---

layout: page

title: "சந்தேகத்திற்கிடமான செய்திகள் எனக்கு கிடைக்கப்பெற்றன"

author: Abir Ghattas, Donncha Ó Cearbhaill, Claudio Guarnieri, Michael Carbone

language: en

summary: "சந்தேகத்திற்கிடமான செய்திகள்,இணைப்பு அல்லது மின்னஞ்சல் எனக்கு கிடைக்கப்பெற்றன, இது குறித்து நான் என்ன செய்வது?"

date: 2023-05

permalink: /en/topics/suspicious-messages

parent: Home

---

# சந்தேகத்திற்கிடமான செய்திகள் எனக்கு கிடைக்கப்பெற்றன

சந்தேகத்துக்கிடமான மின்னங்கால்களில் மிகவும் பிரபலமானது தகவல்திருட்டு மின்னஞ்சலாகும். எனினும் நீங்கள் சந்தேகத்துக்கிடமான செய்திகளினை சமூக வலைத்தள கணக்குகளிலிருந்தும்கூட பெற்றுக்கொள்ளுவீர்கள் .உங்களுடைய மின்னஞ்சல், சமூக வலைத்தள மற்றும்/அல்லது ஏனைய செய்திப்பரிமாறல் செயலிகளின் உட்பெட்டிக்குள் சந்தேகமான செய்திகள் வரலாம்.சந்தேகத்திற்கிடமான மின்னஞ்சலின் பொதுவானவடிவமானது பிஷ்ஷிங் (phishing) மின்னஞ்சல்களாகும்.இவை உங்களுடைய தனிப்பட்ட, நிதிசார்,அல்லது கணக்கு தொடர்பான தகவல்களினை நீங்களே வழங்குவதற்கு ஏமாற்றுவதே இதன் நோக்கமாகும்.இவர்கள் உங்களை போலியான வலைப்பக்கத்துக்கு செல்லவோ அல்லது போலியான வாடிக்கையாளர் சேவை இலக்கத்துடன் தொடர்புகொள்ளவோ கேட்பர். இந்த பிஷ்ஷிங் மின்னஞ்சல்கள் அதனை திறக்கும் வேளையில் தீங்கான மென்பொருட்களை சாதனத்தில் நிறுவி விடக்கூடிய இணைப்புகளினையும் கொண்டு காணப்படும்.

உங்களுக்கு வந்த செய்தியின் நம்பகத்தன்மை தொடர்பாக அல்லது என்ன செய்வதென்பது தொடர்பாக நிச்சயமல்லாது காணப்படும்போது இந்த நிலைமை தொடர்பாக மேலும் அறிந்துகொள்வதற்கு அல்லது வேறு நம்பகந்தகுந்த நிறுவனகளுக்கு அனுப்பி உங்களுடைய செய்தியின் விரிவான புகுப்பாய்வு செய்யப்பட்ட தகவலினைப் பெற்றுக்கொள்ள பின்வரும் கேள்விக்கொத்தினை வழிகாட்டற் கருவிகளாக பயன்படுத்தலாம்.

சந்தேகத்திற்கிடமான செய்திகளினைப் பெறும் எல்லாச் சந்தர்ப்பங்களிலும் உங்களுடைய கணக்கு தாக்கப்பட்டதாக கருத்தப்படமுடியாது என்பதனை மனதில் வைத்திருங்கள். எதாவது செய்தி அல்லது மின்னஞ்சல் சந்தேகத்திற்கிடமாக இருந்தால் அதனைத் திறக்க வேண்டாம். அதற்குப் பதிலளிக்க வேண்டாம், அதனுடன் இணைக்கப்பட்ட எதனையும் பதிவிறக்க வேண்டாம்.

## Workflow

### intro அறிமுகம்

அந்த செய்தி அல்லது இணைப்பில் ஏதாவது செயலைச் செய்தீர்களா?

