# Okostelefon.zip


## Információk

**A dokumentum verziója**: v0.2.4
**Projekt honlapja**: https://kiberitiner.hu/okostelefon
**Készíti**: Szőke Ágoston
**Közreműködők**: `<! -- Legyél te is közreműködő! -->`
**Visszajelzés:** https://kiberitiner.hu/okostelefon/#%F0%9F%93%A0hol-tudok-visszajelezni

## Verziótörténet

| Dátum | Verzió | Főbb változtatások |
|---|---|---|
| 2023.02.14. | v0.2.4 | |
| | | |

## Kapcsolódó dokumentumok

| Név | Verzió | Link |
|---|---|---|
| Kockázatelemzés - okostelefon.zip - gyerek | v0.7 | Drive |
| L1.1 - Irányítótorony | v1.0 | Drive |
| | | |

# Bevezető

Az okostelefonod életed meghatározó része lesz. Sok mindenre fogod tudni használni,  például kapcsolattartásra, mindennapi ügyek intézésére, szórakozásra, fotózásra, információszerzésre, játszásra. Az okostelefonod lesz az az ajtó, amin keresztül a legkönnyeben be tudsz lépni a digitális világba. A digitális világ nagyon érdekes és izgalmas, de elsőre nem könnyű kiigazodni benne.

Az okostelefon.zip felkészítő célja, hogy minél hamarabb megtaláld a tájékozódási pontokat ebben az okostelefonok által elérhető digitális világban. Az első „igazi” okostelefon, az iPhone 2007-ben jelent meg, azóta gyűlik a tudás a tudatos okostelefonhasználatról. Ezt a tudást vegyítettem a saját tapasztalatommal és tömörítettem bele ebbe a felkészítőbe. Remélem, hogy ennek segítségével Te már speedrunnolni tudod az okostelefon tudatos használatának megtanulását (az én generációmnak ez több évbe telt, ha egyáltalán sikerült).

Az okostelefon.zip felkészítőt négy fejezetre tagoltam:

1. Setup, használat: ez arról szól majd, hogy mire érdemes figyelni a telefon beállításakor, és tippeket adok a használatához. (nincs elkezdve)
2. Biztonság: ez a rész arról szól, hogyan tudod biztonságban tartani magad az online világban. Megtudhatod, hogy milyen fenyegetésekkel találkozhatsz az online térben és ezektől hogyan tudod magad megvédeni. (work in progress),
3. Mentális egészség: ez a fejezet azt mutatja be, hogy a közösségi média, a cyberbullying hogyan hat a mentális egészségedre. Szó lesz arról is, hogyan tartsd egyensúlyban az online és offline tevékenységeket. (nincs elkezdve)
4. Tartalomfogyasztás és produktivitás: Nem minden képernyőidő egyenértékű. Ez a fejezet abban segít, hogy a képernyő előtti időd minél tartalmasabb legyen.(nincs elkezdve)

A felkészítő nagy része szöveg, ami, tudom, instant RIP a rövid videók és a videójátékok korában. A szövegsűrűséget belinkelt videókkal (work in progress), tesztfeladatokkal és beállítási útmutatókkal igyekeztem oldani: bőven van lehetőség videót nézni és kattintgatni. Sőt, van néhány kinyomtatható lap is, amin lehet írni, kreatívkodni.

Az egyes fejezeteket és az egész felkészítőt rövid, feleletválasztós tesztek zárják, illetve van néhány gyakorlati feladat is (pl. telepíts egy alkalmazást és állítsd be rajta az adatvédelmi és biztonsági beállításokat). A sikeres feladatok és tesztkitöltések igazolásául kapsz egy oklevelet. A felkészülés során a feladatok megoldására jár pont, amiket a végén kis jelvényekre válthatsz be (work in progress) és akár felragaszthatsz majd az okostelefonodra.



Jelvény conceptek, a DALL·E 2 képgeneráló MI segítségével készültek.

[Press Any Button to Start]

# Tartalom



# Setup, használat

# Biztonság

## Mi a célja ennek a résznek?

Ez a rész az okostelefonodhoz kapcsolódó értékek védelméről, a Te biztonságodról szól.

Az okostelefonod tele van értékes adatokkal: fotók, bizalmas üzenetek, jelszavak, közösségimédia-appok. Az okostelefonon keresztül tudsz másokkal kapcsolatot tartani, információkhoz jutni. Ha ezek az értékes adatok elvesznek, más megismeri, vagy például online bántalmaznak az okostelefonodon keresztül, az kellemetlen, és néha sajnos kifejezetten fájó tud lenni. A rengeteg előnye mellett ez is hozzátartozik az okostelefon-használathoz, és ezért foglalkozunk ebben a részben a biztonsággal.

Biztonság?! Akkor itt a bonyolult jelszavakról, PIN kódokról, tiltásokról, rettegésről, sőt *kétfaktoros hitelesítésről* lesz szó? A rövid válasz az az, hogy igen, viszont furcsa módon a célja ennek a résznek, hogy minél több időt és idegességet spóroljunk meg neked. Valóban, a biztonság és a kényelem nem puszipajtások. Ha arról lenne szó, hogy van néhány internetes fiókunk, amikre néha ránézünk, akkor lehet hagyhatnánk ezt sok kényelmetlen biztonsági megoldást. A helyzet viszont nem ez: rengeteg fiókunk és alkalmazásunk van, és ezeket érdemes védeni. Ráadásul az alkalmazások valamilyen biztonsági megoldást alkalmaznak (sőt néha *kikényszerítik*, hogy használjuk ezeket). És ha már így-is úgy is be kell ezeket állítani, állítsuk be őket minél gyorsabban, hatékonyabban és fájdalommentesen.

## A biztonság elemei

### A biztonság elemei: üveggomb, kalapács és pajzs

Az alábbiak közül szerinted mi a biztonság?

a. A félelem hiánya.
b. A fenyegetések hiánya, vagy a fenyegetések kivédésének képessége.
c. Nem csinálok hülyeséget, ami miatt baj érhetne, és az eszközeim sem romlanak el maguktól.

Alapvetően a „B" a helyes válasz. A biztonság egy olyan állapot, amikor minimális a fenyegetettség, így „a biztonság a sérülékenységek [fenyegetések] hiányát vagy a fenyegetésekkel szembeni védelmet jelenti."[1] Ha az „A" választ jelölted, ne csüggedj, mert lehet egy nyelvész veszett el benned. A biztonság angol megfelelője, a security a latin se (fosztóképző) + cura -ae (f) (félelem)=securitas szóból jön, ami „félelem nélküliséget" jelent.

(Csöndben jegyzem meg, hogy van amikor csak biztonságban *érezzük* magunkat, de igazából nem *vagyunk* biztonságban – ez a hamis biztonságérzet. Erre példa, amikor valaki azt mondja, hogy ő teljesen biztonságban van, mert beállította a kétlépcsős hitelesítés, de egyébként minden linkre gondolkodás nélkül rákattint, és gyenge jelszavakat használ. Az alábbiakban arra törekszünk, hogy a biztonság valós szintjét növeljük.)

A biztonság több elemből tevődik össze: védendő elem, védelmi intézkedés, fenyegetés.[2] A fenyegetés legyen egy kalapács, a védelmi intézkedés egy pajzs, a védendő elem meg egy üveggömb. Mikor vagyunk biztonságban? Akkor biztos biztonságban vagyunk, ha nincs olyan kalapács (fenyegetés), ami össze akarná törni a szeretett üveggömbüket. Valamilyen kalapács ugyanakkor általában pályázik arra az üveggömbre, azaz fenyegeti azt. Ilyenkor kell egy olyan pajzs (védelmi intézkedés), ami kivédi a kalapács ütéseit, azaz kivédi a fenyegetést.

Az online biztonságodat hasonló módon tudod megteremteni. Az üveggömb az valamilyen védendő elem, érték. fontos adat, kép, jelszó, de akár a mentális egészséged is. Az a védendő elemet érheti fenyegetés (kalapács). A kibertérben kalapács lehet például a kétlépcsős azonosítással nem védett fiók feltörése. A kalapács ellen az üveggömb védelme érdekében pajzs, azaz védelmi intézkedés lehet kétlépcsős azonosítás beállítása.

A kibertérben sokféle kalapács, pajzs és üveggömb van. A biztonság eléréséhez ezeket ügyesen kell összeválogatni.

## Üveggömb-vadászat – Mi a védett elem?

A biztonságot értelmezhetjük úgy, hogy egy érték mekkora veszélyben van.[3] Ezt a védett értéket célozza a támadás, és ezt próbálja a védelem megvédeni.[4] Azaz, ha a kalapács csattan a pajzson, az nem azért van, mert jó a hangja, hanem azért mert egy üveggömböt össze szeretne törni. Az online biztonságodnál milyen üveggömbök jöhetnek szóba? Mik azok a védendő értékek, és az értéket hordozó védendő elemek, amiket a fenyegetésektől meg kell védeni?

Feladat: Kattints a linkre és döntsd el, hogy az adott érték mennyire fontos neked.

- F1.1 – Védendő értékek: https://forms.gle/HckhERdMoGdrft318

Ahova nagyon fontost, vagy fontost jelöltél, azok az üveggömbök amiket védeni érdemes, hogy biztonságban legyél.

---

[1] IT biztonság közérthetően 11. o. https://njszt.hu/hu/webform/it-biztonsag-kozerthetoen

[2] https://books.google.hu/books?hl=hu&lr=&id=4KOJ0m9M1MUC&oi=fnd&pg=PP1&dq=security+definition+theory&ots=Q-Z9XHSPHq&sig=V9cfg1r9x1SGywVddBOYC8OpZA4&redir_esc=y#v=onepage&q&f=true 15-16. o.

[3] https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/12604 18. o.

[4] https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/18030 6. o.

Ezeket az értékeket írd fel erre a lapra (vagy számítógépen írd be).

- L1.1 – Irányítótorony https://drive.google.com/drive/folders/10FOVB5WtJ6vtGkOogHqWRzuMmcYpuZr7

Konkretizáljuk, hogy ezek az értékek milyen védendő elemekben jelenhetnek meg az okostelefonodon.

Feladat: az egyes értékeknél válaszd ki a releváns védendő elemeket. [Google felmérés]

| **Védendő elemek az okostelefonodhoz kapcsolódóan** | |
|---|---|
| **Információ** | **Appok** |
| Chat üzenetek | Közösségi média alkalmazás |
| Bejelentkezési adatok (e-mail, jelszó) | Chat alkalmazás |
| Személyes adatok | E-mail alkalmazás |
| E-mailek | Google/IOS fiók |
| Képek | 2FA |
| Egészségügyi adatok | Játék |
| Névjegyzék | Okosotthon-vezérlés |
| Fájlok | Felhőszolgáltatás (Google Drive, OneDrive, iCloud) |
| Zenék | Jelszószéf |
| Bankkártya adatok | Zene streaming app |
| Tartózkodási hely | Videó streaming app |
| Érdeklődési kör | Android / iOS operációs rendszer |
| Információ | Telefon |
| Chat üzenetek | Böngésző |
| Bejelentkezési adatok (e-mail, jelszó) | SMS |
| Személyes adatok | Play Áruház / App Store |
| E-mailek | |
| Képek | **Hardverek** |
| Egészségügyi adatok | Okostelefon |
| Névjegyzék | Okosóra |
| Fájlok | Fitnesszkarkötő |
| Zenék | Fülhallgató |
| Bankkártya adatok | Töltő + kábel |
| Tartózkodási hely | Egyéb okoseszköz |
| Érdeklődési kör | |
| Információ | **Hálózat** |
| Chat üzenetek | WiFi |
| Bejelentkezési adatok (e-mail, jelszó) | Mobilinternet |
| | Bluetooth |
| | AirDrop |

Mellékelt táblázatban a vagyontárgyaknál láthatók a védendő elemek.

Az idő előrehaladtával egyre több üveggömböd lesz, azaz egyre több lesz a védendő érték és a védendő elem.

## Kalapács – milyen fenyegetésekkel nézünk szembe?

A kalapács széttörheti az üveggömböt, ami így sérül. Az online biztonságodat érintő fenyegetések olyan lehetséges műveletek, események, amik az okostelefonod és végső soron a Te biztonságodat sérthetik.[5]

Mielőtt megnézünk néhány példát a fenyegetésekre, ismerkedjünk meg gyorsan a sérülékenység fogalmával és a BSR hármasával. A sérülékenység a védendő elem, vagy védelmi intézkedés olyan gyengesége, amit a fenyegetés ki tud használni, vagyis amin keresztül a fenyegetés megvalósul.[6] Azaz, ha a pajzsunkon tátong egy lyuk, akkor a kalapács ezt ki tudja használni az üveggomb széttörésére.

A BSR rövidítés a következő fogalmakból tevődik össze:

- bizalmasság: az adathoz csak a jogosultak férnek hozzá (illetéktelenek nem)[7]. Példa: sérül a bizalmasság, ha egy támadó feltöri az e-mail fiókodat és elolvassa az üzeneteidet.
- Sértetlenség: az adat pontos és teljes.[8] Példa: sérül a sértetlenség, ha egy támadó a kórházi rendszerben átállítja a vércsoportod típusát a kórházi rendszerben.
- Rendelkezésre állás: az okostelefonod számodra elérhető, a rajta lévő adatokat tudod használni.[9] Példa: Lemerül a telefonod, sérül a rendelkezésre állás.

[Google űrlap BSR kvíz]

Az információbiztonság az adatok bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzéséről szól. Bármelyik sérül, sérül a biztonság is.[10]

Feladat

Miközben nézed a videókat jegyezd le a fenyegetés mit és hogyan célozhat (azaz mi a célzott üveggömb, milyen típusú kalapácsról van szó)?

https://www.youtube.com/watch?v=kzxwN8k4MSs Okostelefonos zsarolóvírus

https://www.youtube.com/watch?v=K8sPUexlZXc Zsarolólevél

https://www.youtube.com/watch?v=bJrIh94RSiI Meghackelt kávéfőzőgép

Mindegyik fenyegetés esetében a végső cél pénzszerzés. Az első és harmadik videóban zsarolóvírussal van dolgunk, míg a másodikban egy levélben zsarol a támadó.

Feladat: nézz utána az interneten a következő fenyegetéseknek.

- Zsarolóvírus
- Adathalász SMS (smishing)
- Grooming

Válaszolj a következő kérdésekre:

- Mi a védendő érték, a védendő elem?

[5] Ibtv 1 par 14., ISO 27000 3.74.
[6] ISO 27000 3.74, IT biztonságról közérthetően 15. o., IBTV 1 par 40.
[7] ISO 27000 3.10, Ibtv 1 par 8.
[8] ISO 27000
[9] ISO 27000 3.7 és Ibtv 1 par 38. alapján
[10] ISO 27000 3.28

- Mi a sérülékenység?
- Mi a fenyegetés? (Három mondatban, a saját szavaiddal)

| Fenyegetés | Sérülékenység | Védendő elem | Védett érték |
|---|---|---|---|
| | | | |

[Kockázatelemzésnél feladathoz itteni információk felhasznál]

Most nézzünk néhány példát a fenyegetésekre:

*Új telefon vs „vicces" osztálytárs*

Szituáció: Szünetben az egyik osztálytársad hozzáfér az új okostelefonodhoz, amin még nincs beállítva a PIN kóddal, vagy az ujjlenyomattal feloldható képernyőzár. Az osztálytársad úgy dönt, hogy itt az ideje egy jó kis pranknek, és a közös osztály-chatcsoportba, illetve néhány random ismerősödnek a Snap/Viber/Messenger stb. chatalkalmazáson elküldi a „buta vagyok 🙈" üzenetet.

| Fenyegetés | Fenyegetés típusa | Sérülékenység | B/S/R | Védendő elem | Védett érték |
|---|---|---|---|---|---|
| Illetéktelen hozzáférés chatalkalmazásokhoz | Cyberbullying | Képernyőzár hiánya | B | Chatalkalmazások | Mentális egészség |

*Adatvédelmi beállítások*

Szituáció: Kedvenc zenekarod a nyáron jön Budapestre, de hamar elkapkodták a jegyeket. Egy ismeretlen személytől egyszer csak kapsz egy üzenetet. Ebben azt írja, hogy neki van egy jegye, ami neki nem kell, és Neked adja, ha megírod a címedet, ahova küldheti. Furcsállod az esetet, ezért letiltod az illetőt. Néhány nappal később egy másik felhasználó ír rád, hogy látja a Pinterest/Facebook oldaladon, te is szereted a Wednesday sorozatot Netflixen. Ekkor már szólsz a szüleidnek. Közösen megnézitek a profilodat, ahol a Pinterestre/Facebookra regisztráltaknak látszanak a kedveléseid.

| Fenyegetés | Fenyegetés típusa | Sérülékenység | B/S/R | Védendő elem | Védett érték |
|---|---|---|---|---|---|
| Érdeklődésed ismeretén alapuló üzenetekkel becserkészés | Becserkészés | Hibás adatvédelmi beállítások | B | Közösségi média profil, érzékeny személyes adatok, preferenciák | Mentális egészség, magánszféra |

*Erőszakos tartalom*

Szituáció: Nemrég regisztráltál egy üzenetküldő alkalmazásra. Egyszer csak azt veszed észre, hogy az valamelyik ismerősöd berakott egy chatcsoportba anélkül, hogy arról neked előre szólt volna. Az egyik, számodra ismeretlen csoporttag egy felkavaró fotót küld be csoportba.

| Fenyegetés | Fenyegetés típusa | Sérülékenység | B/S/R | Védendő elem | Védett érték |
|---|---|---|---|---|---|
| Véletlen találkozás erőszakos, felkavaró tartalommal | Erőszakos tartalom | Chat alkalmazások működési módja | - | - | Mentális egészség |

