4. JELSZAVAK ÉS JELMONDATOK

A jelszó, egy olyan szó vagy karaktersor, amit azonosítás során használunk, annak érdekében, hogy hozzáférjünk valamilyen szolgáltatáshoz. A felhasználói név azonosítja a felhasználót, a jelszó pedig hitelesíti a személyt, igazolja, hogy jogosult a belépésre. Ha a jelszavunkat valaki megszerzi (kitalálja, feltöri), akkor be tud lépni a fiókunkba és hozzáférhet az ott tárolt információkhoz, fájlokhoz.

A JELSZÓ MEGSZERZÉSÉNEK MÓDSZEREI

Nyers erő – brute force

A módszer lényege, hogy egy jelszófeltörő program szisztematikusan végigpróbálja az összes lehetséges kombinációt.

- Egy olyan jelszónak, ami négy karakterből és számokból áll (mint pl. a PIN kódok) 10.000 lehetséges változata van és viszonylag könnyen feltörhető.
- Egy olyannak, ami 8 karakterből áll, kisbetűket és számokat is tartalmaz már 2,8 billió kombinációja. Ennek feltöréséhez néhány óra is elegendő lehet.
- Egy olyannak, ami 12 karakterből áll, nagybetűket, kisbetűket és számokat, valamint egyéb karaktereket is tartalmaz: 96^{12} azaz 621 trilliárd. Ennek feltörése a jelenleg elérhető legnagyobb teljesítményű számítógéppel is több mint 63 ezer évig tartana.

Az internetes felhasználói fiókok esetében sok esetben néhány sikertelen próbálkozás után a rendszer letiltja a felhasználói fiókot. Ilyenkor új jelszót kell generálni.

Szótár használata

Egy, már ismert jelszavakat tartalmazó lista elemeit próbálgatja végig a támadó egy program segítségével.

Ha a jelszó rövid és szokásos szó, akkor viszonylag könnyen feltörhető.

Ez könnyen kivédhető, ha hosszabb kifejezést választ (pl. jelmondatot) vagy nem szokásos karaktersort, ami kisbetűt, nagybetűt, számot és egyéb karaktert is tartalmaz, ezt viszont nehéz megjegyezni.

JELSZAVAK ÉS JELMONDATOK

A jó jelszó

- inkább hosszú, mint bonyolult,
- nem köthető a személyhez: nem tartalmazza a felhasználó nevét, születési dátumát, házi kedvencét, kedvenc csapatának vagy előadójának nevét,
- nem tartalmaz egymást követő betűket vagy számokat pl: qwertz, abc123.

Az ilyen jelszavak megjegyzése elég nehézkes, különösen, ha minden fiókhoz egyedi jelszót használunk, ahogy az egyébként ajánlott.

Ennek kiküszöbölését segíti, ha egy jelmondatot, több értelmes szóból álló kifejezést használunk. Ez akár lehet valamelyik irodalmi műből származó, általunk kedvelt idézet is.

KIBERBIZTONSÁGI TIPPEK

JELSZÓKEZELŐ PROGRAMOK

Minden oldalhoz egyedi, hosszú és értelmetlen jelszó megjegyzése gyakorlatilag lehetetlen. Ebben segítenek a jelszókezelő programok. Ezek minden egyes általunk használt oldalhoz megjegyzik a felhasználói nevet és a jelszót, és az oldalra történő belépéskor a böngészővel együttműködve kitöltik a megfelelő mezőket. Ahol erre nincs lehetőség, a felhasználónév és jelszó a vágólap segítségével beilleszthető a megfelelő helyre.

A felhasználói neveket és jelszavakat, mint egy trezorban, titkosítva tárolják egy mesterjelszó segítségével, így csak ezt kell megjegyezni. A trezorba való belépéshez – a titkosítás feloldásához – meg kell adni a mesterjelszót. Ha kilépünk a böngészőből vagy újraindítjuk a számítógépet, a mesterjelszót ismét meg kell adni.

A jelszókezelő programok segítségével minden egyes oldalhoz, megfelelően összetett és megfelelően hosszú jelszavakat használhatunk. A programok elérhetőek a különböző számítógépes és telefonos operációs rendszerekre, és egyes programok alkalmasak arra, hogy a különböző eszközök között szinkronizálják a tárolt felhasználói neveket és jelszavakat.

AJÁNLOTT JELSZÓHASZNÁLATI PROTKOLL

- Használjon jelszókezelő alkalmazást! Válasszon hosszú, de könnyen megjegyezhető jelszót mesterjelszónak!
- Használjon erős (hosszú és bonyolult) jelszót a közösségi oldalakhoz (Google, Facebook), azt tárolja jelszókezelő alkalmazásban!
- Használja a Single Sign On szolgáltatást: Google/Facebook fiók használata más honlapokon való belépésre!
- Ahol erre nincs lehetőség, ott állítson be erős és honlaponként/felhasználói fiókonként különböző jelszót, és ezeket tárolja a jelszókezelő alkalmazásban!
- Jelszavait tartsa titokban, azokat ne ossza meg másokkal és ne tegye azokat hozzáférhetővé mások részére!
- A böngészőben ne mentse el a jelszavakat, különösen nem nyilvános számítógépen!

