

Készüljünk együtt

BIZTONSÁGOSAN

az ünnepekre!



NEMZETI
KIBERBIZTONSÁGI
INTÉZET



NEMZETI
KIBERBIZTONSÁGI
INTÉZET



Az ünnepi szezon talán mindenki számára egy stresszes időszak, hiszen számos elintéznivaló akad ilyenkor.

Ezt a nagy kapkodást a csalók is igyekeznek minden évben kihasználni, ezért az ünnepeket megelőző időszakban jellemzően megugrik a kibercsalások száma.

Kis odafigyeléssel és kellő gyanakvással azonban megvédhetjük magunkat az online átverésektől, amihez a soron következő játékokkal és IT biztonsági tanácsokkal igyekszünk segítséget nyújtani.





Találd meg a képen elrejtett
10 db NKI jelet (🍷)!



Néha elég hasonló alapossággal átvizsgálni egy-egy webáruházat vagy ajánlatot, hogy észrevegyük a gyanús jeleket. Az alábbiakat mindenképpen érdemes ellenőrizni mielőtt leadnánk rendelésünket és személyes adatokat osztanánk meg magunkról.

- **Ismerjük meg más felhasználók személyes tapasztalatait, véleményét!** Kis keresgéléssel biztosan találunk felhasználói véleményeket, amelyekből kiderülhet, hogy mennyire megbízható egy adott áruház vagy termék.
 - **Olvassuk el a vásárlási feltételeket!** Különösen fontos a termék visszaküldésére és visszafizetésére vonatkozó részek megismerése.
 - **Utánvétes fizetés előnyben!** Bár sok webáruháznál számolnak fel rá plusz költséget, mivel kevesebb anyagi kockázattal jár, így is érdemes ezt a fizetési módot választani, különösen, ha a tanácsok ellenére, mégis egy számunkra ismeretlen webáruházból rendelünk.
- 



Igaz vagy hamis?

Döntsd el, hogy az alábbi hirdetések közül melyik valódi és melyik átverés!



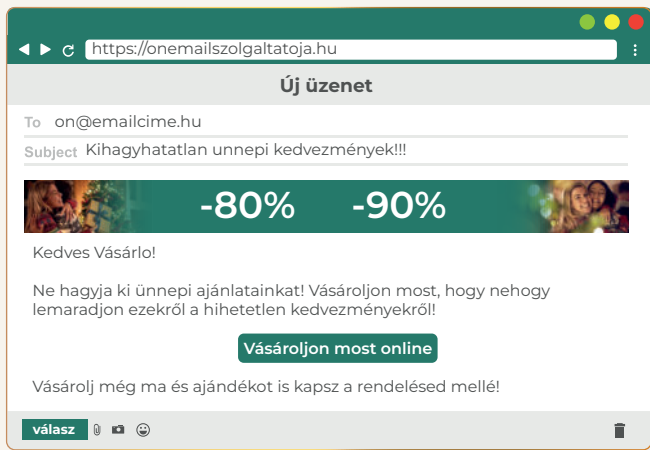
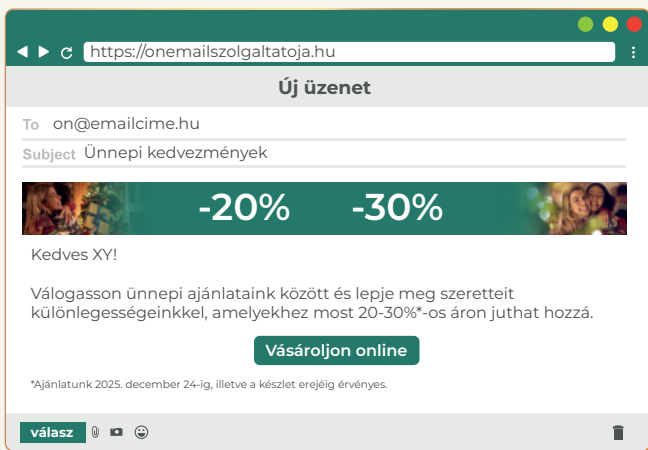


A csalókon kívül az ünnepi szezon az online kereskedők számára is egy kiemelt időszak, hiszen sok cég kedveskedik ilyenkor különböző akciókkal a vásárlóknak. Az egyre kifinomultabb támadási módszerek mellett egyre nehezebb megállapítani, hogy egy adott hirdetés valódi-e vagy sem, ezért érdemes figyelembe venni az alábbiakat:

- **Ha túl szép ajánlattal kecsegtetnek minket, akkor az nagy valószínűséggel átverés.** Érdemes egy kis piackutatást végezni a már jól ismert, megbízható webáruházaknál is egy-egy adott termék esetén, mert a 80-90%-os árengedmény bizony gyanúra adhat okot.
 - **Mindig ellenőrizzük az URL címeket,** kimondottan az ismeretlen feladóktól kapott linkeket! A támadók gyakran használnak az eredetihez hasonló domaineket, mint például yOoutube.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.
 - **Ne kattintsunk a hirdetésekre!** Helyette látogassunk el magára a webshopra és keressük meg az adott terméket!
 - **Legyünk gyanakvóak a kihagyhatatlan, sürgető ajánlatokkal!** A csalók gyakran hajszolják gyors, átgondolatlan lépésekre a felhasználókat ilyen módszerekkel.
- 

Mi a különbség?