*Törött kijelző*

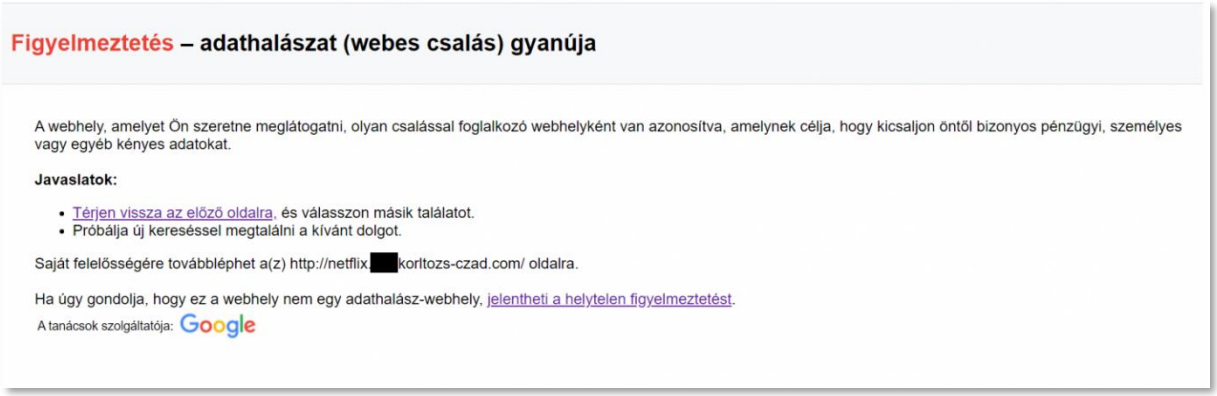
Szituáció: Rohansz, hogy elérd a reggeli buszt, zsebedben az okostelefonnal. Az utolsó métereken kicsusszan a teló a zsebedből, és néhány bukfenc után képernyővel lefelé kényszerleszállást hajt végre a térköves járdaszakaszon. Az telefonodon (ami nem egy Nokia 3310) nem volt sem üvegfólia a képernyőjén, sem ütésálló tok. A képernyő emiatt betört, csak egy része világít, és csak egy részén érzékeli az érintéseket. Pech, mert így most nem tudod használni a telódat, sőt lehet, hogy oda vannak a képek, és a kétlépcsős azonosításhoz tartozó alkalmazást sem éred el.

| Fenyegetés | Fenyegetés típusa | Sérülékenység | B/S/R | Védendő elem | Védett érték |
|---|---|---|---|---|---|
| Fizikai behatás miatt az okostelefon működésképtelenné válik, egyes adatok elveszhetnek | Technológia/fizikai | Üvegfólia, tok hiánya. Adatokról nincs biztonsági mentés. | R | Okostelefon, adatok. | Okostelefonhoz való hozzáférés. |

*Adathalász SMS*

Szituáció: Az iskolából edzésre sietsz, a vezeték nélküli Bluetooth-os fülhallgatón zenét hallgatsz. Pont eléred a villamost, csukódnak az ajtók, amikor egy pillanatra elhalkul a zene és egy értesítési hang hallatszik. A zene visszaerősödik, közben csekkolod az értesítéseket. Egy SMS-ed érkezett, a következő üzenettel:


Furcsa a szöveg, de elvégre Netflix fiókodról van szó, ezért rákattintasz a linkre, ahol ez a képernyő fogad:



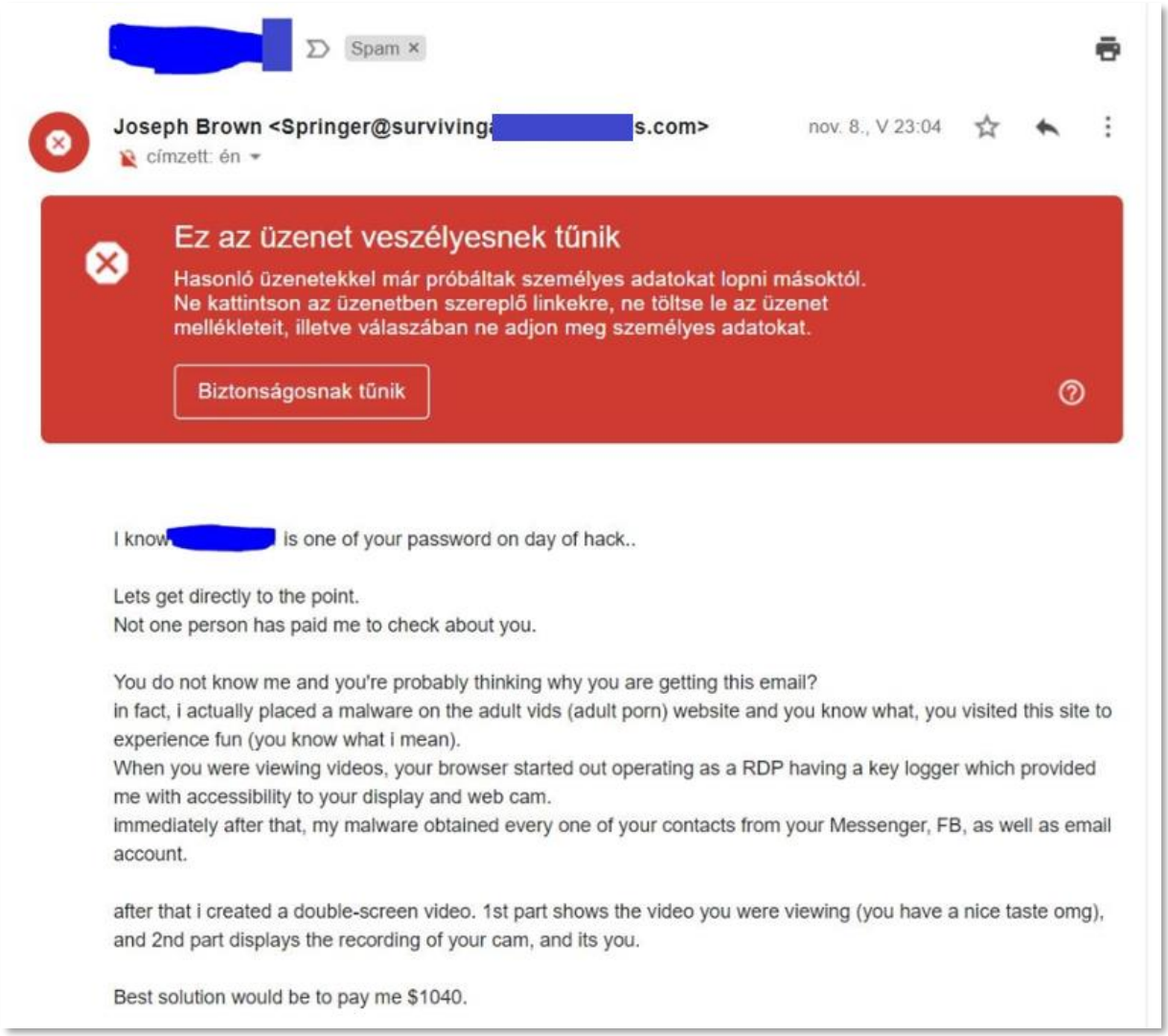

(Forrás: https://telex.hu/tech/2022/12/25/csalas-netflix-sms )

Itt már gyanús a történet[11], így bezárod a böngészőt. Később utánanézel a neten a Netflixes SMS üzeneteknek és kiderül, hogy ez egy adathalász kísérlet volt. Ha megadtál volna bankkártya adatokat, vagy Netflix felhasználónevet és jelszót, az adatok nem a Netflixhez, hanem csalókhoz kerülhettek volna.

| Fenyegetés | Fenyegetés típusa | Sérülékenység | B/S/R | Védendő elem | Védett érték |
|---|---|---|---|---|---|
| Smishing | Technológiai, social engineering adathalászat, | Emberi figyelmetlenség | B | Bankkártyaadatok, e-mail cím, jelszó | Pénz |

*Zsarolás*

Szituáció: Hazaértél az edzésről. Szerencsére nem dőltél be a Netflixes SMS-nek, így még hozzáférsz a sorozataidhoz. Egyszer csak pittyen a telefon. Egy e-mail érkezett:




[11] https://telex.hu/tech/2022/12/25/csalas-netflix-sms , https://24.hu/tech/2022/12/25/netflix-elofizetes-sms-atveres-csalas-adathalasz-uzenet/ , https://index.hu/tech/cellanaplo/2022/12/26/sms-uzenet-netflix-elofizetes-atveres-csalas/

Az e-mailben azt állítják, hogy hozzáfértek a webkamerádhoz és levideóztak. Ahhoz, hogy ezt ne publikálják pénzt kérnek tőled. Hallottál már az ilyen jellegű zsaroló üzenetekről, viszont azt veszed észre, hogy a zsarolók bizonyítékul egy jelszavadat is megküldték az e-mailben – és valóban egy olyan jelszóról van szó, amit korábban használtál. Ekkor már megfordul veled a világ és szüleid segítségét kéred. Megbeszélitek a dolgot, de nem fizettek (hisz mi gátolja meg a zsarolót utána abban, hogy mégis kiposztolja a videóidat). Szüleiddel együtt jobban utánanéztek a témának. Kiderül, hogy a jelszavad egy *adatszivárgás* miatt kerülhetett a zsarolókhoz.

| Fenyegetés | Fenyegetés típusa | Sérülékenység | B/S/R | Védendő elem | Védett érték |
|---|---|---|---|---|---|
| Zsarolás útján anyagi kár, adatok kiadása | Technológiai, social engineering , zsarolólevél | Adatszivárgás, emberi tényező | B | Bankkártyaadatok, e-mail cím, jelszó | Pénz, mentális egészség |

### *Google fiók, kizárás*

Egy délután sorozatot nézel, amikor sorban érkezik néhány értesítés a telefonodra. Az értesítések a Google-től érkeztek, ami kicsit szokatlan, mert nem emlékszel arra, hogy ilyen alkalmazást telepítettél volna. Az értesítések arról szólnak, hogy valaki máshonnan bejelentkezett a Google fiókodba és megváltoztatta a jelszót. Ez nem hangzik túl jól, mert az e-mailjeiden túl ott vannak a Drive-ban fájlok, fotók, elmentett jelszavak, illetve, húha, egy csomó fiók ezzel az e-maillel van regisztrálva. Ekkor már eluralkodik rajtad a pánik…

| Fenyegetés | Fenyegetés típusa | Sérülékenység | B/S/R | Védendő elem | Védett érték |
|---|---|---|---|---|---|
| A támadó hozzájut a jelszavadhoz és kizár a Google fiókodból | Technológiai | Adatszivárgás, 2FA és biztonsági e-mail cím hiánya | B | Google fiók és az ahhoz kapcsolódó adatok | Személyes adatok. Online fiókok elérése. |

Figyelem!
🔞 Az alábbi fenyegetés példa alkalmas lehet a nyugalom megzavarására, alapvetően 18 éven felülieknek szóló tartalom. A példa azért szerepel az anyagban, mert a tizenéves fiatalok sajnos kerülhetnek ilyen helyzetbe és a megelőzés fontos ezen a téren. A példa átugrásáért kattints ide.

### *Sexting*

„Pfú, csak ezek a hétfő reggelek ne lennének… Miért nem lehetne kedden kezdeni az iskolát, de úgy, hogy ne legyen hétfő hangulata, attól függetlenül, hogy akkor a kedd lenne a hétfő…” Ilyen gondolatok foglalkoztatnak, amikor belépsz az osztályterem ajtaján, ahol legalább már van élet, zsivaj. Most reggel viszont, amikor belépsz, egy pillanatra elhalkulnak a többiek és sutyorognak egy kicsit. Nem érted mi történik. Odamész a helyedre. Ekkor lép oda hozzád az egyik barátnőd és kérdezi, hogy igaz-e hogy szakítottatok. „Micsoda? Hisz eddig senkinek sem mondtam el” gondolod. Aztán kiderül, hogy a barátod, akibe megbíztál többeknek is elküldte a meztelen képeidet, amiket a Snapen küldtél.

| Fenyegetés | Fenyegetés típusa | Sérülékenység | B/S/R | Védendő elem | Védett érték |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| Sextinget követő bosszúpornó | Humán | Meztelen képek küldése | B | Képek | Magánszféra, mentális egészség, jó hírnév |

### *Kockázatokkal arányos védelem*

Mielőtt tovább megyünk a védelmi intézkedésekre fontos egy dolgot leszögezni: nem lehet és nem is éri meg *minden* kalapácsot kivédeni. Vannak olyan kalapácsok, amik olyan üveggömbökre pályáznak, amik neked (még) nem értékesek. Gyerekként például valószínűleg nincs sok pénzed, így például a biztonságos netbankolás kevésbé érint. Aztán lehetnek olyan kalapácsok, amik akkorát ütnek, hogy bármilyen általunk beszerezhető pajzs hatástalan velük szemben. Ilyen például a korlátlan erőforrással rendelkező, állami hátterű támadók esete, akik célzott támadásával szemben nagyon nehéz védekezni. Szerencsére magánszemélyként ilyen kalapáccsal nem nagyon találkozunk szembe. Azt is mondhatjuk, hogy egy ilyen támadás által okozott *kár* nagy lehet, a *valószínűsége* mégis nagyon alacsony. Azaz ennek a támadásnak számodra alacsony a *kockázata*.

A fenyegetések számbavételénél tehát vizsgálni kell annak a mértékét, azaz kockázatot[12]. A kockázat két dologtól függ:

- A fenyegetés bekövetkezési valószínűségétől,
- A kár nagyságától.

[Példa: Lila Lali, szorzás, + idő/pénz táblázat] , [Feladat: meghatározott fenyegetések – kár és valószínűség – 5 lalipénz elhelyez]

Láthatjuk, hogy Lali nem tudta a világ összes pénzét elkölteni a védelemre, így a legnagyobb kockázatok kezelésére költött. Lehet Lali nem tudott róla, de így *kockázatokkal arányos védelmet* valósította meg, ahol a védelem költségei arányosak a fenyegetések által okozható károk értékével.[13] A továbbiakban mi is erre törekszünk, azaz:

- Olyan üveggömböket védünk, amik valóban értékesek;
- Olyan kalapácsokat veszünk figyelembe, amik nem túl nagyok és valószínűleg a mi üveggömbjeinkre pályáznak;
- Olyan pajzsot választunk magunknak, ami megfelelően véd, de közben fel is bírjuk emelni.

[12] Ibtv. 1 par 28.
[13] Ibtv. 1 par 31.

*Mik azok a kockázatok, amiket csökkenteni érdemes?*

Az alábbi táblázatban megpróbáltam összefoglalni a legfontosabb kockázatokat, amik téged érhetnek.

A részletes táblázat itt található: https://docs.google.com/spreadsheets/d/1GgXzcGHK6qEWQl-p8jowPDyuxWHpxWaQ/

Feladat: menj végig a táblázaton és válaszd ki a top10 fenyegetést, ami téged szerinted érint, és írd rá a lapra. Ha van olyan ami kimaradt a táblázatból, azt írd le.

| Adatvagyon kategória | Kockázatos terület | Sérülékenység | Fenyegetés | Kockázat | Valószínűség | Következmény | Kockázati értéke | Prioritás |
|---|---|---|---|---|---|---|---|---|
| Információ | Bejelentkezési adatok (e-mail, jelszó) | Ugyanolyan jelszavak | Adatszivárgás | Illetéktelen hozzáférés sok online fiókokhoz (pl. Google, Spotify, Facebook stb.), akár egyszerre. | 3 | 5 | 15 | |
| Appok | E-mail alkalmazás | Hiányos biztonsági beállítások | Támadó feltöri az e-mail fiókot / hozzáfér. | Azzal az e-maillel regisztrált fiókoknál visszaállíthat jelszót más alkalmazásokban. | 3 | 5 | 15 | |
| Appok | Google/iOS | Adatszivárgásban jelszó kiderül (amit több helyen használsz), 2FA hiánya | Támadók hozzáférnek a fiókodhoz, kizárnak a fiókból | Fiók visszaszerzése időigényes, idegőrlő folyamat lehet. Támadok hozzáférhetnek a fiókban lévő adatokhoz (pl. képek, fájlok, e-mailek, névjegyzék), ezeket letölthetik, törölhetik. Elmentett bankkártyákkal fizethetnek bizonyos esetben. | 3 | 5 | 15 | |
| Információ | Érdeklődési kör | Hibás adatvédelmi beállítások | Érdeklődésed ismeretén alapuló üzenetekkel becserkészés | Ragadózó az érdeklődési körök alapján bizalmat megszerzi, érzékeny adatokhoz jut, zsarol stb. Mentális egészség, magánszféra sérülhet. | 3 | 4 | 12 | |
| Információ | Bejelentkezési adatok (e-mail, jelszó) | 2FA hiánya | Adatszivárgásban támadók hozzájutnak bejelentkezési adatokhoz | Illetéktelen hozzáférés online fiókokhoz (pl. Google, Spotify, Facebook stb.). (Ha egy jelszót több helyen használsz, akkor súlyosabb lehet a kár, több fiók lesz érintett - lásd eggyel lejjebb). | 3 | 4 | 12 | |
| Információ | Tartózkodási hely | Átgondolatlan megosztás. | Nyilvánosságra kerülés | Támadó, becserkésző fizikailag felkereshet. Biztonságérzet csökkenhet. | 3 | 4 | 12 | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Appok | Chat alkalmazás | Képernyőzár hiánya | Illetéktelen hozzáférés chatalkalmazásokhoz | "Buta vagyok 🤦" üzenet elküldése osztálytársaknak. Mentális egészség, jó hírnév sérülése. | 3 | 4 | 12 | |
| Appok | Chat alkalmazás | Hiányos biztonsági beállítások | Becserkészés, kéretlen üzenetek | Ragadozó megtalál a chatalkalmazásban, megpróbál becserkészni, a bizalmadba kerülni. Mentális egészség sérülhet. | 3 | 4 | 12 | |
| Appok | Chat alkalmazás | Tudatosság hiánya. Kíváncsiság | Az egyik ismerősöd mindenféle figyelmeztetés nélkül küld neked egy sextet, vagy más felkavaró, vagy erőszakos tartalmat. | Nehezen dolgozod fel a nem várt sextet, erőszakos tartalmat. Mentális egészség sérül. | 3 | 4 | 12 | |
| Appok | Jelszószéf | Emberi feledékenység | Mesterjelszó elfelejtése | Jelszavak visszaállítása időigényes (ha tudjuk, mit kell visszaállítani), bizonyos esetekben nem lehetséges. Stressz. | 3 | 4 | 12 | |
| Appok | Böngésző | Emberi kíváncsiság, véletlen | Erőszakos vagy pornográf tartalmakkal találkozás | Mentális egészség sérülhet. | 4 | 3 | 12 | |
| Hardverek | Okostelefon | Üvegfólia, tok hiánya. Adatokról nincs biztonsági mentés. | Fizikai behatás miatt az okostelefonon működésképtelenné válik (kijelző eltörik) | Okostelefon nem használható. Adatok elvesznek. | 3 | 4 | 12 | |
| Információ | Képek | Sexting (Meztelen képek tárolása, küldése) | Sextingből eredő képek nyilvánosságra kerülése | Meztelen képek nyilvánosságra kerülése, jó hírnév, magánszféra, mentális egészség sérül | 2 | 5 | 10 | |
| Appok | Böngésző (Android) | Figyelmetlenség, sietés. Utánaolvasás, tudatosság hiánya. "Olcsóbbnak tűnik." | Sideloading (az alkalmazást nem a hivatalos, Play Áruházból töltöd le, hanem egy weboldalról töltöd le, majd telepíted az alkalmazás apk fájlját) | Az app érzékeny adatokhoz fér hozzá. | 2 | 5 | 10 | |
| Információ | Bejelentkezési adatok (e-mail, jelszó) | Pszichológiai tényezők | Zsaroló e-mail (adatszivárgásban kikerült jelszó is lehet benne) | Ijedtség miatt fizetés a támadóknak, vagy érzékeny adatok megadása. Stressz. | 3 | 3 | 9 | |
| Információ | Személyes adatok | Biztonsági hiányosságok.* | Identitás lopás | Barátoknak a nevünkben üzenetek küldése, becsapása. Tevékenységek végzése a nevünkben. | 3 | 3 | 9 | |
| Appok | Közösségi média alkalmazás | Emberi érzelmekre hatás, emberi hiszékenység, figyelmetlenség. Tudatosság hiánya. | A hírfolyamban álhírrel találkozol. | Nem ismered fel az álhírt a hírfolyamban. Az érzelmileg befolyásol. | 3 | 3 | 9 | |
| Appok | Böngésző | Legális megoldás drága vagy körülményes. | Illegális tartalmak letöltése internetről. | Illegális tartalom káros kódot tartalmaz, ami megfertőzi a telefont. Adatvesztés veszélye. | 3 | 3 | 9 | |

## Pajzsok – hogyan védheted magad?

A kalapácsok ütéseit pajzsokkal lehet felfogni. Azaz a védelmi intézkedésekkel lehet csökkenteni a korábban bemutatott fenyegetések hatásait, valószínűségét, így végső soron a kockázatokat. Most nézzük meg, most nézzük, meg, hogy a korábban említett kalapácsokat milyen pajzsokkal tudtad volna kivédeni. Utána bemutatom a jó gyakorlatokat, azaz azokat a pajzsokat, amiket általában érdemes használni.

