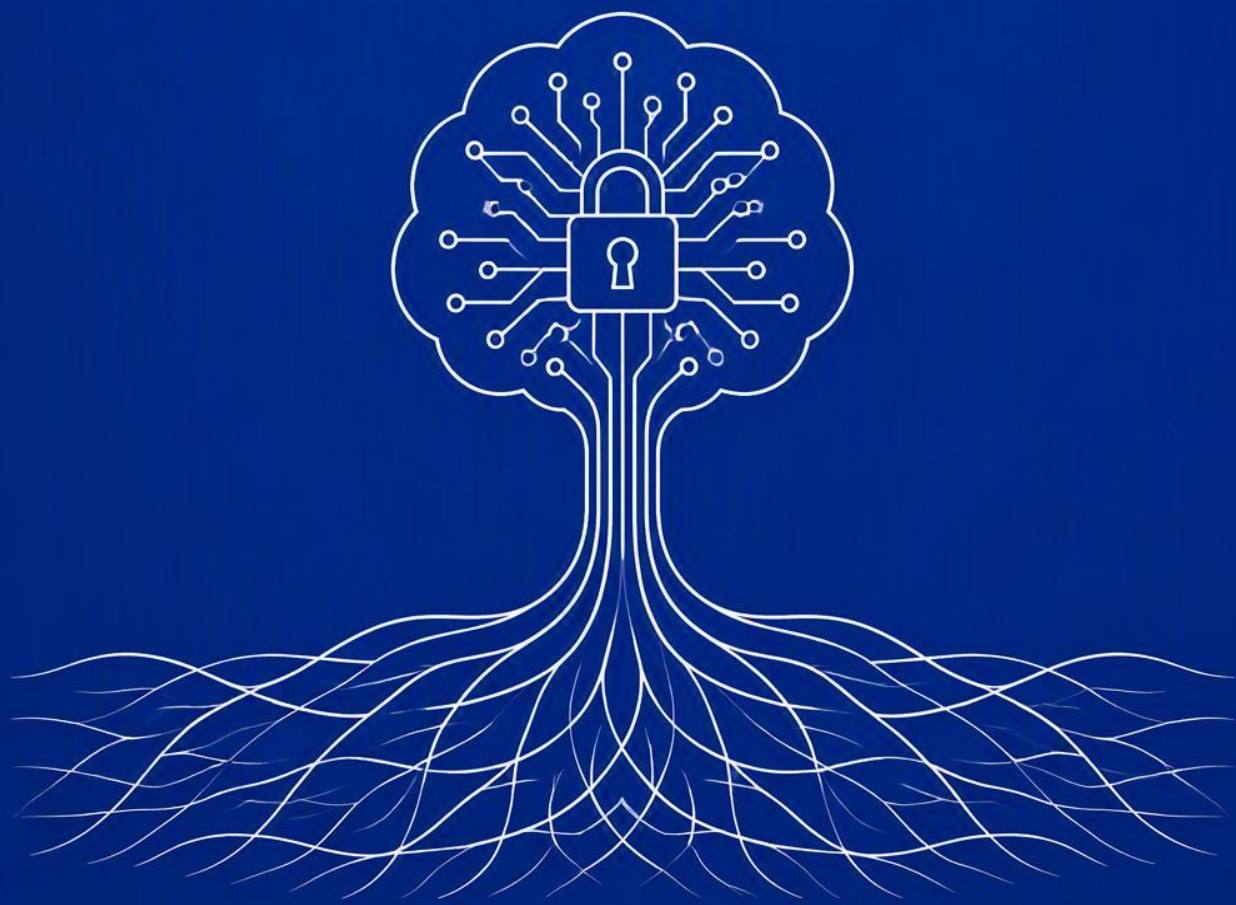




**Co-funded by
the European Union**

Digitális biztonság – útmutató civil szervezeteknek



A digitális biztonsági útmutató egy „A civil szervezetek rezilienciájának elősegítése a szűkülő mozgástérrel szemben, valamint kapacitásaik erősítése egyéni mentorálás és érték integrálása révén Magyarországon és Szlovákiában” (FOREST) című projekt keretében dolgozták ki, amelyet az Alternatív Közösségek Egyesülete (ACA), a Partners for Democratic Change Slovakia (PDCS) és a Transatlantic Foundation (TF) közösen valósított meg.

Szerző: Lukáš Zorád

Fordítás: www.gyorsforditas.hu

Közzététel: 2026. augusztus 31.



**Co-funded by
the European Union**

A FOREST projektet az Európai Unió társfinanszírozza. A cikkben kifejtett nézetek és vélemények azonban kizárólag a szerző(k) véleményét tükrözik, és nem feltétlenül egyeznek meg az Európai Unió vagy az Európai Oktatási és Kulturális Végrehajtó Ügynökség álláspontjával. Sem az Európai Unió, sem a támogatást nyújtó hatóság nem tehető felelőssé azokért.

Tartalomjegyzék

1	Kézikönyv használata	4
2	Az online biztonság alapelvei:	4
3	Adatszivárgások	5
4	Jelszavak	5
5	Adattitkosítás	7
5.1	Az eszközök titkosítása	8
5.1.1	Android esetén:	8
5.1.2	Windows esetén (csak a Professional verzióban):	9
5.1.3	Mac OS X esetén:	9
6	Kártékony szoftverek (malware).....	10
6.1	Hogyan juthat el Önhöz a kártékony szoftver?.....	11
6.2	Hogyan védekezhetünk a kártékony szoftverek ellen?	11
6.3	Hogyan kerülheti el az adathalászatot, és hogyan ismerheti fel egyáltalán?	12
6.4	Pszichológiai manipuláció (social engineering)	13
6.5	A kártékony szoftverek típusai.....	13
7	IP-cím és VPN	14
7.1	Módok, hogyan valaki megszerezheti az Ön IP-címét.....	14
7.2	VPN.....	16
8	Biztonság a közösségi hálózatokon és az adatvédelmi beállítások.....	17
9	Felhasznált források	19
10	1. melléklet: Gyakorlat: Mit vagyunk hajlandók feltölteni a közösségi médiába, és miért?	21
11	2. melléklet: Biztonsági terv tervezete.....	23

1 Kézikönyv használata

Az egyes fejezetek áttekinthetően tartalmazzák a nem kormányzati szervezetek digitális biztonságának javítását célzó tanácsokat és konkrét lépéseket. Nem szükséges a teljes kézikönyvet egyszerre elolvasni; az egyes lépések megvalósításakor elegendő a vonatkozó fejezetet kiválasztani. Ha például VPN-t szeretnék telepíteni a személyes adatok védelme és a hackertámadások megelőzése érdekében, a VPN-ről szóló fejezetet nézze meg.

2 Az online biztonság alapelvei:

Ahhoz, hogy biztonságosabban mozogjunk az interneten, érdemes megjegyeznünk ezt a négy alapelvet. Segítenek megérteni, mi történik, ennek milyen hatása lehet, és milyen lépéseket kell tennünk a biztonságunk megőrzése vagy a lehetséges károk csökkentése érdekében.

1) **Ami felkerül az internetre, az az interneten is marad, és nem névtelen.**

Az interneten közzétett információkat nagyon nehéz teljesen eltávolítani. A fényképeket, hozzászólásokat, bejegyzéseket vagy dokumentumokat mások az Ön tudta nélkül lemásolhatják, archiválhatják vagy elmenthetik. Még álnév vagy névtelen fiók használata esetén is gyakran lehetővé teszi egy konkrét személy azonosítását a különböző adatok összekapcsolása. Ezért a közzététel előtt érdemes mérlegelni, hogy az adott információ okozhat-e a jövőben problémát.