TOVÁBBI INFORMÁCIÓK ÉRHETŐEK EL AZ ALÁBBI LINKEKEN

www.police.hu/hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag

www.facebook.com/internettudatosan

INTERNET ONLINE IS BIZTONSÁGBAN TUDATOSAN

Országos Rendőr-főkapitányság

5. FELHASZNÁLÓI FIÓKOK BIZTONSÁGA

A felhasználói fiókok (pl. közösségi oldal, levelezési fiókok) védelme a tárolt adatok, információk, fényképek, videók miatt különösen fontos. Ha illetéktelen személy lép be a felhasználói fiókba, az ott tárolt információkat ugyanúgy láthatja, még ha azokat nem is osztotta meg a profil tulajdonosa. A megszerzett információkkal visszaélhetnek, nagy nyilvánosság részére közzé tehetik vagy akár zsarolhatják is vele az áldozatot.

A felhasználói fiókok védelmének célja, hogy csak a jogosult tudjon belépni és hozzáférni a fiókban tárolt adatokhoz.

ELEMEI:

- megfelelő **JELSZÓ** és a jelszó védelme,
- **KÉTFAKTOROS HITELESÍTÉS**,
- **MUNKAMENET LEZÁRÁSA** – kilépés a fiókból.

A megfelelő jelszóról részletesebben a JELSZAVAK kiadványban olvashat.

BIZTONSÁGI TANÁCSOK

- Mindig válasszon megfelelő jelszót!
- Ha lehet, kapcsolja be a kétfaktoros hitelesítést!
- Nem kizárólagosan használt számítógépen lépjen ki a felhasználói fiókból! A böngésző bezárása nem mindig elég!
- Okostelefonján, tabletjén állítson be képernyőzárat!
- Jelszavát mindig tartsa titokban, ne adja meg senkinek!

KÉTFAKTOROS HITELESÍTÉS

A kétfaktoros hitelesítés azt jelenti, hogy a hagyományos **FELHASZNÁLÓI NÉV – JELSZÓ PÁROS** mellett a rendszer még egy **MÁSIK MÓDON** is hitelesíti a felhasználót. A hitelesítés módja lehet:

- **BIOMETRIKUS HITELESÍTÉS**: arc, ujjlenyomat, retina,
- **TUDÁS ALAPÚ HITELESÍTÉS**: jelszó, válasz, PIN kód, minta,
- **BIRTOKLÁS ALAPÚ HITELESÍTÉS**: token, kártya.

A felhasználó név – jelszó páros tudás alapú hitelesítésnek minősül.

Ha a második hitelesítés módja megegyezik az elsődleges hitelesítés módjával, jelen esetben az is tudásalapú, akkor kétlépcsős hitelesítés történik, ha a második módja eltér az elsődlegesétől, (pl. biometrikus vagy birtoklás alapú hitelesítés), akkor beszélünk kétfaktoros hitelesítésről.

A kétfaktoros hitelesítés nagyobb biztonságot nyújt a felhasználói fiókokra. Jellemzően új, korábban nem használt eszközön történő belépéskor használandó. Az általunk rendszeresen használt eszközökön **KIKAPCSOLHATÓ**, meggyorsítva ezzel a belépés folyamatát.

KIBERBIZTONSÁGI TIPPEK

A kétfaktoros hitelesítés általában a felhasználó okostelefonjának segítségével történik, legbiztonságosabb, ha valamilyen alkalmazáson keresztül. Ez lehet a szolgáltatás **SAJÁT ALKALMAZÁSA** (Facebook, Google vagy az adott bank applikációja). Ebben az esetben az alkalmazásban lehet jóváhagyni a másik eszközön (pl. számítógépen) történő bejelentkezést.
Léteznek **AUTENTIKÁCIÓS ALKALMAZÁSOK**, amelyekben egy **QR KÓD** segítségével lehet rögzíteni az adott oldalt, és bejelentkezéskor az adott oldalhoz rendelt – rendszeres időközönként változó – kódot kell megadni a másik eszközön.
Az oldal küldhet egyszeri alkalomra szóló hitelestő kódot **SMS-BEN VAGY E-MAILBEN**. Ezek kevésbé biztonságosak, mint az előző megoldások.

A különböző szolgáltatók kétfaktoros hitelesítést hívják **KÉTFAKTOROS VAGY KÉTLÉPCSŐS AZONOSÍTÁSNAK** is. Az eltérő elnevezés ellenére ugyanarról a technikai megoldásról van szó.

