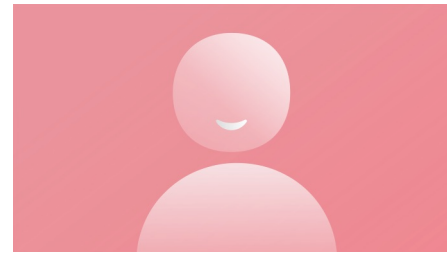


CSALÁDI KIBERBIZTONSÁG

Gyermekeink védelme az online világban



AZ ONLINE TÉR ELTERJEDÉSE

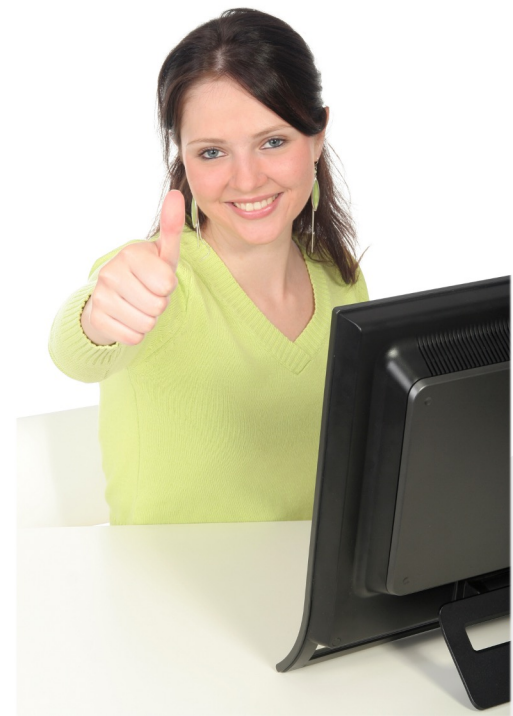
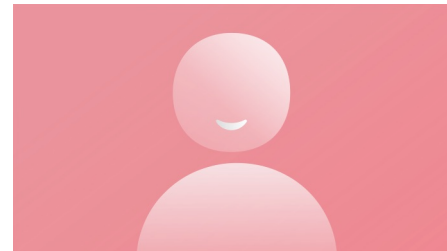


- Az online tér térnyerése
- A digitális átalakulás hatása
- Közösségi kapcsolatok és kommunikáció
- Információhoz való hozzáférés
- Munkavégzés és tanulás
- Szórakozás és szabadidős tevékenységek
- Gazdasági- és üzleti lehetőségek



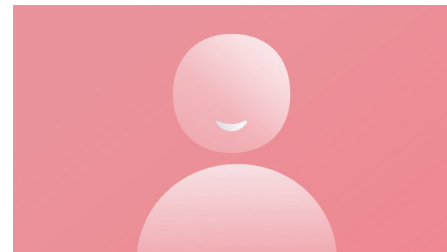
AZ INTERNET **POZITÍV** HATÁSAI

- Oktatás
 - oktatási forráshoz és eszközhöz > segítik a tanulást és a tudás bővítését
 - online oktatási platformok, weboldalak és videók > otthontanulás
 - távoktatást és a virtuális osztálytermek
- Kommunikáció
 - kommunikáció világszerte
 - videóhívás
 - üzenetküldés
 - közösségi média platformok
- Információhoz való hozzáférés
 - újságok
 - cikkek
 - kutatási eredmények
 - enciklopédiák
- Kreatív kibontakozás > azonnali visszajelzés
 - digitális művészet
 - videóképzítés
 - zenealkotás
 - blog

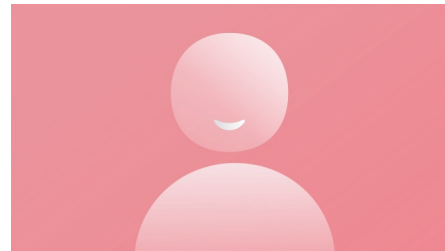


AZ INTERNET **NEGATÍV** HATÁSAI

- online kommunikáció szerepe a mindennapi életünkben
- Cyberbullying és online zaklatás
 - gyűlöletbeszéd
 - személyes támadások
 - fenyegetések
- Személyes adatok és adatvédelem
 - a személyes információk védelme
 - adathalászat (phising)
 - identitással való visszaélés
- Megkárosító tartalmak és online bűnözés
 - például erőszakos vagy pornográf tartalmak
 - online csalás
 - drog- vagy alkoholértékesítés
- Képernyőfüggőség és online jelenlét
 - az idő és az energia túlzott mértékű eltöltése az online térben
 - a valóság és a virtuális világ elmosódása



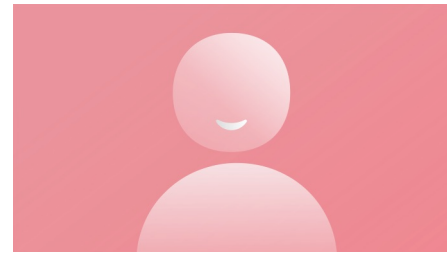
ONLINE PLATFORMOK



1. Szórakozás és játék:
 - Videójátékok: Fortnite, Minecraft, Roblox, Among Us
 - Streaming platformok: YouTube, Netflix, Twitch
2. Szociális média:
 - Közösségi média: Facebook, Instagram, Snapchat, TikTok
 - Üzenetküldő alkalmazások: WhatsApp, Messenger, Viber
3. Online tanulás és oktatás:
 - Online kurzusok és oktatási platformok: Coursera, Udemy, Khan Academy
 - Digitális taneszközök: Google Classroom, Microsoft Teams
4. Kommunikáció és üzenetküldés:
 - Chataalkalmazások: WhatsApp, Telegram, Signal
 - Videohívások: Zoom, Microsoft Teams, Skype
5. Kreatív tevékenységek:
 - Kreatív alkalmazások: Adobe Creative Cloud, Procreate, Canva
 - Videószerkesztők: iMovie, Adobe Premiere Pro, Final Cut Pro

VESZÉLYEK AZ ONLINE TÉRBEN

- ismeretlen emberekkel való „találkozás”
- kiberzaklatás
- szexuális kizsákmányolás
- lelki bántalmazást
- tartalomhozzáférés és tartalomkockázatok
 - bántó
 - erőszakos
 - erőszakos-, vagy szexuális tartalmak
 - gyűlöletbeszéd
- adatvédelmi kockázatok
- csábítás a veszélyes viselkedésekre
 - kábítószer
 - alkohol
 - erőszak
- pszichológiai manipuláció
- alkalmazás-hozzáférése



Nem tudtuk kézbesíteni a csomagját, az ujrakezbesítéshez látogasson el erre a linkre:

<https://deilverminute.com/r/twFprDI>

Szokatlan tevékenységet észleltünk fiókjában. Az oldalad korlátozott, ami azt jelenti, hogy a fiókod által kezelt oldal sérti a közösségi szabványait. Az Ön védelme érdekében oldaladat nem mindenki láthatja a , és nem használható a fiókod által kezelt oldalt.

Az alábbi linke kattintva igazolnunk kell személyazonosságát:

• <http://tinyurl.com/9981632626>

Közösségi alapelveink segítenek megőrizni a biztonságát.

Ne feledje, hogy 24 órája van ezen lépések végrehajtására, hogy megakadályozza fiókja végleges letiltását.

Üdvözléssel.

Security Group.

Vegyen részt a felmérésben és nyerjen 100 000 Ft-ot

Csak felnőtt ügyfelek számára

→ [Kattintson a felmérés linkjére](#)

szekciószerkesztés
új internet- és mobilbank
Részlettel és ismerd meg új digitális szolgáltatásainkat

További információ

Tisztelt Ügyfelünk,

A tájékoztatta, hogy az Ön szállítása: 9795744946, és díjfizetésre vár

Díjak: 805,28 HUF

Dátum : 16/01/2023.

Küldd el a csomagomat

A megadott címre nem tudtuk kiszállítani a csomagot. Kerjen második kiserletet a következő link segítségével <https://expresscardparcel.com/r/lpli1UM>

[]
Utolsó figyelmeztetés a fiókjának korlátozása előtt, kérjük, erősítse meg adatait 24 órán belül : <http://korlatozas-.x.com>



+48

On fizetni próbált 50,000HUF értékben, ha mégsem on volt kattintson ide: <https://hu-.com/login>

CSOMAG VÁRAKOZIK

Csomag száma:
#HUN984652POSTA

Utolsó alkalommal emlékeztettük a kifizetésre váró szállítási költség kapcsán.