### *Új telefon vs „vicces" osztálytárs*

| Fenyegetés | Fenyegetés típusa | Sérülékenység | B/S/R | Védendő elem | Védett érték |
|---|---|---|---|---|---|
| Illetéktelen hozzáférés chatalkalmazásokhoz | Cyberbullying | Képernyőzár hiánya | B | Chatalkalmazások | Mentális egészség |

**Pajzs** (védelmi intézkedés): képernyőzár beállítása. Tudatosság.

**Magyarázat**: Ahogyan az e-mail fiókodat, vagy egy laptopon a felhasználói fiókodat védeni lehet jelszóval, ugyanúgy az okostelefonnál is be lehet állítani egy PIN kódot, mintát, vagy biometrikus azonosítást (fura szó, de általában ujjlenyomatról, vagy arcfelismerésről van szó), aminek segítségével a lezárt képernyő feloldható. A képernyőzár beállítása mellett fontos a tudatosság is. Hiába van PIN kóddal levédve a telefonunk, ha azt valaki a vállunk fellett kilesi, amikor bepötyögjük (ezt a támadást hívják shoulder surfingnek), vagy ha az okostelefont feloldott állapotban hagyjuk ott a padunkon.

**Beállítás**: [wip] Ne használjunk egyszerű PIN kódot (1234)…

**Rendszer**: Az ujjlenyomatos feloldás kényelmes, és többnyire kiváltja a PIN kód használatát. De ne felejtsük el a PIN kódunkat! Az okostelefon újraindítása után például a rendszer kérni fogja azt, és csak utána használhatjuk megint az ujjlenyomatunkat. Szerencsére az operációs rendszerek már segítenek nekünk, és időről időre rákérdeznek a PIN kódra. Ha valaki feledékeny, lehet érdemes a kezdeti időszakban biztonságos helyre felírni a PIN kódot. (Tipp egy idő után megjegyezhetetlen mennyiségű PIN kódunk lesz, így szerintem ha okosan csináljuk, akkor több helyen is lehet ugyanazt a PIN kódot használni, és esetleg egy kis füzetben vezetni, hogy mely helyeken, mit használunk).

### *Adatvédelmi beállítások*

| Fenyegetés | Fenyegetés típusa | Sérülékenység | B/S/R | Védendő elem | Védett érték |
|---|---|---|---|---|---|
| Érdeklődésed ismeretén alapuló üzenetekkel becserkészés | Becserkészés | Hibás adatvédelmi beállítások | B | Közösségi média profil, érzékeny személyes adatok, preferenciák | Mentális egészség, magánszféra |

**Pajzs** (védelmi intézkedés): Amikor egy közösségi oldalra regisztrálsz, érdemes rögtön a beállításokban leellenőrzni, hogy az általad megadott adatokból *ki* és *mit láthat¸* illetve, hogy *ki* és *hogyan* léphet veled kapcsolatba.

**Beállítás**: Van két fogalom: az alapértelmezett adatvédelem[14] és alapértelmezett biztonság. Ez azt jelenti, hogy pl. egy közösségi oldalnál az lenne a legjobb, ha az oldal működtetője neked egyből úgy állítaná be a biztonsági és adatvédelmi beállításokat, hogy idegenek minél kevesebb adatot lássanak a profilodban. Ebbe az irányba haladunk, de sajnos még mindig szoktak trükközni a szolgáltatók. Ezért

[14] https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679&from=HU GDPR 25. cikk

azt javaslom, hogy regisztráció után nézd végig a beállításokat, állítsd be mindenhol a legszigorúbb lehetőséget. Utána, ahogy egyre jobban kiismered a platformot, lazíts ezeken a beállításokon. Olyan ez mintha egy házban először minden ablakot és ajtót becsuknál, a függönyöket elhúznád és csak után a kezdenél el azon gondolkodni, hogy vajon mennyire probléma, ha itt belátnak, kinek nyitom ki az ajtót, ha kopogtat stb.

**Rendszer**: Legyen a rutin része a regisztráció után az adatvédelmi beállítások átnézése. Útmutatók[15] keresése beállítás előtt.

*Erőszakos tartalom*

| Fenyegetés | Fenyegetés típusa | Sérülékenység | B/S/R | Védendő elem | Védett érték |
|---|---|---|---|---|---|
| Véletlen találkozás erőszakos, felkavaró tartalommal | Erőszakos tartalom | Chat alkalmazások működési módja | - | - | Mentális egészség |

**Pajzs** (védelmi intézkedés): Tudni róla.

**Magyarázat**: Ez egy különleges eset, mert nem biztos, hogy a fenyegetés bekövetkezését meg lehet előzni. A Magyarországon elterjedt chatalkalmazások közül egyelőre sem a Viber, sem a Messenger nem rendelkezik olyan funkcióval, amivel ki lehetne kapcsolni azt, hogy az ismerősök hozzáadhassanak egy csoporthoz. Azaz, ha valakivel ismerősök vagytok, akkor pikk-pakk berakhat egy csoportba, ahol számodra ismeretlen emberek is lehetnek. Ebben az esetben csökkentheti a kockázatokat, hogy tényleg csak olyanokat jelölsz vissza, akiket ismersz. Ami a leginkább segíthet, hogy egyáltalán tudsz róla, hogy ez lehetséges és így kevésbé lepődsz meg rajta, ha megtörténik.

[E-mail, vírusok[16] - az online világ működésének részei / 100%-os védelem nincs, nem mindig lesz mindenre beállítás].

**Beállítások**:[17]

**Rendszer**: Üzenetküldő alkalmazásoknál regisztráció után legyen rutin, hogy a beállításokban megnézed, ki és hogyan léphet veled kapcsolatba, ki rakhat be csoportokba. Regisztráció előtt ennek utána lehet nézni.

*Törött kijelző*

| Fenyegetés | Fenyegetés típusa | Sérülékenység | B/S/R | Védendő elem | Védett érték |
|---|---|---|---|---|---|
| Fizikai behatás miatt az okostelefon működésképtelenné válik, egyes adatok elveszhetnek | Technológia/fizikai | Üvegfólia, tok hiánya. Adatokról nincs biztonsági mentés. | R | Okostelefon, adatok. | Okostelefonhoz való hozzáférés. |

**Pajzs**: kijelzővédő üvegfólia, ütésálló tok. Biztonsági mentés

[15] https://kiberitiner.hu/tag/utmutatok/ , theverge.com, wired.com
[16] https://www.sciencedirect.com/science/article/pii/0167404887901222
[17] https://hu-hu.facebook.com/help/messenger-app/1759354747722950
https://help.viber.com/en/article/control-who-can-add-me-to-groups

**Magyarázat**: a törött kijelzők a mindennapok részei, így legalább egy üvegfólia rakass fel a telefonra, mielőtt *bármit* csinálnál rajta. Pont az első hetek az az időszak, amikor nagyobb eséllyel történik baleset a telefonoddal.

*Adathalász SMS*

| Fenyegetés | Fenyegetés típusa | Sérülékenység | B/S/R | Védendő elem | Védett érték |
|---|---|---|---|---|---|
| Smishing | Technológiai, social engineering adathalászat, | Emberi figyelmetlenség | B | Bankkártyaadatok, e-mail cím, jelszó | Pénz |

**Pajzs** (védelmi intézkedés): tudatosság, vírusirtó.

**Megjegyzés**: Vannak kalapácsok, amik ellen a legjobb pajzs az a te odafigyelésed, tudatosságod. A SMS-ben, vagy bármilyen más formában érkező adathalász kísérletek egy részét kiszűrhetik a SPAM védelmi rendszerek, de van ami így is átjut. Ilyenkor kell a gyanús jelekre odafigyelni (részletesen erről később):

- Olyan fiókhoz kérnek bejelentkezési adatot, ami nekünk nincs.
- A megadott link nem a hivatalos weboldalra mutat.
- Bejelentkezési adatokat kérnek.
- Sürgető hangvételű az üzenet.
- Külföldi számról érkezett az SMS.

Az ilyen SMS-ek kiküldése sokszor kampányokban zajlik, azaz tömegesen küldik ki őket. Ha figyeljük a híreket, sokszor lehet ezekről értesülni. Illetve ha gyanút fogunk, akkor célzottan utánanézhetünk az interneten, hogy más is kapott-e ilyen üzenetet.

**Beállítás**: vírusírtó. Hírek figyelemmel követése.

**Rendszer**:

*Zsarolás*

| Fenyegetés | Fenyegetés típusa | Sérülékenység | B/S/R | Védendő elem | Védett érték |
|---|---|---|---|---|---|
| Zsarolás útján anyagi kár, adatok kiadása | Technológiai, social engineering , zsarolólevél | Adatszivárgás, emberi tényező | B | Bankkártyaadatok, e-mail cím, jelszó | Pénz, mentális egészség |

**Pajzs**: Tudatosság. Jelszószéf. 2FA.

**Megjegyzés**: Ez egy elsőre nagyon kellemetlen fenyegetés. Emlékszem, amikor először kaptam ilyen e-mailt, frászt kaptam. Ami itt segít az az, hogy ismerjük a jelenség hátterét. A zsarolólevelek, különösen az ilyen sextortion típusúak túlnyomó többsége mögött nincs célzott támadás, azaz nem készült rólad ciki webkamerás felvétel. Ez inkább egy olyan pszichológiai trükk, aminek pont az a célja, hogy megijedj. Valószínűleg rajtad kívül több száz ezer másik embernek is küldtek ilyen levelet, és ha már néhányan rákattintanak, az megéri a támadóknak. És hogyan kerül a jelszó a levélbe? Mert az igazi frász amiatt jön az emberre, hogy egy valódi, általa használt jelszó is ott van. Ezt a jelszót a támadók valószínűleg egy adatszivárgásból ismerték meg. Honnan szivárog az adat? Sajnos még a

nagyobb cégeknél is előfordul, hogy az általunk megadott adatokat (e-mail cím, jelszó, telefonszám stb.) nem tudják kellőképpen megvédeni, és ahhoz hackerek hozzáférnek, akik aztán azt pénzért más hackereknek eladják, vagy a sötét weben elérhetővé teszik. A kedves zsarolóink meg fogják ezeket a kiszivárgott jelszavakat és beszúrják a nekünk küldött levélbe, ami már így egy fokkal szívhez szólóbb lett. Ezért érdemes minden oldalon más jelszót használni (jelszókezelő segítségével), és ahol lehet, a kétlépcsős azonosítást beállítani. Na, így hogy ismerjük a hátteret, lehetőleg ne adjunk meg semmilyen adatot a zsarolóknak, és ne is fizessünk nekik.

**Beállítások**:

**Rendszer**: Jelszókezelő. 2FA. Adatszivárgás figyelése.

*Google fiók, kizárás*

| Fenyegetés | Fenyegetés típusa | Sérülékenység | B/S/R | Védendő elem | Védett érték |
|---|---|---|---|---|---|
| A támadó hozzájut a jelszavadhoz és kizár a Google fiókodból | Technológiai | Adatszivárgás, 2FA és biztonsági e-mail cím hiánya | B | Google fiók és az ahhoz kapcsolódó adatok | Személyes adatok. Online fiókok elérése. |

**Védelmi intézkedés**: erős, egyedi jelszó. 2FA. Biztonsági e-mail cím. Biztonsági mentés.

**Megjegyzés**: Az online életednek kettő fontos bástyája van. Az egyik az okostelefon, amin keresztül rengeteg mindenhez hozzá lehet férni, a 2FA-s kódok, üzenetek is ide érkeznek. A másik pedig az iOS vagy Google fiókod, de Google fiókja szinte mindenkinek van. A Google fiókhoz elvesztése igen kellemetlen tud lenni: egyrész az ott tárolt adatok miatt (ha azok elvesznek, vagy a támadóhoz kerülnek), illetve sokszor a Google fiókhoz tartozó e-mail címmel regisztrálunk más oldalakra. A fentiek miatt érdemes átgondolni, hogy hogyan védjük a Google fiókunkat és ha elveszítjük hogyan férjünk hozzá. Az erős jelszó jó kiindulópont, de a fiók fontossága miatt állítsunk be 2FA-t is. Ezek használata már nagyon megnehezíti a támadók dolgát. A biztonsági e-mail cím beállítása segíthet fiókunk visszaszerzésében.

**Beállítások**: jelszó (link), kétlépcsős azonosítás (link),

[Adatszivárgás magyarázat]

*Sexting* [18]

| Fenyegetés | Fenyegetés típusa | Sérülékenység | B/S/R | Védendő elem | Védett érték |
|---|---|---|---|---|---|
| Sextinget követő bosszúpornó | Humán | Bizalom, meztelen képek küldése | B | Képek | Magánszféra, mentális egészség, jó hírnév |

**Pajzs** (védelmi intézkedés): Meztelen képek küldésének mellőzése. Ha mégis küldesz, akkor ne legyen könnyen beazonosítható.

**Megjegyzés**: [statisztika]. A meztelen képek nyilvánosságra kerülése, elterjedése borzasztó lelki problémákat okozhat, ezért a legegyszerűbb, ha senkinek nem küldünk ilyeneket. Persze, lehet csökkenteni a kikerülés valószínűségét, ha pl. Snapen, vagy más olyan alkalmazásban küldjük, ahol eltűnnek a képek. De ez se bombabiztos megoldás. Egyrészt képernyőképet lehet készíteni (amiről

[18] https://www.forbes.com/sites/brucelee/2018/09/08/here-is-how-much-sexting-among-teens-has-increased/ 27% kap

kapunk értesést), de akár egy másik telefonnal is le lehet fotózni. Küldhetjük olyan embernek a képet, aki éppen életünk szerelme és megbízunk benne, de sajnos ez is változhat.

**Beállítások**: -

**Rendszer**: -

## Védelmi intézkedés – jó gyakorlatok

Számtalan pajzs van, amivel védekezni lehet a támadások ellen, de nincs mindegyikre szükséged. Elég, hogy legyen egy megfelelő kollekció (vagy ha jobban tetszik loadout) a legszükségesebb pajzsokból.

Az, hogy kinek milyen pajzsokat érdemes összeválogatnia a védelem kialakításához attól függ, hogy mik a védett üveggömbök és milyen kalapácsokkal számol, illetve mennyit szeretne ráfordítani a biztonságra (pénzben, időben, kényelmetlenségben). Vannak azonban olyan pajzsok, amik általánosságban sok kalapácsnak megnehezítik a dolgát, így használatuk neked is ajánlott. Ezeket a védelmi megoldásokat szoktuk *jó gyakorlatoknak* hívni, azaz olyan hatékony módszerek, amiket az adott pillanatban a szakértők mindenkinek javasolnak használni.

Amikor biztonságról van szó, sajnos nincsenek csodaszerek. A biztonság mindig idő, kényelmetlenség és pénz. De mégis miért szúrunk ki magunkkal? Azért, mert ami nekünk kis kellemetlenség, az a támadóknak lehet, hogy nagyon nagy nehézséget okoz. A kétlépcsős azonosítás például nyűg. Én is nagyokat szoktam sóhajtani, amikor a gépen bejelentkezek valahova, de a másik szobába még át kell mennem a telefonért, hogy ott is megerősítsem a bejelentkezést. Ami viszont nekem plusz egy perc és öt méter séta, az a támadónak lehet, hogy egy plusz kártékony kód telepítése a telefonomra, vagy még egy célzott adathalász támadás – azaz nehezített pálya.

A pajzsok összeválogatását úgy is felfoghatjuk, hogy akadálypályát építünk a támadóknak. Kicsit hasonlóan ahhoz, ahogy Kevin a *Reszkessetek betörőkben* mindenféle csapdát állít a házában a két betörőnek, Harrynek és Marvnak.

