---

layout: page

title: " මගේ උපාංගය සැක සහිත ලෙස ක්‍රියා කරයි "

author: Donncha Ó Cearbhaill, Claudio Guarnieri, RaReNet

language: en

summary: " ඔබගේ පරිගණකය හෝ දුරකථනය සැක සහිත ලෙස ක්‍රියා කරන්නේ නම්, ඔබගේ උපාංගයේ අනවශ්‍ය හෝ අනිෂ්ට මෘදුකාංග තිබිය හැක."

date: 2023-04

permalink: /en/topics/device-acting-suspiciously

parent: Home

---

# මගේ උපාංගය සැක සහිත ලෙස ක්‍රියා කරයි

අනිෂ්ට මෘදුකාංග ප්‍රහාර වසර ගණනාවක් තිස්සේ පරිණාමය වී ඉතා සංකීර්ණ වී ඇත. මෙම ප්‍රහාරයන් විවිධ තර්ජන ඇති කරන අතර ඔබගේ පුද්ගලික සහ ආයතනික යටිතල පහසුකම් සහ දත්ත වලට බරපතල බලපෑම් ඇති කළ හැක.

අනිෂ්ට මෘදුකාංග ප්‍රහාර වෛරස්, තතුබෑම්, කප්පම් මෘදුකාංග, ට්‍රෝජන් සහ රූට්කිට් වැනි විවිධ ආකාරවලින් පැමිණේ. සමහර තර්ජන නම්: පරිගණක බිඳවැටීම, දත්ත සොරකම් කිරීම (එනම්: සංවේදී ගිණුම් අක්තපත්‍ර, මූල්‍ය තොරතුරු, බැංකු ගිණුම් ඇතුළුවීම්), ප්‍රහාරකයෙක් ඔබේ උපාංගය පාලනය කර ගැනීමෙන් හෝ ඔබේ උපාංගයේ පාලනය ගෙන එය භාවිත කිරීමෙන් කප්පම් මුදලක් ගෙවීමට ඔබට බ්ලැක්මේල් කරයි. ඔබ මාර්ගගතව කරන සෑම දෙයක් ගැනම ඔත්තු බැලීමට හෝ DDoS ප්‍රහාර දියත් කිරීමට.

ප්‍රහාරකයන් විසින් ඔබව සහ ඔබේ උපාංග සම්මුතියට පත් කිරීම සඳහා පොදුවේ භාවිතා කරන සමහර ක්‍රම සාමාන්‍ය ක්‍රියාකාරකම් ලෙස පෙනේ, එනම්:

- ඇමුණුමක් විවෘත කිරීමට හෝ සබැඳියක් ක්ලික් කිරීමට ඔබව පොළඹවන විද්‍යුත් තැපෑලක් හෝ සමාජ මාධ්‍යවල පළ කිරීමක්.

- විශ්වාස නොකළ මූලාශ්‍රයකින් මෘදුකාංග බාගත කර ස්ථාපනය කිරීමට මිනිසුන් යොමු කිරීම.

- නීත්‍යනුකූල ලෙස පෙනෙන නමුත් එසේ නොවන වෙබ් අඩවියකට තම පරිශීලක නාමය සහ මුරපදය ඇතුළත් කිරීමට යමෙකු යොමු කිරීම.

- ඔබ එය අවධානයෙන් තොරව සහ අගුළු හැර තබන විට ඔබේ උපාංගයේ වාණිජ ඔත්තු මෘදුකාංග යෙදුමක් ස්ථාපනය කිරීම.

ඩිජිටල් ප්‍රථමාධාර කට්ටලයේ මෙම කොටස ඔබගේ උපාංගය ආසාදනය වී ඇත්ද නැද්ද යන්න සොයා ගැනීමට මූලික පියවර කිහිපයක් හරහා ඔබව ගෙන යනු ඇත.

ඔබේ පරිගණකය හෝ ජංගම උපාංගය සැක සහිත ලෙස ක්‍රියා කිරීමට පටන් ගෙන ඇති බව ඔබ සිතන්නේ නම්, ඔබ මුලින්ම සිතිය යුත්තේ රෝග ලක්ෂණ මොනවාද යන්නයි.

සැක සහිත උපාංග ක්‍රියාකාරකම් ලෙස සාමාන්‍යයෙන් කියවිය හැකි රෝග ලක්ෂණ, නමුත් බොහෝ විට කනස්සල්ලට පත්වීමට ප්‍රමාණවත් හේතුවක් නොවේ:

- දුරකථන ඇමතුම් අතරතුර ශබ්ද ක්ලික් කිරීම

- අනපේක්ෂිත බැටරි කාන්දු වීම

- උපාංගය භාවිතයේ නොමැති විට අධික උනුසුම් වීම

- සෙමින් ක්‍රියාත්මක වන උපාංගයක්

මෙම රෝග ලක්ෂණ බොහෝ විට කනස්සල්ලට පත්වන උපාංග ක්රියාකාරිත්වයේ විශ්වසනීය දර්ශක ලෙස වැරදි ලෙස සලකනු ලැබේ. කෙසේ වෙතත්, ඒවායින් කිසිවක් තනිවම ගැනීම සැලකිලිමත් වීමට ප්රමාණවත් හේතුවක් නොවේ.

