AZ ÚJ FIZETÉSI MÓD

Információbiztonsági tájékoztató

Binx Zrt. H-1031 Budapest, Záhony utca 7. HX épület

A BinX Zrt. a Magyar Nemzeti Bank felügyelete alatt működő, magyar alapítású intézmény.

MNB Engedélyszámok: H-EN-I-351/2022., H-EN-I-381/2023.

www.binx.hu

Ügyelj az eszközeid biztonságára!

A BinX mobilbank alkalmazást csak a Google vagy az Apple hivatalos alkalmazásboltjából telepítsd.

Ne töltsd le alkalmazásokat ismeretlen forrásból, nem megbízható alkalmazásboltokból vagy internetes helyekről.

Az eszköz beépített védelmi beállításait, szolgáltatásait ne kapcsold ki, ne kerüld meg. (pl. ne engedélyezd a hivatalos alkalmazásbolttól különböző forrásból származó mobil alkalmazások telepítését, mobil eszközödet ne „root-old", ne „jailbreak-eld".)

Alkalmazások telepítése, használata során az alkalmazások hozzáférést kérhetnek bizonyos eszközökhöz, adatokhoz, funkciókhoz (pl. a kamera, mikrofon használata, telefonhívások indítása, SMS üzenetek küldése, média tartalmak elérése). Csak olyan jogosultságokat engedélyezz, melyek az alkalmazás deklarált céljával összhangban vannak. Ha az alkalmazás funkciójához nem illő jogosultságokat kér, szakítsd meg a telepítést, vagy töröld az app-ot.

A bankolásra használt eszközödre ne telepíts távoli vezérlésére szolgáló alkalmazást. Ne engedélyezz távoli hozzáférést az eszközhöz senkinek.

A BinX szolgáltatások elérésére használt eszközeidet tartsd naprakészen, a biztonsági frissítéseket haladéktalanul telepítsd.

Asztali számítógépeden, laptopodon mindig használj naprakész végpontvédelmi szoftvert (tűzfal, antivírus, böngésző védelem).

Használat után az eszközt mindig zárold.

Ha mobileszközödet, melyen a BinX mobilbank alkalmazást használod, elveszíted vagy ellopják, értesítsd a BinX ügyfélszolgálatát egy másik regisztrált BinX mobil alkalmazáson keresztül (ha van ilyen), vagy hívd a BinX ügyfélszolgálat telefonszámát.

Ügyelj a kommunikáció biztonságára!

Saját WiFi hálózatodat erős titkosítással védd, a hálózati eszköz alapértelmezett jelszavát változtasd meg hosszú, véletlenszerű, egyedi jelszóra.

Kerüld a nyilvános vagy nem megbízható WiFi hálózatokat internetes bankoláshoz vagy egyéb internetes tevékenységhez.

Legyél óvatos az adathalász kísérletekkel!

Ne kattints gyanús linkre vagy tölts le mellékleteket ismeretlen forrásból.

Nem várt üzeneteket (pl. email, SMS) mindig a megfelelő kontextusban vizsgáld, pl.

- Ha nem rendeltél semmit, akkor egy csomagkézbesítésre vonatkozó üzenet nem lehet valós, lehetséges, hogy internetes támadás része.
- Bármilyen sürgetést az üzenetben kezelj gyanakvással. (Pl. „zároljuk a számláját, ha azonnal nem frissíti az adatait a következő linken…”, „óriási nyeremény, ha 5 percen belül…”, stb.)
- Ha valami túl szép ahhoz, hogy igaz legyen, akkor valószínűleg nem is igaz (pl. „ingyenes iPhone az első 10 jelentkezőnek”)

A BinX Zrt soha nem kéri felhasználóknak címzett email-ben, SMS-ben vagy egyéb nyilvános internetes üzenetküldő platformon bármilyen alkalmazás letöltését. Ha ilyen üzenetet kapsz, ne hajtsd végre a telepítést.

A BinX Zrt elsődleges kommunikációs platformja ügyfelei irányába a mobil alkalmazás. Minden BinX nevében érkező telefonhívást fokozott óvatossággal kezelj.

Legyél óvatos az interneten!

Lehetőség szerint csak megbízható oldalakat látogass, kerüld a klikkvadász hirdetéseket, a bizonytalan hátterű weboldalakat.

Internetes szolgáltatásokba való regisztrációkor mindig különböző jelszavakat használj.

Internetes jelszavaidat ne mentsd el böngészőben, ne tárold szövegfájlban, titkosítatlan dokumentumban. Jelszavaid, internetes azonosítóid tárolására használj biztonságos jelszószéf alkalmazást.

Online fizetéskor bankkártya adataidat csak ismert, megbízható kereskedelmi vagy pénzügyi szolgáltatóknak add meg. Megnyugtató, ha fizetéskor a webshop egy közismert bank fizetési felületére irányít. Ismeretlen webshop, szolgáltatás saját fizetési felületét inkább ne használd.

Bizonyos webshop-ok, fizetési szolgáltatások felajánlják a bankkártya adatok mentését későbbi fizetések meggyorsítása céljából. Csak jól ismert, megbízható platformok, szolgáltatások esetén élj ezzel a lehetőséggel.

Bankkártyás Internetes vásárlás esetén lehetőség szerint használj

- virtuális kártyát, melyre csak a vásárlásnak megfelelő összeget tölts, vagy
- egyszer használatos virtuális kártyát, ahol a kártyaadatok a felhasználást követően érvénytelenné válnak, vagy
- használd ki az online vásárlásra rugalmasan beállítható vásárlási limitet, ha a kártyakibocsátó biztosít ilyen lehetőséget. Az online vásárlási limit alapbeállítása legyen nulla, vásárlás előtt állítsd át a vásárlás összegének megfelelő értékre, majd a fizetést követően állítsd vissza az alapbeállításra.

Számláddal, bankkártyáddal kapcsolatos kimenő pénzügyi tranzakciókról kérj azonnali értesítést mobil eszközre küldött push üzenet vagy SMS formájában.