2) **A kiberbiztonság leggyengébb láncszeme az emberi tényező.**

A sikeres kibertámadások többsége nem a technológia feltörésével kezdődik, hanem az emberek megtévesztésével. A támadók a figyelmetlenséget, a kíváncsiságot, az időnyomást vagy a bizalmat használják ki annak érdekében, hogy jelszavakhoz, érzékeny adatokhoz vagy a rendszerekhez való hozzáféréshez jussanak. A legjobb technikai védelem is csődöt mondhat, ha a felhasználó csaló linkre kattint, vagy illetéktelen személynek ad meg információkat. A biztonságos felhasználói magatartás ezért ugyanolyan fontos, mint a jó minőségű szoftver.

3) **Készüljön fel arra, hogy a hackerek megtámadják — ez bizonyosan megtörtént már korábban, és meg fog történni újra.**

A támadásokkal szembeni teljes védelem nem létezik. Minden felhasználó, szervezet vagy vállalat automatizált vagy célzott támadások potenciális célpontja. Ezért nemcsak a támadások megelőzésére kell törekedni, hanem fel kell készülni arra a helyzetre is, amikor bekövetkeznek. A rendszeres frissítések, a biztonsági mentések, az erős jelszavak és a többtényezős hitelesítés jelentősen csökkentik a támadás által okozott kárt.

4) **A beépített megoldásokkal biztosított adatvédelem megbízhatóbb, mint a megígért adatvédelem.**

A magánszféra védelme során célszerűbb technikai megoldásokra támaszkodni, mint a szolgáltatók nyilatkozataira. Ha a kommunikáció titkosított, az adatkezelés minimalizált, és a biztonsági intézkedések közvetlenül a rendszerbe vannak beépítve, a védelem nem csupán az üzemeltető jóindulatán múlik. Az adatvédelemre vonatkozó ígéretek idővel változhatnak, a technikai biztosítékok viszont konkrét és ellenőrizhető szintű védelmet nyújtanak.

3 Adatszivárgások

Azt, hogy adatszivárgás következtében sérült-e valamelyik fiókja, a következő oldalon ellenőrizheti: <https://haveibeenpwned.com/>. Ez egy olyan felület, amely ma már közvetlenül a Firefox böngészőbe is beépült, és ahol biztonsági értesítéseket állíthat be arra az esetre, ha a jelszava vagy az adatai kiszivárognának. Egyszerűen adja meg az e-mail-címét vagy a felhasználónevét, és megtudhatja, hogy a jelszava biztonságos-e.

Ha azt tapasztalja, hogy a fiókjainak adatai kiszivárogtak (ez pirossal jelenik meg, a szöveg pedig pontosan leírja, mely adatai kerültek ki a dark webre), kövesse a javasolt lépéseket. A legtöbb esetben elegendő megváltoztatni a jelszót, kijelentkeztenni a fiókot az összes eszközről, és ha a fiók fontos, kétlépcsős hitelesítéssel védeni.

<https://monitor.firefox.com/>

<https://haveibeenpwned.com/>

<https://haveibeenpwned.com/Passwords>

4 Jelszavak

A jelszavak számos általunk használt dolog védelmének fontos részét képezik — a közösségi médiától kezdve az e-mailen át a banki ügyintézésig.

Gyakran ezek jelentik az első és egyetlen akadályt az Ön adatai és bárki között, aki azokat az Ön hozzájárulása nélkül elolvashatná, felhasználhatná vagy megsemmisíthetné.

Használhatja a legfejlettebb biztonsági eszközöket is, de ha a jelszava gyenge, vagy ha hagyja, hogy illetéktelen kezekbe kerüljön, azok sem segítenek.

Használta például valaha az alábbi jelszavak valamelyikét?

1 - 123456 (2018 óta a leggyakoribb jelszó)

- 2 - 123456789
- 3 - qwerty
- 4 - password (két helyet visszaesett; hosszú ideig a második helyen állt)
- 5 - 1234567
- 6 - 12345678
- 7 - 12345
- 8 - iloveyou
- 9 - 111111
- 10 - 123123
- 11 - abc123
- 12 - qwerty123
- 13 - 1q2w3e4r
- 14 - admin
- 15 - qwertyuiop
- 16 - 654321
- 17 - 555555
- 18 - lovely
- 19 - 7777777
- 20 - welcome

A leggyakoribb jelszavak teljes rangsorát és annak időbeli változását itt tekintheti meg:

https://en.wikipedia.org/wiki/List_of_the_most_common_passwords

Ha ezek közül bármelyik jelszót használja, feltétlenül változtassa meg.

Miért?

Mert a támadók a leggyakoribb jelszavak listáit használják a fiókjához való hozzáféréshez.

További kockázatot jelent a jelszavak újrahasználata. A szolgáltatásokat időnként feltörik, és a jelszavakat ellopják.

Ez azt jelenti, hogy ha ugyanazt a jelszót két szolgáltatásnál is használta, és az elsőt feltörik, a támadó megpróbálja ezt a jelszót a második szolgáltatásnál is.

Ha újra felhasználta a jelszót, hozzáférhetnek a fiókjaihoz.

Hogyan hozzunk létre erős jelszavakat?

Ellenőrizze, milyen könnyen feltörhető a jelszava: <https://howsecureismypassword.net/>

Tippek/szabályok az erős jelszó létrehozásához

- **A jelszó hossza fontosabb, mint a szimbólumok/számok/kis- és nagybetűk használata** (A Lukas38! jelszó például gyenge jelszó; a feltöréséhez mindössze 8 óra szükséges.)
- **Használjon kifejezést vagy egész mondatot magyarul:** „a kedvenc kultuszkönyvem egy barnamedvéről” (2×10^{93} év)

- **Soha ne használja újra ugyanazokat a jelszavakat,**
- **Ne jelentkezzen be más alkalmazásokon keresztül** (Facebook, Gmail), még akkor sem, ha ez kényelmes
- **Kapcsolja be a kétlépcsős hitelesítést a valóban fontos fiókoknál** (a bankok megkövetelik; e-mail-fiókok, Facebook)

További jó tanácsok: <https://www.eset.com/sk/blog/domaca-it-bezpecnost/ako-vytvorit-nepriestrelne-heslo/>

Jelszókezelő mint megoldás arra, hogy ne felejtjük el a jelszavakat:

Használhatja a <https://www.keepassx.org/>,

Bitwarden <https://bitwarden.com/> vagy a fizetős szolgáltatást:

1password <https://1password.com/haveibeenpwned/ohno/>

és mindig használjon kétlépcsős hitelesítést.

5 Adattitkosítás

A titkosítás olyan módszer, amely az üzenet vagy a fájl tartalmának kódolásával növeli annak biztonságát, így azt csak a megfelelő titkosítási kulccsal vagy jelszóval rendelkező személy tudja visszafejteni és elolvasni.

Mit tesz a titkosítás?

Megvédi az adatait attól, hogy olyan személy férjen hozzájuk vagy módosítsa azokat, akinek nem szabadna látnia őket.

A kommunikációban a titkosítás abban is segít, hogy valóban a megfelelő személlyel beszéljünk, és ne egy csalóval.

Hogyan titkosíthatom az adatokat?

A VeraCrypt jó minőségű, ingyenes, nyílt forráskódú titkosítóeszköz. A VeraCrypt egyfajta széfként titkosított tárolót hoz létre a számítógépén vagy a merevlemezén, amelybe tetszőleges számú fájlt helyezhet el.

Ne feledje:

- A titkosított tárolót mindig be kell zárnia ahhoz, hogy működjön.
- Azok a támadók, akik nem tudják feltörni a titkosítást, megpróbálhatják ellopni a jelszavát, és így hozzáférni az adatokhoz.
- Ügyeljen arra, hogy nagyon erős jelszavakat használjon, és kövesse a kártékony szoftverekről szóló kurzus útmutatásait is.

