---

layout: page

title: " මට සැක සහිත පණිවිඩයක් ලැබුණි "

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

language: en

summary: " මට සැක සහිත පණිවිඩයක්, සබැඳියක් හෝ විද්‍යුත් තැපෑලක් ලැබුණි, මම ඒ ගැන කුමක් කළ යුතුද?"

date: 2023-05

permalink: /en/topics/suspicious-messages

parent: Home

---

මට සැක සහිත පණිවිඩයක් ලැබුණා

සැක සහිත ඊමේල් වල වඩාත් සුලභ ආකාරය වන්නේ තතුබෑම් ඊමේල් ය, නමුත් ඔබට සමාජ මාධ්‍ය ගිණුම් සහ/හෝ පණිවිඩ යැවීමේ යෙදුම් වෙතද \_සැක සහිත\_ පණිවිඩ ලැබෙනු ඇත. තතුබෑම් පණිවිඩවල අරමුණ වන්නේ ඔබේ පුද්ගලික, මූල්‍ය හෝ ගිණුම් තොරතුරු අත්හැරීමට ඔබව රැවටීමයි. ව්‍යාජ වෙබ් අඩවියකට පිවිසීමට හෝ ව්‍යාජ පාරිභෝගික සේවා අංකයක් ඇමතීමට ඔවුන් ඔබෙන් ඉල්ලා සිටිය හැක. තතුබෑම් පණිවිඩ විවෘත කළ විට ඔබේ පරිගණකයේ අනිෂ්ට මෘදුකාංග ස්ථාපනය කරන ඇමුණුම් ද අඩංගු විය හැක.

ඔබට ලැබුණු පණිවිඩයේ සත්‍යතාව පිළිබඳව හෝ ඒ සම්බන්ධයෙන් කළ යුත්තේ කුමක්ද යන්න පිළිබඳව ඔබට විශ්වාසයක් නොමැති නම්, තත්වය තවදුරටත් හඳුනා ගැනීමට හෝ ඔබට ලබා දෙන බාහිර විශ්වාසදායක සංවිධාන සමඟ පණිවිඩය බෙදා ගැනීමට මාර්ගෝපදේශක මෙවලමක් ලෙස ඔබට පහත ප්‍රශ්නාවලිය භාවිතා කළ හැකිය. ඔබගේ පණිවිඩය පිළිබඳ වඩාත් සවිස්තරාත්මක විශ්ලේෂණයක්.

සැක සහිත විද්‍යුත් තැපෑලක් ලැබීමෙන් ඔබේ ගිණුම අවදානමට ලක්ව ඇති බවක් අදහස් නොවන බව මතක තබා ගන්න. විද්‍යුත් තැපෑලක් හෝ පණිවිඩයක් සැක සහිත යැයි ඔබ සිතන්නේ නම්, එය විවෘත නොකරන්න. පණිවිඩයට පිළිතුරු නොදෙන්න, කිසිදු සබැඳියක් ක්ලික් නොකරන්න, සහ කිසිදු ඇමුණුමක් බාගත නොකරන්න.

## වැඩ ප්‍රවාහය

### හැඳින්වීම

ඔබ පණිවිඩය හෝ සබැඳිය මත කිසියම් ක්‍රියාවක් කර තිබේද?

- [මම සබැඳියක් ක්ලික් කළෙමි](#link-clicked)

- [මම අක්තපත්‍ර ඇතුළු කළෙමි](#ගිණුම්-ආරක්ෂක\_අවසානය)

- [මම ගොනුවක් බාගත කළෙමි](#උපාංග-ආරක්ෂක\_අවසානය)

- [මම තොරතුරු සමඟ පිළිතුරු දුන්නා](#පිළිතුරු-පුද්ගලික-තොරතුරු)

- [මම තවම කිසිදු ක්‍රියාමාර්ගයක් ගෙන නැත](#ඔබ-දන්න-යවන්නා)

### ඔබ-දන්නා-යවන්නා

පණිවිඩය යවන්නා ඔබ හඳුනා ගන්නවාද? පණිවිඩය යවන්නා ඔබ විශ්වාස කරන කෙනෙකු ලෙස පෙනී සිටීමට [spoofed](https://en.wikipedia.org/wiki/Spoofing\_attack) විය හැකි බව මතක තබා ගන්න.

