CTI Jelentés

Tudnivalók a biztonságos online vásárláshoz – I. rész

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET

Tartalomjegyzék

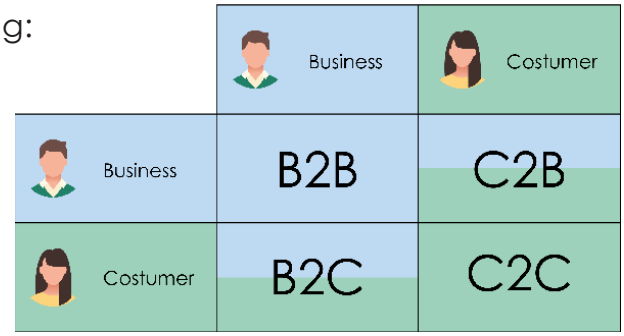
Bevezetés

Az e-kereskedelem röviden az online lebonyolított üzleti tranzakciókat jelenti. Legnépszerűbb formája az online kereskedelem, és olyan típusú tevékenységeket is magába foglal, mint például az online jegyértékesítés és aukciók. Lényege, hogy teljes mértékben megegyezik „offline" párjával annyi eltéréssel, hogy valamilyen elektronikus hálózaton, elsősorban interneten keresztül zajlik.

A Statista és a Medium kutatásai is azt mutatják, hogy rohamos léptékben nő az e-kereskedelem szerepe világszerte. Míg 2014-ben összesítve 1300 milliárd dollár értékben zajlottak le tranzakciók ebben a szektorban, addig átlagosan ez az összeg 20%-kal nőtt évente, és megközelítette az 5000 milliárd dollárt a 2021-es év végére. Egyes becslések szerint 2025-re a 7000 milliárd dollárt is meghaladhatja. Az országokat tekintve 2019-ben Kína állt az első helyen, és több mint 1000 milliárd dollár értékű összesített tranzakciós értéket prognosztizálnak számára a 2023. évben.

A világ 10 legnagyobb forgalmát generáló ország az e-commerce szektorban, forrás: https://medium.com/swlh/the-growth-of-ecommerce-2220cf2851f3

Az üzletben résztvevő felek szerint az e-kereskedelem 4 típusát különböztetjük meg:



- Business-to-Business (B2B): Amikor a vállalkozások a termékeiket tovább értékesítik más vállalkozások számára, hogy azok saját árucikkeik előállításához használják fel.
- Customer-to-Business (C2B): Amikor a fogyasztók eladják termékeiket vagy szolgáltatásaikat a vállalkozásoknak.
- Business-to-Customer (B2C): Az e-kereskedelem leggyakoribb fajtája, amikor a fogyasztó vásárol valamilyen árucikket vagy szolgáltatást. Ez a legtöbb esetben az online áruházakban valósul meg.
- Customer-to-Customer (C2C): A fogyasztók más fogyasztóknak adnak el termékeket. Ezek a termékek lehetnek újak is, de a legtöbb esetben ezek valamilyen használt áru kereskedelmét jelenti olyan oldalakon, mint a Vatera vagy eBay.

Jelen dokumentumban a B2C és C2C biztonsági kockázatait taglaljuk és olyan praktikákat mutatunk be, amelyekkel az e-kereskedelem biztonságosan használható bármely felhasználó számára. A másik két értékesítési csatorna részleteit egy másik, ennek a sorozatnak a következő részének szánt tájékoztatóban részletezzük.

Biztonsági kihívások az online vásárlások során

Ugyan a Covid időszak felgyorsította az e-kereskedelem terjedését a világon, azonban nem kizárólag ennek tudható be a növekvő tendencia. Néhány évtizeddel ezelőtt a pénzünk nagy részét lakhelyünkön, helyben költöttük el a különféle kereskedelmi egységekben, azonban manapság ezek a szokások megfordulni látszanak. Ehhez nagy mértékben hozzájárul az a tény, hogy a globális és lokális pénzintézetek és kormányok folyamatosan törekszenek arra, hogy a szükséges infrastruktúrák kiépítése után teljesen kivonásra kerüljön a készpénz, mint fizetőeszköz, így egyre nagyobb szerepet kapnak a bank- és hitelkártyák.

