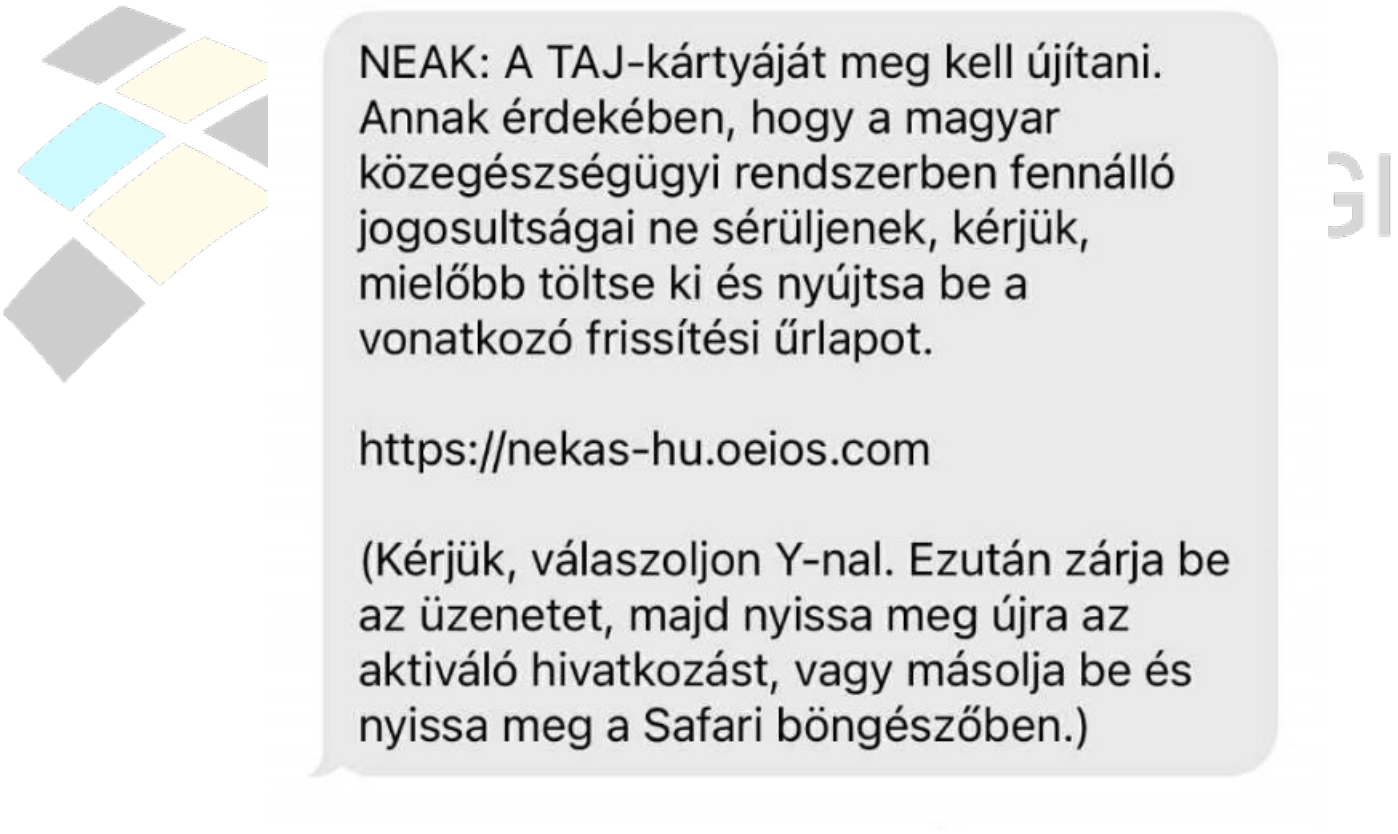
TLP:CLEAR
Szabadon terjeszthető!

