

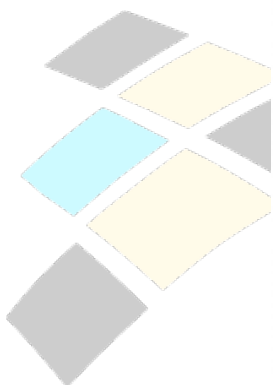
Riasztás

Káros hivatkozást tartalmazó csaló SMS-ről

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ NKI) a **Nemzeti Egészségbiztosítási Alapkezelő (NEAK)** névvel visszaélő, **káros hivatkozást tartalmazó szöveges üzenetek (SMS)** terjedésére hívja fel a figyelmet.

Intézetünkhöz bejelentés érkezett a Nemzeti Egészségbiztosítási Alapkezelőtől kéretlen, a NEAK névvel visszaélő, **káros hivatkozást** tartalmazó, NEAK TAJ kártya megerősítéséről szóló **SMS üzenettel** kapcsolatban.

A folyamat egy SMS üzenettel indul, amely látszólag a NEAK-tól érkezik. Az üzenet arra figyelmeztet, hogy a **TAJ-kártyát meg kell újítani**, és a jogosultságok elvesztésével fenyeget. Egy linket is tartalmaz, amely a felhasználót egy **hamis weboldalra** irányítja. A gyanús link a `nekas-hu[.]oeios[.]com`, ami **nem** a hivatalos NEAK webcím. Az ilyen gyanús domain nevek az adathalász kísérletek tipikus jelei.



NEAK: A TAJ-kártyáját meg kell újítani.
Annak érdekében, hogy a magyar
közegészségügyi rendszerben fennálló
jogosultságai ne sérüljenek, kérjük,
mielőbb töltsse ki és nyújtsa be a
vonatkozó frissítési űrlapot.

<https://nekas-hu.oeios.com>

(Kérjük, válaszoljon Y-nal. Ezután zárja be
az üzenetet, majd nyissa meg újra az
aktiváló hivatkozást, vagy másolja be és
nyissa meg a Safari böngészőben.)

1. ábra A káros hivatkozást tartalmazó SMS szövege.

A linkre kattintva egy olyan weboldalra jutunk, amely **megtévesztésig hasonlít** a NEAK hivatalos oldalára. Egy hivatalos közleményt imitál, amely a **TAJ-kártyák frissítését sürgeti**. Fontos azonban megjegyezni, hogy az oldalon ismét a `nekas-hu[.]oeios[.]com` domain látható. Ezen a ponton már egyértelmű, hogy **nem** a

hivatalos oldalon járunk.

DEUTSCH ENGLISH

Nemzeti Egészségbiztosítási Alapkezelő

TAJ kártya frissítése

Hivatalos közlemény

Protokoll: TAJ-FRISS-2025/605
Dátum: 2025.09.14.

A Nemzetgazdasági Minisztérium és az Egészségügyi Minisztérium egyúttműködésében bejelentik a TAJ kártyák frissítési fázisának megkezdését a UT-ÁEEK-2024/639 számú technikai utasításnak megfelelően.

Frissítés szükséges

A 2025.09.18. dátumtól kezdve a jelenleg használt TAJ kártyák már nem lesznek kompatibilisek az új nemzeti és európai egészségügyi informatikai rendszerekkel.

A TAJ kártya rendszer technológiai fejlesztése miatt szükséges a jelenleg forgalomban lévő kártyák cseréje. Az új kártya a következő előnyöket biztosítja:

- Legújabb generációs biztonsági chip európai szabványoknak megfelelően
- Fejlett adatvédelmi rendszerek személyes egészségügyi információk védelmére
- Teljes kompatibilitás az új digitális egészségügyi szolgáltatásokkal

Frissítési kötelezettség: Minden olyan állampolgárnak, aki 2023 előtt kiadott TAJ kártyával rendelkezik.

A frissítési eljárás egyszerű és teljes mértékben online végezhető el. Az új kártyát a megadott postai címre küldjük el. **Kérjük, gondosan ellenőrizze a megadott adatokat,** mivel a kérelem jóváhagyása után a címet nem lehet módosítani.