A két kártyatípus közt annyi a különbség, hogy amíg az előbbivel az ember a saját pénzét költi, addig utóbbival a bankét, és rendszerint kamatot számolnak fel a használatuk után. A bankok azt az emberi tulajdonságot használják ki, hogy amíg bizonyos mennyiségű készpénz birtokában vagyunk és abból vásárolunk, párosul egy olyan tudatalatti érzés a költekezéssel, amely spórolásra int minket, vagyis gondolkodás nélkül ügyelünk arra, hogy mennyit költünk a készpénzünkből. Ezzel szemben a bank- és hitelkártya használata során a tudatalattink azt sugallja, mintha korlátlan mennyiségű pénz lenne a számlánkon. Természetesen ez sem írható le feketén fehéren, nem mondható, hogy mindig, mindenki gondolkodás nélkül, két kézzel szórja a pénzét, ha kártyát használ, de az említett pszichológiai tényező fontos szerepet tölt be az évről évre növekvő költekezésben, amelynek a hasznát az e-kereskedelmi szolgáltatók is élvezik.

Természetesen ez sem írható le feketén fehéren, nem mondható, hogy mindig, mindenki gondolkodás nélkül, két kézzel szórja a pénzét, ha kártyát használ, de az említett pszichológiai tényező fontos szerepet tölt be az évről évre növekvő költekezésben, amelynek a hasznát az e-kereskedelmi szolgáltatók is élvezik.

Ennek tudatában fontos megjegyezni, hogy amíg egyre nagyobb forgalmat generál a szektor, sajnálatos módon egyre többen fognak olyan lehetőségek után kutatni, amelyeket kihasználva vissza tudnak élni a vásárlók jóhiszeműségével, figyelmetlenségével vagy a nem tudatos vásárlási szokásaival. Éppen ezért körültekintően kell eljárni, és nem csak a vásárlásaink során, hanem a mindennapos internethasználat során is. Erre azért van szükség, mert lehetséges, hogy bár arra figyelünk, hogy ne egy adathalász oldalon böngésszünk és adjunk le rendelést az érzékeny adatainkat megadva, azonban, ha például kapunk egy e-mailt egy ismeretlen feladótól és gyanútlanul megnyitjuk a mellékletet, elképzelhető, hogy egy kártevő már telepítésre is került a készülékünkön, és onnantól kezdve minden legitim oldalon megadott információ rossz kezekbe kerül.

Az Internet adta kényelem nagy prioritást élvez a vásárlásaink során is. Ha például szeretnénk egy számunkra megfelelő paraméterekkel rendelkező terméket vásárolni, egy fizikai üzletben nem adatik meg az a kényelmi lehetőség, hogy másodpercek alatt átmenjünk egy másik áruházba és az ott található termékeket is megtekintsük. Az internetes webáruházak közti böngészés, a legjobb ajánlat megtalálása azonban töredék energiát és időt igényel, hiszen azonnal válthatunk két webshop között. Ennek még gyorsabb, még hatékonyabb kihasználásában a különböző árösszehasonlító oldalak is segítséget nyújtanak. Az ilyen oldalakon szereplő áruházak bizonyos mértékű garanciát jelentenek, ám ehhez is célszerű szkeptikusan hozzáállni. Annak kisebb a kockázata, hogy egy adott terméket megvásárolva a kereskedő eltűnik a pénzükkel, azonban sokkal nagyobb az esély, hogy nem megfelelő minőségű szolgáltatást nyújt (például hibás vagy másfajta terméket küld, gondok vannak a kiszállítással vagy visszaküldéssel, hónapokig húzódik a pénzvisszatérítés stb.).