Riasztás
Káros hivatkozást tartalmazó csaló SMS-ről

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

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

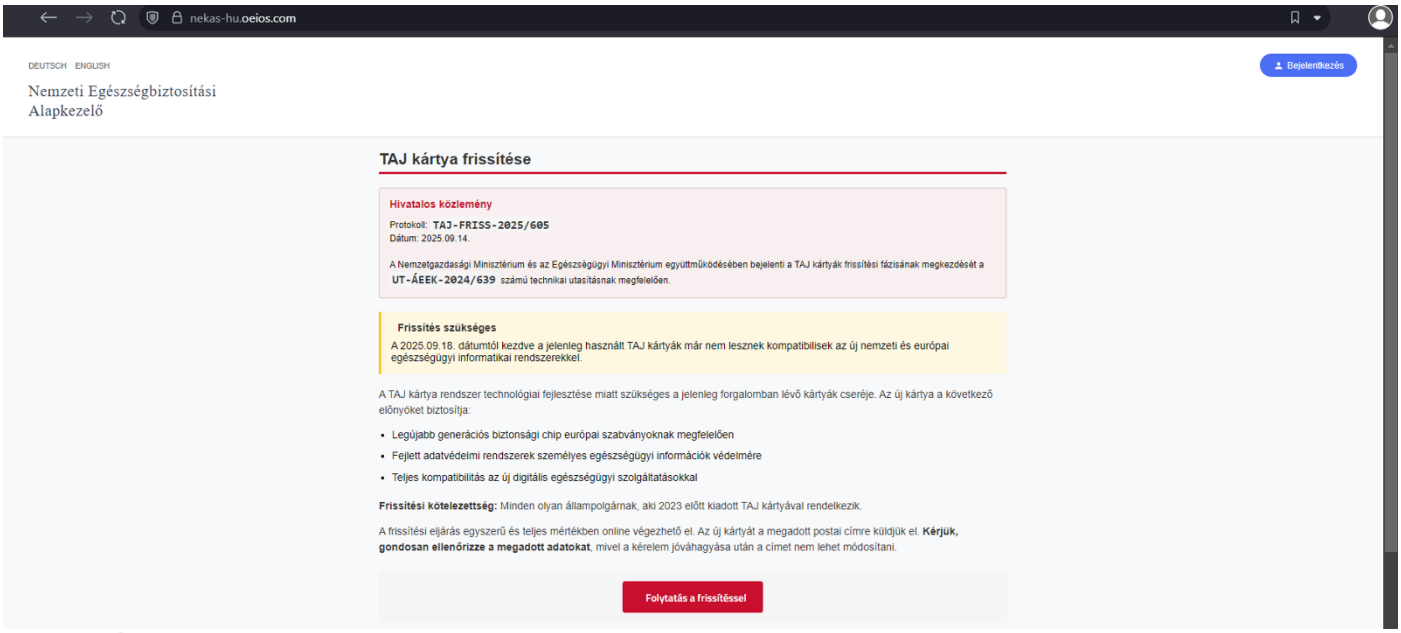
A folyamat egy SMS üzenettel indul, amely látszólag a NEAK-tól érkezik. Az üzenet arra figyelmeztet, hogy a **TAJ-kártyát meg kell újítani**, és a jogosultságok elvesztésével fenyeget. Egy linket is tartalmaz, amely a felhasználót egy **hamis weboldalra** irányítja. A gyanús link a nekas-hu[.]oeios[.]com,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



1. ábra A káros hivatkozást tartalmazó SMS szövege.