Folytatás a frissítéssel

2. ábra A csaló weboldal

Az oldalon található "Folytatás a frissítéssel" gombra kattintva egy **újabb űrlap** jelenik meg, amely **személyes adatok** (pl. név, cím, email, telefonszám, TAJ-szám) **megadását kéri**. A csalók ezeket az adatokat később felhasználhatják más támadásokhoz, például **személyazonosság lopáshoz**.

DEUTSCH ENGLISH

Nemzeti Egészségbiztosítási Alapkezelő

Adatok ellenőrzése

Személyes adatok

A TAJ kártya frissítésének folytatásához kérjük, ellenőrizze és töltsen ki személyes adatait.

TAJ szám *

Adja meg TAJ számát

Keresztnév * Vezetéknév *

Keresztnév Vezetéknév

Lakcím *

Utca, házszám

Város * Irányítószám *

Lakóhely városa Irányítószám

E-mail cím *

E-mail cím frissítések fogadásához

Telefonszám *

Telefonszám

A megadott adatokat az Ön személyazonosságának ellenőrzésére és az új TAJ kártya kibocsátására használjuk fel. Kérjük, győződjön meg róla, hogy minden adat helyes és naprakész.

Adatvédelmi tájékoztató

A személyes adatokat az EU 2016/679 számú rendelet (GDPR) szerint kezeljük. Az adatokat kizárólag a TAJ kártya frissítésére használjuk fel, és harmadik féllel nem osztjuk meg.

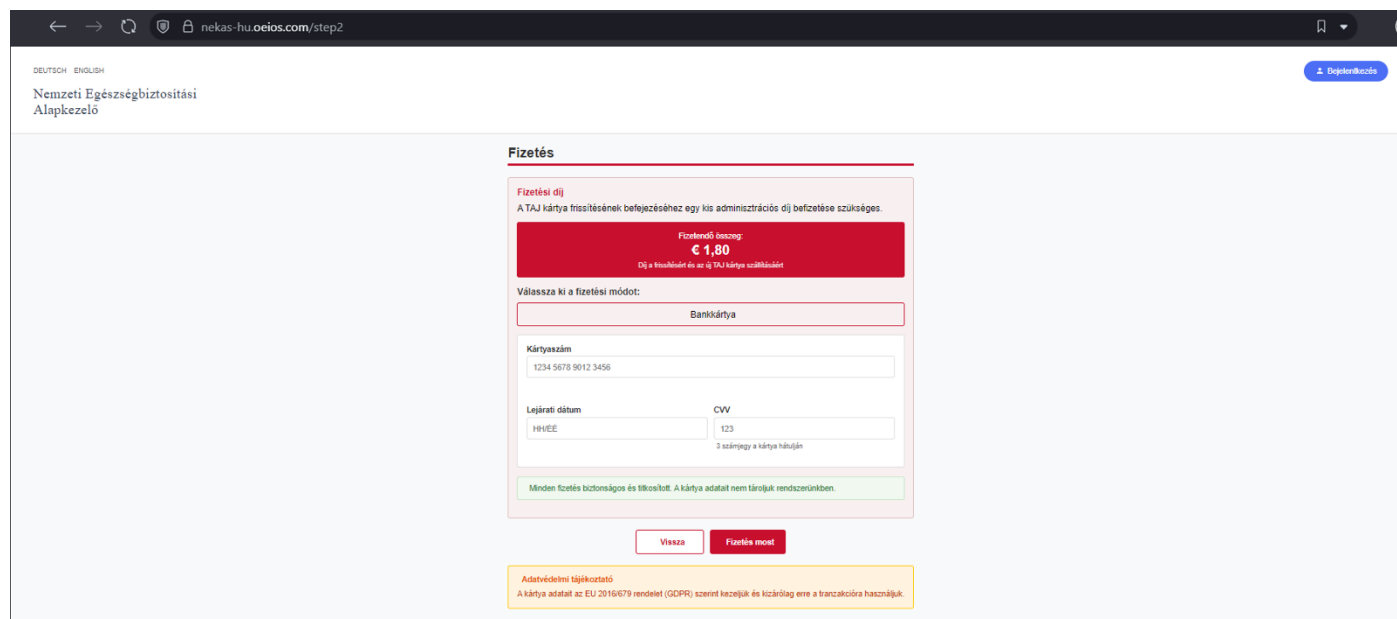
Viszra Folytatás

3. ábra A csaló weboldal űrlapja.

TLP:CLEAR

Szabadon terjeszthető!