Minden évben jelennek meg olyan adathalász kampányok, amelyek például közösségi oldalak hirdetéseiben terjednek és valamilyen terméket kínálnak rendkívül kedvező áron vagy olyan nyereményjátékot hirdetnek, amiben néhány ezer forintért lehet részt venni. Érdemes mindig olyan jó hírű kereskedőnél vásárolni, amelyet ismerünk. A jó ár vagy ár/érték arány is fontos, de mindig legyünk körültekintők, hogy milyen oldalon kívánunk vásárolni, ne csak azt vegyük figyelembe, hogy hol a legolcsóbb az adott termék.

Ha találunk valamilyen visszautasíthatatlannak tűnő ajánlatot, tájékozódjunk a webshop kilétéről, annak legitimitásáról és több platformon keressünk vásárlói véleményezéseket. Amennyiben nem, vagy csak nagyon kevés véleményt találunk, melyek kivétel nélkül 5 csillagosra értékelik az oldalt, jó, ha megszólal a fejünkben a vészcsengő, ugyanis elképzelhető, hogy valaki így akarja becsapni az áldozatait.

Egy fizikai üzletbe betérve garantáltan megkapjuk a biztonságérzetet: ismerjük a boltot, lehet évek óta odajárunk, és sokan mások is oda járnak vásárolni. Az internetes vásárlások során is ugyanúgy ügyelnünk kell erre, és figyelni kell az árulkodó jelekre, ha egy kártékony oldalra tévedünk.

A vásárlókat érintő leggyakoribb támadási technikák

A kiberbűnözők különböző, jól bevált technikákat használnak azért, hogy elérjék céljukat, ami lehet anyagi haszonszerzés vagy, hogy ellopják a felhasználók érzékeny adatait.

Ezt leggyakrabban úgy érik el, hogy átveszik az irányítást a felhasználók fiókjai felett úgy, hogy megszerzik a fiókhoz szükséges hitelesítő adatokat, majd azokkal belépve tranzakciókat és egyéb műveleteket hajtanak végre az áldozat nevében. A pénzutalások mellett a kiberebűnözők rendszerint nagyobb értékű ajándékkártyákat is vásárolnak.

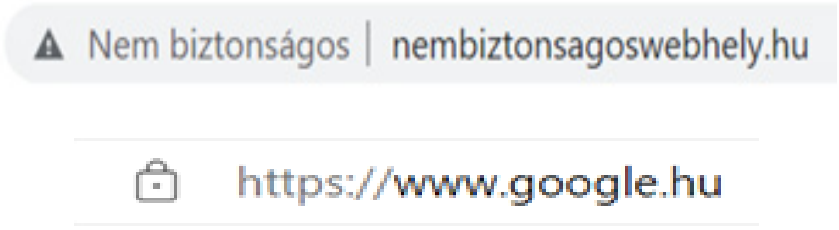
A hitelesítő adatok megszerzését több technikával is végrehajthatják. Egyik ilyen módszer az adathalászat, amelyrről az NBSZ NKI korábban már készített egy kiberbiztonsági elemzést, Adathalászat – a leghatékonyabb kiberfegyver címmel, ezért jelen dokumentumban nem kerülnek mélyebben bemutatásra a támadás módszerei.

Másik ilyen állandó problémát jelentő technika a rosszindulatú programok és reklámprogramok (malware/adware), különösen az e-kereskedelemben használt platformok esetén. Ezekkel a szoftverekkel elfoghatják az adatokat, és hozzáférhetnek a felhasználói hitelesítő adatokhoz. Normál körülmények között az adware-ek törvényesek, és sokszor kedvezményekkel kínálnak termékeket, ezért van létjogosultságuk, azonban

a kiberbűnözők igyekeznek ezt is kihasználni. Az adware-eket használhatják arra is, hogy olyan rosszindulatú webhelyekre csalogassák a vásárlót, ahol arra ösztönzik őket, hogy megadják a személyes és hitelkártya adataikat. Azonban már egy alapszintű vírusirtóval sokat tehetünk a védelmünkért, hiszen ezek képesek figyelmeztetni a legtöbb rosszindulatú szoftverre, és eltávolítani azokat, ha már települtek az eszközeinkre.

