් කරුණක් ලෙස ලෝකය පිළිගෙන හමාර යි. එනිසාවෙන් වන්නට ඇති මේ ඩොමේන් නාමයන් මෙතරම් මිලකට අලෙවි වෙන්නේ.

සමහර විට අද ඔබ ඔබේ නමට register කර ගන්නා ඩොමේන් නාමයන්, විශේෂයෙන්ම. com සහිත ඩොමේන් නාමයන්, පසු කලෙක විශාල මුදලකට විකුණන්න හැකියාව ලැබෙන්න ඉඩ තියෙනවා. අද වෙද්දී මේක ව්‍යාපාරයක් බවට පත් වෙලා හමාර යි. ඔබත් උත්සාහ කර බලන්න.

2019 වසර තාක්ෂණික ලෝකයේ විශාල පෙරළි ගණනාවක් සිදු වෙන්ට නියමිත වසරක් ලෙසින් හැඳින්වුවොත් එහි වරදක් නම් නැහැ. මේ වසරේ ගෙවුණු කෙටි කාලය ඇතුළත සිදුවූ බොහෝ දේ පිළිබඳ තොරතුරු අප ඔබ වෙත ගෙන ආවා. මේ කියන්න යන්නේ නව වසරත් සමගින් අලුත් වෙන, වෙනස් වෙන වෙබ් බ්‍රවුසර (web browser) පිළිබඳව යි. අපට අන්තර්ජාලයේ සැරිසරන්න පහසු කරවන web browser 21 වෙනි සියවසේ ජීවත් වෙන බොහෝ දෙනෙකුට නුහුරු දෙයක් නෙවෙයි. කාලයෙන් කාලයට විවිධ, අලුත් පහසුකම් එකතු කරමින් මේ web browsers වෙනස් මුහුණුවරක් ගන්නවා. ආරක්ෂාව, සහ පරිශීලක කැමැත්ත මත නව සංස්කරණයන් වෙත විවිධ අංගයන් එකතු කරන්නත් ඔවුන් කටයුතු කරනවා .

1995 වසරේ Opera Software AS සමාගම මඟින් නිකුත් කළ opera web browser එක ඔබ හොඳින් දන්නා web browser එකක්. මෙහි නවතම සංස්කරණය සහ එහි එන නව විශේෂාංගයන් පිළිබඳව ඔවුන්ගේ නිල බ්ලොග් අඩවියේ සටහනක් තබා තිබුණා. ඔවුන් මේ නවතම සංස්කරණය හඳුන්වා තිබෙන්නේ R3 (Reborn 3) නමින්. නවතම අංගයන් රාශියකින් සහ නව අතුරු මුහුණතක් සමගින් මෙය ඉතාම ඉක්මනින් නිකුත් වීමට නියමිත යි. මේ වන විටත් මෙහි developer සංස්කරණය නිකුත් කර අවසාන යි. තවමත් පරීක්ෂණ මට්ටමේ තිබෙන මෙහි සමහර අංගයන් ඔබේ අන්තර්ජාල අත්දැකීම නවමු මානයකට රැගෙන යාමට සමත් වෙයි කියල යි ඔවුන් විශ්වාස කරන්නේ. මේ වන විටත් Web Browser Market Shareවලින් 2.91%ක් පමණ හිමිව තිබෙන්නේ opera සමාගම වෙත යි. ඔවුන්ට අනුව මේ නව Web Browser එක හරහා වඩාත් ඉක්මනින් සහ වේගවත්ව අන්තර්ජාලයේ සැරිසරන්නට හැකියාව ලැබේවි. ඒ වගේම මෙයට නව dark theme පහසුකමක් ද එකතු වන්නට නියමිත යි. නව toolbar area එක ඇතුළත නව අංගයන් ගණනාවකුත් ඇතුළත් කිරීමට ඔවුන් සුදානමින් සිටිනවා.

පසුගිය දිනෙක වසරේ Opera Browser (android version) එකට ethereum tokens සමග ගනුදෙනු කළ හැකි cryptocurrency wallet එකක් එකතු කරන්න සමාගම කටයුතු කළා. මේ නව Reborn වීම සමග ඒ පහසු කම පරිගණකය සමග සම්බන්ධ කර ගැනීමටත් අවස්ථාව ලබා දෙන්නට opera සමාගම සුදානම් වෙනවා.

ඔවුන්ගේ ජංගම දුරකථන වෙත ලබාදෙන opera සංස්කරණය සමග ඔවුන් පෙර නවතා දැමුණු opera VPN පහසුකම යළි ලබා දීමත් සිදු වුණා.

2008 වසරේ google සමාගමේ නිල web browser එක ලෙසින් නිකුත් වුණ google chrome අද වෙනකොට ලෝකයේ වැඩිම දෙනෙක් භාවිතා කරන web browser එක බවට පත්වී තියෙනවා. Web browser market share එකෙන් 70%කට පමණ හිමිකම් කියන්නේ google chrome. කොතරම් ජනප්‍රිය වුණත් මෙය device එකේ memory, processing power, battery power අධිකව භාවිතා කරන resource hungry web browser එකක් ලෙසින් කා අතරත් කුප්‍රකට යි. වසර ගණනාවක් තිස්සේ web browser එකට ආදරය කරන බොහෝ දෙනෙක් මේ ගැන මැසිවිලි නැගුවත් ඒ පිළිබඳව කිසිවක් කරන්නට සමාගම ක්‍රියා කළේ නැහැ. නමුත් දැන් Chromium Gerrit (Chromium ව්‍යාපෘතිය) සම්බන්ධව නිකුත් කරන ලද commit එකක මේ පිළිබඳව සඳහනක් තිබෙනවා. කෙසේ වෙතත් තවමත් development stage එකේ පවතින මෙම පහසුකම, ජනතාවට නිකුත් කෙරෙන public version එකට ලබා දීමට තවත් කාලයක් ගතවනු ඇති බව තමයි බොහෝ දෙනෙකුගේ මතය. Chrome Canary හෝ Beta සංස්කරණයක් භාවිතා කරනවා නම් ඔබට මෙම පහසුකම් අත් විඳින්නට හැකියාව ලැබේවි. ඒ වගේම අලුතින් මේ වෙබ් අතිරික්සුවට වෙත dark mode එකකුත් හඳුන්වා දීමට නියමිත යි. එය ස්ථායී ලෙසින් පැමිණෙන තෙක් දැනට ඔබට ඒ වෙනුවට theme එකක් යොදා ගන්නට හැකියාව තියෙනවා.

