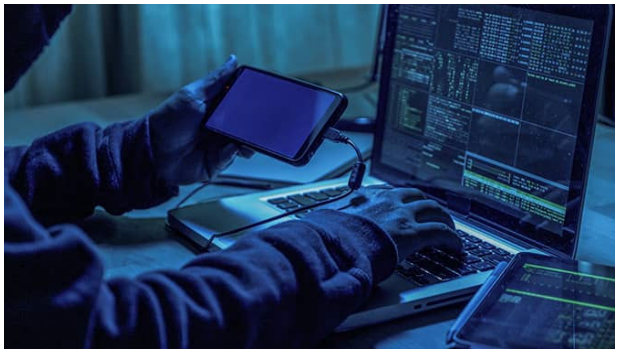
HÍVÓSZÁM SPOOFING: HÍVÓSZÁM-HAMISÍTÁS!



A hívószám **spoofing**, azaz hívószám-hamisítás a vishing (hamis banki hívások) adathalász tevékenységek egyik speciális elkövetési technikája. Lényege, hogy az elkövetők módosítják a hívószámot, ami a hívott fél telefonjának kijelzőjén megjelenik, ezzel elrejtve a valódi hívó fél azonosságát. Vagyis híváskor nem a hívást kezdeményező igazi telefonszáma jelenik meg a potenciális áldozatok készülékén, hanem egy másik, jellemzően olyan, ami ismerős: például egy banké, ezáltal még inkább hitelesnek beállítva a hívást. Az ilyen hívások célja elsősorban a bizalom kiépítése, illetve az adathalász támadások elsőszámú védvonalának, az óvatosságnak a kiiktatása: ha az áldozat ismerős telefonszámot lát, amikor hívják, kevésbé lesz gyanakvó és megnő az esélye annak, hogy teljesíti, amit a hívó fél kér tőle.

Mit tegyen?

- Kezelje óvatosan, fenntartással a kéretlen telefonhívásokat!
- Minél sürgetőbb a hívás és az üzenet, annál gyanúsabb! Lassítson és gondolja át alaposan, hogy mit is kérnek valójában!
- Gyanús telefonhívás esetén ne adjon meg személyes adatokat és szakítsa meg a beszélgetést!
- Ha a kijelzett telefonszám valóban a bank ügyfélszolgálati telefonszáma, az sem garancia arra, hogy tényleg onnan keresik. Annak ellenőrzésére, hogy az illető valóban az, akinek mondja magát, keresse meg a szervezet telefonszámát és lépjen vele kapcsolatba közvetlenül! Fontos, hogy az ügyfélszolgálat felé a kapcsolatfelvételt, hívást Ön kezdeményezze az ismert telefonszámon, ne hagyatkozzon visszahívásra vagy átkapcsolásra, amit a csalók felajánlanak.
- Az ellenőrzéshez ne használja a hívó által megadott telefonszámot! A szám hamis lehet vagy létrehozhatták kifejezetten a csaláshoz.
- A csalók az interneten könnyen megszerezhetik az alapvető információkat Önről, például a közösségimédia-profilok felhasználásával. Nem bízhat meg a hívóban csak azért, mert ő ismeri ezeket az adatokat.
- Ha hitelesnek gondolja a telefonhívást, akkor is kérjen keresztazonosítást, melynek során a feltett kérdésekre (például anyja születési neve) a válaszok egyik felét az intézmény ügyintézője adja meg, a válaszok másik felét pedig Ön!

PEST VÁRMEGYEI RENDŐR-FŐKAPITÁNYSÁG
BŰNMEGELŐZÉSI OSZTÁLY

1145 Budapest, Róna utca 124. ✉: 1557 Budapest, Pf. 20. ☎: 460-7101; BM: 28-811
E-mail: elbir@pest.police.hu KÉR azonosító: ORFK PEST

- Soha ne adja meg a betéti vagy hitelkártyája PIN-kódját, CVV-kódját, online banki jelszavát vagy az egyszer használható, második hitelesítési kódot! A bankok, banki ügyintézők sosem kérik el ezeket az információkat!
- Soha ne telepítsen mások kérésére olyan programot számítógépére vagy telefonjára, amit nem ismer! A csalók sokszor vírusvédelmi megoldásnak vagy szoftverfrissítésnek beállítva, álcázva próbálják rávenni áldozatukat arra, hogy visszaéléshez használható programot telepítsenek.
- Soha ne utaljon pénzt telefonon érkező kérésre! Egyik bank sem kér ilyet.
- A csalási szándékú hívásokat jelentse a bankjának!

Pest Vármegyei Rendőr-főkapitányság

PEST VÁRMEGYEI RENDŐR-FŐKAPITÁNYSÁG
BŰNMEGELŐZÉSI OSZTÁLY

1145 Budapest, Róna utca 124. ✉: 1557 Budapest, Pf. 20. ☎: 460-7101; BM: 28-811
E-mail: elbir@pest.police.hu KÉR azonosító: ORFK PEST