---

layout: page

title: “මම හිතන්නේ මාව සෝදිසි කරනවා කියලා "

author: Carlos Guerra, Peter Steudtner, Ahmad Gharbeia

language: en

summary: " ඔබ ඩිජිටල් ඔත්තු බැලීමේ ඉලක්කයක් විය හැකි යැයි ඔබ සිතන්නේ නම්, මෙම කාර්ය ප්‍රවාහය නිරීක්ෂණයේ හැකි දර්ශක හඳුනා ගැනීමට ප්‍රශ්න හරහා ඔබට මග පෙන්වනු ඇත.."

date: 2023-05

permalink: /en/topics/surveilled

parent: Home

---

# මම හිතන්නේ මාව සෝදිසි කරනවා කියලා

මෑතක දී, සිවිල් අවකාශයේ ජනයේ වෙත, අපවාදාත්මක හවුල්කරුවන් විසින් ස්ටාකර්වෙයාර් භාවිතය සහ සේවකයින්ගේ ආයතනික නිරීක්ෂණ, මහා රාජ්‍ය නිරීක්ෂණ සහ ක්‍රියාකාරීන්ට සහ මාධ්‍යවේදීන්ට එරෙහිව ඉලක්කගත ඔත්තු මෘදුකාංග ව්‍යාපාර දක්වා ඔත්තු බැලීමේ සිදුවීම් රාශියක් අපි දැක ඇත්තෙමු. නිරීක්‍ෂණය කරන ලද තාක්ෂණික ක්‍රම සහ පූර්වාදර්ශවල පුළුල් වර්ණාවලිය අනුව, විශේෂයෙන් හදිසි සහාය සඳහා නිරීක්‍ෂණයේ සෑම අංශයක්ම ආවරණය කළ නොහැක.

එනම්, මෙම කාර්ය ප්‍රවාහය ඩිජිටල් ක්ෂේත්‍රයේ දක්නට ලැබෙන සහ ක්‍රියාකාරී ප්‍රතිචාරයක් සහිත හදිසි අවස්ථා නියෝජනය කරන අවසාන පරිශීලක උපාංග සහ සබැඳි ගිණුම්වලට සම්බන්ධ පොදු අවස්ථා කෙරෙහි අවධානය යොමු කරනු ඇත. ශක්‍ය විසඳුමක් නොමැති විට, අපි එය හදිසි අවස්ථාවක් ලෙස නොසලකන අතර, එය පුළුල් ලෙස ආවරණය නොකරනු ඇත (ඒ වෙනුවට, යොමු කිරීම් බෙදාගනු ඇත).

මෙම කාර්ය ප්‍රවාහය ආවරණය නොවන සමහර අවස්ථා වන්නේ:

- භෞතික නිරීක්ෂණ. ඔබ භෞතික සුපරීක්‍ෂණයෙන් ඉලක්ක කර ගනු ඇතැයි ඔබ බිය නම් සහ සහාය අවශ්‍ය නම්, ඔබට ඩිජිටල් ප්‍රථමාධාර කට්ටලය [සහාය පිටුව](../../සහාය) තුළ භෞතික ආරක්ෂාව කෙරෙහි අවධානය යොමු කරන ආයතන වෙත ළඟා විය හැකිය.

- පොදු, ආයතනික සහ පෞද්ගලික අවකාශයන්හි CCඨ්V කැමරා වැනි දෘඩාංග සමඟ දැවැන්ත නිරීක්ෂණ

- දෘඪාංග දෝෂ අන්තර්ජාල සම්බන්ධතාවයක් මත රඳා නොපවතී

දෙවන අදාළ වියාචනය නම්, නූතන දිනවල සෑම කෙනෙකුම යම් තරමකින් පෙරනිමියෙන් නිරීක්ෂණය කරනු ලැබේ:

- ජංගම දුරකථන යටිතල ව්‍යුහය නිර්මාණය කර ඇත්තේ අප ගැනම විශාල දත්ත ප්‍රමාණයක් රැස් කිරීමට වන අතර, අපගේ ස්ථානය, සම්බන්ධතා ජාලය වැනි විස්තර දැන ගැනීමට නළුවන් කිහිප දෙනෙකුට එය භාවිතා කළ හැකිය.

- සමාජ ජාල සහ විද්‍යුත් තැපැල් සපයන්නන් වැනි සබැඳි සේවාවන් ද අප ගැන විශාල දත්ත ප්‍රමාණයක් රැස් කරයි, උදාහරණයක් ලෙස අපගේ පළ කිරීම්වල මාතෘකා හෝ එකින් එක පණිවිඩවලට අදාළ දැන්වීම් අපට පෙන්වීමට වෙළඳ ප්‍රචාරණ ව්‍යාපාරවලට සම්බන්ධ කළ හැක.

- බදු හෝ සෞඛ්‍ය තොරතුරු සඳහා ලේඛන ඉල්ලීම් මත පදනම්ව "පැතිකඩ" නිර්මාණය කිරීමට හැකි වන පරිදි අපගේ අනන්‍යතාවය භාවිතා කරන සහ විවිධ රාජ්‍ය ආයතන සමඟ අපගේ අන්තර්ක්‍රියා පිළිබඳ තොරතුරු රැස් කරන අන්තර් සම්බන්ධිත පද්ධති වැඩි වැඩියෙන් රටවල් සතුව ඇත.

මෙම මහා ඔත්තු බැලීමේ උදාහරණ සහ ඉලක්කගත මෙහෙයුම්වල බොහෝ පූර්වාදර්ශයන්, සෑම කෙනෙකුම (විශේෂයෙන් ක්‍රියාකාරී අවකාශයේ) නිරීක්‍ෂණය කරන බවට හැඟීමක් ඇති කරයි, එය ව්‍යාකූලත්වයට තුඩු දිය හැකි අතර අපට මුහුණ දිය හැකි සැබෑ තර්ජන සමඟ කටයුතු කිරීමට අපගේ චිත්තවේගීය හැකියාවට බලපායි. එනම්, අපගේ අවදානම් පැතිකඩ, අප කරන කාර්යය සහ අපගේ විභව විරුද්ධවාදීන්ගේ හැකියාවන් මත පදනම්ව - අප විසින් නිරීක්ෂණය කරනු ලබන බවට සැකයක් ඇති කර ගත හැකි විශේෂිත අවස්ථා තිබේ. එය ඔබගේ කාරණය නම්, දිගටම කියවන්න.

Aa තුන්වන වියාචනය, බොහෝ නිරීක්ෂණ යෝජනා ක්‍රම (විශේෂයෙන් වඩාත්ම ඉලක්කගත ඒවා), සාමාන්‍යයෙන් දර්ශක කිහිපයක් හෝ කිසිවක් වින්දිතයින්ට ප්‍රවේශ විය හැකි අතර, එය හඳුනා ගැනීම දුෂ්කර වන අතර සමහර විට කළ නොහැක්කකි. කාර්ය ප්‍රවාහයේ සැරිසැරීමේදී කරුණාකර මෙය මතක තබා ගන්න, ඔබ තවමත් ඔබේ නඩුව ආවරණය නොවන බව හෝ වඩාත් සංකීර්ණ යැයි විශ්වාස කරන්නේ නම්, කරුණාකර කාර්ය ප්‍රවාහය අවසානයේ ලැයිස්තුගත කර ඇති සංවිධාන වෙත සම්බන්ධ වන්න.

අවසාන සලකා බැලීමක් ලෙස, නිරීක්ෂණ උත්සාහයන් දැවැන්ත හෝ ඉලක්කගත විය හැකි බව කරුණාකර මතක තබා ගන්න. දැවැන්ත නිරීක්ෂණ මෙහෙයුම් සාමාන්‍යයෙන් වේදිකාවක සියලුම පරිශීලකයින්, නිශ්චිත කලාපයක සිටින සියලුම පුද්ගලයින් වැනි සමස්ත ජනගහනය හෝ ඒවායේ විශාල කොටස් ආවරණය කරයි. මේවා සාමාන්‍යයෙන් තාක්‍ෂණය මත වැඩි වශයෙන් රඳා පවතින අතර සාමාන්‍යයෙන් ඉලක්කගත නිරීක්ෂණවලට වඩා අඩු අනතුරුදායක වේ. පුද්ගලයන් කුඩා සංඛ්‍යාවකට, කැප වූ සම්පත් (මුදල්, කාලය, සහ/හෝ ධාරිතාව) අවශ්‍ය වන අතර, සාමාන්‍යයෙන් නිශ්චිත පුද්ගලයන්ගේ ක්‍රියාකාරකම් සහ සන්නිවේදනයන් නිරීක්ෂණය කිරීම සඳහා සම්පත් දැමීම පිටුපස ඇති අභිප්‍රේරණයන් ලබා දෙන දැවැන්ත නිරීක්ෂණවලට වඩා භයානක ය.