Ha az összeg nincs kifizetve 48 órán belül, a függőben lévő kézbesítés törölve lesz.

Csomag adatai Állapot:

Állapot: A csomag a 2-es Terminálön várakozik

Csomag:

Kézbesítési idő: (2) munkanapon belül

Követ

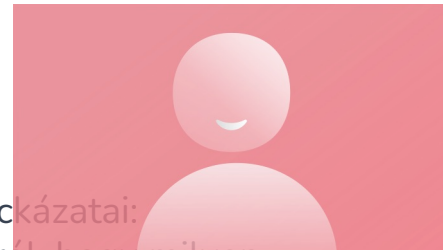
Te vagy a videóban? 🤖



<http://tiktok.r317j.cloud/ZTV5Ebc>

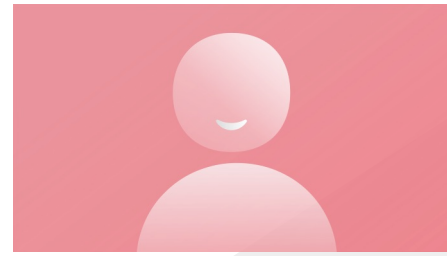
Kuldemenykerület 2/2
- 36203305754 - az On
#IPS208497103HU
csomagja, vissza lesz
kuldve 14-10-2022,
ha nem erosi meg:
efuvul.link/4DVAsbZ

GYERMEKVÉDELEM



- Az online privát szféra fontossága és a személyes adatok megosztásának kockázatai:
 - Tájékoztassák a gyerekeket az online privát szféra fontosságáról, és arról, hogy milyen személyes információkat nem szabad megosztaniuk ismeretlenekkel.
 - Ismertessük meg velük, hogy az online térben megosztott információk, fotók vagy videók visszafordíthatatlanul elterjedhetnek, és bántó vagy kártékony célra felhasználhatók.
- Szülői felügyeleti szoftverek használata és korlátozások beállítása:
 - Telepítsenek és használjanak olyan szülői felügyeleti alkalmazásokat, amelyek lehetővé teszik a gyerekek online tevékenységeinek monitorozását és korlátozását.
 - Állítsanak be időkorlátokat, hogy korlátozzák az online tartózkodást, és blokkolják a veszélyes vagy inaktív webhelyeket és alkalmazásokat.
- A szülői bizalom és kommunikáció szerepe az online tevékenységekben:
 - Biztosítsák a gyermekeket arról, hogy mindig számíthatnak rájuk, ha problémába ütköznek az online térben.
 - Tartsanak nyitott kommunikációt a gyerekekkel, és beszéljenek velük az online kockázatokról és azok megelőzéséről.
 - Tanítsák meg nekik, hogy jelentsék a gyanús vagy zaklató viselkedést, és segítsenek nekik megérteni, hogy az ő biztonságuk az elsődleges szempont.
- Mutassunk példát!

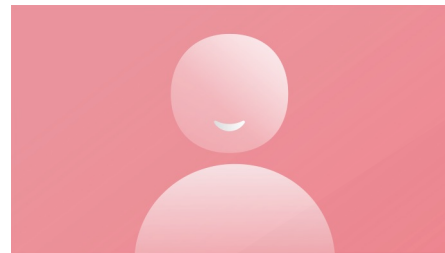
BIZTONSÁGTUDATOS POSZTOLÁS



- NE posztoljon
 - személyes információkat
 - pénzügyi információkat
 - helyszíni információkat
 - magánéleti információkat
 - értékek védelme
 - kellemetlen következményekkel járó képek
 - családunk védelme
 - szenzitív információkat (munkahelyi, vagy magán)
 - provokatív, vagy sértő tartalmakat
 - jogvédett tartalmakat
 - átverésre utaló tartalmakat
 - visszaélésre felhasználható tartalmakat



