Sajtóközlemény

Körültekintéssel az elektronikus csalások ellen

Budapest, 2015. október 20. - ***A számlavezető hitelintézetek soha nem kérik el ügyfeleiktől az elektronikus banki ügyintézéshez szükséges egyedi azonosítókat (pl. a PIN kódot) telefonon, sms-üzenetben vagy e-mailben. Az ilyen megkeresések mögött mindig csalók állnak. Ha banki vagy államigazgatási üzenetnek álcázott felkérés érkezik az egyedi ügyfél-azonosító megadására, célszerű haladéktalanul értesíteni a pénzügyi szolgáltatót, vagy az adott államigazgatási intézményt, illetve a jegybankot.***

Egy számlavezető bank vagy egy takarékszövetkezet sem kérheti el ügyfelei elektronikus (pl. PIN kód) vagy egyéb azonosító adatait telefonon (szóban vagy SMS formájában), e-mailen vagy írásban. Az ilyen üzenetek minden esetben csalóktól és nem az érintett pénzügyi intézménytől származnak. Ezekben az esetekben a fogyasztónak azonnal értesítenie kell szolgáltatóját, vagy az érintett államigazgatási intézményt, hogy az megtehesse az ilyenkor szükséges lépéseket (figyelemfelhívás, nyomozó hatóságok értesítése, fokozott biztonsági intézkedések).

Új módszer, hogy egyes csalók a Nemzeti Adó- és Vámhivatal (NAV) nevében helyeznek kilátásba sms üzenetben adó-visszatérítést, ha a címzett az interneten keresztül megadja adatait. A csalók által küldött link egy hamis, látszólag adóhivatali felületre visz, amely egy űrlapot tölt be a személyes adatok megadásához. Aki a csaló sms utasításait követve megadja adatait, számolnia kell azzal, hogy bankkártyájáról pénzt emelhetnek le.

A NAV értesítési gyakorlata merőben eltér a megtévesztő módszertől. A hivatal ugyanis ügyfélkapun keresztül, illetve postán, folyószámla-kivonaton értesíti az adózókat a többletként megjelenő tételekről, és hivatalos honlapja a www.nav.gov.hu címen található. A NAV az adózók figyelmeztetésén túl feljelentést tesz.

Az internetes banki csalások tipikus esetei a következők: Az adathalászat során a csalók a pénzügyi intézmény nevében telefonhívással, e-mailben, sms-ben ráveszik a számlatulajdonost, hogy árulja el azonosítóját és jelszavát, azaz, adja meg a banki műveletekhez szükséges bizalmas, titkos adatait. Az intézmény valójában soha semmilyen formában nem kéri el az ügyfél titkos adatait.

Előfordulhat, hogy a csalók e-mailjükben egy „banki alkalmazás” letöltését kérik, valójában azonban a linkre kattintva az ügyfél ártó szándékú vírusokat, úgynevezett trójai programot helyez el saját számítógépén. A megfelelő vírusvédelem, tűzfal és kémelhárító képes e kártékony programok behatolását megakadályozni.

Egyes adathalászok e-mailek segítségével az ügyfeleket hamis – de az eredetire hasonlító – megtévesztő internetbanki oldalra csalják. A pénzügyi intézmények valódi honlapján viszont a böngésző alsó sávján/felső címsorában szerepel a biztonságos kapcsolat meglétét jelző lakat ikon. Ezen oldalak használatakor a normál „http” helyett „https” védett kapcsolat épül fel az ügyfél gépe és az intézmény között.

A elektronikus banki szolgáltatások biztonságáról, s a csalások elleni védekezésről az *MNB Pénzügyi Fogyasztóvédelmi Központjának* honlapján olvashatók további információk.

Nemzeti Adó- és Vámhivatal **Magyar Nemzeti Bank**

Magyar Nemzeti Bank
Kommunikáció

Telefon: + 36/06 (40) 203-776, **Fax:** + 36 (1) 429-8000, **Email:** felugyeletisajto@mnb.hu, **Web:** www.mnb.hu