ඔබ නිරීක්ෂණය කර ඇති බවට දර්ශකයක් ඔබ සොයා ගත්තේ නම්, වැඩ ප්‍රවාහය සමඟ ආරම්භ කිරීමට ආරම්භය ක්ලික් කරන්න.

## වැඩ ප්‍රවාහය

### ආරම්භය

> ඔබ මෙහි සිටින්නේ නම්, ඔබේ සන්නිවේදනය, ස්ථානය හෝ වෙනත් සබැඳි ක්‍රියාකාරකම් නිරීක්ෂණය කළ හැකි යැයි සිතීමට ඔබට හේතු තිබේ. පහතින් ඔබට නිරීක්ෂණයට අදාළ සැක කටයුතු ක්‍රියාකාරකම් පිළිබඳ පොදු දර්ශක මාලාවක් සොයාගත හැකිය. ඉදිරියට යාමට ඔබගේ නඩුව මත ක්ලික් කරන්න.

හැඳින්වීමෙහි සපයා ඇති තොරතුරු අනුව, ඔබ අත්විඳින්නේ කුමන ආකාරයේ ගැටලුවක්ද?

- [මට සමීපව ලුහුබැඳීමේ උපාංගයක් හමු විය](#tracking-device-intro)

- [මගේ උපාංගය සැක සහිත ලෙස ක්‍රියා කරයි](#උපාංගය-හැසිරීම-හැඳින්වීම)

- [යාවත්කාලීන හෝ යෙදුම් ස්ථාපනය කිරීම සඳහා මා අනාරක්ෂිත http-වෙබ් අඩවි වෙත හරවා යවනු ලැබේ](#සැක සහිත-යළි යොමු කිරීම්-හැඳින්වීම)

- [විශ්වාසදායක සේවාවන්ගෙන් මට ආරක්ෂක පණිවිඩ සහ ඇඟවීම් ලැබේ](#security-alerts-intro)

- [මගේ පරිගණකයට හෝ ජාලයට සම්බන්ධ සැක සහිත උපාංගයක් මට හමු විය](#සැක සහිත-උපාංගය-හැඳින්වීම)

- [මම විද්‍යුත් තැපෑල, පණිවිඩකරු හෝ ඒ හා සමානව පුද්ගලිකව බෙදාගත් තොරතුරු විරුද්ධවාදියා දනී](#ලීක්-අන්තර්ජාල තොරතුරු-හැඳින්වීම)

- [දුරකථන ඇමතුම් හෝ කෙටි පණිවුඩ හරහා බෙදාගත් රහස්‍ය තොරතුරු ප්‍රතිවාදියාට කාන්දු වී ඇති බව පෙනේ (විශේෂයෙන් සංවේදී සිදුවීම් අතරතුර)](#leaked-phone-info-intro)

- [ඔබ වටා සිටින පුද්ගලයින් නිරීක්ෂණ පියවර මගින් සාර්ථකව ඉලක්ක කර ඇත](#peer-compromised-intro)

- [වෙනත් දෙයක් / මම දන්නේ නැහැ](#වෙනත් හැඳින්වීමක්)

### tracking-device-intro

> ඔබට සමීපව අනපේක්ෂිත උපාංගයක් හමු වූවා නම් සහ එය නිරීක්ෂණ උපාංගයක් බව ඔබ විශ්වාස කරන්නේ නම්, පළමු පියවර වනුයේ උපාංගය ඇත්ත වශයෙන්ම ඔබව නිරීක්ෂණය කිරීමට ඇති බවත්, එය වෙනත් අදාළ කාර්යයන් ඉටු නොකරන බවත්ය. Internet of Things (IoT) උපාංග හඳුන්වාදීමත් සමඟ, ඒවා ටික වේලාවක් භාවිතා කිරීමෙන් පසු අපට අමතක කළ හැකි විශාල ක්‍රියා මාලාවක් කරන උපාංග සොයා ගැනීම බහුලව දක්නට ලැබේ. එය නිරීක්ෂණ උපාංගයක් බව තහවුරු කර ගැනීමේ පළමු පියවරවලින් එකක් වන්නේ වෙළඳ නාමය, මාදිලිය, ආදිය පිළිබඳ තොරතුරු සඳහා උපාංගය පරීක්ෂා කිරීමයි. වෙළඳපොලේ අඩු මිලට ලබා ගත හැකි සමහර පොදු ලුහුබැඳීමේ උපාංග අතර Apple Airtags, Samsung Galaxy SmartTag, හෝ Tile ඇතුළත් වේ. ට්රැකර්ස්. මෙම උපාංග පුද්ගලික ලිපි සොයා ගැනීමට උදවු කිරීම වැනි නීත්‍යානුකූල අරමුණු සඳහා විකුණනු ලැබේ. කෙසේ වෙතත්, අනිෂ්ට නළුවන් කැමැත්තෙන් තොරව වෙනත් පුද්ගලයින් සොයා ගැනීමට ඔවුන් අපයෝජනය කළ හැකිය.

>

> අපව අනපේක්ෂිත ට්රැකර් විසින් අනුගමනය කරන්නේ දැයි පරීක්ෂා කිරීමට, ඒවා භෞතිකව ස්ථානගත කිරීමට අමතරව, සමහර නිශ්චිත විසඳුම් සලකා බැලීම ප්රයෝජනවත් විය හැකිය:

>

> - Apple Airtags සඳහා, iOS තුළ [නොදන්නා උපාංගය යම් කාලයක් හඳුනා ගැනීමෙන් පසු ඔබට ස්වයංක්‍රීය දැනුම්දීමක් ලැබිය යුතුය](https://support.apple.com/en-us/HT212227).

> - Android සඳහා, [අසල එයාර් ටැග් සඳහා පරීක්ෂා කිරීමට යෙදුමක්](https://play.google.com/store/apps/details?id=com.apple.trackerdetect) ඇත.

> - ටයිල් උපාංග සඳහා, [ටයිල් යෙදුම](https://www.tile.com/download) නොදන්නා ට්‍රැකර් සඳහා පරීක්ෂා කිරීමට විශේෂාංගයක් ඇත.

> - Samsung Galaxy SmartTags සඳහා, ඔබට සමාන විශේෂාංගයක් සඳහා [SmartThings යෙදුම](https://www.samsung.com/us/smartthings/) භාවිත කළ හැක.

>

ඔබට සොයාගත හැකි තවත් උපාංගයක් වන්නේ GPS ට්රැකර් ය. මේවාට ඉලක්කය ඇති ස්ථානය නිතර සටහන් වන අතර සමහර අවස්ථාවලදී දුරකථන මාර්ගයක් හරහා තොරතුරු සම්ප්‍රේෂණය කළ හැකිය, නැතහොත් බාගත කිරීමට සහ විශ්ලේෂණය කිරීමට පසුව භෞතිකව එකතු කළ හැකි යම් අභ්‍යන්තර ගබඩාවක ස්ථාන ගබඩා කළ හැකිය. ඔබ මෙවැනි උපකරණයක් සොයා ගන්නේ නම්, උපාංගය ක්‍රියාත්මක වන ආකාරය අවබෝධ කර ගැනීම උපාංගය රෝපණය කළේ කවුරුන්ද සහ ඔවුන් තොරතුරු ලබා ගන්නේ කෙසේද යන්න පිළිබඳ වඩා හොඳ හැඟීමක් ඇති කර ගැනීමට ප්‍රධාන වේ.

>

> ඔබ සොයා ගන්නා ඕනෑම ආකාරයක නිරීක්ෂණ උපකරණයක් සඳහා, ඔබ ඒ පිළිබඳ සෑම දෙයක්ම ලේඛනගත කළ යුතුය: වෙළඳ නාමය, ආකෘතිය, එය රැහැන් රහිත ජාලයට සම්බන්ධ වන්නේ නම්, ඔබ එය හරියටම සොයාගත් ස්ථානය, අදාළ යෙදුමේ ඇති උපාංගයේ නම් යනාදිය.

උපාංගය හඳුනා ගැනීමෙන් පසුව, ඔබට අනුගමනය කිරීමට අවශ්‍ය විය හැකි උපාය මාර්ග කිහිපයක් තිබේ. ඔබට උපාංගය සමඟ කිරීමට අවශ්‍ය කුමක්ද?