- [நான் இணைப்பைக் கிளிக் செய்தேன்](#link-clicked)

- [விபரங்களினைப் பதிவிட்டேன்](#account-security\_end)

- [கோப்பினை தரவிறக்கம் செய்தேன்](#device-security\_end)

- [தகவலுடன் பதிலளித்தேன்](#reply-personal-info)

- [இதுவரை எந்த நடவடிக்கையும் எடுக்கவில்லை](#do-you-know-sender)

### do-you-know-sender அனுப்பியவரை உங்களுக்கு தெரியுமா?

அந்தச் செய்தி அனுப்பியவரை அடையாளம் கண்டுள்ளீர்ளா? அவதானமாக இருங்கள்,அந்த செய்தி அனுப்புனர் உங்களுக்கு நம்பகமான ஒருவர் போல தென்படலாம். [spoofed](https://en.wikipedia.org/wiki/Spoofing\_attack)

- [இது எனக்குத் தெரிந்த நபர் அல்லது நிறுவனம்](#known-sender)

- [இது ஒரு சேவை வழங்குநர் (மின்னஞ்சல்,சமூகத்தளங்கள் போன்றவை)](#service-provider)

- [செய்தியானது தெரியாத நபர் அல்லது நிறுவனத்திடமிருந்து அனுப்பப்பட்டுள்ளது](#share)

### known-sender தெரிந்த அனுப்புனர்

> வேறொரு தொடர்பாடல் முறைமையொன்றினூடாக அனுப்பினரை உங்களால் தொடர்புகொள்ள முடியுமா? உதாரணமாக,உங்களுக்கு ஒரு மின்னஞ்சல் வந்திருந்தால், சமிக்கை மூலமாக அனுப்பினரினை உங்களால் சரிபார்த்துக்கொள்ள முடியுமா? வாட்சாப் அல்லது தொலைபேசி? ஏற்கனவே உள்ள தொடர்பு முறையைப் பயன்படுத்துவதை உறுதிப்படுத்திக் கொள்ளுங்கள். சந்தேகத்திற்கிடமான செய்தியொன்றில் பட்டியலிடப்பட்டுள்ள இலக்கத்தினை நீங்கள் நம்ப வேண்டுமென்ற அவசியமல்ல.

அனுப்பியவர் தான் அந்த செய்தியை உங்களுக்கு அனுப்பினார் என்பதை உறுதிப்படுத்திக்கொண்டீர்களா?

- [ஆம்](#resolved\_end)

- [இல்லை](#share)

### service-provider சேவை வழங்குநர்

> இந்த சூழலில், சேவை வழங்குனரானது ஏதாவதொரு கம்பெனியாகவோ அல்லது நீங்கள் சந்தாசெய்த அல்லது நீங்கள் பயன்படுத்துகின்ற சேவையினை வழங்கும் ஒரு நிறுவனமாகவோ இருக்கும்.இந்த பட்டியலானது மின்னஞ்சல் வழங்குநர் (Google, Yahoo, Microsoft, ProtonMail...),சமூக வலைத்தளங்கள் வழங்குநர் , (Facebook, Twitter, Instagram...), அல்லது உங்களது நிதிசார் தகவல்களைக் கொண்டிருக்கின்ற தளங்களையோ(Paypal, Amazon, banks, Netflix...)கொண்டிருக்கலாம்.

>

> செய்தியின் உண்மைத் தன்மையினை கண்டறிய ஏதாவது வழிமுறைகளுண்டா? பல சேவை வழங்குநர்கள் உங்கள் கணக்குப்பக்கத்துக்கான அறிவிப்புக்கள் மற்றும் ஏனைய ஆவணங்காயினுடைய பிரதியினை வழங்குவர். உதாரணமாக செய்தியானது முகப்புத்தகத்திலிருந்து வந்திருந்தால் அது உங்களுடை அறிவிப்புக்களுக்களான மின்னஞ்சல் பட்டியலில் உள்ளடக்கப்பட்டிருக்கும் [list of notification emails](https://www.facebook.com/settings?tab=security&section=recent\_emails), அல்லது உங்களுடைய வங்கியிலிருந்து வந்திருந்தால் உங்களுடைய வாடிக்கையாளர் சேவைப் பிரிவுக்கு நீங்கள் அழைக்கலாம்.

கீழுள்ளவற்றிலொன்றை ஒன்றை தெரிவுசெய்யுங்கள்:

- [ எனது சேவை வழங்குநரிடமிருந்து இது முறையான செய்தி என்பதை என்னால் சரிபார்க்க முடிந்தது](#resolved\_end)

- [என்னால் சரிபார்க்க செய்தியை முடியவில்லை](#share)

- [நான் இந்த சேவைக்கு சந்தா (subscribe) செய்யவில்லை. மற்றும் அவர்களிடமிருந்து எவ்வித செய்டியையும் எதிர்பாக்கவில்லை](#share)

