---

layout: page

title: " මට මගේ උපාංගය නැති වුණා"

author: Hassen Selmi, Bahaa Nasr, Michael Carbone, past DFAK contributors

language: en

summary: " මට මගේ උපාංගය නැති විය, මා කළ යුත්තේ කුමක්ද??"

date: 2023-04

permalink: /en/topics/lost-device

parent: Home

# මට මගේ උපාංගය නැති විය

ඔබගේ උපාංගය නැති වී තිබේද? කවුරුහරි එය සොරකම් කර හෝ අල්ලාගෙන තිබේද?

මෙම තත්ත්වයන් තුළ, වෙනත් අයෙකු ඔබගේ ගිණුම්, සම්බන්ධතා සහ පුද්ගලික තොරතුරු වෙත ප්‍රවේශ වීමේ අවදානම අවම කිරීමට ඉක්මන් පියවර ගැනීම වැදගත් වේ.

ඩිජිටල් ප්‍රථමාධාර කට්ටලයේ මෙම කොටස මූලික ප්‍රශ්න කිහිපයක් හරහා ඔබව ගෙන යන අතර එමඟින් ඔබට උපාංගයක් අහිමි වීම සම්බන්ධ විය හැකි හානිය අවම කර ගන්නේ කෙසේදැයි තක්සේරු කළ හැක.

## වැඩ ප්‍රවාහය

### ප්‍රශ්නය-1

උපාංගය තවමත් අතුරුදහන් වී තිබේද?

- [ඔව් එය අතුරුදහන්](#උපාංගය-අතුරුදහන්)

- [නැත එය මා වෙත ආපසු ලබා දී ඇත] (#උපාංගය ආපසු ලබා දී ඇත)

### උපාංගය-අතුරුදහන්

> උපාංගයේ තිබූ ආරක්‍ෂාව මොනවාද යන්න මෙනෙහි කිරීම හොඳය:

>

> \* උපාංගයට ප්‍රවේශය මුරපදයකින් හෝ වෙනත් ආරක්‍ෂක පියවරකින් ආරක්‍ෂා කළේද?

> \* උපාංගයේ උපාංග සංකේතනය ක්‍රියාත්මක කර තිබේද?

> \* ඔබගේ උපාංගය නැති වූ විට එය පැවතියේ කුමන තත්වයකද - ඔබ පුරනය වී සිටියාද? උපාංගය ක්‍රියාත්මක වූ නමුත් මුරපදය-අගුළු දමා තිබුණේද? එය නිදාගෙන සිටියාද නැත්නම් ශිශිරතරණය කළාද? එය සම්පූර්ණයෙන්ම අක්රිය කළාද?

මෙම සලකා බැලීම් මනසේ තබාගෙන, ඔබේ උපාංගයේ අන්තර්ගතයට වෙනත් අයෙකුට ප්‍රවේශය ලබා ගැනීමට ඇති හැකියාව ඔබට වඩා හොඳින් අවබෝධ කර ගත හැක.

- [මගේ ගිණුම් වෙත උපාංගයේ ප්‍රවේශය ඉවත් කරමු](#ගිණුම්)

### ගිණුම්

> මෙම උපාංගයට ප්‍රවේශ වූ සියලුම ගිණුම් ලැයිස්තුගත කරන්න. මෙය විද්‍යුත් තැපෑල, සමාජ මාධ්‍ය, පණිවිඩ යැවීම, ආලය කිරීම සහ බැංකුකරණය සඳහා වන ගිණුම් මෙන්ම ද්විතියික සත්‍යාපනය සඳහා මෙම උපාංගය භාවිත කළ හැකි ගිණුම් විය හැකිය.

>

> ඔබගේ උපාංගයට ප්‍රවේශය තිබූ ඕනෑම ගිණුමක් සඳහා (ඊමේල්, සමාජ මාධ්‍ය හෝ වෙබ් ගිණුම වැනි), ඔබ ඒවා සඳහා මෙම උපාංගය සඳහා අවසරය ඉවත් කළ යුතුය. මෙය ඔබගේ ගිණුම් වෙත පුරනය වීමෙන් සහ අවසර ලත් උපාංගවලින් උපාංගය ඉවත් කිරීමෙන් සිදු කළ හැක.

