# Vigyázat: Black Friday és karácsony? Kiváló terep az online csalók számára!

*Az online csalóknak az év vége olyan, mint egy tömött, ringó busz a zsebtolvajoknak*

A Black Friday és a karácsonyi ajándékvásárlás időszaka hagyományosan az év legnagyobb online vásárlási hullámát hozza el. Az elmúlt években az e-kereskedelem robbanásszerű növekedést mutatott, de az év végi akciók idején és az ünnepi időszak heteiben a rendelések száma a legmagasabb az év során. A netes vásárlás egyszerűsége és gyorsasága azonban nemcsak a vásárlók számára, hanem az online csalóknak is nagy lehetőségeket jelent. Van megoldás a biztonságra.

A Yettel országos reprezentatív kutatása szerint évről évre nő azok száma, akik „kizárólag" vagy „nagyrészt online" tervezik megvenni a karácsonyi ajándékokat – idén már tízből négyen vásárolnak így. Az online vásárlók 55%-a időmegtakarítás miatt választja ezt a módszert, 46%-uk kizárólag így éri el a kiválasztott terméket vagy ajándékot, szintén a válaszadók közel fele a zsúfoltságot, tömeget szeretné elkerülni az online vásárlás segítségével. A netes vásárlók 45%-a a kényelem miatt választja az internetet és minden harmadik netes vásárlót az így elérhető alacsonyabb árak vonzzák. A számos pozitívum mellett, amit az online rendelés és csomagkézbesítés kínál, a megnövekedett tranzakciószám a kibertámadások és online csalások számára is nagyobb teret enged. Fontos, hogy a vásárlók tudatosak és elővigyázatosak legyenek kattintásaik során, különösen igaz ez az év végi feladatokkal és plusz teendőkkel teli időszakban, amikor a figyelmünk a szokásosnál is jobban megoszlik.

**A leggyakoribb online csalási formák, amelyekre érdemes figyelni:**

- Megtévesztő SMS-ek csomag érkezéséről vagy nyereményről – Hamis linkekkel csalják ki az áldozatok adatait, vagy kérnek kisebb összegeket „csomagkezelési díjként".
- Hamis webáruházak – Akár nagy márkák weboldalaival azonos megjelenésű, de csalók által üzemeltetett weboldalak, ahol a megrendelés és fizetés után a vásárló sem árut nem kap, sem a kifizetett pénzét nem látja viszont; rosszabb esetben a bankkártya adatokat is megszerzik a csalók, ami további visszaélésre ad lehetőséget számukra.
- Közösségi médiában vagy online hirdetésen keresztüli megtévesztés – Hihetetlenül nagy akcióval hirdetett termékek, amelyek mögött gyakran semmilyen valós szolgáltatás nincs.
- Adathalász e-mailek – Banki, telekommunikációs vagy közműszolgáltatói értesítésnek álcázott üzenetek, amelyek révén érzékeny adatokat próbálnak megszerezni a csalók.
- Telefonos csalások – Olyan hívások, amelyek során az „ügyintéző" a vásárló bankkártyájához vagy személyes adataihoz kér hozzáférést.

**Hogyan védekezhetünk az online fenyegetések ellen?**

A tudatosság és az óvatosság kulcsfontosságú. Például, ha várunk is csomagot, a kézbesítési értesítéseket kezeljük figyelmesen, hogy nem egy csaló üzenet férkőzött-e a várt információk közé. A tudatosság mellett érdemes az elérhető technológiai védelemre is támaszkodni. A Yettel NetPajzs megoldás kifejezetten az online biztonságra fókuszál, hatékony védelmet nyújt az adathalász támadások ellen a mobilszolgáltató hálózatát használó előfizetők számára. Ráadásul ez a szolgáltatás az első hónapban ingyenes, azt követően pedig havonta egy kávé árának megfelelő összegért aktív védelemmel látja el a felhasználókat a Yettel hálózatán.

Ne hagyjuk, hogy az ünnepi készülődés bosszúságot okozzon – legyünk résen, és gondoskodjunk a biztonságunkról!

További információk: yettel.hu/netpajzs

**A számos észlelt csalási kísérletből két sikeres, megtörtént esetpélda a közelmúltból**

*„Csalás miatt nyomoz a Miskolci Rendőrkapitányság egy ismeretlen elkövetővel szemben. Egy helyi cég levelezési címére november 14-én egy bank nevében megtévesztő emailt küldött a csaló, amelyben a netbanki jelszó módosítását kérte. A levél formailag teljesen úgy nézett ki mintha a pénzügyeiket kezelő banktól érkezett volna. A kérésnek eleget tett a cég képviselője, így a csaló megszerezte az új netbankos belépőkódot, amivel közel 7 millió forintot utalt át egy ismeretlen számlára. A cég ügyvezetője észlelte, hogy csalás áldozata lett és azonnal bejelentést tett a rendőrségen, illetve a bankjánál is, így egy magánszámlán közel 4 millió forint továbbutalását sikerült megállítani, a nyomozás pedig jelenleg is folyik.”*

*„Egy Vas vármegyei lakos kapott egy SMS-t, amely látszólag a mobilszolgáltatójától érkezett. Azt gondolta, hogy a felhalmozott pontjait tudja beváltani, ezért rákattintott a linkre, amely egy weboldalra vezetett. Ott megadta a bankkártyája összes adatát és a nevét is. Másnap érkezett egy üzenet a bankos applikációjába arról, hogy többször próbáltak vásárolni a kártyájával. Egy alkalommal sikerrel is jártak a csalók, külföldön használták a sértett kártyaadatait. Ebben az esetben a sértettnek szerencséje volt, mivel a bankjánál észrevették a gyanús tranzakciókat, és felfüggesztették a kártyáját.”*

Sajtókapcsolat:

- sajto@yettel.hu

Eredeti tartalom: Yettel Magyarország Zrt.

Továbbította: Helló Sajtó! Üzleti Sajtószolgálat

Ez a sajtóközlemény a következő linken érhető el:
https://hellosajto.hu/17191/vigyazat-black-friday-es-karacsony-kivalo-terep-az-online-csalok-szamara/