ඒ වගේම Chrome භාවිතා කරන ඕනෑම device එකකින් browser history එක ඔබගේ සෑම Windows 10 device එකකම Timeline එකත් සමග sync වෙන ආකාරයේ extension එකකුත් Microsoft සමාගම නිකුත් කරලා තියෙනවා.

අන්තර්ජාලයේ දී ප්‍රවේශම් විය යුතු ආකාරය ගැන ලිපි ගණනාවක දී ඔබව දැනුවත් කළා. ඔබ safari වෙබ් browser එක භාවිතා කරන පුද්ගලයෙක් නම් එහි තිබූ Do Not Track පහසුකම පිළිබඳව හොඳින් දන්නවා ඇති. පසුගිය දිනක දී apple සමාගම මෙම පහසුකම ඉවත් කරන්නට තීරණය කළා. මේ option එක මඟින් සිදු වන්නේ track වීම block වීමක් නෙවෙයි, අදාළ පරිශීලකයා track නොකරන ලෙස වෙබ් අඩවිවලට පණිවිඩයක් ලබා දීම පමණ යි. නමුත් බොහෝ වෙබ් අඩවි එය පිලි නොගෙන සිතැඟි පරිදි පරිශීලකයා track කරන බව ප්‍රසිද්ධ රහසක්. iOS 12.2 වල සිට ජංගම දුරකථන සඳහාත්, macOS 12.14.4 beta සිට පරිගණක සඳහාත් මෙම පහසුකම ඉවත් කිරීමට ඔවුන් තීරණය කළා.මේ වෙනු‍වට Intelligent Tracking Prevention නම් දියුණු පද්ධතියක් හඳුන්වාදීමට ඔවුන් සුදානම් වෙනවා.

Windows/ Mac/ Linux/ IOS/ Android ඇතුළු බොහොමයක් platform සඳහා සහය දක්වන web browser එකක් ලෙසින් තමයි Brave Browser කරළියට එන්නේ.

මේ browser එක හදල තියෙන්නෙ chromium වල තියෙන ගොඩක් අනවශ්‍ය telemetry codes clean කිරීමක් සිදු කරලා. Powerful adblocker + tracking protection + script blocker + https everywhere වගේම feature add කිරීමක් සිදු කරලා තියෙනවා. මේක open වෙන්න & web surfing speed එක තරමක් වැඩි. ram usage එක අනෙක් chromium පාදක web browser වලට සාපේක්ෂව අඩු යි. ඒ වගේම මෙහි private mode (incognito mode) කොටස් දෙකක් සහිත යි. අවශ්‍ය නම් Tor tunnel එකක් සමග private window එකක් open කිරීමක් කරන්නත් හැකියාව තිබෙනවා. මෙහි UI එකත් සරල වීම මෙහි දකින්න පුළුවන් තව ලක්ෂණයක්. Chromium based නිසා chrome store එකේ තියෙන ඕන extension එකක් මේ සමග භාවිතා කරන්නට හැකියාව තිබෙනවා.

මේ වෙබ් බ්‍රවුසර මිස තව දුරටත් Internet Explorer භාවිතා කිරීම නවතා දමන ලෙස “The perils of using Internet Explorer as your default browser” යන ලිපියක් ඉදිරිපත් කරමින් Microsoft සමාගම Windows පරිශීලකයන්ගෙන් ඉල්ලා සිටිනවා. මේ ලිපිය හරහා එහි ඇති අවදානම පිළිබඳව විස්තර කෙරෙනවා. ඉදිරියේ දී chromium පාදක කර ගනිමින් වඩාත් වේගවත් සහ ආරක්ෂාකාරී ලෙසින් නව මුහුණුවරක් සහිත වෙබ් අතිරික්සුවක් හඳුන්වා දීමට Microsoft සමාගම සමාගම සූදානමින් සිටිනවා.

1983 නිමැවුණු ARPANET අද වෙනකොට අන්තර්ජාලය දක්වා දියුණු වුණ ගමනේ දී බොහෝ දේවල් වෙනස් වුණා. තාක්ෂණයේ දියුණුවත් එක්ක අන්තර්ජාලය එකතු වෙලා එදිනදා කටයුතුවල ඉඳන් අධිතාක්ෂණික සහ අති නවීන බලාගාර, හමුදා කටයුතු දක්වා පාලනය සිදු කෙරෙනවා. අන්තර්ජාලයෙන් පැමිණෙන වෛරස, ransomeware, data breach, hack වීම් පිළිබඳව වගේම තවත් බොහෝ දේ ගැනත් අප පෙර roar ටෙක් ලිපි ගණනාවකින් ඔබව දැනුවත් කරන්න කටයුතු කළා. මේ කියන්න යන්නේ අන්තර්ජාලය සම්බන්ධව ගත් රුසියාවේ හදිසි තීරණයක් පිළිබඳව යි.

අන්තර්ජාලය එක්තරා ආකාරයක යුද පිටියක් ලෙසින් හැඳින්වුවොත් එහි වරදක් නැහැ. එවැනි තත්ත්වයක් උත්සන්න වුවහොත් ගත යුතු ක්‍රියා මාර්ගයන් පිළිබඳව රුසියාව මේ දිනවල සලකා බලමින් සිටිනවා. අන්තර්ජාලය තුළින් පැමිණෙන හදිසි cyber ප්‍රහාරයක දී, මුළු රටම අන්තර්ජාලයෙන් පාලනය නොකර සිටීමට හැකිදැ යි රුසියාව අත්හදා බැලීමට සුදානම් වෙනවා. මෙවැනි ප්‍රහාරයක දී ප්‍රහාරය එල්ල කරන හැකර්කරුවන්ට රටේ සියලු කටයුතු අඩාල කිරීම, ඔත්තු බැලීමේ සිට රටෙහි යුද ශක්තිය අවභාවිතා කිරීම දක්වා ඕනෑම කටයුත්තක් සිදු කරන්නට හැකියාව තිබෙනවා.

