

# Szinte mindenki online vásárol karácsonykor - mutatjuk mire érdemes figyelni

Közeleg a karácsony, az online vásárlások csúcspontja. A Visa felmérést<sup>[1]</sup> készített Magyarországon az év végi ajándékbeszerzésről, online vásárlási szokásainkról. Az idei roham előtt az új és a rutinos vásárlókkal is érdemes átvenni az online rendelések veszélyeit és a legújabb csalási módszereket. Ebben segítenek az OTP Bank és a Visa szakértői.

Szinte minden magyar válaszadó (97%) tervez online vásárlást az év végi ünnepek közeledtével - derül ki a Visa friss kutatásából.

„A karácsonyi időszak alatt nagymértékben növekszik a kereslet az elektronikai eszközökre, játékokra, divatcikkekre és szépségápolási termékekre, sokan vásárolnak nagyobb értékű ajándékokat. Népszerűek a könyvek, a lakásdekorációs tárgyak és a gasztro-ajándékok is, hiszen ezek jól illeszkednek az ünnepi hangulathoz. A sporteszközök és a szabadidős termékek pedig főként az újról fogadalmak miatt népszerűek” - **mondta el Szócs András, a fizz.hu ügyvezető igazgatója.**

Az OTP Bank online piacterének tapasztalatai szerint a vásárlások kétharmadában jellemzően a házhozszállítás a preferált kézbesítési mód. A karácsony közeledtével viszont felértékelődik a bolti, az automatából való vagy a csomagpontos átvételi lehetőség. A vásárlók így biztosítják azt, hogy még az ünnepek előtt időben meg is érkezzon az ajándék. A Visa kutatása szerint az idősebb korosztály (54-65 év) veszi igénybe magasan a legtöbbször a személyes átvételt az internetes rendelések esetében.

A fizetési szokásokat tekintve, a rendelés leadásakor a vásárlók többsége a bankkártyaadatok megadásával (43%) vagy mobiltelefonra mentett bankkártyával (28%) egyenlíti ki a vásárlás értékét. Átvételkor is hasonló tendencia figyelhető meg: a vásárlók nagyobb része a bankkártyás fizetést választja (38%) a készpénzes fizetéssel szemben (28%).

A felmérés szerint háromból két ember (66%) egészen decemberig vár a karácsonyi bevásárlással, sőt a válaszadók 10%-a csak az ünnepek előtti napokban kezdi el az ajándékok beszerzését. Az utolsó pillanatos vásárlások során, az időnyomás miatt lankadhat a figyelem, így könnyebben válhatunk csalás áldozatává.

„A legfontosabb, hogy védjük a bankkártyaadatainkat, belépési kódjainkat és csak biztonságos helyeken használjuk ezeket. Ne feledjük, hogy a bank soha nem fogja kérni tőlünk a fizetési adatainkat, ezért ne is adjuk ki senkinek. Emellett törekedjünk arra, hogy csak megbízható webshopokból vásároljunk” - **mondta Juhász Katalin, a Visa regionális termékfejlesztési vezetője.**

Interneten vásárolni ugyanis olyan, mint kerékpározni: szinte mindenki használja, mert gyors és kényelmes, de elég egy apró figyelmetlenség az úton és könnyen orra bukhat az ember. Az orra bukás pedig ebben az esetben azt jelenti, ha csalók áldozatává válunk.

A csalási módszerek folyamatos megújulását mutatja, hogy tízből négy válaszadó (41,2%) nem biztos abban, hogy minden online csalási módszert ismer és felismer. A válaszadók közel felénél (45,5%)

már próbálkoztak csalók, de sokkal magasabb azok aránya (28,8% kontra 16,7%) akik időben észrevették ezt és ezért nem jártak náluk sikerrel.