සම්මුතියට ලක් වූ උපාංගයක විශ්වාසදායක රෝග ලක්ෂණ සාමාන්‍යයෙන්:

- උපාංගය බොහෝ විට තනිවම නැවත ආරම්භ වේ

- විශේෂයෙන් ආදාන ක්‍රියාවෙන් පසු යෙදුම් බිඳ වැටේ

- මෙහෙයුම් පද්ධති යාවත්කාලීන කිරීම් සහ/හෝ ආරක්ෂක පැච් නැවත නැවතත් අසාර්ථක වේ

- වෙබ් කැමරාව භාවිතයේ නොමැති අතරේ වෙබ් කැමරා ක්‍රියාකාරකම් දර්ශක ආලෝකය ක්‍රියාත්මකයි

- නැවත නැවතත් ["මරණයේ නිල් තිර"](https://en.wikipedia.org/wiki/Blue\_Screen\_of\_Death) හෝ කර්නල් භීතිය

- දිලිසෙන කවුළු

- ප්රතිවයිරස අනතුරු ඇඟවීම්

## වැඩ ප්‍රවාහය

### ආරම්භය

හැඳින්වීමෙහි සපයා ඇති තොරතුරු අනුව, ඔබේ උපාංගය අවදානමට ලක්ව ඇති බව ඔබට තවමත් හැඟේ නම්, පහත මාර්ගෝපදේශය ඔබට ගැටලුව හඳුනා ගැනීමට උපකාරී වනු ඇත.

- [මගේ ජංගම උපාංගය සැක සහිත ලෙස ක්‍රියා කරන බව මම විශ්වාස කරමි](#දුරකථන හඳුන්වාදීම)

- [මගේ පරිගණකය සැක සහිත ලෙස ක්‍රියා කරන බව මම විශ්වාස කරමි](#පරිගණක හඳුන්වාදීම)

- [මගේ උපාංගය අවදානමට ලක්විය හැකි බව මට තවදුරටත් දැනෙන්නේ නැත](#උපාංගය-පිරිසිදු)

### උපාංගය පිරිසිදු කරන්න

> නියමයි! කෙසේ වෙතත්, මෙම උපදෙස් ඔබට ඉක්මන් විශ්ලේෂණයක් කිරීමට පමණක් උපකාරී වන බව මතක තබා ගන්න. දෘශ්‍ය විෂමතා හඳුනා ගැනීමට එය ප්‍රමාණවත් විය යුතු අතර, වඩාත් සංකීර්ණ ඔත්තු මෘදුකාංග වඩාත් ඵලදායී ලෙස සැඟවීමට හැකියාව ඇත.

උපාංගය අවදානමට ලක්විය හැකි බවට ඔබ තවමත් සැක කරන්නේ නම්, ඔබට අවශ්‍ය විය හැකිය:

- [අමතර උදවු සොයන්න](#අනිෂ්ට මෘදුකාංග\_අවසන්)

- [උපාංගයේ යළි පිහිටුවීමකට කෙලින්ම ඉදිරියට යන්න](#නැවත පිහිටුවීම)

### දුරකථන හඳුන්වාදීම

> ඔබගේ උපාංගය අවදානමට ලක්ව ඇති ආකාරය සලකා බැලීම වැදගත් වේ.

>

> - ඔබගේ උපාංගය සැක සහිත ලෙස ක්‍රියා කරන බවට ඔබ කොපමණ කලකට පෙර සැක කිරීමට පටන් ගත්තේද?

> - නොදන්නා මූලාශ්‍රවලින් කිසියම් සබැඳියක් ක්ලික් කළ බව ඔබට මතකද?

> - ඔබ හඳුනා නොගත් පාර්ශ්වවලින් ඔබට පණිවිඩ ලැබී තිබේද?

> - ඔබ විශ්වාස නොකළ මූලාශ්‍රවලින් බාගත කළ කිසියම් මෘදුකාංගයක් ස්ථාපනය කර තිබේද?

> - උපාංගය ඔබ සන්තකයේ නැති වී තිබේද?

ඔබගේ උපාංගය අවදානමට ලක් වීමට හේතු වූ තත්වයන් තිබේ නම් ඒවා හඳුනා ගැනීමට උත්සාහ කිරීමට මෙම ප්‍රශ්න ගැන මෙනෙහි කරන්න.

- [මට Android උපාංගයක් ඇත](#android-intro)

- [මට iOS උපාංගයක් ඇත](#ios-intro)

### android-intro

> ඔබගේ ඇන්ඩ්‍රොයිඩ් උපාංගයේ නුපුරුදු යෙදුම් ස්ථාපනය කර ඇත්දැයි පළමුව පරීක්ෂා කරන්න.

>

> ඔබට සැකසුම් මෙනුවේ "යෙදුම්" කොටසේ යෙදුම් ලැයිස්තුවක් සොයාගත හැකිය. ඔබගේ උපාංගය සමඟ පෙර ස්ථාපනය කර නැති සහ ඔබට බාගත කිරීම මතක නැති යෙදුම් හඳුනා ගන්න.

