2020-1-DE02-KA227-ADU-008321

Co-funded by the
Erasmus+ Programme
of the European Union

Kézikönyv az IKT eszközök használatához

A "DIGITALIZE - eszközök roma felnőttek számára az internet használatához és az oktatás elősegítéséhez" projekt partnerei által készült

Partner szervezetek:

Amaro Foro e.V.

EGYÜTT HATÓ
KÖZÖSSÉGÉPÍTŐ EGYESÜLET

NEVO PARUDIMOS

ROMA

- Kézikönyvem az IKT eszközök használatához -

Projekt "Digitalizálj - eszközök roma felnőttek számára az internet használatához és az oktatás elősegítéséhez "

Ez a dokumentum az Amaro Foro e.V., az Együttható Egyesület, a Nevo Parudimos és a RROMA által megvalósított „Digitalizálj – eszközök roma felnőttek számára az internet használatához és az oktatás elősegítéséhez" projekt keretében készült. A projektet az Európai Unió Erasmus+ programja támogatja. Projektszám: 2020-1-DE02-KA227-ADU-008321. Az Európai Bizottságnak a kiadvány elkészítéséhez nyújtott támogatása nem jelenti a szerzők véleményét tükröző tartalmát, és a Bizottság nem tehető felelőssé az abban foglalt információk bármilyen felhasználásáért.

Szerző: YOZKAN, Pelin - Együttható Egyesület

Co-funded by the Erasmus+ Programme of the European Union

- Tartalomjegyzék -

Íme 10 tippünk ahhoz, hogy biztonságban maradhass a közösségi médiában

1. Tipp Legyen erős jelszavad!

Készíts egyedi jelszót!

Használj különböző jelszavakat minden online fiókodhoz! A jelszavak újrafelhasználása kockázatos!

Facebook Instagram Tiktok Bank account

Ha valaki megszerzi a jelszavadat, hozzáférhet az e-mail címedhez, a címedhez, és még a pénzedhez is

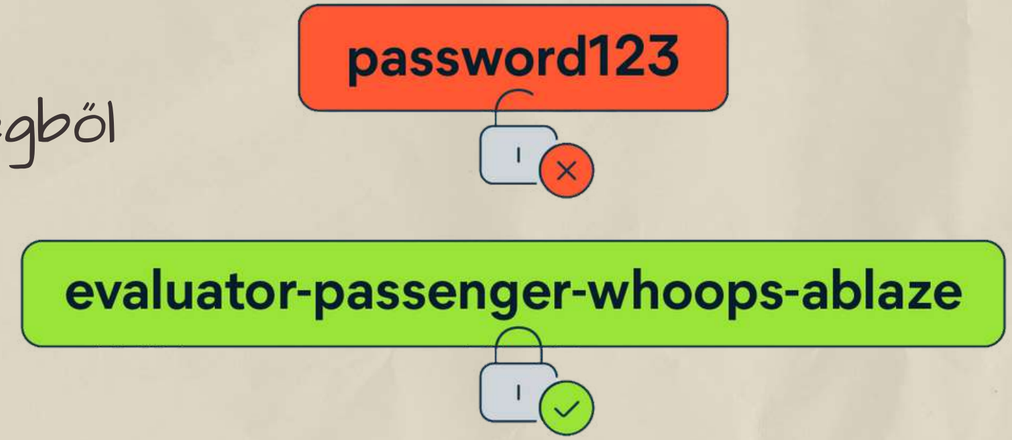
1. Tipp Legyen erős jelszavad!

Legyen hosszú és megjegyezhető jelszavad!

A hosszabb jelszavak erősebbek, legyen a tiéd is legalább 12 karakter hosszú.

Próbáld ki ezeket:

- szövegrészlet egy dalból vagy versből
- számodra fontos idézet egy filmből vagy szövegből
- jelszó olyan szavakból, amik fontosak neked
- rövidítés: jelszó, amit egy mondat minden szavának első betűjéből készítesz.



1. Tipp

Legyen erős jelszavad!

Kerüld a személyes adatokat és a túl gyakori szavakat!

Ne használj személyes adatokat!

Ne készíts jelszót olyan információkból, amiket mások is tudhatnak, vagy könnyen megtudhatnak rólad (például a közösségimédia-profilodból), úgymint:

- a beceneved, nevednek kezdőbetűi
- gyermeked, házikedvenced neve
- fontos születésnapok, évszámok
- az utcád neve
- a lakcímed számjegyei.

1. Tipp Legyen erős jelszavad!

Ne használj gyakori, egyszerű szavakat, kifejezéseket, sablonokat, amiket könnyű kitalálni!

Kerüld például:

- a nyilvánvaló szavakat és szóösszetételeket, mint a "jelszó" vagy az "énnevem"
- az olyan sorozatokat, mint az "abcd" vagy "1234"
- sorokat a billentyűzetről, mint "qwertz" vagy "asdf"

1. Tipp

Legyen erős jelszavad!

Tartsd titokban a jelszavadat!

Ha létrehoztál egy erős jelszót, a biztonság kedvéért a következő lépéseket tedd még meg:

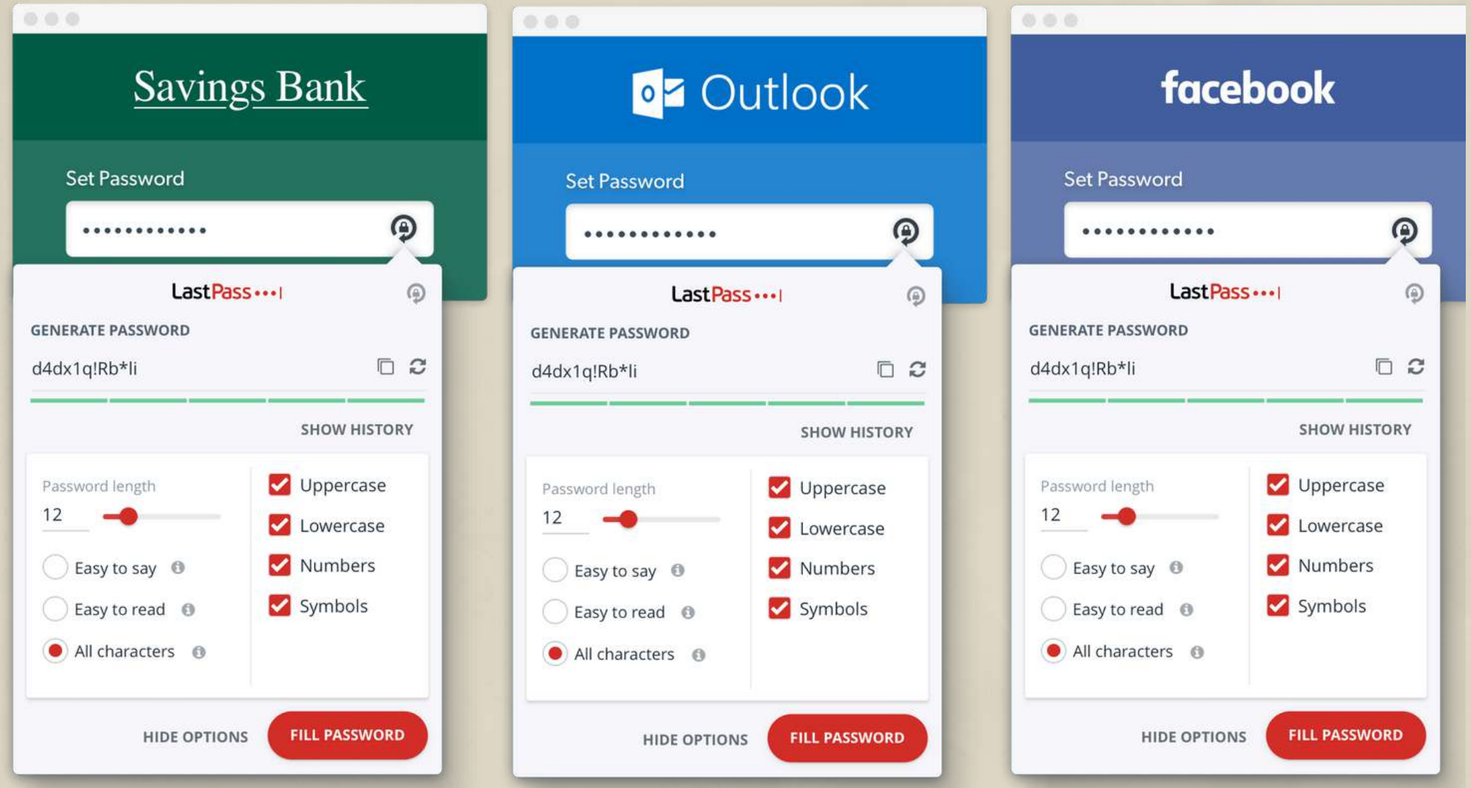
1. lépés: Rejtsd el a leírt jelszót!

Ha le kell írnod a jelszót, hogy meg tudd jegyezni, ne hagyd a számítógépen vagy az asztalon. Győződj meg arról, hogy a leírt jelszavak titkos vagy elzárt helyen vannak.

.

1. Tipp Legyen erős jelszavad!

2. Lépés: Válassz erre való eszközt a jelszavak kezeléséhez!



A jelszavak biztonságos tárolásának és megjegyezésének egyik módja egy olyan eszköz használata, amely titkosított formában tárolja a felhasználónevek és jelszavak listáját. Ezen eszközök némelyike még azzal is segít, hogy bizonyos webhelyeken automatikusan kitölti az információkat. (Példa: LastPass.)

2. Tipp Védd jelszóval a készülékedet!

A jelszó beállítása segít távol tartani az illetéktelen felhasználókat a mobileszköztől, és akkor is segíthet, ha azt elveszíted vagy ellopják. A jelszót mindig kérni fogja a készülék, amint bekapcsolod vagy aktivizálod. Okoseszközöd „Biztonság" menüjében számos zártípus közül választhatsz:

Arcfelismerés - az arcod megmutatásával erősíted meg a személyazonosságodat. Az eszköz egyetlen személyt tud csak azonosítani kizárólagos tulajdonosaként, míg mások hozzáférését korlátozza.

Ujjlenyomat-felismerés - az arcfelismeréshez hasonló, de másik formája a biometrikus azonosításnak..

PIN-kód - 4 számjegyű (egyes eszközökön 6 számjegyű) kódot adhatsz meg az eszköz zárolásának feloldásához.

Képernyőzár-minta - egy rácsra mintát rajzolhatsz, amivel feloldhatod a zárolt eszközt.

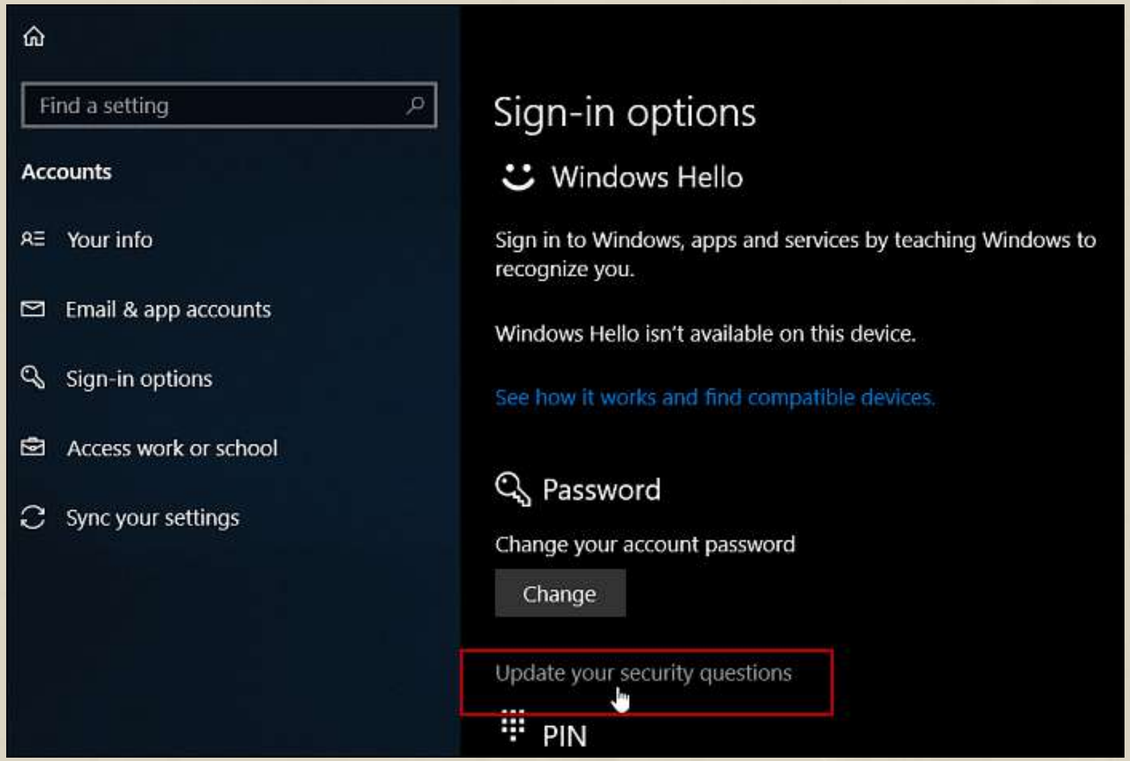
3. Tipp frissítsd rendszeresen az eszközeidet!

