Riasztás

Szabálysértési bírság befizetésére hivatkozó adathalász üzenetekkel kapcsolatban

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet **riasztást ad ki, szabálysértési bírság megfizetésére kötelező,** megtévesztő adathalász e-mailekkel kapcsolatban.

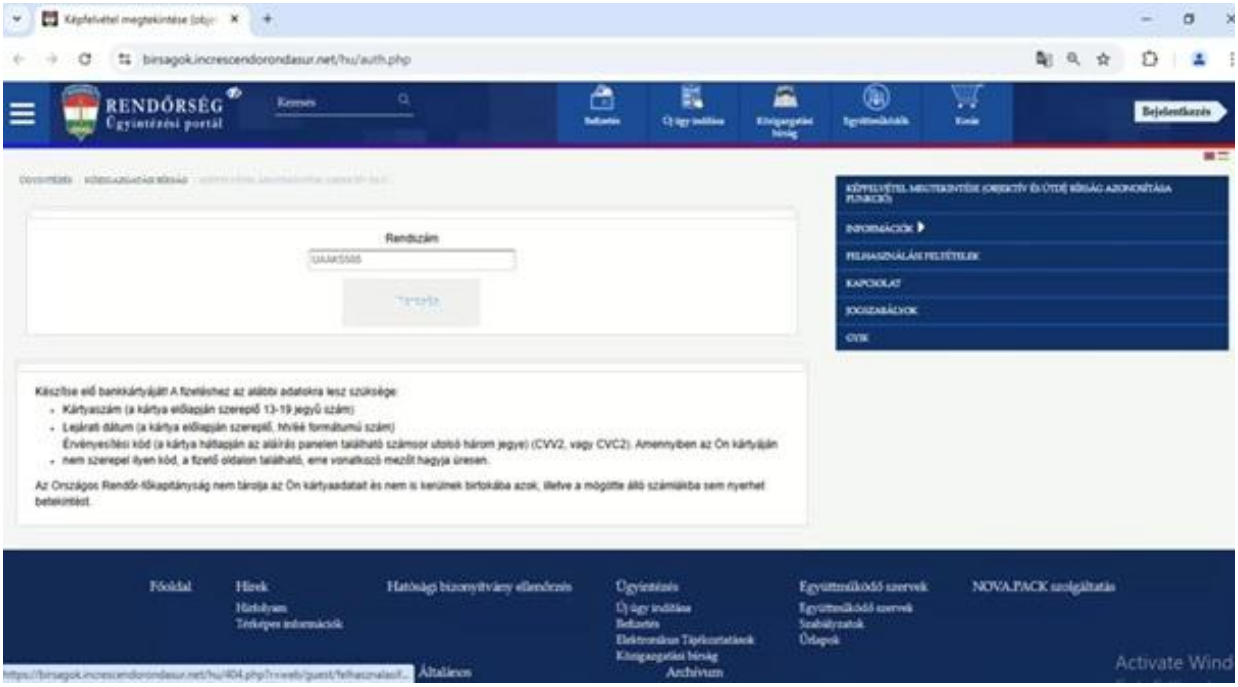
Intézetünkhöz megnövekedett számú állampolgári bejelentés érkezett **káros hivatkozást tartalmazó**, valójában nem fennálló bírság befizetésére hivatkozó, **megtévesztő e-mailekkel** kapcsolatban.

A korábban jellemző **SMS-ben terjesztett káros hivatkozások helyett** a csalók most **e-mail üzenetekben próbálják megtéveszteni a címzetteket**. Az új változat a „*Magyar Országos Központ*” feladótól érkezik, és „*Tisztelt lakos*” megszólítással **szabálysértési bírság befizetésére** próbálnak rávenni, **mobilkommunikációs eszköz közlekedés közbeni használata** miatt. A levél végén az aláíró az „*Országos Rendőrségi Főkapitányság*”.