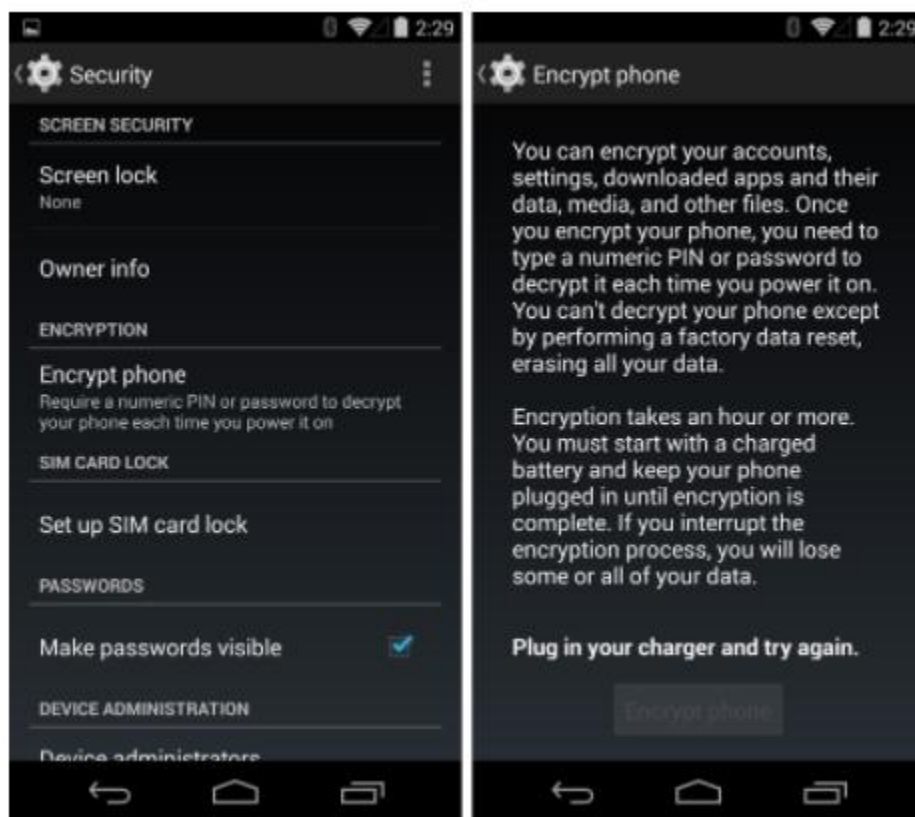
5.1 Az eszközök titkosítása

Fontos az eszközök, például a számítógép és a telefon titkosítása. Enélkül bárki, aki fizikailag hozzáfér az eszközhöz, könnyen hozzájuthat minden információjához. Számos eszköz ma már beépített, a teljes eszközre kiterjedő titkosítással rendelkezik, amelyet ennek megelőzése érdekében bekapcsolhat.

Az alábbiakban bemutatjuk, hogyan kapcsolható be a titkosítás Windows, Mac OS X rendszeren és Android telefonokon.

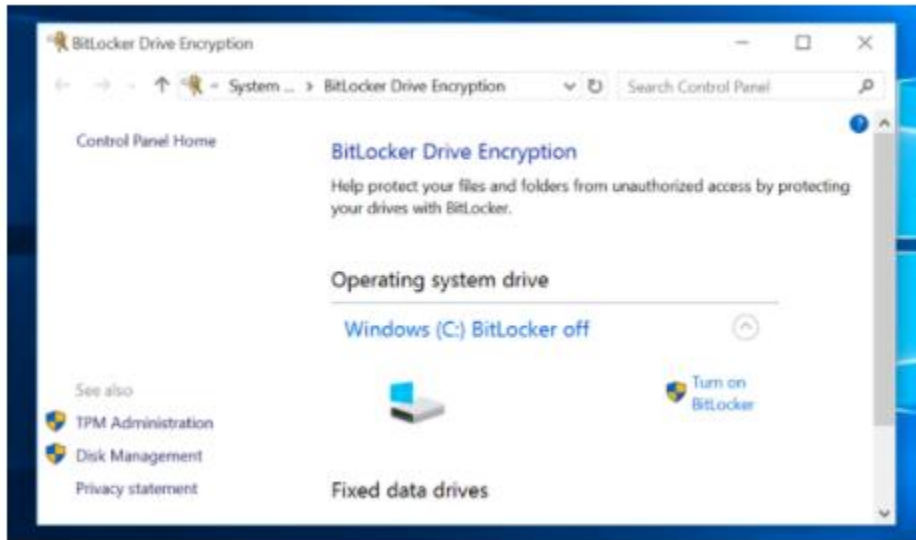
Minden olyan Apple iPhone készüléken, amelyen a legfrissebb szoftververzió fut, a titkosítás automatikusan be van kapcsolva.

5.1.1 Android esetén:



1. Lépjen a Beállítások menübe
2. Lépjen a Biztonság menüpontra
3. Válassza a Telefon titkosítása lehetőséget

5.1.2 Windows esetén (csak a Professional verzióban):



1. Lépjen a Vezérlőpultra
2. Nyissa meg a BitLockert
3. Válassza a „Titkosítás” lehetőséget

5.1.3 Mac OS X esetén:



1. Lépjen a Rendszerbeállításokba
2. Biztonság és adatvédelem
3. Válassza a FileVault lehetőséget

Ne feledje:

- Ahhoz, hogy a titkosítás működjön, mindig ki kell kapcsolnia a számítógépét, illetve zárolnia kell a telefonját.
- A biztonsága csak annyira erős, amennyire a jelszava.
- Ügyeljen arra, hogy nagyon erős jelszavakat használjon.
- Kövesse a kártékony szoftverekről szóló kurzus útmutatásait is.

6 Kártékony szoftverek (malware)

A malware (kártékony szoftver) általános gyűjtőfogalom, amely a rosszindulatú szoftverek több típusát jelöli; ezeket a potenciális támadó megpróbálhatja az Ön eszközére (mobiltelefon, tablet, laptop vagy asztali számítógép) juttatni.

Bizonyára hallott már olyan kifejezéseket, mint számítógépes vírus, féreg, trójai faló, kémprogram és zsarolóprogram. Ezek mind a kártékony szoftverek (az angol „malicious software”, azaz rosszindulatú szoftver kifejezésből) típusai, amelyek célja, hogy bejussanak az eszközére, és információkat lopjanak el róla, vagy megakadályozzák, hogy hozzáférjen az információihoz, és így zsarolhassák Önt. A kártékony szoftverek lehetővé teszik a támadók számára, hogy távolról irányítsák az eszközét. Hozzáférhetnek az érzékeny adataihoz és a bankkártyáihoz, az Ön nevében küldhetnek e-maileket és üzeneteket, továbbterjeszthetik a kártékony kódot és így tovább. Íme néhány példa arra, mit tehet a támadó:

1. Úgynevezett billentyűzetfigyelőt (keyloggert) telepít az eszközére.

Ez rögzíti mindazt, amit az eszközön begépel. Így a támadó elolvashatja például a jelszavait (ezért is szokás a jelszavakat pontokkal vagy csillagokkal elrejtetni).

2. Képernyőképek.

Ez azt jelenti, hogy a támadó néhány másodpercenként képet készít a képernyőjéről, így pontosan rekonstruálhatja, mit csinált, és tartósan eltárolhatja például a személyes beszélgetéseit vagy azokat a fényképeket, amelyekről azt hiszi, hogy csak Ön láthatja őket.

3. Átkutathatja a dokumentumait.

4. Hozzáférhet a webkamerájához és a mikrofonjához, így felvételeket készíthet az otthonáról, az irodájáról és így tovább.

