SANS SECURITY AWARENESS
NEMZETI KIBERVÉDELMI INTÉZET

OUCH! | 2017. November

Havi biztonság tudatossági hírlevél mindenkinek

OUCH!

ebben a kiadásban...

- **Hamisított online üzletek**
- **Számítógépünk/ mobil eszközünk**
- **Bankkártyánk**

Online vásárlás biztonságosan

Áttekintés

Már közeledik az ünnepi szezon és rövidesen a világon emberek milliói igyekeznek a tökéletes ajándékokat megvásárolni. Sokan fogunk úgy dönteni, hogy a hosszú sorok és a türelmetlen tömeg elkerülése érdekében inkább online vásárolunk és keresünk nagyszerű ajánlatokat. Sajnos ebben az időszakban a kiberbűnözők számos hamis bevásárló weboldalt hoznak létre, hogy átverjenek másokat és így pénzt lopjanak tőlük. Az alábbiakban bemutatjuk, hogy milyen veszélyeket hordoz magában az online vásárlás és hogyan lehet ezeket a csodás akciókat biztonságosan kihasználni.

A szerzőről

Lenny Zelter biztonsági termékek fejlesztésével foglalkozik a Minerva Labs-nál, valamint malware elleni harc témában oktat a SANS Intézetnél. Lenny a Twitteren a **@lennyzeltser** néven érhető el, valamint egy biztonsági blogot is ír a **zelters.com**-on.

Hamisított online üzletek

Míg sok legális online üzlet létezik vannak olyan álweboldalak is melyeket kiberbűnözők hoztak létre. A bűnözők a valós oldalak kinézetét utánozva vagy jól-ismert boltok nevekit és márkáit felhasználva hozzák létre ezeket az áloldalakat. Ezen csalárd weboldalakat arra használják, hogy olyan embereket vonzzanak be, akik a lehető legjobb ajánlatot keresik. Amikor online az abszolút legalacsonyabb árat keressük, akkor könnyen irányíthatnak minket egy ilyen álweboldalra. Amikor kiválasztjuk, hogy melyik oldalon vásárolunk, akkor legyünk óvatosak az olyan weboldalakkal melyek a többihez képest drámaian alacsony árakat hirdetnek, illetve ha az oldal olyan terméket ajánl amely országszerte elfogyott. Azért olyan olcsóak és elérhetőek a termékeik, mert amit kapunk az nem törvényes, hamisított vagy lopott, esetenként egyáltalán nem is kerül kézbesítésre. Az alábbiak segítségével védhetjük meg magunkat:

- Ha lehetséges, akkor olyan weboldalról vásároljunk, amit már ismerünk, megbízunk benne és korábban már vásároltunk ezen keresztül.
- Ellenőrizzük, hogy a weboldalnak van e jogszerű levelező címe és telefonszáma értékesítési vagy támogatásra vonatkozó kérdések esetére. Ha az oldal gyanúsnak tűnik akkor hívjuk fel a telefonszámot és beszéljünk egy emberrel. Ha nem tudunk senkivel beszélni, akkor ez lehet az első nagy jele, hogy egy ál weboldallal találkoztunk.
- Keressünk egyértelmű figyelmeztető jeleket, mint például olyan ajánlatot ami túl jól hangzik ahhoz hogy igaz legyen, vagy aminek rossz a nyelvtana és a helyesírása.
- Legyünk nagyon gyanakvóak, ha egy weboldal pontos másolatának néz ki egy olyan jól ismert weboldalnak, amit korábban használtunk, de a weboldal Domain neve vagy az üzlet neve már kicsit eltérő. Például esetleg vásároltunk

Online vásárlás biztonságosan

már online az Amazonon, aminek a weboldala a https://www.amazon.com. Legyünk gyanakvóak ha egy olyan oldalon találjuk magunkat, ami nagyon hasonlít az amazonra, például a http://store-amazoncom.com.

- Gépeljük be az üzlet nevét vagy URL címét a keresőbe és nézzük meg, hogy mások mit mondtak erről a weboldalról korábban. Keressünk olyan kifejezéseket, hogy “csalás”, “átverés”, “ soha többé” vagy „hamis”. A visszajelzések hiánya is egy olyan jel lehet, ami arra utal, hogy az oldal nagyon új és lehet, hogy nem megbízható.
- Mielőtt bármit megvásárolunk, győződjünk meg róla, hogy a titkosított csatornán kapcsolódunk a weboldalhoz. A legtöbb böngésző jelzi a titkosított kapcsolatot egy lakattal és /vagy zöld HTTPS betűkkel rögtön a weboldal neve előtt.