>

> ඔබ ලැයිස්තුවේ ඇති යෙදුම් කිසිවක් සැක කරන්නේ නම්, වෙබ් සෙවුමක් ධාවනය කර යෙදුම අනිෂ්ට ලෙස හඳුනා ගන්නා විශ්වාසදායක වාර්තා තිබේදැයි බැලීමට සම්පත් සොයන්න.

ඔබ කිසියම් සැක කටයුතු යෙදුම් සොයා ගත්තාද?

- [නැහැ, මම එසේ නොකළෙමි](#android-අනාරක්ෂිත-සැකසීම්)

- [ඔව්, මම අනිෂ්ට යෙදුම් හඳුනාගෙන ඇත](#android-badend)

### android-අනාරක්ෂිත-සැකසීම්

> Android පරිශීලකයින්ට ඔවුන්ගේ උපාංගයට පහළ මට්ටමේ ප්‍රවේශය සක්‍රීය කිරීමේ විකල්පය ලබා දෙයි. මෙය මෘදුකාංග සංවර්ධකයින් සඳහා ප්‍රයෝජනවත් විය හැකි නමුත්, අමතර ප්‍රහාරවලට උපාංග නිරාවරණය කිරීමටද මෙය හැකිය. ඔබ මෙම ආරක්ෂක සැකසුම් සමාලෝචනය කර ඒවා ආරක්ෂිත විකල්ප වෙත සකසා ඇති බව සහතික කර ගත යුතුය. නිෂ්පාදකයන්ට අනාරක්ෂිත පෙරනිමි සහිත උපාංග නැව්ගත කළ හැක. ඔබ විසින්ම වෙනස්කම් සිදු කර නොමැති වුවද මෙම සැකසීම් සමාලෝචනය කළ යුතුය.

>

> #### විශ්වාස නොකළ මූලාශ්‍රවලින් අයදුම්පත්

>

> Android සාමාන්‍යයෙන් Google Play Store වෙතින් පූරණය නොවන යෙදුම් ස්ථාපනය අවහිර කරයි. Play Store හි අනිෂ්ට යෙදුම් සමාලෝචනය කිරීමට සහ හඳුනා ගැනීමට Google හට ක්‍රියාවලි ඇත. ප්‍රහාරකයින් බොහෝ විට ස්ථාපන ගොනුවක් අඩංගු හෝ ඊට සම්බන්ධ පණිවිඩයක් හරහා අනිෂ්ට යෙදුම් සෘජුවම පරිශීලකයාට ලබා දීමෙන් මෙම චෙක්පත් වළක්වා ගැනීමට උත්සාහ කරයි. ඔබගේ උපාංගය විශ්වාස නොකළ මූලාශ්‍රවලින් යෙදුම් ස්ථාපනය කිරීමට ඉඩ නොදෙන බව සහතික කිරීම වැදගත් වේ.

>

> නොදන්නා මූලාශ්‍රවලින් යෙදුම් ස්ථාපනය කිරීම ඔබගේ උපාංගයේ අක්‍රිය කර ඇති බවට වග බලා ගන්න. බොහෝ ඇන්ඩ්‍රොයිඩ් අනුවාදවල ඔබට මෙම විකල්පය ආරක්‍ෂක සැකසුම් තුළ සොයාගත හැකි නමුත්, ඔබ ධාවනය කරන ඇන්ඩ්‍රොයිඩ් රසය අනුව එය වෙනත් තැනක විය හැකි අතර නව දුරකථනවල මෙම විකල්පය එක් එක් යෙදුම සඳහා අවසර සැකසීම් තුළ තිබිය හැකිය.

>

> #### සංවර්ධක මාදිලිය

>

> "සංවර්ධක ප්‍රකාරය" තුළ සිටින විට යටින් පවතින මෙහෙයුම් පද්ධතිය මත සෘජුවම විධාන ක්‍රියාත්මක කිරීමට සංවර්ධකයින්ට ඇන්ඩ්‍රොයිඩ් ඉඩ දෙයි. සබල කළ විට, මෙය උපාංග භෞතික ප්‍රහාරවලට නිරාවරණය කරයි. උපාංගයට භෞතික ප්‍රවේශය ඇති කෙනෙකුට උපාංගයෙන් පුද්ගලික දත්තවල පිටපත් බාගැනීමට හෝ අනිෂ්ට යෙදුම් ස්ථාපනය කිරීමට සංවර්ධක මාදිලිය භාවිත කළ හැක.

>

> ඔබ ඔබේ උපාංග සැකසීම් තුළ සංවර්ධක මාදිලියේ මෙනුවක් දුටුවහොත් එය අබල කර ඇති බව ඔබ සහතික විය යුතුය.

>

> #### Google Play Protect

>

> Google Play Protect සේවාව සියලුම මෑත ඇන්ඩ්රොයිඩ් උපාංගවල පවතී. එය ඔබගේ උපාංගයේ ස්ථාපනය කර ඇති සියලුම යෙදුම්වල නිතිපතා ස්කෑන් කිරීම සිදු කරයි. Play Protect හට ඔබගේ උපාංගයෙන් දන්නා ඕනෑම අනිෂ්ට යෙදුම් ස්වයංක්‍රීයව ඉවත් කළ හැක. මෙම සේවාව සබල කිරීමෙන් ඔබගේ උපාංගය (ස්ථාපිත යෙදුම් වැනි) පිළිබඳ තොරතුරු Google වෙත යවයි.

