Tíz tipp a biztonságos online bankoláshoz

Ma már megszokottnak számít, hogy a számlaegyenlegünk ellenőrzését, számláink kifizetését és egyéb pénzügyeink intézését online végezzük. De megteszünk-e mindent a biztonságos internetes bankolás érdekében? Az ESET az Európai Kiberbiztonsági Hónap partnereként és aktív résztvevőjeként 10 pontban foglalta össze a biztonságos online bankolás és fizetés alapelveit.

1. Használjunk megbízható eszközt

Az első és legfontosabb alapelv, hogy az online számlánkhoz való csatlakozás során megbízható eszközt használjunk. A saját (lehetőleg megfelelő védelmi megoldással ellátott) számítógépünk, táblagépünk vagy okostelefonunk a legjobb választás, mivel nagyobb valószínűséggel vennénk észre, ha valamilyen gyanús tevékenység zajlana rajta, vagy az eszköz furán viselkedne.
Ha lehetséges, kerüljük a kölcsönkért vagy nyilvános eszközök használatát, amivel a számlánkat és a megtakarításainkat is veszélyeztetnénk.

2. Legyünk óvatosak, hogy hol lépünk be a fiókunkba

Nem mindegyik internetkapcsolat számít biztonságosnak az online bankolás vagy fizetés szempontjából.
A nyilvános Wi-Fi a kedvenc kávézónkban, vagy a főtéren elérhető hálózat nem feltétlenül a legjobb opciók arra, hogy megnézzük számlaegyenlegünket, vagy kifizessük számláinkat. Ha nem tudjuk elkerülni a nyilvános hálózatok használatát, akkor alkalmazzunk VPN (Virtual Private Network) megoldást, hogy kommunikációnk titkos maradjon, és adataink ne kerüljenek illetéktelen kezekbe.

3. Legyen naprakész a számítógépünk

Tartsuk operációs rendszerünket naprakészen. A rendszeres biztonsági hibajavítások azonnali letöltése és futtatása segít bezárni a támadók által keresett sebezhetőségeket, ugyanis a javítatlan hibák, sérülékenységek lehetővé tehetik, hogy megfertőzhessék számítógépünket.
Sok program automatikusan telepíti a biztonsági frissítéseket, hibajavításokat, illetve új verziókat keres anélkül, hogy szükség lenne külön felhasználói beavatkozásra. Ezzel időt takaríthatunk meg, és egyben maximalizálhatjuk a védelmünket.

4. Használjunk megbízható és naprakész biztonsági megoldást

Mielőtt csatlakoznánk az online számlánkhoz, telepítsünk megbízható, többszintű és naprakész biztonsági megoldást. A komplex internetbiztonsági alkalmazás védelmet nyújt a különféle típusú vírusok, valamint az olyan rosszindulatú átverések ellen, amelyek ártalmatlan e-mailnek vagy weboldalnak álcázzák magukat, hogy így vegyék rá az áldozatokat bizalmas adataik megadására.

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

5. Alkossunk egy erős jelszót és ne használjuk máshol

Az egyik legfontosabb szabály, hogy minden egyes belépési helyszínen különböző egyedi jelszót használjunk. Ha ugyanis ugyanazt a jelszót használjuk az online számlánkhoz, a közösségi média felületeinkhez vagy több más fiókunkhoz is, az könnyen katasztrófához vezethet, ha jelszavunk bármelyik oldalról esetleg mégis kiszivárogna.
Egy nagyon hasznos, és könnyen megjegyezhető alternatíva a jelmondatok használata. Valamint használhatunk olyan jelszókezelő programot is, ami eltárolja az összes kódunkat, nekünk viszont csak egyetlen mester jelszóra kell emlékeznünk.

6. Használjunk kétfaktoros azonosítást

Ha a bankunk felajánlja a kétfaktoros azonosítást (2FA) az online számlánkhoz, akkor használjuk ki a lehetőséget. Így a bank duplán is ellenőrizni tudja, hogy tényleg mi szeretnénk csatlakozni online számlánkhoz a saját eszközünkkel. Így ha a jelszavunk esetleg rossz kezekbe is kerül, a második azonosítás nélkül nem lesz sikeres a belépés.

7. Ne dőljünk be a csapdáknak

A kiberbűnözők szó szerint bármit megpróbálnak, hogy megszerezzék bizalmas adatainkat. Úgy tesznek, mintha bankárok lennének, hamis értesítést küldenek vagy megkérnek, hogy változtassuk meg a jelszavunkat egy linken keresztül, amit e-mailben küldtek el nekünk. Ez csak néhány hazugság azok közül, amikkel megpróbálkoznak azért, hogy megszerezzék a kártyaadatainkat vagy fiókunk jelszavát.
Ha bármilyen üzenetet kapunk, amely arra kér, hogy változtassuk meg a belépési adatainkat vagy kattintsunk egy mellékelt linkre, ne tegyünk, és semmiképpen se kattintsunk. Bank sosem küld ilyen jellegű üzenetet. Gyanú esetén legjobb, ha telefonon vagy személyesen keressük fel bankunkat.

8. Jelentkezzünk ki, ha befejeztük az online bankolást

Ha végeztünk, lépjünk ki az oldalról. Ha egy támadó megpróbálja eltéríteni az online bankolás folyamatát, kevesebb kárt tud okozni, ha nem vagyunk bejelentkezve fiókunkba.

9. Aktiváljuk az SMS értesítéseket

Hasznos, ha folyamatosan figyeljük online egyenlegünket. Ezt legkönnyebben úgy tehetjük meg, ha bankunktól SMS értesítést kérünk az összes számlánkon zajlódó pénzmozgásról, így sokkal könnyebben felfigyelhetünk a gyanús tevékenységekre.

10. Virtuális bankkártya használata

Ma már minden banknál létezik külön internetes vásárlásokhoz való elektronikus (unembossed card) virtuális kártya, amelynek a számát bátran megadhatjuk, akár még a három jegyű CVV ellenőrző kóddal együtt is.
Ám erre az alszámlára érdemes csak a vásárlás előtt közvetlenül a netbankunkon átvezetni a vásárláshoz szükséges pontos összeget, ami így csak pár percig lesz az egyébként üres virtuális számlánkon. Ezzel a módszerrel nem tudnak tőlünk lopni, és így az "igazi" bankkártyánk adatait sosem kell a weboldalakon megadnunk.

Forrás: TŐZSDEFÓRUM

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