### link-clicked இணைப்பு சரிபார்க்கப்பட்டது

> சில சந்தேகத்துக்கிடமான செய்திகளில் காணப்படும் இணைப்புகளானது (links) உங்களுடைய தரவுகளை களவாடக்கூடிய பக்கங்களுக்கோ அல்லது உங்களது தனிப்பட்ட மற்றும் நிதிசார் தகவல்களை களவாடும் பக்கங்களுக்கோ அழைத்துச் செல்லக் கூடும். சில வேளைகளில் இந்த இணைப்புகளானது திறக்கும் வேளையில் தீங்கான மென்பொருட்களை சாதனத்தில் நிறுவி விடக்கூடிய இணைப்புகளினை பதிவிறக்க கோரும்.இந்த இணைப்புகளானது உங்களது சாதனத்தில் தீங்கான மென்பொருட்கள் மற்றும் ரகசியக்கண்காணிப்பு மென்பொருட்களைனைக் கொண்டு தாக்கத்தை ஏற்படுத்தவென வடிவமைக்கப்பட்ட வலைப்பக்கங்களுக்கு இட்டுச்செல்லும்.

அந்த இணைப்பினை அழுத்திய பிறகு என்ன நடந்தது என்பதை கூற முடியுமா?

- [எனது விபரங்களை உள்ளிட கேட்டது](#account-security\_end)

- [கோப்பு ஒன்றினை பதிவிறக்கம் செய்தது](#device-security\_end)

- [ஒன்றும் நடக்கவில்லை,எனினும் நான் உறுதியாகக் கூறவில்லை](#clicked-but-nothing-happened)

### clicked-but-nothing-happened அழுத்தினேன் எனினும் ஒன்றும் நடக்கவில்லை.

> நீங்கள் ஒரு சந்தேகமான இணைப்பினை அழுத்திய பின்னர் எவ்வித மாற்றத்தையும் அவதானிக்கவில்லை என்பதன் அர்த்தம் பின்னணியில் தீங்கான செயற்பாடுகள் எதுவும் இடம்பெறவில்லையென கருத முடியாது.நீங்கள் சிந்திக்க வேண்டிய சில விடயங்கள் காணப்படுகின்றன.நீங்கள் பெற்ற செய்தியானது விளம்பர நோக்கங்களுக்காகப் பயன்படுத்தப்பட்ட கழிவஞ்சல்கள் ஆகும். இதுபோன்ற சூழ்நிலையில், சில விளம்பரங்கள் தோன்றும். சில சமயங்களில் இந்த விளம்பரங்கள் தீங்கிழைக்கும் வகையிலும் இருக்கலாம்.

- [சில விளம்பரங்கள் தோன்றின, அவை தீங்கானதா இல்லையா என்பது குறித்து எனக்கு எனக்கு உறுதியாகத் தெரியவில்லை](#suspicious-device\_end)

> மோசமான சூழ்நிலையொன்றின்போது,இணைப்பில் அழுத்துவதாவது உங்களுடைய கணனியில் தீங்கான கட்டளை ஒன்றினை நிறைவேற்றுவதற்காக வாய்ப்பாக பயன்படுத்தப்படுகிறது. இது நடைபெற்றால்,அது உங்களுடைய உலாவியானது காலத்துக்கு பிற்பட்டதாக காணப்பட்டு இதனை தடுக்கமுடியாதவாறு நலிவுற்றதாக காணப்படுவதனாலாகும்.சில அரிதான சந்தர்ப்பங்களில் உங்கள் உலாவி காலத்துக்கு தகுந்ததாக புதுப்பித்த நிலையில் காணப்பட்டும் இது நடைபெற்றிருந்தால் காரணம் அறியமுடியாததாகும். இந்த இரு சந்தர்ப்பங்களிலும் உங்களது சாதனம் சந்தேகத்திற்கிடமான வகையில் செயலாற்றத் தொடங்கும்.

- [சில விளம்பரங்கள் பாப் அப். அவை தீங்கிழைக்கின்றனவா இல்லையா என்பது எனக்குத் தெரியவில்லை](#சந்தேகத்திற்குரிய சாதனம்\_முடிவு)

- [ஆம் எனது உலாவி புதுப்பித்த நிலையில் இல்லை மற்றும்/அல்லது நான் இணைப்பைக் கிளிக் செய்த பிறகு எனது சாதனம் சந்தேகத்திற்குரிய வகையில் செயல்படத் தொடங்கியது](#suspicious-device\_end)

