



A „Futok a pénzem után” podcast a Marketing Commando és
a K&H Bank Üzletet ide együttműködésében jött létre
a bajba jutott kisvállalkozók megsegítésére.



Az online csaló árnyékként követ – mit tegyél, ha lenullázták a számládat?

Teendőd adathalász csalás esetére, szakértőink és az MNB ajánlásával

Ha felmerül, hogy adathalász csalás áldozatává váltál, azaz illetéktelenekhez kerültek

- személyes vagy bankszámlaadataid,
- online fiókjaid azonosítói, jelszavai,
- bankkártyaszámod és a hozzátartozó CVC-kód, illetve
- egyéb azonosítást és hitelesítést végző eszközöd,

a legfontosabb, hogy ne késlekedj!

Ha úgy véled, olyan kibertámadás ért, amelynek során veszélybe kerülhetett a bankszámlád vagy egyéb pénz- és értékpapírt forgalmazó fiókjaid jelszava – például feltörték e-bankfiókodat vagy általad nem jóváhagyott tranzakcióval szembesülsz, íme, az azonnali tennivalód listája:

Sorrend	Teendő	Kész?
1.	Legelső lépés, hogy azonnal vedd fel a kapcsolatot bankoddal, szolgáltatóddal, és jelezd a csalás gyanúját.	
2.	Ellenőrizd a veszélybe került számla forgalmát, a tranzakciós történetet.	
3.	Ellenőrizd a bankodnál kapcsolattartásra, értesítésekhez beállított saját telefonszámodat, e-mailcímedet (mert előfordulhat, hogy ezeket a visszaélés során megváltoztatták).	
4.	Vizsgáld meg a bankszámládhoz társított, regisztrált eszközeidet és a bankolásra használt számítógépedet, futtass vírusellenőrzést, ellenőrizd, vannak-e rajta ismeretlen alkalmazások.	
5.	Minél hamarabb módosítsd az online bankfiókodhoz vagy értékpapírszámládhoz tartozó bejelentkezési adataidat - de ehhez használj olyan számítógépet vagy más csatornát, pl. telebankot, ami biztosan nem volt érintett a csalásban.	
6.	Ha felmerül benned, hogy a számítógépedre vagy mobiltelefonodra idegen szoftver települt, akkor minden olyan hozzáféréssednek (e-mail, közösségi oldalak stb.) jelszavát meg kell változtatnod, melyet arról az eszközről használtál, vagy jelszavát az eszközön tároltad	
7.	Amennyiben a bankkártyádhoz kapcsolódó visszaélését észleled, mérlegeld a bankkártyának a felfüggesztését vagy letiltását.	
8.	Ez után fordulj a rendőrséghez: a lakóhelyed szerint illetékes rendőrkapitányságon tegyél feljelentést.	
9.	Tegy bejelentést a Nemzetbiztonsági Szakszolgálat – Nemzeti Kibervédelmi Intézet (NKI) felé is.	

Még 5 fontos tanács:

- 1.) **Vírusellenőrzés:** érdemes lefuttatni minden olyan elektronikus eszközödn, amelyen telepítve van az e-bank alkalmazásod, vagy amelyről korábban böngészővel léptél be az online fiókodba. Szükség lehet a gyári beállítások visszaállítására.
- 2.) Olyan **távoli elérést biztosító programok** is kerülhetnek a számítógépedre, telefonodra, amelyeket nem jelez veszélyesnek a víruskereső, azonban hozzáférést biztosíthatnak a csalók számára. Ezeket is **el kell távolítani**, szükség esetén kér informatikus szakember segítségét!
- 3.) Ha nélkülözni tudod annak azt az eszközödet, melyen vélhetően elkövették a csalást és igénybe szeretnéd venni a nyomozóhatóság munkáját, **szüntess be az eszközön mindenfajta tevékenységet, és kapcsolj le minden adatforgalmi hálózatról!**
- 4.) **A rendőrségre lehetőleg vidd magaddal azt az eszközt**, amin észlelted a gyanút és a további rendelkezésére álló bizonyítékaidat, ha vannak.
- 5.) **Fontos! Soha ne kezdj önálló magánnyomozásba**, főleg ne a (feltehetően) fertőzött eszközön! Fontos és visszaállíthatatlan adatokat törölhetsz, vagy változtathatsz meg rajtuk, amik a későbbi nyomozás során „forró nyomként” vagy bizonyítékként szolgálhatnak.

„Bejelentsem – ne jelentsem?”

Igen, jelentsd! A kibertámadás, az adathalászat bűncselekmény, ezért, ha csak a gyanúja merül fel annak, hogy ilyesmi történt veled, **haladéktalanul tegyél feljelentést, lehetőleg személyesen!** Sőt: ne csak akkor értesítsd a hatóságot, ha sikerrel jártak az elkövetők, hanem **akkor is, ha csak a csalás gyanúja merült fel, de végül nem ért téged kár.**

Az online vagy adathalász támadás gyanúját jelezd **a Nemzetbiztonsági Szakszolgálat – Nemzeti Kibervédelmi Intézet (NKI) felé is, itt:**

- ➔ Telefonon a nap 24 órájában az 1/336-4833-as és a 30/344-0704-es telefonszámon, e-mailben a CSIRT@nki.gov.hu e-mail-címen,
- ➔ Online az NKI honlapjának fejlécén elhelyezett [Incidens bejelentése](#) gombra kattintva.
- ➔ Anonim incidensbejelentésre a hacker@nki.gov.hu e-mail-címen, vagy [ezen a linken](#) van lehetőség.

Hazánkban két internetes forrádrót működik:

a biztonsagosinternet.hu és az internethotline.hu.

Mindkét felületen lehet bejelentést tenni, illetve segítséget kérni és káros online tartalmakat bejelenteni. További hasznos információkat olvashatsz még itt is:

<https://www.kh.hu/biztonsag-a-penzugyekben>

Az adásban szakértő vendégeink **Felföldi Rita**, a K&H Bank pénzmosás megelőzési, csalásmegelőzési és üzleti etikai főosztályának vezetője és **Dr Cseszregi Bálint** rendőrszázados kiemelt főnyomozó voltak. Tapasztalataik megosztását, a tőlük kapott hasznos információkat, tanácsaikat ezúton is köszönjük!