- [මට එය අක්‍රිය කිරීමට අවශ්‍යයි](#tracking-disable-device)

- [මම ක්‍රියාකරු නොමග යැවීමට එය භාවිතා කිරීමට කැමතියි](#tracking-use-device)

### tracking-disable-device

> ඔබ සොයා ගත් උපාංගයේ වර්ගය සහ වෙළඳ නාමය අනුව, ඔබට එය සම්පූර්ණයෙන්ම අක්රිය කිරීමට හෝ අක්රිය කිරීමට හැකි වනු ඇත. සමහර අවස්ථාවලදී මෙය පෙර පියවරේදී විස්තර කර ඇති ආකාරයේ ට්රැකර් යෙදුම් හරහා පමණක් නොව, භෞතික බල ස්විචයන් හරහා හෝ උපාංගයට හානි කිරීමෙන් පවා සිදු කළ හැක. ඔබට මෙම සිද්ධිය සම්බන්ධයෙන් ගැඹුරු විමර්ශනයක් කිරීමට අවශ්‍ය නම්, උපාංගය අක්‍රිය කිරීමෙන් උපාංගයේ ගබඩා කර ඇති අදාළ සාක්ෂි වෙනස් විය හැකි බව කරුණාවෙන් සලකන්න.

උපාංගයේ හිමිකරු හඳුනා ගැනීමට ඔබට වැඩිදුර ක්‍රියාමාර්ග ගැනීමට අවශ්‍යද? (\* එසේ කිරීමට ඔබට ලුහුබැඳීමේ උපාංගය සබැඳිව තබා ගත යුතු බව කරුණාවෙන් සලකන්න\*)

- [ඔව්](#උපාංග හිමිකරු හඳුනා ගන්න)

- [නැත](#පෙර-වසා දැමීම)

### tracking-use-device

> ලුහුබැඳීමේ උපාංග සමඟ කටයුතු කිරීම සඳහා එක් පොදු උපාය මාර්ගයක් වන්නේ ඔවුන් අදහස් කළ දෙයට වඩා වෙනස් දෙයක් නිරීක්ෂණය කිරීමයි. උදාහරණයක් ලෙස, ඔබ වෙනත් ස්ථානවලට යන අතරතුර ඔබට එය ස්ථිතික ආරක්ෂිත ස්ථානයක තැබිය හැකිය, නැතහොත් ඔබට එය ඔබට සම්බන්ධ නොවන චලනයේ වෙනත් ඉලක්කයක් හඹා යාමට පවා හැකිය. මෙම සමහර අවස්ථා වලදී ඔබට උපාංගයට ප්‍රවේශය අහිමි විය හැකි අතර ට්‍රැකර් වෙනත් පුද්ගලයෙකු අනුගමනය කිරීමට හෝ නිශ්චිත ස්ථානයක් හඹා යාමට ආරක්ෂාව සහ නීතිමය බලපෑම් ඇති විය හැකි බව කරුණාකර මතක තබා ගන්න.

උපාංගයේ හිමිකරු හඳුනා ගැනීමට ඔබට වැඩිදුර ක්‍රියාමාර්ග ගැනීමට අවශ්‍යද? (\* එසේ කිරීමට ඔබට ලුහුබැඳීමේ උපාංගය සබැඳිව තබා ගත යුතු බව කරුණාවෙන් සලකන්න\*)

- [ඔව්](#උපාංග හිමිකරු හඳුනා ගන්න)

- [නැත](#පෙර-වසා දැමීම)

### උපාංග හිමිකරු හඳුනා ගන්න

> ලුහුබැඳීමේ උපාංගයේ හිමිකරු හඳුනා ගැනීම සමහර අවස්ථා වලදී අපහසු විය හැකි අතර, මෙය බොහෝ දුරට භාවිතා කරන උපාංගය මත රඳා පවතිනු ඇත, එබැවින් ඔබ සොයාගත් ලුහුබැඳීමේ උපාංගය පිළිබඳව විශේෂයෙන් පර්යේෂණ කිරීමට අපි නිර්දේශ කරමු. සමහර උදාහරණ නම්:

- පාරිභෝගික ශ්‍රේණියේ රැහැන් රහිත ට්‍රැකර් සඳහා:

> - පරීක්ෂා කිරීමේ යෙදුම්වල ඒවා පෙන්වන්නේ කෙසේද?

> - ඔබට දැනුම්දීමක් ලැබුණේ කවදාද?

> - අදාළ තොරතුරු අඩංගු විය හැකි උපාංගයෙන් වැඩි දත්ත ලබා ගැනීමට ක්‍රමයක් තිබේද?

> - GPS ට්රැකර් වැනි වඩාත් කැපවූ ට්රැකර් සඳහා:

> - ඒවායේ අභ්‍යන්තර ආචයනය තිබේද? සමහර මාදිලිවල SD කාඩ්පතක් ඇති අතර එය දත්ත ග්‍රහණය කර ගැනීමට පටන් ගත්තේ කවදාදැයි බැලීමට හෝ වෙනත් අදාළ තොරතුරු ලබා ගත හැක.

> - ඔවුන්ට දුරකථන මාර්ගයක් තිබේද? ඔබට උපාංගයෙන් SIM කාඩ්පතක් ලබාගෙන අංකය ලබා ගැනීමට වෙනත් දුරකථනයකින් එය උත්සාහ කළ හැකිදැයි බැලීමට ඔබට හැකිද? මෙම තොරතුරු සමඟ, එම දුරකථන අංකයේ හිමිකරු කවුදැයි ඔබට සොයා ගත හැකිද?

> - පොදුවේ

> - උපාංගයේ ලියා ඇති නම්, ඉන්වෙන්ටරි අංක යනාදිය වැනි ඕනෑම භෞතික ඉඟි සොයන්න.

> - උපාංගය ජාලයට සම්බන්ධ වන්නේ නම්, එය හඳුනාගැනීමේ දත්ත ඇතුළත් කළ හැකි කිසියම් නිශ්චිත උපාංග නාමයක් තිබේද?

> - ඔබ උපාංගය සොයාගත් ස්ථානයට පිවිසිය හැක්කේ කාටද? තැන දැනගෙන කවදද හිටෙව්වේ?

ඔබට ලුහුබැඳීමේ උපාංග හිමිකරුට එරෙහිව නීතිමය ක්‍රියාමාර්ග ගැනීමට අවශ්‍යද?

- [ඔව්](#නීතිමය-ක්‍රියා-උපාංග-හිමිකරු)

- [නැත](#පෙර-වසා දැමීම)

### නීති-ක්‍රියා-උපාංග-හිමිකරු

> ඔබට නිරීක්ෂණ උපාංගයේ හිමිකරුට එරෙහිව නීතිමය ක්‍රියාමාර්ග ගැනීමට අවශ්‍ය නම්, ඔබේ අධිකරණ බල ප්‍රදේශයේ ක්‍රියාවලිය කෙබඳුදැයි පරීක්ෂා කිරීමට ඔබට අවශ්‍ය වනු ඇත. සමහර අවස්ථාවලදී එය නීතිඥයෙකු අවශ්ය වනු ඇත, අනෙක් අය ක්රියාවලිය ආරම්භ කිරීම සඳහා පොලිස් ස්ථානයක් වෙත ළඟා වීමට ප්රමාණවත් වනු ඇත. සෑම නඩුවකටම පොදු එකම උපදෙස නම් ඕනෑම නඩුවක් ඔබ ඒ වටා රැස් කරන සාක්ෂි තරම් ප්‍රබල වනු ඇති බවයි. හොඳ ආරම්භයක් වන්නේ ලේඛනගත කළ යුතු දේ පිළිබඳ මෙම කාර්ය ප්‍රවාහයේ පෙර පියවරවල සපයා ඇති උපදෙස් අනුගමනය කිරීමයි. [ඩිජිටල් හදිසි අවස්ථා ලේඛනගත කිරීම](/../../ලේඛනගත කිරීම) වෙත ඩිජිටල් ප්‍රථමාධාර කට්ටල මාර්ගෝපදේශය තුළ ඔබට වැඩිදුර තොරතුරු සහ උදාහරණ සොයා ගත හැක.

ලුහුබැඳීමේ උපාංග හිමිකරුට එරෙහිව නීතිමය ක්‍රියාමාර්ග ගැනීමට ඔබට උදවු අවශ්‍යද?

- [ඔව්, මට නීතිමය සහාය අවශ්‍යයි](#නීතිමය\_අවසානය)

- [නැහැ, මම හිතන්නේ මම මගේ ප්‍රශ්න විසඳුවා කියලා](# විසඳා\_අවසානය)

- [නැහැ, නමුත් මම වෙනත් නිරීක්ෂණ අවස්ථා සලකා බැලීමට කැමතියි](#පූර්ව-වසා දැමීම)

### උපාංග-හැසිරීම-හැඳින්වීම

> අද වන විට වඩාත් සුලභ ඉලක්කගත නිරීක්ෂණ ශිල්පීය ක්‍රමයක් වන්නේ ඔත්තු මෘදුකාංග මගින් දුරකථන හෝ පරිගණක ආසාදනය කිරීමයි - අනිෂ්ට මෘදුකාංග ක්‍රියාකාරකම් නිරීක්ෂණය කිරීමට සහ අන් අයට සම්ප්‍රේෂණය කිරීමට නිර්මාණය කර ඇත. ඔත්තු මෘදුකාංග විවිධ ක්‍රම හරහා විවිධ ක්‍රියාකරුවන් විසින් රෝපණය කළ හැක, උදාහරණයක් ලෙස අපයෝජන හවුල්කරුවන් විසින් උපාංගය තුළ ඔත්තු බැලීමේ යෙදුමක් (සාමාන්‍යයෙන් ස්ටාකර්වෙයාර් හෝ කලත්‍රයා ලෙස හඳුන්වනු ලැබේ) බාගැනීම හෝ යෙදුමක් බාගත කිරීම සඳහා තතුබෑම් සබැඳි යැවීම සංවිධානාත්මක අපරාධ.