A számítógép-fejlesztők rendszeresen frissítéseket adnak ki a termékek biztonságának megőrzése érdekében. Tartsd naprakészen az eszköz szoftverét, hogy megvédd a rosszindulatú programoktól.

Ezenkívül víruskereső szofter telepítésével is védd számítógépedet.

4. Tipp

Állíts be biztonsági kérdéseket és válaszokat!



A biztonsági kérdések a felhasználói fiók biztonságban tartására valók. Ha elfelejtetted a jelszavadat, és ezért nem tudsz hozzáférni a fiókodhoz, ezek megválaszolásával tudod azonosítani magad. A legtöbb közösségi oldalon beállíthatsz ilyet.

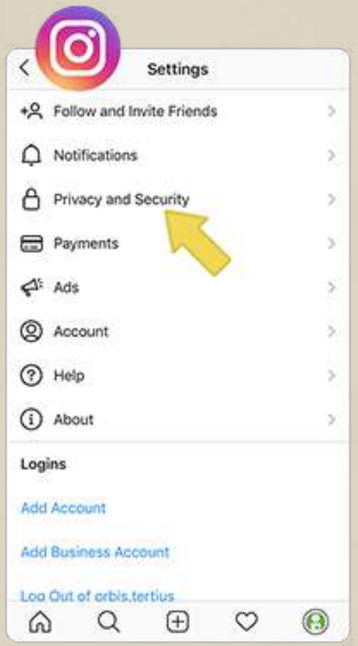
5. Tipp Ismerd meg az adatvédelmi beállításokat!

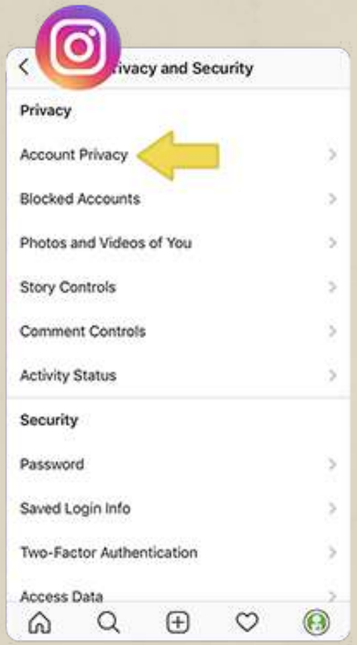
Bármilyen eszközt, alkalmazást vagy szolgáltatást is használsz, nézd meg az adatvédelmi szabályzatát!

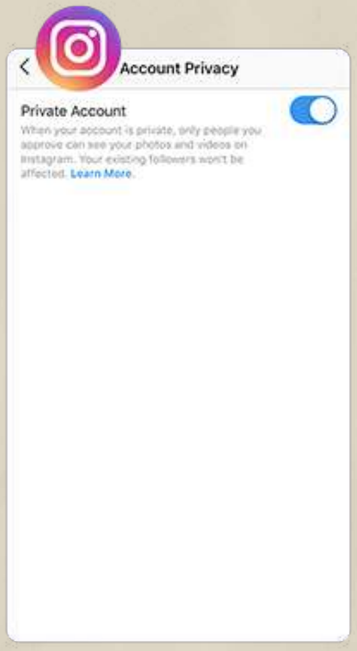
Egyes alkalmazások engedélyt kérnek a fényképek és egyéb személyes adatok eléréséhez. Tájékozódj, hogy ne ossz meg semmi olyat, amit nem szeretnél.

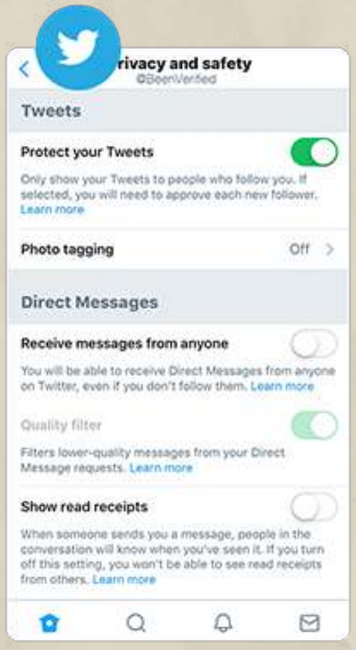
6. Tipp

Állítsd privátra a profiljaidat!









Gondold át alaposan, hogy kivel szeretnéd megosztani bejegyzéseidet és személyes adataidat. A profilodat úgy állítsd be, hogy csak ismerősöknek és követőknek legyen látható. A privátra állított profillal közzétett tartalmakhoz csak az elfogadott követőid férhetnek hozzá..

7. Tipp

Óvatosan ossz meg bármit is!

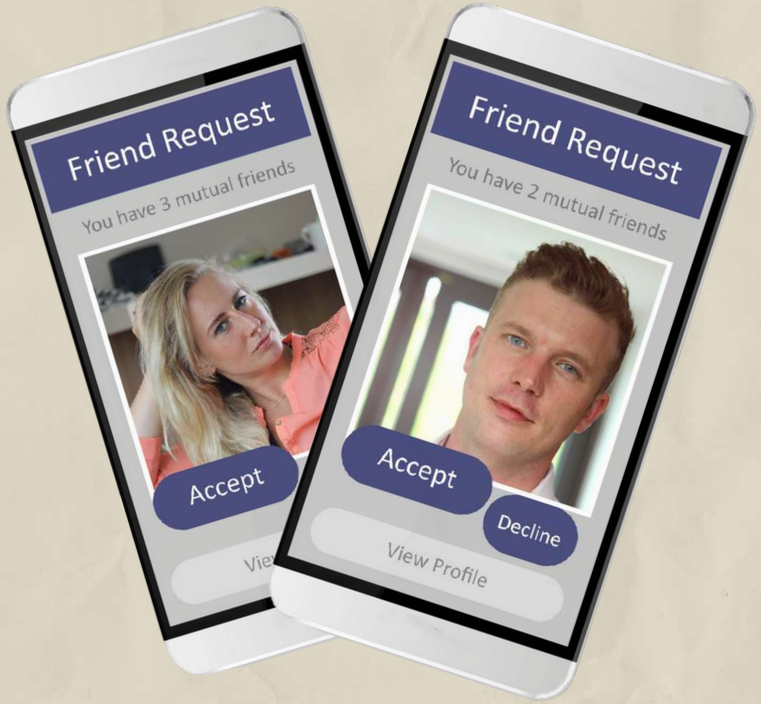
Még az erős adatvédelmi beállítások mellett is fontos észben tartani, hogy amit az interneten közzéteszel, az sosem igazán privát, ezért megosztható. Így fontos, hogy mindig gondolkodj, mielőtt posztolsz valamit.

8. Tipp

Szelektálj a baráti felkérések között!

Ha nem ismered az illetőt, ne fogadd el a felkérést!

Még ha ismered is, kattints a profiljára, hogy megbizonyosodj arról, hogy nem egy hamis fiókkal próbálnak hozzáférni az adataidhoz. A kiberbűnözők kiadhatják magukat olyan személyeknek, akiket online ismersz. Tehetik ezt azzal a céllal, hogy pénzt csaljanak ki az emberekből, politikai nyomást gyakoroljanak, vagy bármilyen más rossz szándék miatt is.



9. Tipp

Óvatosan kattints a hivatkozásokra!

Légy óvatos a gyanús hivatkozásokat tartalmazó webhelyekkel vagy e-mailekkel. Egyes webhelyek kvízekkel, ajándékokkal vagy csábos sztorikkal próbálják elérni, hogy kattints rájuk, hogy azután ellophassák a személyes adataidat.

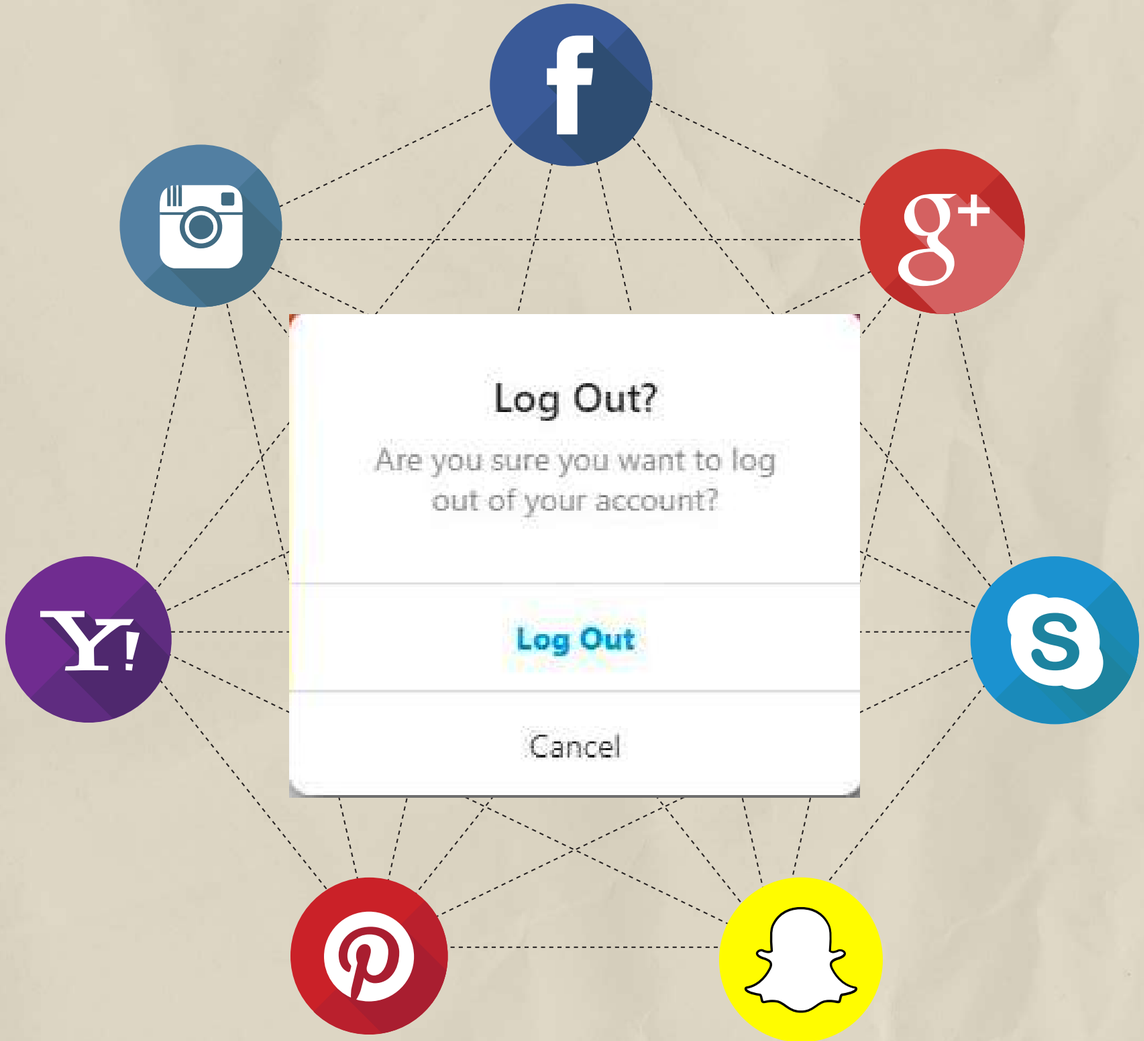
Ellenőrizd a weboldal megbízhatóságát!

