Vágner Máté:

AZ IOT BIZTONSÁGVÉDELMI KIHÍVÁSAI ÉS A KIBERTUDATOS FELHASZNÁLÓVÁ NEVELÉS CÍMŰ KUTATÁS MELLÉKLETEI

I. Melléklet – Források a kutatás egyes pontjaihoz

[1] - http://itsecurity-privacy.blog.hu/2017/09/07/az_iot_helyes_hasznalata_veszelyei
[2] - https://hu.wikipedia.org/wiki/Szolg%C3%A1ltat%C3%A1smegtagad%C3%A1ssal_j%C3%A1r%C3%B3_t%C3%A1mad%C3%A1s
[3] - https://www.hwsw.hu/hirek/56250/biztonsag-botnet-iot-dvr-mirai-malware.html
[4] - http://www.bain.com/publications/articles/finding-europes-edge-in-the-internet-of-things.aspx
[5] - Illéssy Miklós – Nemeslaki András – Som Zoltán: Elektronikus információbiztonság-tudatosság a magyar közigazgatásban http://real.mtak.hu/41849/1/i_tarsadalom_2014_1_illessy_nemeslaki_som.pdf
[6] - http://nepszava.hu/cikk/1155705-adatbotrany-a-facebooknal
https://www.portfolio.hu/vallalatok/szamonkerik-a-facebookot-50-millio-ember-adataival-jatszottak-a-valasztasi-kampanyban.4.279848.html
https://24.hu/mobil/2018/03/19/hatalmas-csapast-kapott-a-facebook-az-adatbotrany-utan/
[7] - https://www.i40platform.hu/
[8] - Som Zoltán: Interoperabilitási kérdések és informatikai biztonsági tükrében a közigazgatásban http://real.mtak.hu/41851/7/interoperabilitasi_kerdesek.pdf
[9] - http://resources.infosecinstitute.com/iot-sec-awareness-will-security-awareness-protect-me-from-my-toaster/
[10] - https://www.businesswire.com/news/home/20160111005217/en/
[11] - https://index.hu/tech/2018/03/19/ez_a_telefon_olyan_biztonsagos_hogy_a_keszitoje_bortonben_fog_megrohadni/

II. Melléklet – Források a kutatás egészéhez

Angol cikkek, kiadványok:

- https://www2.deloitte.com/insights/us/en/focus/industry-4-0/cybersecurity-managing-risk-in-age-of-connected-production.html
- http://www.computerweekly.com/news/2240236390/The-human-factor-a-key-challenge-to-information-security-say-experts
- http://www.computerweekly.com/opinion/The-human-factor-is-key-to-good-security
- https://www.cio.com/article/3104116/internet-of-things/iot-security-suffers-from-a-lack-of-awareness.html
- http://www.eejournal.com/article/20160629-humanfactor/
- Cisco - Cybersecurity: Everyone's Responsibility https://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/C45-626825-00_Cyber_Security_Responsibility_AAG.pdf
- UL – Smart Home Security White Paper https://www.ul.com/consumer-technology/wp-content/uploads/2017/07/CS10027_SmartHomeCyberSecurityWhitePaper_Web_17.pdf
- Lawrence Miller – IoT Security for Dummies https://www.insidesecure.com/Markets/Internet-of-Things/IoT-Security-for-Dummies
- Susan W. Brenner & Leo L. Clarke - Civilians in Cyberwarfare: Casualties https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1650748

Magyar cikkek, kiadványok:

- https://magyaridok.hu/belfold/tanulnunk-kell-kiberbiztonsagot-2294839/
- Árvay Anett - A manipuláció és a meggyőzés pragmatikája a magyar reklámszövegekben www.arts.u-szeged.hu/download.php?docID=47853
- Cikk a biztonságos Wi-Fi hálózathoz: Egri Imre – Tökéletes Wi-Fi: https://pcworld.hu/szoftver/tokeletes-wi-fi-biztonsagos-es-gyors-halozat-percek-alatt-162211.html

DDoS támadási térkép: http://map.norsecorp.com/

Ikonok:

- A kávébab ikont készítette Freepik a www.flaticon.com oldalról. Licensz: CC 3.0 BY
- Az Internet ikont készítette Smashicons a www.flaticon.com oldalról. Licensz: CC 3.0 BY

III. Melléklet – Táblázatok

1. táblázat - Kérdések, miket érdemes feltenni egy okoseszköz vásárlása előtt:

Mennyire kell okosnak lennie az eszköznek?
Megéri-e a haszna és a benne rejlő veszélyek alapján?
Kell-e egyáltalán az eszköz „felokosított” változata, vagy egy rendes is elég? Mennyire tartható fent az eszköz? Meg van-e a megfelelő infrastruktúra?
Tényleg szükség van-e az összes funkciójára az eszköznek? Például: Tényleg kell nekem egy okos tojástartó, ami tojást rendel nekem, de cserébe kiszivárogtathatja a bankszámlám adatait bárkinek, aki egy kicsit jobban ért az eszközök feltöréséhez?