Találd meg a két kép közötti különbségeket (5 db), és derítsd ki, hogy melyik ajánlat az átverés!



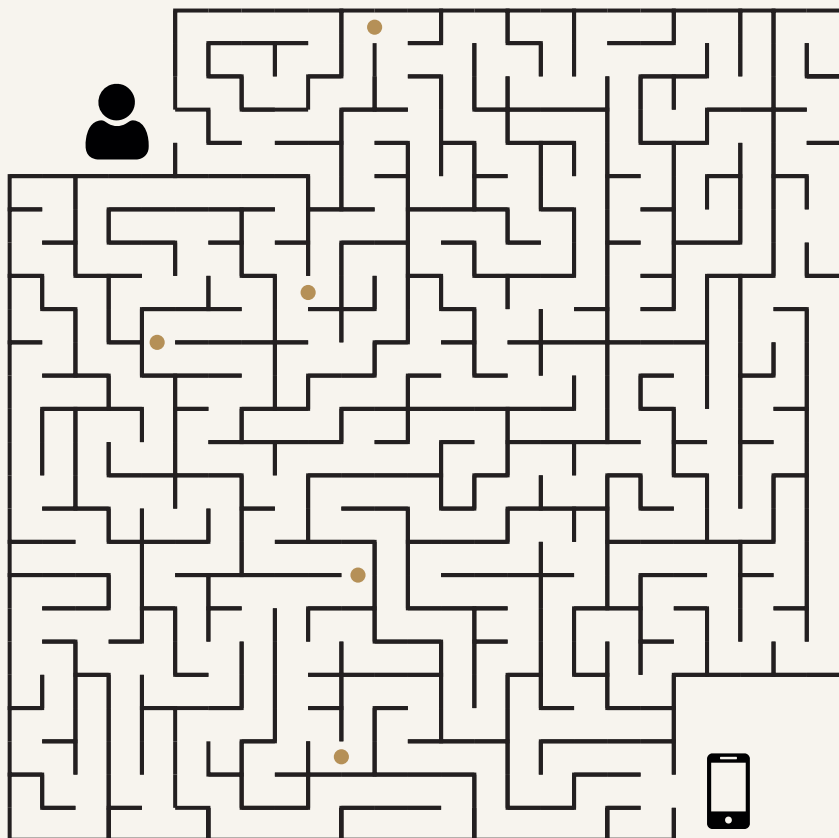


Sajnos évről-évre egyre nehezebb az üzenetekben érkező, hivatalosnak tűnő átverések felismerése, ezért általános tanácsként elmondható, hogy **mindig kellő gyanakvással kezeljük** az ilyen formában érkező ajánlatokat.

- **Olvassuk át többször az e-mailt**, hátha találunk valami nem szokványosat az üzenetben (helyesírási hibát, megszólítás, tegeződés és magázódás váltakozása, stb)!
- Ne feledjük, a **túlzó kedvezmények gyanúra adhatnak okot!**
- **Sose kattintsunk az üzenetekben küldött hivatkozásokra**, helyette inkább **keressük fel a cég hivatalos weboldalát** és győződjünk meg ott, hogy valóban érhetők-e el kedvezmények!
- Bár a szezonális ajánlatok végesek, **ne engedjünk a sürgető, azonnali cselekvésre buzdító felszólításoknak!**



Okoseszközt adnál ajándékba?



A megállópontok segítségével juss el
a biztonságos eszközhasználatig!

Mint minden internethez csatlakoztatható eszköz esetén, okoseszközöknél és digitális játékoknál is érdemes figyelmet fordítani a biztonsági és adatvédelmi kockázatokra.

- Fontos, hogy tisztában legyünk azzal, hogy a termékek funkcionalitásukból adódóan **milyen adatokat rögzítenek**, például készítenek-e hangfelvételeket, vagy végeznek-e arcfelismerést.
- Minden esetben **olvassuk el az adatvédelmi irányelveket!** Különösen javasolt az adatok gyűjtésére (mit, miért), kezelésére (kinek adják tovább) és tárolására (titkosítják-e) vonatkozó részek alapos megismerése.
- Ellenőrizzük, hogy **a játék által gyűjtött adatok mentése belső, vagy külső tárhelyen történik!** Belső tárolás esetén nem kell aggódni a külső szerverek biztonsága miatt, viszont mindkét esetben fontos, hogy az adatok titkosítva kerüljenek mentésre.
- Lehetőség szerint olyan terméket válasszunk, ami **minél hosszabb gyártói támogatással rendelkezik** és állítsuk be az **automatikus frissítést!**
- Egyes okoseszközök használata felhasználói fiókhoz kötött. Ilyen esetekben ügyeljünk arra, hogy **a fiókhoz társított jelszó kellő mértékben összetett és hosszú legyen!** A regisztráció során mérlegeljük, hogy valóban szükséges-e a valódi adatok, beleértve a teljes név, születési dátum stb. megadása, amennyiben nem, javasolt inkább alias, vagy becenév használata.

*Kellemes
Karácsonyi ünnepeket
kívánunk!*



NEMZETI
KIBERBIZTONSÁGI
INTÉZET