

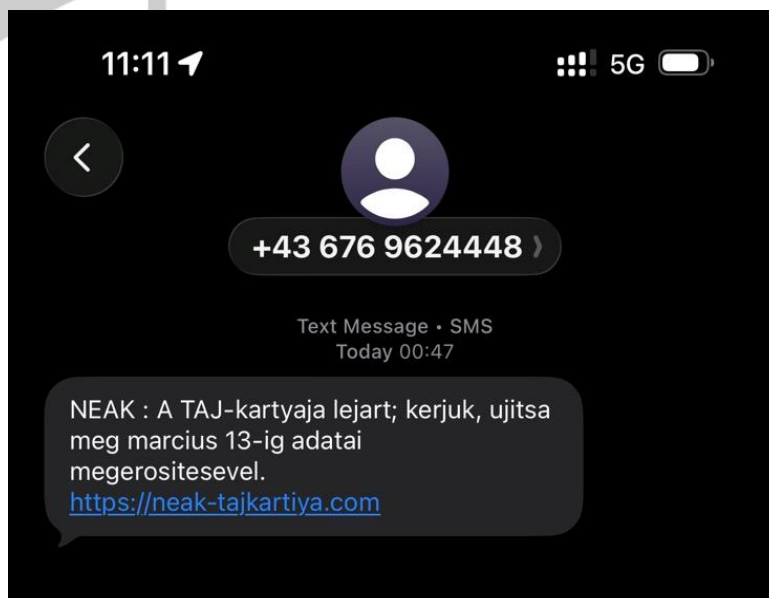
## Tájékoztatás a NEAK-ot megszemélyesítő adathalász SMS üzenetekről

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ NKI) tájékoztatót ad ki a Nemzeti Egészségbiztosítási Alapkezelő (NEAK) névvel visszaélő, káros hivatkozást tartalmazó szöveges üzenetek (SMS) kapcsán, amelyekkel a támadók a TAJ kártya lejáratára hivatkozva próbálnak meg érzékeny adatokat kicsalni az áldozatoktól.

Az SMS-ben terjesztett hivatkozás egy a NEAK névvel visszaélő adathalász weboldalra irányítja a felhasználókat. Az oldal több lépésben próbál adatokat megszerezni: a felhasználót először egy ellenőrző felületen vezeti át, majd egy, a NEAK arculati elemeit utánzó oldalon személyes adatok (például név, születési idő, lakcím, TAJ-szám, telefonszám) megadását kéri. A folyamat végén bankkártyaadatok megadására is felszólít, egy állítólagos szállítási díj kifizetésére hivatkozva.

Intézetünkhöz több bejelentés érkezett, amelyek a NEAK-ot megszemélyesítő +436769624448 és +436769624432 osztrák telefonszámokról érkeztek. Az üzenetekben a hxxps://neak-tajkartiya[.]com címre mutató adathalász hivatkozás található.

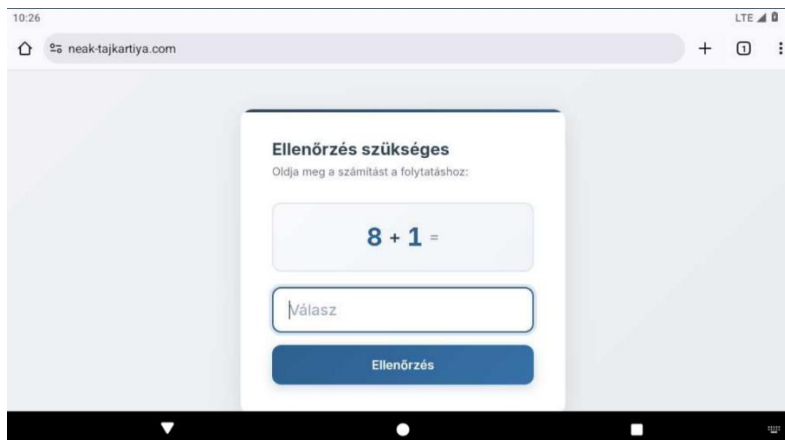


1. ábra: Az adathalász üzenet

Az adathalász weboldal megnyitásakor a rendszer egy egyszerű matematikai feladatot tartalmazó CAPTCHA segítségével próbálja ellenőrizni, hogy valódi felhasználó látogatja-e az oldalt.

