

OUCH!

Havi biztonság tudatossági hírlevél mindenkinek

# Állítsuk meg az adathalászatot

## Áttekintés

Az email és az üzenetküldő alkalmazások (mint a Skype, Twitter vagy a Snapchat) a leggyakrabban használt kommunikációs megoldások közé sorolhatóak. Mindennapi életünk során nemcsak munkánk kapcsán használjuk őket, hanem a családukkal, barátainkkal való kapcsolattartásra is. Amióta világszerte nagyon sok ember függ ezektől a technológiáktól, ők váltak a kiberbűnözők adathalász típusú támadásainak elsődleges célpontjaivá. Alább megismerhetjük mi az adathalászat, hogyan lehet észrevenni egy adathalász próbálkozást, hogyan lehet azt megállítani, függetlenül attól, hogy otthon vagy munkahelyen vagyunk.

## Mi az adathalászat

Az adathalászat egy olyan típusú támadás, ami email vagy üzenetküldő alkalmazásokat használva hivatott a felhasználót megtéveszteni és rábírní, hogy olyat tegyen, amit általában nem tenne: kattintson rá egy káros hivatkozásra, ossza meg a jelszavát, vagy nyisson meg egy káros levélmellékletet. A támadók keményen dolgoznak azon, hogy ezek az üzenetek meggyőzőek legyenek, érzelmi reakciókat váltsanak ki az áldozatból, sürgősnek tűnjenek vagy felkeltsék a kíváncsiságunkat. A támadók úgy fogalmazzák meg az üzeneteket, hogy úgy tűnjön olyantól kaptuk akit, vagy amit ismerünk, mint például egy barát, vagy egy megbízható cég, akivel rendszeresen kapcsolatban vagyunk. Esetleg még a bankunk logóját is felhasználják a levélben vagy meghamisítják a feladó címét, hogy úgy tűnjön, a levél valódi. Ezt követően a támadók, milliók számára elküldik a levelet. A támadók nem tudják, hogy ki harap rá a csalíra, de azt tudják, minél több embernek küldik el, annál több áldozat várható.

## Védjük meg önmagunkat

A legtöbb esetben egy levél vagy üzenet megnyitása és elolvasása nem hordoz kockázatot. Ahhoz, hogy az adathalász támadás működjön, a rossz fiúknak meg kell téveszteniük minket és rávenni, hogy tegyünk meg valamit. Szerencsére van pár jel, ami alapján azonosítható, hogy egy üzenet támadás-e. Alább található néhány ilyen jellemző:

- ✓ Kiemelt sürgősség, ami azonnali beavatkozást igényel, mielőtt valami rossz történik, mint például egy bankszámla megszüntetése, vagy börtönbüntetés kilátásba helyezése. A támadó célja, hogy behajszolja minket egy hiba elkövetésébe.
- ✓ Nyomást gyakorol, hogy kerüljük meg vagy hagyjuk figyelmen kívül a céges szabályokat vagy eljárásrendeket.
- ✓ Az üzenet nagy kíváncsiságot ébreszt bennünk, vagy a tartalma túl jó ahhoz, hogy igaz legyen (például.: nem, nem nyertük meg a lottót).
- ✓ Általános megszólítás, mint például "Kedves Ügyfelünk". A legtöbb cég, vagy barát név szerint szólít meg.

- ✓ Bizalmas információk megadását kéri, mint például bankkártya adatok, jelszavak, vagy bármi, amit egy valódi feladónak már ismernie kellene.
- ✓ Az üzenet tartalma szerint hivatalos szervezettől érkezett, de gyatra a helyesírása, nyelvtanilag nem helyes, valamint személyes postafiókból küldték el, mint például a @gmail.com.
- ✓ Az üzenet a hivatali csatornán keresztül érkezett (mint például a főnöktől), de a válaszcím valaki más személyes címére mutat.
- ✓ Olyan valakitől kapunk üzenetet, akit ismerünk, de a hangnem vagy a szóhasználat nem jellemző rá. Ha gyanúsnak találjuk az üzenetet, hívjuk fel a feladót, és ellenőrizzük, hogy Ő küldte-e az üzenetet. Egy támadó számra könnyű olyan levelet hamisítani, ami olybá tűnik, mintha egy barát vagy munkatárs lenne a feladó.

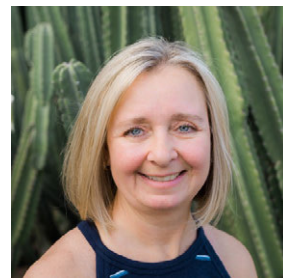
Kövessük ezeket a tippeket, egy sokkal biztonságosabb online élmény érdekében. Ha többet szeretnénk megtudni a közösségi média oldalak biztonságos használatáról vagy a jogosulatlan tevékenységek bejelentéséről akkor ellenőrizzük a közösségi média oldalak biztonsági szabályait.

## Magyar Kiadás

A Nemzeti Kibervédelmi Intézet (NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. A Nemzeti Kibervédelmi Intézet rendeltetése, hogy előmozdítsa a kormányzati szektor elektronikus informatikai rendszerei biztonsági szintjének emelését, valamint, hogy fejlessze a közigazgatásban dolgozó felhasználók biztonságtudatos viselkedését a kibertérben. A nemzetközi és hazai partnerkapcsolatai révén az NKI hozzájárul a magyar kibertér biztonságának erősítéséhez. További információ az Intézetéről a <http://www.govcert.hu/> és a <http://neih.gov.hu> oldalon olvasható.

## A szerzőről

**Tonia Dudley** 2011. óta szervez és bonyolít le biztonságtudatossági programokat, többek között egy díjnyertes adathalászat elleni programot is. Tonia profilja megtalálható a <https://www.linkedin.com/in/toniadudley> címen.



## Források

Pszichológiai befolyásolás:	<a href="https://www.sans.org/u/Cb1">https://www.sans.org/u/Cb1</a>
Segítsünk másoknak a biztonságban:	<a href="https://www.sans.org/u/Cb6">https://www.sans.org/u/Cb6</a>
Email tudnivalók:	<a href="https://www.sans.org/u/Cbg">https://www.sans.org/u/Cbg</a>
Vezérgazgató család:	<a href="https://www.sans.org/u/Cbl">https://www.sans.org/u/Cbl</a>
OUCH! fordítások és archívumok:	<a href="https://www.sans.org/u/Cbq">https://www.sans.org/u/Cbq</a>

## License

Az OUCH! a Sans Securing The Human részleg által közzétett és a [Creative Commons BY-NC-ND 4.0 licenz](https://creativecommons.org/licenses/by-nc-nd/4.0/) alapján terjesztett hírlevél. A hírlevél szabadon terjeszthető vagy tudatosító programokban felhasználható mindaddig, amíg az nem kerül módosításra. A Fordításért vagy további információért lépjen kapcsolatba velünk a [www.sans.org/security-awareness/ouch-newsletter](http://www.sans.org/security-awareness/ouch-newsletter) címen. Szerkesztette: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Fordította: Tikos Anita