> \* [Google Account](https://myaccount.google.com/device-activity)

> \* [Facebook Account](https://www.facebook.com/settings?tab=security&section=sessions&view)

> \* [iCloud Account](https://support.apple.com/en-us/HT205064)

> \* [Twitter Account](https://twitter.com/settings/sessions)

> \* [Yahoo Account](https://login.yahoo.com/account/activity)

ඔබ ඔබගේ ගිණුම් විසන්ධි කිරීම අවසන් කළ පසු, උපාංගයේ තිබූ ඔබගේ මුරපද සුරක්ෂිත කරමු.

- [හරි අපි මුරපද සමඟ ගනුදෙනු කරමු](#මුරපද)

### මුරපද

> උපාංගයට කෙලින්ම සුරකින ලද මුරපද හෝ සුරකින ලද මුරපද ගබඩා කර ඇති ඕනෑම බ්‍රව්සරයක් ගැන මෙනෙහි කරන්න.

>

> මෙම උපාංගයට ප්‍රවේශ විය හැකි සියලුම ගිණුම් සඳහා මුරපද වෙනස් කරන්න. ඔබ මුරපද කළමනාකරුවෙකු භාවිතා නොකරන්නේ නම්, ශක්තිමත් මුරපද වඩා හොඳින් නිර්මාණය කිරීම සහ කළමනාකරණය කිරීම සඳහා එකක් භාවිතා කිරීම තරයේ සලකා බලන්න.

ඔබගේ උපාංගයේ ඔබගේ ගිණුම් සඳහා මුරපද වෙනස් කිරීමෙන් පසු, ඔබ මෙම මුරපදවලින් කිසිවක් වෙනත් ගිණුම් සඳහා භාවිතා කළේ දැයි සිතා බලන්න - එසේ නම්, කරුණාකර එම මුරපද ද වෙනස් කරන්න.

- [මම මගේ සමහර මුරපද නැතිවූ උපාංගයේ වෙනත් ගිණුම් සඳහා භාවිතා කළෙමි](#එකම-මුරපදය)

- [අවධානයට ලක් වී ඇති මගේ සියලුම මුරපද අද්විතීයයි](#2fa)

### එකම මුරපදය

නැතිවූ උපාංගය හැර වෙනත් ගිණුම්වල හෝ උපාංගවල ඔබ එකම මුරපදය භාවිත කරන්නේද? එසේ නම්, එම ගිණුම්වල මුරපදය වෙනස් කරන්න, මන්ද ඒවාද අවදානමට ලක් විය හැකිය.

- [හරි, මම දැන් අදාළ මුරපද සියල්ල වෙනස් කර ඇත](#2fa)

### 2fa

> ප්‍රවේශ වීමේ අවදානමක් ඇතැයි ඔබ සිතන ගිණුම් සඳහා ද්වි-සාධක සත්‍යාපනය සක්‍රීය කිරීමෙන් ඒවා වෙනත් අයෙකුට ප්‍රවේශ විය හැකි සම්භාවිතාව අඩු කරයි.

>

> මෙම උපාංගයට ප්‍රවේශ විය හැකි සියලුම ගිණුම් සඳහා ද්වි-සාධක සත්‍යාපනය ක්‍රියාත්මක කරන්න. සියලුම ගිණුම් 2-සාධක සත්‍යාපනයට සහාය නොදක්වන බව කරුණාවෙන් සලකන්න. ද්වි-සාධක සත්‍යාපනයට සහාය දක්වන සේවා සහ වේදිකා ලැයිස්තුවක් සඳහා කරුණාකර [Two Factor Auth](https://twofactorauth.org) වෙත පිවිසෙන්න.

- [මගේ ගිණුම් තවදුරටත් සුරක්ෂිත කිරීම සඳහා මම ද්වි-සාධක සත්‍යාපනය සක්‍රීය කර ඇත. මම මගේ උපාංගය සොයා ගැනීමට හෝ මැකීමට උත්සාහ කිරීමට කැමතියි](#find-erase-device)

### සොයන්න-මකන්න-උපාංගය

> ඔබ මෙම උපාංගය භාවිතා කළේ කුමක් සඳහාද යන්න ගැන සිතන්න - මෙම උපාංගයේ සම්බන්ධතා, ස්ථානය හෝ පණිවිඩ වැනි සංවේදී තොරතුරු තිබේද? මෙම දත්ත කාන්දු වීම ඔබට, ඔබේ කාර්යයට, හෝ ඔබට හැර අන් අයට ගැටලුකාරී විය හැකිද?