Az adatok titkosítása elengedhetetlen webes alkalmazásbiztonsági gyakorlat. Egyes webhelyek nem titkosítják az adatokat. Ezek elavult SSL tanúsítványokkal és HTTP protokollokkal működnek, ami sebezhetővé teszi őket és a vásárlókat a támadásokkal szemben.

Minden olyan weboldal, amelynek URL címe HTTPS helyett HTTP-vel kezdődik, nem titikosított, ezért különösen figyeljünk ezen oldalak használatának mellőzésére. Míg utóbbinál egy „nem biztonságos" felirattal figyelmeztetnek a böngészők, úgy a HTTPS protokollt használó webhelyeknél egy lakat jelenik meg a felhasználó számára.



HTTP és HTPPS protokollt használó weboldalak jelölése

Ha olyan weboldalakra regisztrálunk, amelyeknek nincsenek komolyabb biztonsági megoldásaik a támadások megakadályozására, előfordulhat, hogy **személyazonosság-lopás** áldozatává válhatunk, ha a kiberbűnözők sikeresen feltörik a webhelyeket.

Nem minden e-kereskedelmi oldal valódi. Léteznek olyan szoftverek, amelyek képesek lemásolni bármilyen, például egy sokak által használt, jóhírű weboldal arculatát, így megtévesztve a vásárlókat. A regisztrációt követően a leadott megrendeléseket azonban soha nem szállítják ki. Ezek a hamis oldalak sok esetben olyan promóciós ajánlatokat tesznek közzé a közösségi médiákban, amelyek visszautasíthatatlannak tűnnek.

Csaló, megtévesztő hirdetés

A nyílt, nem biztonságos Wi-Fi használata mindig potenciális veszélyeket rejt magában, mivel lehetővé teszi az adatok titkosítás nélküli továbbítását a hálózatokon keresztül. Az ilyen hálózatok legtöbbször nincsenek vagy nagyon gyengén vannak védve, ami tökéletes lehetőséget teremt a kiberbűnözők számára, hogy lehallgathassák a hálózati forgalmat. Ezzel a támadók megszerezhetnek minden olyan adatot, amit például egy regisztrációs felületen megad a vásárló.

Az NBSZ NKI javaslatai az online vásárlások során

- Ha számítógépen internetezünk, érdemes a hivatkozások megnyitása előtt - különösen az e-mailben érkező linkek esetén - a link fölé mozgatni a kurzort, így láthatjuk, hogy az adott hivatkozás milyen oldalra vezet valójában. Fontos azt is megemlíteni, hogy bár ritkán használt módszer, a kiberbűnözők képesek az így megjelnő hivatkozásokat is manipulálni, ezért a lenti tanácsok betartása is javasolt.

- Mindig ellenőrizzük az URL címeket, kimondottan az ismeretlen feladóktól kapott linkeket! A támadók gyakran használnak az eredetihez hasonló domaineket, mint például y0utube.com, faceb00k.com, official-paypal.com.

- Ellenőrizzük a https:// meglétét azokon az oldalakon, ahol érzékeny adatokat kell megadnunk! Fontos, hogy ez önmagában nem elegendő művelet, ugyanis adathalász oldalakon is használhatnak ilyen protokollt.

- Tartsuk mindig naprakészen a böngészőnket és a vírusírtónkat!

- Egyes szűrőprogramok kijátszása érdekében a támadók képként is beilleszthetik a szöveget az e-mailben. Mindig legyünk körültekintők azokkal az e-mailekkel is, amelyek a szöveget kép formájában jelenítik meg.

