

OUCH!

Havi biztonság tudatossági hírlevél mindenkinek

# Email bakik és hogyan lehet elkerülni azokat

## Áttekintés

Az email még mindig az egyik legfőbb kommunikációs forma, a magán is a hivatali életünk során egyaránt. Habár emailezéskor gyakran a saját magunk legrosszabb ellenségei lehetünk. Bemutatjuk a négy leggyakoribb hibát, amit el szoktunk követni, illetve a megoldásokat, hogy hogyan tudjuk elkerülni ezeket.

### Automatikus –kiegészítés

Az automatikus kiegészítés gyakori funkciója a legtöbb email kliensnek. Ahogy begépeljük a személy nevét, akinek az emailt akarjuk küldeni, az email szoftverünk automatikusan kiválasztja az email címüket nekünk. Így nem kell emlékeznünk az összes kontaktunk email címére, elég csak a nevüket tudni. Akkor jelenthet ez problémát, amikor több ismerősünk is van hasonló névvel, mert könnyen előfordulhat, hogy az automatikus kiegészítés funkció rossz email címet választ ki nekünk. Például, szeretnénk volna egy nagyon érzékeny emailt írni „Janet Roberts”-nek a számvitelen dolgozó kollégánknak, de helyette az automatikus kiegészítés „Janice Rodriguez”-nek a gyermekünk futball edzőjének az email címét választotta ki. Ennek köszönhetően, egy igazán érzékeny hivatali levelet elküldtünk valakinek, akit alig ismerünk. Hogy megkíméljük magunkat az ilyen esetektől, mindig ellenőrizzük le a nevet és az email címet mielőtt megnyomjuk a küldés gombot legyen az bármennyire is érzékeny tartalmú üzenet.

### Válasz mindenkinek

Amikor emailt írunk a “címezett” mezőn kívül van egy “másolat” (“CC”) lehetőségünk is. A “CC” azaz másolatot kap mező lehetővé teszi, hogy tájékoztatás céljából mások is megkapják az email másolatát. Amikor valaki olyan emailt küld nekünk, melyben másolatba bele tett másokat is akkor el kell döntetnünk, hogy csak a küldő személynek akarunk válaszolni, vagy mindenkinek, aki szerepelt az email címezettjei között. Abban az esetben, hogyha a válaszuk érzékeny, akkor valószínűleg csak a küldőnek akarjuk megküldeni azt. Legyünk óvatosak, amikor a válasz gombra kattintunk, mert könnyen előfordulhat, hogy „Válasz mindenkinek” gombra nyomunk tévesen, mely azt jelenti, hogy mindenkinek szeretnénk válaszolni. Tehát mindig ellenőrizzük le, hogy kik az email címezettjei mielőtt elküldünk egy érzékeny emailt vagy válaszolunk egyre.

### Érzelem

Sose küldjünk emailt amikor érzelmileg zaklatottak vagyunk, mert az az email árthat nekünk a jövőben, talán még egy barátságunkba vagy akár a munkánkba is kerülhet. Helyette, inkább álljunk meg egy pillanatra és nyugodtan rendezzük gondolatainkat. Ha valahogy le kell vezetnünk a frusztrációnkat, akkor nyissunk meg egy új üzenetet (győződjünk meg

arról, hogy nem szerepel se név se email cím a címzett mezőben) és írjuk le, hogy mit mondanánk, mit érzünk most. Aztán álljunk fel a számítógépünkötől, esetleg főzzünk egy kávét vagy sétáljunk egyet. Amikor visszaérünk, töröljük az üzenetet és kezdjük elölről. Vagy még jobb, ha felveszük a telefont, és telefonon megbeszéljük a másik féllel, vagy ha lehetséges, személyesen beszélünk vele. Néha nehéz meghatározni a hangszínünket és szándékunkat emailen keresztül, így az üzenet személyesen vagy telefonon jobban hangozhat. Ne feledjük, hogy a humort (főként a száraz humor) nem mindig lehet megfelelően lefordítani az érzelmes mailekben, így mások nem biztos, hogy megértik az üzenetünket.

## Adatvédelem

Végül az emailek kevés adatvédelmmel rendelkeznek. Az emailben küldött képeslapokhoz hasonlóan, az emailünket is bárki elolvashatja, aki hozzáférést szerez. Az emailünket könnyen továbbíthatják másoknak, publikus fórumokon közzétehetik, megjelenethetik egy bírósági végzés miatt, vagy megoszthatják a szerver feltörését követően. Hogy ha igazán privát dolgot szeretnénk mondani valakinek, akkor vegyük fel a telefont és hívjuk fel. Fontos, hogy emlékezzünk arra is, hogy több országban az email bizonyítékként felhasználható a bíróságon. Végül, amikor a céges számítógépünket használjuk emailzésre, emlékezzünk arra, hogy a munkáltatónknak joga van monitorozni, sőt akár olvasni is az emailjeinket abban az esetben, ha a hivatali forrásokat használunk.

## 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 biztonság tudatos viselkedését a kibertérben. A nemzetközi és hazai partnerkapcsolatai révén az NKI hozzájárul a magyar kibertér biztonságának erősítéséhez. További információ az Intézetről a <http://www.govcert.hu/> és a <http://neih.gov.hu> oldalon olvasható.

## A szerzőről

**Keith Palmgren** a biztonsági szakemberként dolgozik már több mint 30 éve a biztonsági iparban. A *NetIP. Rt.* ügyvezetője valamint a "Bevezetés a kiberbiztonságba" című öt napos SANS SEC301 képzés szerzője. <https://sans.org/sec301>.



## Hivatkozások

Állítsuk meg az adathalászatot: <https://www.sans.org/u/IJj>

A pszichológiai manipuláció: <https://www.sans.org/u/IJo>

Hogyan kezeljük az mailjeink automatikus kiegészítés listáit:

### Windows Mac

Az OUCH! a Sans Security Awareness 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