>

> Google Play Protect ඔබගේ උපාංග ආරක්ෂණ සැකසීම් යටතේ සබල කළ හැක. වැඩිදුර තොරතුරු [Play Protect](https://www.android.com/play-protect/) අඩවියෙන් ලබා ගත හැක.

ඔබ කිසියම් අනාරක්ෂිත සැකසුම් හඳුනා ගත්තාද?

- [නැහැ, මම කළේ නැහැ](#android-bootloader)

- [ඔව්, මම අනාරක්ෂිත විය හැකි සැකසුම් හඳුනා ගත්තෙමි](#android-badend)

### android-bootloader

> Android bootloader යනු ඔබ ඔබගේ උපාංගය ක්‍රියාත්මක කළ වහාම ක්‍රියාත්මක වන ප්‍රධාන මෘදුකාංගයකි. ඇරඹුම් කාරකය මඟින් මෙහෙයුම් පද්ධතියට දෘඩාංග ආරම්භ කිරීමට සහ භාවිතා කිරීමට හැකියාව ලැබේ. සම්මුතියට පත් ඇරඹුම් කාරකයක් ප්‍රහාරකයෙකුට උපාංග දෘඪාංග වෙත පූර්ණ ප්‍රවේශය ලබා දෙයි. නිෂ්පාදකයින්ගෙන් බහුතරයක් ඔවුන්ගේ උපාංග අගුලු දැමූ ඇරඹුම් කාරකයක් සමඟ යවයි. නිෂ්පාදකයාගේ අත්සන් කරන ලද ඇරඹුම් කාරකය වෙනස් කර ඇත්දැයි හඳුනා ගැනීමට පොදු ක්‍රමයක් වන්නේ ඔබේ උපාංගය නැවත ආරම්භ කර ඇරඹුම් ලාංඡනය සෙවීමයි. විස්මයාර්ථ ලකුණක් සහිත කහ ත්‍රිකෝණයක් දිස්වන්නේ නම්, මුල් ඇරඹුම් කාරකය ප්‍රතිස්ථාපනය කර ඇත. ඔබගේ උපාංගය අගුලු හරින ලද ඇරඹුම් කාරක අනතුරු ඇඟවීමේ තිරයක් පෙන්වයි නම් සහ LineageOS හෝ GrapheneOS වැනි අභිරුචි Android ROM එකක් ස්ථාපනය කිරීමට ඔබ විසින්ම එය අගුළු හැර නොමැති නම් එය අවදානමට ලක් විය හැක. ඔබ බලාපොරොත්තු නොවන අගුළු හරින ලද ඇරඹුම් කාරක අනතුරු ඇඟවීමේ තිරයක් පෙන්නුම් කරන්නේ නම්, ඔබ ඔබේ උපාංගයේ කර්මාන්තශාලා යළි පිහිටුවීමක් සිදු කළ යුතුය.

ඇරඹුම් කාරකය අවදානමට ලක් වී තිබේද නැතහොත් ඔබේ උපාංගය මුල් ඇරඹුම් කාරකය භාවිතා කරන්නේද?

- [මගේ උපාංගයේ ඇරඹුම් කාරකය අවදානමට ලක්ව ඇත](#android-badend)

- [මගේ උපාංගය මුල් ඇරඹුම් කාරකය භාවිතා කරයි](#android-goodend)

### android-goodend

> ඔබගේ උපාංගය අවදානමට ලක්ව ඇති බවක් නොපෙනේ.

ඔබගේ උපාංගය අවදානමට ලක්ව ඇතැයි ඔබ තවමත් කනස්සල්ලෙන්ද?

- [ඔව්, මම වෘත්තීය සහාය ලබා ගැනීමට කැමතියි](#අනිෂ්ට මෘදුකාංග\_අවසන්)

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

### android-badend

> ඔබගේ උපාංගය අවදානමට ලක් විය හැක. කර්මාන්තශාලා සැකසීම් වෙත යළි පිහිටුවීම ඔබගේ උපාංගයේ පවතින ඕනෑම තර්ජනයක් ඉවත් කරනු ඇත. කෙසේ වෙතත්, එය සෑම විටම හොඳම විසඳුම නොවේ. ඊට අමතරව, ඔබේ නිරාවරණයේ මට්ටම සහ ඔබ විඳදරාගත් ප්‍රහාරයේ නිශ්චිත ස්වභාවය හඳුනා ගැනීම සඳහා ඔබට මෙම කාරණය තවදුරටත් විමර්ශනය කිරීමට අවශ්‍ය විය හැකිය.

>

> ඔබට ස්වයං-රෝග විනිශ්චය සඳහා [හදිසි VPN](https://www.civilsphereproject.org/emergency-vpn) හෝ [PiRogue](https://pts-project.org/), හෝ භාවිතා කිරීමට අවශ්‍ය විය හැක. උදව් කළ හැකි සංවිධානයකින් සහය පතන්න.