>

> නිරීක්ෂණ දර්ශකවල සමහර උදාහරණ වලට මයික්‍රොෆෝනය, කැමරාව, ජාල ප්‍රවේශය යනාදිය සඳහා අවසර ඇති ඔබේ උපාංගයේ ඔබ සොයාගත් සැක සහිත යෙදුම් ඇතුළත් විය හැක. වෙබ් කැමරාවේ දර්ශක ක්‍රියාත්මක කළ යුතු කිසිදු යෙදුමක් භාවිතා නොකර හෝ උපාංගයේ ඇති ගොනු වල අන්තර්ගතය නැරඹීමෙන් තොරව " කාන්දු විය".

>

> එවැනි අවස්ථා සඳහා, ඔබට ඩිජිටල් ප්‍රථමාධාර කට්ටලය "මගේ උපාංගය සැක සහිත ලෙස ක්‍රියා කරයි" වෙත යොමු විය හැක.

ඔබ කුමක් කිරීමට කැමතිද?

- [සැක සහිත කාර්ය ප්‍රවාහය ක්‍රියා කරන උපාංගය වෙත මාව රැගෙන යන්න](../../../උපාංගය-ක්‍රියා කිරීම-සැක සහිත)

- [මෙහි මීළඟ පියවරට මාව රැගෙන යන්න](#පෙර-වසා දැමීම)

### සැක සහිත යළි-යොමුවීම්-හැඳින්වීම

> මෙය සාමාන්‍ය දෙයක් වුවද, සමහර විට අපි යෙදුම් යාවත්කාලීන කිරීමට උත්සාහ කරන විට හෝ අපගේ උපාංගවල මෙහෙයුම් පද්ධතිය පවා ආරක්ෂක ඇඟවීම් දකිමු. මේ සඳහා බොහෝ හේතු ඇත, ඒවා නීත්යානුකූල හෝ ද්වේෂසහගත විය හැකිය. අප අපගෙන්ම ඇසිය යුතු මඟ පෙන්වන ප්‍රශ්න කිහිපයක් නම්:

>

> - මගේ උපාංගයට නිවැරදි දිනයක් සහ වේලාවක් තිබේද? අපගේ උපාංග වඩාත් ආරක්ෂිතව ක්‍රියා කිරීමට සේවාදායකයන් විශ්වාස කරන ආකාරය නිශ්චිත කාල රාමුවක් තුළ වලංගු වන ආරක්ෂක සහතික පරීක්ෂා කිරීම මත රඳා පවතී. උදාහරණයක් ලෙස, ඔබේ පරිගණකය පෙර වසරක් සමඟ වින්‍යාස කර ඇත්නම්, වෙබ් අඩවි සහ සේවා ගණනාවක් සඳහා මෙම ආරක්ෂක පරීක්ෂාවන් අසාර්ථක වනු ඇත. ඔබගේ දිනය සහ වේලාව නිවැරදි නම්, එය සපයන්නා ඔවුන්ගේ සහතික යාවත්කාලීන නොකළ බව හෝ සැක කටයුතු යමක් සිදුවෙමින් පවතින බව ද යෝජනා කළ හැක. ඕනෑම අවස්ථාවක, ඔබ මෙම ආරක්ෂක අනතුරු ඇඟවීම් හෝ යළි-යොමුවීම් දුටුවහොත් කිසි විටෙකත් ඔබගේ උපාංගයේ යෙදුම් යාවත්කාලීන කිරීම හෝ ක්‍රියාත්මක නොකිරීම හොඳ රීතියකි.

> - දැන්වීමක් ක්ලික් කිරීම, යෙදුමක් ස්ථාපනය කිරීම හෝ ලේඛනයක් විවෘත කිරීම වැනි අසාමාන්‍ය සිදුවීමකින් පසුව ගැටලුව දිස් වූවාද? බොහෝ ප්‍රහාර නීත්‍යානුකූල මෘදුකාංග ස්ථාපනයන් සහ යාවත්කාලීන කිරීම් වැනි ව්‍යාජ ක්‍රියාවලීන් මත රඳා පවතී, එබැවින් මෙය ඔබගේ උපාංගය එය හඳුනාගෙන අනතුරු ඇඟවීමක් ලබා දීම හෝ ක්‍රියාවලිය සම්පූර්ණයෙන්ම නතර කිරීම විය හැකිය.

> - ඔබ අසාමාන්‍ය ආකාරයෙන් සිදුවීම සම්බන්ධයෙන් ඔබට ගැටළු ඇති ක්‍රියාවලියද, උදා. සාමාන්‍යයෙන් එම යෙදුමේ යාවත්කාලීන ක්‍රියාවලිය ඔබ දකින ක්‍රියාවලියට වඩා වෙනස් ක්‍රියාවලියක් අනුගමනය කරයිද?

ඕනෑම අවස්ථාවක, සෑම දෙයක්ම හැකි තරම් සවිස්තරාත්මකව ලේඛනගත කිරීමට අමතක නොකරන්න, විශේෂයෙන් ඔබට විශේෂිත උපකාර ලබා ගැනීමට, ගැඹුරු පරීක්ෂණයක් කිරීමට හෝ ඕනෑම නීතිමය ක්‍රියාමාර්ගයක් ගැනීමට අවශ්‍ය නම්.

>

> සෑම අවස්ථාවකම පාහේ, උපාංගය සහ සංචලනය යථා තත්ත්වයට පත් කිරීමට පෙර ගැටලුවේ මූල හේතුව ආමන්ත්‍රණය කිරීම ප්‍රමාණවත් වේ. කෙසේ වෙතත්, ඔබ ඇත්තටම යෙදුමක් (හෝ මෙහෙයුම් පද්ධතිය) සැක සහිත තත්වයන් යටතේ ස්ථාපනය කර හෝ යාවත්කාලීන කළහොත් තවත් ගැටළු ඇති විය හැක.

ඔබ සැක සහිත තත්වයන් යටතේ කිසියම් මෘදුකාංගයක් හෝ යාවත්කාලීනයක් ක්ලික් කර බාගත කර හෝ ස්ථාපනය කළේද?

- [ඔව්](#පෙර-වසා දැමීම)

- [නැත](#සැක සහිත-මෘදුකාංග ස්ථාපනය කර ඇත)

### සැක සහිත-මෘදුකාංග ස්ථාපනය කර ඇත

> බොහෝ අවස්ථාවන්හිදී, යෙදුම් හෝ මෙහෙයුම් පද්ධතිවල ස්ථාපනය හෝ යාවත්කාලීන ක්‍රියාවලීන් පැහැරගැනීම් ප්‍රහාර පද්ධතිය තුළ අනිෂ්ට මෘදුකාංග ස්ථාපනය කිරීම අරමුණු කර ගෙන ඇත. මෙය ඔබගේ සිදුවීම යැයි ඔබ සැක කරන්නේ නම්, "මගේ උපාංගය සැක සහිත ලෙස ක්‍රියා කරයි" යන ඩිජිටල් ප්‍රථමාධාර කට්ටල කාර්ය ප්‍රවාහය වෙත යාමට අපි නිර්දේශ කරමු.

ඔබ කුමක් කිරීමට කැමතිද?

- [සැක සහිත වැඩ ප්‍රවාහය ක්‍රියා කරන උපාංගය වෙත මාව රැගෙන යන්න](../../../උපාංගය-ක්‍රියා කිරීම-සැක සහිත)

- [මෙහි ඊළඟ පියවරට මාව රැගෙන යන්න](#පූර්‍ව-වසා දැමීම)

### ආරක්ෂක-ඇඟවීම්-හැඳින්වීම

> ඔබට ඊමේල් සේවා, සමාජ ජාල වේදිකා හෝ ඔබ සැබවින්ම භාවිතා කරන වෙනත් සබැඳි සේවාවකින් පණිවිඩ හෝ දැනුම්දීම් ඇඟවීම් ලැබෙන්නේ නම් සහ ඒවා නව උපාංග හෝ ස්ථානවලින් නව සැක සහිත පිවිසුම් වැනි ආරක්ෂක ගැටලුවලට සම්බන්ධ නම්, ඔබට පළමුව පණිවිඩය පරීක්ෂා කළ හැක. නීත්‍යානුකූල හෝ එය තතුබෑම් පණිවිඩයක් නම්. මෙය සිදු කිරීම සඳහා, ඉදිරියට යාමට පෙර ඩිජිටල් ප්‍රථමාධාර කට්ටලයේ කාර්ය ප්‍රවාහය [මට සැක සහිත පණිවිඩයක් ලැබුණි](../../../suspicious-messages) පරීක්ෂා කිරීමට අපි නිර්දේශ කරමු.