>

> සමහර අවස්ථාවල රඳවාගෙන සිටින පුද්ගලයෙකුගේ උපාංගයේ ඇති දත්ත දුරස්ථව පිසදැමීම, එහි දත්ත අනිසි ලෙස භාවිත කිරීම සහ ඔවුන්ට හෝ වෙනත් ක්‍රියාකාරීන්ට එරෙහිව භාවිතා කිරීම වැළැක්වීමට උපකාරී වේ. ඒ අතරම, මෙය රඳවාගෙන සිටින පුද්ගලයාට (විශේෂයෙන් වධහිංසා පැමිණවීම් සහ අනිසි ලෙස සැලකීමට ඉඩ ඇති අවස්ථාවන්හිදී) ගැටළුකාරී විය හැකිය - විශේෂයෙන් රඳවාගෙන සිටින පුද්ගලයාට උපාංගයට ප්‍රවේශය ලබා දීමට බල කෙරුනේ නම්, උපාංගයෙන් දත්ත හදිසියේ අතුරුදහන් වීම, රඳවා තබා ගන්නා බලධාරීන් බවට පත් කළ හැකිය. වඩාත් සැක සහිත. ඔබත් එවැනිම තත්වයකට මුහුණ දෙන්නේ නම්, අපගේ කොටස ["මම දන්නා අයෙක් අත්අඩංගුවට ගෙන ඇත"](/../../../අත්අඩංගුවට ගෙන ඇත) කියවන්න.

>

> සමහර රටවල දුරස්ථව පිසදැමීම නීත්‍යානුකූලව අභියෝගාත්මක විය හැකි බැවින් එය සාක්ෂි විනාශ කිරීමක් ලෙස අර්ථ දැක්විය හැකි බව සඳහන් කිරීම වටී.

>

> සම්බන්ධ වූ සෑම කෙනෙකුටම සෘජු සහ නෛතික ප්‍රතිවිපාක පිළිබඳව ඔබට පැහැදිලි නම්, ඔබේ මෙහෙයුම් පද්ධතිය සඳහා උපදෙස් අනුගමනය කිරීමෙන් ඔබට උපාංගය දුරස්ථව පිසදැමීමට උත්සාහ කිරීම දිගටම කරගෙන යා හැක:

>

> \* [Android උපාංග](https://support.google.com/accounts/answer/6160491?hl=en)

> \* [iPhone හෝ Mac](https://www.icloud.com/#find)

> \* [iCloud භාවිතයෙන් iOS උපාංග (iPhone සහ iPad)](https://support.apple.com/kb/ph2701)

> \* [Windows උපාංග](https://support.microsoft.com/en-us/help/11579/microsoft-account-find-and-lock-lost-windows-device)

> \* Windows හෝ Linux උපාංග සඳහා, ඔබ ඔබගේ උපාංගයේ දත්ත සහ ඉතිහාසය දුරස්ථව මකා දැමීමට ඉඩ සලසන මෘදුකාංග (සොරකම්-විරෝධී හෝ ප්රති-වයිරස මෘදුකාංග වැනි) ස්ථාපනය කර තිබිය හැක. එසේ නම්, එය භාවිතා කරන්න.

උපාංගයේ තොරතුරු දුරස්ථව මකා දැමීමට ඔබ කළමනාකරණය කර ඇතත් නැතත්, ඔබේ සම්බන්ධතාවලට දැනුම් දීම හොඳ අදහසකි.

- [ඔබගේ උපාංගය නැතිවී යාම ගැන ඔබේ සම්බන්ධතා දන්වන්නේ කෙසේද යන්න පිළිබඳ ඉඟි සොයා ගැනීමට ඊළඟ පියවර වෙත යන්න](#inform-network)

### තොරතුරු ජාලය

> ඔබගේම ගිණුම් වලට අමතරව, ඔබගේ උපාංගයේ අනෙක් අය ගැන තොරතුරු තිබිය හැක. මෙයට ඔබේ සම්බන්ධතා, අන් අය සමඟ සන්නිවේදනය, හෝ පණිවුඩකරණ කණ්ඩායම් ඇතුළත් විය හැක.

>

> නැතිවූ උපාංගය ගැන ඔබේ ජාලයට සහ ප්‍රජාවට දැනුම් දීම ගැන සලකා බැලීමේදී, අන් අය වෙත ළඟා වීමෙන් ඔබ ඔවුන්ව වැඩි අවදානමකට ලක් නොකරන බව සහතික කර ගැනීමට [හානි අඩු කිරීමේ මූලධර්ම](/../../අත්අඩංගුවට ගත්#හානි-අඩු කිරීම) භාවිතා කරන්න.

නැතිවූ උපාංගය ගැන ඔබේ ජාලයට දන්වන්න. මෙය ප්‍රධාන අධි අවදානම් සම්බන්ධතා සමඟ පුද්ගලිකව සිදු කළ හැකි අතර, එසේ කිරීම සුදුසු යැයි ඔබට හැඟෙන්නේ නම්, ඔබේ වෙබ් අඩවියේ හෝ සමාජ මාධ්‍ය ගිණුමක ප්‍රසිද්ධියේ අවදානමට ලක්විය හැකි ගිණුම් ලැයිස්තුවක් පළ කිරීම.

- [මම මගේ සම්බන්ධතා දැනුවත් කර ඇත](#සමාලෝචන-ඉතිහාසය)

### සමාලෝචන-ඉතිහාසය

> හැකි නම්, උපාංගයට සම්බන්ධ සියලුම ගිණුම්වල සම්බන්ධතා ඉතිහාසය/ගිණුම් ක්‍රියාකාරකම් සමාලෝචනය කරන්න. ඔබ සබැඳිව නොසිටි අවස්ථාවක ඔබේ ගිණුම භාවිත කළේද නැතහොත් ඔබේ ගිණුම නුහුරු නුපුරුදු ස්ථානයකින් හෝ IP ලිපිනයකින් ප්‍රවේශ වී තිබේද යන්න බැලීමට පරීක්ෂා කරන්න.

>

> ඔබට පහත සමහර ජනප්‍රිය සැපයුම්කරුවන් මත ඔබේ ක්‍රියාකාරකම් සමාලෝචනය කළ හැක:

> \* [Google Account](https://myaccount.google.com/device-activity)

> \* [Facebook Account](https://www.facebook.com/settings?tab=security&section=sessions&view)

> \* [iCloud Account](https://support.apple.com/en-us/HT205064)

> \* [Twitter Account](https://twitter.com/settings/sessions)

> \* [Yahoo Account](https://login.yahoo.com/account/activity)

ඔබ ඔබේ සම්බන්ධතා ඉතිහාසය සමාලෝචනය කර තිබේද?

- [මා සතුව සැක සහිත කිසිවක් හමු නොවීය](#පරීක්ෂා-සැකසීම්)

- [මා සතුව යම් සැක කටයුතු ක්‍රියාකාරකමක් තිබේ, සහ සොයා ගන්නා ලදී](../../../ගිණුම්-ප්‍රවේශ-ගැටලු/)

### පිරික්සුම්-සැකසීම්

> උපාංගයට සම්බන්ධ සියලුම ගිණුම්වල ගිණුම් සැකසීම් පරීක්ෂා කරන්න. ඒවා වෙනස් කර තිබේද? විද්‍යුත් තැපැල් ගිණුම් සඳහා, ස්වයංක්‍රීයව ඉදිරියට යැවීම, උපස්ථ/නැවත පිහිටුවීමේ ඊමේල් ලිපිනය හෝ දුරකථන අංක වෙත විය හැකි වෙනස්කම්, දුරකථන, පරිගණක හෝ ටැබ්ලට් ඇතුළු විවිධ උපාංග වෙත සමමුහුර්ත කිරීම සහ යෙදුම් හෝ වෙනත් ගිණුම් අවසර සඳහා පරීක්ෂා කරන්න.

>

> ඔබගේ ගිණුමේ කිසිදු සැක කටයුතු ක්‍රියාකාරකමක් නොපෙන්වන බව සහතික කර ගැනීම සඳහා අවම වශයෙන් සතියකට වරක් මසකට වරක් ගිණුම් ක්‍රියාකාරකම් පිළිබඳ ඉතිහාසය සමාලෝචනය කරන්න.