- [එය මා දන්නා පුද්ගලයෙකු හෝ සංවිධානයකි](#දන්නා-යවන්නා)

- [එය සේවා සපයන්නා (ඊමේල් සපයන්නා, සත්කාරක, සමාජ මාධ්‍ය හෝ බැංකුව වැනි)](#සේවා සපයන්නා)

- [පණිවිඩය යවා ඇත්තේ නොදන්නා පුද්ගලයෙකු හෝ සංවිධානයක් විසිනි](#share)

### දන්නා-යවන්නා

> වෙනත් සන්නිවේදන නාලිකාවක් භාවිතයෙන් ඔබට යවන්නා වෙත ළඟා විය හැකිද? උදාහරණයක් ලෙස ඔබට විද්‍යුත් තැපෑලක් ලැබුනේ නම්, ඔබට එය යවන්නා සමඟ Signal, WhatsApp හෝ දුරකථනය මගින් සෘජුවම සත්‍යාපනය කළ හැකිද? පවතින සම්බන්ධතා ක්‍රමයක් භාවිතා කිරීමට වග බලා ගන්න. සැක සහිත පණිවිඩයේ ලැයිස්තුගත කර ඇති දුරකථන අංකයක් ඔබට අනිවාර්යයෙන්ම විශ්වාස කළ නොහැක.

ඔබට මෙම පණිවිඩය එවූ තැනැත්තා යවන්නා බව ඔබ තහවුරු කළාද?

- [ඔව්](#විසඳුණු\_අවසානය)

- [නැහැ](#බෙදාගන්න)

### සේවා සපයන්නා

> මෙම අවස්ථාවෙහිදී, සේවා සපයන්නා යනු ඔබ භාවිතා කරන හෝ දායක වී ඇති සේවාවන් සපයන ඕනෑම සමාගමක් හෝ සන්නාමයකි. මෙම ලැයිස්තුවට ඔබේ විද්‍යුත් තැපැල් සපයන්නා (Google, Yahoo, Microsoft, ProtonMail...), ඔබේ සමාජ මාධ්‍ය සපයන්නා (Facebook, Twitter, Instagram...) හෝ ඔබේ මූල්‍ය තොරතුරු ඇති සබැඳි වේදිකා (Paypal, Amazon, බැංකු,) අඩංගු විය හැක. Netflix...).

>

> පණිවිඩය සත්‍ය දැයි පරීක්ෂා කිරීමට ඔබට ක්‍රමයක් තිබේද? බොහෝ සේවා සපයන්නන් ඔබගේ ගිණුම් පිටුවේ දැනුම්දීම් හෝ වෙනත් ලේඛනවල පිටපත් ද ලබා දෙනු ඇත. උදාහරණයක් ලෙස, පණිවිඩය Facebook වෙතින් නම්, එය ඔබගේ [දැනුම්දීම් ඊමේල් ලැයිස්තුවේ](https://www.facebook.com/settings?tab=security&section=recent\_emails) හෝ එය ඔබගේ බැංකුවෙන් නම්, ඇතුළත් කළ යුතුය. ඔබට ඔබේ පාරිභෝගික සේවය ඇමතිය හැක.

පහත විකල්ප වලින් එකක් තෝරන්න:

- [එය මගේ සේවා සපයන්නාගේ නීත්‍යානුකූල පණිවිඩයක් බව සත්‍යාපනය කිරීමට මට හැකි විය](#resolved\_end)

- [මට පණිවිඩය සත්‍යාපනය කිරීමට නොහැකි විය](#බෙදා ගන්න)

- [මම මෙම සේවාවට දායක නොවෙමි සහ/හෝ ඔවුන්ගෙන් පණිවිඩයක් බලාපොරොත්තු වෙමි](#share)

### සබැඳිය-ක්ලික් කළා

> සමහර සැක සහිත පණිවිඩවල, සබැඳි ඔබට ඔබේ අක්තපත්‍ර හෝ ඔබේ පුද්ගලික හෝ මූල්‍ය තොරතුරු සොරකම් කළ හැකි වෙනත් ආකාරයේ පිටු සොරකම් කරන ව්‍යාජ පිවිසුම් පිටු වෙත ඔබව රැගෙන යා හැක. සමහර විට, විවෘත කළ විට ඔබේ පරිගණකයේ අනිෂ්ට මෘදුකාංග ස්ථාපනය කරන ඇමුණුම් බාගත කිරීමට සබැඳිය ඔබෙන් ඉල්ලා සිටිය හැක. සබැඳිය මඟින් ඔබව අනිෂ්ට හෝ ඔත්තු බැලීමේ මෘදුකාංගයකින් ඔබේ උපාංගයට ආසාදනය කිරීමට උත්සාහ කළ හැකි විශේෂයෙන් සකස් කළ වෙබ් අඩවියකට ඔබව රැගෙන යා හැක.