Miután megadjuk a személyes adatainkat, a következő lépés egy **1,80 eurós "fizetési díj"** kifizetése. A weboldal a **bankkártyaadataink** (kártyaszám, lejárat dátum, CVC/CVV) megadását kéri. Ez a csalás kulcsfontosságú eleme, hiszen ezekkel az adatokkal a **csalók hozzáférhetnek a bankszámlánkhoz**. A csalók ezzel az elenyésző összeggel azt a benyomást keltik, hogy a tranzakció jelentéktelen, így a felhasználó kevésbé lesz gyanakvó — valójában azonban a **bankkártyaadatok megszerzése a céljuk**.



4. ábra A csaló weboldal fizetési oldala.

A fizetési adatok megadása után a támadók egy úgynevezett **mobilverifikációt kezdeményeznek**. Ez egy valós folyamatot imitál, azonban, a valóságban a csalók a **bankkártyaadatainkkal egy nagyobb összegű tranzakciót indítanak a bankszámlánkon**.

TLP:CLEAR

DEUTSCH ENGLISH

Nemzeti Egészségbiztosítási
Alapkezelő

Bejelentkezés

Mobilverifikáció

Erősítse meg személyazonosságát a szállítás befejezéséhez

Új biztonsági verifikáció szükséges

Apple-lel és Google-lel együttműködve új típusú biztonsági verifikációs kódot küldtünk a regisztrált mobiltelefonszáma. Ez a fejlett verifikáció maximális védelmet biztosít a csalás ellen és megerősíti személyazonosságát.

SMS elküldve:
*** **500

Adja meg a verifikációs kódot

Betöltés folyamatban...

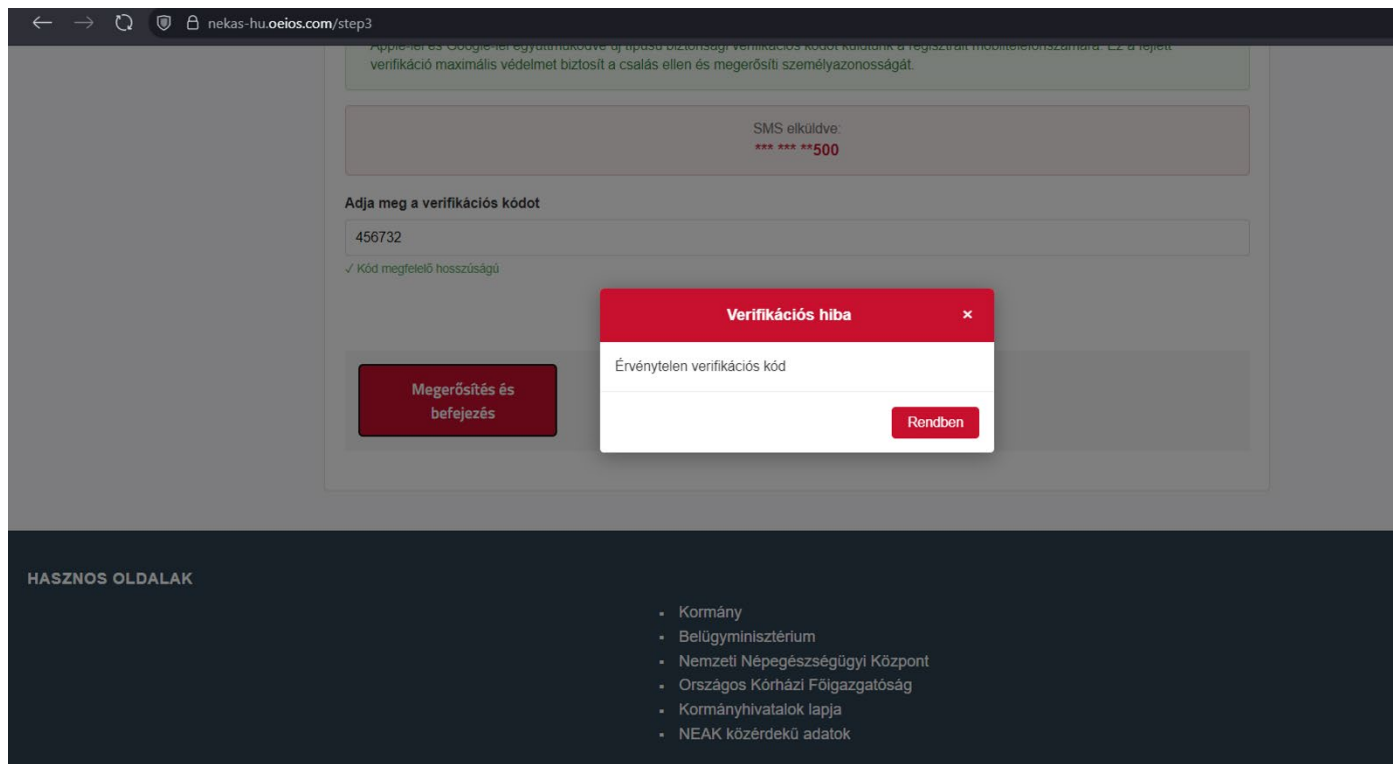
Adjon meg 6-8 számjegyű verifikációs kódot

