OUCH! | 2015. november

Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadásban...

- **Hamis online üzletek**
- **A számítógépről/mobil eszközről**
- **A bankkártyákról**

Biztonságos online vásárlás

A fokozott óvatosság hónapja

A karácsonyi bevásárlási szezon a nyakunkon van, és hamarosan világszerte milliók akarják megvásárolni a tökéletes ajándékokat. Sokunk a legkedvezőbb ajánlatok miatt online keressük és vásároljuk a termékeket, ráadásul így meg lehet úszni a hosszú sorban állást és a türelmetlen embereket is. Sajnos a bűnözőknek is ez a kedvenc időszakuk, mert ilyenkor követik el a legtöbb online és pénzügyi csalást. Az OUCH mostani számában bemutatjuk az online vásárlás veszélyeit és azt is, hogy előzhetjük meg a bajt.

A szerzőről

Jonathan Homer (**@JonathanLHomer**) a kiberbiztonsági tudatosítás egy elismert vezető személyisége, aki egyaránt dolgozik a kormányzati és a privát szektornak. Jon szakterülete a hallgatóság bevonása és egyéb élvonalbeli oktatási technikák.

Hamis online üzletek

Bár a legtöbb online üzlet valódi, vannak olyan kivételek, amelyeket bűnözők készítenek. Az ilyen hamis weboldalak megjelenése vagy elnevezése gyakran hasonlít a jól ismert online üzletekére, hogy aztán ezeket felhasználva lépre csalják a gyanútlan, a legjobb ajánlatokat kereső vásárlókat. Amikor a legalacsonyabb árat keressük, lehet, hogy pont egy ilyen oldalra fogunk eljutni.

Amikor kiválasztunk egy weboldalt, legyünk óvatosak az olyan oldalakkal, amelyek más weboldalakhoz képest lényegesen olcsóbban kínálják a keresett terméket, vagy ha egyáltalán olyan hiánycikket reklámoznak, amit sehol másutt nem lehet kapni. Az ehhez hasonló online üzletek azért tudnak alacsony árakat ajánlani, mert például az áru nem legális forrásból származik, hamisítvány vagy lopott termék, vagy egyszerűen a vevő sohasem kapja meg. Az alábbi tanácsok segíthetnek megvédeni magunkat:

- Győződjünk meg arról, hogy a weboldalnak van valódi email-es és telefonos elérhetősége a vásárlási és garanciális ügyek intézéséhez! Ha az oldal gyanúsnak tűnik, hívjuk fel őket!
- Keressünk nyilvánvaló figyelmeztető jeleket, mint például helyesírási hibák!
- Legyünk óvatosak, ha az oldal szinte pontosan úgy néz ki, mint egy általunk korábbról már ismert weboldal, de ennek ellenére az oldal neve némileg eltér attól! Például ha korábban már vásároltunk valamit az Amazon webshopjában, akkor ismerjük a https://amazon.com oldalt. Ebben az esetben elég gyanúsnak tűnhet egy olyan oldal, amelynek a címe pl. http://store-amazon.com.

Biztonságos online vásárlás

- Nézzünk utána az internetes fórumokon a kinézett weboldal nevének vagy címének, járjunk utána, hogy mit mondanak róla az emberek! Keressünk olyan szavakat a fórumokban, hogy például „csalás”, „soha többé”, „hamis”! Az értékelések és kommentek hiánya szintén nem biztos, hogy a legjobb jel, mert azt is jelenti, hogy az üzlet még nagyon új.

Jegyezzük meg, attól, hogy valami nagyon profinak néz ki, még nem biztos, hogy valódi! Ha az oldallal kapcsolatban valami beindítja a vészcsengőt, akkor szánjunk időt arra, hogy utánajárunk! Ha valami kényelmetlenséget tapasztalunk a weboldallal kapcsolatban, akkor inkább ne használjuk! Ehelyett inkább keressünk egy jól ismert, akár már korábban használt üzletet! Előfordulhat, hogy nem találunk olyan nagyszerű ajánlatot, mint a gyanús weboldalon, de biztosak lehetünk benne, hogy legális terméket és valódi számlát kapunk a vásárlásunk eredményeképpen.

Csak olyan online üzletben vásároljunk, amely már kiérdemelte a felhasználók bizalmát!