> வேறு சூழ்நிலைகளில், இந்த இணைப்பிற்குச் சென்று பார்வையிடுவதானால் குறுக்குத் தள தாக்குதலுக்குள்ளாகுவீர்கள் [cross-site script attack (or XSS)](https://en.wikipedia.org/wiki/Cross-site\_scripting).இந்த தாக்குதலின் விளைவானது நீங்கள் பார்வையிட்ட வலைத்தளங்களில் உங்களை அங்கீரிக்கவெனப் பயன்படுத்தப்பட்ட cookie திருடப்படும்.எனவே தாங்குதல் காரர் உங்களது பயனாளி பெயரினை (user name) வைத்து தளங்களினுள் நுழையலாம். அந்த தளத்தினிடைய பாதுகாப்பினைப் பொறுத்து குறித்த தாக்குதல் தாறன் கடவுச்சொல்லினை மாற்றவும் மாற்ற முடியாமலும் இருக்கும். குறித்த வலைத்தளமானது XSS இற்கு நலிவுடையதாக காணப்படின் தாக்குதல் காரன் உங்களது வலைத்தளத்துக்கு தன்னை நிர்வாகியாக (admin) மாற்றக்கூடியதால் நிலமை இன்னும் தீவிரமானதாக அமையும். XSS தாக்குதலை அடையாளம் காணவும்,நீங்கள் அழுத்திய இணைப்பில் XSS காணப்படுகின்றதா என்பதனை சரிபாருங்கள்.[script string](https://owasp.org/www-community/attacks/xss/). இதை HEX அல்லது unicode இலும் குறியாக்கம் செய்யலாம்.

- [அந்த இணைப்பில் script காணப்படுகிறதா அல்லது இது பகுதியளவு குறியாக்கம் (partially encoded செய்யப்பட்டுள்ளதா)](#cross-site-script)

- [எவ்வித script உம் அடையாளம் காணப்படவில்லை](#suspicious-device\_end)

### cross-site-script 1

நீங்கள் பார்த்த தளமானது நீங்கள் கணக்கொன்றினை வைத்திருக்கும் தளமா?

- [ஆம்](#account-security\_end)

- [இல்லை](#cross-site-script\_2)

நீங்கள் சென்றுமுடித்த தளம் நீங்கள் நிர்வகிக்கும் ஒரு தளத்தில் உள்ளதா?

- [ஆம்](#cross-site-script-admin-compromised)

- [இல்லை](#cross-site-script\_3)

### cross-site-script-admin-compromised

> இச்சூழ்நிலையில், தாக்குபவர் உங்கள் நிர்வாகி கணக்கை அணுக அனுமதிக்கும் வலிதான cookie யினைக் கொண்டிருக்கலாம். முதல் நோக்கம், உங்கள் நிர்வாக இடைமுகத்தில் (interface) உள்நுழைந்து செயற்பாட்டிலுள்ள உள்ள எந்த அமர்வையும் (session) அழிக்கவும் அல்லது கடவுச்சொல்லை மாற்றுதலுமாகும். மேலும், தாக்குபவர் உங்கள் தளத்தில் ஏதேனும் கலைப்பொருட்களைப் பதிவேற்றியிருக்கிறார்களா மற்றும்/அல்லது ஏதேனும் தீங்கிழைக்கும் உள்ளடக்கத்தை இடுகையிட்டாரா என்பதை நீங்கள் சரிபார்க்க வேண்டும், அவ்வாறெனில் அதனை நீக்கவும்.

பின்வரும் நிறுவனங்கள் இதுபோன்ற சம்பவங்களை விசாரித்து பதிலளிப்பதற்கு உதவும்:

:[](organisations?services=forensic)

### cross-site-script\_3

> இது நன்மையானது. எவ்வாறிருப்பினும், சில அரிதான சந்தர்ப்பங்களில்,XSS ஆனது வேறு சில தாக்குதல்களை மேற்கொள்ள உங்களது உலாவியினைப் பயன்படுத்துவதற்காகவும் பயன்படுத்தப்படலாம்.

- [எனது சாதனம் பாதிக்கப்பட்டுள்ளதா என மதிப்பீடு செய்ய விரும்புகிறேன்](../../../device-acting-suspiciously)

- [நான் நன்றாக உள்ளேன் என நினைக்கிறேன்](#final\_tips)

### reply-personal-info

> நீங்கள் பகிர்ந்த செய்தியின் தன்மையினைப் பொறுத்து உடனடியான நடவடிக்கைகள் மேற்கொள்ள வேண்டும்.

எப்படிப்பட்ட தகவல்களினை பகிர்ந்திருந்தீர்கள்?