ඔබ Hollywood ක්‍රියාදාම චිත්‍රපට නරඹන අයෙක් නම් එවැනි සිදුවීම් නුහුරු වන්නට බැහැ. මෙවැනි අවදානම් තත්ත්වයන් නිසාවෙන් රුසියාව තමන්ගේ රටවැසියන් එවැනි අවස්ථාවක දී කළ යුතුව ඇති දේ පිළිබඳව පහදන්නට මේ පෙර පුහුණුව යොදාගනිවී. බොහෝ විට ඔවුනුත් චීනයේ භාවිතා වන Great Firewall of China වැනි එකක් භාවිතා කරමින් වෙබ් අඩවි block කිරීමට සහ filter කිරීමට කටයුතු කරනු ඇති. එම censoring system එක මඟින් රටවැසියන්ගේ internet traffic රජයේ server වෙත යොමු කෙරෙනු ඇති. ඒ අතරම ඔවුන්ටම ආවේණික Domain name system එකක් හරහා අන්තර්ජාලයේ localized version එකක් ලබා දීමට කටයුතු කෙරෙනු ඇති. මේ කටයුත්ත ලබන අප්‍රේල් පළමු වෙනි දාට ප්‍රථම සිදු කිරීමට තීරණය කර ඇතත්, නියමිත දිනයක් තවමත් ස්ථිර කරගෙන නැහැ.

වෙනත් රටවලින් තම රට අන්තර්ජාලයට සම්බන්ධ වීම කපා හැරීමක් සිදු වුණොත්, එයට මුහුණ දීමට පෙර පුහුණුවක් බවට මෙය පත් කර ගැනීම රුසියානු ආණ්ඩුවේ අරමුණක් බවට කියැවෙනවා. ඒ වගේම NATO සංවිධානයට අයත් රටවලින් රුසියාවට එරෙහිව cyber සම්බාධක පැනවීම් සහ ප්‍රහාරයන් එල්ලවීම් ඉහළ යාමත් මෙම පෙර පුහුණුවට එක්තරා හේතුවක්. රුසියාවේ සියලුම අභ්‍යන්තර web traffic roskomnadzor හරහා සමීප නිරීක්ෂණයක් සිදු වේවි. ඒ වගේම ඒ හරහා රුසියානු web traffic අභ්‍යන්තරයේම රඳවාගැනීමට වග බලා ගනීවි. ඔවුන් නිර්මාණය කර ගන්නා ජාලය Runet යන නමින් හැඳින්වෙනු ඇති බවයි පැවසෙන්නේ.

රුසියානුන් මේ ව්‍යාපෘතිය සැලසුම් කරන්නේ වසර කිහිපයක සිට යි. 2020 වසර වන විට 95% පමණ internet traffic රුසියාව තුළම රඳවා ගැනීමට ඔවුන්ට හැකියාව තිබේයැ යි ඔවුන් විශ්වාස කරනවා. කෙසේ නමුත් බොහෝ විට මෙම තීරණයට හේතුව ඇමරිකාව ඇතුළු රටවලින් තමන්ගේ රටේ අභ්‍යන්තර කටයුතු පිළිබඳ සිදු වන ඔත්තු බැලීමේ ක්‍රියාවලින් අඩපණ කිරීම විය හැකියි. මේ වන විටත් රුසියාවේ ප්‍රධාන අන්තර්ජාල සේවා සැපයුම් ආයතන මේ ක්‍රියාවලියට සහය දක්වා තිබෙනවා. Internet traffic re-route කරන්නට යන වියදම සහ නව server ස්ථාපනයට යන වියදම් රුසියානු රජය දැරීමට සූදානම්. බොහෝ විට නේටෝ පාක්ෂික රටවල් විශ්වාස කරන අන්දමට ගුවන් ප්‍රහාරකට වඩා විශාල විනාශයක් සිදු කිරීමට මේවැනි cyber ප්‍රහාරයකට හැකියාව තිබෙනවා. මේ ක්‍රියාවලිය එවැනි රටවල්වලට සිදු කරන යම් ආකාරයක රතු සංඥාවක්, එහෙම නැති නම් තමන් (රුසියාව) යුද්ධයට සූදානම් බව හැඟවීමක් ලෙසින් ද බොහෝ දෙනෙකු අර්ථ දක්වා තිබෙනවා. රුසියාව මෙලෙසින් cyber ප්‍රහාරයන්ගෙන් ගැලවීම සහ පෙර සූදානම් වීම පිළිබඳ ප්‍රකාශයන් සිදු කළත්, රුසියාවේ හැකර්වරුන් නිසාවෙන් ඔවුන් අප්‍රසිද්ධියට පත් වූ වාර ගණන විශාල යි. පසු ගිය වසරේ රුසියානු හැකර්වරුන් සිව් දෙනෙකු ලන්දේසි පොලිසිය විසින් අල්ලා ගත්තේ රසායනික අවි පර්යේෂකයින් පිරිසක් එල්ල කරගෙන සිදු කරන්නට ගිය ප්‍රහාරයක් අතරතුර දී යි. ඒ සිදුවීම මහත් ආන්දෝලනාත්මක සිදුවීමක් බවට පත්වුණා.