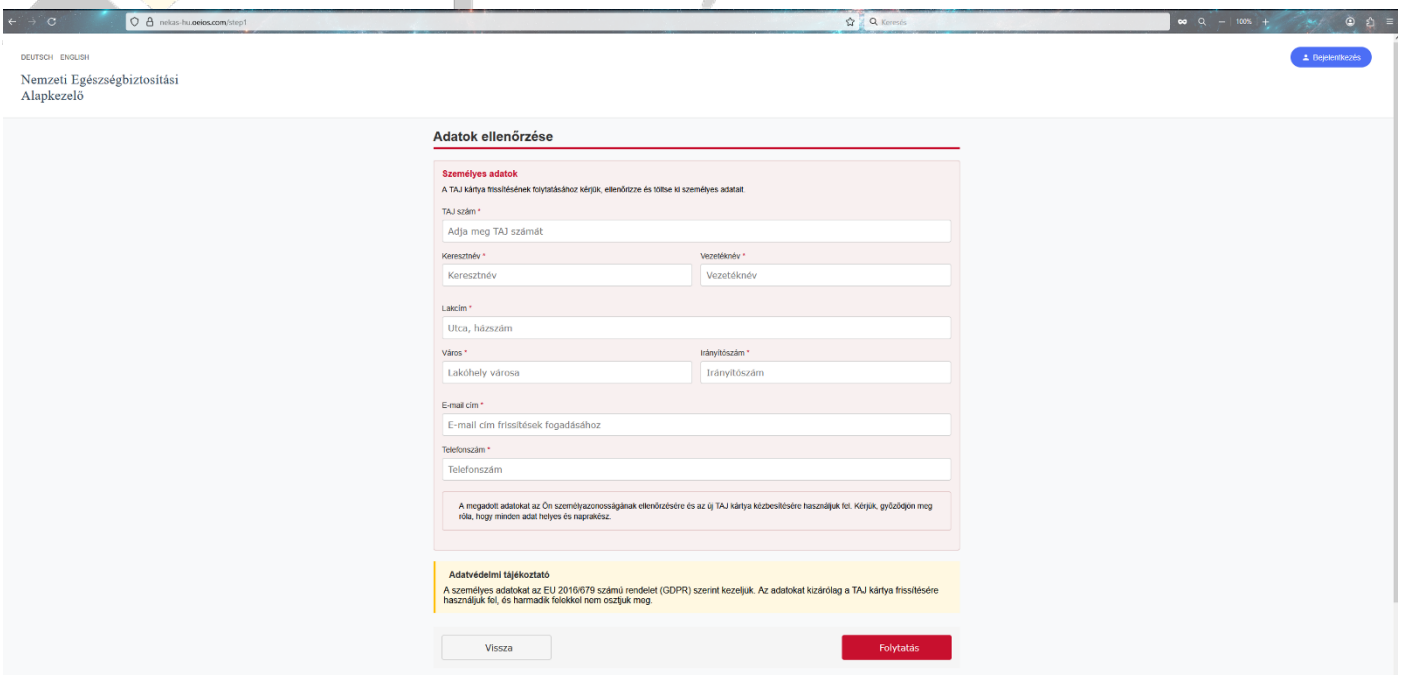
A linkre kattintva egy olyan weboldalra jutunk, amely **megtévesztésig hasonlít** a NEAK hivatalos oldalára. Egy hivatalos közleményt imitál, amely **a TAJ-kártyák frissítését sürgeti**. Fontos azonban megjegyezni, hogy az oldalon ismét a nekas-hu[.]oeios[.]com domain látható. Ezen a ponton már egyértelmű,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

hivatalos oldalon járunk.