MUNKAMENET LEZÁRÁSA

A nem kizárólag általunk használt számítógépen (iskolában, munkahelyen, ismerősnél, nyilvános helyen) mindig **JELENTKEZZÜNK KI** a felhasználói fiókból, a böngésző **BEZÁRÁSA NEM ELEGENDŐ**, mivel az oldal újbóli megnyitása esetén belép az utóljára használt felhasználói fiókba. Egy ilyen számítógépeken a felhasználói nevünket és jelszavunkat se jegyeztessük meg a böngészővel! Célszerű a böngésző **PRIVÁT/ INKOGNITÓ MÓDJÁNAK** használata. Ebben az esetben a böngésző nem menti a böngészési előzményeket, a cookie-kat, a webhelyadatokat és az űrlapokon megadott adatokat.
A privát/inkognitó mód bekapcsolása:

- Internet Explorer: CTRL+SHIFT+P
- Mozzila Firefox: CTRL+SHIFT+P
- Chrome: CTRL+SHIFT+N

TOVÁBBI INFORMÁCIÓK ÉRHETŐEK EL AZ ALÁBBI LINKEKEN

www.police.hu/hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag

www.facebook.com/internettudatosan

INTERNET ONLINE IS BIZTONSÁGBAN TUDATOSAN
Országos Rendőr-főkapitányság

6. ADATHALÁSZAT

Személyes és pénzügyi adataink komoly értéket képviselnek. Ha ezek illetéktelen személyek részére hozzáférhetővé válnak, az komoly anyagi károkat is okozhat. A bűnözők megtévesztő e-mailek és közösségi oldalakon keresztül küldött üzenetek segítségével próbálnak meg hozzájutni a felhasználók adataihoz. Az e-maileket és üzeneteket nagyon sok embernek elküldik, bízva abban, hogy néhányan bedőlnek és megadják az adataikat.

Az adathalászok jellemzően egy **HAMISÍTOTT WEBOLDALON** keresztül próbálnak személyes és pénzügyi adatokhoz (tipikusan felhasználói név, jelszó, bankkártya-adatok) jutni. Megbízható szervezetek, bankok, elektronikus kereskedelemmel foglalkozó weboldalak, online fizetési szolgáltatók ismertségét kihasználva, azok weboldalait **LEMÁSOLVA** igyekeznek a felhasználók bizalmába férkőzni. A csalók **E-MAILT** vagy közösségi oldalon, illetve egyéb üzenetküldő szolgálatáson keresztül **ÜZENETET KÜLDENEK** a címzettnek, amiben ráveszik az e-mailben vagy üzenetben szereplő **HIVATKOZÁS** követésére. Arra kérik a felhasználót, hogy **JELENTKEZZEN BE** valamilyen megbízható szervezet (levelezési szolgáltató, PayPal, eBay, bank, stb.) honlapjához nagyon hasonlító weboldalra, amit azonban a csalók üzemeltetnek, és az itt megadott személyes és pénzügyi adatok a csalókhoz kerülnek.

BIZTONSÁGI TANÁCSOK

- Mindig **ELLENŐRIZZE**, hogy valóban a feladónak tűnő személy, szervezet küldte-e az e-mailt!
- A bankok **NEM KÉRNEK** e-mailben bankkártya-adatokat, más szervezeteknek pedig ne adjuk meg azokat!
- Online bankkártyás fizetésnél mindig **GYŐZŐDJÜNK** meg arról, hogy valódi bank oldalon adjuk meg az adatokat, más oldalon (pl. kereskedő oldalán) ne adjuk meg azokat!
- Amikor belépünk egy banki vagy bármilyen más oldalra, **GYŐZŐDJÜNK** meg arról, hogy az valóban ahhoz **SZERVEZETHEZ TARTOZIK.** Felhasználói nevet és jelszót csak tanúsítvánnyal rendelkező (**HTTPS** előtag) oldalon adjunk meg!

TIPIKUS ÜZENETEK

- **FRISSÍTSE JELSZAVÁT** az alábbi linken!
- **LÉPJEN BE A FIÓKJÁBA**, ellenkező esetben 24 órán belüli törlődik!
- A mellékelt számla befizetéséhez a linken **ADJA MEG A BANKKÁRTYA-ADATAIT**!