- [கணக்குகளுடன் தொடர்புடைய ரகசியமான தகவல்கள் பகிர்ந்தேன்](#account-security\_end)

- [பொதுத் தகவல்களினைப் பகிர்ந்தேன்](#share)

- [தகவளினுடைய முக்கியத்துவம் குறித்து எனக்கு தெரியவில்லை, எனக்கு உதவிகள் தேவைப்படுகின்றன. help](#help\_end)

### share பகிர்தல்

> சந்தேகத்துக்கிடமான செய்திகளினைப் பகிர்தலானது உங்களது சமுதாயம் மற்றும் சகபாடிகள் பாதிக்கப்படுவதிலிருந்து தடுக்க உதவும்.செய்தி ஆபத்தானதாக இருந்தால் உங்களுக்கு ஆலோசனை வழங்க நீங்கள் நம்பும் ஒருவரை உதவிக்கு அணுகலாம். செய்திகளினை பகுப்பாய்வு செய்யக்கூடிய நிறுவங்களிடம் பகிர்வது தொடர்பாகவும் ஜோசியுங்கள்.

>

> சந்தேகமான செய்திகளினைப் பகிர, அதன் அனுப்புநர் தொடர்பான தகவலினையும் சேர்த்திருப்பதை உறுதிசெய்துகொள்ளுங்கள். அந்த செய்தி ஓரு மின்னஞ்சலாக காணப்பட்டால் பின்னரும் வழிகாட்டலினைப் பயன்படுத்தி தலைப்பு (headers) உட்பட முழு மின்னஞ்சலினையும் உள்ளடக்கியிருப்பதனை உறுதிசெய்து கொள்ளுங்கள்.[ guide by the Computer Incident Response Center Luxembourg (CIRCL)](https://www.circl.lu/pub/tr-07/).

உங்களுக்கு மேலதிக உதவிகள் தேவைப்படுகின்றனவா?

- [ஆம்,எனக்கு மேலதிக உதவிகள் தேவைப்படுகின்றன](#help\_end)

- [இல்லை,எனது பிரச்சினைகளைத் தீர்த்து விட்டேன்](#resolved\_end)

### device-security\_end

> உங்கள் சாதனத்தில் சில கோப்புகள் பதிவிறக்கம் செய்யப்பட்டிருந்தால், உங்கள் சாதனம் ஆபத்தில் இருக்கக்கூடும்!

தயவுசெய்து உங்களுக்கு உதவி செய்யக்கூடிய கீழுள்ள நிறுவனங்களை தொடர்புகொள்ளுங்கள். பின்னர், சந்தேகமான செய்திகளைப் பகிருங்கள். [share your suspicious message](#share).

:[](organisations?services=device\_security)

### account-security\_end

> உங்களது விபரங்களை நீங்கள் உள்ளிட்டிருந்தால், அல்லது நீங்கள் குறுக்குத்- தள தாக்குதலுக்குட்பட்டிருந்தால் (cross-site script attack)உங்களது கணக்கு ஆபத்திலிருக்கக் கூடும்!

>

> உங்களுடைய கணக்கு தாக்கப்பட்டுள்ளதாக நீங்கள் எண்ணினால், பாதிக்கப்பட்ட கணக்குகள் தொடர்பான டிஜிட்டல் பாதுகாப்பு பொதியினுடைய compromised accounts பகுதியினுடைய சொற்கோவையினை பின்பற்ற பரிந்துரைக்கிறோம்.[compromised accounts](../../../account-access-issues).

>

> இந்த ஃபிஷிங் பிரச்சாரத்தைப் பற்றி உங்கள் சமூகத்திற்கும் தெரிவிக்கவும், மேலும் சந்தேகத்திற்குரிய செய்தியை அவற்றை பகுப்பாய்வு செய்யக்கூடிய நிறுவனங்களுடன் பகிரவும் பரிந்துரைக்கிறோம்.

உங்களுக்கு கிடைக்கப்பெற்ற செய்தியின் தகவல்களை பகிர்ந்துகொள்ள விரும்புகிறீர்களா? அல்லது அதற்கு முன்னர் மேலதிக உதவிகள் பெற விரும்புகிறீர்களா?

- [சந்தேகத்திற்கிடமான செய்திகளை நான் பகிர வேண்டும்](#share)

- [எனது கணக்கினை பாதுகாத்துக்கொள்ள எனக்கு மேலதிக உதவிகள் தேவை](#account\_end)

- [செய்தியினை பகுப்பாய்வு செய்வதற்கு எனக்கு மேலதிக உதவிகள் தேவை](#analysis\_end)

### suspicious-device\_end

> நீங்கள் ஒரு இணைப்பினை அழுத்திவிட்டு என்ன நடந்தது என்பது தொடர்பாக உறுதியாக இல்லாதவிடத்து, உங்களது அறிவுக்கு எட்டாமலே உங்களது சாதனம் தாக்கப்பட்டிருக்கலாம். இதனை கண்டறியவோ அல்லது உங்களது சாதனம் தாக்கப்பட்டிருக்கலாம் என நீங்கள் எண்ணினாலோ பின்வரும் செயற்பாட்டிற்குச் செல்லுங்கள் ["My device is acting suspiciously"](../../../device-acting-suspiciously).