- Rendkívül fontos a cégeknél, hogy rendszeresen biztosítsanak biztonságtudatossági képzést az ott dolgozóknak, naprakészen tartva ezáltal a tudásukat. Magánszemélyként is fontos az önképzés, mindig tájékozódjunk a legújabb támadási módszerekről és trendekről.

- Ha egy számunkra ismeretlen személy vagy cég keres fel bennünket egy visszautasíthatatlan ajánlattal, győződjünk meg a megkereső hitelességéről!
- Mobileszközeinkkel kerüljük a nyilvános Wi-Fi hálózatokat, használjunk helyettük mobil internetet!
- Lehetőség szerint használjunk VPN szolgáltatást!
- Ha tehetjük válasszuk inkább az utánvétes fizetést vagy egy olyan közvetítő fizetési szolgáltatást, ami garanciát vállal az online szolgáltatások során.

A PayPal például nagy figyelmet fordít arra, hogy kizárólag olyan cégekkel, vállalatokkal legyen kapcsolatban, amelyek önmagukban garanciát jelentenek, de ha véletlenül átverés áldoztává válna egy felhasználó, a PayPal az okozott kárt teljes mértékben megtéríti.

- Mindig használjunk több faktoros hitelesítést, ahol csak lehetőségünk van rá!
- Használjunk virtuális hitelkártyát! Ez a kártyatípus csak virtuálisan létezik és kizárólag internetes vásárlásokra használható.
- Ha papíralapú számlakivonatot vagy bármilyen olyan jellegű dokumentumot kapunk a vásárlásról, amely személyes, érzékeny adatokat tartalmaz, ne dobjuk egyszerűen a szemétbe, hanem semmisítsük meg olyan módon, hogy azon ne maradjon visszanyerhető információ!
- Ha csalás áldozatává váltunk, jelentsük mielőbb a bankunknál, és tegyünk rendőrségi feljelentést!


End
Ins

Milyen szempontokat érdemes figyelembe venni jelszóválasztásnál?

- Ne legyen ránk jellemző, mert kevés információ birtokában is könnyen kitalálható (pl.: családtag neve + születési dátum egy rövid kereséssel a közösségi oldalakon kideríthető).
- Nem szerencsés, ha a jelszó csak egy szóból áll (például az „almafa" szó biztosan szerepel egy támadó által kipróbálandó jelszavak listájában).
- Jó, ha a jelszó hosszú és többféle karaktert (kisbetű, nagybetű, szám, írásjel) tartalmaz, mert ezzel megnehezíti a brute force technikával való feltörést.
- A legjobb, ha néhány szóból álló jelmondatot választunk, amelyben van kisbetű, nagybetű, szám és írásjel is. Ezt könnyű megjegyezni, azonban nehéz kitalálni, brute force technikával feltörni pedig szinte lehetetlen.

Hogyan kezeljük a jelszavainkat?

- Fontos, hogy ne adjuk „kölcsön" a jelszavunkat, hiszen nem tudhatjuk, hogy az adott személy körültekintően fogja-e kezelni.
- Ne írjuk fel a jelszavunkat, mert ez könnyen illetéktelen kezekbe kerülhet.
- Ne használjuk mindenhol ugyanazt a jelszót, ha a támadók egyet feltörnek, minden más rendszerünkhöz is hozzáférhetnek.
- Rendszeresen változtassuk meg a jelszavainkat, a támadónak minél több ideje van próbálkozni, annál nagyobb valószínűséggel tudja megszerezni a hozzáférésünket.
- Használjunk valamilyen jelszókezelő rendszert! Ezek olyan szoftverek, amelyek titkosított formában tárolják jelszavainkat, így azokhoz illetéktelenek (ideális esetben) nem — vagy csak irreálisan nagy erőforrás ráfordításával — férhetnek hozzá. A megoldás előnye, hogy ehhez csupán egyetlen, ún. mesterjelszót kell fejben tartanunk, azt, amellyel hozzáférhetünk az elmentett jelszavakhoz. A jelszókezelőkről bővebben az NBSZ NKI weboldalán itt írtunk.

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2022