Ezt úgy teheted meg, hogy ellenőrzöd, van-e kis lakat ikon vagy „https" az URL előtt. Az "s" a "https"-ben a "secure"-t (biztonságos) jelenti, a zár pedig azt, hogy a böngésző megerősítette, hogy biztonságos a webhely.

10. Tipp

Ha végeztél, jelentkezz ki!

Ne engedd a böngészőnek, hogy megjegyezze a bejelentkezési adataidat. Sokkal biztonságosabb ezeket minden belépéskor újra megadni még akkor is, ha így egy kicsit tovább tart belépni.



Adatvédelem

és

Digitális lábnyom:

"Mit hagysz magad mögött?"

Mi az a digitális adat?

Adat: " Számítógépes rendszerben tárolt információ "

Annak ellenére, hogy a digitális platformok „ingyenesként" hirdetik magukat, nem azok. A közösségi média cégek profitot termelnek az adathalászatból. -a felhasználók saját adataikkal és magánéletükkel fizetnek a szolgáltatásokért.

Ezeknek a cégeknek az a célja, hogy mindenki minél több információt osszon meg magáról, és mindenkiről minél több adatot gyűjtsön. Ezeket az adatokat pedig adatbázisokká alakítják a hatékony, jól célzott hirdetések érdekében.

Milyen adatokat gyűjtenek rólad, miközben a neten böngészel?

Keresések

Demográfiai adatok (pl. születési dátum, nem stb.)

A böngésző neve (pl. Chrome, Firefox stb.) és egyéb információk, például az alapértelmezett nyelv

A kosaradban lévő tételek, valamint a megtekintett és megvásárolt termékek

Információk a számítógép rendszeréről, az asztali számítógépről vagy a mobilról, a CPU és GPU modellekről, a kijelző felbontásáról stb

A barátaid neve, milyen gyakran látogatsz egy éttermet, stb. - gondolj bele, mit tud rólad a Facebook, hova és kivel jársz, stb.

IP Címek

Elhelyezkedés

Egérmozgások, egérkattintások és egyéb böngészőműveletek

Milyen Youtube videókat néztél meg

A nap mely szakában böngészel a legszívesebben

Weboldalak, amiket megnéztél

Hogyan kezeljük digitális lábnyomunkat?

Digitális lábnyom: "Amit magad után hagysz"

A „digitális lábnyom" alapvetően a te teljes online jelenléted nyoma - minden információ, bejegyzés, kép és adat, amiket szándékosan vagy sem, de megjelenítesz az interneten. Minél több információt teszel fel az internetre, annál többet tudhatnak meg rólad. Némelyek ezt az információt felhasználhatják arra, hogy meghatározzák, mit vásárolnál szívesen, de más, akár rosszindulatú célokra is, például megpróbálhatják feltörni online fiókjaidat, és így hozzáférni jelszavakhoz, banki adatokhoz stb.

Hogyan kezeljük digitális lábnyomunkat?

A digitális lábnyomok, beleértve a metaadatokat és a tartalmat, szorosan kapcsolódnak a biztonsághoz, a magánügyeinkhez és a bizalomhoz. Ahogy az internetet egyre szélesebb körben használják, egyre fontosabbá válik, hogy átgondoljuk, mi történhet a saját fényképeink és írott tartalmaink tulajdonjogával. Akár digitális személyazonosság-lopás célpontjaivá is válhatunk..

⚠ Ne feledd, hogy ami az internetre felkerül, az általában meg is marad, még ha törlöd is a bejegyzéseket, a hátrahagyott adatok ott maradnak.

Íme a 10 legfontosabb dolog, amivel csökkentheted és kezelheted digitális lábnyomodat

Hogyan kezeljük digitális lábnyomunkat?

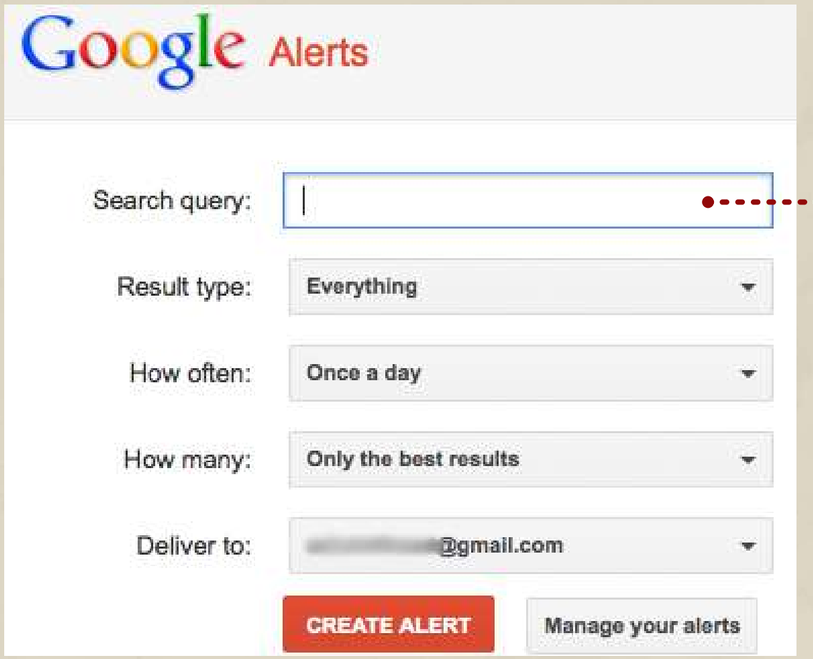
1. Keress rá magadra az interneten és lásd, mi jelenik meg.

Ahhoz, hogy kezelni tudd, pontosan tudnod kell, hogy mekkora is a te digitális lábnyomod. Keress rá különböző keresőmotorokon (Google, Yahoo stb.) a nevedre, és nézd meg a találatokat. Készíts listát mindenről, amitől szeretnél megszabadulni vagy javítani rajta.

Hogyan kezeljük digitális lábnyomunkat?

2. Állíts be Google-értesítést a saját nevedhez!

Így értesítést kapsz arról, ha bármilyen említés megjelenik rólad az interneten.



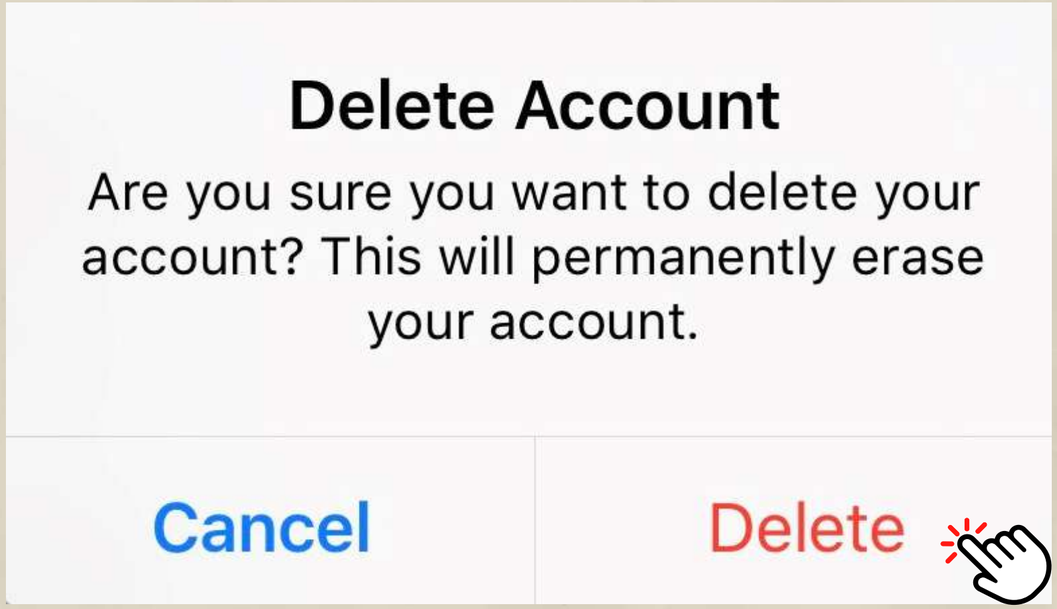
Ide írja be a nevét!

Nem mindig szabhatod meg, hogy mi jelenjen meg az interneten. További segítségért fordulj ahhoz a keresőmotorhoz, amelyen az eredmények megjelennek, és kérd a törlését. Például a Google Google Támogatási oldalán jelentheted, ha törölni szeretnéd a keresőmotorjában megjelenő személyes vagy privát információkat.

Hogyan kezeljük digitális lábnyomunkat?

3. Tiltsd le azokat a profilokat vagy fiókokat, amiket már nem használsz, és váltsd a fiókbeállításokat privátra.

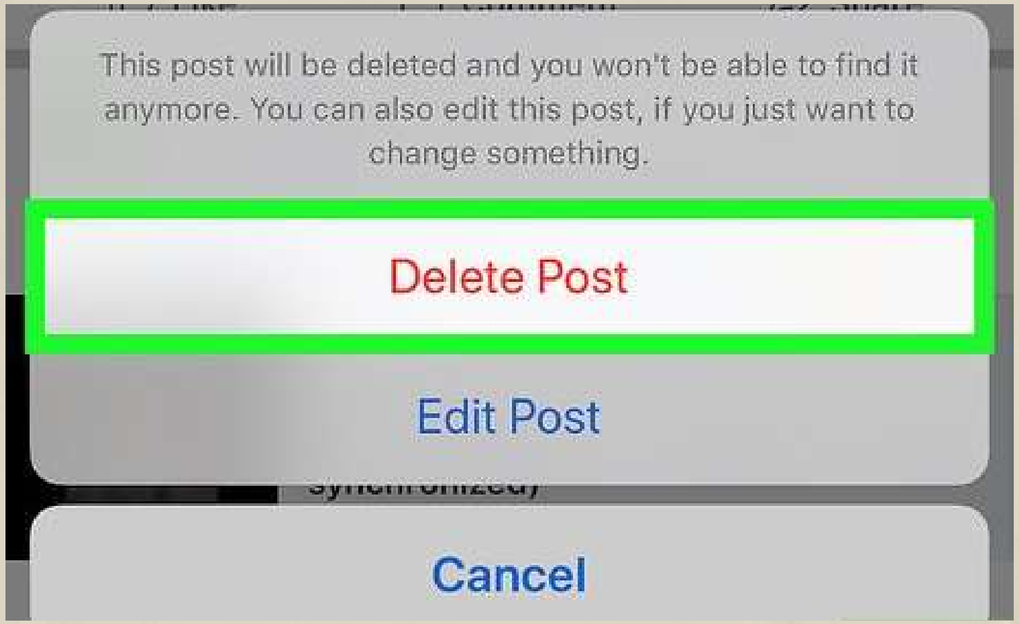
Nincs értelme olyan fiókokat megtartani, amelyeket nem használ. Ha ezek a fiókok nyitva vannak, az csak növeli az Önről szóló online információ mennyiségét. Ez összezavarja online jelenlétét, ezért zárja be vagy törölje azokat a fiókokat, amelyeket már nem használ



Ezenkívül váltsd át a beállításokat privátra az összes fennmaradó platformon, amivel szabályozni és korlátozni tudod, hogy ki láthassa a bejegyzéseidet.

Hogyan kezeljük digitális lábnyomunkat?

