Az MNB telefonszámait is klónozzák a kibercsalók, banki ügyintézőnek hazudják magukat

Az MNB több telefonszámának másolásával is telefonálnak ismét csalók magánszemélyeknek, akár a jegybank, akár valamelyik hitelintézet nevében. A beszélgetés során az ügyfelek bizalmas banki adatait, pénzét szereznék meg, vagy kémprogramot töltetnének le velük. Az MNB és a bankok nem keresnek meg ügyfeleket ilyen ürügyekkel. A megkárosított állampolgároknak célszerű a rendőrséghez fordulni.

A Magyar Nemzeti Bankra (MNB) hivatkozó tavaly szeptemberi adathalász támadások után újabb telefonos csalási kampány zajlik a jegybank telefonszámaival visszaélve. Az MNB ügyfélszolgálatára csupán az elmúlt egy hét alatt 14 ügyféljelzés érkezett emiatt.

A bűnözők az MNB egyes telefonszámait másolják le, s így hívnak fel magánszemélyeket. Valamelyik kereskedelmi bank ügyfélszolgálataként vagy magának az MNB-nek a nevében jelentkeznek, mivel állításuk szerint gyanús tranzakciót észleltek az ügyfél számláján vagy bankkártyájánál. Konkrét, ám valójában nem létező személyeket (pl. „Szabó Zoltán”) is megneveznek, akik kibercsalókként épp támadják az ügyfelet.

A csalók az állítólagos „támadás” elhárítására állításuk szerint biztonságba helyeznék az áldozatok pénzét. Ehhez bizalmas banki adatait kérik el (például: bankkártyaszám, lejárat, cvc kód, PIN kód; internet- vagy mobilbanki jelszavak és megerősítő kódok); vagy megpróbálják rávenni az áldozatot, hogy utalja át „biztonságos” – valójában a csalók által kezelt – számlára a pénzét. Más esetekben „vírusirtót” – valójában az ügyfél számítógépéhez és banki alkalmazásához távoli hozzáférést biztosító kémprogramot – töltetnének le velük.

Ha állítólagosan kereskedelmi banktól jött a hívás, s az ügyfél esetleg visszahívja a csalókat, meglepődve tapasztalhatja, hogy a telefonszám valódi tulajdonosa, az MNB jelentkezik. A telefonbeszélgetéses csalások (vishing) a személyes kontaktus miatt jóval hihetőbbnek tűnhetnek, mint az e-mail-es vagy sms alapú adathalász támadások, ráadásul olyanokat is elérnek, akik nem használnak internet- vagy mobilbankot.

Sem az MNB, sem a kereskedelmi bankok nem kérik el soha az ügyfelektől telefonon vagy elektronikus úton azok bizalmas, a banki rendszerbe történő belépésre szolgáló adatait. Ilyen telefonhívásnál érdemes pontosító kérdéseket feltenni, gyanú esetén megszakítani a kapcsolatot és az ismert (az adott bank honlapján is feltüntetett) banki ügyfélszolgálati telefonszámon, illetve az MNB ügyfélszolgálatán érdeklődni. Azonnali gyanúra adhat okot, ha a telefonáló állítólag állami hatóságnál, intézménynél vagy bűnüldöző szerveknél dolgozik, mégis – miután az ügyfél bizalmatlan vagy nem hisz neki – fenyegető hangnemet használ.

Ha egy ügyfél mégis küldött pénzt a csalóknak, átadta adatait vagy letöltött egy kémprogramot, érdemes azt is haladéktalanul bejelenteni a bankjának (az összeg esetleges visszaszerzése érdekében) és a rendőrségnek. Ha az MNB a nevével való visszaélés kapcsán károsultakról szerez tudomást, minden esetben maga is büntetőfeljelentést tesz a nyomozó hatóságnál.

A kiberbiztonsági kockázatok megelőzésére, csökkentésére 10 állami intézmény, köztük az MNB és a pénzpiac szereplői KiberPajzs néven közös kommunikációs és edukációs kampányt folytatnak, továbbá elemzik a folyamatokat, lehetséges intézkedéseket az elektronikus pénzügyi szolgáltatásokat

igénybe vevő ügyfelek támogatására, védelmére. Az együttműködő hatóságok lépéseket tesznek a hívószám-hamisítás megelőzése érdekében is. Érdemes felkeresni az MNB Pénzügyi Navigátor weboldalának digitális biztonsággal kapcsolatos oldalát is, amelyen hasznos információkat találhatók a témában.

Sajtókapcsolat:

- +36 1 428 2600
- sajto@mnb.hu

Eredeti tartalom: Magyar Nemzeti Bank

Továbbította: Helló Sajtó! Üzleti Sajtószolgálat

Ez a sajtóközlemény a következő linken érhető el:
https://hellosajto.hu/13288/az-mnb-telefonszamait-is-klonozzak-a-kibercsalok-banki-ugyintezonek-hazudjak-magukat/