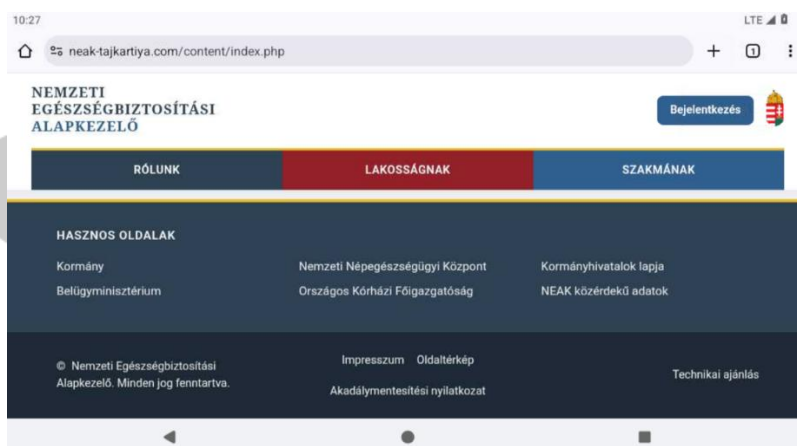
**TLP: CLEAR**

**Szabadon terjeszhető!**



2. ábra: Valódi felhasználó ellenőrzése

Az ellenőrző összeg megadását követően **egy, a NEAK arculati elemeit felhasználó hamis weboldal jelenik meg, amely a felhasználók megtévesztésére szolgál.**



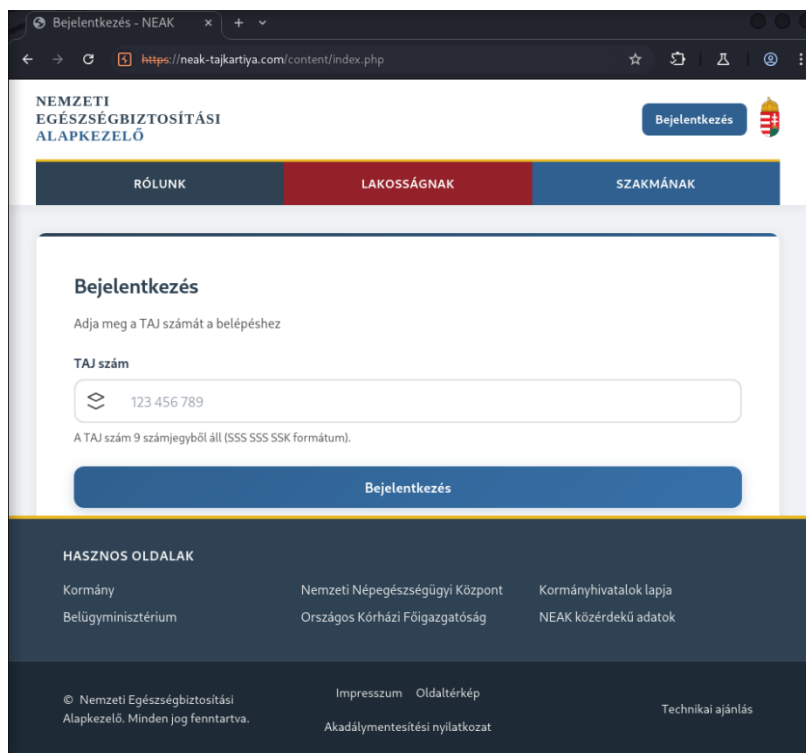
3. ábra: A NEAK-ot megszemélyesítő hamis oldal

Az adathalász weboldal több személyes adat – például TAJ-szám, lakcím – valamint bankkártyaadatok megadását kéri a felhasználóktól. A megadott adatok a háttérben **a csalók által üzemeltetett szerverre továbbítódnak.**