BIZTONSÁGOS JELSZÓ HASZNÁLATA



védelem hackerek ellen

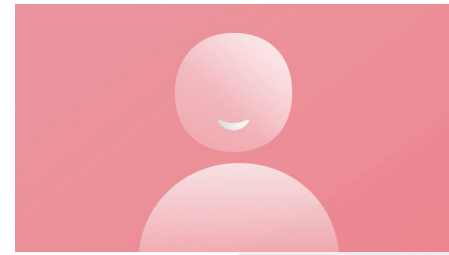
- Használjon hosszú jelszavakat: legalább 11 karakter
 - kisbetű
 - nagybetű,
 - szám
 - speciális karakter
- Egyedi jelszavak használata
- Kerülje a könnyen kitalálható információkat
- Változtassa időről időre a jelszavát
- Használjon jelszókezelő alkalmazást
- Kétlépcsős azonosítás bekapcsolása
- Vigyázzon a adathalász támadásokkal

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD

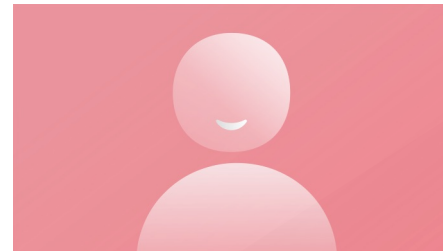
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

KÉTFAKTOROS AZONOSÍTÁS

- biztonsági eljárás
- faktorok:
 - tudás
 - birtoklás
 - lehet dinamikusan generált
 - mobilalkalmazás
 - hardveres eszköz
 - kártya
 - OTP token
 - SMS üzenet
 - jelszókezelő alkalmazás
 - tulajdonság



JELSZÓKEZELŐ ALKALMAZÁSOK

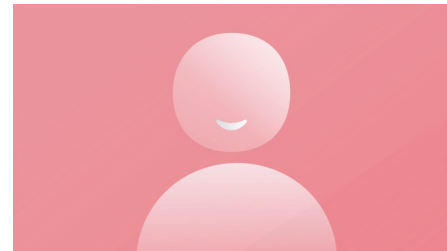


- biztonságos jelszókezelés
- egyszerű és erős jelszó generálás
- egyszerű bejelentkezés
- többeszköz támogatás
- jelszókategóriák és címkék
- megosztási funkciók



MAXIMUM EGY JELSZÓT KELL MEGJEGYEZNI!

BIZTONSÁGOS E-MAIL CÍMEK HASZNÁLATA

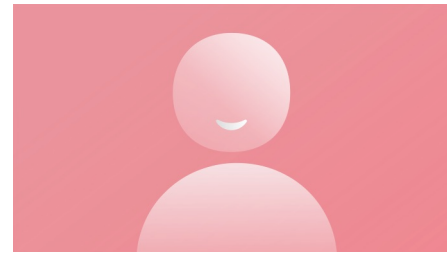


- NE használjunk céges e-mail címet a fiókunk használatához
- Az e-mail címhez használjon biztonságos jelszót
- Használjon kétfaktoros autentikációt hozzá
- Profiloknál használjon „egyedi” e-mail címet
 - pl.: demo.tamas@gmail.com
 - ugyanaz:
 - demotamas@gmail.com
 - d.emotamas@gmail.com
 - d.e.m.o.t.amas@gmail.com
 - ugyanoda beérkezik:
 - demotamas+facebook@gmail.com
 - dem.otamas+blabla@gmail.com
- Titkosított levelezés
 - PGP-zet levél a szolgáltatótól
 - facebook: <https://www.facebook.com/me/about?section=contact-info>

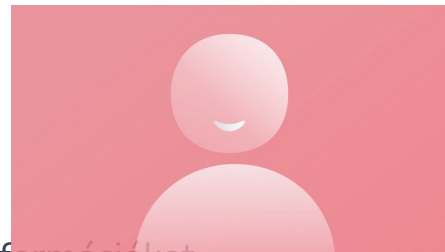


SZÜLŐI FELÜGYELETI SZOFTVEREK

- Mobilra:
 - Bark - Gyermekfelügyelet, figyelmeztetés
 - Qustodio - Tartalom szűrés, időkorlátozás
 - Norton Family - Online monitoring, tartalom szűrés
 - Net Nanny - Tartalom szűrés, időkorlátozás
 - FamilyTime - Tartalom szűrés, GPS helymeghatározás
 - Kaspersky SafeKids - Tartalom szűrés, alkalmazáskorlátozás
 - Screen Time - Időkorlátozás, alkalmazáskorlátozás
 - Kidslox - Időkorlátozás, alkalmazáskorlátozás
- Laptopra:
 - Norton Family Premier - Tartalom szűrés, időkorlátozás
 - Kaspersky Safe Kids - Tartalom szűrés, alkalmazáskorlátozás
 - Net Nanny - Tartalom szűrés, időkorlátozás
 - Qustodio - Tartalom szűrés, időkorlátozás
 - FamilyTime - Tartalom szűrés, időkorlátozás
 - McAfee Safe Family - Tartalom szűrés, időkorlátozás
 - Windows Live Family Safety - Tartalom szűrés, időkorlátozás
 - OpenDNS FamilyShield - Tartalom szűrés, webhely blokkolás
 - ESET Parental Control - Tartalom szűrés, alkalmazáskorlátozás