Azok között, akiket ért már kár online csalás során (16,7%) a leggyakoribb eset az e-mailben vagy sms-ben kapott hamis linkre kattintás (26%). Ettől a módszertől alig marad el (24,1%) a nem létező termék megvásárlása, a harmadik leggyakoribb pedig a hamis weboldalon megadott bankkártyaadatokkal történő csalás (18,4%).

A csalók egyre inkább a fogyasztókat veszik célba és pszichológiai módszerekkel igyekeznek az ember gyengeségeit kihasználni. Ennek egyik legfőbb oka, hogy a folyamatos fejlesztéseknek köszönhetően a technológia mára egyre biztonságosabb. A Visa például az elmúlt öt évben több mint 10 milliárd dollárt fektetett be többek között a csalásellenes és biztonsági technológiáinak folyamatos korszerűsítésére, amivel csak a 2023-as évben 40 milliárd dollárnyi csalást akadályozott meg.

„Néhány aranyszabály betartásával jelentősen csökkenthetjük a sikeres csalások esélyét. Mielőtt az online térben vásárlunk, mindig ellenőrizzük azt, hogy hol járunk: a legbiztosabb módszer, ha a weboldal címét – a felső URL sávban – betűről betűre ellenőrizzük. Már 1 karakter eltérésnél biztosak lehetünk benne, hogy hamis weboldalon járunk, még ha az oldal első ránézésre hasonlít az eredetire. Soha ne utaljunk pénzt ismeretlen személy kérésére, felhívására, akkor sem, ha hivatalos személyként, vagy banki ügyintézőként mutatkozik be, illetve ne telepítsünk ismeretlen szoftvereket saját eszközeinkre, még akkor sem, ha arra telefonhívás során, vagy üzenetben, e-mailben kérnek. Soha ne kattintsunk üzenetben érkező csatolt linkre, mivel ezen üzentekben hamis információkkal próbálnak befolyásolni minket: letiltásra kerül a bankkártyánk, lejárt az előfizetésünk, csomagot várunk, de probléma merült fel a szállítás során. Mindig olvassuk el a banktól érkező figyelmeztető SMS-eket, Push üzeneteket, hiszen ezek fontos információk! A legfontosabb, hogyha elbizonytalanodunk, ne csináljunk semmit, amit a hívó kér, fejezzük be a beszélgetést, és hívjuk fel a saját bankunkat az ismert számokon, vagy keressük fel a bankfiókot vagy a mobilalkalmazásban 2 lépésben ellenőrizhetjük, hogy valóban a banktól hívnak, az alkalmazásra, majd a profil ikonra kattintva azonnal megjelenik az üzenet: jelenleg nem hívunk, vagy hívunk. Praktikus biztonsági megoldás, ha a vásárlási és átutalási limitünket alacsony összegre állítjuk és csak arra azon alkalmak során emeljük meg az összeget, amikor nagyobb összegben vásárlunk”  
- **mondta Sonjic László, az OTP Bank Biztonsági Igazgatóságának vezető tanácsadója.**

A szakértő hozzátette, hogy fontos felvértezni magunkat a támadásokkal szemben, ezért érdemes rendszeresen tájékozódni a legújabb csalási formákról a bank, valamint a Kiberpajzs honlapján. Az OTP Bank és a Visa is csatlakozott a KiberPajzs programhoz, amelynek weboldalán hasznos tippeket és friss híreket találhatunk a csalások megelőzéséről és a biztonságos online vásárlásról.

## **A Visáról**

A Visa (NYSE: V) a világ egyik vezető digitális fizetési szolgáltatója, amely fizetési tranzakciókat bonyolít le a fogyasztók, kereskedők, pénzügyi intézmények és kormányzati szervek között több mint 200 országban és területen. Küldetésünk, hogy a világot a leginnovatívabb, legkényelmesebb, legmegbízhatóbb és legbiztonságosabb fizetési hálózaton keresztül összekapcsoljuk, lehetővé téve az egyének, a vállalkozások és a gazdaságok gyarapodását. Hiszünk abban, hogy az olyan gazdaságok, amelyek mindenkit, mindenhol magukba foglalnak, mindenkit, mindenhol felemelnek, a hozzáférést pedig a pénzmozgás jövője alapjának tekintjük. Tudjon meg többet a [Visa.co.uk](https://www.visa.co.uk) oldalon.

