Az Ön havi biztonságtudatossági hírlevele

Biztonságos Online vásárlás

Áttekintés

Sokunk számára közelednek az ünnepek és hamarosan emberek milliói szeretnék majd megvásárolni a tökéletes ajándékot. Annak érdekében, hogy megtaláljuk a legjobb ajánlatokat, valamint, hogy elkerüljük a zajos tömegeket, sokan vásárolunk majd online. Sajnos a kiberbűnözők is aktívak lesznek majd, hamis weboldalakat készítve és egyéb trükköket alkalmazva az emberek átveréséhez. Ebben a hírlevélben bemutatjuk, hogy hogyan tud biztonságosan vásárolni online, és hogyan kerülheti el, hogy áldozattá váljon.

Hamis online boltok

A kiberbűnözők hamis webáruházakat készítenek, amelyek utánozzák a valódi weboldalak megjelenését, vagy jól ismert üzletek és márkák neveit használják fel. Miközben a legjobb online ajánlatokat keresi, előfordulhat, hogy egy efféle oldalon találja magát. Az ilyen weboldalakról történő vásárlás hamis, vagy lopott termék beszerzéséhez vezethet, valamint az is előfordulhat, hogy a megvásárolt termékek nem is kerülnek kézbesítésre. Védje magát a hamis online boltoktól:

- Amennyiben lehetséges, olyan webshopokban vásároljon, amelyeket már ismer, amelyekben megbízik és ahonnan már rendelt korábban. Jelölje meg a már felkeresett és megbízható online boltokat.
- Figyeljen oda azokra az árakra, amelyek jelentősen kedvezőbbek, mint amelyeket a bevált online áruházakban látni. Ha az ajánlat túl jó ahhoz, hogy igaz legyen, az valószínűleg hamis.
- Legyen gyanakvó, ha egy webhely hasonlít a korábban meglátogatott weboldalra, azonban a domain név, vagy az üzlet neve némiképp eltérő. Például, lehet, hogy szokott vásárolni az Amazonon, aminek weboldal címe www.amazon.com, azonban végül egy hamis webhelyen találja magát, amelynek hasonló webcíme van, de az „o” betűt nullával („0”) helyettesítették.
- Gépelje be az online bolt nevét vagy webcímét a keresőbe, hogy lássa mások mit mondanak róla. Keresse a „csalás”, „átverés”, „soha többé” vagy „hamis” kifejezéseket.
- Használjon egyedi jelszót minden online fiókjánál. Nem emlékszik az összes jelszavára? Fontolja meg azok jelszókezelőben történő tárolását.

Csalók a valós weboldalakon

Legyen óvatos, még ha megbízható weboldalon vásárol is. A nagy online áruházak gyakran ajánlják más magánszemélyek vagy társaságok termékeit, akiknek esetleg csalási szándékuk lehet. Ezek az online áruházak olyanok, mint a valós piacok, ahol egyes eladók megbízhatóbbak másoknál. Rendelés előtt minden egyes eladó értékelését ellenőrizze le. Legyen óvatos azokkal az értékesítőkkel, akik újak az adott online boltban, vagy akik szokatlanul alacsony árat adnak meg. Nézze át az online bolt szabályzatát a harmadik féltől való vásárlásra vonatkozólag. Ha kétségei vannak, vásároljon olyan termékeket, amelyeket közvetlenül az online áruház árul, nem pedig az online piacon részt vevő harmadik fél.

Online fizetés a vásárláskor

Rendszeresen nézze át banki számlaforgalmát, hogy azonosítani tudja a gyanús levonásokat. Ha lehetséges, engedélyezze az e-mail, SMS, illetve alkalmazás általi értesítést arra az esetre, ha megterhelnék bankkártyáját. Ha gyanús tevékenységet észlel, azonnal hívja a kártya kibocsátóját és jelentse az esetet. Amikor csak lehetséges, kerülje a betéti kártyák használatát. Betéti kártyák használata esetén közvetlenül a bankszámlájáról vonják le az összeget, így ha csalást követnek el, sokkal több időbe telik, hogy visszakapja pénzét. Másik lehetőség az online vásárlások esetében a jól ismert fizetési szolgáltatások, mint például a PayPal használata, amelyek nem igénylik, hogy hitelkártya számát közölje az eladóval. Végül, érdemes megfontolni az ajándék kártya használatát online vásárlások esetén.

Attól, hogy egy online bolt jól megtervezett és professzionális kinézetű, még nem feltétlenül valós is. Ha egy webhely gyanút kelt Önben, inkább ne használja azt. Ehelyett keressen fel egy jól ismert weboldalt, amiben megbízik, és amit már korábban is használt. Lehet, hogy nem talál hihetetlenül jó üzletet, de sokkal valószínűbb, hogy eredeti terméket kap és elkerüli a csalást.

Magyar Kiadás

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. Az NKI rendeltetése, hogy előmozdítsa a kormányzati szektor elektronikus informatikai rendszerei biztonsági szintjének emelését, valamint, hogy fejlessze a közigazgatásban dolgozó felhasználók biztonságtudatos viselkedését a kibertérben. A nemzetközi és hazai partnerkapcsolatai révén az NKI hozzájárul a magyar kibertér biztonságának erősítéséhez. További információ az Intézetről a https://nki.gov.hu oldalon olvasható.

A szerzőről

Lenny Zeltser *az Axonius információbiztonsági vezetője, valamint szerző és oktató a SANS Intézménynél. Követheti őt a Twitteren, a @lennyzeltser felhasználói néven, vagy olvashatja blogját a zelster.com oldalon.*

Források

Pszichológiai befolyásolás:	http://www.sans.org/u/X7k
Átverés a közösségi médián keresztül:	http://www.sans.org/u/X7p
Egyszerű jelszókezelés:	http://www.sans.org/u/Xu9