KIBERBIZTONSÁGI TIPPEK

ÁRULKODÓ JELEK: E-MAILEK, ÜZENETEK

Bár az adathalász e-mailek és üzenetek egyre kifinomultabbak, azért viszonylag könnyű felismerni, hogy az e-mailt vagy üzenetet csalók küldték:

- a küldő e-mail címe bár **HASONLÍT** valamelyik megbízható szervezetéhez, attól eltér:
  - a második szintű tartomány névben: google helyett gooogle vagy g00gle,
  - legfelső szintű tartomány nevében (.hu, .com, stb.) google.com helyett google.xyz,
- a szervezet **HIVATALOS** e-mail címe helyett **PRIVÁT** e-mailről érkezik: pl. support@paypal.com helyett paypal@gmail.com,
- olyan szolgáltató nevében küldték ki, akivel **NEM ÁLLUNK** kapcsolatban,
- a levélben használt **MEGSZÓLÍTÁS ÁLTALÁNOS**, nem szerepel benne a címzett neve,
- a szöveg **HELYESÍRÁSI, NYELVHELYESSÉGI HIBÁKAT** tartalmaz, magyartalan, valószínűsíthető, hogy fordítóprogrammal készült,
- bár a megadott link látszólag hasonlít az eredeti oldal címére, a kattintás után a **CÍMSORBAN** teljesen más jelenik meg.

ÁRULKODÓ JELEK: ADATHALÁSZ WEBOLDALAK

Az áloldalak sok esetben kinézetükben, szerkezetükben nagyon **HASONLÍTANAK** az eredeti oldalhoz, más esetben csak a szervezet arculati elemeit (színek, logók) alkalmazzák egyszerűsített formában. Vannak az olyan egyértelmű jelek, amelyek jelzik, hogy áloldalról van szó.

- A böngésző címsorában nem a szervezet **HIVATALOS HONLAPJÁNAK** internetes (URL) címe szerepel, hanem teljesen ismeretlen, a hivatalos oldal címére esetleg hasonlító más szöveg.
- Az URL címben **HTTPS HELYETT CSAK A HTTP** szerepel, vagyis az oldal nem rendelkezik tanúsítvánnyal és a felhasználó számítógépe és az oldal közötti kommunikáció sem titkosított.
- A megbízható tanúsítványnyal rendelkező oldalakat a böngészők általában jelzik (általában **KIS LAKATTAL**), illetve **ZÖLD JELZÉSSEL** a böngésző címsorában.

TOVÁBBI INFORMÁCIÓK ÉRHETŐEK EL AZ ALÁBBI LINKEKEN

www.police.hu/hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag

www.facebook.com/internettudatosan

INTERNET ONLINE IS BIZTONSÁGBAN TUDATOSAN

Országos Rendőr-főkapitányság

7. A SZEMÉLYES ADATOK VÉDELME

Az online jelenlét ún. digitális lábnyomot hoz létre, amely tartalmazhat a személyre (pl. személyes adatok, képmás), internet használati szokásokra (pl. érdeklődési körre) vonatkozó, valamint egyéb, személyhez kötődő (pl. pénzügyi) adatokat. Ezek egy része ún. aktív nyom, amelyeket a felhasználó maga oszt meg (pl. egy közösségi oldalon) másik részük passzív nyom, amelyek gyűjtése a felhasználó aktív közreműködése nélkül történik (pl. látogatott oldalak naplózása). A személyes adatokhoz vagy egyéb információkhoz történő illetéktelen hozzáférés komoly veszélyeket jelent a felhasználókra.

FÉNYKÉPEK A NETEN

Egy fénykép online **MEGOSZTÁSA** témája (jellemzően személy vagy tárgy) miatt, már önmagában is kérdéses lehet. A témán kívül azonban a kép tartalmazhat olyan **INFORMÁCIÓKAT**, amiket már nem biztos, hogy szeretnénk megosztani. A képen a téma mellett a **HÁTTÉR VAGY A KÖRNYEZET** is árulkodó lehet a személyünkkel kapcsolatban és hasznos információkat szolgáltathat rosszszándékú emberek számára.

A digitális fényképezők (és így a mobiltelefonok is) számos információt tárolnak el az általuk készített képfájlokban (fényképekben). Ezeket az adatokat **EXIF ADATOKNAK** hívjuk. Tartalmazzák (többek között):

- kép készítésének **DÁTUMÁT ÉS IDŐPONTJÁT**,
- a fényképezőgép vagy telefon **GYÁRTÓJÁNAK NEVÉT, TÍPUSÁT**,
- kép készítésének **FÖLDRAJZI HELYÉT** (a GPS-szel fel-szerelt készülékeken)

Ezek szintén olyan információk, amelyek megosztása súlyos kockázatot jelent.

AMIT BIZTOS NE OSSZON MEG!

- teljes születési dátum,
- aktuális helyzet, különösen nyaralás vagy hosszabb távollét esetén,
- lakcím, telefonszám
- családi állapot és családi kapcsolatok,
- képek a gyermekekről, különösen névvel megjelölve,
- képek földrajzi hely információval,
- utazási tervei,
- olyan információk, amiket nem osztana meg családjával, munkatársaival vagy a szomszédjaival,
- munkájával kapcsolatos aktualitások.

