OUCH! 2021. november

Biztonságos Online alkalmazások

Közeleg a karácsonyi szezon. Hamarosan emberek milliói keresik a tökéletes ajándékokat, és sokan az online vásárlást részesítik majd előnyben. Sajnos ilyenkor a kiberbűnözők is aktivizálják magukat, hamis webshopokat hoznak létre, vagy más online vásárlási csalásokkal próbálják ellopni az adatainkat, valamint a pénzünket. Tanuljuk meg, hogyan köthetünk jó üzletet, anélkül, hogy áldozattá válnánk!

Hamis online boltok

A bűnözők hamis online áruházakat hoznak létre, amelyek utánozzák a valódi webhelyek megjelenését, vagy jól ismert üzletek és márkák neveit használják. Amikor a legjobb ajánlatok után kutatunk, könnyen egy ilyen csaló weboldalon találhatjuk magunkat. Ha ilyen webhelyekről vásárolunk, előfordulhat, hogy hamisított vagy lopott termékekhez jutunk, vagy vásárlásainkat soha nem szállítják ki. A saját védelmünk érdekében kövessük az alábbi lépéseket:

- Ha lehetséges, vásároljunk olyan online áruházakból, amelyeket ismerünk, megbízhatónak tartunk, és ahonnan már korábban is vásároltunk. Az ilyen webáruházak címeit mentsük el a könyvjelzők közé!
- Legyünk gyanakvóak a keresőkben vagy a közösségi médiában megjelenő olyan hirdetésekkel vagy promóciókkal szemben, amelyek lényegesen olcsóbbak, mint a jól bevált webshopok! Ha egy ajánlat túl szép, ahhoz, hogy igaz legyen, az egy lehetséges csalás.
- Legyünk óvatosak azokkal a webhelyekkel, amelyekkel semmilyen módon nem lehet kapcsolatba lépni, vagy amelyek nem működő kapcsolatfelvételi űrlapokkal vagy magán e-mailes elérhetőséggel rendelkeznek!
- Vegyük észre, ha egy webhely úgy néz ki, mint egy általunk korábban használt webhely, azonban domainnév vagy az üzlet neve eltérő! Például tegyük fel, hogy korábban vásároltunk az Amazonon, amelynek webcíme a www.amazon.com, és most egy ehhez hasonló weboldalra kerülünk, amely a www.amazonshoppers.com címen érhető el.
- Írjuk be az online áruház nevét vagy webcímét a keresőbe, hogy megtudjuk, mit mondtak róla mások! Keressünk olyan kifejezéseket, mint például: "csalás", "átverés", "soha többé" és "hamis"!
- Használjunk erős, egyedi jelszót minden eszközünkhöz és online felhasználói fiókunkhoz! Problémát jelent az összes jelszó észben tartása? Fontoljuk meg egy jelszókezelő használatát!

Csalók a törvényes webhelyeken

Akkor is résen kell lennünk, ha megbízható webhelyeken vásárolunk! Az online áruházak gyakran olyan harmadik felek - különböző személyek vagy vállalatok - által értékesített termékeket kínálnak, amelyek csalárd szándékúak lehetnek. Ezek a webshopok olyanok, mint a valós piacok, ahol egyes eladók megbízhatóbbak, mint mások.

- A megrendelés előtt ellenőrizzük minden eladó reputációját, olvassuk el a róla írt véleményeket!
- Legyünk óvatosak azon eladókkal, akik újak az online áruházban, nem rendelkeznek értékelésekkel, vagy szokatlanul alacsony áron árulnak termékeket!
- Tekintsük át az online áruház harmadik féltől származó vásárlásokra vonatkozó irányelveit!
- Ha kétségeink vannak, vásároljunk közvetlenül az online áruháztól, ne az online piactéren szereplő harmadik felektől!
- Még a törvényes szállítók esetében is győződjünk meg arról, hogy a vásárlás előtt megértettük az eladó garanciára és termékvisszaküldésre vonatkozó szabályzatát!

Online fizetés

Rendszeresen nézzük át a kártyakimutatásainkat a gyanús terhelések azonosítása érdekében! Ha lehetséges, engedélyezzük azt a lehetőséget, hogy e -mailben, szöveges üzenetben vagy alkalmazásban értesítést kapjunk a kifizetésekről! Ha gyanús tevékenységet észlelünk, azonnal jelezzük a számlavezető bankunknak! Használjunk hitelkártyát bankkártya helyett az online fizetéshez! A bankkártyák közvetlenül a bankszámlát terhelik, ezért csalás esetén sokkal nehezebb lesz visszakapni a pénzünket. Az elektronikus fizetési szolgáltatások vagy az e-pénztárcák, mint például a PayPal biztonságosabb fizetést jelentenek az online vásárlások során, mivel nem követelik meg, hogy megadjuk a hitelkártya számunkat az eladónak. Kerüljük az olyan webhelyeket, amelyek csak kriptovalutában fogadnak el fizetést, vagy homályos fizetési módokat igényelnek!

Az, hogy egy online áruház professzionális megjelenésű, még nem jelenti azt, hogy valódi is. Ha a webhely rossz érzést kelt bennünk, inkább ne vásároljunk ott! Ehelyett keressünk fel egy megbízható vagy már korábban használt, jól ismert webhelyet. Lehet, hogy ott nem találunk hihetetlen ajánlatokat, de sokkal valószínűbb, hogy elkerülhetjük az átverést.

A szerzőről

Mark Orlando biztonsági vezető, aki a Pentagonban, a Fehér Házban és számos magánszektorbeli ügyfél esetében végzett már hálózatbiztonsági tevékenységet. Ma a Bionic kiberbiztonsági cég vezérigazgatója és társalapítója, valamint oktató és tanfolyamszerző a SANS Intézetben. [Twitter: @markaorlando]

Források

Egyszerű jelszókezelés: https://www.sans.org/security-awareness-training/resources/making-passwords-simple/
Pszichológiai manipulációs támadások: https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering/
Üzenetküldéses/SMS csalások: https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks/
Átverés a közösségi médián keresztül: https://www.sans.org/newsletters/ouch/scamming-you-through-social-media/

A fordítást készítette: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI)