---

layout: page

title: " எனது சாதனத்தை தொலைத்து விட்டேன்"

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

language: en

summary: "எனது சாதனத்தை தொலைத்து விட்டேன்,நான் இப்போது என்ன செய்வது?"

date: 2023-04

permalink: /en/topics/lost-device

parent: Home

---

# எனது சாதனத்தை தொலைத்து விட்டேன்

உங்களுடைய சாதனம் தொலைந்து விட்டதா? அது திருடப்பட்டு விட்டதா அல்லது மூன்றாம் நபரினால் கைப்பற்றப்பட்டுவிட்டதா?

இவ்வாறான சூழ்நிலைகளில், உங்களுடைய கணக்குகள்,தொடர்புகள்,மற்றும் தனிப்பட்ட தகவல்கள் என்பன வேறொரு நபரினால் கையாளப்படுவதை குறைப்பதற்குரிய உடனடி நடவடிக்கைகளினை மேற்கொள்ளுதல் முக்கியமானதாகும்.

டிஜிட்டல் முதலுதவி பொதியினுடைய இந்த பகுதியானது உங்களை அடிப்படை கேள்விகளினூடாக இட்டுச்செல்லும். எனவே சாதனத்தை தொலைப்பதுடன் தொடர்புடைய தீங்குகளை எவ்வாறு குறைத்துக் கொள்வது என்பது தொடர்பாக நீங்கள் மதிப்பீடு செய்து கொள்ளலாம்.

## பணிப்பாய்ச்சல் -Workflow

### வினா-1

சாதனமானது இன்னும் கிடைக்கவில்லையா?

- [ஆம் அது கிடைக்கவில்லை](#சாதனம்-காணவில்லை)

- [இல்லை, அது என்னிடம் மீள ஒப்படைக்கப்பட்டுவிட்டது](#சாதனம் -மீளளிக்கப்பட்டது)

### சாதனம்-காணவில்லை

> அந்த சாதனத்தில் எந்த விதமான பாதுகாப்புகள் காணப்பட்டன என்பதன் அடிப்படையில் செயற்படுதல் சிறப்பானது:

>

> \*சாதனத்தினுடைய அணுகலானது கடவுச்சொல் அல்லது வேறு ஏதாவது பாதுகாப்பு உத்திகள் மூலம் பாதுகாக்கப்பட்டதா?

> \* சாதனத்தில் சாதன குறியாக்கம் (device encryption) செயற்படுத்தப்பட்டதா?

> \* தொலையும்போது உங்களது சாதனம் எந்நிலையில் காணப்பட்டது- நீங்கள் உள்நுழைந்திருந்தீர்களா? இயக்கப்பட்டு கடவுச்சொல் இடப்பட்டு மூடப்பட்டிருந்ததா? அது உறங்கு நிலை அல்லது முடக்க நிலையில் (sleeping or hibernating)காணப்பட்டதா? அது முற்றாக நிறுத்தி வைக்கப்பட்டதா?

இவற்றை மனதில் கொண்டு, உங்களது சாதனத்திலுள்ள உள்ளடக்கங்களைனை வேறொரு நபர் இயக்க கூடிய சாத்தியக் கூறுகள் தொடர்பாக தெளிவாக விளங்கிக்கொள்ள முடியும்.

- [எனது கணக்குகளுக்கான சாதனத்தினுடைய அணுகலினை நீக்குவோம்](#கணக்குகள்)

### கணக்குகள்

> அந்த சாதனத்தினால் அணுகக்கூடிய அனைத்து கணக்குகளினையும் பட்டியலிடுதல். இது மின்னஞ்சலாகவோ, சமூக ஊடகமாகவோ,செய்திப்பரிமாற்ற சேவைகளாகவோ, உல்லாச தளங்களாகவோ,மற்றும் வங்கிக் கணக்குகளாகவோ அல்லது இந்த சாதனத்தினை துணைநிலை அங்கீகாரத்திற்காகப் பயன்படுத்தும் கணக்குகளாகவேனும் காணப்படலாம்.