KIBERBIZTONSÁGI TIPPEK

KOCKÁZATOK

Az egy személyre **ÖSSZEGYŰJTÖTT ADATOK** alapján vizsgálható a személy viselkedése, meghatározhatóak a **SZOKÁSAI**, kellő mennyiségű adat esetében viszonylag pontosan megalkotható akár a személy pszichológiai **PROFILJA** is.

Hosszabb időn keresztül történő adatgyűjtést követően az érintett személy **ÉLETTÖRTÉNETE** is megrajzolható.

A megosztott személyes adatok és információk birtokában (születési hely, idő, családi kapcsolatok, lakcím, képmás) bűnözők magukat a sértettnek adhatják ki (**SZEMÉLYISÉGLOPÁS**), és ezzel erkölcsi, illetve anyagi **KÁRT OKOZHATNAK**.

A megosztott képek **ZAKLATÁS,** gúnyoldás célpontjává tehetik a felhasználót.

MEGOSZTÁS A KÖZÖSSÉGI OLDALAKON

- Ne legyen nyilvános a profilja, a személyes adatait, a megosztott tartalmakat csak az ismerősei láthassák!
- Csoportosítsa ismerőseit és ezáltal korlátozhatja, hogy ki mit láthat!
- Állítsa be, hogy csak a jóváhagyása után jelölhessék meg egy posztban!
- Korlátozza az idővonala láthatóságát, és azt hogy ki tehet tartalmat közzé rajta!
- Ismerősei körét idegenek ne láthassák!
- Egyéb oldalra vagy alkalmazásba közösségi profiljával történő bejelentkezés során ellenőrizze, hogy az oldal vagy alkalmazás milyen személyes adatához fér hozzá (születésnap, e-mail cím, ismerőseinek köre stb.)! Szükség esetén módosíthatja az elérhető információk körét. A hozzáférést az adatvédelmi beállításokban ellenőrizheti, visszavonhatja vagy módosíthatja!

AMIT KÉT EMBER TUD, AZ MÁR NEM TITOK!

A MEGOSZTOTT INFORMÁCIÓ FELHASZNÁLÁSÁT NEM LEHET KONTROLLÁLNI.

AZ INTERNET NEM FELEJT. AMI EGYSZER FELKERÜL, AZ OTT IS MARAD.

TOVÁBBI INFORMÁCIÓK ÉRHETŐEK EL AZ ALÁBBI LINKEKEN

www.police.hu/hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag

www.facebook.com/internettudatosan

INTERNET ONLINE IS BIZTONSÁGBAN TUDATOSAN

Országos Rendőr-főkapitányság

8. BIZTONSÁGBAN A KÖZÖSSÉGI OLDALAKON

A közösségi oldalak kiváló lehetőséget biztosítanak az ismerőseinkkel való kapcsolattartásra, arra, hogy a velünk kapcsolatos információkat, eseményeket, élményeket barátainkkal, családtagjainkkal megosszuk. Segítségükkel a kommunikáció könnyebbé vált, a megosztott személyes információk mennyisége ugrásszerűen megnőtt. A közösségi oldalak az előnyök mellett ugyanakkor kockázatot is jelentenek a felhasználóknak.

SZEMÉLYES ADATOK MEGOSZTÁSA

- A közösségi oldalak lehetőséget biztosítanak a **SZEMÉLYES ADATAINK** megadására, amelyek nem megfelelő biztonsági beállítások esetén mások, akár idegen részére is **LÁTHATÓAK** lesznek.
- Mindig mérlegelje, hogy milyen személyes adatot ad meg, és azt is, hogy azt ki láthatja!
- A személyes adatok, mint a születési hely, idő vagy lakcím, családi kapcsolatok visszaélésre adnak lehetőséget, így ezeket láthatóságát érdemes **KORLÁTOZNI**.

AMIT BIZTOS NE OSSZON MEG!

- teljes születési dátum,
- aktuális helyzet, különösen nyaralás vagy hosszabb távollét esetén,
- lakcím, telefonszám
- családi állapot és családi kapcsolatok,
- képek a gyermekekről, különösen névvel megjelölve,
- képek földrajzi hely információval,
- utazási tervei,
- olyan információk, amiket nem osztana meg családjával, munkatársaival vagy a szomszédjaival,
- munkájával kapcsolatos aktualitások.

BEJEGYZÉSEK MEGOSZTÁSA

- Egy bejegyzés, fénykép, szintén tartalmazhat olyan információt, ami **VISSZAÉLÉSHEZ VAGY ZAKLATÁSHOZ** vezethet. Gondolja végig, hogy tényleg **SZÜKSÉGES-E** a bejegyzést, fényképet megosztani, illetve, hogy azt **KIVEL OSZTJA MEG**!
- Több közösségi oldalon lehetőség van arra, hogy a bejegyzést csak az **ISMERŐSEI EGY RÉSZÉVEL** (pl. közeli családtagok) ossza meg.
- A feltöltött információ, fénykép interneten történő terjedését nem tudjuk kontrollálni, így az **ELJUTHAT IDEGENEKHEZ** is.