ඔබ කුමක් කිරීමට කැමතිද?

- [මම මගේ උපාංගය කර්මාන්තශාලා සැකසීම් වෙත යළි පිහිටුවීමට කැමතියි](#reset).

- [මම වෘත්තීය සහාය ලබා ගැනීමට කැමතියි](#අනිෂ්ට මෘදුකාංග\_අවසන්)

- [මට වෘත්තීය උපකාර සඳහා සම්බන්ධ විය හැකි දේශීය ආධාරක ජාලයක් ඇත](#resolved\_end)

### ios-intro

> [ඔබගේ iPhone හෝ iPad වෙත ප්‍රවේශය ඇත්තේ කාටදැයි බැලීමට] (https://support.apple.com/en-gb/guide/personal-safety/ipsb8deced49/web) එම පියවර අනුගමනය කරන්න. අසාමාන්‍ය දෙයක් තිබේදැයි බැලීමට iOS සැකසුම් පරීක්ෂා කරන්න.

>

> සැකසීම් යෙදුම තුළ, ඔබගේ උපාංගය ඔබගේ Apple ID එකට බැඳී ඇති බව පරීක්ෂා කරන්න. වම් පස ඇති පළමු මෙනු අයිතමය ඔබේ නම හෝ ඔබේ Apple ID සඳහා භාවිතා කරන නම විය යුතුය. එය මත ක්ලික් කර නිවැරදි විද්‍යුත් තැපැල් ලිපිනය පෙන්වා ඇත්දැයි පරීක්ෂා කරන්න. මෙම පිටුවේ පතුලේ මෙම Apple ID එකට බැඳ ඇති සියලුම iOS උපාංගවල නම් සහ මාදිලි සහිත ලැයිස්තුවක් ඔබට පෙනෙනු ඇත.

>

> ඔබගේ උපාංගය ඔබ හඳුනා නොගත් ජංගම උපාංග කළමනාකරණ (MDM) පද්ධතියකට බැඳී නොමැති බව පරීක්ෂා කරන්න. සැකසීම් > සාමාන්‍ය > VPN සහ උපාංග කළමනාකරණය වෙත ගොස් ඔබට පැතිකඩ සඳහා කොටසක් තිබේදැයි පරීක්ෂා කරන්න. ඔබට [ඕනෑම නොදන්නා වින්‍යාස පැතිකඩක් මකා දැමිය හැක](https://support.apple.com/en-gb/guide/personal-safety/ips41ef0e8c3/1.0/web/1.0#ips68379dd2e). ඔබට ලැයිස්තුගත කර ඇති පැතිකඩ නොමැති නම්, ඔබ MDM හි ලියාපදිංචි වී නොමැත.

- [සියලු තොරතුරු නිවැරදි වන අතර මම තවමත් මගේ Apple ID පාලනය කරමි](#ios-goodend)

- [නම හෝ වෙනත් විස්තර වැරදියි, නැතහොත් ලැයිස්තුවේ මගේ නොවන උපාංග හෝ පැතිකඩ මා දකිමි](#ios-badend)

### ios-goodend

> ඔබගේ උපාංගය අවදානමකට ලක්ව ඇති බවක් නොපෙනේ.

ඔබගේ උපාංගය අවදානමට ලක්ව ඇතැයි ඔබ තවමත් කනස්සල්ලෙන්ද?

- [ඔව්, මම වෘත්තීය සහාය ලබා ගැනීමට කැමතියි](#අනිෂ්ට මෘදුකාංග\_අවසන්)

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

### ios-badend

> ඔබගේ උපාංගය අවදානමට ලක් විය හැක. කර්මාන්තශාලා සැකසීම් වෙත යළි පිහිටුවීම ඔබගේ උපාංගයේ පවතින ඕනෑම තර්ජනයක් ඉවත් කරනු ඇත. කෙසේ වෙතත්, එය සෑම විටම හොඳම විසඳුම නොවේ. ඊට අමතරව, ඔබේ නිරාවරණයේ මට්ටම සහ ඔබ විඳදරාගත් ප්‍රහාරයේ නිශ්චිත ස්වභාවය හඳුනා ගැනීම සඳහා ඔබට මෙම කාරණය තවදුරටත් විමර්ශනය කිරීමට අවශ්‍ය විය හැකිය.

>

> ඔබට ස්වයං-රෝග විනිශ්චය සඳහා [හදිසි VPN](https://www.civilsphereproject.org/emergency-vpn) හෝ [PiRogue](https://pts-project.org/), හෝ භාවිතා කිරීමට අවශ්‍ය විය හැක. උදව් කළ හැකි සංවිධානයකින් සහය පතන්න.

ඔබ කුමක් කිරීමට කැමතිද?

- [මම මගේ උපාංගය කර්මාන්තශාලා සැකසීම් වෙත යළි පිහිටුවීමට කැමතියි](#reset).