>

> உங்கள் சாதனம் அணுகலினைக் கொண்டுள்ள கணக்குகளில் (மின்னஞ்சல், சமூக ஊடகங்கள் அல்லது வலைத்தள கணக்குகள் போன்றவை)இந்தச் சாதனத்துக்கான அனுமதியினை நீக்குதல் வேண்டும். இவை நீங்கள் உங்கள் கணக்குகளில் உள்நுழைந்து அனுமதிக்கப்பட்ட சாதனங்களிலிருந்து குறித்த சாதனத்தை நீக்குவதன்மூலம் செய்துகொள்ள கூடியதாக இருக்கும்.

>

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

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

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

> \* [கீச்சகக் கணக்குகள்](https://twitter.com/settings/sessions)

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

உங்களது கணக்குகளிற்கான இணைப்பினை நீக்கிய பின்னர் அந்த சாதனத்தில் காணப்படும் கடவுச் சொல்லினை பாதுகாப்போம்.

- [சரி, இப்போது கடவுச்சொல்லினைக் கையாள்வோம்](#கடவுச்சொற்கள்)

### கடவுச்சொற்கள்

> சாதனத்தில் நேரடியாகச் சேமிக்கப்பட்ட கடவுச்சொற்கள் அல்லது சேமித்த கடவுச்சொற்களைச் சேமித்துள்ள உலாவிகளைப் பற்றி சிந்தியுங்கள்.

>

> இந்த சாதனத்தினால் அணுகக்கூடிய அனைத்துக் கணக்குகளுக்குமான கடவுச்சொல்லினை மாற்றுங்கள். நீங்கள் கடவுச்சொல் முகாமையினைப் பயன்படுத்தவில்லையெனின், பலமான கடவுச்சொல்லினை உருவாக்கி முகாமை செய்வதற்காக இவற்றில் ஒன்றினை பயன்படுத்துவது தொடர்பாக கருத்திலெடுங்கள்.

உங்களுடைய சாதனத்திலுள்ள கணக்குகளுக்கான கடவுச்சொல்லினை மாற்றிய பின்னர் அந்த கடவுச்சொற்களில் எவற்றையாவது வேறு கணக்குகளிற்கு உபயோகித்துள்ளீர்களா என்பதை ஜோசியுங்கள்- அப்படியெனில், அந்த கடவுச்சொற்களினையும் மாற்றம் செய்யுங்கள்.

- [தொலைந்த சாதனத்தில் எனது சில கடவுச்சொற்களை மற்ற கணக்குகளுக்குப் பயன்படுத்தினேன்](#ஒரே-கடவுச்சொல்)

- [மாற்றம் செய்யப்பட்ட அனைத்து கடவுச்சொற்களும் தனித்துவமானவை](#2fa)

### ஒரே-கடவுச்சொல்

நீங்கள் வேறு கணக்குகளிற்கு அல்லது தொலைந்த சாதனத்திற்கு பக்கமாகவுள்ள ஏனைய சாதனைகளில் ஒரே கடவுச்சொல்லினை பயன்படுத்துகின்றீர்களா? ஆம் எனில், அவையும்கூட பாதிக்கப்படக்கூடியனவாக காணப்படுவதால் அந்த கணக்குகளின் கடவுச்சொல்லினையும் மாற்றுங்கள்.

- [சரி, நான் தற்போது தொடர்புபட்ட அனைத்து கடவுச்சொல்லினையும் மாற்றிவிட்டேன்.](#2fa)

### 2fa

> இன்னுருவரினால் அணுகப்படக்கூடிய அபாயமுள்ளது என நீங்கள் எண்ணும் கணக்குகளிற்கு இரு காரணி உறுதிப்படுத்தலினை (two-factor authentication) செயற்படுத்தலானது இன்னொரு நபரினால் அது அணுகப்படக்கூடிய சாத்தியங்களினைக் குறைக்கும்.