KIBERBIZTONSÁGI TIPPEK

FELHASZNÁLÓI FIÓKOK BIZTONSÁGA

A felhasználói fiókok (pl. közösségi oldalak, levelezési fiókok) védelme az ott tárolt **ADATOK, INFORMÁCIÓK,** fényképek videók miatt különösen fontos. Ha illetéktelen személy lép be a felhasználói fiókba, az ott tárolt információkat ugyanúgy **LÁTHATJA**, még akkor is, ha azokat a profil tulajdonosa nem osztotta meg. A megszerzett információkkal **VISSZAÉLHETNEK**, nagy nyilvánosság részére **KÖZZÉ TEHETIK** vagy akár **ZSAROLHATJÁK** is vele az áldozatot.

Az illetéktelen hozzáférés megelőzése érdekében válasszon **MEGFELELŐ JELSZÓT**, amely nem kapcsolódik a személyéhez. A különböző oldalak többféle lehetőséget biztosítanak a felhasználói fiókok védelmére. Ismerje meg ezeket, válassza ki az Önnek megfelelőt!

A nem kizárólagosan használt számítógépen (iskolában, munkahelyen, ismerősnél, nyilvános helyen) mindig **JELENTKEZZEN KI** a felhasználói fiókból, a böngésző bezárása nem elegendő, mivel az oldal újbóli megnyitása esetén belép az utoljára használt felhasználói fiókba. Az ilyen számítógépeken a felhasználói nevét és jelszavát soha ne jegyeztesse meg a böngészővel!

BIZTONSÁGI TANÁCSOK

- **NE LEGYEN NYILVÁNOS** a profilja, a személyes adatait, a megosztott tartalmakat csak az ismerősei láthassák!
- **CSOPORTOSÍTSA** ismerőseit és ezáltal korlátozhatja, hogy ki mit láthat!
- Állítsa be, hogy a **JÓVÁHAGYÁSA** után jelölhessék meg egy posztban!
- Korlátozza az **IDŐVONALA LÁTHATÓSÁGÁT**, és azt is, hogy ki tehet tartalmat közzé rajta!
- Ismerősei körét **IDEGENEK** ne láthassák!
- Egyéb oldalra vagy alkalmazásba közösségi profiljával történő bejelentkezés során ellenőrizze, hogy az oldal vagy alkalmazás milyen személyes adatához **FÉR HOZZÁ**. (születésnap, e-mail cím, ismerőseinek köre, stb.)!
- Szükség esetén **MÓDOSÍTHATJA** az elérhető információk körét. A hozzáférést az adatvédelmi beállításokban ellenőrizheti, visszavonhatja vagy módosíthatja!

ZAKLATÁS

Az egyszerű kommunikációnak köszönhetően a közösségi oldalak színterei lehetnek az online zaklatásnak. A zaklatás megvalósulhat **BÁNTÓ, FENYEGETŐ, GÚNYOLÓDÓ** személyes üzenetek vagy egy csoportban írt hozzászólások formájában. Az ilyen bejegyzéseket **JELENTENI** lehet az oldal üzemeltetőjének. Javasoljuk, hogy készítsen róluk **KÉPERNYŐMENTÉST**, **SZAKÍTSA MEG A KAPCSOLATOT** a zaklatóval, tiltsa le, hogy ne léphessen kapcsolatba Önnel! Ha folytatja (más felhasználói fiókkal vagy más csatornán), forduljon a **RENDŐRSÉGHEZ**!

INTERNET ONLINE IS BIZTONSÁGBAN TUDATOSAN
Országos Rendőr-főkapitányság

KIBERBIZTONSÁGI TIPPEK

CSALÁSOK

A közösségi oldalak lehetővé teszik, hogy **IDEGENEK** is kapcsolatban lépjenek velünk. A rólunk közzétett információk alapján könnyen **CSALÓK CÉLTÁBLÁJÁVÁ** válhatunk. Tipikus elkövetési forma, hogy nagyon kedvező **ÜZLETI LEHETŐSÉGET** kínálnak, minimális befektetéssel lehet szert tenni jelentős haszonra, vagy külföldi, jól fizető munkát ajánlanak némi közvetítői díjért cserébe. Óvakodjon az ilyen ajánlatoktól, mert ezek jellemzően csalóktól érkeznek!

A csalások másik formája az **ONLINE NYEREMÉNYJÁTÉKKAL** kapcsolatos. A csalók azzal keresik meg a kiszemelt áldozatot, hogy valamilyen nyereményjátékon nyert, de a nyeremény véglegesítéshez szükség van arra, hogy feltöltse egy **TELEFONKÁRTYA EGYENLEGÉT** vagy egy **ÜZENETET KÜLDJÖN** el egy telefonszámra (ez szintén egyenleget tölt fel a saját számlánk terhére). Ne dőljön be az ilyen ajánlatoknak!