## A KiberPajzsról

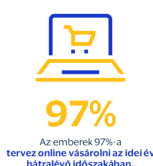
A digitális térben elkövetett pénzügyi visszaélések megelőzése és visszaszorítása érdekében kötött megállapodást a Magyar Nemzeti Bank, a Magyar Bankszövetség, a Nemzeti Média- és Hírközlési Hatóság, a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet, valamint az Országos Rendőr-főkapitányság „KiberPajzs” elnevezéssel 2022 novemberében. Az együttműködéshez később az Igazságügyi Minisztérium a Gazdaságfejlesztési Minisztérium, a Magyar Államkincstár, valamint a Szabályozott Tevékenységek Felügyeleti Hatósága és a Nemzeti Védelmi Szolgálat is csatlakozott. A KiberPajzs program célja, hogy az ügyfelek, a hatósági és piaci szereplőkkel közösen, „golyóálló” védelmet alkossanak a digitális bűnözőkkel szemben. A KiberPajzs projekt keretében a kiberbiztonsági kockázatok és az ellenük való védekezési lehetőségek bemutatásáról széleskörű, összehangolt kommunikációs kampányokat folytatnak az intézmények és a piaci szereplők, valamint kommunikációs partnerként a Médiaunió Alapítvány (kiberpajzs.hu, akulcstevagy.hu). Fontos, hogy itt megtalálható az összes aktuális elkövetési módszer, az ismérvekkel együtt, amelyek segítségével felismerheti az ügyfél, hogy csálókkal áll szemben, valamint tartalmazza azon információkat, amelyek ismerete nagymértékben hozzájárul, hogy ne váljunk csalás áldozatává.

<sup>[1]</sup> A kutatást az Ipsos végezte a Visa megbízásából 2024 szeptemberében Magyarországon, online adatgyűjtési módszerrel, 1014 fős mintán.

### Sajtókapcsolat:

- OTP Bank
- kommunikacio@otpbank.hu

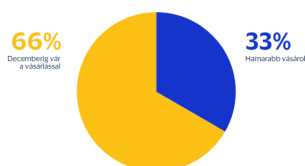
© Visa



Forrás: A kutatást az Ipsos végezte a Visa megbízásából 2024 szeptemberében Magyarországon, online adatgyűjtési módszerrel, 1014 fős mintán.

1

### Az emberek többsége kívár a vásárlással

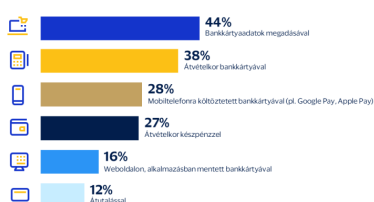


Forrás: A kutatást az Ipsos végezte a Visa megbízásából 2024 szeptemberében Magyarországon, online adatgyűjtési módszerrel, 1014 fős mintán.

2

© Visa

### Az online vásárlók így fizetnek leggyakrabban rendeléseikért:

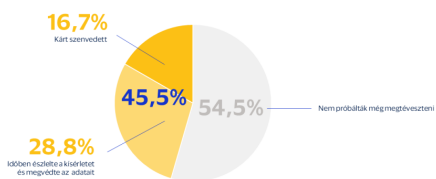


Forrás: A kutatást az Ipsos végezte a Visa megbízásából 2024 szeptemberében Magyarországon, online adatgyűjtési módszerrel, 1014 fős mintán.