### *Jó gyakorlatok*

### Google fiók biztonsági beállításai

#### Mire lesz szükségünk

- Google fiók (Gmail-es e-mail)
- Laptop vagy számítógép internetkapcsolattal (lehet okostelefon is, de most számítógépet célszerű használni).
- Okostelefon (lehetőleg SIM kártyával)
    - butatelefon vs okostelefon sorrend tisztáz (próba beállítás, vagy éles beállítás?)
    - Butatelefonban SIM kártya marad, okostelefon Wi-Fi-re csatlakoztat?
- Nyomtató vagy papír + ceruza
- Kis doboz vagy széf
- Egy másik e-mail cím (saját vagy családtag)

#### Előkészület

1. Ha nincs még, készíts egy Google fiókot.
2. Nyisd meg egy böngészőben a https://myaccount.google.com/security oldalt. Ha nem vagy még bejelentkezve a Google fiókba jelentkezz be.

#### Erős, egyedi jelszó

1. Görgess lefele a **Bejelentkezés a Google-ba** címsorig. Kattints a **jelszó** alcímre.

2. A biztonság kedvéért a Google kéri a jelenlegi jelszavadat (ez azért kell, hogy ha például valaki hozzáfér a laptopodhoz, a jelszavadat ne tudja egyszerűen megváltoztatni).
3. Adj meg egy új jelszót, a következőkre figyelj:
    a. Legyen minimum 8 karakter hosszú, de én inkább 14 vagy több karakteres jelszót ajánlok (Minél hosszabb és bonyolultabb a jelszó, annál nehezebb kitalálni).
    b. Legyen egyedi, máshol ne használd.
    c. Legyen megjegyezhető. (Ez fontos. A jelszavaknál azt mérlegeld mindig, hogy kellően bonyolult legyen, de meg is tudd jegyezni.)
    d. Ne legyen hozzád köthető (kutyád neve, születési dátum stb. ne legyen benne).
    e. A nagyobb biztonság érdekében rakhatsz bele nagybetűt, számokat, speciális karaktereket (pl. #, !, ., @ $ stb.)
    f. Nézzünk néhány praktikus módszert és példát
        i. Három véletlenszerű szó (vagy négy): válassz három véletlenszerű, nem túl rövid szót, és írd őket egymás után.
            1. pl.: `kalauz`**`bemondo`**`kaposzta`
            2. Előny
                a. megjegyezhető,
                b. kellően hosszú.
            3. Hátrány
                a. nem olyan erős, mintha lenne benne szám, speciális karakter.
        ii. Három véletlenszerű szó, „megfűszerezve”: nagybetű, szám, speciális karakterek beleírása, hozzáadása
            1. pl.: `kalau`**`Z`**`bemond`**`0`**`k`**`@`**`poszta`
            2. Előny
                a. kellően hosszú és komplex
            3. Hátrány
                a. A speciális karakterekbe, számokba, nagybetűkbe bele lehet kavarodni
        iii. Brutál-metál jelszó: válassz egy verset, mondókát, dalt és a betűk kezdőbetűit írd össze, majd fűszerezd meg kis és nagy betűkkel, speciális karakterekkel (javasolható?)
            1. Pl. **M**ég **ny**ílnak **a** **v**ölgyben **a** **k**erti **v**irágok, // **M**ég **z**öldel **a** **n**yárfa **a**z **a**blak **e**lőtt, (Petőfi Sándor: Szeptember végén)
            2. → `mnyavaKev?Mzany4ae`
            3. Előny
                a. Nagyon komplex
            4. Hátrány
                a. Bepötyögés sok idő lehet,
                b. Bele lehet kavarodni.
    g. Játék
        i. A következő oldalakon kipróbálhatod, hogy milyen erős egy jelszó. Hasonlítsd össze például azt, hogy az `123456`, az `almafa` és a `kalau`**`Z`**`bemond`**`0`**`k`**`@`**`poszta` jelszavak kitalálásához mennyi idő kell.
        ii. Ugyan ezek megbízható oldalak, a valós jelszavaidat a biztonság kedvéért ide ne írd be.
        iii. Oldalak

1. https://nordpass.com/secure-password/ (kattints a **No, use online strenght checker** gombra)
2. https://bitwarden.com/password-strength/

h. Tippek
   i. A friss jelszót könnyen elfelejthetjük, így az elején egy kis papírra felírhatjuk a jelszót, de tároljuk biztonságos helyen. 5-10 bejelentkezés, vagy mondjuk egy hét után biztonságosan semmisítsük meg a papírt.
   ii. Időről időre (minimum havonta) lépjünk ki a fiókunkból és jelentkezzünk be újra, hogy gyakoroljuk a jelszót. A bejelentkezve maradok opció ugyan kényelmes, de egy idő után elfelejthetjük a jelszavunkat.
   iii. Ha használunk külön jelszókezelőt, gondoljuk meg, hogy a fő Google fiókunkhoz tartozó jelszót is annak a segítségével akarjuk-e generálni és tárolni. Én azt javaslom, hogy a fő Google fiókhoz tartozó jelszót mi találjuk ki és jegyezzük meg. Így ha a jelszószéfünkhöz tartozó mesterjelszót elfelejtjük, a Google fiókhoz még hozzá fogunk tudni férni, és az onnan regisztrált oldalakhoz tudunk jelszóvisszaállítást kérni.

### Kétlépcsős azonosítás beállítása

1. Győződj meg arról, hogy tudsz nyomtatni, vagy legyen nálad papír + íróeszköz (a biztonsági kódokat kell majd kinyomtatni vagy leírni). Legyen nálad egy kis doboz vagy széf.
2. Legyen nálad az okostelefonod is, amin be vagy jelentkezve a Google fiókodba. Lehetőleg legyen SIM kártya is benne (azaz legyen hozzá telefonszám).
3. A https://myaccount.google.com/security oldalon görgess a **Bejelentkezés a Google-ba** címsorig. Kattints a **kétlépcsős azonosítás** alcímre.
4. Kattints az **Első lépések** gombra.
5. Add meg a jelszavadat (ez azért kell, hogy ha például valaki hozzáfér a laptopodhoz, a kétlépcsős azonosítás beállításait ne tudja egyszerűen megváltoztatni).
6. Többféle lehetőség közül választhatunk:
   a. A lehetőségek
      i. Telefonszám megadása
      ii. Biztonsági hardverkulcs használata
      iii. Google értesítések fogadása
   b. Melyiket válasszuk?
      i. A legbiztonságosabb ezek közül a biztonsági hardverkulcs (erről később), de ehhez kell egy külön, USB-re hasonlító eszköz.
      ii. Az SMS és az értesítés kevésbé biztonságos, mint a hardverkulcs, de még mindig sokkal jobb, mintha nem lenne semmilyen második lépcsős azonosítás.
         1. SIM swapping támadás
         2. MFA fatigue attack
      iii. Elsőre azt javaslom, hogy állítsuk be az SMS-es és az értesítéses megoldást. Utána leírom a többi lehetőséget is.
7. Adjuk meg a telefonszámunkat. Nyomjuk meg a **Tovább** gombot.
8. A telefonunkra érkező SMS-ben lévő kódot adjuk meg a weboldalon, majd nyomjunk a **Tovább** gombra, majd a **Bekapcsolás** gombra.
9. Sikerült! Már van SMS-es második lépcsős azonosítás. De mi a helyzet akkor, ha elveszik a telefonunk, vagy megváltozik a számunk? Erre megoldás a **Biztonsági kódok** menüpont. Itt 10

olyan, egyszer felhasználható kódot kapunk, amik segítségével egy-egy alkalommal tudjuk második lépcsőben azonosítani magunkat. Állítsuk be most ezeket.

10. Kattintsunk a **Biztonsági kódok** menüpontra, majd adjuk meg a jelszavunkat.
11. Kattintsunk a **Biztonsági kódok beszerzése** gombra, ekkor megjelennek a biztonsági kódjaink.
12. Kattintsunk a **Kódok nyomtatása** gombra és nyomtassuk ki a kódokat.
    a. Ha nincs nyomtatónk, akkor írjuk le azokat egy papírra.
13. A kinyomtatott kódokat pedig rakjuk az előkészített dobozba, amit rakjunk egy biztonságos helyre.
    a. Miért kell a doboz? Egy csomó fiók lesz még, ahol szükség lehet biztonsági kódok nyomtatására és tárolására, úgyhogy nagy segítség, ha ezek egy helyen vannak és nem kavarodnak el.
    b. Miért nem csak lementjük a gépre, vagy egy pendrive-ra a kódokat? Ha a támadó hozzáfér a gépedhez, akkor ezeket a fájlokat megszerezheti, törölheti. Ha a pendrive-ot ide oda hurcolod, az is elveszhet (ilyenkor egyébként újra lehet generálni a kódokat).
14. ++
    a. authenticator alkalmazás beállítása
    b. Biztonsági hardverkulcs

### Fiók helyreállításának módjai

Mi történik akkor, ha

- elfelejtjük a jelszavunkat,
- vagy elveszik a telefon, és vele együtt a kétlépcsős azonosítás,
- vagy feltörik a fiókunkat és kizárnak belőle?

Ilyenkor nagyon jól jön, ha van valamilyen helyreállítási lehetőségünk. Ez lehet a telefonszámunk, vagy lehet egy másik e-mail cím. A telefonos helyreállítás megint lehet, hogy egy fokkal gyengébb, mint a biztonsági e-mail cím (pl. ha hozzáférnek a telefonunkhoz, vagy SIM kártyához, akkor lehet, hogy a jelszavunkat sem kell a támadónak tudni ahhoz, hogy teljes hozzáférést szerezzen a fiókunkhoz és kizárjon belőle), de egyelőre ezt ne gondold túl. A lényeg, hogy legalább az egyik helyreállítási módot állítsd be, hogy a fenti problémák esetén ne teljen túl sok időbe a fiók visszaállítása.

Helyreállítási telefonszám beállítása[19]

1. A https://myaccount.google.com/security oldalon görgess a **Hogyan ellenőrizhetjük személyazonosságát?** címsorig. Kattints a **Helyreállítási telefonszám** alcímre.
2. Add meg a jelszavadat (ez azért kell, hogy ha például valaki hozzáfér a laptopodhoz, a helyreállítás beállításokat ne tudja egyszerűen megváltoztatni).
3. Kattints a **Helyreállítási telefonszám hozzáadása** szövegre.
4. Add meg a telefonszámodat, majd az SMS-ben érkező kódot add meg a webes felületen.
    a. Tipp: Ennek a telefonszámnak nem kell ugyanannak lennie, mint amit a kétlépcsős azonosításnál megadtál. Lehet valamelyik szülőd telefonszáma is.
5. Készen is vagyunk, ezentúl, ha valami fura történik a fiókodban, akkor itt a Google el tud érni. Illetve ha elfelejted a jelszót, akkor is segítség lehet ez a telefonszám.

Biztonsági e-mail-cím beállítása

[19] https://support.google.com/accounts/answer/183723

1. Gondold ki, hogy milyen e-mail címet szeretnél biztonsági e-mail címként megadni. Olyan e-mail címet érdemes megadni, amit rendszeresen használsz. Megadhatod valamelyik szülőd e-mail címét is. Utóbbi esetben szólj neki, hogy együtt csináljátok a beállítást, mert szükség lesz egy ellenőrző kódra, ami majd a szülőd e-mailjére érkezik.
2. A https://myaccount.google.com/security oldalon görgess a **Hogyan ellenőrizhetjük személyazonosságát?** címsorig. Kattints a **Biztonsági e-mail-cím** alcímre.
3. Add meg a jelszavadat (ez azért kell, hogy ha például valaki hozzáfér a laptopodhoz, a helyreállítás beállításokat ne tudja egyszerűen megváltoztatni).
4. Adj meg egy biztonsági e-mail címet (ne az legyen, amit most használsz). Érdemes valamelyik szülőd e-mail címét megadni, de lehet egy általad gyakran használt másik e-mail cím is (és annak is kell biztonsági e-mail cím, meg annak is… ez egy olyan ördögi kör, amibe bele lehet őrülni, még én se tudom, hogy erre a mi a jó megoldás, ha egyáltalán van. Ha van erre ötleted kérlek írd meg nekem.)
5. A megadott e-mail címre (pl. anyukád e-mailjére) érkezik egy ellenőrző kód, ezt kell a megjelenő űrlapon. Kattints az **Igazolás** gombra.
6. Készen is vagyunk, ezentúl, ha valami fura történik a fiókodban, akkor itt a Google el tud érni. Illetve ha elfelejted a jelszót, akkor is segítség lehet ez a biztonsági e-mail cím.

*Dokumentálás*

Gratulálok! A Google fiókodat már komoly pajzsok védik a kalapácsoktól. Nem ez lesz az utolsó e-mail cím, illetve kétlépcsős azonosítást amit beállítasz, úgyhogy még néhány percet szánjál arra, hogy leírod, hogy ehhez az e-mail címhez milyen bejelentkezési, biztonsági módok vannak. Ebben segít ez a [lap]. Ide fel tudod vezetni, hogy a fontosabb fiókjaidat milyen e-mail címmel regisztráltad, milyen kétlépcsős azonosítási módok vannak beállítva és az e-mail címek esetén mik a megadott helyreállítási módok. Ha kész vagy, tedd be ezt a lapot a dobozba a biztonsági kódok mellé, később még jól fog jönni. (Idővel rengeteg fiókod lesz, ahol szinte lehetetlen észben tartani, hogy hol milyen második lépcsőt használsz azonosításra).

### Jelszókezelő beállítása [próba, teszt – nem feltétlen egyből személyes használatra]

- Google Passwords?, Bitwarden?
- [Passkey technológia ismertető][20]

### Letöltés, adatvédelmi és biztonsági beállítások alkalmazásoknál

A népszerű appok készítői *mindent is* megtesznek azért, hogy minél könnyebben lehessen regisztrálni és utána használni az alkalmazásukat. Az adatvédelmi és biztonsági beállítások azonban már nem szoktak olyan egyértelműek lenni. Ebből a szempontból az appok az *easy to learn, hard to master* kategóriába esnek, azaz, könnyű az alapvető működést megtanulni, de a megfelelő beállítások megtalálása már nehezebb.

### Alkalmazás letöltése előtti teendők

1. Kutatás, tesztelés

Mielőtt letöltesz, vagy úgy igazából elkezdesz használni egy alkalmazást, végezz egy kis kutatómunkát, vagy teszteld az alkalmazást.

Keress rá az interneten, hogy miről szól az adott app, mi a története. Ha tudsz angolul, akkor érdemes úgy is rákeresni (vagy akár az oldalt lefordítani a Google-lel). Az angol nyelvű kutatáshoz nyugodtan kérhetsz segítséget szüleidtől is.

[20] https://blog.1password.com/unlock-1password-with-passkeys/ https://en.wikipedia.org/wiki/WebAuthn

pl. Mi a [BeReal]? vagy What is [BeReal]?

Keress útmutatókat az interneten arról, hogy milyen adatvédelmi, biztonsági beállításokat érdemes használni.

pl. [BeReal] adatvédelmi, biztonsági beállítások, [BeReal] privacy, security settings

Néhány angol oldal, ahol a népszerűbb alkalmazásokról lehet információt találni:

https://www.commonsensemedia.org/

https://protectyoungeyes.com/apps/

Angol nyelvű online újságok, amik szoktak útmutatókat is publikálni

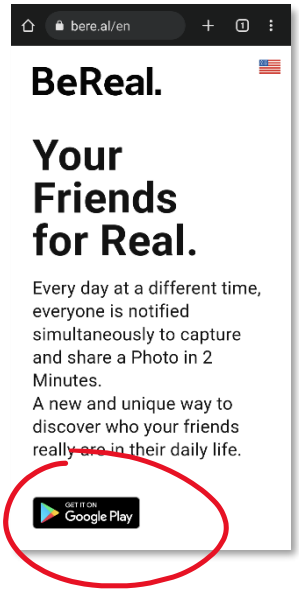
https://www.theverge.com/

https://www.wired.com/

A kiberitiner.hu oldalon itt találsz útmutatókat https://kiberitiner.hu/tag/utmutatok/ (egyelőre kevés van belőlük, de igyekszem 😊 )

Ha kevés az információ az appról, akkor lehet tesztelni is. Ehhez töltsd le az appot, regisztrálj rá egy másik e-mail címmel és addig nyomkodd, ameddig úgy nem érzed, hogy nagyjából átlátod a működését és a beállítási lehetőségeket. Ha végeztél, egyszerűen csak töröld a fiókodat. (Az igazán profik lejegyzetelheti, hogy mit, hol találnak).

2. Honnan




Fontos szabály, hogy alkalmazást csak a hivatalos app áruházból (Google Play Áruház, App Store) töltsél le. Androidon van lehetőség .apk fájlokat letölteni és telepíteni (*sideloading*). Ehhez viszont nagyon nagy körültekintés kell, mert így nagyobb eséllyel fertőződhet meg a telefonunk. A hivatalos app áruházba feltöltött alkalmazásokat szűrik.

A hivatalos app áruházból letöltött alkalmazásoknál is érdemes figyelni. Kicsi az esélye, de előfordulhat, hogy figyelmetlenségből a kívánt app helyet egy másikat töltesz le. Az ismertebb, régebbi alkalmazásoknál ennek kisebb az esélye, ilyenkor rákereshetsz az alkalmazás nevére az app áruházban.

Újabb, kevésbé ismert alkalmazásoknál érdemes megkeresni az app weboldalán a letöltésre mutató linket. A linkre rákattintva megnyílik majd az app áruház és onnantól mehet a menet.

**Kivédett kalapács:** káros kódot tartalmazó alkalmazás telepítése, ami elérhetetlenné teheti a telefont, vagy adatokat lop el róla.

