wmn.hu /wmn-life/61419-egyetlen-hibas-kattintassal-elbukhatod-az-osszes-penzed

Egyetlen hibás kattintással elbukhatod az összes pénzed

A néhány héttel ezelőtti Black Friday-akciók idején percenként 1,3 millió dollárt költöttek el világszerte a netes vásárlók… és ha decemberben nem lesz is ilyen óriási vásárlási bumm, az biztos, hogy nagyjából annyit költünk a neten az év utolsó két hónapjában, mint az összes többi tízben. Ez pedig óriási kockázatot jelent az adathalászat szempontjából, bőséges lehetőséget kínálva a netes csalások és lopások elkövetőinek. Te biztos vagy benne, hogy mindent megteszel a bankkártyád adatai és ezáltal a pénzed védelmében? Én nem – ezért megkérdeztem egy szakértőt: az ESET termékeket forgalmazó Sicontact Kft. **kiberbiztonsági szakértőjét, Csizmazia-Darab Istvánt. Tóth Flóra írása.**

–

Az internetes vásárlás szuper dolog, ha időt spórolnál, ha szeretnél néhány ügyet érthető okokból titokban (a Jézuska, Mikulás nevében) intézni vagy ha egyszerűen olyan termékre vágysz, ami nem elérhető a közeledben.

De a rossz hírem az, hogy

> *az adataid nemcsak akkor vannak veszélyben, amikor éppen a neten keresztül fizetsz – hanem igazából bármikor, ha valaha megadtad a bankkártyád adatait, és nem jársz vagy jártál el körültekintően adatbiztonság tekintetében.*

Egyre többféle módszerrel próbálnak lehúzni a csalók

Csizmazia-Darab István segítségével először végigvesszük, hogy pontosan melyek a leggyakoribb csalási módszerek, kezdve a legsúlyosabb problémát okozókkal, amelyekkel letakaríthatnak minden pénzt a számlánkról.

Ez történhet úgy, hogy valami kihagyhatatlan akcióval, ajándékkártyával vagy egy állítólagos, szállítás alatt lévő csomaggal (ami lehet, hogy nem is létezik) rávesznek, hogy kattints egy linkre, ami valójában adathalász weboldalra mutat, vagy kémprogramot telepít az eszközödre, onnantól pedig egyetlen tárolt adatod (így akár a bankkártyád adatai) sincs biztonságban.

> Szintén kockázatos, ha nyilvános wifihálózatot igénybe véve vásárolsz, lépsz be egy szolgáltatásba vagy használod a bankkártyádat online fizetésre.

Előfordul, hogy nem vásárolni szeretnél, hanem épp ellenkezőleg, eladni. Egy vevőjelölt pedig azonnal jelentkezik, felajánlja, hogy ő fizeti a szállítást, csak éppen arra kér, hogy egy linkre kattintva lépj be a bankodba, aztán várd a beígért futárt – vagy valami hasonló (gyakran tört magyarsággal).

De mit tehetünk ezek ellen?

Néhány fontos lépés betartásával azért minimalizálhatjuk a kockázatát annak, hogy nagyobb kár érhessen minket.

A legfontosabb dolgok, amiket Csizmazia-Darab István összefoglalása szerint tehetünk a pénzünk védelmében:

- Használj virtuális kártyát (ebben segíthet a saját bankod, de vannak olyan online banki rendszerek, például a Revolut vagy a Wise, amik szintén tudják ezt, ha esetleg a saját bankod nem). A virtuális kártyák között vannak egyszer használatosak, de olyanok is, amiket hosszabban lehet használni, és lehet úgy csinálni, hogy mindig csak annyi pénzt utalsz rá, amennyi éppen az adott vásárláshoz kell. Ez lehet, hogy macerás, de ahelyett, hogy esetleg az egész fizetésed válna köddé egy nem megfelelő kattintás miatt, szerintem megéri három perccel lassabban fizetni minden egyes vásárlásnál.
- Telepíts az eszközeidre olyan védelmi rendszert, ami kifejezetten adathalászat ellen segít (ebből a fizetős szolgáltatások jobbak – nemrég írtam a digitális rezsiről –, a legtöbb nem kerül annyiba havonta, mint egy streaming-előfizetés). Idősebb vagy egyszerűen ilyen téren kevésbé figyelmes családtagjaidnak adhatsz ilyen védelmet akár ajándékba is, ha szükséges, telepítési segítséggel együtt.
- Minden olyan felületen, ahol fontos információt tárolsz (banki applikáció, levelezőrendszer), legyen legalább kétfaktoros vagy többtényezős hitelesítés (igazolni kell valamilyen más módon, külön hitelesítő alkalmazással, sms-kóddal, hogy te vagy, aki be akar lépni). A jelszavakat sose a böngészőben tárold, hanem jelszószéf alkalmazásban. Az még jobb, ha van biometrikus (ujjlenyomatos vagy arcfelismerős) azonosításod, mert akkor tényleg minden esetben neked kell engedélyezned a pénz elküldését.
- > *Ne kattints olyan e-mailben vagy üzenetben érkező linkre, ami „túl szép” ajánlatot ígér, pláne ha magyartalanul, gyanúsan van megfogalmazva.*
- Ha bármilyen használt cikkes felületen árusítasz, sose kattints olyan linkre, amit a vevő küld, akkor

sem, ha azt ígéri, hogy ő fizeti cserébe a szállítást.