>

> இந்த சாதனத்தினால் அணுகப்படக்கூடிய அனைத்து கணக்குகளிற்கும் இரு காரணி உறுதிப்படுத்தலினை செயற்படுத்துங்கள். எனினும் அனைத்து கணக்குகளும் இரு காரணி உறுதிப்படுத்தலினை ஆதரிப்பதில்லையென்பதை நினைவிற்கொள்ளுங்கள்.இருகாரணி உறுதிப்படுத்தலினை ஆதரிக்கும் சேவைகள் மற்றும் தளங்களிற்கு இந்த இணைப்பினை நாடுங்கள். [Two Factor Auth](https://twofactorauth.org).

- [எனது கணக்குகளை மேலும் பாதுகாப்பானதாக்க இரு காரணி உறுதிப்படுத்தலினை செயற்படுத்தியுள்ளேன்.எனது சாதனத்தைக் கண்டறிய அல்லது அழிக்க விரும்புகிறேன்](#கண்டறிதல்-அழித்தல்-சாதனம்)

### கண்டறிதல்-அழித்தல்-சாதனம்

> நீங்கள் இந்த சாதனத்தை எதற்காகப் பயன்படுத்தினீர்கள் என சிந்தித்து பாருங்கள்,- இந்த சாதனத்தில் ஏதாவது தொடர்புகள், இருப்பிடம் அல்லது செய்திகள் போன்ற முக்கியமான தகவல்கள் காணப்படுகின்றதா? இந்த தரவுகள் வெளியிடப்பட்டால் உங்களுக்கு, உங்கள் வேலைக்கு அல்லது உங்களைச் சார்ந்த யாருக்காவது பிரச்சினையாகுமா,

>

> சில சந்தரங்களில் தடுப்புக்காவலிலுள்ளவருடைய சாதனத்திலுள்ள தரவுகளினை தொலைவாகவிருந்து நீக்குதலானது அதிலுள்ள தரவுகள் துஸ்பிரயோகம் செய்யப்பட்டு அவர்களுக்கெதிராகவோ அல்லது ஏனைய செயற்பாட்டாளர்களுக்கெதிராகவோ பயன்படுத்தப்படுவதனைத் தடுப்பதற்கு உதவுவதாக அமையும். அதேவேளை, இது தடுப்பிலுள்ள நபரிற்கு பிரச்சனையாக அமையலாம் (குறிப்பாக சித்திரவதை தவறாக நடத்தப்படுத்தல் சாதகமாக காணப்படும் சந்தர்ப்பங்களில்.)- குறிப்பாக தடுப்புக்காவலிலுள்ளவர் சாதனத்துக்கான அணுகலினை வழங்க கட்டாயப்படுத்தப்பட்டால், திடீரென தகவல்கள் நீக்கப்படுத்தலானது தடுத்து வைத்துள்ள அதிகாரிகளுக்கு மேலும் சந்தேகத்தினை ஏற்படுத்தும்.நீங்கள் இதுபோன்ற சூழ்நிலைக்கு முகம் கொடுக்க நேர்ந்தால் பின்வரும் பகுதியினை வாசியுங்கள். ["எனக்குத் தெரிந்த சிலர் கைதாகியுள்ளனர்"](../../../../arrested).

>

> சில நாடுகளில் தொலைவிலிருந்து நீக்குதலானது, ஆதாரங்களை அழித்தலாக கருதப்பட்டு சட்டபூர்வமாக சவாலுக்குட்படுத்தப்படக்க கூடியதாக காணப்படுவதனால் இது பயனற்றதாக கூட ஆகலாம்.

