Legyen óvatos, csalók élnek vissza a bankok nevével!

A bankszámlákon található összegek megszerzésére irányuló kísérletek ma már sajnos mindennaposak, ezért érdemes tisztában lenni azzal, hogy milyen módszerekkel próbálkoznak a bűnözők adataink és a bankszámlánk feletti rendelkezés megszerzése érdekében.

Cél az adataink és a belépési azonosítók megszerzése:

Ahhoz, hogy elérjék céljukat, a személyes adatainkra (név, születési név, anyja neve, születési hely és idő, lakcím) és a bankszámlánk online vagy telefonos azonosítói, jelszavai szükségesek. Egyik megoldás amikor telefonhívás útján megpróbálják elhitetni, hogy a bank munkatársai, további adatokat kérnek vagy előadják, hogy az ügyfél bankszámláját veszély fenyegeti, ezért a hívás során meg kell adni részükre a belépési kódokat. Az is előfordul, hogy a gyanútlan banki ügyfelet miután sikerült meggyőzni, hogy a bankból telefonálnak, arra veszik rá, hogy maga utalja át a „veszély” miatt egy „biztonságos” számlára a saját pénzét.

Adathalászat emailben:

A hozzáféréshez szükséges adatokat adathalász emailek (phishing) segítségével is igyekeznek megszerezni, amikor tömegesen küldik ki a megtévesztő email címről banki logóval ellátott emaileket. Az emailben olyan internetes linket helyeznek el, ami megjelenésében, domain nevében a tényleges banki weboldalra hasonlító honlapra vezet. Ha ott begépeli az ügyfél a banki azonosítóit, már részben át is adta a bűnözők részére a hozzáférését. Ilyenkor már csak a belépési, biztonsági kódot igyekeznek kicsalni telefonon keresztül az ügyfélből és ha ez sikerült, már be is jutottak a valós banki rendszerbe.

Ezek a hamis levelek sokszor furcsa nyelvtani hibákat, rossz szóhasználatot tartalmaznak, mert az elkövetők nem mindig az adott ország lakói, nem vagy nem jól beszélik a nyelvet és csupán ellenőrizetlen gépi fordításokkal operálnak.

Kit terhel a felelősség?

Ha az elkövetők azért tudták elutalni a számlánkról a pénzt, mert a megtévesztés miatt mi megadtuk az adatainkat, a hozzáférésünket, kémszoftvert telepítettünk a mobiltelefonunkra a csalók kérésére, akkor aktívan segítettük ezzel a bűnözőket, intézkedéseinkkel megszegtük a banki előírásokat és ezzel mi hoztuk magunkat olyan helyzetbe, ahol kárunk keletkezett.

PEST VÁRMEGYEI RENDŐR-FŐKAPITÁNYSÁG
BŰNMEGELŐZÉSI OSZTÁLY

1133 Budapest, Pozsonyi út 56. ✉: 1557 Budapest, Pf. 20. ☎: 237-4345; BM: 21-794, fax: 21-797, e-mail: elbir@pest.police.hu

Ezen esetben a bank általában mentesül a felelősség alól, viselnünk kell a teljes kárt, ami bekövetkezett a számlánk jogellenes kiürítése során.

!!! Az ilyen esetek elkerülése érdekében mindig óvatosnak és gyanakvónak kell lennünk minden esetben ha emailben, telefonon keresnek meg minket és a bankszámlánkhoz kapcsolódóan bármilyen adatot kérnek tőlünk. Az a biztonságos, ha minden esetben akár személyesen, akár az általunk ellenőrzött honlapon, telefonszámokon vagy applikáción mi lépünk kapcsolatba az általunk választott időpontban és módon a bankkal. Így elkerülhetjük, hogy akaratunkon kívül ismeretlenek részére adjunk át bármilyen banki információt.

Pest Vármegyei Rendőr-főkapitányság
Bűnmegelőzési Osztály

PEST VÁRMEGYEI RENDŐR-FŐKAPITÁNYSÁG
BŰNMEGELŐZÉSI OSZTÁLY

1133 Budapest, Pozsonyi út 56. ✉: 1557 Budapest, Pf. 20. ☎: 237-4345; BM: 21-794, fax: 21-797, e-mail: elbir@pest.police.hu