5. Törölheti a dokumentumait.

6. Titkosíthatja a dokumentumait, és váltságdíj megfizetésére kényszerítheti, ha valaha újra hozzájuk szeretne férni.

7. Hozzáférhet a rendszereszközeihez, és tetszés szerint módosíthatja azokat

6.1 Hogyan juthat el Önhöz a kártékony szoftver?

- Fertőzött hardveren keresztül, például USB-meghajtón. Ismertek olyan esetek különböző konferenciákról, ahol a résztvevők a promóciós anyagok között fertőzött USB-meghajtókat kaptak.
- Ismeretlen kártékony linkre kattintva, amelyen keresztül vírus töltődik le az eszközére, például hamis hirdetési banneren keresztül.
- E-mail-melléklet letöltésével.
- Úgynevezett „drive-by download” útján — ez olyan kártékony szoftver, amelynek letöltése automatikusan elindul, amikor feltört vagy csapdába ejtett weboldalt látogat meg.
- Nem licencelt, úgynevezett „feltört” szoftvereken keresztül. A támadók rendszerint azt használják ki, hogy az emberek ingyen szeretnék kipróbálni az új szoftvereket, és a hivatalos forgalmazónak való fizetés nélkül töltik le azokat, vagy egyszerűen nincs rá elég pénzük; erre gyakori példa a Windows. Bár az interneten elérhető ingyenes szoftverek nem mindegyike kártékony, letöltésükkel nagyobb a kockázata annak, hogy fertőzött szoftver kerül az eszközére.

6.2 Hogyan védekezhetünk a kártékony szoftverek ellen?

Az, ahogyan a kártékony szoftver eljut hozzánk, egyben választ ad arra is, hogyan védekezhetünk.

- Telepítsen jó hírű vírusirtó szoftvert; ingyenes vírusirtó verziók is léteznek. A vírusirtó cégek ma naponta akár 300 000 új és korábban ismeretlen kártékony kódmintát azonosítanak, és segíthetnek abban, hogy a legalapvetőbb kártékony kódot még kattintás előtt kiszűrje. Fontosak a rendszeres vírusirtó-frissítések; ideális esetben hagyja bekapcsolva az automatikus rendszeres frissítéseket.
- Használjon licencelt szoftvert, és engedélyezze a rendszeres frissítéseket. Minden szoftverben lehetnek olyan potenciális biztonsági rések, amelyek felfedezésre várnak. A megbízható cégek ezért rendszeresen adnak ki úgynevezett javítócsomagokat, amelyek megvédik a szoftvert az ismert biztonsági sebezhetőségek kihasználásától.
- Legyen nagyon óvatos az úgynevezett adathalászattal (phishing) szemben. Óvakodjon a támadásnak ettől a formájától, mert a támadók gyakran olyan személynek adhatják ki magukat, akit ismer és akiben megbízik, és az ismerőse címéhez hasonló címről küldhetnek Önnek kártékony szoftvert, akár link, akár

e-mail-melléklet formájában. Mivel ez a támadások egyik leggyakoribb formája, részletesebben is foglalkozunk vele.

- Ügyeljen a social engineeringre: ez az emberek pszichológiai manipulálása annak érdekében, hogy bizalmas információkat adjanak ki. A social engineering lehet jó és rossz célú is; a részleteket lásd alább.

6.3 Hogyan kerülheti el az adathalászatot, és hogyan ismerheti fel egyáltalán?

E-mailet vagy privát üzenetet kap a közösségi médiában. Ha olyan személytől érkezik, akit nem ismer, vagy akitől nem vár üzenetet, azonnal ellenőrizze, hogy valódi kapcsolatról van-e szó. Sokkal rosszabb, ha olyan személytől kap kártékony mellékletet vagy linket, akit ismer, vagy akiben megbízik. Ez azt jelenti, hogy a támadó feltörte az illető fiókját, és az ő nevében küld e-maileket vagy üzeneteket. Ilyenkor is mérlegelheti azonban annak valószínűségét, hogy várt-e ilyen üzenetet az adott személytől. Ha például a főnökétől vagy az édesanyjától kap furcsa mellékletet vagy linket minden konkrét magyarázat nélkül, és tudja, hogy nem ilyen stílusú e-maileket szokott tőlük kapni, automatikusan gyanakodnia kell. A kifinomultabb támadások ma már a megszokott kommunikációs stílust és módot is másolják, ilyen esetekben pedig az adathalászat felismerése valóban nehéz.

A jó hír az, hogy ahhoz, hogy az adathalászattal küldött kártékony szoftver működjön, be kell jutnia az eszközére, ezt pedig meg tudjuk akadályozni.

Az adathalászat másik formája az, amikor a támadók a rendszeresen látogatott weboldalakon, például a Gmailen, a Facebookon vagy az olvasott online újságokon keresztül szerzik meg a bejelentkezési nevét és jelszavát. Rendszerint hamis e-mailet kap, amely a szolgáltató üzenetének adja ki magát, sürgős felszólítással a jelszó megváltoztatására és egy linkkel, ahol ezt megteheti. Ha ezt pánikban és sietve teszi meg, a jelszavát a támadóknak adja meg. Ezt követően teljesen kizárhatják Önt a szolgáltatásból, és természetesen hozzáférhetnek az adataihoz. Különösen ebben az esetben nyújthat védelmet a kétlépcsős hitelesítés.

Ajánlás: Töltsön ki egy rövid kvízt a kártékony szoftverekről és az adathalászatról, és figyeljen a részletekre. Nyugodtan töltsse ki a kvízt egymás után 2–3 alkalommal is, mert az ilyen gyakorlás növeli az érzékenységet a csaló e-mailekkel szemben, és segít abban, hogy rutint szerezzen azoknak a részleteknek az észrevételében, amelyekre figyelnie kell.

1) angolul <https://phishingquiz.withgoogle.com>

2) magyarul: [6-fejezet-adathalaszat-es-megtevesztes](#) | [ResilienceLab.online](#) / [quiz-chapter-6-phishing-and-social-engineering](#) | [ResilienceLab.online](#)

6.4 Pszichológiai manipuláció (social engineering)

A social engineering az emberek pszichológiai manipulálása annak érdekében, hogy bizalmas információkat adjanak ki. Történhet online, például telefonon, vagy offline, például egy irodában, a recepción és így tovább. Valaki például kiadhatja magát postai kézbesítőnek, futárszolgálat munkatársának vagy szerelőnek — egyszóval olyan személynek, aki nem kelt gyanút. Ha fizikailag hozzáfér valamelyik eszközhöz, könnyebben férhet hozzá az eszközeihez, és kerülheti meg a biztonsági beállításokat; ezért is szükséges, hogy minden eszközön különböző védelmi rétegek legyenek aktiválva, például jelszó, PIN-kód és így tovább. Soha ne engedje meg idegennek — bármilyen megbízhatónak tűnjön is —, hogy bármit tegyen az eszközén, például ha megkérdezi, küldhet-e róla e-mailt vagy telefonálhat-e vele.

Fordítson különös figyelmet az ismeretlen USB-meghajtókra, amelyeket állítólag valaki valahol otthagyott. A kíváncsiságunk arra készíthet minket, hogy megnézzük, mi van az USB-meghajtón, és tudtukon kívül kártékony szoftvert futtassunk az eszközünkön, hozzáférést adva ezzel a hackereknek.

6.5 A kártékony szoftverek típusai

Stalkerware, azaz kémprogram

Ez olyan alkalmazás, amely lehetővé teszi a támadó számára, hogy kémkedjen az eszközén, illetve az Ön hozzájárulása nélkül nyomon kövesse a tartózkodási helyét és egyéb adatait. Meg kell jegyezni, hogy számos legális alkalmazás, például a Gmail, a Facebook, a csevegőszolgáltatások és így tovább, automatikusan gyűjti ezeket az információkat Önről, hacsak manuálisan ki nem kapcsolja ezt. Az ilyen típusú alkalmazások egy része ikon nélkül is telepíthető, így könnyen elkerülhetik a figyelmét, az eszközét pedig távolról megfigyelhetik.