ඔබ සබැඳිය ක්ලික් කිරීමෙන් පසු සිදුවූයේ කුමක්දැයි ඔබට පැවසිය හැකිද?

- [එය අක්තපත්‍ර ඇතුළත් කිරීමට මගෙන් ඉල්ලා සිටියේය](#ගිණුම්-ආරක්ෂක\_අවසානය)

- [එය ගොනුවක් බාගත කර ඇත](#උපාංගය-ආරක්ෂක\_අවසානය)

- [කිසිවක් සිදුවී නැත, නමුත් මට විශ්වාස නැත](#ක්ලික් කළ නමුත්-කිසිවක් සිදු නොවීය)

### ක්ලික් කළ නමුත් කිසිවක් සිදු නොවීය

> ඔබ සැක සහිත සබැඳියක් ක්ලික් කළ නිසා සහ ඔබ අමුතු හැසිරීමක් නොදැක්කා සේ කිසිදු ද්වේෂසහගත ක්‍රියාවක් පසුබිමේ සිදු නොවූ බව අදහස් නොවේ. ඔබ සිතා බැලිය යුතු අවස්ථා කිහිපයක් තිබේ. අවම වශයෙන් අදාළ වන්නේ ඔබට ලැබුණු පණිවිඩය වෙළඳ දැන්වීම් අරමුණු සඳහා භාවිතා කරන ලද අයාචිත තැපැල් ය. මෙම අවස්ථාවේදී සමහර දැන්වීම් මතු වී තිබිය හැක. සමහර අවස්ථාවලදී මෙම දැන්වීම් අනිෂ්ට විය හැකිය.

>

> නරකම අවස්ථාවක, සබැඳිය ක්ලික් කිරීමෙන් ඔබේ පද්ධතියේ අනිෂ්ට විධානයක් ක්‍රියාත්මක කිරීමට සූරාකෑමක් සිදු විය. මෙය සිදු වූයේ නම්, මෙය ඔබගේ බ්‍රවුසරය යාවත්කාලීන නොවීම සහ මෙම සූරාකෑමට ඉඩ දෙන අවදානමක් තිබීම නිසා විය හැක. ඔබ බ්‍රවුසරය යාවත්කාලීන වූ විට සහ මෙම තත්ත්වය සිදු වූ දුර්ලභ අවස්ථාවන්හිදී, සූරාකෑමට ලක් වූ අවදානම දැනගත නොහැක. අවස්ථා දෙකේදීම, ඔබගේ උපාංගය සැක සහිත ලෙස ක්‍රියා කිරීමට පටන් ගත හැක.

> වෙනත් අවස්ථා වලදී, මෙම සබැඳිය වෙත පිවිසීමෙන් ඔබ [හරස් අඩවියේ ස්ක්‍රිප්ට් ප්‍රහාරයකට (හෝ XSS)](https://en.wikipedia.org/wiki/Cross-site\_scripting) ගොදුරක් වී තිබිය හැක. මෙම ප්‍රහාරයේ ප්‍රතිඵලය වනුයේ ඔබ පිවිසි වෙබ් අඩවියට ඔබව සත්‍යාපනය කිරීමට භාවිතා කරන ඔබේ කුකිය සොරකම් කිරීමයි, එබැවින් ප්‍රහාරකයාට ඔබේ පරිශීලක නාමය සමඟ වෙබ් අඩවියට ඇතුළු වීමට හැකි වනු ඇත. අඩවියේ ආරක්ෂාව මත, ප්රහාරකයාට මුරපදය වෙනස් කිරීමට හෝ නොහැකි වීමට ඉඩ ඇත. XSS වලට ගොදුරු විය හැකි වෙබ් අඩවිය ඔබ කළමනාකරණය කරන වෙබ් අඩවියක් නම් මෙය වඩාත් බරපතල වේ, මන්ද එවැනි අවස්ථාවලදී ප්‍රහාරකයාට ඔබේ වෙබ් අඩවියේ පරිපාලක ලෙස සත්‍යාපනය කිරීමට හැකි වනු ඇත. XSS ප්‍රහාරයක් හඳුනා ගැනීම සඳහා, ඔබ ක්ලික් කළ සබැඳියේ [script string] (https://owasp.org/www-community/attacks/xss/) අඩංගු දැයි පරීක්ෂා කරන්න. මෙය HEX හෝ Unicode වලින්ද කේතනය කළ හැක.