**TLP: CLEAR**

**TLP: CLEAR**

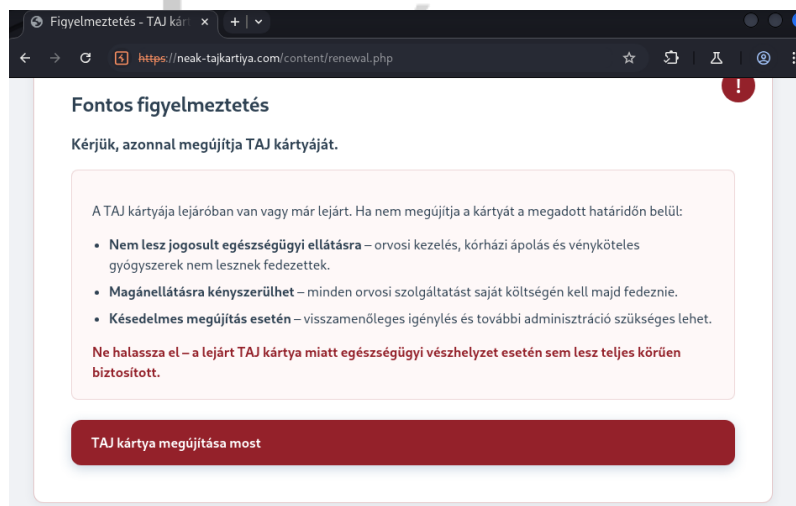
**Szabadon terjeszhető!**



The screenshot shows a web browser window with the URL <https://neak-tajkartya.com/content/index.php>. The page title is "Bejelentkezés - NEAK". The main content area is titled "Bejelentkezés" and contains a form for entering a TAJ number. The form has a label "TAJ szám" and a text input field containing "123 456 789". Below the input field, there is a note: "A TAJ szám 9 számjegyből áll (SSS SSS SSK formátum)." and a blue button labeled "Bejelentkezés". The page also features a navigation menu with "RÓLUNK", "LAKOSSÁGNAK", and "SZAKMÁNAK" tabs, and a footer with various links and contact information.

4. ábra: TAJ szám kinyerése

Rövid várakozást követően az alábbi felület jelenik meg, amely a **TAJ-kártya megújításának szükségességére hivatkozik**, és arra kéri a felhasználót, hogy indítsa el a megújítási folyamatot.



The screenshot shows a web browser window with the URL <https://neak-tajkartya.com/content/renewal.php>. The page title is "Figyelmeztetés - TAJ kár". The main content area is titled "Fontos figyelmeztetés" and contains a warning message: "Kérjük, azonnal megújítja TAJ kártyáját." Below the message, there is a text box explaining the consequences of not renewing the card: "A TAJ kártyája lejárában van vagy már lejárt. Ha nem megújítja a kártyát a megadott határidőn belül:" followed by a list of consequences: "Nem lesz jogosult egészségügyi ellátásra", "Magánellátásra kényszerülhet", and "Késedelmes megújítás esetén". A red button labeled "TAJ kártya megújítása most" is at the bottom.

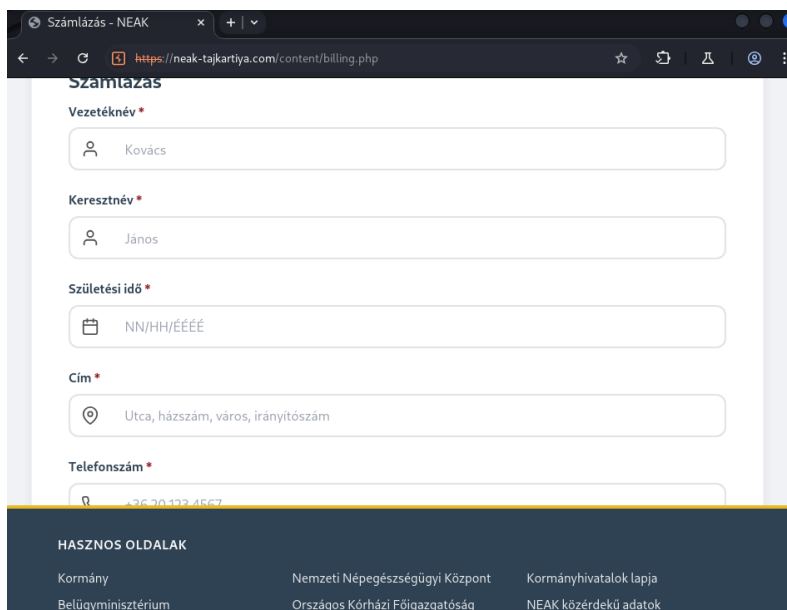
5. ábra: Félrevezető figyelmeztető szöveg

Ezt követően az oldal **több személyes adat megadását kéri a felhasználótól**, többek között a vezeték és keresztnév, a születési idő, a lakcím, valamint a telefonszám megadását. Az így megszerzett adatok a támadók számára lehetőséget adhatnak a felhasználók további megtévesztésére vagy visszaélések elkövetésére.