Védjük meg magunkat online azzal, hogy csak megbízható és megalapozott hírnévvel rendelkező weboldalakról vásároljuk.

Ne feledjük, hogy ha a weboldal profinak is tűnik, még nem jelenti azt, hogy legális is. Ha kételyek merülnek fel bennünk a weboldallal kapcsolatosan, akkor inkább ne használjuk. Helyette keressünk egy ismert weboldalt, amiben megbízhatunk vagy már használtuk biztonságosan korábban. Lehet, hogy ott nem fogunk hihetetlenül jó ajánlatot találni, de a végén egy jogszerű terméket kapunk és elkerüljük, hogy a személyes és pénzügyi adatainkat ellopják.

Számítógépünk / mobil eszközünk

Továbbá ahhoz, hogy legitim weboldalon vásároljunk, biztosítanunk kell azt is, hogy a számítógépünk vagy mobil eszközünk biztonságos. A kiberbűnözők megpróbálhatják megfertőzni az eszközeinket, hogy megszerezzék a banki hozzáférésünket, bank kártya információinkat és jelszavainkat.
A következő lépsekkel őrizhetjük meg az eszközeink biztonságát:

- Ha az otthonunkban van gyermek, akkor fontoljuk meg, hogy két eszközünk legyen, egy a gyerekeknek egy pedig a felnőtteknek. A gyerekek kíváncsiak és interaktívak a technológia vonatkozásában, melynek következtében nagyobb eséllyel fertőződhetnek meg az eszközeik. Csökkenthetjük az esélyt, hogy fertőzötté váljuk, ha külön számítógépet vagy tabletet használunk az olyan online tranzakciók lebonyolítására, mint az online banki ügyintézés, vásárlás.
- Mindig telepítsük fel a legújabb frissítéseket és használjunk napra kész vírus irtó programot. Ez megnehezíti a kiberbűnözők számára, hogy meg tudják fertőzni az eszközünket.

Bankkártyánk

Rendszeresen ellenőrizzük a bank kártya kivonatainkat, kifejezetten több online vásárlást követően, illetve ha egy új

Online vásárlás biztonságosan

online felületen használtuk, azért hogy észre tudjuk venni a gyanús kifizetéseket. Néhány bankkártya szolgáltató felkínál olyan lehetőséget, hogy értesít emailben vagy smsben minden alkalommal amikor használtuk a kártyát vagy ha a díjak meghaladnak egy meghatározott összeget. Egy másik megoldás, hogy legyen egy kártyánk, amit csak az online vásárlásokkor használunk, így probléma esetén le tudjuk cserélni a kártyát anélkül, hogy a többi pénzügyi tevékenységünkre hatással lenne. Ha szerintünk csalás áldozatai lettünk, akkor azonnal hívjuk fel a bank kártya kibocsátóját. A folyószámához kapcsolt kártyák egyenesen a bankszámlánkról veszik le a pénzt, így csalás esetén sokkal nehezebb visszaszerezni a pénzünket. Végül fontoljuk meg olyan bank kártya használatát, mely egyedi kártya számot generál minden vásárláshoz, ajándékkártyákat, vagy használjuk az olyan jól ismert fizetési szolgáltatókat, mint a PayPal, melyeknek nem szükséges megosztani az eladóval a bankkártya számunkat.

További információ

Iratkozzon fel a havi OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a securingthehuman.sans.org/ouch/archives weboldalon.

Magyar Kiadás

A Nemzeti Kibervédelmi Intézet (NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. A Nemzeti Kibervédelmi Intézet 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 http://www.govcert.hu/ és a http://neih.gov.hu oldalon olvasható.

Hivatkozások

Pszichológiai manipuláció:	https://securingthehuman.sans.org/ouch/2017#january2017
A Biztonság megőrzése négy lépésben:	https://securingthehuman.sans.org/ouch/2016#october2016
Otthoni hálózat biztonsága:	https://securingthehuman.sans.org/ouch/2016#february2016
A nap SANS Biztonsági Tippje:	https://www.sans.org/tip_of_the_day.php

Szerkesztette: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Fordította: Tikos Anita