>

> இதில் ஈடுபட்டுள்ள அனைவருக்கும் ஏற்படக்கூடிய நேரடி மற்றும் சட்டரீதியான விளைவுகள் குறித்து நீங்கள் தெளிவாக இருந்தால் உங்கள் இயக்க முறைமைக்கான(operating system) அறிவுறுத்தனைப் பின்பற்றி தொலைவிலிருந்தே நீக்குவதற்கான நடவடிக்கைகளினைத் நீங்கள் தொடரலாம்:

>

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

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

> \* [iOS devices (iPhone and iPad) by using iCloud](https://support.apple.com/kb/ph2701)

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

> \* [Blackberry phones](https://docs.blackberry.com/en/endpoint-management/blackberry-uem/12\_9/blackberry-uem-self-service-user-guide/amo1375908155714)

> \* Windows or Linux சாதனங்களுக்கு,தொலைவிலிருந்தே உங்களது சாதனத்திலுள்ள தரவுகளினைஅழிக்கக்கூடிய anti-theft or anti-virus software போன்ற மென்பொருட்களை நீங்கள் நிறுவியிருக்கலாம். அவ்வாறிருப்பின் அதனை பயன்படுத்துங்கள்.

நீங்கள் சாதனத்தில் உள்ள தகவலை தொலைவிலிருந்து அழித்திருந்தாலும்சரி அழிக்காது விட்டாலும்சரி, உங்கள் தொடர்புகளுக்குத் தெரிவிப்பது நல்லது.

- [சாதனம் தொலைந்தமை தொடர்பாக உங்களது தொடர்புகளுக்கு எவ்வாறு என்பதற்கான அறிவுறுத்தல்களிற்காக அடுத்த படிக்குத் தொடருங்கள்.](#வலையமைப்புக்கு-தெரியப்படுத்தல்)

### வலையமைப்புக்கு-தெரியப்படுத்தல்

> உங்களுடைய சொந்தக் கணக்குளைத் தவிர்த்து, உங்களுடைய சாதனமானது ஏனையோரின் தகவல்களினைக் கொண்டிருக்கவும் வாய்ப்புகள் காணப்படுகின்றது.இது உங்களது தொடர்புகள், ஏனையோருடனான தொடர்பாடல்கள் , செய்திப்பரிமாறல் குழுக்கள் என்பவற்றினை உள்ளடக்கலாம்.

>

> உங்களுடைய சாதனம் தொலைந்தமை தொடர்பாக உங்களது வலையமைப்பு மற்றும் சமூகத்திடம் தெரிவிக்கும்போது அவர்களைச் சென்றடையும்போது நீங்கள் அவர்களினை பெரும் ஆபத்தினுள் இட்டுச்செல்லாததனை உறுதிப்படுத்தும் முகமாக தீங்கு தணிக்கும் கோட்பாட்டினைப் பின்பற்றுங்கள்[harm reduction principles](../../../../arrested#harm-reduction).

தொலைந்த சாதனம் தொடர்பாக உங்களது வலையமைப்புக்குத் தெரிவியுங்கள். அதிக ஆபத்தான முக்கியமான தொடர்புகளுக்கு தனிப்பட்ட ரீதியில் தெரிவிக்கப்படலாம், அல்லது தகுந்தது என நீங்கள் எண்ணினால் பாதிக்கப்பட்ட கணக்குகளின் பட்டியலினை உங்களுடைய வலைத்தளத்தில் அல்லது சமூக ஊடகத்தில் பொதுவெளியில் பதிவிடலாம்.

- [எனது தொடர்புகளுக்கு தெரியப்படுத்திவிட்டேன்] (#கடந்த கால- மீளாய்வு)

### கடந்தகால- மீளாய்வு

> முடியுமெனில் சாதனத்துடன் தொடர்புடைய அனைத்து கணக்குகளினதும் கடந்தகால இணைப்புகள்/ கணக்கின் செயற்பாடுகள் என்பவற்றை மீளாய்வு செய்து பாருங்கள். நீங்கள் நிகழ்நிலையில் இல்லாதபோது உங்களது கணக்குகள் பாவனைக்குட்படுத்தப்பட்டுள்ளதா அல்லது உங்களது கணக்குகள் உங்களுக்கு தொடர்பில்லாத இருப்பிடத்திலிருந்து அல்லது IP address இலுருந்து பாவிக்கப்பட்டுள்ளதா என்பதனை தெரிந்துகொள்ள சோதனை செய்யுங்கள்.