>

> පණිවිඩය නීත්‍යානුකූල නම්, ඔබ ඔබෙන්ම ඇසිය යුතු ඊළඟ ප්‍රශ්නය වන්නේ මෙම පණිවිඩය නීත්‍යානුකූල වීමට හේතුවක් තිබේද යන්නයි. උදාහරණයක් ලෙස, ඔබ VPN සේවාවක් හෝ Tor භාවිතා කරන්නේ නම්, සහ සේවාවක වෙබ් අනුවාදය වෙත සංචාලනය කරන්නේ නම්, එය ඔබ ඔබේ VPN සේවාදායකයේ හෝ Tor පිටවීමේ නෝඩයේ රටේ සිටින බව සිතනු ඇත, එය නව සැක සහිත පිවිසුමක් පිළිබඳ ඇඟවීමක් අවුලුවාලනු ඇත. එය ඔබ විසින්ම පරිවර්තන විසඳුමක් භාවිතා කරයි.

>

> අපෙන්ම අසාගත යුතු තවත් ප්‍රයෝජනවත් දෙයක් නම්, අපට ලැබෙන්නේ කුමන ආකාරයේ ආරක්ෂක ඇඟවීමක් ද යන්නයි: එය ඔබගේ ගිණුමට ලොග් වීමට උත්සාහ කරන කෙනෙකු ගැනද නැතහොත් ඔවුන් සාර්ථක වීම ගැනද? පිළිතුර මත පදනම්ව, අවශ්ය ප්රතිචාරය බෙහෙවින් වෙනස් විය හැකිය.

>

> අසාර්ථක පුරනය වීමේ උත්සාහයන් පිළිබඳව අපට දැනුම් දීමක් ලැබුනේ නම් සහ අපට හොඳ මුරපදයක් තිබේ නම් (දිගු, වෙනත් අනාරක්ෂිත සේවා සමඟ බෙදා නොගත් යනාදිය) සහ බහු සාධක සත්‍යාපනය භාවිතා කරන්නේ නම් (MFA හෝ 2FA ලෙසද හැඳින්වේ), අපි කරදර විය යුතු නැත. ගිණුම අවදානමට ලක්වීම වැඩියි. ගිණුමේ සම්මුති තර්ජනය කෙතරම් බරපතල වුවත්, අපට සාමාන්‍යයෙන් ස්ථානය සහ උපාංග වර්ගය ඇතුළුව අපගේ පිවිසුම් ඉතිහාසය සමාලෝචනය කළ හැකි මෑත කාලීන ක්‍රියාකාරකම්වල ඕනෑම ලොගයක් පරීක්ෂා කිරීම සැමවිටම හොඳය.

>

> ඔබගේ ක්‍රියාකාරකම් ලොගවල සැක සහිත යමක් ඔබ දුටුවහොත්, ගිණුම මත පදනම්ව, වඩාත් පොදු උපාය මාර්ගවලට ඇතුළත් වන්නේ:

>

> - මුරපද වෙනස් කිරීම

> - MFA සබල කිරීම

> - ගිණුමෙන් සියලුම උපාංග විසන්ධි කිරීමට උත්සාහ කරමින්

> - අනවසරයෙන් ඇතුළුවීමේ උත්සාහයේ දර්ශක ලේඛනගත කිරීම (අපට උදව් සෙවීමට, වැඩිදුර විමර්ශන කිරීමට හෝ නීතිමය ක්‍රියාමාර්ගයක් ආරම්භ කිරීමට අවශ්‍ය නම්)

>

> මෙම දැනුම්දීම් තක්සේරු කිරීමට උපකාර වන තවත් වැදගත් ප්‍රශ්නයක් නම්, අනතුරු ඇඟවීම ප්‍රේරණය කළ හැකි වෙනත් අයෙකු සමඟ අප උපාංග බෙදා ගන්නේ නම් හෝ ගිණුමට ප්‍රවේශය වේද යන්නයි. මෙය එසේ නම්, ඔබ ඔබේ තොරතුරු සඳහා අන් අයට ලබා දෙන ප්‍රවේශ මට්ටම ගැන ප්‍රවේශම් වන්න සහ ඔබට මෙම තුන්වන පුද්ගලයා සඳහා ප්‍රවේශය අවලංගු කිරීමට අවශ්‍ය නම් ඉහත පියවර නැවත කරන්න.

>

ඔබට පරීක්ෂා කිරීමට අවශ්‍ය කාර්ය ප්‍රවාහයේ ආරම්භයේ ලැයිස්තුගත කර ඇති වෙනත් විභව තර්ජන ඇති බව ඔබ විශ්වාස කරන්නේ නම්, හෝ වඩාත් සංකීර්ණ නඩුවක් තිබේ නම් සහ උදවු සෙවීමට අවශ්‍ය නම්, ඊළඟ ක්ලික් කරන්න.

- [ඊළඟ](#පෙර-වසා දැමීම)

### සැක සහිත-උපාංගය-හැඳින්වීම

> අපට සැක සහිත උපකරණයක් හමු වී ඇත්නම්, අප අපගෙන්ම විමසිය යුතු පළමු දෙය නම් මෙම උපාංගය අනිෂ්ටද නැතහොත් එය තිබෙන තැනට යාමට අදහස් කරන්නේද යන්නයි. මක්නිසාද යත් පසුගිය වසර කිහිපය තුළ අපගේ නිවෙස්වල සහ සේවා ස්ථානවල සන්නිවේදන හැකියාවන් සහිත උපාංග සංඛ්‍යාව සැලකිය යුතු ලෙස වර්ධනය වී ඇති බැවිනි: මුද්‍රණ යන්ත්‍ර, ස්මාර්ට් ලයිට්, රෙදි සෝදන යන්ත්‍ර, තාප ස්ථාය ආදිය. මෙම උපාංග විශාල සංඛ්‍යාව අනුව, අපි ඒ ගැන සැලකිලිමත් විය හැකිය. අපට සකසන බව මතක නැති හෝ වෙනත් කෙනෙකු විසින් වින්‍යාස කර ඇති නමුත් එය අනිෂ්ට නොවන උපාංගයකි.

>

> ඔබ සොයාගත් උපාංගය අනිෂ්ටදැයි ඔබ නොදන්නේ නම්, කළ යුතු පළමු දෙය නම් ඒ පිළිබඳ තොරතුරු ලබා ගැනීමයි: වෙළඳ නාමය, ආකෘතිය, එය රැහැන්ගත ජාලයට හෝ රැහැන් රහිත එකට සම්බන්ධ වී තිබේ නම්, එය පවසන්නේ නම් එය කරන්නේ කුමක්ද, එය බලගන්වන්නේ නම්, යනාදිය. ඔබ තවමත් උපාංගය කරන්නේ කුමක්දැයි නොදන්නේ නම්, ඔබට මෙම තොරතුරු වෙබයේ සෙවීමට සහ උපාංගය කුමක්ද සහ කරන්නේ කුමක්ද යන්න පිළිබඳව වැඩිදුර දැන ගැනීමට භාවිතා කළ හැකිය.

උපාංගය සමාලෝචනය කිරීමෙන් පසුව, එය නීත්‍යානුකූල එකක් යැයි ඔබ සිතනවාද?