Új kód küldése
Új kódot kérhet 40 másodperc múlva

Megerősítés és
befejezés

5. ábra A csaló weboldal verifikációs oldala.

A folyamat utolsó lépésénél a felhasználó megadja a kapott kódot, de a weboldal **"Érvénytelen verifikációs kód"** hibaüzenetet ad. Ekkor már **a tranzakció megtörtént, és a pénz elhagyta a számlánkat**. A hibaüzenet célja az, hogy **a felhasználó ne gyanakodjon azonnal**, hanem azt higgye, technikai hiba történt, miközben a csalás már sikeres volt.



6. ábra A csaló weboldal hibaüzenete.

A Nemzeti Egészségbiztosítási Alapkezelő (NEAK) tájékoztatása szerint az ügyfelek értesítése kizárólag postai kézbesítés útján és az ismert elektronikus csatornákon (magyarország.hu) keresztül történik meg a TAJ kártyával kapcsolatos ügyintézés esetén.

A Nemzeti Egészségbiztosítási Alapkezelő nem kezel olyan adatokat, amelyek alapján telefonon vagy SMS-ben értesítést küldene. A csallók által küldött SMS-ben a csatolt link maga a támadás.

Az esettel kapcsolatban a NEAK által kiadott közlemény [NEAK weboldalán](#) olvasható.

Az NBSZ NKI az alábbiakat javasolja:

- Ne kattintsunk e-mail/SMS üzenetben érkező — különösen fenti tárgyú — hivatkozásokra!
- Mindig kezeljük kellő gyanakvással az SMS-ben vagy e-mailben érkező linkeket, különösen azokat, amelyekben csak egy rövid, figyelemfelhívó vagy sürgető üzenet szerepel!
- Mindig ellenőrizzük a weboldal címét a böngésző címsorában! A NEAK hivatalos weboldala a neak.gov.hu. Bármilyen ettől eltérő cím (például neaks.com, nekas.hu stb.) gyanúra ad okot.
- A hivatalos szervek, mint a NEAK, soha nem kérnek pénzügyi adatokat (pl. bankkártyaszámot), és soha nem kérik, hogy fizessünk a szolgáltatásaikért SMS-ben küldött linken keresztül!
- Az adathalász üzenetek gyakran a félelemkeltésre építenek, és sürgetik a felhasználót, hogy azonnal cselekedjen (pl. "azonnal frissíteni kell", "elveszíti a jogosultságait").

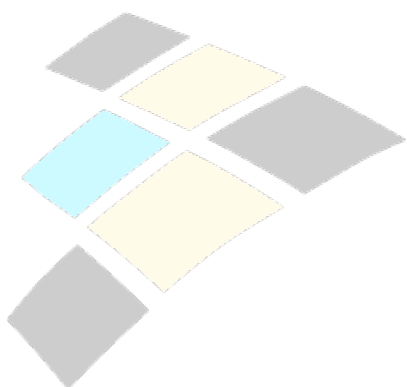


TLP:CLEAR

Szabadon terjeszthető!

- Ha egy ilyen csalással találkozunk, a legjobb, ha azonnal töröljük az üzenetet és a linket, és semmilyen körülmények között ne adjunk meg semmilyen adatot!

Nemzetbiztonsági Szakszolgálat
Nemzeti Kiberbiztonsági Intézet
Telefon: +36-1-336-4833



NEMZETI
KIBERBIZTONSÁGI
INTÉZET

TLP:CLEAR