කෙසේ වෙතත්, අන්තර්ජාලයෙන් විසන්ධී විම වගේම අන්තර්ජාල භාවිතය නිරීක්ෂණය කිරීම පිළිබඳවත් පක්ෂව වගේම විපක්ෂවත් විශාල පිරිසක් පෙළ ගැසෙන බව නම් නොරහසක්. අන්තර්ජාලයේ නිදහසේ සැරිසැරීමට ඇති හැකියාව වගේම, තමන්ගේ අන්තර්ජාල ක්‍රියාකාරකම් සමීපව නිරීක්ෂණය කිරීම ඔස්සේ පෞද්ගලිකත්වයට හානි වන බවත් ඔවුන් සඳහන් කරනවා. රුසියාවේ මේ ක්‍රියාවලිය ගැන ඔබ මොකද හිතන්නේ කියලා පහළින් comment කරන්න අමතක කරන්න එපා!

අද වෙද්දී පුද්ගලයෙකු එදිනෙදා කරන කටයුතුවල අනිවාර්යය අංගයක් බවට අන්තර්ජාලයට පිවිසීම පත් වී හමාර යි. එදිනෙදා කටයුතු සිදු කරගන්න වගේම තවත් අවශ්‍යතාවයන් උවමනාවන් විශාල ප්‍රමාණයක් සපුර ගන්නට මෙලෙස දිනපතා අන්තර්ජාලයේ සැරිසරන ඇති විශාල මට්ටමේ පරිශීලකයන් ඩැහැගන්න මාන බලන හැකර්වරුන් නිසාවෙන්ම අද වෙනකොට අන්තර්ජාලය එතරම්ම ආරක්‍ෂිත නැහැ. විශේෂයෙන්ම මෙලෙසින් අන්තර්ජාලයේ සැරිසරන පරිශීලකයන් බිලිගන්නටම නිර්මාණය වූ spams/ phishing sites වගේ දේවල් අද වෙද්දී සුලභ කරනු බවට පත්වී හමාර යි. මේවා අපට හඳුනාගන්න සහ ගැලවෙන්න ඉතාම අපහසු මට්ටමට ඉතා සූක්ෂමව සහ තාත්විකව නිර්මාණය කරන්න hackerවරුන් පියවර ගන්නවා. අන්තර්ජාලයේ සැරිසරද්දී ඔබට ආරක්ෂා වෙන්නට ගත හැකි පියවර ගැන අපි පෙර ලිපි කිහිපයක කතාබහ කළා. මේ ලිපිය හරහා කියන්න යන්නේ spams/phishing sitesවලට එරෙහිව google සමාගම ගන්න යන අලුත්ම පියවර ගැන.

ඇත්තටම phishing attacks කියන්නේ ඉතාම ප්‍රාථමික hacking/ attacking method එකක්. මේ හරහා සිදු වෙන්නේ ඔබ නිතර භාවිතා කරන වෙබ් අඩවියකට සමාන වෙබ් අඩවි ලිපිනයක් (URL) එකක් සහ පෙනුමක් සහිතව නිර්මාණය වෙන ව්‍යාජ වෙබ් අඩවියක් හරහා ඔබේ ගිණුම් දත්ත සහ පරිශීලක දත්ත සොරකම් කිරීමක්. උදාහරණයක් විදිහට ටික කලකට පෙර අතිශය ජනප්‍රිය වූ “මේ video පටයේ ඉන්නේ ඔබ ද?” වැනි ප්‍රශ්නයක් රැගත් facebook spam පණිවිඩය ඔබට මතක ඇති. මෙය click කළ සැණෙකින් ඔබව facebook වෙබ් අඩවියට පෙනුමෙන් ඉතා සමාන, වෙනත් ව්‍යාජ “ෆේස්බුක්” වෙබ් අඩවියක් වෙත යැවෙනවා. එයට log වෙන්න ඔබේ facebook ගිණුමේ මුරපද (password) සහ පරිශීලක නාමය (user name) අහනවා. එය වෙත මුර පද ලබා දුන් සැණෙන් ඔබේ මුර පද හැකර්කරුවා වෙත ලැබෙනවා. 2014 වසරේ ලෝකයේ වැඩිම කතාබහට පත්වූ iCloud හැක් වීමත් සිදු වුණේ මෙවැනි ක්‍රමයක් භාවිතාවෙන්.

\*phishing කියන යෙදුම භාවිතයට එන්නේ, ආකර්ෂණීය උපායක් භාවිතා කරමින් පුද්ගලයන් ව්‍යාජ වෙබ් අඩවි වෙත ගෙන්වා ගැනීම නිසා (හරියට ඇමක් භාවිතා කර මාළු ඇල්ලීම වගේම) යි. හැකර්වරුන් අතර “f” වෙනුවට “ph” භාවිතා වන නිසාවෙන් fishing ලෙස භාවිතා නොවී phishing ලෙසින් යෙදුණා.

බොහෝවිට මේ උපක්‍රමය භාවිතා කරන හැකර් කරුවන් ඒ පණිවිඩ සහ links බෙදාහරින්න සමාජ මාධ්‍යන් භාවිතා කරනවා. ආකර්ෂණීය පණිවිඩයක් සමගින් මේ phishing උපක්‍රම යොදාගන්නවා. මෙවැනි උපක්‍රමයන් පිළිබඳව ප්‍රජාව දැනුවත් කරන්න google සමාගම අලුතින් ව්‍යාපෘතියක් ආරම්භ කර තිබෙනවා. ඒ ඔවුන්ගේ jigsaw කියන විශේෂිත කණ්ඩායම සමගින් එකතුවෙලා. මේක ප්‍රශ්නාවලියක්. මේ මඟින් ඔබ කොතරම් දුරට phishing ගැන දැනුවත් ද, සහ නවීන phishing උපක්‍රම මඟහරින්නේ කොහොමද කියන එක පිළිබඳ ඔබව දැනුවත් කෙරනවා. phishingquiz.withgoogle.com වෙබ් අඩවියෙන් ඔබටත් මෙම ප්‍රශ්නාවලියට මුහුණ දී ඔබේ දැනුම උරගා බලන්න පුළුවන්.