3. Play store check
    a. Mielőtt a Google Playről, Apple Store-ból vagy az App Galleryből letöltesz egy alkalmazást három dolgot vizsgálj meg:
        i. van-e már három éve, hogy az alkalmazást megjelent,
        ii. megjelent-e már három verziója az alkalmazásnak,

iii. milyen adatokat gyűjt az alkalmazás?

b. A megjelenés ideje és a verziószám ellenőrzése segít kiszűrni a még „erősen fejlesztés alatt álló”/hiányos funkciójú appokat. A fiatal alkalmazások fejlesztésénél inkább az app működtetése és nem feltétlen a biztonsági szempontok vannak előtérben. Amikor eltelik néhány év, esetleg már túl van az app néhány biztonsági/adatvédelmi botrányon, akkor már nagyobb hangsúly lehet ezeken a szempontokon is.
   i. Google Play: Az app adatlapján görgessünk **az alkalmazásról** alcímig (játékok esetén **A játékról**) és kattintsuk is rá → Görgessünk lefele (viszonylag sokat) és nézzük meg az **Alkalmazás adatai** alcím alatt a **Verzió**t és a **Megjelenés idejét**.

c. A gyűjtött adatok ellenőrzése segíthet az olyan alkalmazások kiszúrásában, amik az általuk nyújtott szolgáltatáshoz képest több adatra tartanak igényt. Ha egy „zseblámpa” alkalmazás, vagy „akkuidőt hosszabbító/telefonkarbantartó” app hozzá akar férni egy csomó, nem releváns dologhoz (névjegyek, tartózkodási hely, képek stb.), akkor fogjunk gyanút.
   i. Play Store: Az app adatlapján görgessünk az **Adatbiztonság** alcímig és kattintsuk is rá → Nézzük meg a **Gyűjtött adatok** alcímnél miket gyűjt az alkalmazás
   ii. Apple Store:

d. példa: Elvileg anno az Instagramnál nem volt in-app megoldás a jelszavak visszaállítására. (Sarah Frier, No Filter)

**Kivédett kalapács:** bizonytalan adatgyűjtési módszereket alkalmazó appok telepítése, kiforratlan appok telepítése.

### Helyadat

A tartózkodási helyünk az érzékenyebb információk közé tartozik, ezért ennek megosztását az alkalmazással, de még inkább másokkal (pl. poszt elkészítésének helye) nagyon érdemes megfontolni.

Nézd meg az alkalmazás beállításokban (általában az adatvédelmi résznél van), hogy van-e lehetőség kikapcsolni a helyadatok megosztását másokkal.

Pl. A Snapnek van olyan funkciója, hogy folyamatosan megosztja a tartózkodási helyedet másokkal. Ennek kikapcsolása: **Beállítások → Privacy Control** címszó alatt **See My Location → Ghost Mode** bekapcsolása.

Ha olyan alkalmazásról van szó, ahol lehet posztolni, akkor vizsgáld meg, hogy a posztolásnál van-e lehetőség a tartózkodási hely megadására.

Pl. BeRealen megoszthatunk információt a poszt elkészítésének helyéről. Az alapértelmezett beállítás az az, hogy nem osztjuk meg helyzetünket, így itt nincs teendőnk, de érdemes tudni róla.

**Kivédett kalapács:** támadó, betörő, becserkésző a fizikai térben is megtalál, vagy a helyadataidat zsarolásra felhasználja. Stalking.

### Nyilvánosság, láthatóság

Bármilyen (közösségi) appnál három kérdést tegyél fel magadnak:

- Ki látja a felhasználói profilomat, adatlapomat?
- Milyen információkat és ki lát a profilomon, adatlapomon?

- Ki látja a bejegyzéseimet, posztjaimat?

A felhasználói profil láthatósága általában két kategóriába esik: bárki láthatja az interneten, illetve az adott app felhasználói láthatják. Ha bárki láthatja az interneten, az akár azt is jelentheti, hogy egy Google keresés során is felbukkanhat a profilod a keresési eredmények között. Ezt érdemes elkerülni, így ha esetleg nyilvánosra van állítva a profil láthatósága, azt kapcsold ki.

Nézd meg, hogy a profilodon milyen információk szerepelnek és ezeket ki látja. Egyes alkalmazások (pl. Facebook, de akár a Spotify is) meglepően sok személyes adatot kipakolhatnak a profilodra. Ezeket az adatokat több kategóriába sorolhatjuk:

1. Érzékeny személyes adatok, amiket lehetőleg senki ne láthasson a profilodon:
    a. Születési idő
    b. Tartózkodási hely, lakóhely
    c. E-mail cím, telefonszám
2. Személyes adatok, amik alapján érdeklődési köröd, tevékenységeid feltérképezhetőek
    a. Lájkolt, követett személyek, oldalak
    b. Kedvenc zenék, műsorok
    c. Legutóbbi posztok, lájkolt posztok
    d. Ismerősök
3. Profilra kirakott, „másoknak szánt” személyes adatok
    a. Profilkép
    b. elérhetőség, más oldalakra link (pl. Instagram)
    c. Munkahely, családi állapot (valaki ezeket kirakja, én nem javasolnám).

A harmadik kategória viszonylag egyértelmű, mert ezeket az adatokat aktívan szeretnénk másokkal közölni. Ilyenkor is figyelj viszont arra, hogy az alkalmazásban kik láthatják ezeket az adatokat (pl. csak ismerősök).

Az első és második kategória trükkösebb, mert ezek az adatok akár a tudtad nélkül gyűlhetnek fel a profilodon. Regisztrálsz egy e-mail címmel az alkalmazásra, belájkolsz néhány posztot, Spotify-on létrehozol lejátszási listákat, elmentesz képeket a Pinteresten – azaz egyszerűen csak használod az appot. Az alkalmazás viszont ezeket az információkat lehet, hogy nemes egyszerűséggel hozzácsapja a profilodhoz és bárki a platformon rád keres ilyen információkat is lát. Itt két dolgot lehet tenni:

1. Nyisd meg a saját profilodat és kattintgasd végig a megjelenített kategóriákat. Ahol lehet állítsd az adatok láthatóságát privátra.
    a. Facebookon pl. facebook.com/profile
2. Menj be az alkalmazás beállításaiba és keress olyan beállításokat, amik a profilodon lévő információk láthatóságával kapcsolatosak.

Ha ezeket megtetted, nézd meg, hogy más mit lát a profilodból (szokott lenni erre külön opció). Egyik ismerősödet is megkérheted, hogy keressen rá és nézze meg a profilodat.

[Instagram] – fiók privátra állítása

[Spotify] – kereshetőség korlátozása

A közösségi média appoknál nézd meg, hogy milyen beállítási lehetőségek vannak a posztolásnál. Itt érdemes majd azt az opciót választani, hogy csak az ismerősök lássák a posztjaidat (azaz ne legyen nyilvános, vagy az ismerős, ismerőse ne lássa, mert az már elég sok ember).

Tipp! A posztok az idővonaladon, profilodon a bejegyzést követően is ott maradnak és mondjuk az ismerőseid láthatják. Az ismerőseid száma viszont idővel nőni fog, így időről időre érdemes végiggondolni, hogy szeretnéd-e, hogy az új ismerőseid is lássák a régebbi posztjaidat.

**Kivédett kalapács:** érdeklődési köreid felmérésén alapuló becserkészés, identitás lopás. Stalking.

### Egyéb adatvédelmi beállítások

A helyadatok megosztása és a láthatósági beállítások talán a legfontosabb adatvédelmi beállítások, mert ezekkel csökkenthető a rólad könnyen elérhető információk mennyisége. Ezek mellett vannak olyan beállítások, amik haszna talán kevésbé kézzel fogható, de érdemes róluk tudni.

Az üzenetküldő és közösségi alkalmazások egyik kedvenc hobbija, hogy megkérdeznek arról, hogy hozzáférhetnek-e a kontaktjaidhoz. Az üzenetküldő alkalmazásoknál, ahol a telefonszám alapján történik az azonosítás (pl. Viber, WhatsApp, Signal) ez indokolt lehet, viszont más közösségi appoknál (pl. Facebook) már érdemes meggondolni, hogy van-e bármi előnye számunkra annak, ha hozzáférést adunk a kontaktjainkhoz.

Egyes üzenetküldő alkalmazásoknál van lehetőség eltűnő üzeneteket beállítani, vagy elküldött üzeneteket törölni. Ha érzékeny adatot osztunk meg (pl. jelszó, lakcím) akkor használhatjuk az eltűnő üzenet funkciót, hogy később, ha esetleg feltörik a partneredhez, vagy a hozzád tartozó fiókot, akkor ehhez ne férjenek hozzá. Az ismertebb chat appokon (pl. Messenger, Viber) csak rövidebb időre állítható be eltűnő üzenet, de más appokon (pl. Signal, WhatsApp) akár több hetes időt is beállíthatunk az üzenet eltűnésére, így ha esetleg valaki hozzáfér a fiókunkhoz, akkor csak az elmúlt néhány hét üzeneteit látja.

Trükkös tud lenni az, hogy az általunk posztolt, elküldött képekkel mi történik. Több alkalmazásban (Instagram, Snap, BeReal) van sztori funkció, ahol a kirakott kép/poszt csak egy bizonyos ideig látható a többiek számára. Ugyanakkor szokott lenni olyan beállítás, hogy számunkra az app elmenti a kirakott sztorit/posztot és azt később is megnézhetjük. Ennek bekapcsolásakor azt érdemes mérlegelni, hogy mennyire fontos nekünk, hogy megmaradjanak az emlékek vs mennyire lenne probléma, ha a fiókunk feltörése esetén ezt más is látná.

### Biztonsági beállítások

A közösségi alkalmazásoknak az a lényege, hogy egymással kapcsolatba kerüljenek a felhasználók. Vannak viszont olyan felhasználók, akikkel nem biztos, hogy kapcsolatba szeretnél kerülni. Ilyenek a becserkészők, idegenek. A közösségi alkalmazások többségében lehet szabályozni, hogy **kik jelölhetnek ismerősnek, illetve kik küldhetnek neked üzenetet**. Mind a kettő lehetőséget javasolt szűkíteni, azaz „ismerősök, ismerősei”, vagy „ismerősökre” beállítani. Az idegenektől érkező üzeneteket lehet külön helyre (pl. üzenetküldési engedélykérésekre) is kérni.

Ha valaki zaklat, vagy valamilyen más okból nem szeretnéd, hogy kapcsolatba legyetek egymással, az illetőt lehet **blokkolni**.

Az üzenetküldési appoknál nézd meg, hogy **ki rakhat be egy csoportba**. Lehetőleg erre csak ismerősök, vagy meglévő kontaktok legyenek képesek.

**Kivédett kalapács:** becserkészés, zaklatás.

A közösségi média alkalmazásoknál szokott lenni lehetőség képeken való **taggelés**re. Azaz, ha egy ismerősöd feltölt egy fotót, amin te is rajta vagy, akkor bejelölhet a képen egy profilodra mutató linkkel. A beállításokban általában lehet szabályozni, hogy csak akkor taggelhet be, ha te azt jóváhagytad.

Az alkalmazás fontosságától függően állíts be **kétlépcsős azonosítást**. Fontos, hogy a második faktor beállítását követően megjelenő **biztonsági kódokat** írd le, vagy nyomtasd ki és tedd az erre használt kis dobozba.

- [Google Authenticator beállítása útmutató – itt, vagy Google fióknál, SMS kód]

**Kivédett kalapács:** adathalászatból eredő fiókfeltörés.

## Biztonsági rendszer

### *Kapcsolatok az elemek között*

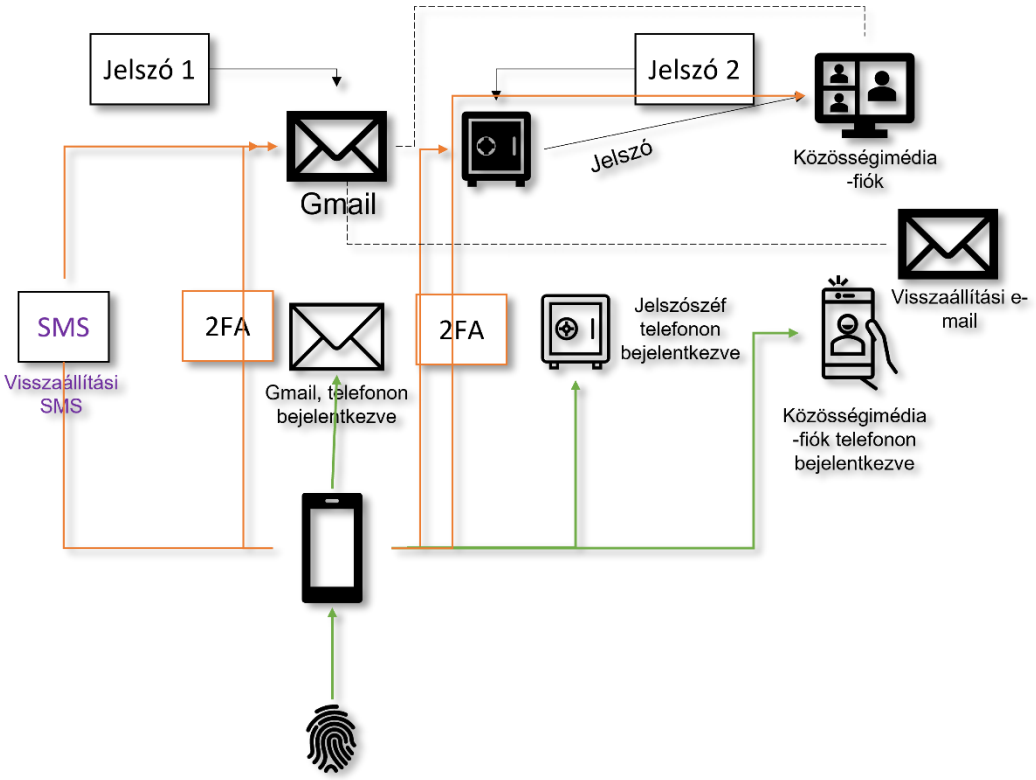
Mit csináltunk eddig?

- Létrehoztunk egy erős jelszót a Google fiókodnak,
- Beállítottunk kétlépcsős azonosítást a Google fiókodon, ehhez nyomtattunk backup kódokat,
- Beállítottunk SMS-es és e-mailes helyreállítási módokat a Google fiókodhoz,
- Beüzemeltünk egy jelszó kezelőt (szintén 2FA, backup kódok),
- A Google fiókodhoz tartozó e-mail címmel regisztráltunk egy appba, amihez a jelszót elmentettük, a jelszókezelőbe. Az apphoz beállítottunk 2FA-t és nyomtattunk hozzá backup kódot. Az app a telefonon elérhető, a telefonhoz van ujjlenyomat…

Egyelőre ennyi elég, most arra kérlek, hogy rajzold le az Google fiók, az okostelefon, a jelszókezelő és az app közötti kapcsolatokat.

- a regisztráció (gyakorlatilag a visszaállítás) legyen -----
- a bejelentkezés, ujjlenyomattal feloldás →

Én erre jutottam.



Igen, szerintem is elég borzasztóan[21] néz ki. De ez a valóság… Bocsánat, a valóság így néz ki:

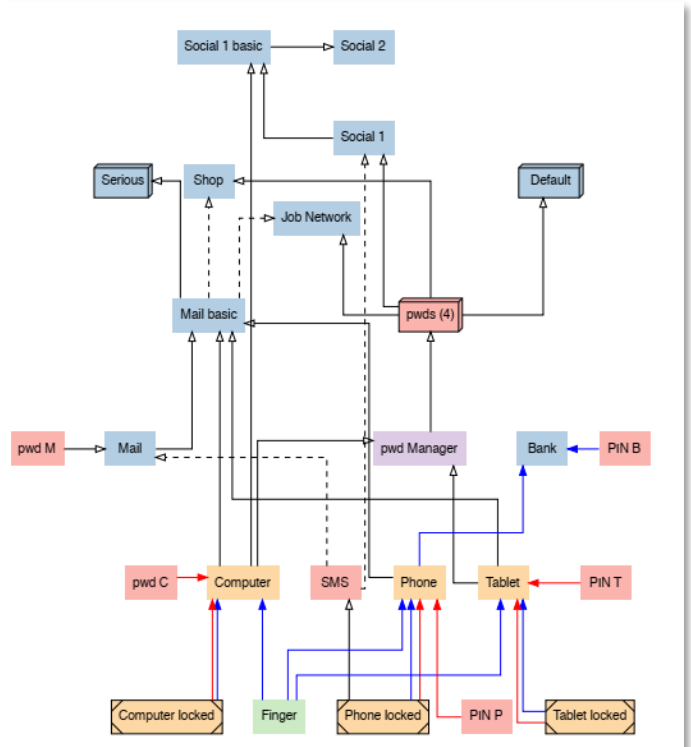



**Figure 3: Simplified Access Graph of participant P18. Some accounts have been removed. 3D-box-shaped vertices are contractions of vertices with the same access pattern.**

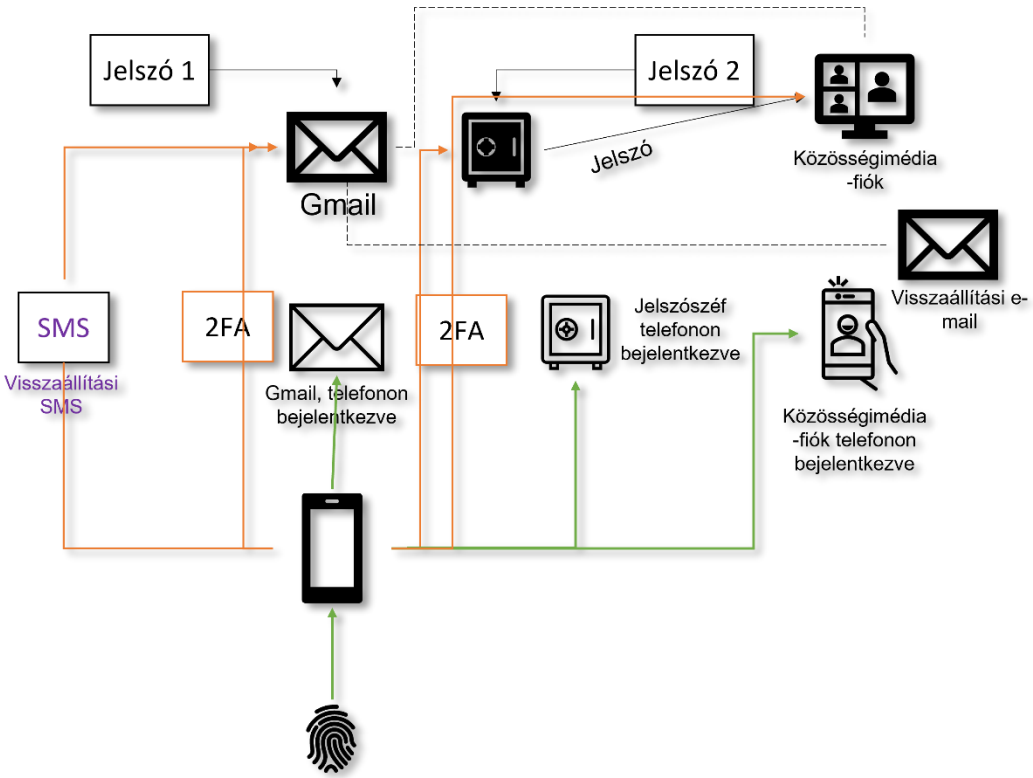
[22]

Az fiókjaid, az okostelefonod, SIM kártyád, a jelszavak, a számítógéped, az appok egy csomó módon kapcsolódnak egymáshoz, egy rendszert alkotnak. Ezt a rendszert átlátni is nehéz, nemhogy jól megtervezni.