Az adathalász hivatkozás működése

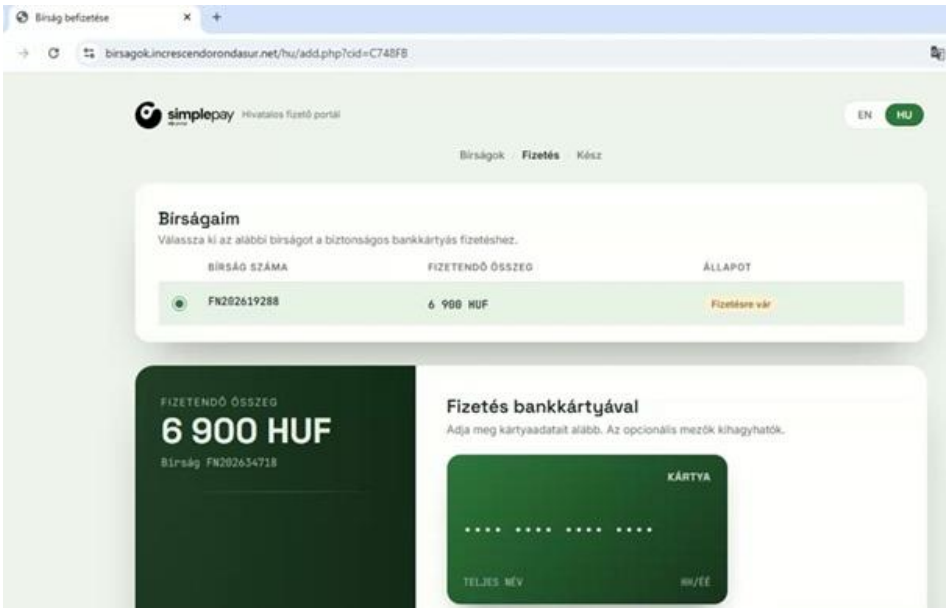
A hivatkozás megnyitását követően egy **hamis Rendőrségi portál** jelenik meg, ahol a **rendszámunk megadását kérik** (1. ábra). A csaló oldal célja, hogy a felhasználó a rendszám megadása után a „Keresés” gombra kattintva továbblépjen. Ezt a műveletet ne hajtsuk végre, és ne adjunk meg adatokat az oldalon.

+36-1-336-4833 csirt@nki.gov.hu



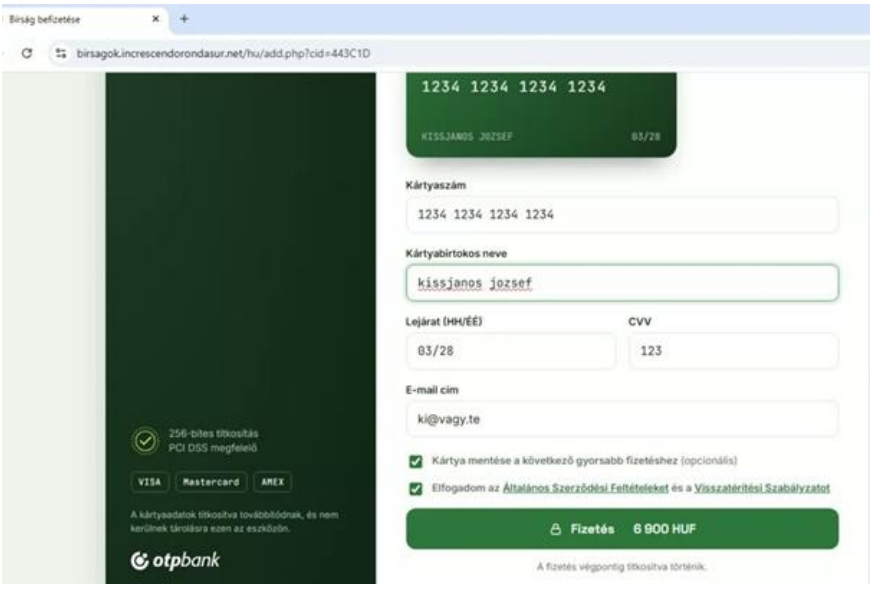
1. ábra Hamis rendőrségi oldal

Ezt követően **megnyílik egy hamis Simplepay oldal**, rajta, „*Bírságaim*”: 6900 HUF befizetendő összeggel (2. ábra).