- [සමහර දැන්වීම් මතු විය. ඒවා අනිෂ්ටද නැද්ද යන්න මට විශ්වාස නැත](#සැක සහිත-උපාංග\_අවසන්)

- [ඔව් මගේ බ්‍රවුසරය යාවත්කාලීන නොවේ සහ/හෝ මම සබැඳිය ක්ලික් කළ පසු මගේ උපාංගය සැක සහිත ලෙස ක්‍රියා කිරීමට පටන් ගත්තේය](#සැක සහිත-උපාංග\_අවසන්)

- [සබැඳිය තුළ ස්ක්‍රිප්ට් එකක් තිබේ හෝ එය අර්ධ වශයෙන් කේතනය කර ඇත](#හරස්-අඩවි-ස්ක්‍රිප්ට්)

- [කිසිදු පිටපතක් හඳුනාගත නොහැකි විය](#සැක සහිත-උපාංග\_අවසන්)

### හරස්-අඩවි-ස්ක්‍රිප්ට්\_1

ඔබ පැමිණි අඩවිය ඔබට ගිණුමක් ඇති අඩවියක්ද?

- [ඔව්](#ගිණුම්-ආරක්ෂක\_අවසානය)

- [නැත](#හරස්-අඩවි-ස්ක්‍රිප්ට්-2)

### හරස්-අඩවි-ස්ක්‍රිප්ට්-2

ඔබ අවසන් කළ අඩවිය ඔබ කළමනාකරණය කරන වෙබ් අඩවියකද?

- [ඔව්](#හරස්-අඩවි-ස්ක්‍රිප්ට්-පරිපාලක-සම්මුති\_අවසානය)

- [නැත](#හරස්-අඩවි-ස්ක්‍රිප්ට්-3)

### cross-site-script-admin-compromised\_end

> මෙම අවස්ථාවේදී, ප්‍රහාරකයාට ඔබගේ පරිපාලක ගිණුමට ප්‍රවේශ වීමට ඉඩ සලසන වලංගු කුකියක් තිබිය හැක. පළමු දෙය නම් ඔබේ පරිපාලන අතුරුමුහුණතට ඇතුළු වී ඕනෑම සක්‍රීය සැසියක් මරා දැමීම හෝ මුරපදය වෙනස් කිරීමයි. ප්‍රහාරකයා ඔබේ වෙබ් අඩවියට කිසියම් කෞතුක වස්තු උඩුගත කර තිබේද සහ/හෝ කිසියම් ද්වේෂසහගත අන්තර්ගතයක් පළ කර තිබේද යන්න ඔබ පරීක්ෂා කළ යුතුය, එසේ නම් එය ඉවත් කරන්න.

මෙම සිද්ධිය විමර්ශනය කිරීමට සහ ප්‍රතිචාර දැක්වීමට පහත සංවිධානවලට උදවු කළ හැක.

:[](සංවිධාන?services=forensic)

### හරස්-අඩවි-ස්ක්‍රිප්ට්-3

> මෙය හොඳ විය යුතුය. කෙසේ වෙතත්, සමහර දුර්ලභ අවස්ථාවන්හිදී, XSS වෙනත් ප්‍රහාර දියත් කිරීමට ඔබගේ බ්‍රවුසරය භාවිතා කිරීමට භාවිතා කළ හැක.

- [මට මගේ උපාංගය ආසාදනය වී ඇත්දැයි තක්සේරු කිරීමට අවශ්‍යයි](../../../උපාංගය-සැක සහිත ලෙස)

- [මම හිතන්නේ මම හොඳින්](#අවසාන\_ඉඟි)

### පිළිතුරු-පුද්ගලික-තොරතුරු

> ඔබ බෙදාගත් තොරතුරු වර්ගය අනුව, ඔබට ඉක්මන් ක්‍රියාමාර්ග ගැනීමට අවශ්‍ය විය හැක.

ඔබ බෙදාගත්තේ කුමන ආකාරයේ තොරතුරුද?

