ELBIR
Elektronikus Lakossági Bűnmegelőzési Információs Rendszer

Biztonsági tanácsok NetBank ügyfeleknek

Az elmúlt években jelentős mértékben bővült az elektronikus csatornák használata (netbank, mobilbank) a banki ügyfelek körében, így ennek megfelelően a bűnözői csoportok is új technikákat fejlesztettek ki céljaik elérése érdekében. A kifejlesztett új támadási technikákkal támadók elsődleges célja a netbank használatához szükséges adatok megszerzése közvetlenül az ügyfelektől, majd azok anyagi haszonszerzés céljából csalásra történő felhasználása.

Az Erste Bank Hungary Zrt. az alkalmazott különféle biztonsági megoldások révén már eddig is számos lépést tett a kockázatok csökkentése érdekében. Ezek megfelelő működéséhez azonban az ügyfelek aktív közreműködésére is szükség van. Ezért fontos, hogy megfogadják biztonsági tanácsaikat.

Általános biztonsági tanácsok:

- Használjanak naprakész vírusvédelmi, tűzfalvédelmi programokat eszközeik (számítógép, mobiltelefon, táblagép) vírus, kémprogram, kártékony szoftverek elleni védelme érdekében!
- Tartsák naprakészen az eszközeik által használt operációs rendszereket (Windows, Linux, MacOS, iOS, Android) és az eszközökre telepített alkalmazásokat a gyártók által kiadott hivatalos frissítések, javító verziók rendszeres telepítésével!
- Kizárólag legális szoftvereket használjanak eszközeiken, melyekre ne telepítsenek ismeretlen forrásból származó, kétes eredetű alkalmazásokat!
- Idegen, ismeretlen eredetű adathordozót (pen drive, memóriakártya, CD, DVD, floppy lemez, külső merevlemez stb.) ne csatlakoztassanak a számítógéphez!
- Használjanak korlátozott jogosultságokkal rendelkező felhasználót a mindennapos használathoz (pl. internetezés), és kerüljék az adminisztrátori jogosultságokkal rendelkező felhasználók használatát!

- Tiltsák le eszközeik esetében az ismeretlen vezeték nélküli hálózatokhoz (Wi-Fi, Bluetooth) történő automatikus csatlakozást!
- Kérjük, azonnal vegyék fel a kapcsolatot a bankjuk telefonos ügyfélszolgálatával amennyiben látszólag a banktól érkező személyes vagy bizalmas adatok (név, telefonszám, NetBank azonosító, jelszó) megadására felszólító üzenetet kap, mert a pénzintézet ügyfeleitől ilyen jellegű adatokat soha nem kér e-mail üzenetben vagy SMS-ben!

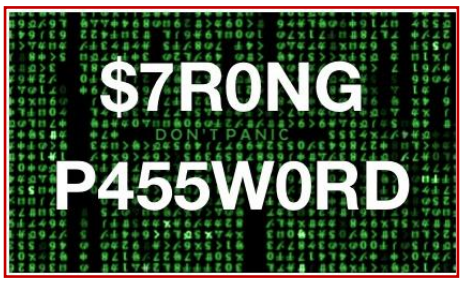
BÁCS-KISKUN MEGYEI RENDŐR-FŐKAPITÁNYSÁG
BŰNMEGELŐZÉSI OSZTÁLY
K E C S K E M É T
6000 Kecskemét, Batthyány u. 14., Postacím: 6001 Kecskemét, Pf.:302 Tel:76/513-300/30-27, BM: 33/30-27, Fax: 76/513-300/30-98 BM 33/30-98, Mobil:: +3620/560-5146
e-mail: elbir@bacs.police.hu web: http://www.police.hu/hirek-es-informaciok/bunmegelozes

- Böngészőjükhöz használt kiegészítőket, bővítményeket (add-on-ok, plugin-ek) korlátozottan használják! Ne telepítsenek olyan bővítményt a böngészőjükhöz, amelynek a fejlesztőjében/forgalmazójában nem bíznak meg, vagy a bővítményt nem, vagy csak ritkán használják!

- Ismeretlen feladótól származó üzenetet, csatolmányt, linket minden esetben kezeljenek kiemelt körültekintéssel, a levélre történő válaszadást vagy megnyitásukat pedig - amennyiben lehetséges - mellőzzék!

Jelszókezeléssel, bankkártya adatokkal kapcsolatos biztonsági tanácsok:

- Ne használjanak jelszavaikban személyes információkat (születési dátum, telefonszám, lakcím, kedvenc háziállat, házastárs neve, PIN vagy TPIN kód stb.), valamint szótár alapú szavakat!



- Javasolt rendszeresen, legalább háromhavonta megváltoztatni a használt jelszót.

- Használjanak legalább 8 karakter hosszú, kis és nagybetűt, számot, speciális karaktereket tartalmazó jelszavakat!

- Kapcsolják ki a böngészőben a jelszavak automatikus megjegyzésére szolgáló funkciót!

- Bankkártya adatait (bankkártyaszám, lejárati dátum, CVV/CVC2 kód) csak olyan weboldalakon adják meg, amelyeket ismernek és megbízhatónak tartanak. E-mail üzenetben vagy bármilyen felugró felhívás során soha ne adják meg ezeket!