Lookalike URLs කියන්නේ google chrome වෙබ් අතිරික්සුව (web browser) වෙත එකතු වෙන්න තියෙන පහසුකමක්. chrome canary වැඩසටහන යටතේ තවමත් පරීක්ෂණ මට්ටමේ පවතින මෙම විශේෂාංගය හරහා ඔබට පැමිණෙන phishing links ඉතාම පහසුවෙන් හඳුනාගෙන ඔබව දැනුවත් කිරීමක් සිදු වෙනවා. ලිපියේ මුල දී පැවසු අන්දමට බොහෝ විට phishing attacking strategy භාවිතා කරන හැකර්වරුන් අදාළ මුල් වෙබ් වෙබ් අඩවියේ URL එකට සමාන වෙබ් ලිපිනයක් නිර්මාණය කරගැනීම සිදු වෙනවා. ඉදිරියේ දී මේ Lookalike URLs විශේෂාංගය chrome වෙත එකතු වීම ඔස්සේ phishing උපක්‍රම අඩාල කිරීම google සමාගමේ අරමුණ යි.

මීට අමතරව chrome web browser එක වඩා වේගවත් කිරීමට අලුතින් තවත් පහසුකම් කිහිපයක් හඳුන්වා දීමට නියමිත යි. ඒ අතර “Never Slow Mode”, “Best Effort Tasks”, සහ “Password Checkup” පහසුකම් අඩංගු යි. ඒ පිළිබඳව තවත් ලිපියකින් විස්තර ගෙන එන්නම්.

අන්තර්ජාලයේ අප භාවිතා කරන තවත් ප්‍රධාන පහසුකමක් තමයි email (විද්‍යුත් ලිපින) සේවාවන් කියන්නේ. ඒ අතරිනුත් වැඩිම පිරිසක් භාවිතා කරන්නේ google සමාගම ලබාදෙන Gmail කියන සේවාව. අප පෙර ලිපියක email ලිපිනයන් හා බැඳුනු Data Breach පිළිබඳව කතාබහ කළා. මේ කියන්න යන්නේ email භාවිත කරද්දී අපිට ලැබෙන කරදරකාරී spam පණිවිඩවලින් ඔබව ගලවා ගැනීමට google සමාගම භාවිතා කරනා උපක්‍රමයක් ගැන. ඔවුන් tensorflow නම් machine learning platform එක භාවිතා කරමින් කෘත්‍රිම බුද්ධියක් සහිත පද්ධතියක් (Artificial Intelligence system) නිර්මාණය කර තිබෙනවා. ඒ හරහා දිනකට ලෝකය පුරා ව්‍යාප්ත වෙන මිලියන 100කට අධික spam email ප්‍රමාණයක් නැවත්වීමට සහ ඒවා කෙළින්ම spam folder එක වෙත යොමු කිරීමට මෙම වැඩසටහනට හැකියාව ලැබෙනවා. Google සමාගම පවසන අන්දමට දිනකට ලැබෙන spam පණිවිඩවලින් 99.99% ම මෙම වැඩසටහනට හඳුනා ගැනීමට හැකියාව තියෙනවා. දිනපතාම spammersලා ඔවුන්ගේ ක්‍රමවේදයන් වෙනස් කරන නිසාවෙන් මේ කටයුත්ත සිදු කිරීමට AI වැඩසටහනක් වඩාත් සුදුසු බවයි google සමාගමේ අදහස. මේ සඳහා භාවිත කර තිබෙන නවීන Algorithm නිසාවෙන් ලැබෙන spam emailවල ලක්ෂණ හඳුනා ගනිමින් එහි රටාවන් අධ්‍යයන කරමින් ඒවා block කිරීමට මෙයට හැකියාව ලැබෙනවා. Spamවලට විරුද්ධව සටනේ ප්‍රබල අවියක් බවට මෙය පත් වෙනවා නොඅනුමාන යි.

සාමාන්‍යයෙන් android භාවිතා කරන අප බොහෝ දෙනෙක් අපට අවශ්‍ය apps download කර ගන්නේ google play store හරහා. ඒ, වෙනත් වෙබ් අඩවිවලින් ගන්නවාට වඩා ආරක්ෂාකාරී බව අතින් වැඩි නිසාවෙන්. ආරක්ෂණ මෘදුකාංග නිර්මාණය කරන සමාගමක් වුණ AVAST සමාගම වරක් හෙළිදරව්වක් කර තිබුණා. ඒ userට ඉවත් කරන්නට අපහසු ලෙසින් adware ආදිය පෙන්වන apps ගණනාවක් පිළිබඳව යි.මේ සිදුවීම ඇතුළු සිදුවීම් ගණනාවක් හේතුවෙන් තමයි google protect කියන සේවාව google සමාගම හඳුන්වා දෙන්නේ. එය phone එකේ වගේම Play Store එකේ ආරක්ෂාවට හඳුන්වා දීපු feature එකක්. එමඟින් app එකේ behaviour එක analyze කරලා malware එකක් වගේ හැසිරීමක් තියෙනවා නම් phone එකෙන් සහ Play Store එකෙන්ම ඉවත් කිරීම සිදුවෙනවා. ඒ සමගම තමාගේ appsවල performance සහ stability එක maintain කරගැනීම පිළිබඳ අවවාදයකුත් google සමාගමෙන් developersලා වෙත ලබා දුන්නා. නමුත් මේ පහසුකම ලබා දුන්නේ ඉතාම මෑතක දී යි. ඊට පෙර play store වෙත upload වී තිබු apps ගණනාවක මෙවැනි අනවශ්‍ය adds දැකගන්නට හැකියාව ලැබුනා.