உங்கள் சாதனம் சந்தேகத்திற்கிடமான முறையில் செயல்படுவதால் உங்களுக்கு உடனடி உதவி தேவைப்பட்டால், உங்களுக்கு ஆதரவளிக்கும் நிறுவனங்களை நீங்கள் தொடர்பு கொள்ளலாம். பின்னர் தயவுசெய்து [உங்கள் சந்தேகத்திற்குரிய செய்தியைப் பகிரவும்](#பகிர்வு).

:[](organisations?services=device\_security)

### help\_end

> நீங்கள் பகிரும் தகவலிலுள்ள அபாயங்களை நன்கு புரிந்துகொள்ள உங்கள் சக பணியாளர்கள் அல்லது பிறரிடம் உதவி பெற வேண்டும். உங்கள் நிறுவனத்தில் அல்லது வலையமைப்பினுள் உள்ள வேறு பணியாளர்களும் இதே போன்ற கோரிக்கைகளைப் பெற்றிருக்கலாம்.

தயவுசெய்து உங்களுக்கு உதவி செய்யக்கூடிய கீழுள்ள நிறுவனங்களை தொடர்புகொள்ளுங்கள். பின்னர், சந்தேகமான செய்திகளைப் பகிருங்கள்.[share your suspicious message](#share).

:[](organisations?services=digital\_support)

### account\_end

உங்களுடைய கணக்கானது தாக்கப்பட்டு அதனைப் பாதுக்காக்க உங்களுக்கு உதவிகள் தேவைப்படுமெனின், கேழே தரப்பற்றுள்ள உங்களுக்கு உதவக்கூடிய நிறுவனகளை நாடுங்கள்.

:[](organisations?services=account)

### analysis\_end

பின்வரும் நிறுவங்கள் சந்தேகத்திற்கிடமான செய்திகளினை ஏற்று உங்களுக்காக மேலதிக விசாரணைகளினச் செய்வர்:

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

### resolved\_end

இந்த DFAK ஆனது பயனுள்ளதாக அமைந்திருக்கும் என நம்புகிறோம்: உங்களுடைய பின்னூட்டல்களுக்கு [மின்னஞ்சலூடாக](mailto:incoming+rarenet-dfak-8220223-issue-@incoming.gitlab.com).

### இறுதிக் குறிப்புகள்

நினைவிற்கொள்ள வேண்டிய முதலாவது விதி: மின்னஞ்சல்களில் எவ்விதமான தனிப்பட்ட தகவல்களையும் வழங்கக் கூடாது. எந்த ஒரு நிறுவனமோ வங்கியோ இந்த தகவல்களை மின்னஞ்சலூடாக ஒருபோதும் கோரமாட்டார்கள். ஒரு மின்னஞ்சல் அல்லது வலைப்பக்கம் சட்டபூர்வமானதா இல்லையா என்பதை எல்லா வேளையிலும் கூறுவதென்பது கடினமானதாகும் எனினும், நீங்கள் பெற்ற மின்னஞ்சல் தொடர்பாக மதிப்பீடு செய்வதற்கு சில குறிப்புகள் உதவியாய் அமையும்.

\* அவசர தன்மை: சந்தேகத்திற்கிடமான மின்னஞ்சல்கள் பொதுவாக ஏற்படக்கூடிய திடீர் மாற்றங்கள் குறித்த எச்சரித்து உங்களது கணக்கினை உறுதிப்படுத்த உடனடியாக செயலாற்றும்படி கோரும்.

\* மின்னஞ்சலின் “உடல்-(body” பாகத்தில் உங்களது கணக்கினை “உறுதிப்படுத்த” அல்லது “மேம்படுத்தவோ கோரி” (“update your account” அல்லது “உங்களுடைய பதிவுகளை மேம்படுத்தாவிடில் கணக்கு இடைநிறுத்தம் செய்யப்படும்” என்ற கேள்விகள் காணப்படும். உங்கள் தகவலை நீங்கள் வழங்கிய எந்த நம்பகமான நிறுவனமும் அதை மீண்டும் உள்ளிடுமாறு உங்களைக் கேட்காது என்று கருதுவது பொதுவாக பாதுகாப்பானது, எனவே இந்த சூழ்ச்சியில் விழ வேண்டாம்.