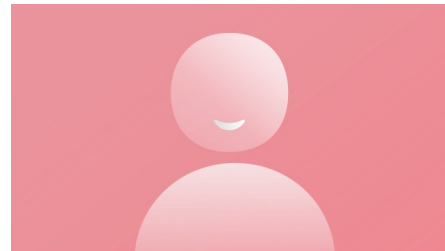
BIZTONSÁGOS BANKOLÁS



1. Ne ossza meg a banki információkat senkivel:
 - Ne adjon ki bankszámlaszámot, PIN-kódot vagy más személyes banki információkat ismeretleneknek.
 - Ne válaszoljon kéréstlen e-mailekre vagy telefonhívásokra, amelyek banki információkat kérnek.
2. Használjon erős jelszavakat
3. Használjon kétfaktoros azonosítás
4. Ellenőrizze az online banki fiókot rendszeresen:
 - Győződjön meg róla, hogy rendszeresen ellenőrzi bankszámláját és tranzakcióit.
 - Észreveheti az esetleges gyanús tevékenységeket vagy nem ismert tranzakciókat.
5. Ne hagyja felügyelet nélkül a bankkártyát:
 - Mindig vigyázzon a bankkártyájára és ne hagyja felügyelet nélkül.
 - Tartsa távol a kártyáját a személyes adataitól.



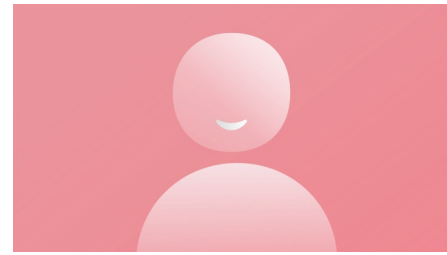
EGYÉB TANÁCSOK



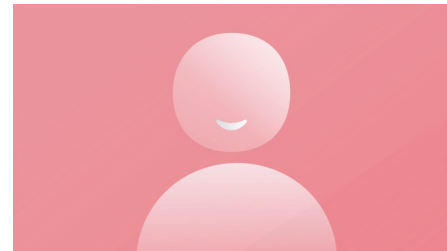
- Szoftverek és operációs rendszerek frissítése:
 - Frissítse rendszeresen a szoftvereket, alkalmazásokat és az operációs rendszert
 - Engedélyezze az automatikus frissítéseket
- Gyanús e-mailek és üzenetek felismerése, valamint spam szűrés
 - Gyanús vagy ismeretlen küldőtől érkező e-mailek és üzenetek
 - Ne kattintson gyanús linkekre vagy nyitott mellékletekre, és ne osszon meg személyes adatokat váratlan vagy kétséges kérések esetén.
 - Használjon spam szűrőt vagy megbízható e-mail szolgáltatót
- Biztonságos online vásárlás és banki tranzakciók
 - Vásárlás vagy banki tranzakciók esetén használjon biztonságos, titkosított kapcsolatot (<https://>).
 - Győződjön meg arról, hogy a webhely, ahol vásárolsz vagy banki tranzakciót végzel, hiteles és megbízható.
 - Ne osszon meg banki vagy személyes adatokat nyilvános vagy bizonytalan hálózatokon.
- Kerülje a nem biztonságos vezeték nélküli hálózatokat

JELEK

- Hangulatváltozások
- Titkolózás és zárt kommunikáció
- Alvászavarok és csökkenő iskolai teljesítmény
- Megváltozott viselkedés az offline világban
- Gyorsan reagáló és eltitkolt eszközhasználat



