BIZTONSÁGOS BANKOLÁS

A TRIVE BANK ZRT. mindent megtesz a biztonságos bankolásért és ennek keretén belül ügyfeleit az alábbi tanácsokkal látja el annak érdekében, hogy a bankolás során az adatait, pénzügyi tranzakcióit biztonságban tudhassa.

Általános tanácsok:

- **Figyeljen az hátköznapi nyelven nevezett "adathalász levelek"-re.** Egyes csalók látszólag a bank nevében küldött e-mailekben kérhetik fel Önt a legkülönbözőbb indokkal (rendszerfrissítés, azonosító tiltás, rendszerkarbantartás, adategyeztetés stb.) kéri arra, hogy megadja banki adatait a bankhoz hasonlító weboldalon. A levelekben jellemzően közös, hogy minden esetben kérik a csaló weboldal felkeresését, és a személyes / pénzügyi adatok megadását**.** Az oldal eredetiségét, hitelességét könnyen ellenőrizheti: az egeret a megadott linkre húzva a böngésző megmutatja az oldal címét, így azonnal kiderül, hogy az nem banké. (Figyelmesen nézze meg a hivatkozásokat, néha csak 1-2 betű tér el az eredetitől!) **Soha ne kattintson ilyen oldalakra, és semmiképpen ne adja meg adatait. A TRIVE BANK Zrt. nem küld ilyen típusú és ilyen kéréseket tartalmazó leveleket ügyfeleinek.**
- Mindig ez eredeti linket használja, soha ne használjon közösségi felületeken vagy közösségi médiában keresztül érkezett banki linket!
- Amikor új felhasználóként / ügyfélként regisztrál akkor az úgynevezett "mobil" kódot különös gonddal kezelje. Ügyeljen rá, hogy ez a kód más kezébe ne kerüljön.
- Ha bármilyen gyanús körülményt észlel, vagy véletlenül megadta adatait egy csaló weboldalon, azonnal hívja a +36 30 534 9857-es telefonszámot vagy írjon nekünk a központi ügyfélszolgálati címre ugyfelszolgalat@trive.hu

Internetes vásárláshoz kapcsolódó tanácsok:

- Bankkártya-adatait soha ne mentse el a vásárlás során!
- Ellenőrizze a webáruház megbízhatóságát, ismertségét. Ha korábban még nem vásárolt az adott online boltban, ellenőrizze, hogy esetleges probléma esetén hol lehet elérni a bolt üzemeltetőit. Ha semmilyen cégadat, címadat nem szerepel, csak egy e-mail cím, vagy egy mobiltelefonszám, érdemes megfontolni a vásárlástól való elállást. Ha mindenképpen rendelne, érdemes lehet először egy kisebb összeggel kipróbálni, tényleg elküldik-e a terméket. Az internetes értékelések, vélemények segíthetnek, ám nincs rá garancia, hogy azok valóban függetlenek.
- Külföldi webáruházak esetében megrendelés és fizetés előtt tájékozódjon az esetleges garanciális, illetve panaszkezelési lehetőségekről. Különösen a kisebb értékű termékek esetén a visszaküldés költsége olykor magasabb, mint a termék vételára.
- Ami túl szép ahhoz, hogy igaz legyen, az általában nem igaz, főleg ha ingyenes! Reálisan mérlegelje a kihagyhatatlan ajánlatokat és ha a megszokottnál jelentősen olcsóbban kínálnak egy terméket, alaposan olvasson utána a részleteknek, különösen márkás szórakoztató-elektronikai cikkek vagy ruhák esetén.

Eszköz, jelszó és hálózati tanácsok:

- Számítógép/Notebook és okos (telefon, táblagép) termékek naprakész operációs rendszer és antivírus/ kártékony kód elleni védelmi alkalmazások aktív használata.
- Naprakész internetes böngésző használata.
- Tűzfal szoftver aktív használata
- A jelszó ne utaljon a használójára, vagy a használat céljára, rendszerre.
- A jelszó ne legyen szótárban megtalálható szó, telefonszám, név, dátum, stb.
- A jelszó legyen könnyen megjegyezhető, de nehezen kitalálható.
- Soha ne ossza meg, vagy írja le jelszavát.
- Minden hozzáféréshez eltérő és minden esetben ún. erős jelszót használjon.
- A jelszó feleljen meg a TRIVE Bank által javasolt jelszóképzési szabályaira.
- Mielőtt belépne a TRIVE Bank felületre, kérjük ellenőrizze a böngésző címsorában a nevet.
- Lehetőség szerint kerülje a publikus, jelszóval nem védett WiFi hálózaton keresztül bonyolított tranzakciókat.
- A böngészők által kínált felugró ablak blokkolót kapcsolja be.
- Csak megbízható, Ön által ismert számítógépről jelentkezzen be a TRIVE Bank felületére.
- Ne használja a böngészők által felajánlott jelszó megjegyzése opciót.