3

© Visa

A válaszadók közel felét próbálták már megtéveszteni

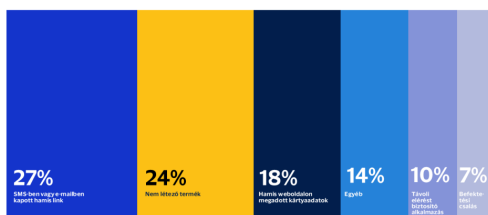


Forrás: A kutatást az Ipsos végezte a Visa megpályázott 2024. évszámában Magyarországon, online adatszolgáltatásokkal. Kérjük, nevével

4

© Visa

A leggyakoribb visszaélési módszerek



Forrás: A kutatást az Ipsos végezte a Visa megpályázott 2024. évszámában Magyarországon, online adatszolgáltatásokkal. Kérjük, nevével

5

© Visa

A biztonságos online vásárlás 5 aranyabálya

**Védje a bankkártya és belépési adatait!**  
 Összes biztonságot előidéző bankkártya és belépési adatait, ne csak a kártya magját, hanem a kártya hátoldalán lévő adatokat is meg kell őriznie.  
 Ha adatait hirtelen elveszté, azonnal jelezze a banknak, és azonnal töröltesse az adatait.  
 Az internetes vásárlás során ne a kártya hátoldalán lévő adatokat használja a kártya adatait megadni, hanem a kártya hátoldalán lévő adatokat.  
 Ha adatait elveszté, azonnal jelezze a banknak, és azonnal töröltesse az adatait.

**Soha ne kattintson ismeretlen forrásból származó linkekre!**  
 Először ellenőrizze, hogy a linkeket a bank honlapján vagy a bank mobilalkalmazásában találja-e. Ha ismeretlen forrásból érkezett a link, ne kattintson rá.  
 Az internetes vásárlás során ne a kártya hátoldalán lévő adatokat használja a kártya adatait megadni, hanem a kártya hátoldalán lévő adatokat.  
 Ha adatait elveszté, azonnal jelezze a banknak, és azonnal töröltesse az adatait.

**Ne telepítsen ismeretlen forrásból származó szoftvereket!**  
 Kerülje az ismeretlen forrásból származó szoftverek telepítését, és ne használja a kártya adatait az ismeretlen forrásból származó szoftverekkel.  
 Ha ismeretlen forrásból származó szoftvert telepít, azonnal jelezze a banknak, és azonnal töröltesse az adatait.  
 Ha ismeretlen forrásból származó szoftvert telepít, azonnal jelezze a banknak, és azonnal töröltesse az adatait.

**Csak megbízható webshoppokról vásároljon!**  
 Mindig ellenőrizze, hogy a vásárlás előtt a weboldal biztonságos-e, azaz az URL-cím végén szerepel-e a https:// előjel.  
 Figyeljen a weboldalon megjelenő adatokra, és ne adja ki a kártya adatait ismeretlen forrásból.  
 Ha ismeretlen forrásból származó szoftvert telepít, azonnal jelezze a banknak, és azonnal töröltesse az adatait.  
 Ha ismeretlen forrásból származó szoftvert telepít, azonnal jelezze a banknak, és azonnal töröltesse az adatait.

**Figyelmesen ellenőrizze a banki értesítéseket!**  
 Azonnal jelezze a banknak, ha a banki értesítések nem az Ön nevére érkeznek, vagy ha a banki értesítések nem az Ön nevére érkeznek.  
 Ellenőrizze a banki értesítéseket, és ha szükséges, jelezze a banknak.  
 Ellenőrizze a banki értesítéseket, és ha szükséges, jelezze a banknak.

6

© Visa

Eredeti tartalom: OTP Bank

Továbbította: Helló Sajtó! Üzleti Sajtószolgálat

Ez a sajtóközlemény a következő linken érhető el:

<https://hellosajto.hu/17064/szinte-mindenki-online-vasarol-karacsonykor-mutatjuk-mire-erdemes-figye/lni/>