- [එය නීත්‍යානුකූල උපාංගයකි](#පූර්‍ව වසා දැමීම)

- [මම පරීක්ෂා කළ නමුත් උපාංගය කුමක් කරන්නේ දැයි තවමත් නොදනිමි හෝ එය අනිෂ්ට ද යන්න](#සැක සහිත-උපාංග2)

### සැක සහිත-උපාංගය2

> මූලික සමාලෝචනයකින් පසුව ඔබ තවමත් උපාංගය ගැන සැලකිලිමත් වන්නේ නම්, එය නිරීක්ෂණ උපකරණයක් වීමේ දුරස්ථ හැකියාව සලකා බැලිය යුතුය. සාමාන්‍යයෙන් මෙම උපාංග ඔවුන් සම්බන්ධ වී ඇති ජාලයේ ක්‍රියාකාරකම් නිරීක්ෂණය කරයි, නැතහොත් ඔත්තු මෘදුකාංග මෙන් ශ්‍රව්‍ය සහ/හෝ වීඩියෝ පටිගත කර සම්ප්‍රේෂණය කිරීමට පවා හැකිය. මෙම අවස්ථාව ඉතා දුර්ලභ වන අතර සාමාන්‍යයෙන් ඉතා ඉහළ අවදානම් සහිත පැතිකඩ සමඟ බැඳී ඇති බව වටහා ගැනීම වැදගත්ය. කෙසේ වෙතත්, මෙය ඔබට අදාළ නම්, ඔබට කළ හැකි සමහර දේවල් ඇතුළත් වේ:

>

> - ජාලය/බලය වෙතින් උපාංගය විසන්ධි කිරීම සහ අවට ඇති සියලුම අපේක්ෂිත සේවාවන් ගැටළු නොමැතිව ක්‍රියා කරන්නේ දැයි පරීක්ෂා කිරීම. ඊට පසු, ඔබට අත්දැකීම් ඇති අයෙකු විසින් උපාංගය විශ්ලේෂණය කර ගත හැකිය.

> - එය තවත් පර්යේෂණ කිරීම සහ උපකාරය සොයමින් (මෙය සාමාන්යයෙන් ජාලය සිතියම්ගත කිරීම හෝ අසාමාන්ය සංඥා සෙවීම වැනි වඩාත් උසස් පරීක්ෂණ ඇතුළත් වේ).

> - VPN, Tor, හෝ ඔබේ වෙබ් බ්‍රවුස් කිරීම සංකේතනය කරන සමාන මෙවලමක් මෙන්ම අන්තයේ සිට අග සංකේතනය සහිත සන්නිවේදන මෙවලම් භාවිතයෙන් උපාංගය සම්බන්ධ කර ඇත්නම් ඕනෑම ජාල නිරීක්‍ෂණයක් අවම කිරීමට වැළැක්වීමේ පියවරක් ලෙස.

> - උපාංගය සම්බන්ධ කර ඇත්නම්, විභව ශ්‍රව්‍ය/වීඩියෝ පටිගත කිරීම් අවම කිරීම සඳහා වැළැක්වීමේ පියවරක් ලෙස, උපාංගය භෞතිකව හුදකලා කිරීම නිසා එය කිසිදු වටිනා ශ්‍රව්‍ය හෝ වීඩියෝ ග්‍රහණය නොකරනු ඇත.

ඔබට පරීක්ෂා කිරීමට අවශ්‍ය, හෝ උදවු සෙවීමට අවශ්‍ය මුලදී ලැයිස්තුගත කර ඇති වෙනත් විභව තර්ජන ඇති බව ඔබ විශ්වාස කරන්නේ නම්, ඊළඟ ක්ලික් කරන්න.

- [ඊළඟ](#පෙර-වසා දැමීම)

- [මම හිතන්නේ මම මගේ ප්‍රශ්න විසඳුවා කියලා](# විසඳා\_අවසානය)

### කාන්දු වූ-අන්තර්ජාල තොරතුරු-හැඳින්වීම

> මෙම කාර්ය ප්‍රවාහයේ ශාඛාව අන්තර්ජාල සේවා සහ ක්‍රියාකාරකම් වලින් කාන්දු වූ දත්ත ආවරණය කරයි. දුරකථන සන්නිවේදනයෙන් කාන්දු වූ තොරතුරු සඳහා, කරුණාකර ["දුරකථන ඇමතුම් හෝ කෙටි පණිවුඩ හරහා බෙදාගත් රහස්‍ය තොරතුරු විරුද්ධවාදියාට කාන්දු වී ඇති බව පෙනේ"] (#ලීක්-දුරකථන-තොරතුරු-හැඳින්වීම) කොටස බලන්න.

>

> සාමාන්‍යයෙන්, හේතු තුනක් නිසා අන්තර්ජාල පාදක සේවා වලින් කාන්දුවීම් සිදුවිය හැක:

>

> 1. තොරතුරු ප්‍රථමයෙන් පොදු වූ අතර, එය මෙම සම්පතෙන් ආවරණය නොවේ.

> 2. තොරතුරු කෙලින්ම ගිණුමෙන් කාන්දු විය (ගොදුරට සමීප "කුඩා" විරුද්ධවාදීන්ට වඩාත් පොදු).

> 3. තොරතුරු ප්‍රථමයෙන් උඩුගත කරන ලද වේදිකාවෙන් කාන්දු විය (ආණ්ඩු සහ විශාල සමාගම් වැනි "විශාල" විරුද්ධවාදීන්ට වඩාත් පොදු).

>

> සිවිල් අභ්‍යවකාශ ප්‍රජාව තුළ දක්නට ලැබෙන පොදු හදිසි අවස්ථා වලට වඩාත් සම්බන්ධ වන බැවින් අපි අවසාන අවස්ථා දෙක ආවරණය කරන්නෙමු. පහත ප්‍රශ්නයෙන් ඔබට වැඩ ප්‍රවාහය අනුගමනය කළ හැක:

ඔබ ඔබේ විරුද්ධවාදියා සමඟ උපාංග හෝ ගිණුම් බෙදා ගන්නවාද?

- [ඔව්](#බෙදාගත්-උපාංග-හෝ-ගිණුම්)

- [නැහැ](#ලීක් වූ-අන්තර්ජාල තොරතුරු2)

### බෙදාගත්-උපාංග-හෝ-ගිණුම්

> සමහර අවස්ථාවල දී, ගිණුම් ප්‍රවේශය අන් අය සමඟ බෙදාගැනීමෙන් අනපේක්ෂිත පාර්ශ්වයන්ට සංවේදී තොරතුරු වෙත ප්‍රවේශය ලබා දිය හැකි අතර, ඒවා පහසුවෙන් කාන්දු විය හැක. එසේම, සාමාන්‍යයෙන් අපි ගිණුම් බෙදා ගන්නා විට, අපි ක්‍රියාවලිය ප්‍රායෝගික කිරීමට අවශ්‍ය වන අතර, බොහෝ විට ගිණුම් ප්‍රවේශ යාන්ත්‍රණවල ආරක්‍ෂාවට බලපායි, එනම් මුරපද පහසුවෙන් බෙදා ගැනීමට දුර්වල කිරීම සහ බොහෝ දෙනෙකුට ලොග් වීමට ඉඩ දීම සඳහා බහු සාධක සත්‍යාපනය (MFA හෝ 2FA) අක්‍රීය කිරීම වැනි ය. එකම ගිණුමට.

>

> එක් පළමු උපදෙසක් වනුයේ අදාළ ගිණුම් හෝ සම්පත් වෙත ප්‍රවේශ විය යුත්තේ කාටද යන්න තක්සේරු කිරීමයි (Cloud ගබඩාවේ ඇති ලේඛන වැනි) සහ මෙය හැකිතාක් අඩු පිරිසකට සීමා කරන්න. තවත් ප්‍රයෝජනවත් මූලධර්මයක් නම්, එක් එක් පුද්ගලයා සඳහා එක් ගිණුමක් තිබීම, සෑම කෙනෙකුටම ඔවුන්ගේ ප්‍රවේශ සැකසුම් හැකි තරම් ආරක්ෂිත ආකාරයෙන් වින්‍යාස කිරීමට ඉඩ සලසයි.

>

> සැක සහිත ප්‍රවේශයකදී ගිණුම් දැඩි කිරීමට ඔබට ඉඟි සොයා ගත හැකි ["මට විශ්වාසදායක සේවාවන්ගෙන් ආරක්ෂක පණිවිඩ සහ ඇඟවීම් ලැබේ"](#security-alerts-intro) යන කොටස පරීක්ෂා කිරීම ද නිර්දේශ කෙරේ.

ඔබගේ තත්වය වඩාත් විස්තරාත්මකව ගවේෂණය කිරීමට ඊළඟ ක්ලික් කරන්න.

- [ඊළඟ](#ලීක් වූ-අන්තර්ජාල තොරතුරු2)

### කාන්දු වූ-අන්තර්ජාල තොරතුරු2

ඔබේ විරුද්ධවාදියාට ඔබ භාවිතා කරන සබැඳි සේවාවන් පාලනය කිරීමට හෝ ප්‍රවේශ වීමට සහ කාන්දු වූ තොරතුරු ගබඩා කිරීමට හැකිද? (\*මෙය සාමාන්‍යයෙන් රජයට, නීතිය ක්‍රියාත්මක කරන ආයතනවලට හෝ සපයන්නන්ටම අදාළ වේ\*)

- [ඔව්](#Control-on-online-services)

- [නැත](#ලීක් වූ-අන්තර්ජාල තොරතුරු3)

### මාර්ගගත සේවා පාලනය

> සමහර විට අපි භාවිතා කරන වේදිකා වලට පහසුවෙන් ප්‍රවේශ විය හැකිය, නැතහොත් විරුද්ධවාදීන් විසින් පාලනය කරනු ලැබේ. ඔබට ඔබෙන්ම ඇසිය හැකි පොදු ප්‍රශ්න කිහිපයක් නම්:

>

> - සේවාව අයිති කාටද?