\* உரிமை கோரப்படாத செய்திகள், இணைப்புகள், கோப்புகள், உள்நுழைவுப் பக்கங்கள் தொடர்பாக விழிப்பாயிருங்கள்.

\* எழுத்துப்பிழைகள், மற்றும் இலக்கணப்பிழைகள் தொடர்பாக அவதானியுங்கள்.

\* மின்னஞ்சலில் வெளியே தெரியப்படுத்தியுள்ள பெயர் மட்டுமல்லாது அனுப்பியவரது முழு முகவரியினையும் தெரிந்துகொள்ள click செய்யுங்கள்.

\* குறிக்கப்பட்ட இணைப்புகள் தொடர்பாக அவதானமாக இருங்கள் - அதனது இறுதி இடத்தினை பரிசீலிக்க முடியாததனால் இவை தீங்கான இணைப்புகளை அதற்குபின்னாக கொண்டிருக்கலாம்.

\* உங்கள் சுட்டியை ஒரு இணைப்பின் மீது நகர்த்தும்போது, நீங்கள் அனுப்பப்படும் உண்மையான URL ஒரு popup இல் அல்லது உங்கள் உலாவியின் கீழ்ப்பகுதியில் காட்டப்படும்.

\* "from:" உட்பட மின்னஞ்சலுடைய தலைப்புகள் (headers) ஒரு சட்டபூர்வமான ஒரு மின்னஞ்சலைப் போல தோன்றும் வகையில் வடிவமைக்கப்படலாம். SPF மற்றும் DKIM தலைப்புகளினை ஆராய்வதன்மூலம் அனுப்பிய நபரினுடைய டொமைன் சார்பாக மின்னஞ்சலினை அனுப்புவதற்கு அந்த IP address க்கு அனுமதி வழங்கப்பட்டுள்ளாதா இல்லையா என்பதனையும் , மற்றும் தலைப்பு அல்லது உள்ளடக்கங்கள் ஏதாவது இடையில் மாற்றப்பட்டுள்ளதா என்பதனையும் கூறலாம். ஒரு சட்டபூர்வமான மின்னஞ்சலின் SPF [SPF](https://dmarcly.com/blog/how-to-implement-dmarc-dkim-spf-to-stop-email-spoofing-phishing-the-definitive-guide#what-is-spf) மற்றும் DKIM [DKIM](https://dmarcly.com/blog/how-to-implement-dmarc-dkim-spf-to-stop-email-spoofing-phishing-the-definitive-guide#what-is-dkim) பெறுமானங்களானவை எப்போதுமே “சித்தி -'PASS' ஆக காணப்பட வேண்டும்,இல்லாவிடில் அது நம்பகமற்ற மின்னஞ்சலாகும்.காரணம் அந்த மின்னஞ்சலானது பாசாங்கு செய்யப்பட்டதாக அல்லது சில அரிதான சந்தர்ப்பங்களில் மின்னஞ்சலுடைய சேவகம் முறையாக உள்ளமைக்கப்படாமையின் காரணமாக இருக்கும்.

\* டிஜிட்டல் ஒப்பங்களானவை [Digital signatures](https://www.gnupg.org/gph/en/manual/x135.html) குறித்த மின்னஞ்சலானது சட்டபூர்வமான அனுப்புநரால் அனுப்பப்பட்டுள்ளதா அல்லது இடையில் மாற்றியமைக்கப்பட்டிருக்கின்றதா என்பதனைக் கூறும். மின்னஞ்சலில் ஒப்பம் காணுப்படுமாயின் அது உறுதிப்படுத்தப்பட்ட ஒப்பமா அல்லது இல்லையா என்பதனை பரிசோதியுங்கள்.கையொப்பத்தை உறுதிப்படுத்திக்கொள்ள, உங்களுக்கு OpenPGP மற்றும் செய்தியின் கையொப்பத்தில் உள்ள ID உடன் தொடர்புடைய பொது விசை தேவைப்படும். டிஜிட்டல் ஒப்பத்தினை ஆதரிக்கின்ற பெரும்பாலானவை தங்களது interface இனை பயன்படுத்தி குறித்த ஒப்பம் உறுதிப்படுத்தப்பட்டதா இல்லையா என்பதனை தானியங்கி முறையிலேயே வழங்குகின்றன.