A számítógépről/mobil eszközről

Amikor egy valódi online üzletben vásárolunk, biztosak lehetünk abban, hogy a számítógépünk vagy mobil eszközünk nem fog megfertőződni semmilyen káros szoftverrel. Ezzel ellentétben a kiberbűnözők meg fognak próbálkozni azzal, hogy megfertőzzék a rendszerünket, hogy hozzájussanak az azon tárolt információkhoz (bankszámlaszámok, jelszavak, stb.). Az alábbi tanácsokat betartva megóvhatjuk ezen adatainkat a bűnözőktől:

- Ha van gyermek, akkor érdemes megfontolni, hogy ő a saját számítógépét használja. A gyerekek nagyon kíváncsiak, és szeretnek mindent kipróbálni, ennek eredményeképpen valószínűbb, hogy megfertőződnek egy (vagy több) káros szoftverrel. Ha egy külön gépet vagy tablet-et tartunk online vásárlásokra és internetes banki használatra, akkor nagyban tudjuk csökkenteni a megfertőződés veszélyét! Ha erre nincs lehetőség, akkor használjunk külön felhasználói fiókot, és gondoskodjunk arról, hogy a gyerekeknek ne legyen rendszergazdai jogosultsága.
- Csak olyan WiFi hálózathoz kapcsolódjunk, amit mi magunk kezelünk (például az otthoni), vagy amiben maximálisan megbízhatunk online pénzügyi tranzakciók végrehajtásához. A publikus WiFi hálózatok (például egy kávézóban) jók lehetnek arra, hogy híreket olvassunk, de arra nem, hogy pénzt utaljunk át.
- Mindig telepítsük a víruskereső szoftverünk legújabb frissítéseit, mivel így a bűnözők sokkal nehezebben fertőzhetik meg a rendszerünket.

A bankkártyákról

Kövessük nyomon a bankszámlánk egyenlegének változásait, hogy észrevegyük a gyanús utalásokat! Legalább havonta egyszer át kell nézni a banktól kapott kimutatást. A banki szolgáltatóknál lehet kérni, hogy minden egyes utalásról kapjunk

Biztonságos online vásárlás

email vagy SMS értesítőt, vagy ha az utalás összege átlép egy beállított értéket. Ha van lehetőségünk, akkor használjunk egy második bankkártyát kizárólag az internetes vásárlásokhoz, így ha az valamilyen módon kompromittálódik, akkor anélkül tudunk intézkedni, hogy egyéb fizetési kötelezettségeink problémába ütközne. Ha arra gyanakszunk, hogy csalás áldozataivá váltunk, haladéktalanul értesítsük a bankunkat, és vázoljuk fel nekik a helyzetet! Ezért jobb, ha hitelkártyát használunk betéti kártya helyett az online vásárlásokhoz. A betéti kártyákról a bank azonnal levonja az összeget, így ha csalás áldozatává váltunk, sokkal nehezebb lesz visszaszerezni a pénzt.

Léteznek olyan megoldások is, amelynél nem kell kiadnunk a banki adatainkat az online üzletek felé. Például minden egyes online vásárláshoz egyedi bankkártya azonosítót lehet generálni, vagy igénybe lehet venni a PayPal-hoz hasonló szolgáltatásokat is.

További Információ

Iratkozzon fel a havi rendszerességű OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a http://www.securingthehuman.org weboldalon keresztül.

Magyar Kiadás

Kormányzati, távközlési és informatikai szolgáltatóként, Magyarország egyik stratégiai fontosságú gazdasági társasága a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Társaságunk kiemelt feladata a kormányzati infrastruktúra működtetése, az e-közigazgatási megoldások támogatása, valamint kormányzati szintű informatikai szolgáltatások nyújtása. További információ a http://www.nisz.hu oldalon olvasható.

Hivatkozások

A biztonságtól öt lépésben:	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201410_hu.pdf
Az otthoni hálózat védelme:	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201401_hu.pdf
A tablet-ek biztonsága:	https://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201312_hu.pdf
SANS napi biztonsági tipp (angolul):	https://www.sans.org/tip_of_the_day.php

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Fordította: Birkás Bence, Árvai Gábor, Pál Benyó