> - එය විරුද්ධවාදියාද?

> - නෛතික දත්ත විමසීම් හරහා විරුද්ධවාදියාට සේවාදායකයන්ට හෝ දත්ත වෙත ප්‍රවේශය තිබේද?

>

> එවැනි අවස්ථාවක, අනාගත කාන්දුවීම් වලක්වා ගැනීම සඳහා තොරතුරු විරුද්ධවාදියා විසින් පාලනය නොකරන ලද වෙනත් වේදිකාවකට ගෙන යාම සුදුසුය.

>

> වෙනත් ප්රයෝජනවත් දර්ශක විය හැකිය:

>

> - පිවිසුම් ක්‍රියාකාරකම් (භූගෝලීය ස්ථාන ඇතුළුව), තිබේ නම්

> - කියවන සහ නොකියවූ අංගවල අමුතු හැසිරීම

> - ලැබෙන විට යළි හරවා යැවීම්, ඊමේල් පෙරලීමේ නීති, යනාදී පණිවිඩ හෝ තොරතුරුවලට කරන දෙයට බලපාන වින්‍යාසයන්

>

> අපට [canarytokens.org](https://canarytokens.org/generate) තුළ උත්පාදනය කළ හැකි ඒවා වැනි කැනරි ටෝකන භාවිතයෙන් ඔබේ පණිවිඩ අනපේක්ෂිත කෙනෙකු විසින් කියවා ඇත්දැයි ඔබට පරීක්ෂා කළ හැක.

ඔබගේ තත්වය වඩාත් විස්තරාත්මකව ගවේෂණය කිරීමට ඊළඟ ක්ලික් කරන්න.

- [ඊළඟ](#ලීක් වූ-අන්තර්ජාල තොරතුරු3)

### කාන්දු වූ-අන්තර්ජාල තොරතුරු3

ඔබේ විරුද්ධවාදියාට නිරීක්ෂණ උපකරණ සඳහා ප්‍රවේශය සහ එය ඔබට සමීපව යෙදවීමට හැකියාව තිබේද?

- [ඔව්](#ලීක් වූ-අන්තර්ජාල තොරතුරු4)

- [නැත](#පෙර-වසා දැමීම)

### කාන්දු වූ-අන්තර්ජාල තොරතුරු4

> වඩාත් බලවත් විරුද්ධවාදීන්ට ඔවුන්ගේ වින්දිතයන් වටා විශේෂිත නිරීක්ෂණ උපකරණ යෙදවීමේ හැකියාව තිබිය හැකිය, ලුහුබැඳීමේ උපාංග සිටුවීම හෝ ඔත්තු මෘදුකාංග සමඟ ඔබේම උපාංග ආසාදනය කිරීම වැනි.

ඔබ ලුහුබැඳීමේ උපකරණයක් මඟින් ඔබව හඹා යා හැකි යැයි ඔබ සිතනවාද නැතහොත් ඔබ ගැන ඔත්තු බැලීම සඳහා ඔබේ පරිගණකය හෝ ජංගම දුරකථනය අනිෂ්ට මෘදුකාංගවලින් ආසාදනය වී ඇතැයි ඔබ සිතනවාද?

- [මම ලුහුබැඳීමේ උපාංග ගැන තව දැන ගැනීමට කැමතියි](#tracking-device-intro)

- [මගේ උපාංගය අනිෂ්ට මෘදුකාංග සමඟ සම්මුතියට පත්වීමේ හැකියාව ගැන තව දැන ගැනීමට මම කැමතියි](#device-behaviour-intro)

### කාන්දු වූ දුරකථන-තොරතුරු-හැඳින්වීම

> මෙම කාර්ය ප්‍රවාහය හඳුන්වාදීමේ විස්තර කර ඇති පරිදි, විශාල දුරකථන නිරීක්ෂණ බොහෝ (සියල්ලම නොවේ නම්) කලාප සහ රටවල සර්වසම්පූර්ණ තර්ජනයකි. මූලික පදනමක් ලෙස, වාහකයන්ට (සහ ඒවාට පාලනය හෝ ප්‍රවේශය ඇති ඕනෑම කෙනෙකුට) මෙවැනි තොරතුරු පරීක්ෂා කිරීම ඇත්තෙන්ම පහසු බව අප දැන සිටිය යුතුය:

>

> - ඓතිහාසික ස්ථානය (දුරකථනය සක්රිය කර ජාලයට සම්බන්ධ වන සෑම අවස්ථාවකදීම), ජංගම දුරකථන කුළුණු වලින් දත්ත දුරකථනය සම්බන්ධ කරයි

> - ඇමතුම් ලඝු-සටහන් (කාටද, කවදාද සහ කොපමණ වේලාවකටද අමතන්නේ)

> - SMS (ලඝු-සටහන් සහ පණිවිඩවල සත්‍ය අන්තර්ගතය)

> - අන්තර්ජාල ගමනාගමනය (මෙය අඩු පොදු සහ විරුද්ධවාදීන්ට අඩු ප්‍රයෝජනවත් වේ, නමුත් කුමන යෙදුම් භාවිතා කරන්නේද, කුමන වෙබ් අඩවි උපදේශනය කරන්නේද යනාදිය මෙයින් අනුමාන කළ හැකිය.)

>

> සමහර සන්දර්භයන් තුළ තවමත් නිරීක්ෂණය වන තවත් දර්ශනයක්, අසාමාන්ය නමුත්, stingrays හෝ IMSI-Catchers ලෙස හැඳින්වෙන භෞතික ප්රතිරෝධක උපාංග භාවිතයයි. මෙම උපාංග ළඟා විය හැකි සමීප භෞතික ප්‍රදේශයක සිටින පුද්ගලයින්ගේ දුරකථන ගමනාගමනය ඔවුන් හරහා හරවා යැවීමට නීත්‍යානුකූල ජංගම ජාල කුළුණක් ලෙස පෙනී සිටියි. මෙම උපාංග සක්‍රීය කරන දුර්වලතා නව ප්‍රොටෝකෝල (4G/5G) සමඟ විසඳමින් හෝ අවම කරන අතරේ, පවතින එකම ප්‍රොටෝකෝලය 2G (මෙම උපාංගවලින් බහුලවම අපයෝජනය කරනු ලබන්නේ) දුරකථනවලට විශ්වාස කිරීමට සංඥාව අවහිර කිරීමට තවමත් හැකිය. මෙම අවස්ථාව සඳහා, 4G හෝ 5G තිබිය යුතු හෝ අවට සිටින වෙනත් පුද්ගලයින් ගැටළු නොමැතිව නව ප්‍රොටෝකෝලවලට සම්බන්ධ වී ඇති ප්‍රදේශවල විශේෂයෙන් 2G වෙත "පහළට" ඇති සමහර විශ්වසනීයත්වය සහිත සමහර දර්ශක තිබේ. වැඩි විස්තර සඳහා ඔබට [FADe ව්‍යාපෘති වෙබ් අඩවිය](https://fadeproject.org/?page\_id=36) පරීක්ෂා කළ හැක. එසේම, ඔබේ විරුද්ධවාදියා වෙනත් දේවල් අතර මෙවැනි උපාංගයකට ප්‍රවේශය ඔප්පු කර ඇත්දැයි ඔබෙන්ම අසාගත හැකිය.

>

> මෙම අවස්ථා සඳහා සාමාන්‍ය නිර්දේශයක් ලෙස, අවදානම් සහිත පුද්ගලයින්ට සම්ප්‍රදායික දුරකථන ඇමතුම් සහ SMS වෙනුවට අන්තර්ජාලය මත යැපෙන සංකේතනය කළ නාලිකා වෙත සන්නිවේදනය සංක්‍රමණය කිරීම යෝග්‍ය වේ. (යෙදුම් ඇතුළුව) සංවේදී අන්තර්ජාල ගමනාගමනය සඳහා VPN හෝ Tor භාවිතා කිරීම හා සමානයි. විශාල නොවිසඳුනු අංගය වනුයේ දුරකථන ජාලයට සම්බන්ධව සිටින විට නොවැළැක්විය හැකි පරිශීලක ස්ථානය නිරීක්ෂණය කිරීමයි.

