A BANKSZÁMLÁNK AZ EGYIK LEGFONTOSABB ÉRTÉKÜNK, VIGYÁZZUNK RÁ!

A bankszámlákkal, bankkártyákkal kapcsolatos visszaélések eddig ismert változatai minden esetben az ügyfeleket célozzák. Az általuk önként megadott információk, adatok és hozzáférések teszik lehetővé, hogy a csalások eredményesek legyenek. Az ügyfeleket - legtöbbször véletlenszerűen - elérő támadások különböző formákban jelenhetnek meg, mint például sms, e-mail, WhatsApp, telefonhívások, hirdetések vagy éppen hamis banki oldal formájában. Előbb vagy utóbb várhatóan mindenki találkozni fog a bizalmas adatainak megszerzésére irányuló kísérlettel. Érdemes tehát erre felkészülni, felismerni az árulkodó jegyeket, hogy a rémálomszerű esemény lehetőleg soha ne következzen be.

A megszokás, a rohanó világ elaltatja az ügyfelek figyelmét, a csalók pedig pontosan ezt használják ki. A kis összegű szállítási költség vagy éppen a szokásosnak mondható közüzemi számla befizetésekor például az ügyfelek rutinból járnak el: megadják a bankkártya adataikat a szokott felületen, illetve beírják az SMS-ben érkező internetes vásárlás jóváhagyó kódját. A megszokás, egy késői időpont vagy sietség miatt sokszor végig sem gondolják, hogy egyáltalán van-e folyamatban rendelésük vagy fizetendő közüzemi számlájuk.

A csalók egyre kifinomultabbak! Előfordul, hogy egy sikertelen online vásárlás oka az, hogy valójában nem a bankkártyás vásárlás jóváhagyó kódja szerepel az ügyfélhez érkezett sms-ben, hanem egy új eszköz aktiváló kódja. A csalóknak már ennyi adat elegendő lehet, hogy az ügyfél bankkártyáját digitalizálják a saját telefonjukra letöltött mobilfizetéses (pl.: Apple Pay, Google Pay) szolgáltatásba, majd azzal vásárlásokat hajtsanak végre a világ egy távoli pontján. Így egy kisösszegű sikertelen bankkártyás műveletből több milliós nagyságrendű kár is lehet.

A mindennapi, rutinszerű netbanki belépés is tartogathat veszélyeket! Például az ügyfelek legtöbbször egy internetes keresőbe írják be a bankjuk nevét és a megjelenő találatokból, rendszerint az első kiválasztott oldalon kísérelnek meg netbanki belépést. Az internetes keresőből, e-mailben vagy egyéb üzenetben kapott linkről megnyitott honlapok azonban veszélyesek lehetnek!

Csak a bank által meghatározott módon, az elérési útvonalat közvetlenül beírva vagy a kedvencek közé elmentett hivatkozásra kattintva szabad megnyitni a netbanki felületet.

Számos esetben fordult elő, hogy az ügyfelek hamis netbanki felületeken kezdeményezték a belépést és ott rutinból adták meg az sms-ben kapott kódot, valójában egy bűnözők által kialakított áloldalon. Ez az üzenet azonban nem a netbanki belépés kódját, hanem a bank mobilalkalmazásának regisztrációs kódját vagy éppen a QR alapú belépés jóváhagyásának, esetleg az átutalási limit módosításának a kódját tartalmazta. Az ügyfelek legtöbbször a sikertelen próbálkozások - azaz az egymás után érkező kódok rutinszerű kiadása - után feladták a belépésre tett kísérleteket. Azonban ezzel egyidőben a csalók a megszerzett adatokkal, az ügyfél bankszámlájához kapcsolódóan mobilalkalmazást telepítettek a saját telefonjukra. Így az ügyfél bankszámlája felett rendelkezve, a már megemelt limit mellett, jóváhagyás nélkül számos nagyösszegű vásárlást vagy átutalást kezdeményeztek.

Fontos tudni, hogy a bankok számára az online világban kapott hitelesítő adatok és kódok azonosítják az ügyfeleket. A többlépcsős hitelesítéseket (például sms-ben kapott kódot, mobilalkalmazásban történő arc,- vagy ujjlenyomat-hitelesítést) a banki műveletek biztonságának növelése érdekében vezették be. A bankok ezáltal tudják ellenőrizni, hogy a fizetési műveletet valóban a számlatulajdonos kezdeményezte. Nagyon fontos, hogy az ügyfelek a saját adataik felhasználásával körültekintően járjanak el, hiszen minden egyes adat kiadásával gyengítik a biztonságukat jelentő védelmi vonalat. Olyan ez, mintha az ügyfél először csak a lakásába engedné be a csalót, aztán megmutatná neki a széfet, megadná a kódját, majd illedelmesen elfordulna, hogy a bűnöző szabad kezet kapjon a fosztogatáshoz.

Ha az ügyfél a kapott SMS tartalmát valamilyen okból nem tudja értelmezni, akkor érdemes felhívnia a bankját, egyeztetni az üzenet tartalmát és az általa végzett tevékenységet. Inkább kételkedjünk, mint hogy utólag szaladjunk a pénzünk után!

KiberPajzs
Védelem a pénzügyekben