- [මම වෘත්තීය සහාය ලබා ගැනීමට කැමතියි](#අනිෂ්ට මෘදුකාංග\_අවසන්

>

> #### Google Play Protect

>

> Google Play Protect සේවාව සියලුම මෑත ඇන්ඩ්රොයිඩ් උපාංගවල පවතී. එය ඔබගේ උපාංගයේ ස්ථාපනය කර ඇති සියලුම යෙදුම්වල නිතිපතා ස්කෑන් කිරීම සිදු කරයි. Play Protect හට ඔබගේ උපාංගයෙන් දන්නා ඕනෑම අනිෂ්ට යෙදුම් ස්වයංක්‍රීයව ඉවත් කළ හැක. මෙම සේවාව සබල කිරීමෙන් ඔබගේ උපාංගය (ස්ථාපිත යෙදුම් වැනි) පිළිබඳ තොරතුරු Google වෙත යවයි.

>

> Google Play Protect ඔබගේ උපාංග ආරක්ෂණ සැකසීම් යටතේ සබල කළ හැක. වැඩිදුර තොරතුරු [Play Protect](https://www.android.com/play-protect/) අඩවියෙන් ලබා ගත හැක.

ඔබ කිසියම් අනාරක්ෂිත සැකසුම් හඳුනා ගත්තාද?

- [නැහැ, මම කළේ නැහැ](#android-bootloader)

- [ඔව්, මම අනාරක්ෂිත විය හැකි සැකසුම් හඳුනා ගත්තෙමි](#android-badend)

### android-bootloader

> Android bootloader යනු ඔබ ඔබගේ උපාංගය ක්‍රියාත්මක කළ වහාම ක්‍රියාත්මක වන ප්‍රධාන මෘදුකාංගයකි. ඇරඹුම් කාරකය මඟින් මෙහෙයුම් පද්ධතියට දෘඩාංග ආරම්භ කිරීමට සහ භාවිතා කිරීමට හැකියාව ලැබේ. සම්මුතියට පත් ඇරඹුම් කාරකයක් ප්‍රහාරකයෙකුට උපාංග දෘඪාංග වෙත පූර්ණ ප්‍රවේශය ලබා දෙයි. නිෂ්පාදකයින්ගෙන් බහුතරයක් ඔවුන්ගේ උපාංග අගුලු දැමූ ඇරඹුම් කාරකයක් සමඟ යවයි. නිෂ්පාදකයාගේ අත්සන් කරන ලද ඇරඹුම් කාරකය වෙනස් කර ඇත්දැයි හඳුනා ගැනීමට පොදු ක්‍රමයක් වන්නේ ඔබේ උපාංගය නැවත ආරම්භ කර ඇරඹුම් ලාංඡනය සෙවීමයි. විස්මයාර්ථ ලකුණක් සහිත කහ ත්‍රිකෝණයක් දිස්වන්නේ නම්, මුල් ඇරඹුම් කාරකය ප්‍රතිස්ථාපනය කර ඇත. ඔබගේ උපාංගය අගුලු හරින ලද ඇරඹුම් කාරක අනතුරු ඇඟවීමේ තිරයක් පෙන්වයි නම් සහ LineageOS හෝ GrapheneOS වැනි අභිරුචි Android ROM එකක් ස්ථාපනය කිරීමට ඔබ විසින්ම එය අගුළු හැර නොමැති නම් එය අවදානමට ලක් විය හැක. ඔබ බලාපොරොත්තු නොවන අගුළු හරින ලද ඇරඹුම් කාරක අනතුරු ඇඟවීමේ තිරයක් පෙන්නුම් කරන්නේ නම්, ඔබ ඔබේ උපාංගයේ කර්මාන්තශාලා යළි පිහිටුවීමක් සිදු කළ යුතුය.

ඇරඹුම් කාරකය අවදානමට ලක් වී තිබේද නැතහොත් ඔබේ උපාංගය මුල් ඇරඹුම් කාරකය භාවිතා කරන්නේද?

- [මගේ උපාංගයේ ඇරඹුම් කාරකය අවදානමට ලක්ව ඇත](#android-badend)

- [මගේ උපාංගය මුල් ඇරඹුම් කාරකය භාවිතා කරයි](#android-goodend)

### android-goodend

> ඔබගේ උපාංගය අවදානමට ලක්ව ඇති බවක් නොපෙනේ.

ඔබගේ උපාංගය අවදානමට ලක්ව ඇතැයි ඔබ තවමත් කනස්සල්ලෙන්ද?

- [ඔව්, මම වෘත්තීය සහාය ලබා ගැනීමට කැමතියි](#අනිෂ්ට මෘදුකාංග\_අවසන්)

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

### android-badend

> ඔබගේ උපාංගය අවදානමට ලක් විය හැක. කර්මාන්තශාලා සැකසීම් වෙත යළි පිහිටුවීම ඔබගේ උපාංගයේ පවතින ඕනෑම තර්ජනයක් ඉවත් කරනු ඇත. කෙසේ වෙතත්, එය සෑම විටම හොඳම විසඳුම නොවේ. ඊට අමතරව, ඔබේ නිරාවරණයේ මට්ටම සහ ඔබ විඳදරාගත් ප්‍රහාරයේ නිශ්චිත ස්වභාවය හඳුනා ගැනීම සඳහා ඔබට මෙම කාරණය තවදුරටත් විමර්ශනය කිරීමට අවශ්‍ය විය හැකිය.