Az adware, az angol *advertising-supported software* (reklámokkal támogatott szoftver) kifejezés rövidítése; olyan szoftver, amely automatikusan reklámokat tölt le és jelenít meg az eszközén. Minden alkalommal bevételt termel a fejlesztőknek, amikor egy reklám megjelenik, vagy arra rákattintanak. Gyakran ingyenes programokhoz vagy alkalmazásokhoz „csomagban” adott bónuszként terjed.

A vírus olyan kártékony program (malware), amely lemásolja önmagát, és beilleszti a kódját más fájlokba vagy programokba.

A trójai faló, köznyelvi nevén **trójai**, a kártékony szoftverek (malware) egyik típusa, amely ártalmatlan vagy hasznos programnak álcázza magát, hogy megtévessze a felhasználót. A klasszikus számítógépes vírusokkal ellentétben nem szaporítja önmagát, és nem fertőz meg más fájlokat, hanem arra épít, hogy a felhasználó a tudtán kívül letöltsen és futtasson.

A számítógépes féreg a kártékony szoftverek (malware) olyan típusa, amely képes önmagát sokszorozni, és felhasználói beavatkozás nélkül terjedni a számítógépes hálózatokon. A klasszikus vírussal ellentétben nem kell egy másik programhoz „hozzákapcsolódnia”.

A zsarolóprogram (ransomware) a kártékony szoftverek (malware) olyan típusa, amely észrevétlenül jut be a számítógépébe vagy a hálózatába. Ezt követően blokkolja az eszközhöz való hozzáférést, vagy titkosítja a fájljait, a támadók pedig váltságdíj — leggyakrabban kriptovalutában történő — megfizetését követelik a feloldásért.

A rootkit a kártékony szoftverek alattomos típusa, amely lehetővé teszi a támadó számára, hogy átvegye az irányítást egy számítógép felett, miközben elrejtje a jelenlétét. Az operációs rendszerbe vagy annak kerneljébe mélyen beépülve rejtőzik el a hagyományos vírusirtó programok és feladatkezelők elől.

A billentyűzetfigyelő (keylogger) olyan szoftver vagy fizikai hardvereszköz, amely titokban rögzíti a billentyűzeten leütött minden billentyűt. Fő célja a kémkedés és az érzékeny adatok — például jelszavak, bankkártyaszámok és privát üzenetek — ellopása.

7 IP-cím és VPN

7.1 Módok, hogyan valaki megszerezheti az Ön IP-címét

1

Az eszköze kölcsönkérésével: Amikor valaki az Ön eszközén dolgozik, egyszerűen felkeresheti a [WhatIsMyIPaddress.com](https://www.whatismyip.com/) oldalt, és ennyi.

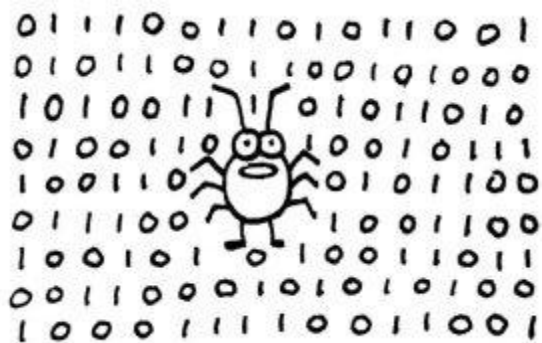
2

A Wi-Fi-hálózatába való betöréssel. Ha bármely vendégnek engedélyezi a Wi-Fi használatát, az illető kiderítheti az IP-címét.

3

Az e-mailjeit megnézve: Szerencsére a legtöbb e-mail-szolgáltatás ma már nem jeleníti meg az IP-címét, a kisebb szolgáltatóknál azonban ez néha előfordulhat. Próbálja ki ezt az eszközt, és nézze meg, mit tudhat meg bárki Önről: [e-mail-nyomkövető eszköz](#).

4



HTML-bug (webjelző) segítségével. Ez a kis bug nem kártékony, és nem vírus. Olyan kódrészlet, amelyet például egy e-mailben lévő képbe illesztenek be. Amikor megnézi — pusztán az e-mail megnyitásával —, a bug jelzi a feladónak, hogy elolvasta az e-mailt, és felfedi az IP-címét is. Léteznek szolgáltatások, amelyek segítenek ilyen bugok beállításában, például a WhoReadMe.com.

5

Webszervernaplók. Minden alkalommal, amikor meglátogat egy weboldalt, ott hagyja az IP-címét. Ez olyasmi, mint az online kapcsolódáshoz használt digitális útlevele. A weboldal — ha az üzemeltetője így állította be — áttekintéssel rendelkezhet mindazokról az IP-címekről, amelyek felkeresték. A weboldalak számára ez hasznos információ, mert így láthatják, hogy egy adott IP-cím rendszeresen látogatja-e az oldalt, mennyi az alkalmi látogatások száma, és honnan érkeznek a látogatók.

6

Internetes fórumok és a blogok, illetve cikkek alatti hozzászólások: Az oldalak üzemeltetői számára itt is nagyon hasznos, ha ismerik az IP-címeit, mert ha megsérti az adott oldal szabályait, blokkolhatják Önt, például amikor különböző felhasználónevek alatt spammel egy fórumon, az üzemeltető látja, hogy ez egy és ugyanazon IP-címről érkezik.

7

Közösségi hálózatokon keresztül (Facebook, Twitter, Instagram, Snapchat stb.) Az IP-címek a felhasználók között nem láthatók, az oldalak üzemeltetői azonban ismerik az IP-címét. Emellett amikor a közösségi médiában egy hirdetésre kattint, rögzítik az IP-címét.

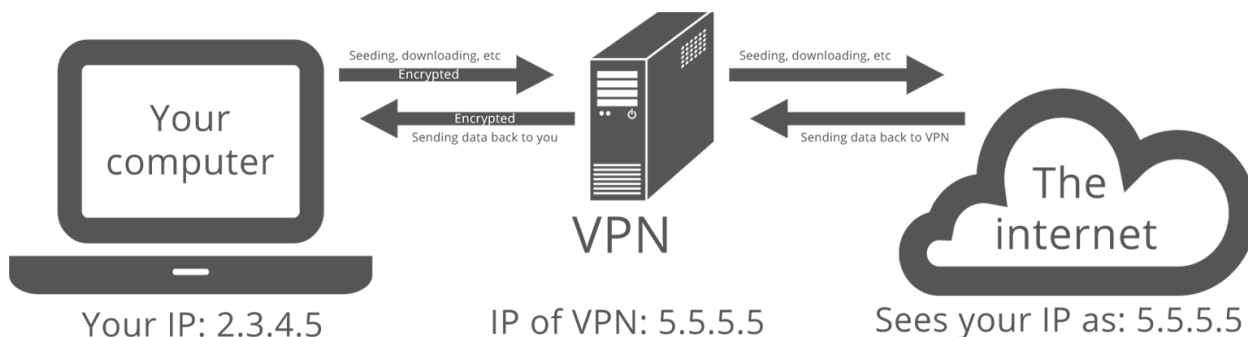
9

Csevegőalkalmazásokon keresztül, például a WhatsAppon vagy a Viberen: amikor egy üzenetben lévő linkre kattint, olyan weboldalra jut, amely rögzíti az IP-címét. Ilyen nyomkövető linkek hozhatók létre például a grabify.link vagy az iplogger.org.

7.2 VPN

Az IP-címünk — és ezáltal online jelenlétünk egyéb adatai — védelmének ajánlott módja a VPN (Virtual Private Network, virtuális magánhálózat) használata, amely egyfajta privát és titkosított alagút, amelyen keresztül az információink és az online tevékenységeink áramlanak. Működését az alábbi ábra szemlélteti. Szokásos körülmények között az eszköze az internetszolgáltatóján (ISP – Internet Service Provider) keresztül csatlakozik az internethez, ahol az IP-címe látható. Ha azonban VPN-szerveren keresztül csatlakozik, ez a szerver megváltoztatja az IP-címét és a földrajzi helyzetét is, valamint titkosítja, azaz elrejtí az online tevékenységét, illetve az adatok és információk áramlását. A VPN a DNS-en (Domain Name System) keresztül a felkeresett weboldalakat is titkosítja, ami azt jelenti, hogy a megfigyelők vagy a célzott hirdetések nem ismerik meg a böngészési előzményeit.