- Használják a Bank által nyújtott biztonsági SMS szolgáltatásokat (Kártyaőr, Számlaőr, Internetes vásárlás ellenőrző SMS kód), és ügyeljenek arra, hogy mobiltelefonjuk mindig Önöknél legyen!

NetBank használattal kapcsolatos biztonsági tanácsok:

- Saját eszközeiket használják Netbankolás céljára, és ne nyilvános (pl. Internet-kávézó, könyvtár) vagy sok különböző ember számára hozzáférhető eszközt!

- Ne használják a Netbank jelszavát más weboldalakon. Mindenkor ellenőrizzék, hogy a NetBank weboldal neve pontosan jelenik-e meg a böngésző címsorában. Különösen ügyeljenek, hogy a cím a https:// karaktersorozattal kezdődik (nem pedig http:// sorozattal), továbbá ellenőrizzék, hogy a böngészőben megjelent-e a biztonságos kapcsolatot jelölő kis lakatot formázó ikon!

- Tanúsítvány hibára történő figyelmeztetések esetében szakítsák meg a kapcsolatot és lépjenek kapcsolatba a bankkal!

- A NetBank bejelentkezéskor csak a NetBank azonosító és a bejelentkezési jelszó megadása szükséges.

- SMS-ben belépési kódot csak a szolgáltatást külön igénybe vevő ügyfeleinek küld a bank.

BÁCS-KISKUN MEGYEI RENDŐR-FŐKAPITÁNYSÁG
BŰNMEGELŐZÉSI OSZTÁLY
K E C S K E M É T
6000 Kecskemét, Batthyány u. 14., Postacím: 6001 Kecskemét, Pf.:302 Tel:76/513-300/30-27, BM: 33/30-27, Fax: 76/513-300/30-98 BM 33/30-98, Mobil:: +3620/560-5146
e-mail: elbir@bacs.police.hu web: http://www.police.hu/hirek-es-informaciok/bunmegelozes

- A tranzakció hitelesítési SMS üzenet, valamint az opcionálisan igénybe vehető belépési SMS üzenet tartalma minden esetben különböző, ezért javasoljuk, hogy minden esetben olvassák el a Banktól kapott SMS üzeneteket, mielőtt az abban szereplő kódot a NetBankban megadják!

- A tranzakciók aláírására szolgáló SMS szövegében ellenőrizzék, hogy ténylegesen azok az adatok szerepelnek-e az üzenetben, amelyeket a NetBankban megadtak, és csak az ellenőrzést követően használják fel a kódot a NetBankban a tranzakció tényleges aláírására.

- NetBank használat befejezését követően minden esetben használják a „Kilépés” gombot, mielőtt bármilyen más weboldalra elnavigálnak vagy bezárják a böngészőt!

Hordozható eszközökkel (táblagép, okostelefon) kapcsolatos biztonsági tanácsok:

- Lehetőleg ne használják NetBank használatra azt a hordozható eszközt, amelyre a Banktól kapott SMS üzeneteket is kapják!

- Javasolt, hogy az eszköz gyári jogosultság beállításait ne változtassák meg; ne root-olják, ne jailbreak-eljék az eszközt!

- Használjanak képernyőzár feloldás elleni védelmet (PIN kód, egyedi mintázat)!

- Ne tároljanak személyes adatokat (bankkártyaszám, PIN vagy TPIN kód) a készüléken!

- Ne telepítsenek internetről közvetlenül letöltött alkalmazást/szoftvert eszközeire, helyette használjanak a hivatalos forrásokat vagy terjesztési csatornákat (pl. Google Play, Apple Appstore, Windows Market)!

- Minden esetben ellenőrizzék a telepíteni kívánt alkalmazás által használni kívánt jogosultságkérelmeket és szolgáltatásokat, és amennyiben egy alkalmazás a profiljába nem illeszkedő funkciókat is használni kívánnak (pl. háttérkép alkalmazás SMS-t akar küldeni), akkor ne folytassák a telepítést! Ezt az ellenőrzést az alkalmazások frissítésekor is mindig végezzék el, mert az új alkalmazás verziók gyakran többlet jogosultságokat kérnek.

- Javasolt a nem használt szolgáltatásokat (Bluetooth, GPS, NFC) kikapcsolni, és csak tényleges használat idejére engedélyezni.

- Amennyiben az eszköz operációs rendszere vagy az eszköz gyártója támogatja, javasolt titkosítani az eszköz háttértárolóin tárolt adatokat.

Forrás: https://www.erstebank.hu/hu/biztonsagi-tanacs-netbank-ugyfelek-szamara

BÁCS-KISKUN MEGYEI RENDŐR-FŐKAPITÁNYSÁG
BŰNMEGELŐZÉSI OSZTÁLY
K E C S K E M É T
6000 Kecskemét, Batthyány u. 14., Postacím: 6001 Kecskemét, Pf.:302 Tel:76/513-300/30-27, BM: 33/30-27, Fax: 76/513-300/30-98 BM 33/30-98, Mobil:: +3620/560-5146
e-mail: elbir@bacs.police.hu web: http://www.police.hu/hirek-es-informaciok/bunmegelozes