

### **Ravaszk trükkkel próbálják lehalászni a facebookozók jelszavát**

*A Facebook jegyzetek funkció segítségével készítene hitelesnek tűnő szerzői jogi figyelmeztetéseket, hogy aztán innen lőjkék át a felhasználókat az adathalász oldalakra.*



Októberben éppen a pénzügyi vonatkozású online csalásokkal kapcsolatban számoltunk be egy friss felmérés eredményeiről, amely szerint az Egyesült Államokban tavaly már a teljes lakosság 10 százaléka esett áldozatul valamilyen trükknek. Ebből kiderült, hogy a csalók az eladókat és a vevőket közvetlenül összekötő szolgáltatásokat felhasználva érik el a legjobb eredményeket, ahol ötből négyen reagálnak a spam üzenetekre, közülük pedig minden második felhasználó el is szenved valamekkora kárt az akció végén. A kutatás alapján majdnem ugyanilyen hatékonyak a technológiai támogatással kapcsolatos csalások is, köztük az úgynevezett megszerkesztett figyelmeztető levelekkel.

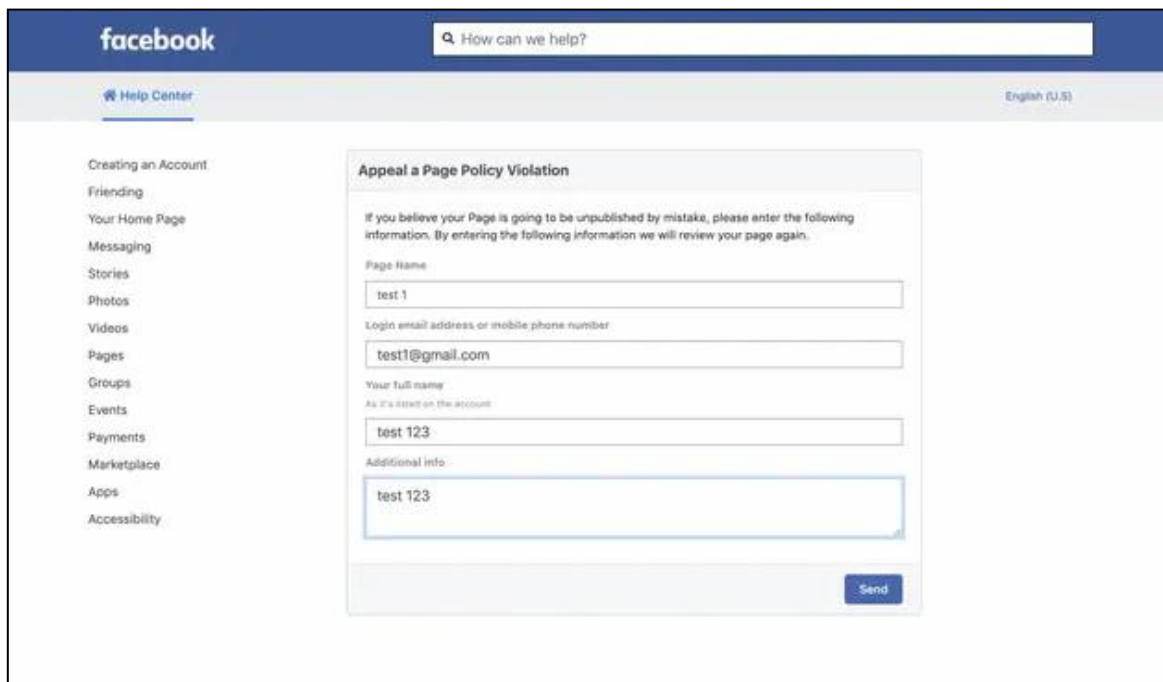
A Business Insider riportja egy hasonló trükköt mutat be, amely ráadásul nem egy Facebookot imitáló oldalon próbálja átvenni az áldozatokat, hanem magát a Facebookot használja: ezzel sikeresen elaltathatja még azok gyanúját is, akik elsőre gyanúsnak találnák az üzenetet. A csalók itt a

Facebook Notes (Jegyzetek) funkciójával operálnak, amit még a rendszeres felhasználók sem feltétlenül ismernek, pedig mindenkinek a rendelkezésére áll. A dolog azért különösen érdekes, mert itt a szolgáltató saját termékét is alkalmazzák, hogy becsapják a közösségi hálózat felhasználóit, ami jól érzékelteti, hogy mennyire folyamatos és változatos a techcégek és a bűnözők közötti küzdelem.

### **A facebookos üzenet tényleg a Facebookról jön**

A lap munkatársai első kézből számolhattak be a módszerről, mivel az adathalászok náluk is próbálkoztak. Ennek alapján a felhasználó egy értesítést kap a Facebookról, amelyben saját oldalával kapcsolatban valamilyen pontosabban meg nem határozott szerzői jogi kifogásra hívják fel a figyelmét. Az üzenet megfogalmazása szerint az illető olyan tartalmat posztolt, amelyet egy meg nem nevezett harmadik fél jogsértőnek jelölt, és felmerült a gyanú, hogy a célpontnak nincs felhatalmazása azt annak a cégnek, szervezetnek vagy személynek a képviselőjére, akit vagy amit a szóban forgó Facebook-profil reprezentál, így szükség van az azonosságának megerősítésére.