4. Törölj mindent, ami nem mutat jó képet rólad.



Előfordulhat, hogy magadra kereseve a neten rátalálsz pár átgondolatlan posztra . Ez azt jelenti, hogy bárki láthatja őket, ami a magánéletedben és a munkádban is hátrányos lehet a számodra. Kényes tartalomnak számítanak a trágár szavak, a merészebb fotók, az italozás, a durva megjegyzések. Ha találsz ilyet, töröld őket, és többet ne posztolj hasonlót.

Hogyan kezeljük digitális lábnyomunkat?

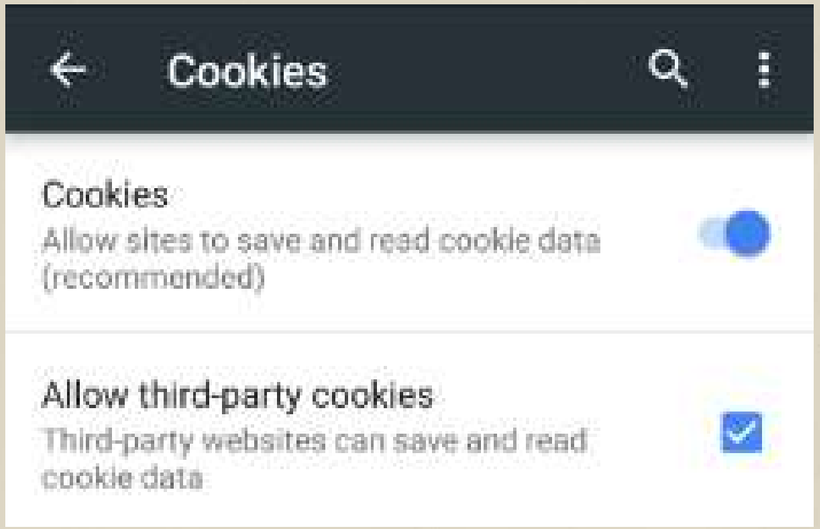
5. Gondolkodj, mielőtt posztolsz!

Gondoljon bele az ön által közzétett bejegyzések minden következményébe, és csak olyan dolgokat osszon meg, amelyek pozitív, szakmai megvilágításban mutatják meg Önt. Próbálja meg elkerülni a közzétételt, ha érzelmes vagy dühös. Lehet, hogy abban a pillanatban nem gondol a következményeire.

Ne feledd, hogy az adatvédelmi beállítások nem helyettesítik azt, hogy körültekintően bánj azzal, amit közzéteszel. Továbbra is kerüld a nem megfelelő bejegyzések közzétételét, még akkor is, ha a fiókod zárolva van.

Hogyan kezeljük digitális lábnyomunkat?

6. A nyomkövetési adatok törléséhez néhány havonta töröld a cookie-kat.



A cookie-k bizonyos webhelyek keresési adatainak nyomon követésére szolgálnak. Ezzel kényelmesebbé lehet tenni az internetes élményt, mert a webhelyek emlékezni fognak rád, de tárolhatják személyes adataidat is.

Hogy ezt elkerüld, néhány havonta töröld a cookie-kat a böngésződből, hogy megszabadulj mindentől, ami nyomon követheti tevékenységedet.

Hogyan kezeljük digitális lábnyomunkat?

7. Vigyázz a gyanús üzenetekkel és az adathalász e-mailekkel!

Nem szabad megbízni azokban az üzenetekben, amelyekben egy rövidített URL mellett olyan szöveg szerepl, mint pl. «OMG, nézd meg ezt a képet rólad...» vagy «Láttad, mit mondanak rólad...» - ne kattints az ilyen üzenetekben kapott hivatkozásokra.

Az adathalász e-mailek is problémát jelentenek. Ezeknek a hamis értesítéseknek a küldői olyan megbízható szervezetnek adják ki magukat, mint a Facebook, hogy megpróbáljanak rábírni téged a bejelentkezésre, és így ellopni az adataidat.

Hogyan kezeljük digitális lábnyomunkat?

8. Ismerd fel a csalást!

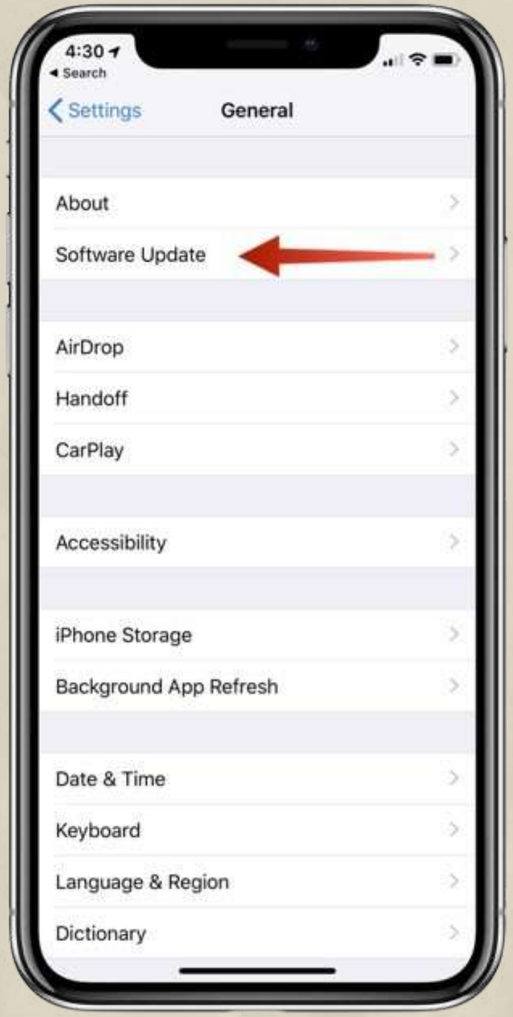
A közösségi médiában nem mindenki az, akinek mondja magát. Lehetnek olyan emberek, akik valaki másnak adják ki magukat, és árthatnak neked - például azzal, hogy révésznek téged téged arra, hogy osszál meg velük olyan személyes adatokat, amiket felhasználhatnak ellened.

Ha valakivel ismerősök lettetek, nem kell örökké annak is maradnotok. Nézd át és tisztogasd rendszeresen ismerőseid körét.

Hogyan kezeljük digitális lábnyomunkat?

9. Mindig frissítsd a szoftvert.

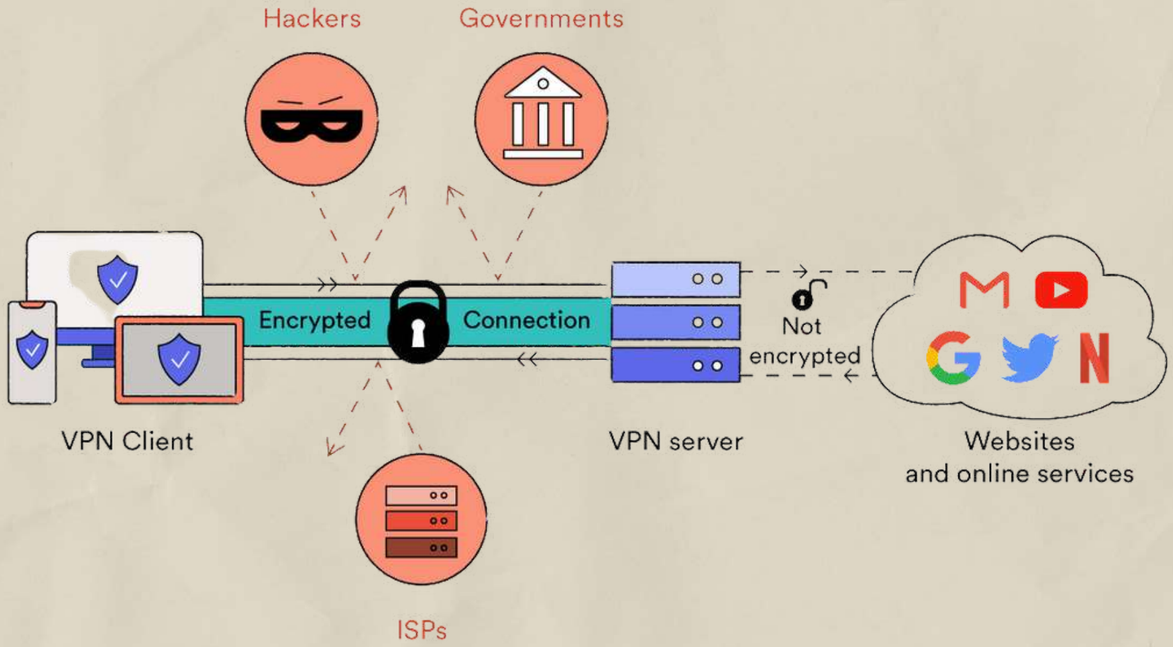
Az elavult szoftverek résein keresztül bejuthatnak a hackerek a személyes adataidhoz. A víruskereső és más programok frissítése azt jelenti, hogy olyan biztonsági javításokat kapsz, amelyek segítenek kijavítani vagy eltávolítani a rendszerhibákat. Beállíthatod a programok és alkalmazások automatikus frissítését, így biztos lehetsz benne, hogy a legújabb szoftver telepítve van.



Hogyan kezeljük digitális lábnyomunkat?

10. Használj privát hálózati eszközöket!

Személyes adataid védelmében használhatsz nyomkövetés elleni eszközöket, privát keresőmotorokat vagy névtelen böngészőket. A virtuális privát hálózatok (VPN) elfedik az IP-címedet, így a tartózkodási helyed, a böngészési előzmények és egyéb információk bizalmasak maradhatnak.



New Tab

Internetes zaklatás és online gyűlöletbeszéd

Mit jelent az internetes zaklatás?

Hogyan védheted meg magát?

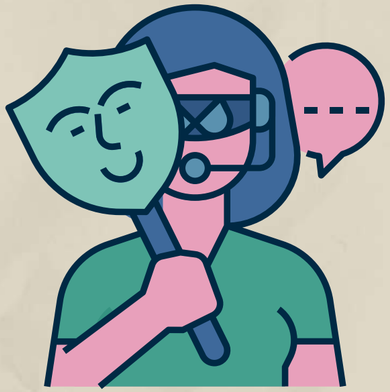
Hogyan lehet megvédeni másokat?

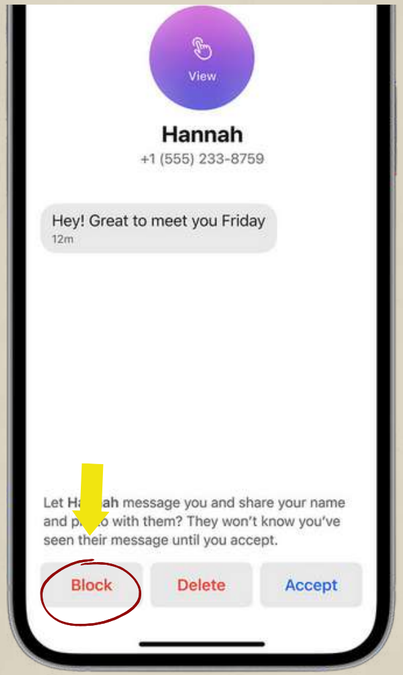
Mit jelent az internetes zaklatás?

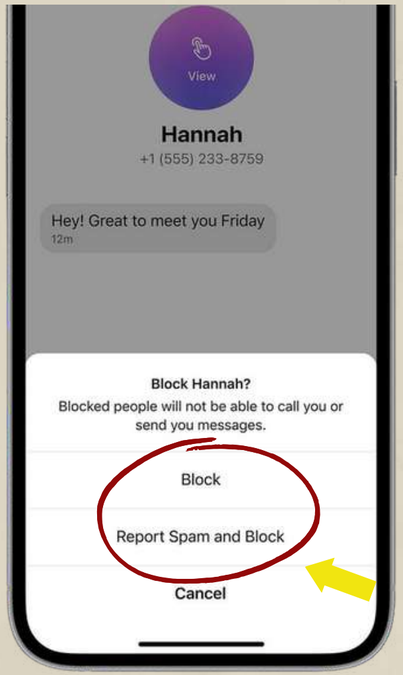
Számos közösségi platform létezik, ahol az emberek különféle tartalmakat hoznak létre és osztanak meg. Ennek egyik legnagyobb veszélye, hogy a kapcsolat, a figyelem és az elismerés iránti vágyból gyakran meggondolatlanul cselekednek. Az interneten sokkal könnyebben és gátlástalanabbul teszik meg azt, amit a való életben amúgy nem tennének meg. Az információs technológiákkal való visszaélést azzal a szándékkal, hogy másoknak kárt okozzanak, internetes zaklatásnak nevezik.