A TechSoup Europe a Proton VPN használatát ajánlja, mert biztonsági szempontból az egyik legjobbra értékelt VPN, többek között azért, mert a központi szervere fizikailag védett. Ez azt jelenti, hogy még ha egy támadó el is jut a VPN-szerverig, illetve feltöri a VPN-szervert, kizárólag titkosított adatokat talál rajta. Maga a Proton VPN sem fér hozzá az adataihoz. Természetesen más VPN-szoftverek is léteznek. Az alábbiakban alapvető tanácsokat olvashat arról, mire érdemes figyelni a VPN kiválasztásakor.



VPN-t választok — mire figyeljek?

A fizetős VPN-ek természetesen jobb szolgáltatásokat nyújtanak, mint az ingyenes verziók, de minden VPN más és más. A kiválasztásnál ügyeljen a következőkre:

Szakmai értékelők minősítései, akik egyik ilyen cégnél sem dolgoznak. Mindig érdemes több rangsorban és értékelésben is ellenőrizni a forrásokat. Ezekből sok elérhető az interneten, és az ilyen ellenőrzés nem tart olyan sokáig.

Megosztott IP-címek: Olyan VPN-t válasszon, amely megosztott IP-címeket kínál, vagyis több, különböző felhasználóhoz tartozó eszköz ugyanazzal az IP-címmel rendelkezik. Minél több ilyen névtelen felhasználó van, annál privátabb a böngészése, mert a támadó számára lehetetlen megkülönböztetni, ki kicsoda.

Szerverek: Minél több szerver áll a cég rendelkezésére, annál jobb lesz a kapcsolat minősége.

Titkosítás: Jelenleg a legbiztonságosabb titkosítás az AES-256 (Advanced Encryption Standard), amely gyakorlatilag feltörhetetlen, mert képletesen szólva több titkosítási kombinációt használ, mint ahány csillag van a világegyetemben.

Protokoll: Kerülje a gyengébb protokollokat, például a PPTP-t, és válassza helyette a megbízhatóbb OpenVPN-t.

Adatnaplók: Olyan VPN-t válasszon, amely nem tárolja az adatait, vagyis nem rögzíti az online tevékenységeit. Azt, hogy így tesz-e, a szabályzatából tudhatja meg.

Ingyenes próbaverzió – Nagyszerű, ha kipróbálhatunk valamit, mielőtt használni kezdenénk.

8 Biztonság a közösségi hálózatokon és az adatvédelmi beállítások

A közösségi hálózatok kétségtelenül különféle előnyöket hoznak az életünkbe, például megkönnyítik a tevékenységek összehangolását a barátokkal, a családdal vagy a kollégákkal. Számos szervezet régóta a közösségi médián keresztül népszerűsíti tevékenységét és tartalmait, üzenetünk pedig nagyszámú emberhez juthat el. A közösségi hálózatok használata azonban különféle kockázatokkal is jár. Ebben a fejezetben ezeket a kockázatokat tekintjük át, és bemutatjuk megelőzésük vagy minimalizálásuk alapvető módjait.

A legtöbb közösségi hálózat ingyenes. Ennél a modellnél rendszerint igaz, hogy ha valami ingyenes, akkor a közösségi hálózatok felhasználói és az adataik válnak termékké: a viselkedésükre, a magánéletükre, az érdeklődésükre és így tovább vonatkozó adatok. Amikor a közösségi hálózatra való regisztrációkor megnyomjuk az „Elfogadom” gombot, rendszerint hozzájárulunk ahhoz, hogy ezek a vállalatok a szolgáltatásaikért cserébe jogosultak legyenek a személyes adataink gyűjtésére. Ennek eredményeként nyomon követhetik a tevékenységünket, és hozzáférnek például az általunk kezelt szervezeti oldalakhoz is.

Mit látnak/tudnak a közösségi hálózatok?

- Kikkel vagyunk barátságban
- Kikkel beszélgettünk és miről
- Mikor beszélgettünk velük
- Mikor töltünk időt a közösségi hálózaton
- Mikor és hol tartózkodunk
- Milyen típusú információkat követünk, és mi érdekel minket
- Mit vásárolunk, és még sok minden mást

A metaadatokat rendszerint a közösségi hálózatok által kínált célzottabb hirdetésekhez és tartalmakhoz használják fel, ami nem feltétlenül rossz. A metaadatoknak azonban vannak árnyoldalaik is. Különböző országokban a kormányok ezeket a polgári aktivisták megfigyelésére használják, de más személyek is hozzáférhetnek ezekhez a metaadatokhoz. A támadók hackeléssel vagy adathalászattal különböző módokon betörhetnek a fiókjába, és átvehetik felette az irányítást. Ezt sokféleképpen felhasználhatják, például arra, hogy dezinformációt osszanak meg Önről, illetve az Ön nevében, vagy hogy kártékony kódot (malware-t) küldjenek annak érdekében, hogy hozzáférjenek mások érzékeny adataihoz, amelyeket zsarolásra használhatnak fel.

E kockázatok minimalizálása érdekében módosíthatjuk a biztonsági beállításainkat.

A közösségi hálózatok használatának alapelvei és ajánlások az adatvédelmi beállításokhoz

- Korlátozza a bejegyzései láthatóságát (nyilvános vs. privát)
- Tartson fenn külön fiókokat: egy munkahelyit és egy magánfiókot
- Korlátozza a személyes és érzékeny bejegyzések számát
- Tartsa zártan a csoportokat, és ellenőrizze, kit enged be azokba
- Ne tegyen közzé részleteket az aktivisták találkozóiról; a találkozó helyszínét semmiképpen ne tegye közzé, hacsak ez nem szükséges
- Kapcsolja ki a helymegosztást (helymeghatározási beállítások)
- Soha ne engedje, hogy egy közösségi hálózat megjegyezze a banki adatait
- Ha nem ismer valakit, soha ne fogadja el az ismerősnek jelölését
- Ügyeljen az ismerőseinek látszó hamis fiókokra. Ha ismerősnek jelöli valaki, akit ismer, ellenőrizze, hogy valóban ő az-e, lehetőleg telefonon. A támadók gyakran adják ki magukat az ismerőseinek.
- Osszon meg a lehető legkevesebbet; ne osszon meg személyes dolgokat
- Legyen tisztában az adatvédelmi és biztonsági beállításokkal — korlátozza őket
- Ne jelöljön meg személyeket a fényképeken, legalábbis a nyilvánosakon ne
- Tartson fenn magánfiókot és munkahelyi fiókot az oldalak kezeléséhez
- Védje jól mindkét fiókot, és használjon kétféle hitelesítést
- Ne használja a Facebookot más alkalmazásokba való bejelentkezéshez!!! A személyes információk és adatok esetleges kiszivárgása miatt
- Sok digitális biztonsági szakértő azt mondáná: egyáltalán ne használjon közösségi hálózatokat; ha pedig már ott van, ne kedveljen semmit, ne nyilvánuljon meg semmilyen formában, legyen névtelen és így tovább (szélsőséges álláspont)

A közösségi hálózatok ma – a nyilvánosság vagy a jogszabályok nyomására – jobb ellenőrzést tesznek lehetővé a személyes adatai felett. Időről időre ellenőrizze, hogy a személyes adatvédelmi és biztonsági beállításai naprakészek-e, és hogy megjelent-e ott valamilyen újdonság.