- [මගේ ගිණුම් ක්‍රියාකාරකම් ඉතිහාසය සැක සහිත ක්‍රියාකාරකම් පෙන්වයි](../../../account-access-issues/)

- [මගේ ගිණුම් ක්‍රියාකාරකම් ඉතිහාසය කිසිදු සැක කටයුතු ක්‍රියාකාරකමක් නොපෙන්වයි, කෙසේ වෙතත් මම එය කාලයත් සමඟ සමාලෝචනය කරමි](#resolved\_end)

### උපාංගය-ආපසු ලැබිණි

> ඔබගේ උපාංගය නැති වූවා නම්, තෙවන පාර්ශවයක් විසින් ගෙන තිබේ නම් හෝ දේශසීමා හරස් මාර්ගයකදී භාර දීමට සිදු වූවා නම්, නමුත් ඔබ එය ආපසු ලබා ගෙන තිබේ නම්, එයට ප්‍රවේශය ඇත්තේ කවුරුන්ද යන්න ඔබ නොදන්නා බැවින් ප්‍රවේශම් වන්න. ඔබ මුහුණ දෙන අවදානම් මට්ටම අනුව, ඔබට උපාංගය දැන් විශ්වාස කළ නොහැකි හෝ සම්මුතියකට ලක් වී ඇති සේ සැලකීමට අවශ්‍ය විය හැකිය.

>

> පහත ප්‍රශ්න ඔබෙන්ම අසන්න සහ ඔබේ උපාංගය අවදානමට ලක්වී ඇති බවට තක්සේරු කරන්න:

>

> \* කොපමණ කාලයක් උපාංගය ඔබේ පාලනයෙන් ඉවත්ව තිබුණේද?

> \* එයට ප්‍රවේශ විය හැක්කේ කාටද?

> \* ඔවුන්ට එයට ප්‍රවේශ වීමට අවශ්‍ය වන්නේ ඇයි?

> \* උපාංගය භෞතිකව විකෘති වී ඇති බවට ලකුණු තිබේද?

>

> ඔබ තවදුරටත් ඔබගේ උපාංගය විශ්වාස නොකරන්නේ නම්, උපාංගය පිසදැමීම සහ නැවත ස්ථාපනය කිරීම හෝ නව එකක් ලබා ගැනීම සලකා බලන්න.

ප්‍රතිස්ථාපන උපාංගයක් ලබා ගැනීමට ඔබ සහාය වීමට කැමතිද?

- [ඔව්](#නව-උපාංග\_අවසානය)

- [නැත](#විසඳුණු\_අවසානය)

### නව-උපාංග\_අවසානය

ඔබට ප්‍රතිස්ථාපන උපාංගයක් ලබා ගැනීමට බාහිර මූල්‍ය සහාය අවශ්‍ය නම්, කරුණාකර ඔබට සහාය දිය හැකි පහත සංවිධාන අමතන්න.

:[](සංවිධාන?services=equipment\_replacement)

### විසඳන ලද\_අවසානය

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

### අවසාන\_ඉඟි

දත්ත කාන්දුවීම් සහ ඔබගේ ගිණුම් සහ තොරතුරු වෙත අනවසරයෙන් පිවිසීමේ අවදානම අවම කිරීම සඳහා උපදෙස් මාලාවක් මෙන්න:

- කිසිවිටෙක ඔබගේ උපාංගය අවධානයෙන් තොරව තබන්න. ඔබට එය රැගෙන යාමට නොහැකි නම්, එය වසා දමා ආරක්ෂිත ස්ථානයක ගබඩා කරන්න.

- සම්පූර්ණ තැටි සංකේතනය සක්රිය කරන්න.

- ඔබගේ උපාංගය අගුලු දැමීමට ශක්තිමත් මුරපදයක් භාවිතා කරන්න.

- හැකි සෑම විටම මගේ දුරකථනය සොයන්න/මකන්න විශේෂාංගය සක්‍රීය කරන්න, නමුත් ඔබගේ ආශ්‍රිත ගිණුම (Gmail/iCloud) අවදානමට ලක්ව ඇත්නම්, මෙය ඔබව නිරීක්ෂණය කිරීමට හෝ ඔබගේ උපාංගය අතුගා දැමීමට භාවිතා කළ හැකි බව කරුණාවෙන් සලකන්න.

[Access Now Helpline Community Documentation: Tips on how to enable full-disk encryption](https://communitydocs.accessnow.org/166-Full-Disk\_Encryption.html)

\* [Security in a Box: Protecting your sensitive information](https://securityinabox.org/en/files/secure-file-storage/)

\* Consider using anti-theft software such as [Prey](https://preyproject.com)

මූලාශ්‍ර

\* [Access Now Helpline Community Documentation: Tips on how to enable full-disk encryption](https://communitydocs.accessnow.org/166-Full-Disk\_Encryption.html)

\* [Security in a Box: Protecting your sensitive information](https://securityinabox.org/en/files/secure-file-storage/)

\* Consider using anti-theft software such as [Prey](https://preyproject.com)