Ahhoz, hogy ez néhány év múlva a rendszer ne legyen teljesen kezelhetetlen, és az összekapcsoltságból eredő kockázatokat kicsit csökkentsük, megpróbálok néhány támpontot adni (a téma elég új, így a támpontok, nos, béta verzióban vannak. Azt ajánlom, vegyél fel sisakot és sárga mellényt, ez még „építési terület” 🪖🦺🏗️👷🚧)

Kezdjük azzal, hogy elemezzük a mi kis ábránkat.

[21] https://knowyourmeme.com/memes/pepe-silvia
[22] https://dl.acm.org/doi/10.1145/3491102.3502125




Keressük meg a központi szereplőket az ábrán:

Az okostelefon központi szerepet játszik, mert egy ujjlenyomatos feloldást követően:

- hozzáférünk a bejelentkezett alkalmazásokhoz
  - Köztük a Google e-mail címhez is, amivel más alkalmazásokba regisztráltunk
  - A jelszószéfhez
- tudjuk fogadni a kétlépcsős azonosítás értesítéseit, hozzáférünk az authentikátor apphoz
- SMS-eket fogadunk

Fontos szerepet játszik az e-mail címünk, amivel az alkalmazásba regisztráltunk, illetve a jelszószéf, amiben a jelszavakat tároljuk.

Az egyensúlyt a között kell megtalálni, hogy ne legyen teljesen átlátatlan a rendszer, de legyen biztonságos is.

Mik a szűk keresztmetszetek:

- jelszavakból, PIN kódokból nem tudunk végtelen számút a fejünkben tartani
- a fontosabb fiókokból sem tudunk sokat menedzselni
- Az okostelefon központi szerepet játszik, de nem jellemző, hogy van otthon belőle egy gyorsan bevethető tartalék, ha az fő okostelefonunk elveszne. Ez főleg a kétlépcsős hitelesítés (és később majd a jelszó nélküli bejelentkezés) miatt lehet problémás.

*Támpontok*

Megjegyzendő jelszavakból próbálj minél kevesebbet használni, a maradékot bízd egy jelszószéfre (vagy később egy jelszónélküli rendszerre). A következő fiókokhoz érdemes külön jelszót kitalálnod:

- Fő e-mail fiók, amivel máshova regisztrálsz: ha itt elveszik a jelszó, akkor elég macerás lehet visszaállítani.

- Jelszószéf.

Ez a minimum szerintem, de általában szokott még lenni néhány jelszó, például másik e-mail címhez, esetleg fontosabb közösségi média profilokhoz, számítógép feloldása. De így együtt is 4-5 jelszónál nem érdemes feljebb menni.

A PIN kódok: a jelszó nélküli, ujjlenyomatos, arcfelismerős, kétlépcsős azonosítási világ rejtett bajkeverői. Amikor egy app, vagy eszköz ártatlanul arra kér, hogy még gyorsan állíts be egy PIN kódot, akkor néha valójában egy időzített bombát kapcsol be, mert ha ritkán írod be a PIN-t nagy esély van rá, hogy elfejted. Ez főleg később lesz érdekes amikor már lesz bankod, Revolutod, ahol egymás után jönnek a PIN kódok. Vannak olyan üzenetküldő alkalmazások is (pl. Signal, Telegramm), ahol az extra biztonság érdekében (kvázi második lépcsőként) egy PIN kódot lehet beállítani.

- Használd újra a PIN kódokat. Okosan. Ne mondjuk a bankkártyád PIN kódját, vagy a Revolutos PIN kódodat használd mindenhol. De például ha egy üzenetküldő app kér még egy PIN kódot a második lépcsőhöz, az lehet a képernyőzár PIN kódja (mert a PIN itt nem a feloldástól, hanem az újraregisztrációtól véd – a képernyőzár PIN kódját meg időről, időre be kell írni).
- Írd fel egy lapra, hogy hol használod ugyanazokat a PIN kódokat (ne magukat a PIN kódokat írd fel).

A kétlépcsős azonosításokhoz legyen tartalék módszered. A második lépcső funkciója hasonló a jelszóhoz, csak nem *tudás* hanem *birtoklás* alapú, azaz van egy olyan eszközöd, ami neked van és támadónak nincs és azon keletkezik, arra érkezik valamilyen kód/jelzés. Ha ez a birtokolt eszköz elveszik, akkor probléma lehet.

- A kétlépcsős azonosítás beállításakor (általában a folyamat végén) figyelj a megjelenő egyszer használatos **biztonsági kód(ok)ra**. Ez(eke)t a biztonsági kódokat nyomtasd ki, vagy írd le egy papírra (lehetőleg ne a számítógépeden tárold őket). Ebből a papírból garantálom, hogy lesz néhány, így ezeket gyűjtsd egy erre kijelölt dobozban (esetleg széfben).
- A fő e-mail cím esetén adj meg helyreállításhoz biztonsági címet/telefonszámot.
- Egy papíron, vagy fájlban érdemes vezetni, hogy melyik fiókhoz milyen második lépcsőst azonosítást használsz.
- Haladóknak: szerezz be biztonsági hardverkulcsot és (ahol lehet), állítsd be azt is második lépcsős azonosításnak (Apple, Google, Microsoft). A Yubico gyárt például ilyen biztonsági hardverkulcsot. Figyelem, egyes hardverkulcsoknál szükség lehet plusz PIN kódra.

Fiókok, regisztrált alkalmazások elkülönítése. Az átláthatóságban és a biztonságban is segíthet, ha nem egy e-mail címre regisztrálsz minden fiókot. Itt elég komoly viták lehetnek, hogy pontosan hányat, meg mire, de alapszinten szerintem két e-mail címet minimum érdemes használni:

- Fő e-mail cím: ezzel regisztrálhatsz a fontosabb alkalmazásokba. Ilyenek a közösségi média profiljaid, Spotify, Steam-fiók stb.
- Második e-mail cím: minden más, kevésbé fontos hely.

Az elkülönítés szempontjából kényes kérdés, hogy a két e-mail cím hogyan kapcsolódik egymáshoz (pl. a fő e-mail címről visszaállítható-e a második), illetve, hogy a fő e-mail címet a telefonra érkező

SMS kód segítségével vissza lehet-e állítani. Kialakulhatnak ugyanis olyan láncok, ahol egy fiók feltörésével, vagy egy helyreállítási mód megszerzésével más fiókokhoz is hozzá lehet férni (pl. SIM kártyához hozzáférés → SMS helyreállítás → fő e-mail fiók → második e-mail fiók → regisztrált fiók). Ez szerintem egyelőre az a kategória, amiről érdemes tudni, de úgy igazán jó megoldás még nincs rá és inkább csak beleőrülni lehet. Egyelőre tehát marad a több e-mail cím, a kétlépcsős azonosítás, illetve a probléma észben tartása.

### Biztonsági mentés

Az okostelefonod elvesztése, meghibásodása esetén a rajta lévő adatok is elveszhetnek. Ezek közül valószínűleg a képek elvesztése fájhat a legjobban, így a képekről készíts biztonsági mentést. A képek biztonsági mentésének a legegyszerűbb módja, ha egy hordozható külső merevlemezre (vagy SSD-re) (vagy a számítógépedre) időről-időre átmásolod a képeket.

Biztonsági mentés menete:

- Csatlakoztasd a külső merevlemezt a számítógéphez
- Egy kábellel csatlakoztasd a telefont a számítógéphez
- Androidos telefon esetén:
    - A telefonon nyisd meg az értesítéseket és keress egy rendszerértesítést: „Az eszköz töltése USB-n keresztül”. Kattints rá erre az értesítésre.
    - A megjelenő lehetőségek közül kattints a **Fájlátvitel**re.
- iOS esetén útmutató
- A számítógéped fájlkezelőjében keresd meg a telefonod ikonját/nevét. Kattints rá és navigálj el a képekhez (pl. Belső tárhely → DCIM → Camera). A telefon márkájától függően ez változhat. Ha problémába ütközöl keress rá az interneten (pl. where to find photos in Samsung/Huawei/Xiaomi file system from computer).
- Az itt talált képeket másold egy mappába a külső merevlemezeden.

A telefonod fotóit időről időre érdemes átválogatni. Ezzel egyrészt helyet lehet megtakarítani, másrészt a neccessebb fotókat is ki lehet gyomlálni. Ha nyugodtan oda tudod adni a telefonodat egy családtagnak, ismerősnek hogy böngéssze végig a képeket, akkor kevés rajta a necces kép.

A fotókat lehet felhőbe is menteni (pl. Google Fotók, iCloud), de ezt a rendszert én még nem teljesen látom át. Nagyon kényelmes megoldás, de azt érdemes észben tartani, hogy a fiók feltörése esetén ezen fotókhoz is hozzáférhetnek. A fotók rendszeres válogatása, a necces képek törlése ilyen megoldás esetén fontos. Azt a fiókot, ahova a képek mentésre kerülnek mindenképp védjük kétlépcsős azonosítással.

A fiókodból, jelszószéfből, okostelefondoból stb. összeálló rendszert karban kell tartani, időről-időre át kell gondolni. Olyan ez mint a biciklid: néha elég meghúzni rajta néhány csavart, kicsit megtisztítani, máskor el kell vinni a szerelőhöz, ahol fékpofákat cserélnek rajta, átállítják a váltót.

A rendszer karbantartása:

- telefonos fotók kiválogatása időről-időre,
- Ritkán használt jelszavak gyakorlása (pl. néhány hetente kijelentkezel a gépen a Gmail fiókból, majd vissza, hogy gyakorold a jelszót),
- Nem használt alkalmazások, fiókok törlése,
- Biztonsági, adatvédelmi beállítások átnézése.

Nagyjavítás, fejlesztés

- Jelszószéf bevezetése,
- Kétlépcsős azonosítás bekapcsolása,
- (jelszó nélküli bejelentkezés bekapcsolása),
- Új e-mail cím létrehozása,
- Biztonsági, adatvédelmi beállítások átnézése.

Ezek olyan dolgok, amiket nem érdemes hirtelen megcsinálni. Találjál rá nyugodt helyet, időt. Esetleg az éles bevezetés előtt teszteld a kinézett megoldást egy próba fiókkal.

Bármilyen változtatást végzel, főleg a PIN kódok, a második lépcsős azonosítás terén, azt valahol dokumentáld. Ez lehet egy jelszóval védett fájl a gépeden, vagy egy A4-es lap/füzet, amit a kis dobozodban/széfben tartasz.

- A4-es lap
    - jelszavak
    - PIN kódok
    - 2FA
    - biztonsági e-mail cím
    - HDD

## Tudatosság

### *Általános tanácsok*[23]

A megfelelő biztonsági beállítások, megoldások használata mellett a te online magatartásod is rendkívül fontos az online biztonságod érdekében. Sőt, talán ez a legfontosabb.

Az iskolában az informatikai tanárom azt mondta, hogy a számítógép, és azon belül az operációs rendszer, végső soron azon igyekszik, hogy a te kívánságodat teljesítse. Ez még szerintem akkor is sokszor így van, amikor a biztonságról van szó. Azaz hiába szól az okostelefonod, hogy „figyu, ez a link gyanús, ne kattints rá”, vagy „ez egy ismeretlen app, ne telepítsd” - ha te mégis úgy döntesz, hogy rákattintasz a linkre, vagy hogy telepíted az alkalmazást, akkor az a link megnyílik, az alkalmazás pedig települ, még akkor is, ha ezek kártékonyak.

Sőt, az okostelefon és rajta minden alkalmazás azért van elsősorban, hogy *használjad.* Persze, fontos szempont a biztonság is, de ha a biztonság lenne az első szempont akkor nem lehetne a telefonon:

- e-mailen, SMS-ben, üzenetben linket küldeni.
- E-mailen fájlt fogadni.
- Böngészőből fájlokat letölteni.
- YouTube-on a Baby Sharkon és a Peppa Malacon kívül mást nézni
- posztolni stb.

De mégis lehet ezeket és sok más dolgot is csinálni. Azaz nagyobb a szabadság, de nagyobb felelősséged is a biztonságot tekintve.

Az okostelefonod használatakor kicsit biztonsági őröset kell játszanod. Itt az álláshirdetés az okostelefonod biztonsági őr posztjára:

[23] https://securityadvice.cs.umd.edu/ , https://research.google/pubs/pub46306/

Az Első Okostelefonom Kft. biztonsági csapata kezdő biztonsági őr tanoncot keres. Csapatunk felelős napi több száz kattintás, üzenet és kép ellenőrzéséért, és végső soron több milliárd 5 nanométeres tranzisztor biztonságos működéséért.

A feladataid a következők lesznek:

- Figyelmeztetni a felhasználót, hogy gondolkodjon mielőtt kattint.
- Linkek, URL-ek biztonsági szempontú vizsgálata.
- Alkalmazások biztonsági átvilágítása.
- A biztonsági rendszerekből érkező figyelmeztetések értékelése.
- Az érkező és elküldendő üzenetek, képek, posztok biztonsági értékelése.

Milyen képességekkel kell rendelkezned?

- Éber vagy és hallgatsz a megérzéseidre.
- Megfontoltság, higgadtság gyors döntést igénylő helyzetekben.
- Elvégezted az okostelefon.zip biztonsági képzését (szakmai tapasztalat nem szükséges).
- Folyamatos tanulás az aktuális fenyegetésekről.

Mit ajánlunk?

- Biztos jövő.
- Okostelefon (részletekről érdeklődj a szüleidnél 😊).

A elvárt képességek közül az egyik legfontosabb és legáltalánosabb a következő:

Gondolkodj mielőtt kattintasz!

Ez mindig segít, legyen szó linkre kattintásról, üzenetküldésről, fájlletöltésről, képmegosztásról, posztolásról, adatvédelmi beállításról stb. Az okostelefonod az esetek többségében teljesíti a kív.. kattintásaidat (még akkor is, ha tudja, hogy az adott oldal, fájl necces lehet), így a kattintásodnak súlya van, egyfajta szupererő, aminek ennek megfelelően is kell bánni.

Biztonsági őrként három dologra kell figyelned:

- ami „be szeretne jönni” az okostelefonra
- ami „ki szeretne menni” az okostelefonról
- ami az okostelefonon történik.

### *Ami bejön*

#### Linkek vizsgálata[24]

- Magyarázat
- feladat

#### Adathalász e-mailek (phishing)

[Phishing átdolgozásra szorul]

Mi ez?[25]

[24] https://www.youtube.com/watch?v=UD-ukjVoeLc The Trouble with URLs

[25] https://attack.mitre.org/techniques/T1566/ , https://us.norton.com/blog/online-scams/what-is-phishing , https://csrc.nist.gov/glossary/term/phishing , https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html

Az adathalászat e-mailekkel a támadók célja, hogy érzékeny információt (felhasználónév, jelszó, személyes adatok) szerezzenek tőled. Ezt teszik, hogy becsapnak téged azzal, hogy az e-mailben másnak adják ki magukat (pl. futárcég, bank, streaming szolgáltató) és így kérik el tőled az információt.

https://www.youtube.com/watch?v=L3BSb_cLT3k , Telekom, mi az adathalászat (HU)

https://youtu.be/N7N4EC20-cM?t=652 Hacking Google, adathalászat példák (EN)

Az adathalász leveleknek több fajtája van.

- Van ahol válaszüzenetben kérik, hogy adjuk meg az adatainkat.
- Van viszont olyan, ahol egy linkre kell kattintani és a megnyíló oldalon kérik az adataidat

[statisztika] , videó, kép

Hogyan ismered fel az adathalász e-mailt?[26]

Technikai jegyek

- e-mail cím ellenőrzése[27]
- link ellenőrzése
    - példák[28]
    - anatómia
    - PC: kurzor fölé visz
    - Mobil: hosszan rányom

E-mailben szereplő információ

- Megszólítás: általános, nem személyre szóló
- feladó: ismeretlen feladó, vagy magát másnak kiadó feladó
- Valamilyen komoly szervezetnek, személynek adják ki magukat
    - Rendőrség, bank, orvos
- Sürgető hangvétel
- Érzelmet vált ki belőled az üzenet (pánik, félelem, remény, kíváncsiság)[29]
- Üzenet tartalma:
    - személyes adatokat kérnek (bejelentkezési adatok, bankkártya, lakcím, név)
    - valamilyen cselekedetre rá akar venni (adat megadása, kattintás, melléklet megnyitása)
- Nyelvtani hibák (profi adathalász leveleknél ez kevésbé)

Körülmények

- Nem vagy regisztrálva az adott szolgáltatásra
- Adott futárcégtől nem vársz csomagot

[26] https://nki.gov.hu/wp-content/uploads/2020/10/phishing_flow-1.pdf , https://www.ncsc.gov.uk/collection/phishing-scams/spot-scams https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/phishing-program-infographic.pdf
[27] https://www.crowdstrike.com/cybersecurity-101/spoofing-attacks/email-spoofing/
[28] https://telex.hu/tech/2022/04/28/kiberbiztonsag-orosz-hekkerek-apt-28-kormanyzati-oldalak-kormanyhivatalok-gov-hu-qov-hu-adathalaszat-typosquatting-misspelling-domain
[29] https://www.ncsc.gov.uk/collection/phishing-scams/spot-scams

- Nem vársz ilyen jellegű üzenetet

Minél célzottabb a támadás, annál nehezebb felismerni. Sőt, kisebb a valószínűsége, de akár az is előfordulhat, hogy egy ismerősöd e-mailjét feltörik és arról küldenek üzenetet.