Hogyan lehet megelőzni az internetes zaklatást?

Vannak olyan nem valódi felhasználók, akik a közösségi oldalak használatával visszaélve zaklatják ismerőseiket. Néha ezek az emberek hamis személyazonosságokat és fiókokat használnak, vagy beazonosíthatlanná teszik eszközeiket, hogy láthatatlanul zaklathassanak másokat.







Íme 7 egyszerű lépés az internetes zaklatás megelőzésére:

- Erősítsd meg adataid védelmét
- Inkább ne válaszolj
- Ne ossz meg túl sokat
- Tiltsd le az adott személyt
- Mentsd el a bizonyítékokat
- Beszélj róla valakinek
- Jelentsd az oldalnak vagy a hatóságnak

Legyél tisztában bejegyzéseid másokra gyakorolt hatásaival

Az emberek néha ártalmatlannak vagy viccesnek gondolják azt, amikor zavarbaejtő videót vagy képet osztanak meg, vagy megbízhatatlan forrásokra hivatkozva osztogatnak alternatív gyógyászati tanácsokat, stb.

De az igazság az, hogy a digitális világ egy valós világ, valódi következményekkel. Amint közzé teszel valamit, elveszted az irányítást afelett, hogy az milyen társas, pszichés, traumatikus hatással lehet valaki másra.

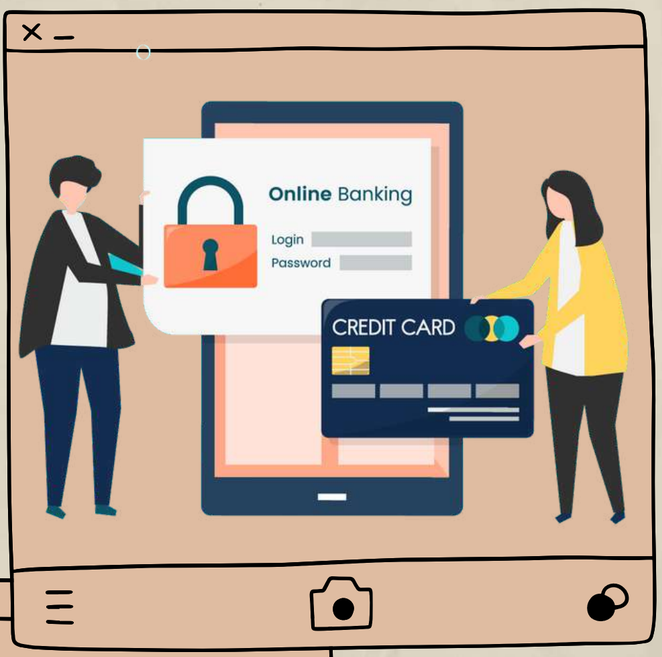
Ne használd a közösségi oldalakat mások megszégyenítésére és zaklatására!

Mindig tedd fel magadnak a következők kérdéseket, mielőtt megnyomod a küldés gombot!

Fontold meg ezt a 10 kérdést, mielőtt posztolnál!

1. Később jól vagy máshogy fogom érezni magam, ha erre gondolok?
2. Miért posztolok?
3. Ezt személyesen is elmondanám?
4. Lehet ezt másként értelmezni?
5. Kedves vagyok?
6. Ez nekem is tetszene?
7. Ez tényleg privát?
8. Fel vagyok hatalmazva erre?
9. Ez legális?
10. Ez pontos?

Online Bankolás és Vásárlás



Mi is az online bankolás?

Az online és mobilbankolás biztonságos módja annak, hogy otthonról intézd pénzügyeidet.

Mire használhatom az online bankolást?

- Ellenőrizheti az egyenlegét.
- Befizetheti a számláit
- Ellenőrizheti a banki nyilatkozatait
- Utalhat pénzt személyeknek.
- Bankszámlák között tud pénzt utalni
- Beállíthatod vagy törölheted a csoportos beszedéseket vagy állandó megbízásokat

Hogyan állíthatom be az online bankolást?

Ha van internet-hozzáféréssel rendelkező eszközöd és online bankszámlád, bármikor elkezdheted:

Az online banki szolgáltatáshoz való hozzáféréshez először regisztrálnod kell a bank weboldalán. A különböző bankok ügymenete eltérhet egymástól az online szolgáltatás beállításakor, így előbb beszélj a te bankoddal. A lépések a következőket tartalmazhatják:

- A személyes adatok és bankszámla adatainak megadása (kód és számlaszám).
- A bank felhívhat téged, hogy feltegyen néhány kérdést a személyazonosságod ellenőrzéséhez, valamint aktiválási kódot küldhet.
- Felhasználónév és biztonságos jelszó vagy jelkód beállítása.

Mit tehetek pénzem és személyazonosságom biztonsága érdekében?

1. Csak biztonságos wifi hálózatokat és eszközöket használj az online banki szolgáltatások eléréséhez.

Ha nyilvános hálózatokat használsz, például kávézókban vagy vasútállomásokon, előfordulhat, hogy ugyanazon a hálózaton lévő személyek hozzáférhetnek az adataidhoz. Legyél óvatos, amikor nyilvános számítógépet használsz az online banki szolgáltatások eléréséhez. Lehetséges, hogy nem rendelkeznek megfelelő szintű védelemmel.

Mit tehetek pénzem és személyazonosságom biztonsága érdekében?

2. Használj különböző bejelentkezési adatokat és jelszavakat az online bankszámlákhoz.

Az online banki tevékenységhez készült bejelentkezési adatokat ne használd más online portálokon vagy szolgáltatásokon. Ügyelj arra, hogy erős jelszót hozz létre, és változtasd meg rendszeresen.

3. Ne add meg senkinek az online banki bejelentkezési adataidat.

Tartsa meg őket, akárcsak minden pin-kódot és más hitelesítési információt.

Mit tehetek pénzem és személyazonosságom biztonsága érdekében?

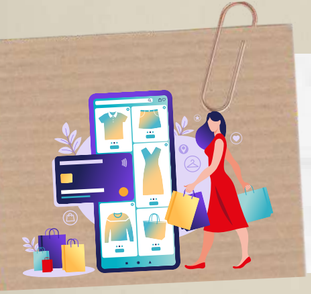
4. Tudd pontosan, hogy kinek utalsz át pénzt.

Csak olyan feleknek utaljon pénzt, akikben megbízol. A pénzátutalás általában nem vonható vissza a fogadó fél kifejezett engedélye nélkül.

Mit tehetek pénzem és személyazonosságom biztonsága érdekében?

5. Használj személyazonosság-lopás elleni védelmi szoftvert vagy VPN-t

Fontold meg a személyazonosság-lopás elleni védelmi szoftver letöltését. Ez egy olyan szolgáltatás, amely titkosítja az internetkapcsolatot a biztonság megőrzése érdekében. Ezek a szolgáltatások gyakran több védelmi intézkedést is tartalmazhatnak, beleértve a VPN-t és a jelszófigyelést.

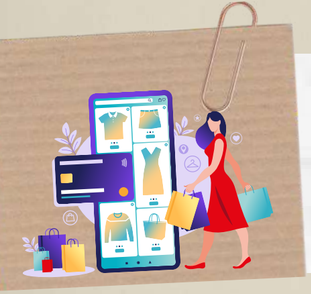


Biztonságos online vásárlás

Az online vásárlás sokkal könnyebbé teheti az életet, és kevesebbet kell vesződni szupermarketekbe, bevásárlóközpontokba járással. A legtöbb szupermartketnél, de már kisebb és független üzletekbnél is vásárolhatsz online.

Az árukat rendelhetjük házhozszállítással, általában alacsony díj ellenében vagy ingyenesen, vagy kérheted átvevőpontra is a rendelést, ekkor az online rendelt termékeket az üzletben veheted át.

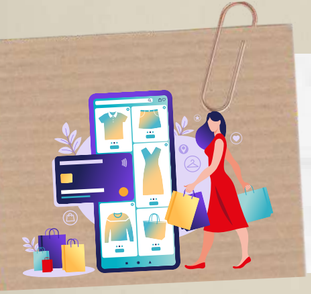
Azonban fontos, hogy biztonságos webhelyeket használjunk. Íme néhány tipp, hogyan vigyázhatsz pénzedre és személyes adataidra online vásárláskor.



Biztonságos online vásárlás

1. Tipp: Gondosan válaszd ki azt a webhelyet és kereskedőt, akinél vásárolsz.

Válassz jó hírnévvel rendelkező online kiskereskedőket, jól ismert szupermarketeket, üzleteket vagy bejáratott online boltokat. Keresd meg a cég teljes elérhetőségét. Egy jó hírű cég ezeket az információkat mindig megjeleníti a honlapján. Keresd meg a cég nevét az interneten, hogy megtudd, nem volt-e negatív tapasztalata valakinek a kereskedővel.



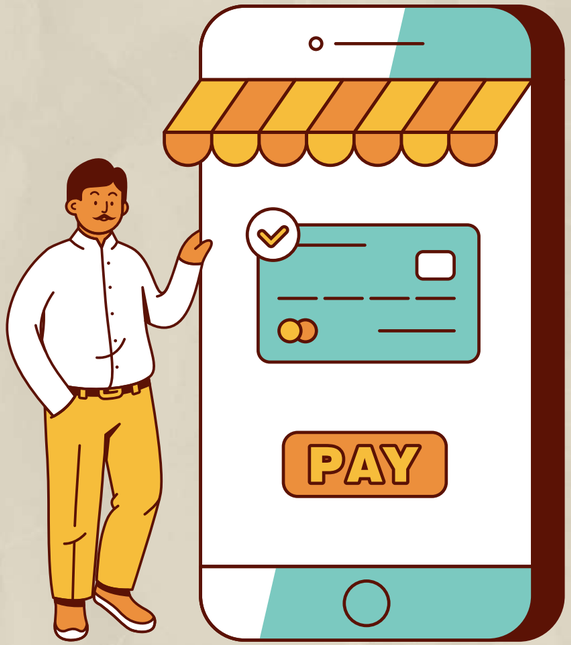
Biztonságos online vásárlás

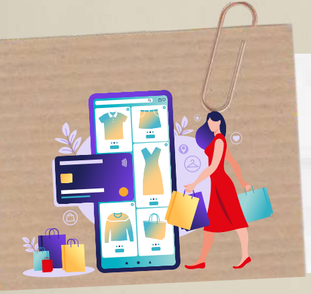
2. Tipp: Internetes tranzakciókhoz használd mindig ugyanazt a kártyát.

Rendszeresen ellenőrizd a kártya bankszámlakivonatát, hogy nem történt-e szokatlan tranzakció, és probléma esetén azonnal fordulj a bankodhoz.

3. Tipp: Az internetes tranzakciókhoz bankkártya helyett inkább hitelkártyát használj.

Ez további védelmet biztosíthat. Ha a vásárlásod meghalad egy bizonyos magas összeget, amit hitelkártyával fizetsz, az eladó és a kártyatársaság egyformán vállalja a felelősséget, ha bármi baj történik.