>

> ඔබට ස්වයං-රෝග විනිශ්චය සඳහා [හදිසි VPN](https://www.civilsphereproject.org/emergency-vpn) හෝ [PiRogue](https://pts-project.org/), හෝ භාවිතා කිරීමට අවශ්‍ය විය හැක. උදව් කළ හැකි සංවිධානයකින් සහය පතන්න.

ඔබ කුමක් කිරීමට කැමතිද?

- [මම මගේ උපාංගය කර්මාන්තශාලා සැකසීම් වෙත යළි පිහිටුවීමට කැමතියි](#reset).

- [මම වෘත්තීය සහාය ලබා ගැනීමට කැමතියි](#අනිෂ්ට මෘදුකාංග\_අවසන්)

- [මට වෘත්තීය උපකාර සඳහා සම්බන්ධ විය හැකි දේශීය ආධාරක ජාලයක් ඇත](#resolved\_end)

### ios-intro

> [ඔබගේ iPhone හෝ iPad වෙත ප්‍රවේශය ඇත්තේ කාටදැයි බැලීමට] (https://support.apple.com/en-gb/guide/personal-safety/ipsb8deced49/web) එම පියවර අනුගමනය කරන්න. අසාමාන්‍ය දෙයක් තිබේදැයි බැලීමට iOS සැකසුම් පරීක්ෂා කරන්න.

>

> සැකසීම් යෙදුම තුළ, ඔබගේ උපාංගය ඔබගේ Apple ID එකට බැඳී ඇති බව පරීක්ෂා කරන්න. වම් පස ඇති පළමු මෙනු අයිතමය ඔබේ නම හෝ ඔබේ Apple ID සඳහා භාවිතා කරන නම විය යුතුය. එය මත ක්ලික් කර නිවැරදි විද්‍යුත් තැපැල් ලිපිනය පෙන්වා ඇත්දැයි පරීක්ෂා කරන්න. මෙම පිටුවේ පතුලේ මෙම Apple ID එකට බැඳ ඇති සියලුම iOS උපාංගවල නම් සහ මාදිලි සහිත ලැයිස්තුවක් ඔබට පෙනෙනු ඇත.

>

> ඔබගේ උපාංගය ඔබ හඳුනා නොගත් ජංගම උපාංග කළමනාකරණ (MDM) පද්ධතියකට බැඳී නොමැති බව පරීක්ෂා කරන්න. සැකසීම් > සාමාන්‍ය > VPN සහ උපාංග කළමනාකරණය වෙත ගොස් ඔබට පැතිකඩ සඳහා කොටසක් තිබේදැයි පරීක්ෂා කරන්න. ඔබට [ඕනෑම නොදන්නා වින්‍යාස පැතිකඩක් මකා දැමිය හැක](https://support.apple.com/en-gb/guide/personal-safety/ips41ef0e8c3/1.0/web/1.0#ips68379dd2e). ඔබට ලැයිස්තුගත කර ඇති පැතිකඩ නොමැති නම්, ඔබ MDM හි ලියාපදිංචි වී නොමැත.

- [සියලු තොරතුරු නිවැරදි වන අතර මම තවමත් මගේ Apple ID පාලනය කරමි](#ios-goodend)

- [නම හෝ වෙනත් විස්තර වැරදියි, නැතහොත් ලැයිස්තුවේ මගේ නොවන උපාංග හෝ පැතිකඩ මා දකිමි](#ios-badend)

### ios-goodend

> ඔබගේ උපාංගය අවදානමකට ලක්ව ඇති බවක් නොපෙනේ.

ඔබගේ උපාංගය අවදානමට ලක්ව ඇතැයි ඔබ තවමත් කනස්සල්ලෙන්ද?

- [ඔව්, මම වෘත්තීය සහාය ලබා ගැනීමට කැමතියි](#අනිෂ්ට මෘදුකාංග\_අවසන්)

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

### ios-badend

> ඔබගේ උපාංගය අවදානමට ලක් විය හැක. කර්මාන්තශාලා සැකසීම් වෙත යළි පිහිටුවීම ඔබගේ උපාංගයේ පවතින ඕනෑම තර්ජනයක් ඉවත් කරනු ඇත. කෙසේ වෙතත්, එය සෑම විටම හොඳම විසඳුම නොවේ. ඊට අමතරව, ඔබේ නිරාවරණයේ මට්ටම සහ ඔබ විඳදරාගත් ප්‍රහාරයේ නිශ්චිත ස්වභාවය හඳුනා ගැනීම සඳහා ඔබට මෙම කාරණය තවදුරටත් විමර්ශනය කිරීමට අවශ්‍ය විය හැකිය.

>

> ඔබට ස්වයං-රෝග විනිශ්චය සඳහා [හදිසි VPN](https://www.civilsphereproject.org/emergency-vpn) හෝ [PiRogue](https://pts-project.org/), හෝ භාවිතා කිරීමට අවශ්‍ය විය හැක. උදව් කළ හැකි සංවිධානයකින් සහය පතන්න.

ඔබ කුමක් කිරීමට කැමතිද?