    - Néven szólít
    - ismerősöd e-mailjét feltörik
- URL, e-mail cím
    - hasonló, de nem ugyanaz
-

Mit csinálj?[30]

- Gyanús e-mailt ne nyiss meg (tárgy)
- Gyanús linkre ne kattints
- Ne küldj érzékeny adatot e-mailen
    - Személyes adat (lakcím, személyi szám, jelszó) – ezeket szolgáltatók így nem szokták kérni
    - Ha ilyet kell csinálni, akkor menj a szolgáltató honlapjára közvetlenül és ott lépj be (semmiképp sem az e-mailben küldött linken keresztül)
- Gyanús fájlt ne tölts le
    - semmitmondó név (pdf.pdf)
    - Tömörített, jelszóval védett fájl.
- zsarolás

Kártékony fájlt tartalmazó e-mail

### Adathalász SMS (smishing)[31]

Mi ez?

A smishing (SMS + phishing) olyan adathalász támadás, ami SMS üzeneten keresztül érkezik. Az e-mailes adathalász támadásokhoz hasonlóan a támadók itt is másnak adják ki magukat (pl. futárcég, bank, Netflix) és így próbálnak meg rávenni,  hogy kattints rá egy linkre.

A linkre való rákattintás után olyan oldalra juthatunk, ahol érzékeny adatok megadását kérik, vagy egy káros alkalmazás letöltésére és telepítésére kérhetnek.

[példák]

[FluBot]

Az e-mailhez képest az SMS egy fokkal „komolyabb” kommunikációs csatornának tűnhet, így az itt érkező üzeneteket fontosnak titulálhatjuk – ez adja a smishing veszélyét.

Hogyan ismered fel a smishinget?

[30] https://nki.gov.hu/figyelmeztetesek/tajekoztatas/tajekoztatas-a-magyar-posta-nevet-es-arculati-elemeit-felhasznalo-adathalasz-uzenetekkel-kapcsolatban/

[31] https://www.bitdefender.com/blog/hotforsecurity/how-to-recognize-and-avoid-smishing-attacks/ , https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it , https://www.telekom.hu/rolunk/telekom_vilaga/biztonsagi_tartalmak/csalas/sms

E-mailhez képest nehezebb, csak szöveg van, nincsenek vizuális támpontok.[32]

Technikai jegyek:

- telefonszám ellenőrzése: külföldi telefonszám (nem +36-tal, vagy 06-tal kezdődik) mindenképp gyanús
- Link ellenőrzése:
    - furcsa domain

Üzenet tartalma:

- hasonló e-mailhez
- Sürgető hangnem
- Személyes adatok megadását kéri

Körülmények

- Nem vagy regisztrálva az adott szolgáltatásra
- Adott futárcégtől nem vársz csomagot
- Nem vársz ilyen jellegű üzenetet

Mit tegyél?

- ne reagálj egyből

Mit ne csinálj?

- linkre ne kattints rá
- Személyes adatokat ne adj meg
- Ne telepíts alkalmazást
- Ha a telefonod spamként jelöli meg az SMS-t, ne kattints rá a linkre!

Phishing teszt

### Üzenetek

Az e-mailes és SMS-es adathalász üzenetek nagy veszélyt jelentenek, de minden más beérkező üzenet esetében sem árt az óvatosság. A chat alkalmazásokban is érkezhet káros link, fájl, vagy felkavaró erőszakos/pornográf tartalom. Elsősorban az idegenektől érkező üzenetekre kell figyelni, de kisebb eséllyel az is előfordulhat, hogy ismerősöd fiókját szerzik meg a támadók, vagy ismerősöd kattint olyan linkre amire nem kéne, és tőle érkezik veszélyes link.

Példa: https://www.kaspersky.com/blog/facebook-messenger-malware/18412/ kártékony facebook üzenet

https://nakedsecurity.sophos.com/2012/04/20/photo-facebook-malware/ te vagy ezen a képen

Hogyan ismered fel?

- Ha idegen küldte neked az üzenetet, légy mindig gyanakvó.
- Ismerőstől érkező veszélyes üzenetet nehezebb felismerni. Ilyenkor az ő stílusától eltérő üzenetek esetén fogjunk gyanút.
- Az üzenet valamire rá szeretne venni:
    - nyiss meg egy linket

[32] https://www.f-secure.com/en/home/articles/what-is-smishing

    - tölts le egy fájlt
- Link vizsgálata
- Fájl vizsgálata
    - furcsa fájlkiterjesztések, tömörített fájlok gyanúsak
- Erőszakos, pornográf tartalom
    - egyes üzenetküldők elhomályosítják az olyan üzeneteket, amin meztelen embereket vagy valamilyen erőszakos cselekedet ábrázoló képet tartalmaznak

Mit tegyél?

- Gyanús linkre ne kattints rá, gyanús fájlt ne tölts le.
    - Ha mégis rákattintottál ne adj meg személyes adatokat, és ne tölts le ismeretlen programokat.
- Ha idegen ír rád, a legegyszerűbb, ha nem válaszolsz neki.
- Ha lehetséges, hogy ismered az illetőt, de nem vagy biztos benne akkor:
    - kérdezz rá olyan nem érzékeny dolgokra, amiket csak ti ismerhettek
    - Valamilyen más kommunikációs csatornán is próbáld meg felvenni vele a kapcsolatot (pl. eddig Viberen kommunikáltatok régen, most bejelölt Facebookon)
- Ha ismerősöd gyanús üzenetet küld:
    - Várj egy kicsit.
    - Kérdezz rá (akár egy másik kommunikációs csatornán), hogy tényleg ő küldte e.
    - Másold ki a szöveget és keress rá Google-n. A „vírusüzenetekről”, ha sok embert elérnek, előbb-utóbb valamelyik hírportál beszámol.
- Ha az app elhomályosítja egy üzenet képét és jelzi, hogy necces tartalom, akkor lehetőleg ne kattints rá.

## Hírfolyam

[felkavaró tartalommal találkozás]

### *Ami kimegy*

A digitális térben nemcsak arra kell figyelni, amit küldenek neked, hanem arra is, amit te osztasz meg magadról.

Miért gondoljuk át, hogy milyen információt adunk ki?

- Támadók felhasználhatják támadáshoz.
- Ha olyanok is hozzájutnak, akiknek nem szántuk, az kellemetlen lehet (főleg a képek, videók esetében).

A támadók, főleg ha nem ismernek téged személyesen, a rólad online elérhető információk alapján támadnak. Minél több személyes információ érhető el rólad, annál inkább személyre tudják szabni a támadást.

Ha például a Facebook oldaladon a zenei érdeklődésedről osztottál meg információt, vagy az Instagram profilodon koncertekről posztoltál, akkor egy becserkésző első üzenet már lehet ez lesz: *„Szia! Te szereted az XY együttest? Én imádom őket, van egy fölös jegyem a következő koncertre, volna kedved eljönni?”.*

Mit lehet tenni?

Lehet hallottad már a mondást, hogy az „internet nem felejt”. Ez arra utal, hogy, ha információt osztasz meg magadról a neten, akkor az *potenciálisan örökre* megtalálható lesz ott. A legjobb tehát

ha *szinte semmi személyeset* nem osztasz meg magadról. Nos, ez szerintem egy lehetetlen, életszerűtlen kérés, mert a digitális kommunikációból nehéz kimaradni. Emiatt én két részre osztanám az információkat a megoszthatóság szempontjából:

- Bizonyos információkat nem osszál meg.
- A többi információnál gondosan válaszd meg a megosztás módját és azt, hogy kikkel osztod meg.

| Eltűnő üzenet | Privát chat | Csoportos chat | Közösségi média profil - ismerősök | Közösségi média profil - nyilvános | Internetről elérhető (pl. Google keresés) |
|---|---|---|---|---|---|
|  | | | | | |
| Az információmegosztás kockázata egyre nő | | | | | |

### Adatok

Adatok, amiket ne ossz meg

- A saját jelszavadat ne oszd meg senkivel online, offline, telefonon.

Érzékeny személyes adatok, amiknek gondold át a megosztását

- E-mail cím
- Lakcím
- Valós idejű tartózkodási hely (pl. Snap)
- Születési idő
- Telefonszám
- Mindenféle kártyaszám: személyi igazolvány száma, diákigazolvány száma, TAJ szám
- Iskolád, sportklubod neve

Ezek olyan adatok, amik alapján a támadók közvetlenül be tudnak azonosítani, el tudnak érni (legrosszabb esetben a fizikai térben), vagy a hitelesség látszatát tudják kelteni (pl. adathalász üzenetben).

De. Mi van akkor, ha a lakásodra szervezel szülinapi bulit, ha valakinek a telefonszámodat meg szeretnéd adni, ha utazni mentek, és szükség van a személyi számodra, születési időre?

Ilyenkor valahogy meg kell osztani ezeket az adatokat is, de nem mindegy, hogy hogyan. Használj AA-as elemet. Jó ez így elég random volt, de a lényeg hogy **A**nnak küldjed az adatot, akinek kell, **A**ddig ameddig kell.

- Szülinapi buli esetén ha a Facebook eseménynél megadod a címedet, akkor az esemény ne legyen nyilvános, és a buli után töröld az eseményt.
- Telefonszám, személyi szám esetén ha már megvolt a beszélgetés, vagy vége a túrának, akkor törölheted a chatüzenetet, amiben az adatokat elküldted. (És elküldés előtt 2x ellenőrizd, hogy megfelelő embernek mennek az adatok).

[Eltűnő üzenetek bekapcsolása - útmutató]

Nyilvánosan megosztott adatok

Előfordulhat, hogy vannak olyan adatok, amiket *mindenkivel az interneten* meg szeretnél osztani, mert például indítottál egy YouTube csatornát, nyilvános insta oldalt, vagy egy személyes weblapot készítettél.

Szürke zónás adatok

A nagyon érzékeny adatok és a nyilvánosan megosztott adatok között van a nagy szürkeség, bizonytalanság. Nem túl szenzitív adatokról van szó, de azért nem is osztanánk meg bárkivel az interneten. Tipikusan a mindennapos kommunikációban megjelenő információkra gondolok: hova mentek moziba, hol találkoztok, mi volt a házi feladat, itt egy vicces TikTok videó.

Az ilyen adatok megosztását nem kell annyira átgondolnod, mint az érzékeny adatok küldését. Annyira viszont érdemes odafigyelned, hogy minél több emberrel osztasz meg információt (pl. privát üzenet < chatcsoport < poszt) annál inkább érdemes átgondolni, hogy valóban meg kell-e osztani az információt.

Itt egy összefoglaló táblázat a fentiekről

| | Eltűnő üzenet | Privát chat | Csoportos chat | Közösségi média profil - ismerősök | Közösségi média profil - nyilvános | Internetről elérhető (pl. Google keresés) |
|---|---|---|---|---|---|---|
| |  | | | | | |
| | Az információmegosztás kockázata jobbra haladva egyre nő | | | | | |
| Jelszavak | - | - | - | - | - | - |
| Érzékeny adatok | speciális esetben | speciális esetben | speciális esetben | speciális esetben (szülinapi buli, privát esemény – lakóhely) | - | - |
| Szürke zónás adatok | | | | | Speciális eset | - |
| Publikus információ | | | | | | |

## Képek, videók

A képek, videók megosztása jelenleg az okostelefonos biztonság vadnyugata. Statisztikák.[33] Napi több (tíz) fotót, szelfit készítünk, osztunk meg komolyabb biztonsági megfontolások nélkül. Van néhány ötletem, javaslatom, hogy mit és hogyan érdemes küldeni, de ezt egyelőre kevésnek érzem a naponta elkészített és megosztott fotók mennyiségéhez képest. C'est la vie, azért lássuk ezt a néhány javaslatot.

[33] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5987044/#B32 , https://www.psychologytoday.com/us/blog/love-digitally/201804/are-you-taking-too-many-selfies https://www.cnet.com/culture/young-women-spend-five-hours-a-week-taking-selfies-says-survey/

### Képek, amiket ne ossz meg senkivel

Meztelen, alsóneműs vagy általánosságban előnytelen képet, videót ne ossz meg senkivel (és, ha már itt tartunk, a telefonodon se tárolj).

Persze, vannak eltűnő üzenetek, meg bízhatunk a fogadó félben… de ha valahogy mégis kikerül egy ilyen kép, az komoly lelki problémákat okozhat. Az eltűnő üzenetekről készülhet kép (akár másik eszközzel, így hiába olyan a program, hogy nem engedi a képernyőkép készítését, vagy szól róla nekünk), amit már nem tudsz kontrollálni, illetve a bizalmas viszony is megszűnhet (például szakítás után).

### Ciki képek

Ezek olyan képek, amik Illetéktelen kézbe kerülése (pl. telefon ellopása/feltörése, saját/partner felhasználói fiókjának feltörése), szélesebb körben terjedése problémát okozna (pl. lelki sérülés, jóhírnév sérülése, cyberbullyingra adna okot).

Ezeket a képeket szerintem max. eltűnő üzenetben küld el, így nem marad ott a chattörténetben, illetve egy fokkal nehezebb a másiknak ezt elmenteni.

Azon képeket is, ahol a lakóhely egyértelműen beazonosítható inkább eltűnő üzenetben küld el (idegenek semmiképp se küldj ilyet).

Szürke zónás képek

Hasonlóak a szürke zónás adatokhoz, azaz a mindennapi életedhez kapcsolódnak. Azt tegyük hozzá, hogy „egy kép többet ér ezer szónál”, tehát sok információt ki lehet szedni egy képből.

A szürke zónás képek szélesebb körben történő  terjesztése kismértékű, de elfogadható problémát jelentene

Ezeknél a képeknél a minél „neccessebb, annál kevesebb embernek való elküldés” ökölszabályát alkalmazhatod.

Neccességi faktorok:

- lakóhely nehezen, de beazonosítható.
- tartózkodási hely (iskola, sportklub) beazonosítható.
- Nagy értékű otthoni tárgy (TV, PC, konzol, ékszer, családi autó stb.) látható rajta.
- Bántalmazásra adhat okot.
- A háttérben árulkodó tárgyak vannak (iskola jelvénye, zenekarok poszterei, hangszer).

Profilkép, nyilvánosságnak szánt képek

Ezek olyan képek, amik szinte nyilvánosak. Egy profilkép lehet nem jelenik meg a Google keresőben, de az adott oldalra regisztráltak általában elérhetik.

Az ilyen képek kirakásánál törekedj arra, hogy minél kevesebb információt lehessen belőle szerezni az érdeklődési területeidre, a tartózkodási helyedre vonatkozólag. A ruha, a háttér és helyszín legyen minél semlegesebb.

| | Eltűnő üzenet | Privát chat | Csoportos chat | Közösségi média profil - ismerősök | Közösségi média profil - nyilvános | Internetről elérhető (pl. Google keresés) |
|---|---|---|---|---|---|---|
| |  | | | | | |
| | Az információmegosztás kockázata jobbra haladva egyre nő | | | | | |
| Ruha nélküli, fürdőruhás, alsóneműs képek | - | - | - | - | - | - |
| Ciki kép | | - | - | - | - | - |
| Szürke zónás kép | | | | | - | - |
| Profilkép | | | | | | - |

Posztolás

- Feladat: segíts Lalinak eldönteni, hogy kiposztolja a képet

*Szörfölés*

- oldalak biztonsága
- fájlletöltés
- kíváncsiság, véletlen
- Nyilvános hálózatok vs mobilnet

Fizikai biztonság

- PIN kód (shoulder surfing)
- telefonra figyelés
- Okostelefon
    - üvegfólia, tok
    - képek
    - képernyőzár
    - vírusirtó
    - backup - képek

## Incidenskezelés (🚋🚋👮👮)[34]

Valami 💩 mindig van, mert a kockázatokat nem lehet (és nem is cél) nullára csökkenteni. Betörik a telefon kijelzője, egy zaklató rádír, elfelejted a jelszavadat, elmegy a mobilinternet, rákattintasz egy linkre, amire nem kéne stb. Ezek közül, eltérő valószínűséggel, de bármelyik bekövetkezhet. Ilyenkor *biztonsági esemény*, vagy más szóval *incidens* történik.

Fogalom:

- incidens (ISO, NIST)

[34] https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final alapján

- Biztonsági esemény (IBTV)
- „Online tűzoltás”[35]

Az incidensek kezelése nem bug, hanem feature. Ezzel a nagyobb vállalatok számolnak, sőt külön központok, ún. biztonsági műveleti központok[36] vannak az incidensek kezelésére. Magyarországon a Nemzeti Kibervédelmi Intézet egyik fő feladata az incidenskezelés.[37] Nyilván egy egész tejüzemet leterítő zsarolóvírus támadás kezelése más, mint egy betört kijelző, de a folyamat hasonló.

Az incidenskezelésnek négy része van:

1. Felkészülés,
2. Észlelés és elemzés
3. Beavatkozás, következmények felszámolása, visszaállás
4. Incidens utáni feladatok

[38]

*Felkészülés*

Az incidensekre való felkészülés a megelőzés és az incidens kezelési eszköztár kialakításából áll.

A megelőzésbe gyakorlatilag minden beletartozik, amiről eddig a pajzsok kapcsán szó volt.

Az incidenskezelési eszköztárban vannak

- technikai eszközök
  - vírusirtó
  - hasznos honlapok
    - adatszivárgás ellenőrzése https://haveibeenpwned.com/
    - gyanús linkek ellenőrzése https://www.virustotal.com/
    - információk: nki.gov.hu , híroldalak
  - nagyon profiknak tartalék telefon
- Ismeretek
  - milyen alkalmazások vannak a telefonodon
  - Hova vagyok regisztrálva
  - Mik a fiók helyreállítási lehetőségei
  - Kinek, milyen elérhetőségen kell szólni, ha baj van
  - Hogyan kell képernyőképet, videót készíteni (bizonyítékot gyűjteni).

[35] https://www.youtube.com/watch?v=QZ0cpBocl3c
[36] https://www.youtube.com/watch?v=9bfQnzyZ2Zo
[37] https://nki.gov.hu/szolgaltatasok/tartalom/incidenskezeles/
[38] https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final 21. o.