>

> கீழே தரப்பட்டுள்ள பிரபல்யமான சேவை வழங்குநர்களை கொண்டு உங்களது செயற்பாடுகளை மீளாய்வு செய்யலாம்:

>

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

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

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

> \* [கீச்சகக் கணக்கு](https://twitter.com/settings/sessions)

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

உங்களுடைய இணைப்புகளின் வரலாற்றினை மீளாய்வு செய்தீர்களா?

- [நான் செய்துள்ளேன், சந்தேகிக்கும்படியாக எதுகுமில்லை](# அமைப்புகளினைப்-பரிசோதித்தல் )

- [நான் செய்துள்ளேன், சந்தேகமான செயற்பாடுகள் காணப்படுகின்றன](../../../account-access-issues/)

### அமைப்புகளினைப்-பரிசோதித்தல்

> சாதனத்துடன் தொடர்புடைய அனைத்துக் கணக்குகளினதும் அமைப்பினைப் பரிசோதியுங்கள். அவை மாற்றப்பட்டுள்ளனவா? மின்னஞ்சலிற்கு தானாகவே முன்னனுப்புதலினையும், காப்புப் பிரதி/ மின்னஞ்சல் முகவரியை மீளுருவாக்கம் அல்லது தொலைபேசி எண்கள், தொலைபேசி,கணனி அல்லது டேப்லட் உட்பட வேறுபட்ட சாதனங்களுடன் ஒத்திசைக்கப்பட்டிருத்தல் அல்லது வேறு கணக்குகளுக்கான அனுமதியினை வழங்கியிருத்தல் போன்றவற்றை பரிசோதித்தல்.

>

> உங்களது கணக்கில் எவ்வித சந்தேகத்துக்கிடமான செயற்பாடுகளும் இல்லையென்பதனை உறுதிப்படுத்த ஆகக்குறைந்தது வாரத்தில் ஒரு தடவை என்ற ரீதியில் தொடர்ச்சியாக ஒரு மாத காலத்துக்கு உங்கள் கணக்கின் செயற்பாடுகளனை மீளாய்வுசெய்யுங்கள்.

- [எனது கணக்கின் செயற்பாடுகளின் வரலாறானது சந்தேகத்துக்கிடமான செயற்பாடுகளினைக் காட்டுகிறது](../../../account-access-issues/)

- [எனது கணக்கின் செயற்பாடுகளின் வரலாறானது சந்தேகத்துக்கிடமான செயற்பாடுகளினைக் காட்டவில்லை, எதுவாயினும் நேரத்துக்கு நேரம் அதனை மீளாய்வு செய்வதனை நான் தொடர்வேன்] (#தீர்க்கப்பட்டது\_முடிவுற்றது)

### சாதனம்-மீள ஒப்படைக்கப்பட்டது.

> உங்களுடைய சாதனம் தொலைந்திருந்தால், மூன்றாம் நபரொருவரால் எடுக்கப்பட்டிருந்தால், அல்லது எல்லையில் வைத்து கையளிக்கப்படவேண்டியிந்தால், எனினும் நீங்கள் அதனை மீள பெற்றால் அதன் அணுகலை யாரெல்லாம் கொண்டிருக்கின்றனர் என்பது தெரியாதபடியினால் நீங்கள் கவனமாக இருத்தல் வேண்டும்.நீங்கள் முகம்கொடுக்க வேண்டிய ஆபத்தினுடைய அளவின் அடிப்படையில், அச்சாதனத்தை நீங்கள் நம்பத்தகாததாக அல்லது தாக்கப்பட்டதாக கருதுதல் வேண்டும்.