බොහෝ කාන්තාවන් අතර අතිශය ජනප්‍රිය Beauty Camera apps ගණනාවක් පිළිබඳව පසුගිය දින කිහිපය තුළ අසන්නට ලැබුනේ නම් එතරම් සුබදායි කතා නෙවෙයි. Trend Micro කියන security firm එක පසුගිය දිනෙක නිකුත් කළ ප්‍රකාශයක් අන්තර්ජාලයේ උණුසුම්ව කතාබහට ලක්වුණු මාතෘකාවක් බවට පත්වුණා. ඒ මිලියන ගණන් download count එකක් තිබෙන Beauty Camera apps ගණනාවක් Pornographic Content ඇතුළු ඇඩ්ස් පෙන්වීම මඟින් පරිශීලකයින් phishing වෙබ් අඩවි වෙත රැගෙන යාම, සහ ඔවුන්ගේ ගිණුම්වල මුර පද සොරා ගැනීම පිළිබඳව යි. ඒ වගේම ඒ apps මඟින් පරිශීලකයින්ගේ පෞද්ගලික ඡායාරූප අවසරයකින් තොරව ලබා ගෙනත් තිබුණා. මේ apps play store වෙතින් ඉවත් කර තිබුණත්, ඉවත් කරන මොහොත වන විටත් download මිලියන ගණනක් තිබූ apps ඒ අතර තිබුණා. මේ apps වැඩිපුරම download කරගෙන තිබෙන්නේ ආසියාතික කලාපයේ ඉන්දියාව ඇතුළු රටවල් බව තමයි Trend Micro සමාගම ප්‍රකාශ කරන්නේ. මේ apps install කර ගැනීමෙන් අනතුරුව විටින් විට home screen එකේ සහ lock screen එකේ ඇතුළුව advertisement පෙන්වීම සිදු වෙනවා. ඒ වගේම සමහරක් apps වරක් install කිරීමෙන් අනතුරුව නැවත un-install කිරීමට හැකියාවක් නැති වන ලෙසින් icon එක එම ස්ථානයෙන් ඉවත් වීම සිදු වෙනවා. එතරම්ම තාක්ෂණික දැනුම ඇති අයෙකුට එය ඉවත් කර ගැනීමට තරමක් අපහසු යි.

මෙ වගේම තවත් සිදුවීමක් පසුගිය දිනක වාර්තා වුණා. ඒ eset වෙබ් අඩවිය සහ softpedia වෙබ් අඩවි කළ හෙළිදරව්වකින් අනතුරුව යි. Clipper යන, malware වර්ගයට අයත් වෛරසයක් අඩංගු app එකක් සොයාගෙන තිබෙනවා. මේ මඟින් සිදු වෙන්නේ ඔබේ උපාංගයේ ඇති cryptocurrency address එක වෙනුවට මේ clipper එකේ නිර්මාපකගේ cryptocurrency address එක මාරු වීම යි. මෙහිදී සිදුවන්නේ යම්කිසි transaction එකක් සිදු කිරීම සඳහා අදාල පරිශීලකයා විසින් තම wallet address එක clipboard එකට copy කරගැනීමෙන් අනතුරුව, එය ඔහු විසින් අදාල තැනට paste කිරීමට ප්‍රථමව, මේ app එක නිර්මාණය කළ පුද්ගලයාගේ wallet address එක කලින් copy කරගත් address එකත් සමගින් මාරු වීම යි. ඒ ඔස්සේ අදාළ මුදල යැවෙන්නේ ඔහුට යි. මේ වංචාව ඔවුන් සිදු කරේ MetaMask සේවාවේ නිල app එක ලෙස පෙනී සිටිමිනුයි. මේ වෙනකොට ඒ අදාළ app එක ඉවත් කර තිබුණත් සිදුවුණු හානිය පිළිබඳව නම් සඳහනක් නැහැ.

පහත වගුවේ සඳහන් වෙන්නේ එසේ ඉවත් කෙරුණු apps කිහිපයක් පිළිබඳව යි.

PACKAGE

APP NAME

com.beauty.camera.years.pro

Pro Camera Beauty

com.cartoon.art.photo.ygy.camera

Cartoon Art Photo

com.lyrebirdstudio.emoji\_camera

Emoji Camera

art.eff.filter.photo.editor

Artistic effect Filter

art.filter.editor.imge

Art Editor

com.beauty.camera.project.cloud

Beauty Camera

com.selfie.camerapro.pro

Selfie Camera Pro

com.camera.beauty.kwok.horizon

Horizon Beauty Camera

com.camera.ygysuper.photograph

Super Camera

com.effects.art.photo.for.self

Art Effects for Photo

com.solidblack.awesome.cartoon.art.pics.photo.editor

Awesome Cartoon Art

com.photoeditor.artfilterphoto

Art Filter Photo

com.photocorner.artfilter.arteffect.prizma

Art Filter Photo Effcts

com.picfix.cartoonphotoeffects

Cartoon Effect

com.picsartitude.arteffect

Art Effect

com.csmart.photoframelab

Photo Editor

com.wallpapers.nuclear.hd.hd3d.best.live.nuclear

Wallpapers HD

com.perfectmakeup.magicartfilter.photoeditor.selfiecamera

Magic Art Filter Photo Editor

appworld.fillartphotoeditor.technology

Fill Art Photo Editor

com.artflipphotoediting

ArtFlipPhotoEditing

com.artphoto.artfilter.artpiczone

Art Filter

com.photoeditor.cartoonphoto

Cartoon Art Photo

com.photoeditor.prismaeffects

Prizma Photo Effect

com.cmds.artphotofiltereffect

Cartoon Art Photo Filter

com.latestnewappzone.photoartfiltereditor

Art Filter Photo Editor

com.livewallpaperstudio.pixture

app.pixelworlds.arteffect

Art Effect

timepassvideostatus.photoarteffect.cartoonpainteffect

Photo Art Effect

com.techbuzz.cartoonfilter

Cartoon Photo Filter

දැනටමත් ඉහත වගුවේ සඳහන් apps ඔබේ දුරකතනයේ තිබේ නම් ඒවා ඉවත් කර ගන්න. Settings වෙත පිවිස එහි apps යන කොටසින් ස්ථාපනය වී ඇති සියලු apps දැකගන්න පුළුවන්. නැවත apps install කරගැනීමට පෙර reviews කියවන්න. හැකි නම් premium ප්‍රතිවෛරස මෘදුකාංගයක් ස්ථාපනය කරගන්න. ඒ වගේම හැම විටම ඔබේ දුරකතනය යාවත්කාලීන කර තබා ගන්න.