- [මම රහස්‍ය ගිණුම් තොරතුරු බෙදා ගත්තෙමි](#ගිණුම්-ආරක්ෂක\_අවසානය)

- [මම පොදු තොරතුරු බෙදාගත්තා](#බෙදාගන්න)

- [තොරතුරු කෙතරම් සංවේදීදැයි මට විශ්වාස නැති අතර මට උදව් අවශ්‍යයි](#උදව්\_අවසන්)

### share කරන්න

> ඔබේ සැක සහිත පණිවිඩය බෙදාගැනීමෙන් බලපෑමට ලක්විය හැකි ඔබේ සගයන් සහ ප්‍රජාව ආරක්ෂා කර ගත හැක. පණිවිඩය අනතුරුදායක නම් ඔබට උපදෙස් දීමට ඔබ විශ්වාස කරන කෙනෙකු වෙත උපකාර ලබා ගැනීමටද ඔබට අවශ්‍ය විය හැක. ඒවා විශ්ලේෂණය කළ හැකි සංවිධාන සමඟ පණිවිඩය බෙදා ගැනීම සලකා බලන්න.

>

> ඔබේ සැක සහිත පණිවිඩය බෙදා ගැනීමට, පණිවිඩය මෙන්ම යවන්නා පිළිබඳ තොරතුරු ඇතුළත් කිරීමට වග බලා ගන්න. පණිවිඩය විද්‍යුත් තැපෑලක් නම්, කරුණාකර [පරිගණක සිද්ධි ප්‍රතිචාර මධ්‍යස්ථානයේ (CIRCL)](https://www.circl.lu/pub/tr-07/ පරිගණක සිදුවීම් ප්‍රතිචාර මධ්‍යස්ථානයේ පහත දැක්වෙන මාර්ගෝපදේශය භාවිතා කර ශීර්ෂ ඇතුළත් සම්පූර්ණ විද්‍යුත් තැපෑල ඇතුළත් කිරීමට වග බලා ගන්න. )

ඔබට වැඩිදුර උදව් අවශ්‍යද?

- [ඔව්, මට තවත් උදවු අවශ්‍යයි](#උදව්\_අවසන්)

- [නැහැ, මම මගේ ගැටලුව විසඳා ඇත](# විසඳා\_අවසානය)

### Device-security\_end

> සමහර ගොනු ඔබගේ උපාංගයට බාගත කර ඇත්නම්, ඔබගේ උපාංගය අවදානමට ලක් විය හැක!

ඔබට සහාය දිය හැකි පහත සංවිධාන සම්බන්ධ කර ගන්න. පසුව, කරුණාකර [ඔබගේ සැක සහිත පණිවිඩය බෙදා ගන්න](#share).

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

### ගිණුම්-ආරක්ෂක\_අවසානය

> ඔබ ඔබේ අක්තපත්‍ර ඇතුළත් කළහොත් හෝ ඔබ හරස්-අඩවි ස්ක්‍රිප්ට් ප්‍රහාරයකට ගොදුරු වූ විට, ඔබේ ගිණුම් අවදානමට ලක් විය හැකිය!

>

> ඔබේ ගිණුම අවදානමට ලක්ව ඇතැයි ඔබ සිතන්නේ නම්, ඔබ [සම්මුතිගත ගිණුම්](../../../account-access-issues) හි ඩිජිටල් ප්‍රථමාධාර කට්ටල කාර්ය ප්‍රවාහය අනුගමනය කිරීම ද නිර්දේශ කෙරේ.

>

> ඔබ මෙම තතුබෑම් ව්‍යාපාරය ගැන ඔබේ ප්‍රජාවට දැනුම් දිය යුතු අතර, ඒවා විශ්ලේෂණය කළ හැකි සංවිධාන සමඟ සැක සහිත පණිවිඩය බෙදා ගත යුතුය.

ඔබට ලැබුණු පණිවිඩය පිළිබඳ තොරතුරු බෙදා ගැනීමට ඔබ කැමතිද නැතහොත් මීට පෙර ඔබට වැඩිදුර සහාය අවශ්‍යද?