9 Felhasznált források

Ingyenes digitális biztonsági képzések és kvízek: [Tanulás indítása](#) | [ResilienceLab.online](#)

Ajánlott irodalom a közösségi hálózatok használatának kockázatairól, azok biztonságáról, adatvédelméről és a közösségimédia-használat egyéb szempontjairól:

- SCHNEIER, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W. W. Norton & Company, 2015. ISBN 978-0-393-35217-7.
- SCHNEIER, Bruce. *Click Here to Kill Everybody: Security and Survival in a Hyper-connected World*. New York: W. W. Norton & Company, 2018. ISBN 978-0-393-60960-8.
- MITNICK, Kevin és Robert VAMOSI: *The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data*. New York: Little, Brown and Company, 2017. ISBN 978-0-316-38050-8.
- Resilience Lab, [Tanulás indítása](#) | [ResilienceLab.online](#)

Felhasznált források:

- Hogyan válasszuk ki a megfelelő VPN-t: <https://blog.avast.com/cs/jak-si-vybrat-tu-spravnou-vpn>)
- Mi az IP-címem: <https://whatismyipaddress.com/get-ip> (rövidítve)
- Biztonság az interneten az ESET-től: <https://bezpecnenanete.eset.com/sk/>
- Kiberbiztonsági szótár: <https://www.koop.cz/kyberbezpecnost-slovník>
- Kaspersky Resource Center: <https://www.kaspersky.com/resource-center>
- A legnagyobb adat szivárgások vizualizálása
<https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>
- Keylogger: Mi az, és hogyan védheted meg magad ellene, 2025. március 5:
<https://gdpr-slovensko.sk/keylogger-co-to-je-ako-funguje-a-ako-sa-pred-nim-chranit/>

- Rootkitek a digitális világban: Fenyegetések és védekezési módszerek, 2026. március 9.:

[Rootkity v Digitálnom Svete: Hrozby a Ako sa Chránit'](#)

10 1. melléklet: Gyakorlat: Mit vagyunk hajlandók feltölteni a közösségi médiába, és miért?

Mit szoktam megosztani a közösségi médiában? (Példák)	+ milyen előnyökkel jár ez számomra? Mit nyerek vele?	Milyen kockázatokkal/hátrányokkal jár?
<i>Fényképek (köztük személyes jellegűek, például nyaralásról, családi ünnepségekről és hasonló eseményekről)</i>	<i>Figyelem a barátoktól és ismerősöktől / nem kell külön mindenkinek elmagyaráznom, hol voltam és mit csináltam ott</i>	<i>Mások irigysége, Valaki tudja, hogy most nem vagyok otthon (betörők), sok olyan személyes információ, amellyel vissza lehet élni (például hogy a gyerekek hová járnak iskolába),</i>
<i>Gyermekekről készült fényképek</i>	<i>Megosztás távoli családtagokkal és barátokkal</i>	<i>Fényképekkel való visszaélés, fényképek ellopása, a gyermekek identitása</i>
<i>Munkahelyi fényképek</i>	<i>Presztízs, névismertség, reklám, márképítés, de egyben figyelemfelhívás is</i>	<i>N/A</i>
<i>Különféle személyes dilemmák</i>	<i>Olyan emberektől kapok rálátást, akikkel egyébként nem beszélek, és akikkel máskülönben nem találkoznék,</i>	<i>Nincs befolyásom arra, ki olvassa el, és mikor hozhatja fel ellenem</i>
<i>Amikor keresek valamit / szükségem van valamire</i>	<i>Gyorsabban hozzájuthatok; különböző véleményeket kapok olyan emberektől, akikben megbízom</i>	<i>Mindenki tudja, mire van szükségem, például hogy felújítom a lakásomat,</i>
<i>Politikai nézetek / társadalmi nézetek</i>	<i>Szélesebb vélemény spektrum</i>	

Mit nem vagyunk hajlandók feltölteni a közösségi médiába, és miért?

Amit soha nem töltenék fel a közösségi médiába	Miért?
<i>Intim fényképek</i>	<i>Zsarolás, mobbing</i>

11 2. melléklet: Biztonsági terv tervezete

Biztonsági terv (SZERVEZET neve)

A biztonsági terv végrehajtásában részt vevő személyek listája

A kiberbiztonsági intézkedések kidolgozásában és végrehajtásában részt vevő személyek			
Név	Szerepkör	Tel.	E-mail

IT-eszközök

Hálózatok, tárolók, szerverek és eszközök.

Az általunk tárolt fontos adatok, akár e-mail-szerveren, akár a felhőben vagy a Salesforce-ban.

Érzékeny adatok — bankkártyaszámok és a célcsoportokra vonatkozó egyéb védett adatok.

Biztonsági eszközök — tűzfal, vírusirtó szoftver, védelmi technikák (adattitkosítás és biztonsági mentés).

Közösen használt eszközök — pl. VPN, felhőalapú monitorozás, jelszókezelő.

Eszköznyilvántartó táblázat

Az információ típusa	Hely (eszköz / online szolgáltatás)	Érték (magas, közepes, alacsony)	Releváns fenyegetések	Szükséges:
Jelszavak		Magas	Illetéktelen használat esetén: kizárás az online	A Bitwarden telepítése/megvásárlása, a

			szolgáltatásokból, a még nem mentett aktuális adatok elvesztése, valamint a szervezet online tevékenységeinek esetleges átvétele.	<i>munkatársak betanítása a használatára, jelszóadatbázis létrehozása.</i>
Érzékeny adatokat tartalmazó mappák (szerződések, bérszámfejtési adatok, pénzügyi adminisztráció)		Magas	GDPR-sértés	
Felhőben megosztott mappák		Közepes	Szervezeti adatok és tartalmak kiszivárgása	
Mappák		Magas	Kizárás a hozzáférésből	
Mobiltelefonok	Szervezeti/személyes	Magas	A személyes és a szervezeti ügyek keveredése, érzékeny információk kiszivárgása, a kommunikáció feletti ellenőrzés	
USB-meghajtók		Alacsony	Részleges adatszivárgás, esetleges GDPR-sértés	
Laptopok + egyéb eszközök / tabletek		Közepes		
Magánfiókon keresztül kezelt közösségi média		közepes	Jelszavak és adatok kiszivárgása, a belső kommunikáció megfigyelése, kártékony tartalom megosztása a nevünkben, zaklatás (stalking), doxxing — a jó hírnév sérülése.	
Szervezeti fiókon keresztül kezelt közösségi média		közepes	Kártékony tartalom megosztása a nevünkben	
Egyéb? Közösen használt szoftverek (Salesforce, Miro, könyvelőprogram stb.)		Közepes	Különféle fenyegetések	

Decentralizált vírusirtó szoftver.....

Ingyenes vírusirtó verzió? Mindenki külön-külön? Közös fizetős vírusirtó?

A közös fiókok beállítása úgy, hogy értesítést küldjenek a szokatlan bejelentkezésekről (szokatlan helyszín, szokatlan eszköz). Melyik címre érkezzenek ezek az értesítések?

Minimumkövetelmények: a Microsoft Defender bekapcsolása a Microsoft Windowsban, tűzfalvédelemmel és folyamatos fájlellenőrzéssel együtt.

Választható beállítások: biztonsági mentés a Microsoft felhőbe.