**TLP: CLEAR**

**TLP: CLEAR**

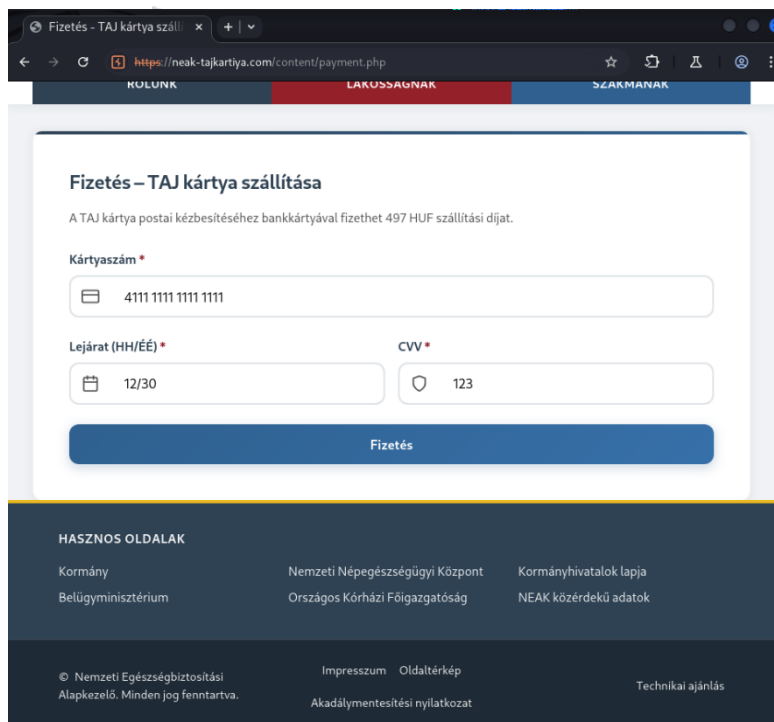
**Szabadon terjeszhető!**



6. ábra Személyes adatok kicsalása

A megadott adatokat az oldal a **csalók által üzemeltetett szerverre továbbítja**, hasonló módon, mint a korábban megadott információk esetében.

A **következő lépésben** az oldal bankkártyaadatok megadását kéri a felhasználótól, többek között a bankkártyaszám, a lejárat idő, valamint a CVC-kód megadását, a TAJ-kártya kiszállításának díjára hivatkozva.



7. ábra: Bankkártya adatok kicsalása

**TLP: CLEAR**

**TLP: CLEAR**

**Szabadon terjeszthető!**

A megadott adatok a támadókhöz kerülhetnek, akik azokat **pénzügyi visszaélésekre, illetve további adathalász vagy csalási kísérletekhez** használhatják fel. Ezért kiemelten fontos, hogy a felhasználók **ne kattintsanak rá az ilyen SMS üzenetekben található hivatkozásokra, és ne adják meg személyes vagy bankkártyaadataikat ismeretlen weboldalakon.**

**Az NBSZ NKI biztonsági javaslatai a következők:**

- Kerülje az **SMS-ben vagy egyéb üzenetküldő alkalmazásokban** kapott hivatkozások megnyitását.
- **Tiltsa le a feladót**, vagy blokkolja a gyanús fiókot az adott üzenetküldő alkalmazásban.
- Használja a **spamként / kéretlen üzenetként történő jelentés** funkciót, ha az alkalmazás lehetőséget biztosít rá.
- **Ne válaszoljon** az ilyen jellegű üzenetekre.
- Kapcsolja be az **ismeretlen feladók szűrését**, ha az alkalmazás ezt lehetővé teszi.
- Kapcsolja ki az **olvasási visszaigazolások küldését**, ha erre lehetőség van (így a támadó kevesebb visszajelzést kap).
- Amennyiben elérhető, kapcsolja ki a **linkelőnézet automatikus megjelenítését**.
- Ellenőrizze, hogy a használt fiókoknál (pl. Apple ID, Google-fiók vagy más szolgáltatói fiók) **be van-e kapcsolva a kétfaktoros hitelesítés**.
- Használjon **erős és egyedi jelszavakat** az online fiókokhoz.
- **Tartsa naprakészen a készülék operációs rendszerét és az alkalmazásokat.**
- Amennyiben lehetséges, tiltsa le az **emelt díjas SMS- és mobil tartalomszolgáltatásokat** a mobilszolgáltatójánál.
- **Rendszeresen ellenőrizze telefonszámláját** ismeretlen vagy gyanús díjak miatt.

Nemzetbiztonsági Szakszolgálat  
Nemzeti Kiberbiztonsági Intézet  
Telefon: +36-1-336-4833  
Incidentsbejelentés: csirt@nki.gov.hu

**TLP: CLEAR**