- [මට සැක සහිත පණිවිඩය බෙදා ගැනීමට අවශ්‍යයි](#share)

- [මගේ ගිණුම සුරක්ෂිත කිරීමට මට තවත් උදවු අවශ්‍යයි](#ගිණුම\_අවසන්)

- [පණිවිඩය විශ්ලේෂණය කිරීමට මට තවත් උදවු අවශ්‍යයි](#විශ්ලේෂණ\_අවසන්)

### සැක සහිත-උපාංගය\_අවසානය

> ඔබ සබැඳියක් මත ක්ලික් කර සිදු වූයේ කුමක්දැයි නිසැක නොවේ නම්, ඔබ නොදැනුවත්වම ඔබගේ උපාංගය ආසාදනය වී තිබිය හැක. ඔබට මෙම හැකියාව ගවේෂණය කිරීමට අවශ්‍ය නම්, හෝ ඔබේ උපාංගය ආසාදනය වී ඇති බවට හැඟීමක් ඇත්නම් ["මගේ උපාංගය සැක සහිත ලෙස ක්‍රියා කරයි"](../../../device-acting-suspiciously) වෙත යන්න.

ඔබගේ උපාංගය සැක සහිත ලෙස ක්‍රියා කරන නිසා ඔබට ක්ෂණික උදවු අවශ්‍ය නම්, ඔබට සහය දිය හැකි පහත සංවිධාන සම්බන්ධ කර ගත හැක. පසුව, කරුණාකර [ඔබගේ සැක සහිත පණිවිඩය බෙදා ගන්න](#share).

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

### උදව්\_අවසන්

> ඔබ බෙදාගත් තොරතුරුවලින් ඇති අවදානම් වඩාත් හොඳින් අවබෝධ කර ගැනීමට ඔබ ඔබේ සගයන්ගෙන් හෝ වෙනත් අයගෙන් උපකාර පැතිය යුතුය. ඔබේ සංවිධානයේ හෝ ජාලයේ සිටින වෙනත් පුද්ගලයින්ට ද එවැනි ඉල්ලීම් ලැබී තිබිය හැක.

ඔබට සහාය දිය හැකි පහත සංවිධාන සම්බන්ධ කර ගන්න. පසුව, කරුණාකර [ඔබගේ සැක සහිත පණිවිඩය බෙදා ගන්න](#share).

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

### ගිණුම\_අවසානය

ඔබගේ ගිණුම අවදානමට ලක්ව ඇත්නම් සහ ඔබට එය සුරක්ෂිත කිරීමට උදවු අවශ්‍ය නම්, කරුණාකර ඔබට සහාය දිය හැකි පහත සංවිධාන අමතන්න.

:[](සංවිධාන?services=ගිණුම)

### විශ්ලේෂණය\_අවසානය

පහත සංවිධානවලට ඔබේ සැක සහිත පණිවිඩය ලැබිය හැකි අතර ඔබ වෙනුවෙන් එය තවදුරටත් විමර්ශනය කළ හැක:

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

### විසඳන ලද\_අවසානය

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

### අවසාන\_ඉඟි

මතක තබා ගත යුතු පළමු රීතිය: ඊමේල් හෝ වෙනත් පණිවුඩකරණ මෙවලම් තුළ කිසි විටෙක පුද්ගලික තොරතුරු ලබා නොදෙන්න. කිසිම ආයතනයක්, බැංකුවක් හෝ වෙනත් ආකාරයකින් මෙම තොරතුරු විද්‍යුත් තැපෑල, සමාජ ජාල වේදිකා හෝ පණිවුඩකරණ යෙදුම් හරහා කිසිදා අසන්නේ නැත. විද්‍යුත් තැපෑලක්, පණිවිඩයක් හෝ වෙබ් අඩවියක් නීත්‍යානුකූලද යන්න පැවසීම සැමවිටම පහසු නොවනු ඇත, නමුත් ඔබට ලැබී ඇති විද්‍යුත් තැපෑල තක්සේරු කිරීමට උපකාර වන ඉඟි කිහිපයක් තිබේ.

හදිසිතාවේ හැඟීම: සැක සහිත ඊමේල් සාමාන්‍යයෙන් ගිණුමකට හදිසි වෙනසක් ගැන අනතුරු අඟවන අතර ඔබේ ගිණුම සත්‍යාපනය කිරීමට වහාම ක්‍රියා කරන ලෙස ඔබෙන් ඉල්ලා සිටී.