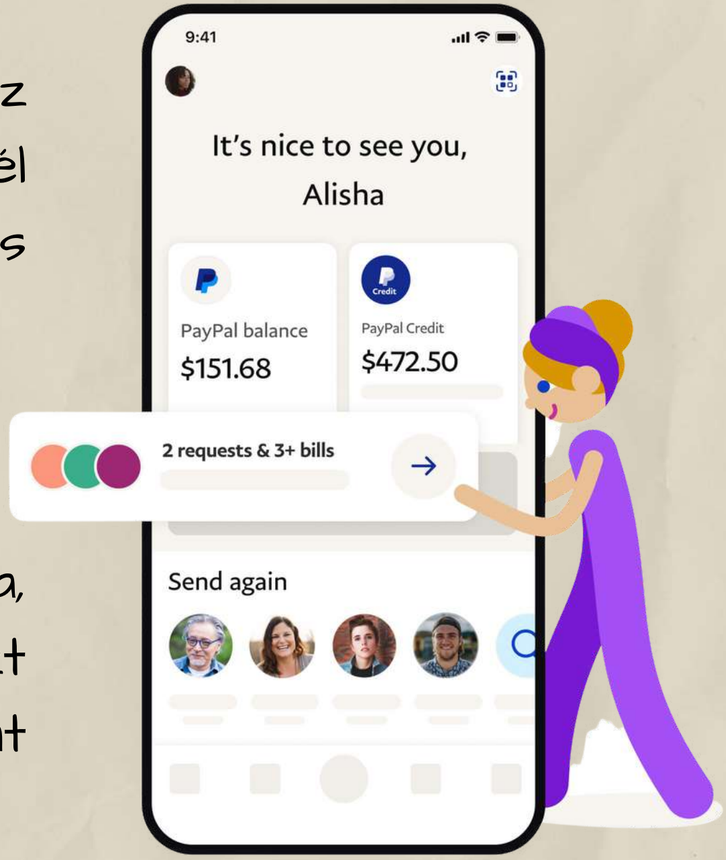


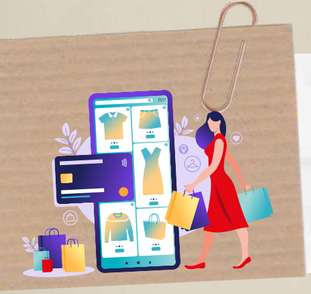
Biztonságos online vásárlás

4. Tipp: Fontold meg a PayPal használatát.

Ez egy online számla, amit hozzákapcsolhatsz a bankszámládhoz vagy kártyádhoz, hogy online vásárolhass vele. Ha nem szeretnél hitelkártyát használni, a PayPal biztonságos alternatíva, és nagyobb fizetési védelmet nyújt, mint a hitelkártya.

Töltsd le az alkalmazást a telefonodra, vagy regisztrálj ingyenesen online. Ezt követően online fizetési lehetőségként használhatod vásárlásaidhoz.

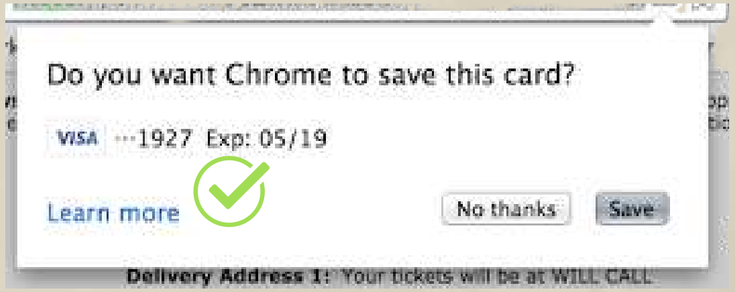


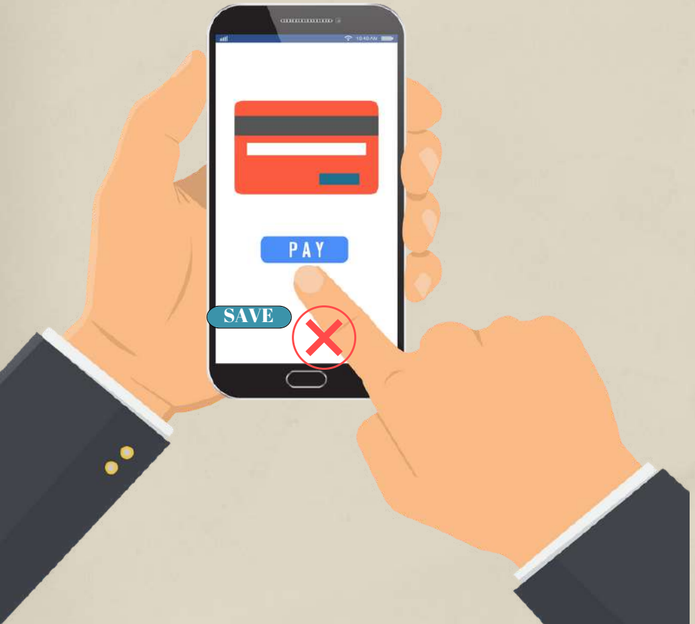


Biztonságos online vásárlás

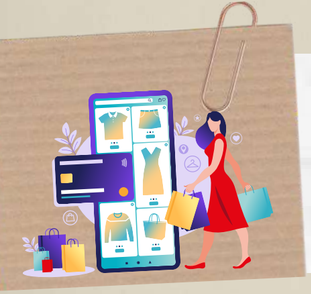
5. Tipp: Soha ne mentsd el a kártyaadataidat!

Néha a webhely vagy az internetböngésző felszólít, hogy mentsd el kártyaadataidat a következő alkalomra.





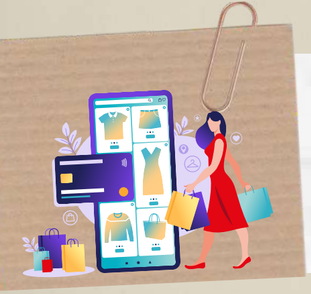
Ezt soha ne tedd meg közösen használt számítógépen, és győződj meg arról is, hogy készüléked jelszóval, PIN-kóddal vagy ujjlenyomat-bejelentkezéssel védett, ha mégis elmentenéd a kártyaadatokat.



Biztonságos online vásárlás

6. Ne dőlj be az e-mailes csalásoknak!

Előfordulhat, hogy nagyszerű akciókat kínáló e-maileket vagy szöveges üzeneteket kapsz, vagy amiben azt állítják, hogy probléma adódott a csomag kézbesítésével. Töröld az ismeretlen feladók gyanús üzeneteit, és ne nyisd meg a mellékleteket, ne kattints az üzenetekben található hivatkozásokra, mert azok megfertőzhetik számítógépedet vagy telefonodat vírusokkal és más rosszindulatú programokkal.



Biztonságos online vásárlás

7. Kövesd nyomon a szállítást!.

Miután befejezted vásárlást, kövesd nyomon a szállítást, hogy megbizonyosodj arról, a kézbesítés elindult. Ha a kereskedő megtagadja a szállítási adatok megadását vagy nem válaszol a szállításra vonatkozó kérdéseidre, fordulj segítségért a hitelkártya kibocsátójához. Előfordulhat, hogy eltávolítják a terhelést a számládról, és kivizsgálják az ügyet.

ÜGYFÉLKAPU

EESZT
Elektronikus
Egészségügyi
Szolgáltatási Tér

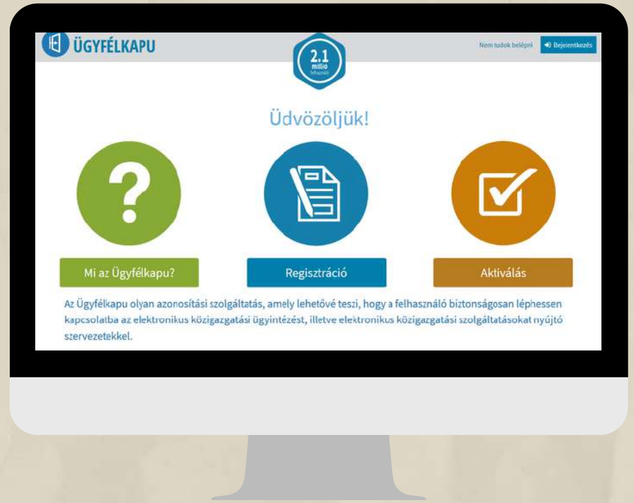
KRÉTA

SZOLGÁLTATÁSOKHOZ VALÓ ONLINE HOZZÁFÉRÉS

Milyen elektronikus közszolgáltatások vannak Magyarországon?

Az Ügyfélkapu

Az Ügyfélkapu a magyar kormányzat elektronikus azonosító- és ügyfélbeléptető rendszere. Biztosítja, hogy használói a személyazonosság igazolása mellett egyszeri belépéssel biztonságosan kapcsolatba léphessenek az elektronikus közigazgatási ügyintézést és szolgáltatást nyújtó szervekkel. Szóval viszonylag egyszerűen és gyorsan tudsz ügyeket intézni vele.



Kinek Lehet Ügyfélkapuja?

Bárkinek. Pontosabban bármely természetes személynek lehet Ügyfélkapuja állampolgárságtól függetlenül.

Milyen ügyeket tudsz intézni az Ügyfélkapun keresztül?

Számos ügyet intézhetsz itt, csak pár dolgot említek meg:

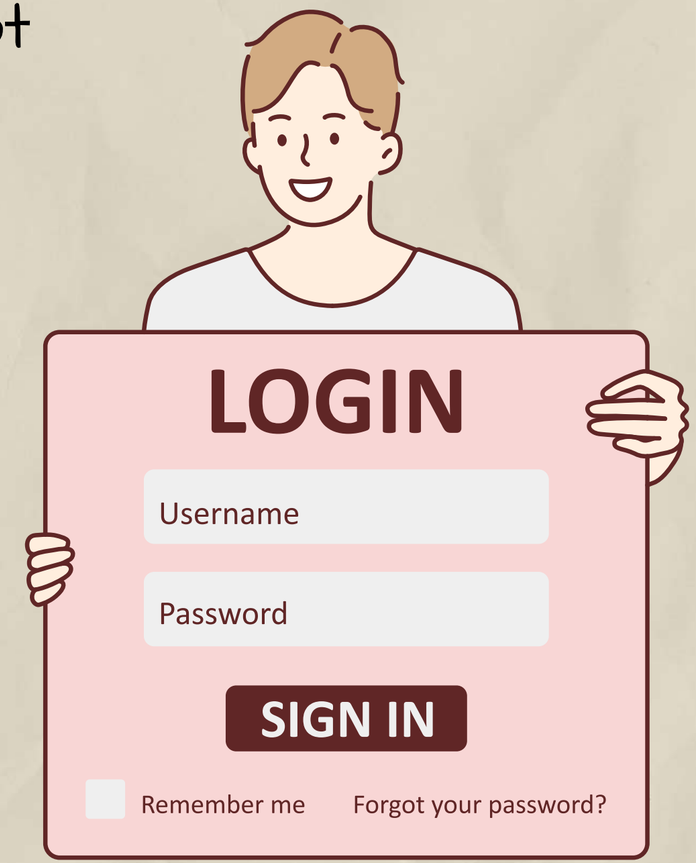
- ellenőrizheted, hogy be vagy-e jelentve a munkahelyeden
- igényelhetsz anyasági támogatást, GYES-t, családi pótlékot
- kérhetsz erkölcsi bizonyítványt
- intézheted az SZJA bevallásod
- lekérdezheted az adófolyószámládat a NAV-tól

A teljes listát itt tudod megnézni:

https://ugyintezes.magyarorszag.hu/szolgaltatasok?selected=A

Hol kérhetsz hozzáférést?

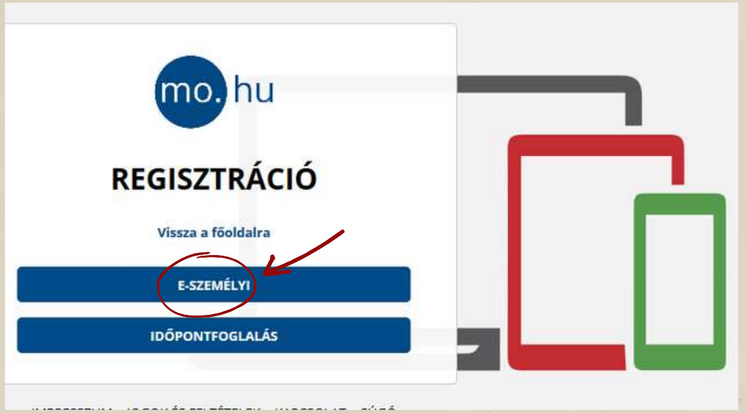
- Bármelyik okmányirodában,
- Kormányablakban (időpontot foglalhatsz online),
- Adóhatóság (NAV) főbb ügyfélszolgálatain (időpontot foglalhatsz online),
- Egyes postai ügyfélszolgálatokon (kistelepüléseken)
- Elektronikusan.