>

> වාහකයන් හරහා දැවැන්ත දත්ත එකතු කිරීම සම්බන්ධයෙන්, සමහර අධිකරණ බල ප්‍රදේශවල පරිශීලකයින්ට ඔවුන් පිළිබඳ අතීතයේ කුමන දත්ත බෙදා ගත්තේ දැයි ඉල්ලා සිටිය හැක. මෙය ඔබට අදාළ වන්නේ නම් සහ එම තොරතුරු විභව නිරීක්ෂණ හඳුනා ගැනීමට විශ්වාසදායක වේ දැයි ඔබට පර්යේෂණ කළ හැක. මෙයට සාමාන්‍යයෙන් නීතිමය පරීක්ෂණයක් ඇතුළත් වන බව මතක තබා ගන්න.

ඔබට වෙනත් විභව තර්ජන පරීක්ෂා කිරීමට අවශ්‍ය නම් හෝ වඩාත් සංකීර්ණ නඩුවක් තිබේ නම් සහ උදවු සෙවීමට අවශ්‍ය නම්, ඊළඟ ක්ලික් කරන්න.

- [ඊළඟ](#පෙර-වසා දැමීම)

### peer-compromised-intro

> ඔබට සම්බන්ධ කිසියම් පුද්ගලයෙකු හෝ සංවිධානයක් ඔත්තු බැලීමේ ගොදුරක් වී ඇත්නම්, ඔවුන් මත භාවිතා කරන ලද ශිල්පීය ක්‍රම තේරුම් ගැනීමට උත්සාහ කරන ලෙස අපි ඔබට නිර්දේශ කරමු, සහ පෙර ලැයිස්තුවේ සමීපතම ඒවා තෝරන්න, එවිට ඔබට වඩාත් අදාළ සන්දර්භය ලබා ගත හැකිය. ඔබත් සමාන තාක්ෂණික ක්‍රමවලට ගොදුරු විය හැකිද යන්න තීරණය කරන්න.

ඔබ කුමක් කිරීමට කැමතිද?

- [මාව පෙර පියවරට ගෙන යන්න](#ආරම්භය)

- [මට විශ්වාස නැත](#පූර්‍ව වසා දැමීම)

### වෙනත් හැඳින්වීමක්

> ඔබ කලින් දුටු ලැයිස්තුවේ සිවිල් අවකාශයේ සහායකයින් විසින් දුටු වඩාත් සුලභ සිද්ධීන් ඇතුළත් කර ඇත, නමුත් ඔබේ තත්වය එහි ආවරණය නොකළ හැකිය. එය ඔබගේ කාරණය නම්, "මට උදව් අවශ්‍යයි" ක්ලික් කරන්න; එසේ නොමැතිනම්, ඔබට වඩාත් පොදු සිද්ධි ලැයිස්තුව වෙත ආපසු ගොස් වඩාත් නිශ්චිත මග පෙන්වීමක් ලබා ගැනීම සඳහා ඔබට අදාළ වන ආසන්නතම අවස්ථාව තෝරාගත හැක.

ඔබ කුමක් කිරීමට කැමතිද?

- [විභව තර්ජන ලැයිස්තුවට මාව රැගෙන යන්න](#ආරම්භය)

- [මට උදවු අවශ්‍යයි](#උදව්\_අවසන්)

### පූර්ව වසා දැමීම

> මෙම කාර්ය ප්‍රවාහය මෙතෙක් ප්‍රයෝජනවත් වී ඇතැයි අපි බලාපොරොත්තු වෙමු. ඔබ සැලකිලිමත් විය හැකි වෙනත් තර්ජන පරීක්ෂා කිරීමට ඔබට මුල් අවස්ථා ලැයිස්තුව වෙත ආපසු යාමට තෝරා ගත හැකිය, නැතහොත් වඩාත් සංකීර්ණ අවස්ථා සඳහා ඔබට උපකාර කිරීමට ඔබ සම්බන්ධ කර ගත හැකි සංවිධාන ලැයිස්තුවට යන්න.

ඔබ කුමක් කිරීමට කැමතිද?

- [වෙනත් නිරීක්ෂණ ක්‍රම ගැන ඉගෙන ගැනීමට මම කැමතියි](#ආරම්භය)

- [මම හිතන්නේ මගේ අවශ්‍යතාවය මෙම කොටසේ ආවරණය කර නැත හෝ එය ඉතා සංකීර්ණයි](#උදව්\_අවසන්)

- [මට සිදුවන්නේ කුමක්ද යන්න පිළිබඳව මට පැහැදිලි අදහසක් ඇතැයි මම සිතමි](# විසඳා\_අවසානය)

### උදව්\_අවසන්

> ඔත්තු බැලීමේ සිද්ධීන් සම්බන්ධයෙන් ඔබට අමතර උපකාර අවශ්‍ය නම්, ඔබට පහත ලැයිස්තුගත කර ඇති සංවිධාන වෙත සම්බන්ධ විය හැක.

>

> \*සටහන: උපකාරය සඳහා ඔබ කිසියම් ආයතනයක් සම්බන්ධ කර ගන්නා විට, කරුණාකර ඔබ මෙහි අනුගමනය කළ මාර්ගය සහ ඕනෑම ඊළඟ පියවර පහසු කිරීමට ඔබ සොයාගත් ඕනෑම දර්ශකයක් බෙදා ගන්න.\*

:[](සංවිධාන?services=legal&services=vulnerabilities\_malware&services=forensic)

### නෛතික\_අවසානය

> ඔබට නීතිවිරෝධී ලෙස ඔත්තු බැලීම සම්බන්ධයෙන් යමෙකුට නඩු පැවරීමට ඔබට සහාය අවශ්‍ය නම්, ඔබට පහත සංවිධානවලින් එකකට සම්බන්ධ විය හැක.

:[](සංවිධාන?services=නීත්‍යානුකූල)

### විසඳන ලද\_අවසානය

මෙම දෝශ නිරාකරණ මාර්ගෝපදේශය ප්‍රයෝජනවත් වේ යැයි බලාපොරොත්තු වෙමු. කරුණාකර ප්‍රතිපෝෂණ ලබා දෙන්න [ඊමේල් හරහා](mailto:incoming+rarenet-dfak-8220223-issue-@incoming.gitlab.com)

### අවසාන\_ඉඟි

- දුරකථන ඇමතුම් සහ කෙටි පණිවුඩ වැනි අනාරක්ෂිත නාලිකාවලින් ඕනෑම සන්නිවේදනයක් අන්තර්ජාලය මත රඳා පවතින සංකේතාත්මක සන්නිවේදන නාලිකා වෙත සංක්‍රමණය කරන්න, එනම් අන්තයේ සිට අගට සංකේතනය කළ මැසෙන්ජර් යෙදුම් සහ HTTPS හරහා ආරක්ෂිත වෙබ් අඩවි වැනි.

- ඔබේ අන්තර්ජාල ගමනාගමනය නිරීක්ෂණය කෙරේ යැයි ඔබ බිය වන්නේ නම් සහ මෙය ආරක්ෂක අවදානමක් විය හැකි යැයි ඔබ විශ්වාස කරන්නේ නම්, VPN හෝ Tor වැනි සංකේතාංකන මෙවලමක් හරහා අන්තර්ජාලයට සම්බන්ධ වීම ගැන සලකා බලන්න.

- ඔබගේ අවකාශයේ ඇති සියලුම උපාංග, විශේෂයෙන්ම අන්තර්ජාලයට සම්බන්ධ කර ඇති උපාංග පිළිබඳව සටහන් තබාගෙන ඒවා කරන්නේ කුමක්දැයි දැන ගැනීමට උත්සාහ කරන්න.

- විරුද්ධවාදියෙකු විසින් පාලනය කරනු ලබන සේවා හරහා සංවේදී තොරතුරු බෙදාගැනීමෙන් වළකින්න.

- ඔබට හැකිතාක් ඔබගේ ගිණුම් හෝ උපාංග බෙදාගැනීම අවම කරන්න.

- සැක සහිත පණිවිඩ, වෙබ් අඩවි, බාගැනීම් සහ යෙදුම් ගැන දැනුවත් වන්න.

මූලාශ්‍ර

- [Apple’s Android App to Scan for AirTags is a Necessary Step Forward, But More Anti-Stalking Mitigations Are Needed](https://www.eff.org/es/deeplinks/2021/12/apples-android-app-scan-airtags-necessary-step-forward-more-anti-stalking).

- [Privacy for Students](https://ssd.eff.org/module/privacy-students): With references of surveillance techniques in schools that can apply to many other scenarios.

- [Security in a Box: Protect the privacy of your online communication](https://securityinabox.org/en/communication/private-communication/)

- [Security in a Box: Visit blocked websites and browse anonymously](https://securityinabox.org/en/internet-connection/anonymity-and-circumvention/)

- [Security in a Box: Recommendations for encrypted chat tools](https://securityinabox.org/en/communication/tools/#more-secure-text-voice-and-video-chat-applications)