Felhasználói útmutatók és egységes eljárások

Bár egyes fenyegetések a szervezeten kívülről érkeznek, sok közülük a csapatunk cselekedeteiből ered. A védelem javítása érdekében a következő eljárások vezethetők be:

Útmutatók és egységes eljárások				
Terület	Az útmutató célja/rendeltetése	Útmutató/eljárás	Kinek szól	Megjegyzés
VPN	A nyilvános Wi-Fi-hálózatokon keresztüli csatlakozás kockázatának csökkentése	<i>A Proton VPN telepítését javasoljuk</i>	Mindenki, aki a munkahelyén vagy az otthonán kívül csatlakozik Wi-Fi-hálózaton keresztül	

Kétlépcsős / többlépcsős hitelesítés	Fontos az adatszivárgás kockázatának csökkentése szempontjából	<i>Javasoljuk a 2FA bevezetését a legfontosabb fiókoknál (e- mail....)</i>		
Biztonsági mentés	Az adatvesztés megelőzése az eszköz elvesztése, lemezhiba vagy zsarolóvírus- támadás esetén		Mindenki, aki új anyagokat hoz létre, és azokat olyan egyéni vagy helyi eszközökön tárolja, amelyek nem csatlakoznak közös hálózathoz, és nincsenek szinkronizálv a a Google Drive-val / OneDrive-val stb.	
Titkosítás	Az adatszivárgás megelőzése az eszköz elvesztése vagy zsarolóvírus- támadás esetén	Azokat az adatokat, amelyek kiszivárgása GDPR-sértést okozhat vagy veszélyeztetheti a szervezet működését,	Mindenki, akinek az által használt eszközön olyan adatok vannak, amelyek kiszivárgása	

		jelszóval védve kell tárolni. A titkosítás egyszerű jelszóval egyes fájlokra és teljes mappákra is alkalmazható.	GDPR-sértést okozhat vagy veszélyeztetheti a szervezet működését	
Szoftverfrissítések	A régebbi biztonsági réseken keresztüli illetéktelen hozzáférés megelőzése	Az operációs rendszer, a vírusirtó szoftver, a böngésző és a védelmet igénylő adatokat kezelő egyéb programok frissítése	Mindenki, aki szervezeti adatokat használ olyan szoftveren keresztül, amely ki lehet téve biztonsági sebezhetőségeknak	

Eljárás tényleges biztonsági incidens kezelésére

A megelőzés a kiberbiztonsági egyenletnek csak az egyik oldala.

Készen kell állnunk arra is, hogy mi a teendő, ha biztonsági incidenst észlelünk. Ez járhat egyszerű lépésekkel, például a jelszavak megváltoztatásával vagy az adatok helyreállításával, de összetett adatelemzést és jogi segítség igénybevételét is jelentheti.

Legalább annyit meg kell tennünk, hogy elszigeteljük a biztonsági incidenst, és az érintett adatokat gyorsan offline állapotba helyezzük.

Azonosítsuk a fenyegetéseket és a lehetőségeket, és mérjük fel a szervezetre gyakorolt lehetséges hatásukat.

Ha ez történik:	Mit kell tenni:	Megjegyzés
Mobiltelefon elvesztése/ellopása	A SIM-kártya letiltása a mobilszolgáltatónál, és cserekártya igénylése ugyanazzal a telefonszámmal. A kétlépcsős hitelesítés miatt a lehető leghamarabb gondoskodni kell csere-mobiltelefonról ugyanazzal a telefonszámmal. Ha felmerül a gyanú, hogy valaki hozzáfért az elveszett/ellopott mobiltelefonon lévő adatokhoz, meg kell változtatni az egyénileg használt szolgáltatások, valamint az esetlegesen érintett közös fiókok jelszavait (pl. amelyeket a mobilböngésző megjegyzett).	
Laptop elvesztése/ellopása	A számítógépen alkalmazott védelem szintjétől függően (bejelentkezési jelszó, biometrikus feloldás, adattitkosítás stb.) fel kell mérni annak kockázatát, hogy valaki hozzáfért az elveszett/ellopott laptopon lévő adatokhoz. Ennek alapján meg kell változtatni az egyénileg használt szolgáltatások, valamint az esetlegesen érintett közös fiókok jelszavait (pl. amelyeket a laptop böngészője megjegyzett), helyre kell állítani az adatokat a biztonsági mentésekből, és megfelelő védelmi szintet kell beállítani az új laptopon.	
Vírussal fertőzött számítógép/laptop	Ne csatlakoztassa a laptopot/számítógépet a közös hálózathoz, és ne jelentkezzen be a szervezet online szolgáltatásaiba. Mentse az adatokat hordozható USB-meghajtóra (ne a belső hálózatra és ne	

	a közös Google Drive-ra/OneDrive-ra), próbálja meg eltávolítani a vírust, az eredménytől függően szükség esetén telepítse újra az egész számítógépet (gyári visszaállítás), ellenőrizze a mentett adatokat vírusirtó szoftverrel, majd állítsa vissza őket. Ezt követően változtassa meg az egyénileg használt szolgáltatások, valamint az esetlegesen érintett közös fiókok jelszavait (pl. amelyeket a laptop böngészője megjegyzett). Vírusirtó szoftverrel ellenőrizze, és szükség esetén törölje azokat az USB-meghajtókat, amelyeket legalább egyszer csatlakoztattak a fertőzött számítógéphez.	
Feltört jelszó (Wi-Fi, online szolgáltatás, a számítógép hozzáférési jelszava stb.)	Azonnal változtassa meg az érintett jelszót. Ellenőrizze azoknak az adatoknak a sértetlenségét, amelyekhez illetéktelenül hozzáférhettek (mi hiányzik, mi változott meg), és futtasson vírusellenőrzést. Ha olyan jelszóról volt szó, amely több szolgáltatáshoz is hozzáférést biztosít (pl. a számítógép bejelentkezési jelszava vagy egy jelszókezelő mesterjelszava), a laptop elvesztésénél/ellopásánál leírtak szerint járjon el.	
Zsarolóvírus-támadás	Válassza le teljesen a számítógépet/laptopot a hálózatról. Tájékoztassa azokat, akik szintén veszélyben lehetnek, hogy időben menthessék az adataikat és megvédhessék a számítógépeiket	

	(azokat a számítógépeket, amelyek az Önével azonos belső hálózathoz csatlakoznak, illetve amelyekre USB-meghajtóval vitt át adatokat abban az időszakban, amikor a zsarolóvírus-fertőzés bekövetkezhetett). A további lépésekről kérje szakértő tanácsát.	
--	---	--

Kiberbiztonsági tesztelés és auditok

Rendszeres intézkedések az új gyenge pontok azonosítására.

Kiberbiztonsági auditok, amelyek lehetővé teszik annak felmérését, mennyire hatékony a védelem, és szükség van-e a biztonsági terv frissítésére.

HaveIBeenPwned / Firefox Monitor (az összes munkatárs címének ellenőrzése, és adat-/jelszószivárgás esetén tájékoztatás küldése számukra a jelszavuk megváltoztatásáról)

<https://haveibeenpwned.com/> <https://monitor.mozilla.org/>

Az ellenőrzés és a Firefox Monitorhoz való hozzáadás dátuma	Munkatárs	Intézkedés / megjegyzés

Rendszeres jelszóváltoztatás (a legfontosabb fiókoknál legalább évente egyszer)

A változtatás dátuma	Mely fiókokat változtattuk meg?	Ki változtatta meg?

Kiberbiztonsági képzés

A szervezet egységes eljárásainak felidézése, a gyanús viselkedés, e-mailek, telefonhívások és weboldalak felismerése és bejelentése, valamint az új fenyegetéstípusok megismerése.

A munkatársak kiberbiztonsági képzése			
A képzés témája	Tervezett időpont (nap vagy hónap)	Felelős személy	Megjegyzés

A biztonsági terv frissítése

A biztonsági terv frissítése			
A biztonsági terv verziója	A frissítés dátuma (hónap)	Személy	Megjegyzés

Hasznos linkek:

- 1) National Cyber Security Centre UK
<https://www.ncsc.gov.uk/section/advice-guidance/all-topics>
- 2) The Hacker News
<https://thehackernews.com/>
- 3) [ResilienceLab.online – Tanulási platform civil szervezeteknek](#)



**Co-funded by
the European Union**

Figyelmeztetés: Az itt kifejtett vélemények kizárólag a szerző(k) véleményét tükrözik, és nem feltétlenül tükrözik a TF, a GMF, a PDCS, az ACA és az EACEA véleményét.

G | M | F **Transatlantic
Foundation**

<https://www.gmfus.org/transatlantic-foundation>



<https://www.pdcs.sk>



<https://altkozegy.hu>