Mi kell Ügyfélkapu nyitásához?

1. Személyazonosításra alkalmas hatósági igazolvány
2. Egyedi felhasználói név
3. E-mail cím

Hogyan Lehet Ügyfélkaput Nyitni Online?



Menj be a https://ugyfelkapu.gov.hu/regisztracio felületre. Itt kattints az „E-SZEMÉLYI" gombra. Megjelenik a "REGISZTRÁCIÓ E-SZEMÉLYIVEL" űrlap:

Az okmányazonosítót: ez az e-személyiden található, 6 számjegyből és 2 betűből álló azonosító

A regisztrációs kódot: ezt a személyazonosító igazolványod igénylésekor kaptad egy lezárt borítékban, ami 11, számjegyekből és betűkből álló karaktersorozat.

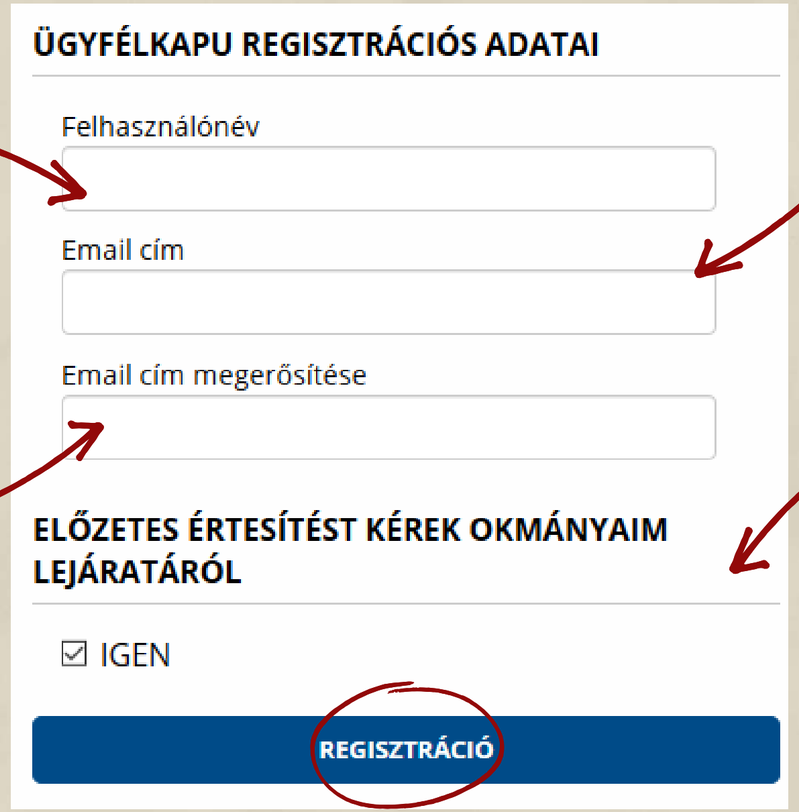
Az adatok megadása után kattints az „ELLENŐRZÉS" gombra.

Hogyan Lehet Ügyfélkaput Nyitni Online?

Látni fogod az adataiddal kitöltött űrlapot. Le kell görgetni, és meg kell adni a következőket:

A felhasználónevedet Te választod ki, de ha már létezik, vagyis már használja valaki, akkor másikat kell kitalálnod.

Az „Email cím megerősítése" mezőbe ugyanezt a címet kell beírni.



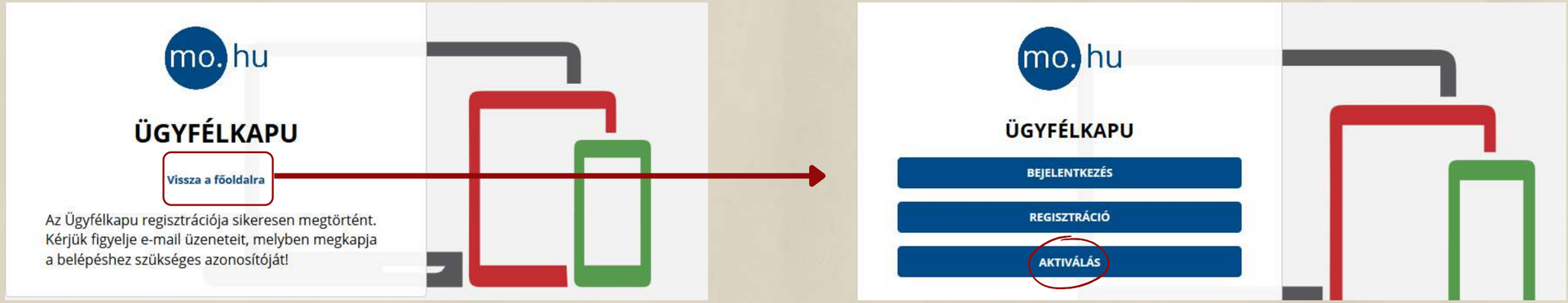
Erre a címre kapod meg emailben az első belépéshez szükséges egyszeri aktiváló kódodat.

Az „Előzetes értesítést kérek okmányaim lejáratáról" mező alapértelmezetten be van pipálva. A szolgáltatás minden Ügyfélkapu-regisztrációval rendelkező számára ingyenes

Ha mindent kitöltöttél, akkor kattints a „Regisztráció" gombra.

Hogyan Lehet Ügyfélkaput Nyitni Online?

A regisztráció sikerességéről üzenetablakban kapsz tájékoztatást. Ha a "Vissza a főoldalra" szövegre kattintasz, akkor a következőt fogod látni a képernyőn:



Kattints az «Aktiválás" gombra. Létre kell hozni egy jelszót. Az Ügyfélkapu jelszó minimum 8 karakter legyen, legalább két számot, valamint kis- és nagybetűt vegyesen tartalmazzon. A jelszó két évig érvényes, két év után módosítani kell a jelszót.

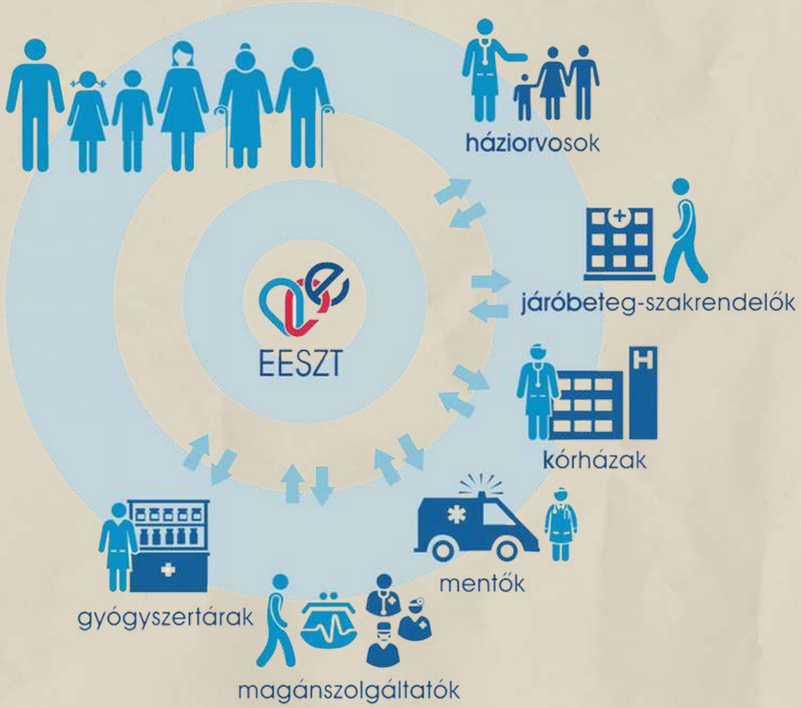
Az Elektronikus Egészségügyi Szolgáltatási Tér

EESZT
Elektronikus
Egészségügyi
Szolgáltatási Tér

Az Elektronikus Egészségügyi Szolgáltatási Tér, röviden EESZT, az egészségügyi szolgáltatási folyamatokat összekapcsoló informatikai rendszer és adatbázis, amely a magyarországi egészségügyi rendszerben ellátottakra vonatkozó kényszer adatgyűjtést előíró törvények megvalósítását teszi lehetővé. Az EESZT adatbázis személyes adatok mellett a leletek, receptek, és különféle egészségügyi vizsgálatokkal kapcsolatos információk, a páciens élethosszáig (és az után még öt évig) tartó időtartam erejéig történő gyűjtésére, tárolására és megosztására szolgál.

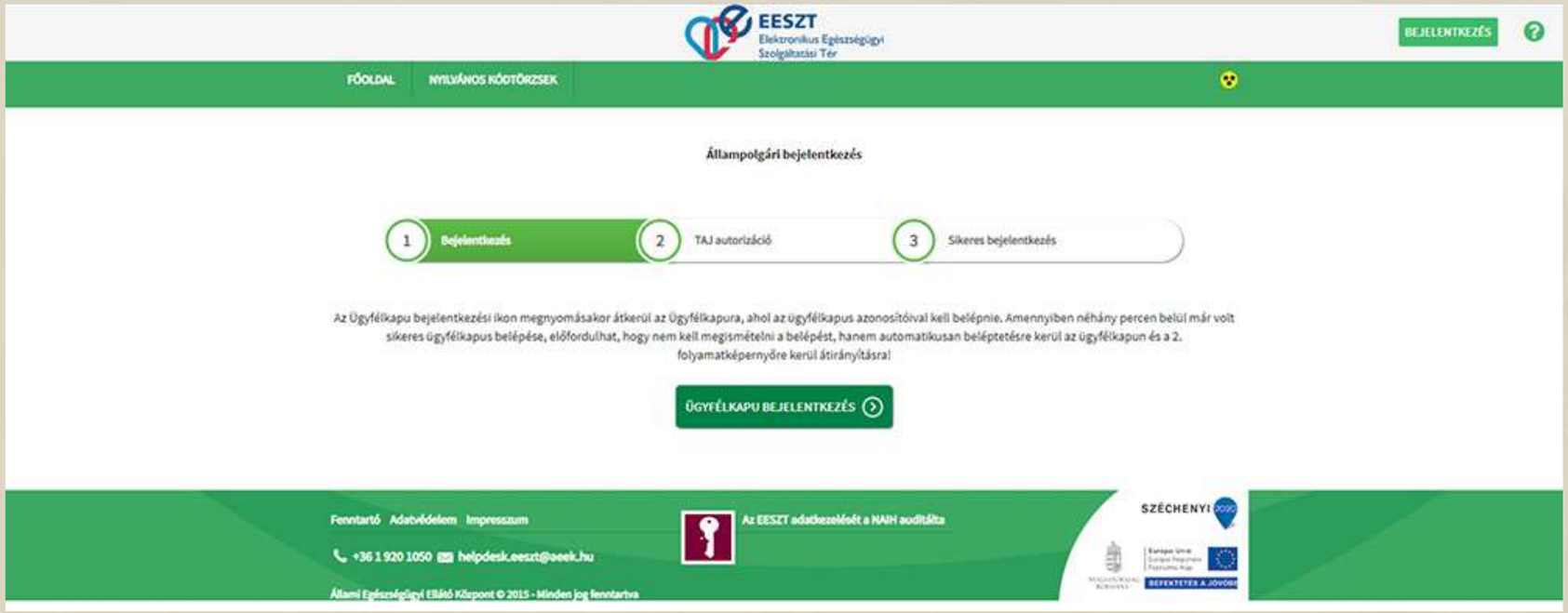
Az Elektronikus Egészségügyi Szolgáltatási Tér

Minden feltöltött egészségügyi információ elektronikusan megtalálható a portálon: receptjeink, beutalóink, ambulánslapjaink, laborleleteink, röntgen-, CT- és MR-leletek, zárójelentések. Ezeket a dokumentumokat akár le is tölthetjük pdf-formátumban, majd elmenthetjük számítógépünkre, és akár ki is nyomtathatjuk.

