



vásárlás az interneten

online fizetés

payu

Mit érdemes tudni a PayU-ról?

egyszerű

kereskedőknek

biztonságos

vásárlóknak

legmagasabb minőség

Mit érdemes tudni a PayU-ról?

A PayU Magyarországon az internetes kártyás fizetési lehetőséget biztosító stabil banki háttérrel, kártyatársasági biztonsági szabványokat alkalmazva, valamint a PayU nemzetközi tapasztalatait felhasználva honosította meg a szolgáltatását.

A fizetés folyamata megegyezik a bankok hasonló szolgáltatása keretében kínált fizetési eljárással. A PayU szolgáltatás jellegzetessége, hogy minden tranzakciót annak státuszával (pl.: sztorrió) a rendszer automatikusan e-mail-en visszaigazol, valamint a tranzakcióval kapcsolatos kérdései megválaszolására saját ügyfélszolgálat áll az Ön rendelkezésére telefonon, e-mail-en. A szolgáltatás keretében a felhasználó, így a kártyabirtokos biztonságát szem előtt tartva a tranzakciókat folyamatosan figyeli, s nem várt események megelőzésében nyújt segítséget.

Küldetésünk, hogy mind a kereskedők és a vásárlók részére integráltan nyújtott többlétszolgáltatásainkkal kényelmes, rugalmas alternatívát nyújtsunk az online fizetés világában, ezért a felhasználói élmény biztosítása érdekében további többletfunkciók bevezetésén dolgozunk.

További információért kérjük, látogasson el a www.payu.hu honlapra! Ügyfélszolgálat: 06 1 510 0707 | info@payu.hu

Melyek a tranzakció lépései?



1 A "Fizetés" gombra kattintva Ön átkerül a PayU fizetési oldalára, ahol az adatok helyességét a kártyaadatok megadásával elindítja a tranzakciót.

2 A kártyaadatok megadását követően kérjük, ellenőrizze a tranzakció feldolgozása elindul a banki feldolgozó rendszereken.

3 A fizetés eredményéről Ön e-mail útján is értesítést kap, valamint visszairányítjuk a szolgáltató oldalára.

4

Elfogadott kártyatípusok

A PayU online kártyás fizetési szolgáltatása keretében a következő kártyákkal fizethet:



MasterCard



Maestro *



VISA



VISA Electron *

*** FIGYELEM!** Nem minden bank által kibocsátott Maestro és VISA Electron típusú kártyával lehet interneten fizetni. Kérjük, érdeklődjön kártyakibocsátó bankjánál.

Megfelelés a biztonsági szabályoknak

A PayU rendelkezik mindazon nemzetközi szintű előírásokkal, melyek az online fizetés biztonságát garantálják. A nemzetközi online fizetési piacon elért sikereinket annak köszönhetjük, hogy a magas minőségű szolgáltatások biztosítása mellett az eszközök biztonságos használatát is garantáljuk. Rendszerünk a kártyatársaságok független szervezete által auditált PCI-DSS tanúsítvánnyal rendelkezik. A fizetés folyamatának biztonságát az adja, hogy érzékeny kártyaadatokat egy fizetőoldal adja meg, amelyen a titkosított kommunikációs kapcsolatot a Thawte 256 bites SSL tanúsítvány, illetve a McAfee Secure rendszer alkalmazása biztosítja.

a. Mi a PCI-DSS?

A PCI-DSS a kártyatársaságok által életre hívott közös biztonsági szabvány, amely informatikai és üzemeltetési követelményeket ír elő az azt alkalmazó szervezetek számára. Szolgáltatásunk biztonságát, a PayU csoport tagja, a PCI-DSS tanúsítvánnyal rendelkező GeCad ePayment International SRL biztosítja.



b. Mi a Thawte?

A Thawte vezető hitelesítő szolgáltató [CA - Certification Authority], valamint a VeriSign cégcsoport része. A nemzetközileg ismert tanúsítvány kibocsátó cég kommunikáció biztonságát tanúsító modulja valamennyi internet böngésző program tanúsítványába be van építve. Az oldal a Thawte SSL Web Server Certificate with Extended Validation 256-bites titkosítású tanúsítványával rendelkezik. Ez a gyakorlatban annyit tesz, hogy az adatok megadása védett, külső szereplő által nem megszerezhető.



c. Kártyaadatok megadásának webáruházról elkülönülő folyamata

Online fizetés során a rendelés esetén kért adatok megadását követően a webáruház fizetést előkészítő oldaláról a PayU biztonságos fizetőoldalára kerül át a vásárló, ahol a fizetéshez szükséges kártyaadatokat szükséges megadnia. A PayU fizetőoldal adattartalmáról a kereskedő nem szerez tudomást, mivel az tőle független és védett internetes oldal.