Facebook වෙබ් අඩවිය සමාජය තුළ සිදු කළ පෙරළිය සුළුපටු එකක් නෙවෙයි. ඒ සමාජ රැල්ල තම පසට හරවා ගැනීමට google සමාගම දැරූ ප්‍රයත්නයක ප්‍රතිඵල ලෙසින් තමයි G+ 2011 වසරේ දී කරළියට එන්නේ. කෙසේ වෙතත් ඒ වෙද්දී facebook සමාජ ජාලය සමගින් රැඳී සිටි පිරිස මේ වෙත අද්දවා ගන්නට google සමාගම අසමත් වුණා. වසර 8ක් පුරාවට ඔවුන් පවත්වාගෙන ආ මෙම සමාජ ජාලය නවතා දමන්නට ඔවුන් සූදානම් වෙමින් ඉන්නවා. එයට හේතුව ලෙසින් ඔවුන් ප්‍රකාශ කරන්නේ මෙය භාවිතා කරන පරිශීලකයින්ගේ අඩු බව යි. නමුත් එයට බලපෑවේ පුද්ගල දත්ත පිටතට නිරාවරණය වන ආකාරයේ bug එකක් සහ පසුගිය වසරේ එල්ල වුණු සයිබර් ප්‍රහාරය හේතුවෙන් පරිශීලකයන් 500,000කට ආසන්න පිරිසකගේ පෞද්ගලික දත්ත නිරාවරණය වීම බව wall street journal, thehackernews.com ඇතුළු වෙබ් අඩවි ගණනාවක ලිපිවල සටහන් වුණා. Google සමාගම පමණක් නෙවෙයි, පසුගිය වසර තුළ සමාගම් ගණනාවකට මෙවැනි ප්‍රහාරයන්ට මුහුණ දෙන්න සිදු වුණා. facebook සමාගමට එල්ල වුණු චෝදනාව ගැන වගේම මෙතෙක් සිදුවුණු විශාලතම දත්ත නිරාවරණය, එහි භයානකත්වය වගේම එවිට ඔබ ගත යුතු ක්‍රියාමාර්ග පිළිබඳවත් පෙර ලිපි කිහිපයක අපි ඔබ දැනුවත් කළා .

සමහරු චෝදනා කරන්නේ G+ සේවාව මඟින් සමාගම ලැබූ ලාභය ප්‍රමාණවත් නොවුණු නිසා එය වසා දමන්නට ඔවුන් තීරණය කළ බව යි. Google සමාගම නවතා දැමුණු සේවාවන් අතරට ලබන අප්‍රේල් මස 2 වන දා පමණ වන විට මේ සේවාවත් එකතු වේවි. කෙසේ වෙතත් මේ වන විටත් Google+ profile, pages, communities, සහ events නිර්මාණය කිරීමේ හැකියාව නවතා දැමීමට ඔවුන් කටයුතු කර අවසන්.

නමුත් G Suit හරහා Google+ සේවාව භාවිතා කළ Google සමාගමේ enterprise customer පිරිසට මෙම සේවාව නවතා දැමීම බලපාන්නේ නැහැ. ඔවුන්ට තවත් වැඩි දියුණු කිරීම් කිහිපයක් සමගින් මෙය භාවිතා කිරීමට අවස්ථාව හිමිවෙනවා. කෙසේ වෙතත් මේ දත්ත මකා දැමීම සඳහා කාලයක් ගතවන බැවින් ඒ අතරතුර සමහර පරිශීලකයන්ට දත්ත පරිහරණයට අවස්ථාව හිමිවිය හැකි බවයි සමාගම සඳහන් කරන්නේ. කෙසේ වෙතත් දැනටමත් මේ සේවාවත් ‘ගූගල් සොහොන’ ලෙසින් හැඳින් වෙන killedbygoogle.com වෙබ් අඩවියේ නවතා දැමීමට ඇති සේවාවක් ලෙසින් හැඳින්වෙනවා.

මේ සේවාවට අමතරව පසුගිය වසර කිහිපය පුරාවට google සමාගමෙන් සේවාවන් විශාල ප්‍රමාණයක් නවතා දමන්නට කටයුතු කළා. ඒ අතරට goo.gl නමින් google සමාගම පවත්වාගෙන ගිය URL shortening සේවාව ඇතුළත් වුණේ පසුගිය වසරේ යි. ඒ සේවාව වෙනුවට ඔවුන් තවත් සේවාවක අනු කොටසක් ලෙසින් ක්‍රියාත්මක වෙනවා. ඒ, firebase.google.com සේවාව යි. මේ සේවාව බොහෝ දෙනෙකු ප්‍රිය කළ සේවාවක් වුවත් ඔවුන් නිර්දේශ කරන firebase සේවාව වෙත බොහෝ දෙනෙක් හුරු වී අවසාන යි.

වසර 4කත පමණ පෙර google සමාගම ඇරඹි Inbox by Gmail සේවාවත් නවතා දමන්නට සමාගම කටයුතු කර තිබෙනවා. මේ සේවාව හරහා ඔබට ලැබෙන email පණිවිඩය වෙත යැවිය යුතු reply එක suggestion එකක් ලෙසින් ලබා දීම, ඊමේල් group කිරීම්, පසුව කියැවීමට සිහිකැඳවුම් සැකසීම් ආදිය එහි ඇතුළත් වුණා. අද වන විට මේ පහසුකම් Gmail වෙතම පවරා මේ සේවාව නවතාලන්නට ඔවුන් තීරණය කර තිබෙනවා. මේ සේවාවට අමතරව December 2019 Google Fusion Tables, Fabric, Google Allo, Chromecast Audio සේවාවන් නවතා දමන්නට google සමාගම තීරණය කර තිබෙනවා.

මෙලෙසින් වසා දැමෙන සේවාවන්ට අමතරව පසුගිය වසර කිහිපය තුළම වසා දැමුණු google සේවාවන් ගණන 100කට අධික යි.

