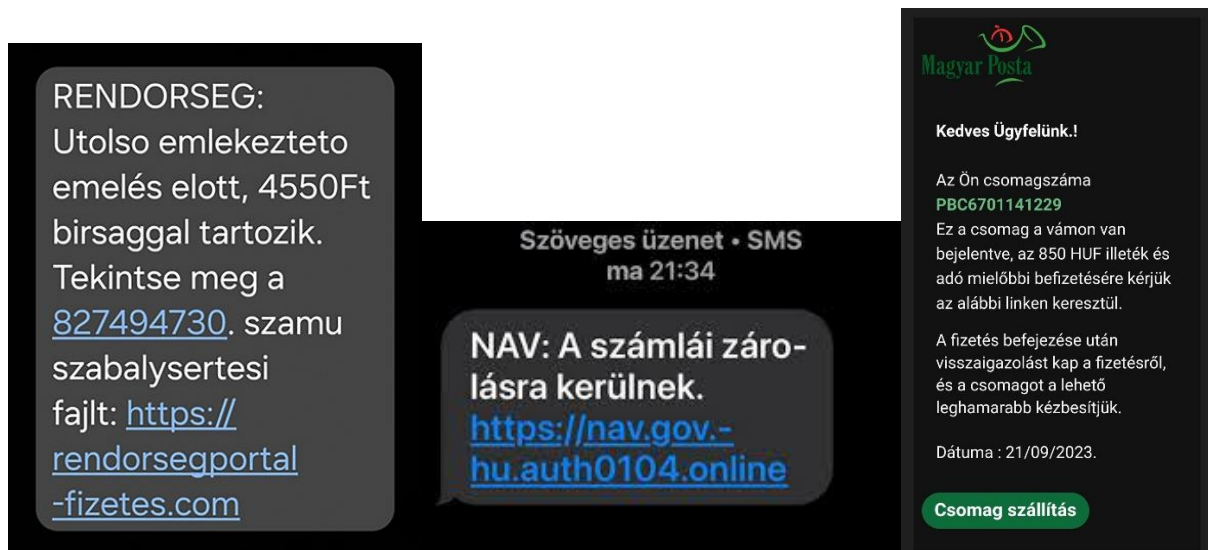


HATÓSÁG NEVÉBEN ÉRKEZŐ CSALÓ SMS



Adathalász csalogók valótlan befizetés kezdeményezésével próbálnak meg jogtalanul pénzhez jutni, valamint személyes- és bankkártya adatokat megszerezni oly módon, hogy valamilyen hatóság (NAV, rendőrség stb.) vagy cég (pl. MVM, posta) nevében lépnek fel, és bírságra, útdíj tartozásra, hátraléokra hivatkozva visszaélnék a hatóságok/cégek nevével. Ismét szeretnénk felhívni a figyelmet arra, hogy a rendőrség bírság esetén nem kommunikál SMS-ben!

Annak érdekében, hogy ne váljanak online csalogók áldozatává, kérjük, fogadják meg tanácsainkat!

- ✓ NE kattintsanak a linkre, töröljék az üzenetet!
- ✓ NE adják meg sem személyes, sem bankkártya adataikat!
- ✓ Adataik védelme érdekében fontos, hogy a rendőrség e-ügyintézési portálját kizárólag a <https://ugyintezes.police.hu/> honlap cím beírásával ériék el!
- ✓

3+1 jel, amiről felismerhetők az átverésgyanús SMS-ek

Az ilyen üzenetekben gyakran ékezetek nélküli szavak szerepelnek, vagy helyesírási hibák fordulnak elő, általában rossz magyarsággal, helytelenül fogalmazzák meg őket.

Legtöbbször külföldi telefonszámról érkeznek ezek az SMS-ek.

Az üzenetben szereplő linkben nem a létező, ismert szolgáltató vagy internetes áruház webcíme, hanem általában egy betűkből és számokból kombinált hivatkozás szerepel.

A +1 általában valami aprócska ráadás szokott lenni, itt viszont talán ez a legfontosabb: a csalogó SMS-ek szinte mindig sürgető jellegűek. Nem sima fizetési felszólítások, hanem azonnali cselekvésre ösztönöznek például azzal, hogy a fizetendő összeg emelkedésével fenyegetnek.

Az internetes csalásokkal kapcsolatban a kiberpajzs.hu oldalon találnak hasznos információkat.