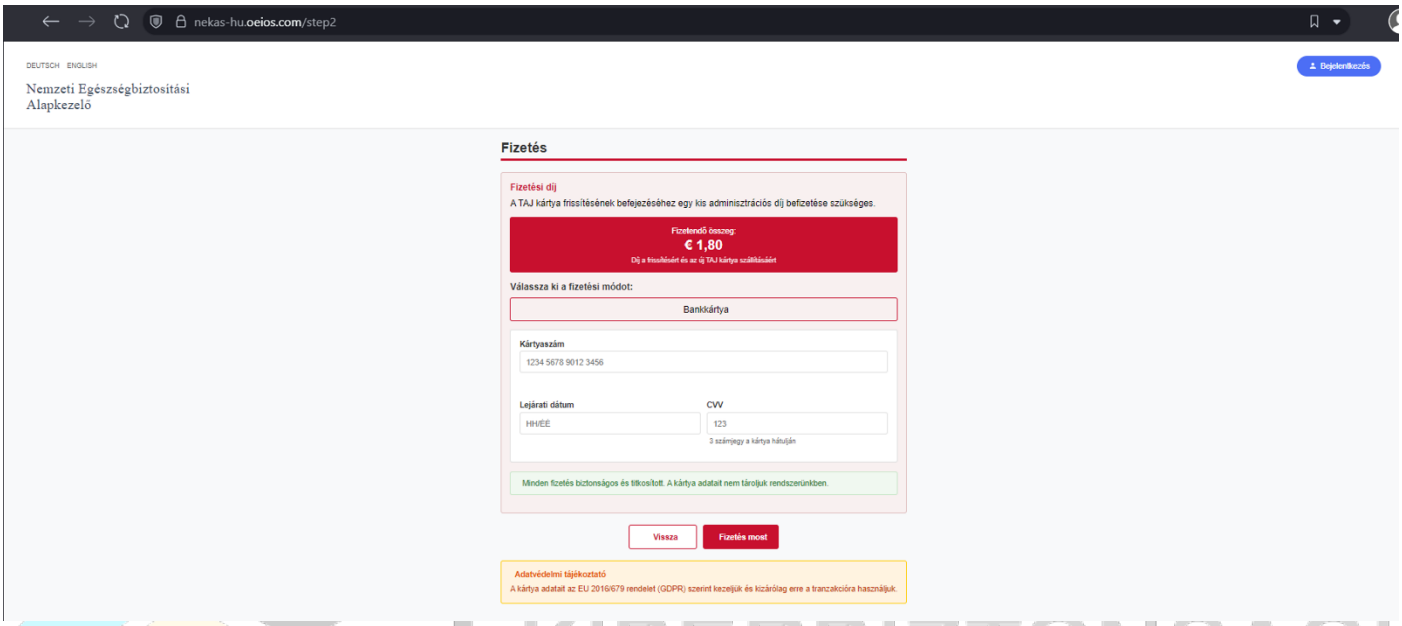
2. ábra A csaló weboldal

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**.



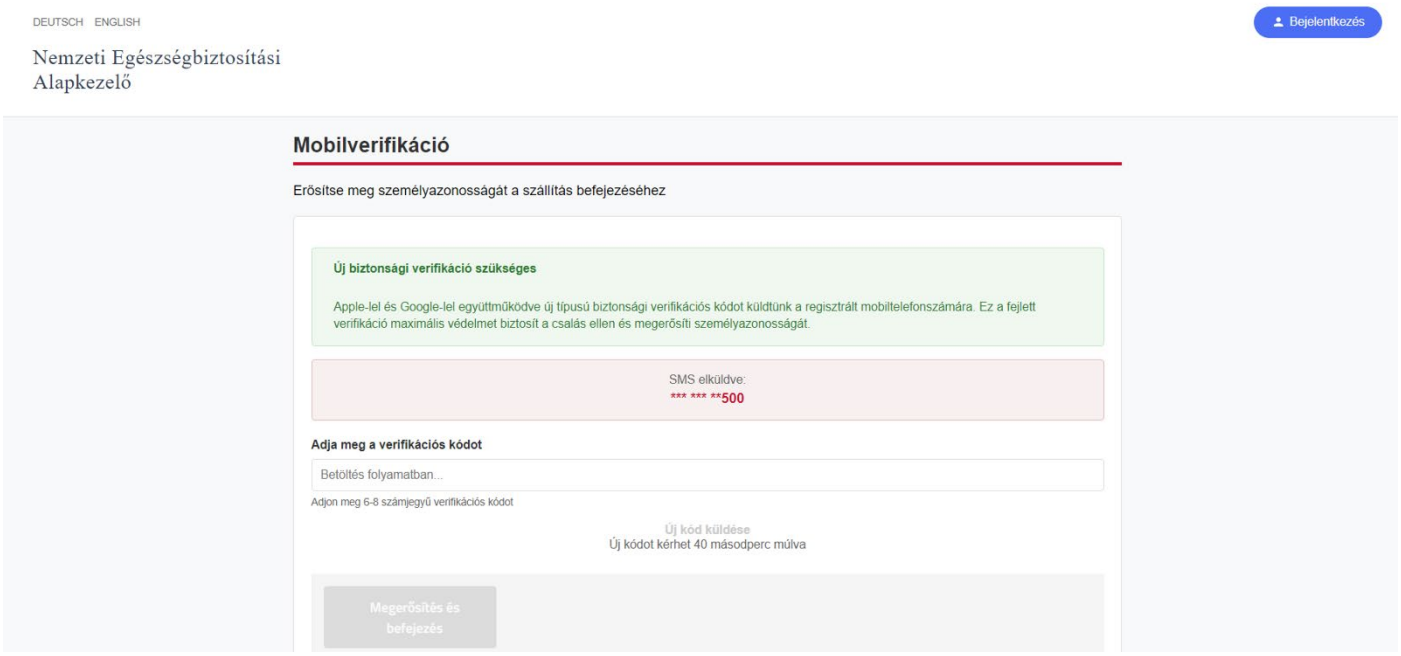
3. ábra A csaló weboldal űrlapja.