- Igyekezz hivatalos webshopokból vásárolni – lehetőleg ne valamilyen promóciós linken keresztül –, ellenőrizve, hogy az oldal használja-e a HTTPS tanúsítványt (ha az URL-ben a honlap címe előtt nem sima HTTP, hanem HTTPS szerepel, akkor az ad valamennyi garanciát arra, hogy biztonságos helyen vagyunk). Érdemes magát a tanúsítványt is ellenőrizni: érvényes-e, annak a nevére szól-e, akinek az oldalán járunk.
- Ne dőlj be a túl jónak tűnő ajánlatoknak. Tényleg. Ha gyanúsan olcsón kínálnak valamit, ott biztosan valami átverés van – ha nem adathalászat, akkor más.
- Lehetőleg ne vásárolj nyilvános wifin csatlakozva a netre, vagy ha igen, akkor használj VPN-t (itt találsz róla részletes infókat).
- Ha arra gyanakszol, hogy ellopták a banki adataidat – ennek lehet jele valamilyen ismeretlen, indokolatlan terhelés a bankszámládon – érdemes haladéktalanul kapcsolatba lépni a bankoddal. Ha nagy a baj, akár a számla zárolására is szükség lehet.
- Ha online fizetsz, nézd meg, milyen fizetésközvetítő oldalra visz, amin keresztül megadod a kártyaadatokat. Ha ez ismertebb (PalPal, SimplePay, Barion, PayU) szolgáltatás, akkor ez pozitív jel. Ezeken a helyeken probléma esetén tudunk reklamálni, bejelentést tenni, pénzt visszakapni.
- És nem győzzük hangsúlyozni: biztonságtudatos figyelem, óvatosság, egészséges gyanakvás és lankadatlan éberség!

Azért is nagyon fontos, hogy mit teszel meg a saját pénzed védelmében, mert míg néhány évvel ezelőtt, amikor ez még sokkal kevésbé volt gyakori, a bankok szinte szó nélkül kártalanították a netes csalások áldozatait, ma már ez egyáltalán nem így van.

> *Ha bizonyítható, hogy a saját hibádból kerültél bajba: például az adathalász oldalon megadtad a bankkártyád minden adatát és biztonsági kódját is, vagy ezeket bediktáltad a csalóknak a telefonba, akkor a bank nem fogja visszaadni az így ellopott pénzed.*

Nekem sajnos van olyan ismerősöm, akinek a leendő otthona kezdőtőkéjét emelték le a számlájáról, és egyáltalán nem biztos, hogy sikerül visszaszereznie az összeget.

Van, amitől semmilyen hitelesítés és védelmi program nem óv meg

Az internetes csalások másik gyakori formája, amikor nem azt kapod, amit rendeltél, esetleg nem kapsz semmit, hiába fizetted már ki előre. Ezek ellen nem lehet online eszközökkel védekezni, csak odafigyeléssel és óvatossággal – de így is benne van a pakliban, hogy a várva várt marketplace-es csomagod helyett egy féltéglát kapsz. A használt árukat kínáló felületeken érdemes nagy figyelmet fordítani az eladók értékeléseire, a gyanúsnak tűnő webshopokat szintén kicsit részletesebben megnézni, rákeresni a vásárlói visszajelzésekre. Nyilván mind szeretünk olcsón vásárolni, de közben meg

> *tele van az összes közösségimédia-platform az „ezt rendeltem vs. ezt kaptam” fotó- vagy videópárokkal. Hiába szeretnénk ugyanis 3200 forintért márkás holmikat venni (nem használtan), ennyiért maximum gyenge utánzatot lehet.*

Elképesztő népszerűségnek örvendenek a filléres termékeket és óriási akciókat kínáló, legtöbbször távol-keleti webshopok. Csizmazia-Darab István azt mondja, ha ilyen helyről rendelsz, tisztában kell lenned a

kockázatokkal: jó eséllyel kapsz rossz minőségű terméket vagy akár semmit, és reklamációkezelésre egyáltalán nincs lehetőség. De ezek nyilván egészen más léptékű problémák, mint amikor a számládon lévő összes pénz forog kockán.

További információkat itt találsz a netes csalásokról.

Tóth Flóra