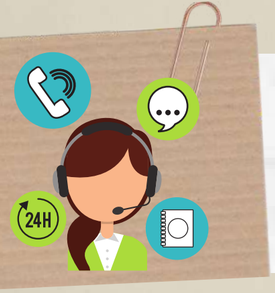


Az eReceptek is megjelennek a listában, jól elkülönítve a már kiváltottakat a még kiváltásra váróktól. 2019. december 31-ig minden esetben kapunk az orvostól egy ún. felírás igazolást is, ami a hagyományos receptet helyettesíti. A patikákban TAJ számunk alapján láthatók az eReceptek.

Belépés az EESZT-rendszerbe lakossági ügyfélként



Az EESZT rendszer használata a páciensek számára ügyfélkapu belépéssel történik. Az ügyfélkapu belépést követően az EESZT-rendszerbe történő belépés a TAJ-szám megadását követően válik lehetővé.



Hol és hogyan használják?

Háziorvosnál

A háziorvosa az **e-Recept** rendszerben észlelte, hogy a beteg nem váltotta ki az egyik fontos szívgyógyszerét. Vért vett a betegtől laborvizsgálat céljából, és az állapotának rosszabbodása miatt kardiológiai szakrendelésre utalta.

Szakrendelésen

A kardiológiai szakrendelésen az **e-beutaló** részletes adatait is figyelembe véve a beteg vízhajtó injekciót kapott, amitől a rövid megfigyelés alatt állapota jelentősen javult, illetve az **EESZT**-n keresztül látható vérvizsgálati eredmények alapján módosították a gyógyszereit, új vényeket is felírtak neki az **e-Recept** rendszerbe.

Gyógyszertárban

A beteg hazafelé betért a legközelebbi gyógyszertárba, ahol **e-Személyi igazolványával** (vagy TAJ kártyája és személyi okmánya) felmutatásával megkapta a felírt gyógyszereket.

Otthon

Kovács úr este kíváncsiságból ránézett az interneten a **Lakossági portál**ra (www.eeszt.gov.hu), végignézte a nap történéseit és megállapította, hogy mind az ellátása, mind pedig adatainak kezelése az elvárásainak megfelelően zajlott.

Otthon

Kovács úr napok óta erősödő lábdagadást és fulladást érzett, emiatt háziorvoshoz fordult.

Háziorvos - másnap

Kovács úr háziorvosa másnapi rendelésének kezdetén utána nézett az előző napi eseményeknek. Az **EESZT**-ből a háziorvosi programja megjelenítette a szakorvosi véleményt, és meggyőződhetett arról is, hogy Kovács úr most nem felejtette el kiváltani a gyógyszereit.

eeszt
elektronikus
egészségügyi
szolgáltatási tér

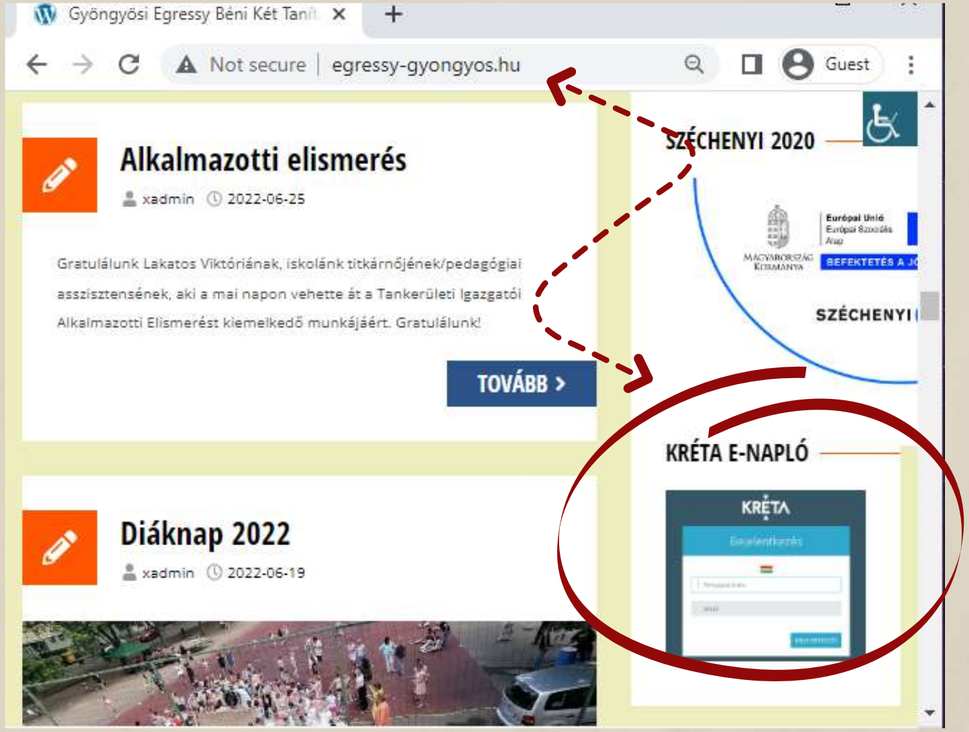
A KRÉTA Elektronikus napló

A KRÉTA Elektronikus ellenőrzője a szülőknek és tanulóknak nyújt segítséget a tanulmányok alatti naprakész információhoz jutásban asztali számítógépen, tetszőleges böngészőprogramon keresztül.

Az e-Ellenőrző bárhonnan elérhetővé teszi a tanulmányi adatokat. A tanulók és szülők általában a saját intézményi rendszerük webcímén keresztül érhetik el, onnan léphetnek be a rendszerbe.

Hogyan Lépjünk Be Krétába?

Keressünk rá az iskola nevére. Miután megvan, keressük meg az iskola oldalán a KRÉTA linket.

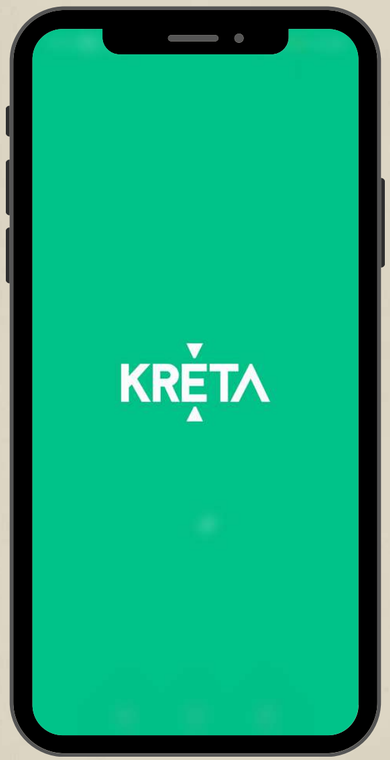


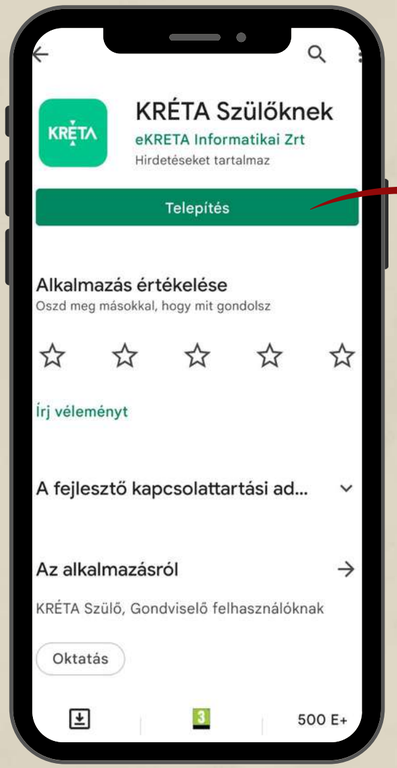
A gyerek OM azonosítójával (ez mindenkinek más, a tanodától el lehet kérni), és jelszóként a születési dátumával, kötőjellel elválasztva (például: 2010-01-01) lehet belépni.

Minden iskolának más KRÉTA oldala van, csak az iskola saját KRÉTA oldalán lehetséges a belépés!

A Kréta Elektronikus ellenőrző használata mobiltelefonon

Az Android, iOS és Huawei eszközökre elérhető KRÉTA Mobil alkalmazások azon intézmények diákjainak és szülőinek nyújt hasznos segítséget, melyek használják a KRÉTA e-naplóját. A rendszer segítséget nyújt a diákok tanulmányi előmenetelének hatékony ellenőrzésében és a kapcsolódó adminisztráció elvégzésében.





Töltsd le az alkalmazást. A letöltés után nyisd meg az alkalmazást, és telepítsd onnan.

A KRÉTA mobil alkalmazásba azzal a tanulói vagy szülői felhasználónévvel és jelszóval kell belépni, mint a webes felületen.

A Kréta Elektronikus ellenőrző használata mobiltelefonon

Az alkalmazás segítségével a felhasználók megtekinthetik a tanulók órarendjét, bejelentett számonkéréseit, házi feladatait, értékeléseit, mulasztásait és egyéb, a tanulókkal kapcsolatos információkat.

A belépéshez szükséges adatok adminisztrációját a tanuló intézményében végzik.

MARADJ BIZTONSÁGBAN A KÖZÖSSÉGI MÉDIÁBAN

https://safety.google/security/security-tips/

https://us.norton.com/internetsecurity-privacy-password-security.html

https://www.kidscape.org.uk/advice/advice-for-young-people/dealing-with-cyberbullying/staying-safe-on-social-media/

https://www.facebook.com/help/122006714548814

ADATVÉDELEM & DIGITÁLIS LÁBNYOM

https://www.gov.uk/data-protection

https://www.familylives.org.uk/advice/your-family/online-safety/digital-footprints

https://www.security.org/digital-safety/

https://staysafeonline.org/online-safety-privacy-basics/5-ways-spot-phishing-emails/

HIVATKOZÁSOK

INTERNETES ZAKLATÁS ÉS ONLINE GYŰLÖLET-BESZÉD

https://www.researchgate.net/publication/358402280_Bullying_Cyberbullying_and_Hate_Speech

https://www.unicef.org/end-violence/how-to-stop-cyberbullying

https://www.kidscape.org.uk/advice/advice-for-young-people/dealing-with-cyberbullying/think-before-you-post/

https://www.brandwatch.com/reports/cyberbullying-2016/

ONLINE VÁSÁRLÁS ÉS BANKOLÁS

https://www.ageuk.org.uk/globalassets/age-uk/documents/digital-instruction-guides/a-beginners-guide-to-staying-safe-online.pdf

https://www.consumerfinance.gov/about-us/blog/online-mobile-banking-tips-beginners/

https://www.safewise.com/blog/10-cybersecurity-tips-for-online-shopping/

HIVATKOZÁSOK

SZOLGÁLTATÁSOKHOZ VALÓ ONLINE HOZZÁFÉRÉS

https://www.bdo.hu/hu-hu/aktualitasok-blog/miert-erdemes-a-maganszemelyeknek-ugyfelkaput-nyitniuk

https://regi.ugyfelkapu.magyarorszag.hu/

https://www.billingo.hu/blog/olvas/ugyfelkapu

https://edinaszamol.blog.hu/2019/08/12/hogyan_nyissak_ugyfelkaput

https://e-egeszsegugy.gov.hu/web/eeszt-information-portal/home

https://www.e-kreta.hu

https://play.google.com/store/apps/details?id=hu.ekreta.guardian&hl=en&gl=US

HIVATKOZÁSOK

SCAN ME

SCAN ME

A "DIGITALIZE - eszközök roma felnőttek számára az internet használatához és az oktatás elősegítéséhez" projekt partnerei által készült

Amaro Foro e.V.
facebook.com/AmaroForo/
instagram.com/amaro_foro/

EGYÜTT HATÓ
KÖZÖSSÉGÉPÍTŐ EGYESÜLET
facebook.com/EgyuttHato/
instagram.com/egyutthato/

NEVO PARUDIMOS
facebook.com/NevoParudimos/
instagram.com/nevoparudimos/

RROMA
facebook.com/rromassn.org/
instagram.com/rromassn/

SCAN ME

SCAN ME

SCAN ME