මුදල් අද වෙනකොට ලෝකයේ අපි හැමෝටම නැතුවම බැරි දෙයක් බවට පත්වෙලා ඉවරයි. මුදල් භාවිතයේ ඉතිහාසය මිනිස් ශිෂ්ටාචාරයේ ආරම්භය දක්වා දිවයන්නක්. ඒ පිළිබඳව අප පෙර පළ කළ “මුදල් භාවිතය ඇරඹුණු අයුරු” ලිපියෙන් සවිස්තරාත්මකව දැනගන්නට පුළුවන්. අද වෙද්දී මේ මුදල් භාවිතය තාක්ෂණයේ සහ බැංකුකරණයේ දියුණුවීම් සමග වෙනස්ම මානයට පැමිණ හමාර යි. අද වෙද්දී අප බොහෝ දෙනෙක් මුල්‍යමය ගනුදෙනු කරන්නට භාවිත කරන්නේ බැංකුවක් මඟින් නිකුත් කරන credit/ debit card පතක්. “ක්‍රෙඩිට් කාඩ් එකේ උපරිම ප්‍රයෝජනය ගත හැකි ක්‍රම” ලිපිය සහ “තොරතුරු යුගයේ මූල්‍යකරණයේ ප්‍රමුඛයා” ලිපි හරහාත් නව මුල්‍ය ක්‍රමයන් ගැන අප ඔබට තොරතුරු ගෙන ආවා. පසුගිය දින කිහිපය පුරාවට ලංකාවේ ප්‍රධාන පෙළේ බැංකු කිහිපයකින් ATM හරහා සිදුවන වංචාවන් පිළිබඳ මහා බැංකුවට පැමිණිලි ඉදිරිපත් වී තිබුණා. ඉතින් අපි හිතුවා ඒ පිළිබඳව වගේම, ඔබ මේ ගනුදෙනු සිදු කරද්දී ආරක්ෂා විය යුතු ආකාරය පිළිබඳත් ඔබව දැනුවත් කරන්න

ණයපත්/ බැරපත් හරහා මුදල් වංචා කිරීමේ සිදුවීම් ගණනාවක් පසුගිය වසර කිහිපය පුරාවට සිදුවුණා. ලංකාවේ එතරම්ම කුප්‍රකටව සිදු නොවුණත්, විදේශ රටවල මේ වංචාවන් හේතුවෙන් පුද්ගලයින්ගේ මුදල් මිලියන ගණන් අහිමි වෙන බව වාර්තා වෙනවා. මූලිකම වශයෙන් මේ ATM සහ බැංකු කාඩ්පත් වංචාවන් සිදුවන්නේ අප කාර්ඩ්පත ATM යන්ත්‍රයට ඇතුළු කරන විවරයට Skimming Device එකක් සූක්ෂම ලෙස සවි කිරීම මඟින්. මේ උපකරණය කිසිදු වෙනසකින් තොරව යන්ත්‍ර සමග සවිවී ක්‍රියාත්මක වෙනවා. ඒ වගේම මුදල් ලබාගැනීමේ ක්‍රියාවලියට කිසිදු වෙනසක් සිදු කරන්නෙත් නැහැ. ඔබේ කාර්ඩ්පතේ තියෙන චුම්බකිත තීරුවේ (Magnetic Strip) අඩංගු සංවේදී දත්ත මේ Skimming Device එක හරහා පිටපත් වෙනවා. ඒ අතරට ඔබේ card number එක, expiry date එක, CVV type වගේ දේවලුත් ඇතුළත් වෙනවා. නමුත් වර්තමානයේ මේ දත්ත මඟින් පමණක් ඔබේ මුදල් ATM යන්ත්‍රයක් හරහා ලබාගන්න ඔවුන්ට හැකියාව නැහැ. ඔවුන්ට ඔබේ රහස්‍ය අංකය අත්‍යවශ්‍ය යි. ඒ නිසාවෙන් ඔවුන් කුඩා රහසිගත කැමරාවක් යන්ත්‍රයේ කොහේ හෝ රඳවනවා. ඉන් පසුව ඔවුන් ඒ ඔස්සේ ඔබේ රහස්‍ය අංකයන් ලබාගනිමින් ව්‍යාජ කාර්ඩ්පත් නිර්මාණය මඟින් හෝ online මාර්ගයෙන් මුදල් වංචාවන් සිදු කරනවා. මේ ගැටලුවට විසඳුමක් ලෙසින් EMV තාක්ෂණය සහිත encrypt (ගුප්ත කේතනය) කරන ලද chip එකක් සහිතව පැමිණෙන ATM Bank Cards අද වෙනවිට සුලභ වුණත්, ඒ කාර්ඩ් පිටුපස තවමත් චුම්බකිත පටිය දැක ගන්නට පුළුවන්. එය තිබෙන තාක් එය එතරම් ආරක්ෂිත නොවන බව පහළ වීඩියෝව නැරඹූ විට ඔබට වැටහේවි.

www.readme.lk වෙබ් අඩවිය මේ පිළිබඳව ඇතැම් බැංකු වෙත දුරකථන මාර්ගයෙන් අමතා තොරතුරු ලබාගෙන තිබුණා. Commercial සහ Amana බැංකු මේ ගැටළුව හඳුනාගෙන විසඳුම් ලබා දුන් බවත්, NTB බැංකුව තාවකාලිකව ඔවුන්ගේ ATM මඟින් මුදල් ලබාදීම නතර කර පරීක්ෂණ පවත්වන බවත් ඔවුන් සඳහන් කර තිබුණා. ඔබේ කාඩ් පතේ ආරක්ෂාව පිළිබඳ සැලකිලිමත් විය යුතු අයුරු විශේෂ ප්‍රකාශයක් නිකුත් කරමින් මහා බැංකුව සඳහන් කර තිබුණා. මේ වංචාවට සම්බන්ධ චීන ජාතිකයින් දෙදෙනෙකු අත්අඩංගුවට පත්වූ බවත්, ඔවුන් සතුව තිබී ලක්ෂ 12ක මුදලක් සහ ව්‍යාජ කාර්ඩ්පත් 200කට ආසන්න සංඛ්‍යාවක් සොයා ගත් බවත් මාධ්‍ය වාර්තා කර තිබුණා.