\* ஒரு பாதிப்புக்குள்ளான கணக்கானது மேலுள்ள நிபந்தனைகள் அனைத்தையும் உறுதிசெய்து சட்டப்பூர்வமானதாக தோன்றுகிற ஒரு தீங்கான மின்னஞ்சலினை அல்லது செய்தியினை அனுப்பலாம். எனினும்,செய்தியினுடைய உள்ளடக்கமானது வழமைக்கு மாறானதாகக் காணப்படும்.மின்னஞ்சல் செய்தியின் உள்ளடக்கம் வித்தியாசமானதாகத் தோன்றினால், எந்த நடவடிக்கையும் எடுப்பதற்கு முன், சட்டப்பூர்வ அனுப்புநரைத் வேறு வழியின் மூலம் தொடர்புகொண்டு சரிபார்ப்பது எப்போதும் நல்லது.

\* உங்களுடைய மின்னஞ்சலினை எப்போதுமே எளிய வடிவில் (plain text) வைத்து வாசித்தல் நல்ல பழக்கமாகும். HTML வடிவில் காணப்படும் மின்னஞ்சல்கள் தீங்கான கோவைகள் மற்றும் URL இனை மறைக்கக்கூடியவாறு காணப்படலாம். பல்வேறுபட்ட மின்னஞ்சல்களில் எவ்வாறு HTML செயலிழப்பு (Disable) செய்வது என்ற ஆலோசனைகளுக்கு [this post](https://www.maketecheasier.com/read-email-in-plain-text/ )

\* உங்களது கணனி அல்லது தொலைபேசியில் இயங்குதளத்தின்(operating system)அண்மையான பதிப்பினை (latest version) பயன்படுத்துங்கள். (அண்மைய பதிப்புகளுக்கு [Android](https://en.wikipedia.org/wiki/Android\_version\_history), [iOS](https://en.wikipedia.org/wiki/IOS\_version\_history), [macOS](https://en.wikipedia.org/wiki/MacOS\_version\_history) and [Windows](https://en.wikipedia.org/wiki/Microsoft\_Windows)).

\* உங்களுடைய இயங்குதளம் மற்றும் நீங்கள் நிறுவியுள்ள அனைத்து விதமான செயலிகள் குறிப்பாக தகவல்களைப் பரிமாறக்கூடிய செயலிகள் (உலாவிகள்,செய்திப்பரிமாறல் செயலிகள்,மின்னஞ்சல்) போன்றவற்றை முடியுமான அளவு விரைவாக புதுப்பித்துக்கொள்ளுங்கள். உங்களுக்குத் தேவையற்ற செயலிகள் போன்றவற்றை அகற்றிவிடுங்கள்.

\* நம்பகமான உலாவியை பயன்படுத்துங்கள் (e.g. Mozilla Firefox). உங்க உலாவியில் நிறுவப்பட்டுள்ள extensions/add-ons இனை மீளாய்வு செய்வதன்மூலம் உலாவியின் பாதுகாப்பினை அதிகரித்துக்கொள்ளுங்கள்.நம்பகமானவற்றை மட்டும் வைத்திருங்கள். (உதாரணமாக:[Privacy Badger](https://privacybadger.org/), [uBlock Origin](https://ublockorigin.com), [Facebook Container](https://addons.mozilla.org/en-US/firefox/addon/facebook-container/), [Cookie AutoDelete](https://github.com/Cookie-AutoDelete/Cookie-AutoDelete), [NoScript](https://noscript.net/)).

.

\* உங்கள் தகவல்களினை வழமையாக காப்பு பிரதிகள் செய்வதனை உறுதிப்படுத்திக்கொள்ளுங்கள்.

\* உங்களுடைய கணக்கினை பலமான கடவுச்சொற்கள், இருகாரணி உறுதிப்படுத்தல்கள் மற்றும் பாதுகாப்பான அமைப்புகளினைக் கொண்டு பாதுகாத்துக் கொள்ளுங்கள்.

#### Resources மூலாதாரங்கள்

சந்தேகத்திற்கிடமான செய்திகளைக் கண்டறிதல் மற்றும் ஃபிஷ் செய்யப்படுவதைத் தவிர்ப்பதற்கான பல ஆதாரங்கள் இங்கே உள்ளன.

\* [Citizen Lab: Communities at risk - Targeted Digital Threats Against Civil Society](https://targetedthreats.net)

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

\* [Security Without Borders: Guide to Phishing](https://guides.securitywithoutborders.org/guide-to-phishing/)