*Észlelés és elemzés*

## Észlelés

Az incidensek észlelése néha egyértelmű: ha betörött a telefon kijelzője, azt látjuk, ha érkezik egy zsarolólevél, vagy a böngésző nagy piros betűkkel figyelmeztet egy gyanús oldalra, az is könnyen észlelhető.

Vannak olyan esetek, amikor az incidens nehezebben észlelhető:

- E-mail címünk, jelszavunk érintett lesz egy adatszivárgásban.
- Nem ismerünk fel egy adathalász levelet és megadjuk az adatainkat.
- Értesítő e-mail elkallódik
- Olyan platformra töltenek fel rólad képet, amin nem vagy fent.

A nehezen észlelhető esetek felderítéséhez több energiára, tudatosságra van szükség.

Az adatszivárgásban való érintettséget például a következő módokon lehet ellenőrizni:

- Keress rá az e-mail címedre a https://haveibeenpwned.com/ oldalon, vagy kérj egy részletesebb összefoglalód a postafiókodba a https://www.f-secure.com/en/home/free-tools/identity-theft-checker oldalon.
    - Jelszót is lehet ellenőrizni, de óvatosan: https://haveibeenpwned.com/Passwords
    - Google-ben, jelszókezelőkben szokott lenne szolgáltatás, ami leellenőrzi az ott tárolt jelszavakat
        - https://passwords.google.com/ → A jelszóvizsgálat megnyitása
- Lehet értesítést kérni
    - Haveibeenpwned e-mailben https://haveibeenpwned.com/NotifyMe
    - Jelszókezelők, vírusirtóknak van figyelő szolgáltatások

**Figyelj a megérzésedre. Ha valami szokatlan, vagy gyanús arra figyelj oda.** A saját telefonodat, online életedet te ismered a legjobban, így a legkisebb változás is furcsa érzést okozhat. Kicsit hasonló ahhoz, mint amikor valaki más rak rendet a szobádban (khm.), és egyből észreveszed, hogy nem a helyükön vannak a dolgok. Néhány példa:

- Olyan értesítések jelennek meg, amikre eddig nem volt példa (lehet, hogy a telefon megfertőződött, vagy a Google biztonsági értesítést küld),
- Nagyon belassul a telefon (lehet, hogy a telefon megfertőződött),
- Olyan kontaktok jelennek meg az üzeneteid között, akiket nem ismersz (lehet hozzáfértek a fiókodhoz és a nevedben küldenek üzeneteket),
- Az elküldött üzenetek közt számodra ismeretlen üzenetek is vannak,
- Egymás után kapsz kétlépcsős azonosításra értesítést (valaki megszerezte a felhasználónevedet és jelszavadat, és most próbál belépni),
- Barátaid érdeklődnek, hogy minden rendben van-e veled (valaki lehet, hogy rosszhíredet kelti a tudtod nélkül).

Sok idő eltelhet, jóval később derül ki – pl. könyv letöltése, fájl másolása.

## Elemzés

Ha valami gyanúsat észleltél, akkor következik az elemzés. Ilyenkor azt kell megállapítani, hogy történt-e incidens, és ha történt, akkor az mennyire súlyos.

Nincs incidens, ha:

- Változott valami, de az nincs hatással a védendő elemekre (pl. frissült a telefon operációs rendszere és megváltozott a grafikus felület).
- Nem érint minket az incidens (pl. egy népszerű szolgáltatótól adatokat vittek el, de mi nem regisztráltunk rá).

Ha azonban történt egy esemény, és az veszélyeztet, vagy már károsított egy védendő elemet, akkor incidensről van szó. Itt kezdődik az igazi elemzés. Az elemzéshez gyűjts be minél több adatot és közben *dokumentálj, dokumentálj, dokumentálj*. A dokumentáció a gyakorlatban azt jelentheti, hogy képernyőfotókat, videókat készítesz, vagy nyitsz egy külön dokumentumot, ahova felírsz minden információt arról, amit tapasztaltál, illetve, amit csináltál. Az incidens kezelésében és incidenst követő elemzésnél ez jól fog jönni, vagy ha súlyos az ügy, akkor a külső féllel (internetszolgáltató, rendőrség) való kommunikációt is segítheti.

A kezdeti elemzés egyik célja, hogy eldöntsd, mennyire súlyos és sürgős az incidens:

- Mennyire akadályoz téged a teendőidben?
- Milyen információkat, eszközöket érint? Mennyire kiterjedt?
- Mennyi idő lesz helyreállni?

Példák a nagy prioritású incidensre:

- Súlyos cyberbullying: valaki durván zaklat az online térben, állandóan üzeneteket küld, zsarol valamivel, az súlyos. Ilyenkor lehet, hogy semmi másra nem tudsz gondolni, csak a zaklatásra és nem tudsz haladni a mindennapi dolgaiddal.
- Google fiókból kizárnak: nem tudsz e-mailt küldeni fogadni, fájlok, fotók veszhetnek el. Mentálisan is nagyon megterhelő.

Példák közepes prioritású incidensre:

- Mesterjelszó elfelejtése a jelszószéfhez: akadályozza a mindennapi dolgaidat, de nem lehetetleníti el (fontos fiókoknál az e-mail címre kérhetsz jelszó visszaállítást), illetve a telefonon még lehet be vagy néhány napig jelentkezve. Ugyanakkor minden fióknál visszaállítani a jelszót finoman szólva is fáj és sok időbe telhet.
- Erőszakos tartalmat láttál az Instagramon: ettől meg csinálod a dolgaidat, de nyomaszt, valakivel meg kell beszélni.

Példák kis prioritású incidensre:

- Kaptál egy adathalász SMS-t, de nem kattintottál rá
- Üvegfóliával védett telefonod leesett, törésnyomok vannak a kijelzőn. Nem tudod eldönteni, hogy csak a védőfólia sérült, vagy a telefon üvege is, de a telefon kijelzője használható.

A közepes és magas prioritású incidenseknél fontold meg mások, például szüleid értesítését. Ha súlyos incidensről van szó lehet, hogy az osztályfőnöknek, rendőrségnek vagy más harmadik személynek is érdemes szólni.

Lehet, hogy nemcsak téged érint az incidens. Ha például feltörik a közösségi média fiókodat, vagy az e-mail fiókodat, akkor a támadók küldhetnek a nevedben az ismerőseidnek is üzenetet. Ilyenkor próbáld meg őket más csatornán figyelmeztetni a veszélyre.

### *Beavatkozás*

Az elemzés eredményeképp van valamilyen elgondolásod, hogy mi történik. A következő lépés a beavatkozás, ami a feltartóztatás (containment), felszámolás és helyreállítás lépésekre bontható.

A feltartóztatás célja, hogy az incidens további hatásait csökkentse. A feltartóztatásra példa:

- Okostelefon leválasztása az internetről, ha megfertőződött.
- Okostelefont ellopták – adatok távoli törlésének megkísérlése.
- Google fiókba ismeretlen bejelentkezés – adott munkamenetből kijelentkeztetése.
- Ciki kép kikerül – ismerősök megkérése, hogy ne osszák tovább.

A feltartóztatás meglépése előtt érdemes mérlegelni, hogy a támadó viselkedésére, vagy a bizonyítékok gyűjtésére milyen hatással lehet. Zaklató üzenetek esetén a felhasználó blokkolása, vagy a közösségi média fiók törlése előtt még lehet érdemes időt szánni képernyőfotók készítésére.

Az incidens feltartóztatás után következik a felszámolás/kiirtás. Ha egy csőtörés esetén a feltartóztatás az, hogy hozunk vödröket, hogy abba folyjon a víz, akkor a felszámolás az, hogy megkeressük a főcsapot és elzárjuk azt. Felszámolásra példák:

- Megfertőződött okostelefonra vírusírtó letöltése, kártékony programok törlése, telefon visszaállítása gyári állapotba.
- Feltört fiók törlése.
- Zaklató által ismert közösségi média fiók törlése, más platform keresése.
- Hiányos adatvédelmi, biztonsági megoldások módosítása (pl. ha eddig bárki kapcsolatba léphet veled egy chatalkalmazásban, ott átállítani, hogy csak ismerősök írhassanak rád).

A feltartóztatást és felszámolást követi a helyreállítás. Itt a cél az, hogy a lehető leghamarabb újra tudjad rendesen használni az okostelefonod. Emiatt azokat a teendőket vedd előre, amik gyorsan elvégezhetők és legnagyobb mértékben segítik a normális állapotba való visszatérést. Utána érdemes a nehezebb, komolyabb utánajárást igénylő feladatokat elvégezni.

Gyors, hatékony megoldások:

- Ha kizártak az e-mail fiókodból, akkor másik e-mail fiók létrehozása. A legfontosabb fiókjaidban az e-mail címek átállítása erre a fiókra.
- Adatszivárgás gyanúja esetén a legfontosabb jelszavak megváltoztatása, legegyszerűbb kétlépcsős azonosítás módok beállítása.
- Zaklató profiljának blokkolása.

Lassabb, nehezebb, de tartós megoldások:

- Új technikai megoldások bevezetése: jelszószéf használata, kétlépcsős azonosítás átgondolt beállítása, több e-mail cím létrehozása.
- Fiók helyreállítási folyamat végigvitele.
- Tájékozódás, tanulás a fenyegetésekről (tudatosítás).
- Biztonsági mentésből visszaállás. Telefon gyári visszaállítása, újbóli beállítása.
- Cyberbullying esetén pszichológushoz fordulás. Ha osztályon belül történt a zaklatás iskolapszichológussal csoportos feldolgozás, osztályfőnök bevonása.
- Külső felek bevonása.

### *Incidens utáni teendők*

Újra rendesen működik az okostelefonod, visszakaptad a fiókodat, kicserélted az üvegfóliát, minden szuperül működik, huh… mehet tovább az élet, gg wp. Egy, gyakran kihagyott, lépés még van: a tanulás. Ne hagyj egy jó krízist kárba veszni! Ha szánsz kis időt annak a végiggondolására, hogy mi és hogyan történt, az segíthet a nagyobb biztonság elérésében és a későbbi incidensek kezelésében. Röviden válaszolj a következő kérdésekre:

- Mely biztonsági megoldások működtek jól?
- Mely incidenskezelési lépések voltak gyorsak, hatékonyak?
- Mi nem sikerült jól?
- A következő incidensnél mit csinálnál másképp?

Az egész folyamatra nézzünk egy példát, ami velem megesett:

Helyzet: egy szép napon megpróbáltam beírni a mesterjelszavamat a jelszószéfemhez, de nem sikerült. Valahogy mindig összekeveredtek a betűk.

Felkészülés

Tudtam, hogy ez probléma lehet, így olyan megoldást alkalmaztam, hogy szinte minden nap be kelljen pötyögnöm a jelszavamat. Azzal is csökkentettem a kockázatot, hogy a nagyon fontos fiókok jelszavait nem jegyeztettem meg a jelszókezelővel.

Észlelés és elemzés

A probléma észlelése egyértelmű volt, nem tudtam belépni a jelszószéfembe. Csak lassan esett le, hogy ez nem egy könnyen kezelhető probléma és ekkor már elkezdtem izgulni és meg is ijedtem.[39] A probléma elemzésével csak nőtt az aggodalom, mert amikor utána olvastam a lehetőségeimnek, bebizonyosodott, hogy ezt a jelszószéf ún. „zero-knowledge” megoldást használ, így csak a mesterjelszóval lehet kinyitni. A szolgáltató a fránya matek és kripto miatt ha akarna se tudna segíteni.

A probléma kiterjedtsége:

- A probléma több száz jelszót érintett. A jelszókezelő alkalmazást egy ismerősöm is használta, aki be tudott lépni, így közvetlenül nem volt érintett, de probléma esetén már nem tudtam volna neki segíteni. A probléma tehát kiterjedt volt.

Mennyire akadályozott a mindennapi teendőkben?

- Közepes mértékben. A telefonomon még ujjlenyomattal még el tudtam érni jelszószéfet, így ha nagyon kellett volna jelszó meg tudom nézni, illetve az e-mail címmel amivel regisztráltam az adott fiókot tudtam volna új jelszót kérni. Ugyanakkor mentálisan megterhelő volt, nem nagyon tudtam másra koncentrálni.

Mennyire lesz nehéz helyreállni?

- Nem lehetetlen, de nagyon macerás, mert egyenként vissza kell állítani a jelszavakat, vagy az ismerőssel létre kell hozni egy közös jelszómappát és oda bepakolni telefonon a jelszavakat.

A probléma tehát súlyos volt, de mennyire sürgető? A telefonon még volt hozzáférésem a jelszavakhoz, de egy idő után kéri ott is a jelszót, úgyhogy emiatt és a mentális megterhelés miatt a magas prioritásura raktam a problémát. Azaz piros gomb, minden félre, tűzoltás 🧯.

Az ismerősömet értesítettem az  incidensről és arról, hogy lehet szükségem lesz a segítségére.

Dokumentálás céljából elővettem egy jegyzetfüzetet, ide írtam az információkat és a szükséges lépéseket.

[39] Kb. hasonló érzés, mint ami ebben a sztoriban van: https://www.wired.com/story/i-forgot-my-pin-an-epic-tale-of-losing-dollar30000-in-bitcoin/

Beavatkozás

Néhány órával az észlelést követően azt a döntést hoztam, hogy megpróbálom az ismerősöm fiókján keresztül „kimenteni” a jelszavaimat. Ehhez a telefonomon át kell pakolnom a jelszavaimat egy közös jelszómappába, aztán kiexportálni a jelszavakat. Ez idő lesz, de ha ezeket egy offline jelszókezelőbe beimportálom (pl KeePass), akkor legalább meglesznek a jelszavak, ha a telefonon időben nem is lehet használni őket.

Rövid távú intézkedések:

- legfontosabb jelszavak közös mappába
- KeePass széf létrehozása, oda jelszavak átmentése
- (a jelszavak kiexportálása ilyenkor nyílt szövegbe történik, amit a felhasználás után biztonságosan kell törölni[40])

Néhány óra után szerencsém volt, mert eszembe jutott a jelszó. Huh. De ezzel nincs vége az incidensnek.

Mit lehet tenni, hogy újra ne forduljon elő?

- Létrehoztam egy új jelszót, ami könnyebben megjegyezhető. Leírással dilemmába voltam, végül kompromisszumos megoldásként egy papírra leírtam a jelszó egy részét.

Hosszú távú intézkedés

- Jelszavak számának csökkentése
- Lista vezetése a legfontosabb jelszavakról.

Poszt-incidens elemzés

Jelszószéf kritikusabb használata. Hosszú, de egyszerűbb jelszavak használata a jövőben. Jobban át kell látni, hogy milyen fiókokhoz tárolok jelszót a jelszószéfben.

Ami jól ment az incidenskezelésben, hogy a problémát gyorsan észrevettem és elemeztem. Hamar döntés hoztam a beavatkozás elkezdéséről. Amin lehet javítani az a mentális megterheléssel való jobb megküzdés.

Feladat: Kattints a linkre és kezelj egy incidenst.

- F1.7 – Lépésről, lépésre incidenskezelés: https://forms.gle/fsbRKbpWE9WkgJ9n6

Egyéb példa incidensekre és kezelésükre

- Példák:
  - flubot
  - telefon elvesztése
- Osztálytárs hozzáfér szünetben a telefonhoz, nincs rajta képernyőzár, Snapen/BeReal/Viber/Messenger üzenetet küld
- Adatvédelmi beállítások FB/pinterest -> cyberstalking/ grooming
- Inappropriate content
- Messenger – közös csoportba bevesznek, kellemetlen fotó
- Snapchat – sexting (egyik osztálytársad)

[40] pl. https://www.lifewire.com/free-file-shredder-software-programs-2619149 biztonságos, ingyenes program keres

- Fizikai
    - Telefon leesik, betörik a kijelző
    - https://www.youtube.com/watch?v=r3VCKixt_l8

### Első rész, követelmények

### Gyakorlati feladatok

- Google Account setup
- App adatvédelmi beállítása
- Jelszókezelőben jelszó létrehozása (passkey plusz pontért)
- Incidens elméleti/gyakorlati kezelése

## Mentális egészség

## Tartalomfogyasztás, produktivitás

## Függelék

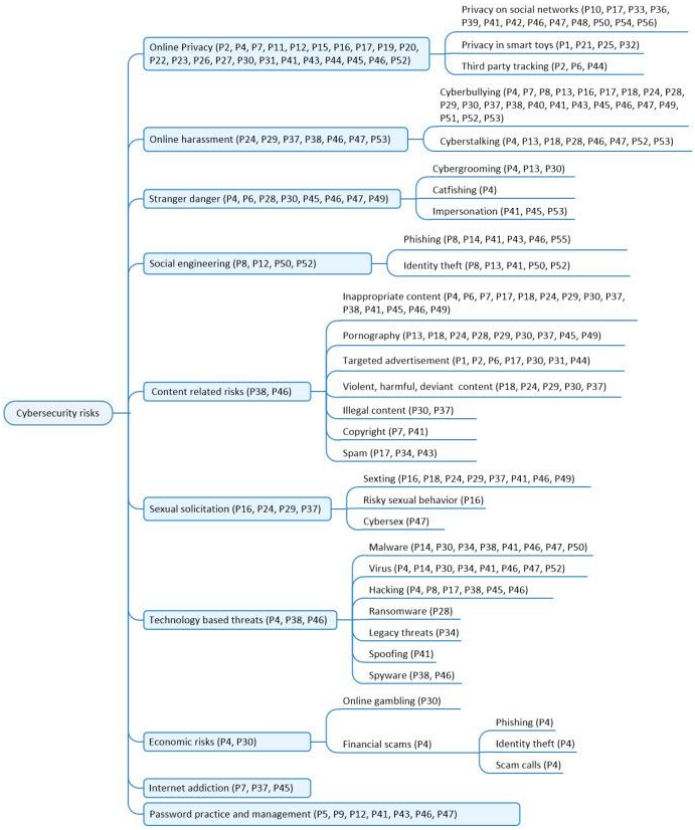
### Feladatok

-

### Fogalomjegyzék

-

### Források




https://www.sciencedirect.com/science/article/pii/S2212868921000581 Cybersecurity awareness for children: A systematic literature review

## Eszköztár

- haveibeenpwned
- virustotal, https://urlscan.io/ , browserling
- weboldalak
  - TheVerge
  - Wired
  - nki.gov.hu
  - protectyoungeyes
- https://www.ncsc.gov.uk/cyberaware/home