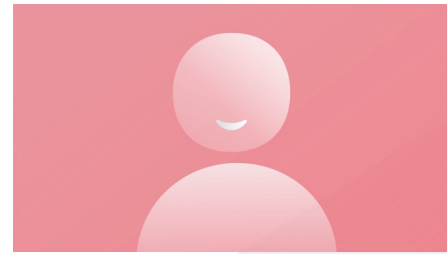
GYANÚS TEVÉKENYSÉGEK JELENTÉSE



1. Lépjen be a fiókjába a közösségi oldalon.
2. Keressék meg az adott felhasználót vagy a gyanús tartalmat, amelyről jelentést szeretnének tenni.
3. Kattints az adott felhasználó nevére vagy a tartalomra, hogy megnyisd a részleteket.
4. Keresse meg a jelentés vagy a panasz opciót. Ez általában egy hárompontos menü vagy egy jelentés ikon lehet. Az elnevezés változhat a különböző közösségi oldalakon.
5. Válassza ki a megfelelő jelentési opciót a felugró menüből. Gyakori opciók közé tartozhatnak a következők: "Jelentés visszaélést", "Jelentés zaklatást", "Jelentés spam tartalmat", "Jelentés hamis profil", "Jelentés kéretlen üzeneteket" stb.
6. Kövesse a további utasításokat, és töltsse ki a szükséges információkat a jelentés elküldéséhez. A közösségi oldalak gyakran kérnek részletes magyarázatot vagy bizonyítékokat a jelentéssel kapcsolatban.
7. Ha lehetséges, mellékeljen képernyőképeket vagy más bizonyítékokat a gyanús tevékenységről, hogy segítsen a közösségi oldalnak a vizsgálatban.

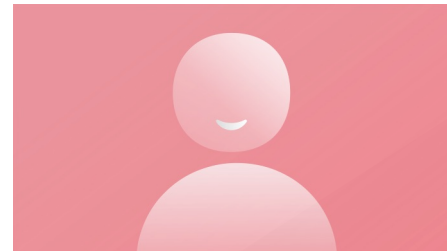
FIÓK VISSZASZERZÉSE

- Jelszó visszaállítása: "Elfelejtetted a jelszavad?"
- Ellenőrizze a fiók biztonsági beállításait
- Ismerősök általi jelentés
- Kapcsolatba lépés a Facebook támogatásával
 - support@fb.com
 - disabled@fb.com
- Azonosítási folyamat elvégzése



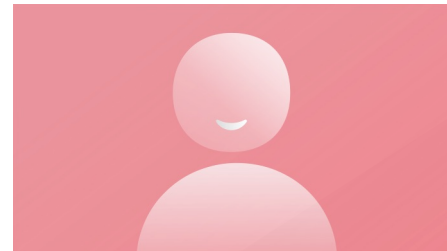
ONLINE ZAKLATÁS ELLENI FELLÉPÉS

- Ne reagáljon az online zaklatásra.
- Mentse el és gyűjtse a bizonyítékokat.
- Blokkolja és jelentse az incidenset.
- Tájékoztassa a közösségi oldal üzemeltetőjét.
- Kérjen segítséget: Ne féljen segítséget kérni.
- Védje meg a személyes adatait.



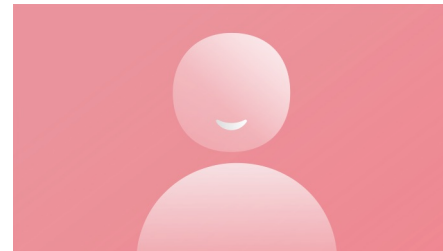
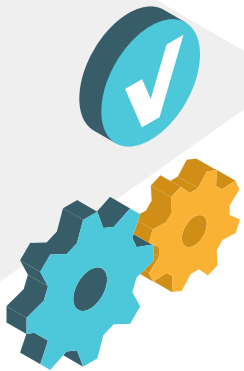
PÉNZÜGYI VISSZAÉLÉSEK

- Jelezzük bankunknak
- Változtassunk jelszavakat
- Jelzés a hatóságok részére



The image features the Kahoot! logo in a bold, purple, sans-serif font. The text is centered horizontally and is the primary focus of the image. The background is white, with two light gray triangular shapes in the corners: one in the top-left and one in the bottom-right, pointing towards the center. The exclamation mark at the end of the word is stylized with a small diamond shape at its base.

Kahoot!



KÉRDÉS?





KÖSZÖNÖM A FIGYELEMET!