- [මම මගේ උපාංගය කර්මාන්තශාලා සැකසීම් වෙත යළි පිහිටුවීමට කැමතියි](#reset).

- [මම වෘත්තීය සහාය ලබා ගැනීමට කැමතියි](#අනිෂ්ට මෘදුකාංග\_අවසන්

[AutoMacTC](https://www.crowdstrike.com/blog/automating-mac-forensic-triage/) ඇමරිකානු සයිබර් ආරක්ෂණ සමාගමක් වන CrowdStrike විසිනි.

මෙම උපදෙස් ඔබට කිසියම් ද්වේෂසහගත ක්‍රියාකාරකමක් හඳුනා ගැනීමට උදවු කළේද?

- [ඔව්, මා සිතන්නේ මාගේ පරිගණකයට හානියක් සිදුව ඇත.)

- [නැත, කිසිදු ද්වේෂ සහගත ක්‍රියාකාරකමක් හඳුනාගෙන නොමැත](#උපාංගය-පිරිසිදු)

### පරිගණකයට හානියක් සිදුව ඇත.

ඔබගේ උපාංගයට හානියක් වී ඇති බව පෙනේ. ඉන් මිදීමට ඔබට අවශ්‍යද?

- [අමතර උදවු සොයන්න](#අනිෂ්ට මෘදුකාංග\_අවසන්)

- [උපාංගයේ යළි පිහිටුවීමකට සෘජුවම ඉදිරියට යන්න](#reset).

### යළි පිහිටුවීම

> අමතර අනතුරු ඇඟවීමේ පියවරක් ලෙස ඔබේ උපාංගය යළි පිහිටුවීම සලකා බැලීමට ඔබට අවශ්‍ය විය හැකිය. පහත මාර්ගෝපදේශ ඔබගේ උපාංග වර්ගය සඳහා සුදුසු උපදෙස් ලබා දෙනු ඇත:

>

> - [Android](https://support.google.com/android/answer/6088915?hl=en)

> - [iOS](https://support.apple.com/en-us/HT201252)

> - [Windows](https://support.microsoft.com/en-us/windows/reinstall-windows-d8369486-3e33-7d9c-dccc-859e2b022fc7)

> - [Mac](https://support.apple.com/en-us/HT201314)

ඔබට අමතර උපකාර අවශ්‍ය යැයි ඔබට හැඟෙනවාද?

- [ඔව්](#අනිෂ්ට මෘදුකාංග\_අවසන්)

- [නැත](#විසඳුණු\_අවසානය)

### අනිෂ්ට මෘදුකාංග\_අවසානය

ආසාදිත උපාංගයක් සමඟ කටයුතු කිරීමට ඔබට අමතර උපකාර අවශ්‍ය නම්, ඔබට පහත ලැයිස්තුගත කර ඇති ආයතන වෙත සම්බන්ධ විය හැක.

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

### විසඳන ලද\_අවසානය

මෙම ඩිජිටල් ප්‍රථමාධාර කට්ටල කාර්ය ප්‍රවාහය ප්‍රයෝජනවත් වනු ඇතැයි අපි බලාපොරොත්තු වෙමු. කරුණාකර අපට ප්‍රතිපෝෂණ ලබා දෙන්න [ඊමේල් හරහා](mailto:incoming+rarenet-dfak-8220223-issue-@incoming.gitlab.com)

### අවසාන\_ඉඟි

ඔබේ උපාංග සහ දත්ත සම්මුතියකට පත් කිරීමට ප්‍රහාරකයෙකුගේ ප්‍රයත්නයන්ට ඔබ ගොදුරු වීමෙන් වළක්වා ගැනීමට උපදෙස් කිහිපයක් මෙන්න:

- ඔබට ලැබෙන ඕනෑම විද්‍යුත් තැපෑලක නීත්‍යානුකූල භාවය, ඔබ බාගත කර ඇති ගොනුවක් හෝ ඔබේ ගිණුමේ පිවිසුම් තොරතුරු ඉල්ලා සිටින සබැඳියක් සෑම විටම දෙවරක් පරීක්ෂා කරන්න.

- සම්පත් වල සම්බන්ධ කර ඇති මාර්ගෝපදේශවල අනිෂ්ට මෘදුකාංග ආසාදනවලින් ඔබේ උපාංගය ආරක්ෂා කරන්නේ කෙසේද යන්න පිළිබඳ වැඩිදුර කියවන්න.

මූලාශ්‍ර

- Security in a Box: [Protect your device from malware and phishing attacks](https://securityinabox.org/en/phones-and-computers/malware)

- Further tips for protecting [Android](https://securityinabox.org/en/phones-and-computers/android), [iOS](https://securityinabox.org/en/phones-and-computers/ios), [Windows](https://securityinabox.org/en/phones-and-computers/windows), [MacOS](https://securityinabox.org/en/phones-and-computers/mac), and [Linux](https://securityinabox.org/en/phones-and-computers/linux) devices

- [Security Self-Defense: How to avoid Phishing Attacks](https://ssd.eff.org/en/module/how-avoid-phishing-attacks)

- [Security without borders: Guide to Phishing](https://github.com/securitywithoutborders/guide-to-phishing/blob/master/SUMMARY.md)