> பின்வரும் வினாக்களை உங்களிடம் வினவி உங்கள் சாதனம் தாக்கப்பட்டதன்மூலமான ஆபத்தினுடைய அளவினை மதிப்பீடு செய்துகொள்ளுங்கள்:

> \* சாதகமானது எவ்வளவு காலம் உங்களது கட்டுப்பாட்டிற்கு அப்பால் இருந்தது?

> \* யார் இதற்குரிய அணுகலினை கொண்டிருக்க முடியும்?

> \* ஏன் அவர்களுக்கு இதன் அணுகல் தேவைப்படுகிறது?

> \* பௌதீக ரிதியாக சாதனம் சேதப்படுத்தப்பட்டதற்கான அறிகுறிகள் ஏதும் காணப்படுகின்றனவா?

> உங்கள் சாதனத்தை நீங்கள் நம்பவில்லையெனில் , சாதனத்தைத் முற்றாக அழித்துவிட்டு மீண்டும் நிறுவுவது பற்றி சிந்திக்கவும் அல்லது புதிய சாதனத்தைப் பெற்றுக்கொள்ளுங்கள்.

மாற்றான சாதனம் ஒன்றினை பெறுவதற்கான உதவி ஒன்றினை விரும்புகிறீர்களா?

- [ஆம்](#new-device\_end)

- [இல்லை](#resolved\_end)

### கணக்குகள்\_முடிவு

உங்களது கணக்கிற்கான அணுகலினை இழந்திருந்தாலோ அல்லது உங்களுடைய கணக்கினை இன்னொருவர் கையாண்டுள்ளார் என எண்ணினாலோ, தயவுசெய்து கீழே பட்டியலிடப்பட்டுள்ள உங்களுக்கு உதவி வழங்கக்கூடிய நிறுவனங்களை தொடர்புகொள்ளுங்கள்.

:[](organisations?services=account)

### new-device\_end

மாற்றான ஒரு சாதனத்தினை பெற்றுக்கொள்ள உங்களுக்கு நிதிசார் அனுசரணைகளில் தேவைப்படின் உங்களுக்கு உதவக்கூடிய கீழே தரப்பட்ட நிறுவனங்களினை நாடுங்கள்.

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

### resolved\_end

இந்த DFAK வழிகாட்டலானது உங்களுக்கு பயனுள்ளதாய் அமைந்திருக்குமென நாம் நம்புகிறோம். உங்களது கருத்துக்களை பின்வரும் மின்னஞ்சலூடாகத் தெரிவியுங்கள்.guide [via email](mailto:incoming+rarenet-dfak-8220223-issue-@incoming.gitlab.com)

### இறுதிக் குறிப்புகள் final\_tips

தரவுகள் வெளியாதல் அபாயங்கள் மற்றும் அனுமதியளிக்கப்படாது உங்களது கணக்குகளினை கையாடல் போன்றவற்றினை தடுப்பதற்கான உதவிக்குறிப்புகளின் தொடரானது இங்கே காணப்படுகின்றது:

- ஒருபோதும் உங்களது சாதனத்தை பாராமுகமாய் விடாதீர்கள். உங்களால் அதனை எடுத்துச் செல்ல முடியவில்லையெனில் அதனை நிறுத்திவிட்டு பாதுகாப்பான ஒரு இடத்தில் வைத்து விட்டு செல்லுங்கள்.

- full-disk encryption இனை செயற்படுத்துங்கள்.

- உங்களது சாதனத்தினை மூடி வைப்பதற்கு பலமான ஒரு கடவுச்சொல்லினை பயன்படுத்துங்கள்.

- இயலுமான போதெல்லாம் Find/Erase My Phone பயன்பாட்டினை செயற்படுத்திவையுங்கள்,எனினும் அதற்கென பயன்படுத்தப்படும் மின்னஞ்சல் முகவரிகள் (Gmail/iCloud) கையாடப்பட்டால் உங்களது சாதனத்தை கண்காணிக்கவும் அதனை முற்றாக அழிக்கவும் இது பயன்படுத்தப்படலாம்.

#### மூலாதாரங்கள்

\* [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)