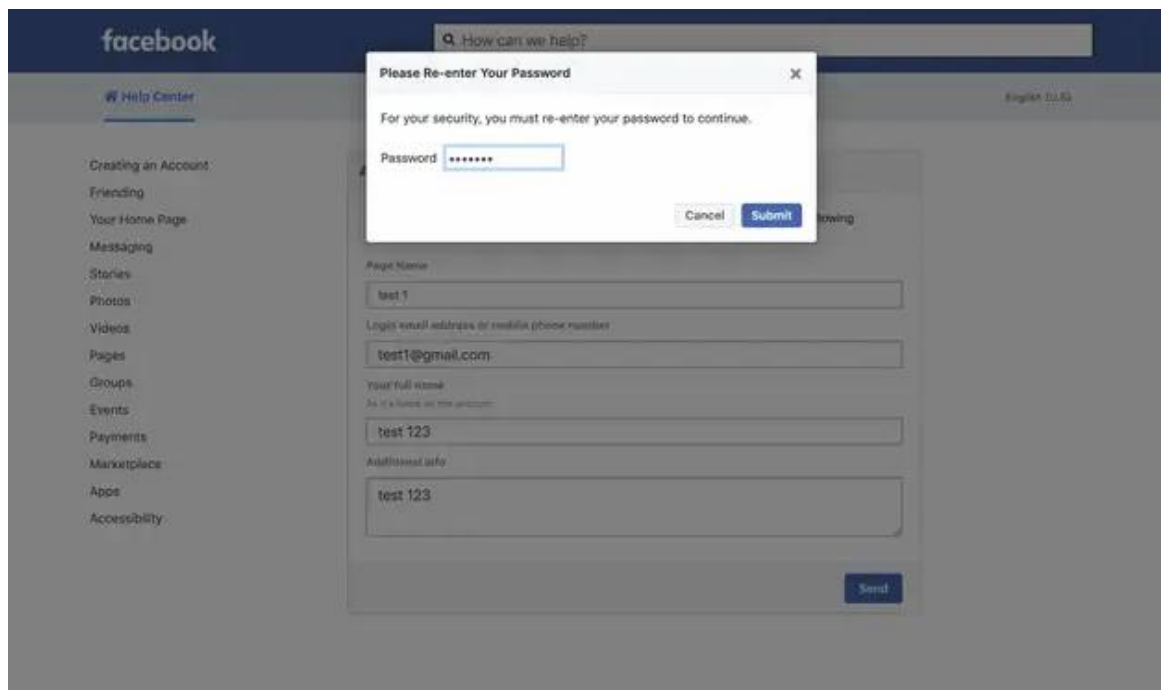
Mivel az üzenet valóban a Facebookra visz a meglehetősen általános „Policy Issues” szerző alatt, a leendő áldozat meggyőződhet róla, hogy nem egy kamu oldalra irányították: látja, hogy be van jelentkezve a Facebookra, amennyiben pedig nincs tisztában a jegyzetek funkció működésével, azt is simán elhiheti, hogy valóban a hálózat üzemeltetőjétől kapott valamilyen hivatalos értesítést. A levélben vázolt fellebbezési folyamat ezután egy másik hivatkozással folytatódik, amely azonban már egy rövidített *bit.ly* linken keresztül visz a kinézetében rendben lévő, a címet tekintve azonban több mint gyanús *facebook.com.fbmailcopyrights.com* oldalra:



forrás: businessinsider.com

A felhasználónak itt meg kell adnia egy nagy csomó adatát, így a nevét, az FB-oldal nevét vagy az email-címét is; a jelszót azonban nem kéri el, csak a legutolsó lépésben, egy szintén hitelesnek tűnő biztonsági promptban, amire elvileg a forma beküldéséhez szolgáló megerősítéshez van szükség. Természetesen aki még ezt is végrehajtja, annak a facebookos belépése egyenesen elröppen

a csalók kezébe, és a következményeket sok esetben súlyosbítja az az általános jelenség, hogy a felhasználók jelentős része ugyanazokat a belépési kulcsokat használja más szolgáltatásokhoz is. A többfaktoros hitelesítés vagy az URL-ek ellenőrzése persze sokat segít, de ez sem jellemző mindenkire.



forrás: businessinsider.com

A Facebook szóvivője a Business Insider kérdésére válaszolva elmondta, hogy időközben elérhetetlenné tették a félrevezető értesítés mögött álló oldalt, ami azonban nem jelenti, hogy ugyanígy nem próbálkozhat meg valaki más címeikkel. A közösségi hálózat a mostani tájékoztatásban is arra ösztönzi minden felhasználóját, hogy jelentsék be a gyanús-nak tartott leveleket vagy üzeneteket, és soha, semmilyen indokkal ne adják meg online csatorná-

kon a facebookos belépési adataikat. A társaság az adathalász technikákkal és a megfelelő intézkedésekkel kapcsolatban a [facebook.com/help/phishing](https://www.facebook.com/help/phishing) oldalon nyújt bővebb tájékoztatást felhasználóinak.

Forrás: <https://bitport.hu/ravasz-trukkel-probaljak-lehalaszni-a-facebookozok-jelszavat>

Válogatta: Fonyó Istvánné