\* විද්‍යුත් තැපෑලක, “තහවුරු කිරීම” හෝ “ඔබේ ගිණුම යාවත්කාලීන කිරීම” හෝ “ඔබේ වාර්තා යාවත්කාලීන කිරීමට අපොහොසත් වීම ගිණුම් අත්හිටුවීමට හේතු වනු ඇත” යන ප්‍රශ්න ඔබෙන් දැකිය හැකිය. සාමාන්‍යයෙන් ඔබ ඔබේ තොරතුරු සපයා ඇති කිසිදු විශ්වාසනීය ආයතනයක් කිසි දිනක එය නැවත ඇතුල් කරන ලෙස ඔබෙන් ඉල්ලා නොසිටින බව උපකල්පනය කිරීම ආරක්ෂිතයි, එබැවින් මෙම උගුලට හසු නොවන්න.

\* අනවශ්‍ය පණිවිඩ, ඇමුණුම්, සබැඳි සහ පිවිසුම් පිටු වලින් පරිස්සම් වන්න.

\* අක්ෂර වින්‍යාස සහ ව්‍යාකරණ දෝෂ ගැන විමසිලිමත් වන්න.

\* විද්‍යුත් තැපෑලෙහි, ප්‍රදර්ශනය කරන ලද නම පමණක් නොව, සම්පූර්ණ යවන්නාගේ ලිපිනය බැලීමට ක්ලික් කරන්න.

\* කෙටි කරන ලද සබැඳි ගැන සැලකිලිමත් වන්න - ඔබට අවසාන ගමනාන්තය පරීක්ෂා කළ නොහැකි බැවින්, ඔවුන් ඔබව අනිෂ්ට වෙබ් අඩවියකට ගෙන යා හැකිය.

\* ඔබ ඔබේ මූසිකය සබැඳියක් මත තබා ඇති විට, ඔබ වෙත යොමු කෙරෙන සත්‍ය URL එක උත්පතනයක හෝ ඔබේ බ්‍රවුසර කවුළුවේ පහළින් දර්ශනය වේ.

\* "වෙතින්:" අගය ඇතුළු ඊමේල් ශීර්ෂයන් නීත්‍යානුකූල බව පෙනෙන පරිදි ප්‍රවේශමෙන් සකස් කළ හැක. SPF සහ DKIM ශීර්ෂයන් පරීක්ෂා කිරීමෙන්, යවන්නාගේ වසම වෙනුවෙන් ඊමේල් යැවීමට IP ලිපිනයකට අවසර තිබේද (හෝ නැත) සහ සංක්‍රමණයේදී ශීර්ෂයන් හෝ අන්තර්ගතය වෙනස් කර තිබේද යන්න ඔබට පිළිවෙලින් පැවසිය හැක. නීත්‍යානුකූල විද්‍යුත් තැපෑලක, [SPF](https://dmarcly.com/blog/how-to-implement-dmarc-dkim-spf-to-stop-email-spoofing-phishing-the-definitive-guide#what- is-spf) සහ [DKIM](https://dmarcly.com/blog/how-to-implement-dmarc-dkim-spf-to-stop-email-spoofing-phishing-the-definitive-guide#what-is -dkim) අගයන් සැමවිටම 'PASS' විය යුතුය, එසේ නොමැතිනම් විද්‍යුත් තැපෑලක් විශ්වාස කළ නොහැක. හේතුව නම් විද්‍යුත් තැපෑල වංචා කර තිබීම හෝ දුර්ලභ අවස්ථාවන්හිදී තැපැල් සේවාදායකය නිවැරදිව වින්‍යාස කර නොතිබීමයි.

\* [ඩිජිටල් අත්සන්](https://www.gnupg.org/gph/en/manual/x135.html) නීත්‍යානුකූල යවන්නා විසින් විද්‍යුත් තැපෑලක් එවා ඇත්නම් සහ එය වෙනස් කර තිබේද නැද්ද යන්න අපට පැවසිය හැකිය. . විද්‍යුත් තැපෑල OpenPGP සමඟ අත්සන් කර ඇත්නම්, අත්සන සත්‍යාපනය කර තිබේද නැද්ද යන්න පරීක්ෂා කරන්න. අත්සනක් සත්‍යාපනය කිරීම සඳහා, ඔබට OpenPGP ස්ථාපනය කර පණිවිඩයේ අත්සනෙහි හැඳුනුම්පත හා සම්බන්ධ පොදු යතුර ආයාත කිරීමට අවශ්‍ය වනු ඇත. ඩිජිටල් අත්සන සඳහා සහය දක්වන බොහෝ නවීන විද්‍යුත් තැපැල් සේවාලාභීන් ඔබ සඳහා සත්‍යාපනය ස්වයංක්‍රීය කර අත්සනක් සත්‍යාපනය කර තිබේද නැද්ද යන්න ඔවුන්ගේ පරිශීලක අතුරුමුහුණත හරහා ඔබට කියනු ඇත.