TOVÁBBI INFORMÁCIÓK ÉRHETŐEK EL AZ ALÁBBI LINKEKEN

www.police.hu/hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag

www.facebook.com/internettudatosan

INTERNET ONLINE IS BIZTONSÁGBAN TUDATOSAN

Országos Rendőr-főkapitányság

9. BIZTONSÁGOS ONLINE VÁSÁRLÁS

Az internet elterjedésének köszönhetően az online vásárlás és az online fizetés is egyre népszerűbb. Amíg a valós életben a fizetés előtt személyesen is meg tudjuk nézni a kiválasztott terméket, addig az online vásárlásnál erre nincs lehetőségünk, ezért ez nagyobb kockázatot jelent. Ezt azonban megfelelő, tudatos magatartással, körültekintéssel csökkenthetjük, és élvezhetjük az online vásárlás nyújtotta előnyöket.
Az internetes vásárlásnak alapvetően két fajtája van: a webáruházakban és az online piactereken történő vásárlás. A webáruházakban általában a kereskedők új terméket árulnak, számlával, jótállással. Az online piactereken viszont sok esetben használt termékek szerepelnek, számla és jótállás nélkül. Így az áruk is alacsonyabb, de a vásárlásnál ezt mindig tartsuk szem előtt.

BIZTONSÁGI TANÁCSOK

- Kevésbé ismert webáruház esetén **ELLLENŐRIZZE** az üzemeltető adatait, a kapcsolattartási adatokat és a vásárlási feltételeket!
- Nézzen után a webáruház **ÉRTÉKELÉSÉNEK** az interneten!
- Online piactéren **ELLENŐRIZZE** az eladót (visszajelzések, közzétett adatok alapján)!
- Bankkártyaadatait csak a **BANK ONLINE FIZETÉSRE LÉTREHOZOTT OLDALÁN** adja meg (kereskedő oldalán vagy e-mailben soha)!
- Ellenőrizze, hogy a fizetésre használt oldal **VALÓDI BANKI OLDAL-E**, rendelkezik-e tanúsítvánnyal?
- Ha lehet, válassza a **SZEMÉLYES ÁTVÉTELT**!

VÁSÁRLÁS WEBÁRUHÁZBAN

Az online vásárlások jelentős része **WEBÁRUHÁZAKON** keresztül történik. A jól ismert, nagy webáruházak alapvetően biztonságosak, de vásárlás előtt **ELLENŐRIZZE AZ OLDAL URL-JÉT**, hogy valóban megfelelő helyen jár-e! A fizetés történhet átutalással, bankkártyával banki oldalon keresztül, fizetési közvetítővel, virtuális vagy fizetési közvetítő által kibocsátott kártyával.

Kevésbé ismert webáruház esetén ellenőrizze az **ÜZEMELTETŐ ADATAIT, A KAPCSOLATTARTÁSI ADATOKAT ÉS A VÁSÁRLÁSI FELTÉTELEKET**! Az üzemeltető lehet cég vagy magánszemély (egyéni vállalkozó), az oldalon fel kell tüntetni a címet, az adószámot és a cégjegyzékszámot, illetve a csomagküldésre jogosító nyilvántartási számot. Nézzen utána a webáruház **ÉRTÉKELÉSÉNEK** az interneten! Javasolt a személyes átvétel vagy az utánvétellel történő vásárlás.

KIBERBIZTONSÁGI TIPPEK

VÁSÁRLÁS ONLINE PIACTÉREN

Az online piacterek esetében az eladó és a vevő az oldalon belül kommunikálnak, a fizetés az oldalon kívül, átutalással vagy utánvétellel történik. A felhasználók **ÉRTÉKELÉST** készítenek a másik félről, ezek alapján körültekintően kell kiválasztani az eladót. Javasolt az utánvétellel történő vásárlás vagy a személyes átvétel.

SZEMÉLYES ÁTVÉTEL

Az online vásárlás legnagyobb kockázata, hogy megkapom-e a pénzemért a kiválasztott árut, illetve azt kapom-e, olyan minőségben, amit kiválasztottam. A webáruházakban és az online piactereken keresztül történő vásárlásoknál többnyire van lehetőség arra, hogy a terméket **SZEMÉLYESEN** vegyük át, a helyszínen fizetve. Ez a legbiztonságosabb, hiszen a fizetés előtt láthatja az árut, és ha az nem felel meg az elképzeléseinek, elállhat a vásárlástól. Online piactér esetében az elállásnak lehetnek negatív következményei, ezért a licitálás előtt **KÉRJEN RÉSZLETES TÁJÉKOZTATÁST** a termékről, így csak akkor kell elállnia, ha a tájékoztatás nem felelt meg a valóságnak.