Bankkártyával történő fizetésről

- A kártyabirtokosok számára az internetes fizetés, csakúgy, mint a hagyományos POS terminálon történő fizetés díjmentes.
- Ma már a Maestro bankkártyával is lehet fizetni az interneten. Érdeklődjön kibocsátó bankjánál!
- A kártyatársaságok a kártyabirtokosok érdekeit védik, ezért amennyiben kártyával vásárol és a kereskedő nem teljesít, úgy a kibocsátó bankjánál megadott reklamáció keretében érvényesítheti panaszát, melynek jogossága esetén Ön visszakapja a pénzt.
- A kártyabirtokos azonosítását szolgálja a kártya aláírási paneljében található 3 jegyű ellenőrző kód - amit CVC2-nek vagy CVV2-nek is szoktak nevezni - (a 3 jegyű ellenőrző kód megtalálható a kártyaszám, illetve annak utolsó négy számjegye után). Ezt a kódot kérjük, ugyanolyan gondossággal kezelje, mint a PIN-kódot!



Biztonsági jótanácsok

- Növeli a biztonságot, ha SMS-szolgáltatást igényel bankjától, melynek eredményeképpen a számlán történt változásokról azonnal értesítést kap.
- Kérjük, készpénzfelvételnél, ill. vásárlásnál használt négyjegyű PIN kódját soha ne adja meg internetes fizetés esetén, illetve ügyeljen arra, hogy a kártyaszámát és a kártya lejárat dátumát ne adja ki illetékteleneknek!
- A vásárlást, fizetést követően mindig jelentkezzen ki a weboldalról! Különösen fontos ez olyan számítógép esetén, amit más is használ! Az adatai védelme érdekében javasoljuk, hogy saját gépről vásároljon, kerülje a nyilvános internetes kávézókat, hotspotokat!
- Kérjük, e-mailben történő adategyeztetéskor fokozottan figyeljen, ugyanis Nyugat-Európában és az Egyesült Államokban egyre gyakoribb, hogy illetéktelenek e-mailben próbálnak meg adatokat kicsalni.
- Amennyiben adatai frissítését kéri Öntől - akár olyan kereskedők is, ahol korábban már vásárolt - legyen elővigyázatos, hiszen akár a kereskedő nevében is eljárhatnak illetéktelenek. Ilyen esetekben kérjük, vegye fel a kapcsolatot a kereskedővel az addig megszokott módon, hogy ellenőrizze a feladót.
- További gyanúra adhat az is okot, ha túl kedvező ajánlattal, nyereményjátékkal vagy soha meg nem rendelt termék lemondásával kapcsolatban kap levelet.
- A kártyatársaságok sem e-mailben, sem telefonon nem keresik meg közvetlenül a kártyabirtokosokat! Amennyiben kártyatársaságok nevében olyan e-mailt vagy telefonhívást kap, melyben arról tájékoztatják, hogy bankkártyájának adatait illetéktelenek szerezték meg kérjük, ne adja meg az adatait, illetve haladéktalanul értesítse a kártyakibocsátót!



Vásárlás az interneten

- A webes vásárlás egyik előnye, hogy könnyedén összehasonlíthatja a hasonló termékek árait, így egyszerűen és gyorsan választhatja ki az Önnek legkedvezőbb ajánlatot.
- Megrendelés előtt - különösen az első megrendelés alkalmával - kérjük, ellenőrizze a a webáruházzal kapcsolatos információkat (mióta működik, mennyire tartják megbízhatónak a céget, a jogszabályok alapján kötelezően előírt általános elérhetőségek szerepelnek -e a honlapon pl. cím, telefonszám).
- Az internetes cégek annak érdekében, hogy védjék vásárlóikat számos biztonsági funkciót építenek be webáruházaikba. A honlapon szereplő nagy kártyacégek biztonsági logói (pl. MasterCard SecureCode) vagy egyéb titkosítások pl. SSL-kódok mindegyike arra utal, hogy az internetes kereskedő megtette a szükséges lépéseket a biztonságos netes vásárlás érdekében.
- A kommunikáció titkosítását mutatja az URL címbe a "https" és az oldal jobb alsó sarkában szereplő lakat is vagy a bal alsó sarkában szereplő kulcs, melyekre kattintva megjelennek a biztonsági tanúsítványok.
- Minden vásárlás alkalmával mentse el vagy nyomtassa ki megrendelését, annak fizetési visszaigazolását, a fizetéskor megadott adatokat, a megrendelt áru termékismertetőjét.
- A webáruház szerződési feltételeit ajánlott elolvasni megrendeléskor, hiszen amennyiben minőségi problémák merülnének fel a megrendelt termék/szolgáltatás esetén hasznos, ha tudja, mennyi időn belül nyújthat be reklamációt, milyen feltételek mellett vonhatja vissza megrendelését, illetve mikor és hogyan kaphatja vissza a pénzét.



A PayU online fizetési rendszerének banki háttérét az OTP Bank Nyrt. biztosítja.