Gyanús (telefon)hívások:

Gyanakodásra akad okot ha

- olyan bank nevében keresik telefonon, amelynek nem ügyfele és esetleg még “át is kapcsolják” a hívást ahhoz a bankhoz, amelynek ügyfele;
- a hívás során a telefonra érkező úgynevezett “megerősítő kód”-ot kell bediktálni;
- biztonsági incidensre hivatkoznak és ezért minden személyes adatot elkérik “egyeztetés” céljából,
- arra kérik, hogy telepítsen egy (új) alkalmazást a telefonra, tábla vagy számítógépre;
- azzal hívják fel, hogy a pénz veszélyben van, és át kell utalni biztonsági okokból egy általuk megadott számlára;
- a bankkártya adatokat (CVV kóddal együtt) - mobilbanki azonosítóval és jelszóval elkérik.

Online játékok esetében:

- Minden olyan üzenettel legyen körültekintő, amiben arra kérnek, hogy valamit töltsünk le vagy kattintsunk egy hivatkozásra! Azok a csalók, akik az adatainkat akarják megszerezni, általában játékon belüli üzenetekkel, adathalász e-mailekkel próbálkoznak. Ha ezekben az üzenetekben sürgetnek minket, vagy egy olyan ajánlat érkezik, amely túl kedvező ahhoz, hogy igaz legyen, gyanakodjunk!

- Ugyanúgy, ahogy az online vásárlásnál, használjon erős jelszót, hogy a csalók ne vehessék át az uralmat a fiókod felett! A jelszó tartalmazzon nagybetűt, kisbetűt, számot és speciális karaktert is! Ha lehetőség van kétlépcsős azonosításra, élj a lehetőséggel a nagyobb biztonság érdekében!
- Csak megbízható webhelyről használjon játékszoftvert vagy kiegészítőt! Arra is figyeljen, hogy ha bármikor azt kérik, hogy blokkoljuk a biztonsági eszközöd, az ne tegyük meg!
- Ne csalj, hogy ne légy a csalók áldozata! A csalás, azaz a cheat-elés az online játékok népszerű témája. A csalóprogramok rosszindulatú kódokat tartalmazhatnak, óvakodj tőlük!
- Mindig ellenőrizze a játékszoftver webhelyét! Ott is hasznos tanácsokat találhat ahhoz, hogy megvédje az eszközét és az adatait.

Néhány gondolat a csalókról (Hogyan próbálnak meg minket manipulálni?)

- Sürgetnek, hogy minél előbb hajtsa végre a kéréseket. Ha a hívó fél azonnali cselekvésre ösztönöz, szinte biztos, hogy csalóval van dolgunk. Ha sietünk, könnyebben hibázunk, és megadunk meg olyan adatot, amit nem kellett volna.
- Bizalmunkba férkőznek és sok esetben olyan személy nevében keresnek, akit ismer(het)ünk, ám ilyenkor a megfogalmazás furcsa lehet, vagy nem megfelelő az aláírás, az e-mail cím.
- Hivatalosnak tűnhet a hívás hiszen cég nevében is kereshetnek. Valósnak tűnhet a megkeresés, de amikor megnézzük az e-mail címet, akkor az nem az ő hivatalos levelezési címük, vagy akár gmail.com-ra végződik.
- Kihasználják a kíváncsiságunkat és sok esetben e-mailt kapunk arról, hogy nyertünk egy olyan játékon, amelyen nem is vettünk részt, vagy ajándékot szeretnének adni, illetve csomagunk érkezik, amelyet nem is rendeltünk meg, szinte biztos, hogy csalókkal van dolgunk. Ne nyissuk meg a csatolmányt, ne kattintsunk semmilyen küldött linkre, és ne adjunk ki semmilyen adatot.
- A csalók sokszor érvelnek azzal, hogy büntetést kapunk, ha nem fizetsz ki egy bizonyos összeget, illetve azzal is érvelhetnek, hogy már csalók vették célba a bankszámlánkat, és ha nem adjuk meg az adatokat, akkor nem tudják megvédeni a pénzünket.
- Telefonos csalók a banki adatainkat, illetve a számítógépünkhöz, mobiltelefonunkhoz és a bankszámlánkhoz való hozzáférést szeretnék megszerezni, hogy átutalást indítsanak. Erre nem feltétlenül használnak bonyolult informatikai rendszereket, mindössze egy telefont és a befolyásolás eszközeit.
- Telefonon sokkal könnyebb becsapni valakit, hiszen élőszóban sokkal inkább befolyásolhatnak minket a csalók, hatnak az érzelmeinkre. Ilyen módon akarják megszerezni pénzügyi adatainkat, a pénzünket vagy a számítógépünkhöz, mobiltelefonunkhoz való hozzáférést. Kiemelten fontos, hogy ismerjük a csalók módszereit, hiszen ilyen támadás esetén csak magunkra számíthatunk.

További hasznos információk, tanácsok, linkek

https://kiberpajzs.hu/

http://www.police.hu/hu/hirek-es-informaciok/bunmegelozes/aktualis/legyen-tudatos-online-vasarlo-elado-es-csomagkuldo

https://nki.gov.hu/

https://nki.gov.hu/it-biztonsag/kia dvanyok/segedletek/

https://nki.gov.hu/it-biztonsag/kiadvanyok/szorolapok/

https://nki.gov.hu/it-biztonsag/tanacsok/

Köszönjük figyelmét,

TRIVE Bank Zrt.