CSOMAGKÜLDÉS

Nem mindig van lehetőség a személyes átvételre (pl. távolság miatt, webshop esetében üzlethelyiség hiánya), ilyenkor marad a postai út. A megrendelés (licitálás) előtt mindig **TÁJÉKOZÓDJON** a **JÓTÁLLÁS FELTÉTELEIRŐL, SZÁLLÍTÁSI KÖLTSÉGEKRŐL ÉS A SZÁLLÍTÁS IDEJÉRŐL.** A webshopok és online piacterek használatához általában **REGISZTRÁCIÓ** szükséges, a kért adatokat (szállítási cím, e-mail, telefonszám) pontosan adja meg, hiszen ezek elengedhetetlenek az üzlet sikeres lebonyolításához.

UTÁNVÉTEL

Az áru kifizetése történhet többféleképpen. Az egyik az **UTÁNVÉTELLEL TÖRTÉNŐ FIZETÉS,** ilyenkor a kézbesítéskor a postásnak vagy a futárnak kell fizetni. Ez a szállítási díjon felül plusz költséget (általában néhány száz forintnyi összeget) jelenthet. Ebben az esetben a csomagot biztosan megkapja. Mindig ellenőrizze, hogy a **CSOMAG BONTATLAN ÉS NEM SÉRÜLT-E**! Ha felbontották vagy sérült, akkor ne vegye át, hanem küldje vissza a feladónak! Ha van lehetősége, nyissa ki és **ELLENŐRIZZE**, hogy tényleg a megrendelt áru van-e benne!

KIBERBIZTONSÁGI TIPPEK

ÁTUTALÁS

Utánvétel helyett lehetőség van az áru **ELŐRE TÖRTÉNŐ KIFIZETÉSÉRE**. Ezt megteheti átutalással, ebben az esetben kap egy előlegszámlát, amin szerepel a számlaszám és az átutalandó összeg. Ezt akár személyesen a bankjában vagy az interneten keresztül is átutalhatja.

BANKKÁRTYA HASZNÁLAT

Az átutalás mellett sok esetben lehet **BANKKÁRTYÁVA**l fizetni az interneten keresztül. Ehhez általában dombornyomott kártyára van szükség, de vannak olyan nem dombornyomott kártyák is, amelyekkel lehet így fizetni. Egyes bankok bocsátanak ki **VIRTUÁLIS KÁRTYÁKAT**, amelyekre előzőleg a kívánt összeget a vásárlás előtt fel tudjuk tölteni, így vásárlás után nem marad rajta pénz. Fizetési közvetítő (Curve, Revolut) által kibocsátott kártyával is fizethet.

A bankkártyás fizetésnél meg kell adni a **KÁRTYA ADATAIT** (bankkártya típusa, száma, tulajdonos neve, lejárati ideje és a hátoldalon található biztonsági kódot). Ezek ismeretében visszaélésre nyílna lehetőség, hiszen a jövőben, aki ismeri ezeket az adatokat, szintén tudna vásárolni. Ennek kiküszöbölése érdekében csak **BANK VAGY FIZETÉSI KÖZVETÍTŐ** által működtetett **BIZTONSÁGOS OLDALON VAGY MOBILALKALMAZÁSBAN** adja meg ezeket az adatokat. Fizetéskor **ELLENŐRIZZE** a böngésző címsorban, hogy valóban a bank fizetési oldalán van. A **TANÚSÍTVÁNY** megléte csak azt garantálja, hogy a kapcsolat a számítógép és az oldal között megfelelően titkosított, az elküldött adatokat nem lehet visszafejteni.

FIZETÉSI KÖZVETÍTŐ

Egyes webshopokban és online piactereken van lehetőség fizetési közvetető (pl. PayPal, Barion, Upay, Simple) által történő fizetéssel. A **SZOLGÁLTATÓNÁL** a regisztráció során meg kell adni a fizetésre használt bankkártya adatait. A fizetési folyamat során a rendszer átirányít a **FIZETÉSI KÖZVETÍTŐNÉL LÉTREHOZOTT FELHASZNÁLÓI FIÓKBA**, ott a belépést követően tudja jóváhagyni a fizetést, amelynek során az összeg a korábban **REGISZTRÁLT BANKKÁRTYÁRA** terhelődik. A módszer biztonságos és egyszerű, a bankkártya-adatok nem kerülnek át a kereskedőhöz, és a bankkártyás fizetéstől eltérően nem kell minden alkalommal megadni azokat.

TOVÁBBI INFORMÁCIÓK ÉRHETŐEK EL AZ ALÁBBI LINKEKEN

www.police.hu/hu/hirek-es-informaciok/bunmegelozes/internet-biztonsag

www.facebook.com/internettudatosan

INTERNET ONLINE IS BIZTONSÁGBAN TUDATOSAN

Országos Rendőr-főkapitányság