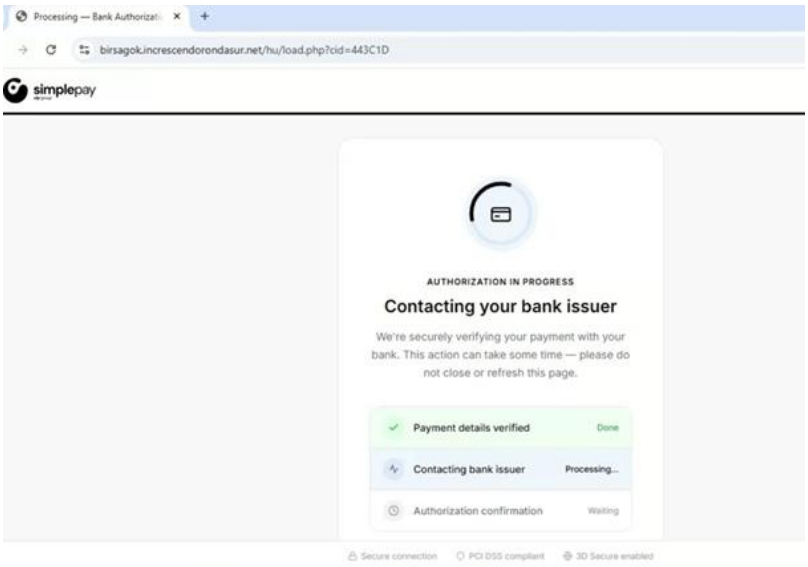
2. ábra Hamis Simplepay oldal

A csaló oldal a kártyaadatok megadása után a „Fizetés” gombra kattintást várja el a felhasználótól (3. ábra). Ezt a műveletet semmiképpen ne hajtsuk végre: ne adjunk meg bankkártya adatokat, és ne kattintsunk a fizetést indító gombra.



3. ábra Kártyaadatok megadása

A fizetés gomb megnyomását követően egy **progress oldal jelenik meg** (4. ábra), mintha beindulna egy fizetési és hitelesítési folyamat a háttérben (ez sosem fejeződik be).



4. ábra Hamis kártyahitelesítési folyamat

Fontos kiemelni, hogy **a támadók folyamatosan alakítják és finomítják módszereiket**, ezért az ilyen üzenetek és a hozzájuk kapcsolódó felületek kezelése során **minden esetben fokozott körültekintés szükséges**. A gyanús tartalmú megkereséseket célszerű kritikusan vizsgálni, és minden esetben ellenőrizni azok hitelességét, mielőtt bármilyen műveletet végrehajtanánk.

Javasolt intézkedések

- Mindig ellenőrizzük a feladó e-mail címét, és hasonlítsuk össze a korábbi, hivatalos üzeneteknél megszokott címmel.
- Legyünk gyanakvók a sürgető, fenyegető vagy nyomást gyakorló hangnemmel szemben, különösen, ha azonnali fizetést kérnek.
- Ne kattintsunk az e-mailben található linkekre, és ne nyissunk meg mellékleteket, ha az üzenet hitelessége nem egyértelmű.

- A fizetési felszólításban szereplő információkat mindig ellenőrizzük más csatornán is, például telefonon vagy a szolgáltató hivatalos ügyfélszolgálatán keresztül.
- Soha ne a levélben megadott elérhetőségeken próbáljuk visszaigazolni az üzenet valódiságát, mert ezek is hamisak lehetnek.
- Ne adjunk meg személyes, banki vagy belépési adatokat e-mailben érkező kérésre.
- Tartsuk naprakészen az operációs rendszert, a böngészőt és a biztonsági szoftvereket, mert ezek csökkentik a kártevők és a csaló oldalak kockázatát.
- Ha az üzenet gyanús, jelezzük azt az informatikai vagy biztonsági felelősnek, illetve az érintett szervezet hivatalos ügyfélszolgálatának.
- Kétség esetén inkább ne fizessünk, amíg a felszólítás jogosságát hiteles forrásból nem igazolták.

Amennyiben támadásra utaló jelet talál, vegye fel velünk a kapcsolatot a CSIRT@nki.gov.hu **email címen!**