\* සම්මුතියකට ලක් වූ ගිණුමකට ඉහත සියලු කොන්දේසි සත්‍යාපනය කළ හැකි සහ නීත්‍යානුකූල ලෙස පෙනෙන අනිෂ්ට විද්‍යුත් තැපෑලක් හෝ පණිවිඩයක් නිකුත් කළ හැකිය. කෙසේ වෙතත්, සාමාන්යයෙන් පණිවිඩයේ අන්තර්ගතය අසාමාන්ය වනු ඇත. විද්‍යුත් තැපැල් පණිවිඩයේ අන්තර්ගතය අමුතු බවක් පෙනේ නම්, ඕනෑම ක්‍රියාමාර්ගයක් ගැනීමට පෙර වෙනත් සන්නිවේදන නාලිකාවක් හරහා නීත්‍යානුකූල යවන්නා සමඟ පරීක්ෂා කිරීම සැමවිටම හොඳ අදහසකි.

\* ඔබේ විද්‍යුත් තැපෑල සරල අකුරුවලින් කියවීම සහ ලිවීම සැමවිටම හොඳ පුරුද්දකි. HTML-පාදක ඊමේල් අනිෂ්ට කේත හෝ URL සඟවන ආකාරයෙන් විදැහුම් කළ හැක. ඔබට [මෙම වෙබ් අඩවියේ](https://useplaintext.email/) විවිධ විද්‍යුත් තැපැල් සේවාලාභීන් තුළ HTML අක්‍රිය කරන්නේ කෙසේද යන්න පිළිබඳ උපදෙස් සොයාගත හැක.

\* ඔබගේ දුරකථනයේ හෝ පරිගණකයේ මෙහෙයුම් පද්ධතියේ නවතම අනුවාදය භාවිතා කරන්න ([Android](https://en.wikipedia.org/wiki/Android\_version\_history සඳහා අනුවාදය පරීක්ෂා කරන්න), [iOS](https://en.wikipedia.org /wiki/IOS\_version\_history), [macOS](https://en.wikipedia.org/wiki/MacOS\_version\_history) සහ [Windows](https://en.wikipedia.org/wiki/Microsoft\_Windows)).

ඔබගේ මෙහෙයුම් පද්ධතිය සහ ඔබ ස්ථාපනය කර ඇති සියලුම යෙදුම්/වැඩසටහන් හැකි ඉක්මනින් යාවත්කාලීන කරන්න, විශේෂයෙන් තොරතුරු ලබා ගන්නා ඒවා (බ්‍රවුසර්, පණිවිඩ යැවීම සහ කතාබස් යෙදුම්/වැඩසටහන්, ඊමේල් සේවාලාභීන්, ආදිය). ඔබට අවශ්‍ය නොවන සියලුම යෙදුම්/වැඩසටහන් ඉවත් කරන්න.

\* විශ්වාසදායක බ්‍රවුසරයක් භාවිතා කරන්න (උදා. Mozilla Firefox). ඔබගේ බ්‍රවුසරයේ ස්ථාපනය කර ඇති දිගු/ඇඩෝන සමාලෝචනය කිරීමෙන් ඔබගේ බ්‍රවුසරයේ ආරක්ෂාව වැඩි කරන්න. ඔබ විශ්වාස කරන අය පමණක් තබන්න (උදාහරණයක් ලෙස: [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 /)).

\* ඔබේ තොරතුරු නිතිපතා ආරක්ෂිත උපස්ථ කරන්න.

\* ශක්තිමත් මුරපද, 2-සාධක සත්‍යාපනය සහ ආරක්ෂිත සැකසුම් සමඟ ඔබේ ගිණුම් ආරක්ෂා කරන්න.

මූලාශ්‍ර

සැක සහිත පණිවිඩ හඳුනා ගැනීමට සහ තතුබෑම් වලින් වැළකී සිටීමට සම්පත් ගණනාවක් මෙහි ඇත.

\* [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)

\* [Google message header analysis tool](https://toolbox.googleapps.com/apps/messageheader/)