Miután megadjuk a személyes adatainkat, a következő lépés egy **1,80 eurós "fizetési díj" kifizetése**. A weboldal a **bankkártyaadataink** (kártyaszám, lejárati 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.**



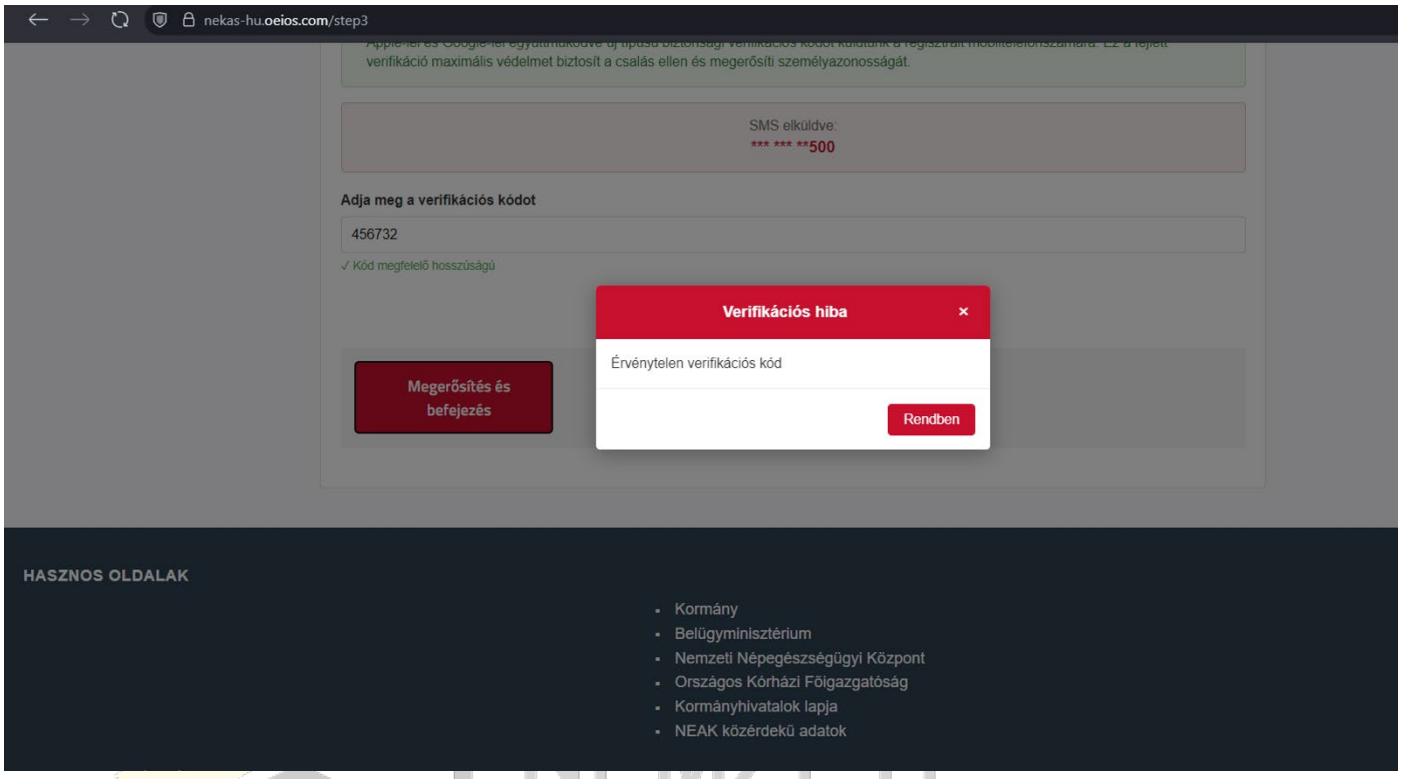
4. ábra A csaló weboldal fizetési oldala.

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**.



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 ügyfeleik értesítése kizárólag **postai kézbesítés útján** és az **ismert elektronikus csatornákon** (magyarorszag.hu) keresztül történik meg a TAJ kártyával kapcsolatos ügyintézések esetén.

A **Nemzeti Egészségbiztosítási Alapkezelő nem kezel** olyan adatokat, amelyek alapján telefonon vagy SMS-ben értesítést küldene. A csalók 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").

- 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