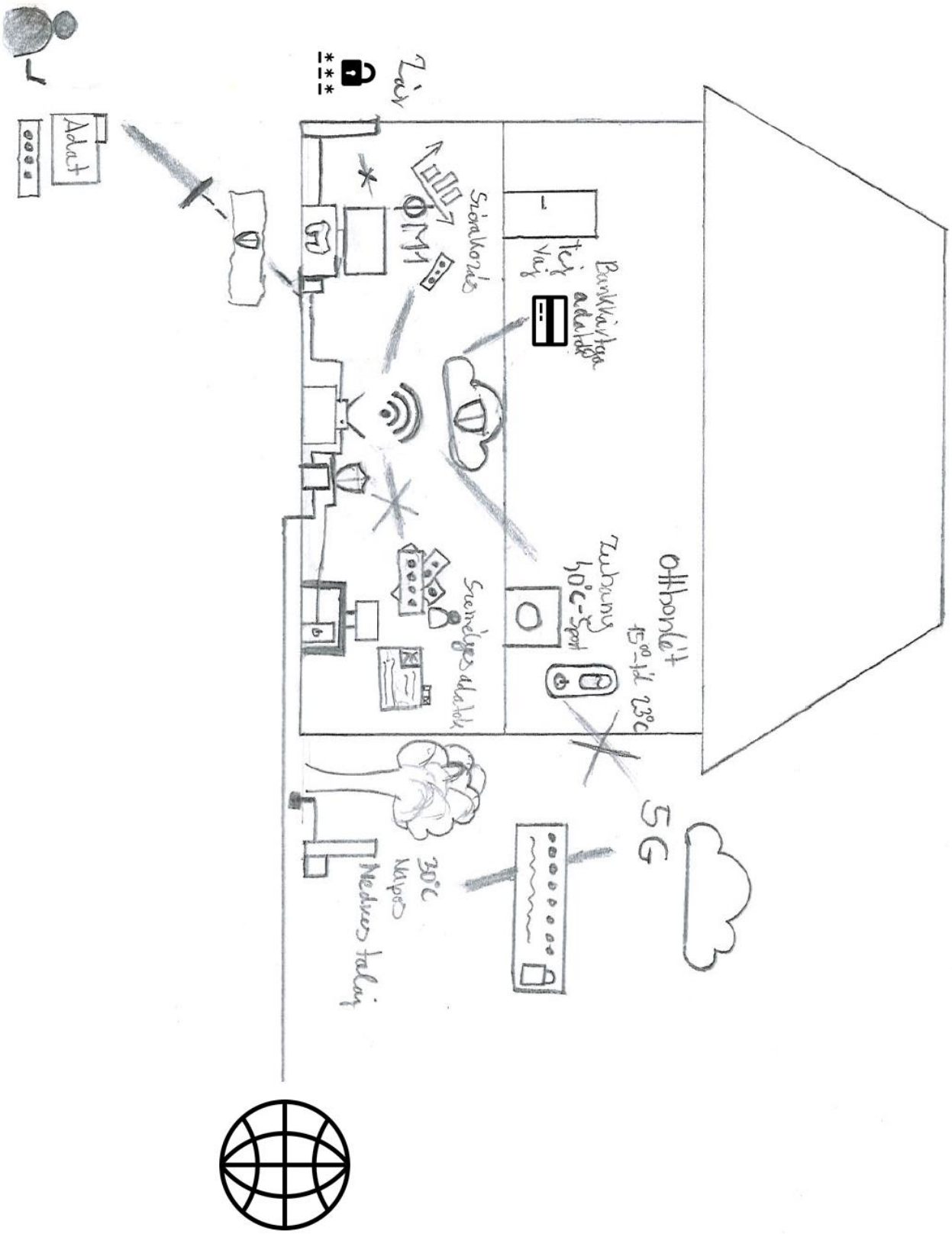
2. táblázat - Tippek felhasználók számára az erős jelszóhoz: [8]

Legyen legalább 8 karakter hosszúságú!
Lehetőleg tartalmazzon minél több szekvenciát, akár mind a négyet!
Ne tartalmazzon személyes vagy hozzánk köthető adatot!
Ne legyen jelmondat, vagy triviálisan visszaalakítható szó!
Ne használjunk online jelszógenerátort!
Változtassuk meg rendszeresen!
Ne írjuk le sehova jelszavunkat!
Ne adjuk meg senkinek!
Egy jelszót csak egy helyre használjunk!
A jelszó személyes használatra való! Ne használjunk közös jelszavakat!
Használjunk jelszószéfet a jelszavak felírása helyett!
Ne jegyeztessük meg a programokkal!
Ne írjuk be idegen, közösen használt számítógépen, vagy ha igen, akkor utána változtassuk meg!

3. táblázat - Tippek felhasználók számára a sikeres mindennapi IoT kibervédelemhez: [9]

Használjunk erős jelszavakat (IoT-s) eszközeink felhasználói fiókjaihoz és a Wi-Fi hálózatokhoz.
Az alapvető, sokszor használt jelszavakat ne használjunk és ezeket változtassuk meg.
Sose nyissunk meg ismeretlen eredetű e-mailekben található linkeket és csatolmányokat. Mindig ellenőrizzük, hogy a levél tartalma valós-e. Előfordulhat, hogy egy ismert cég logójával küldenek nekünk egy figyelmeztető e-mailt egy nem a céghez tartozó e-mail címről. Ezeket egyből töröljük! A legjobb az, ha megemlítjük a levelünk szövegében a csatolmányt vagy az e-mailt, ha mi küldjük.
Egy erősebb titkosítási rendszert válasszunk Wi-Fi hálózatainknak. Ilyen például a WPA2.
Védjük erősen IoT eszközeink távoli hozzáférését, és tiltsuk le, ha nem szükséges.
Ahol lehetséges, ott kábeles kapcsolatot használjunk.
A routereinknél ajánlatos hálózatforgalomfigyelő és blokkoló rendszereket használni. Így sose lesznek közvetlenül az internetre kötve az eszközeink és könnyen leválaszthatjuk a hálózatról baj esetén. Ilyen eszközök például: Bitdefender BOX, F-Secure SENSE.
Használt IoT eszköz vásárlásánál figyelmesek legyünk! Módosíthatták a szoftverük!
Járjunk utána az eladó által megadott eszközbiztonsági méréseknek.
Módosítsuk az eszköz bizalmi és biztonságvédelmi beállításait igényeinkhez mérten.
Tiltsuk le a nem használt funkciókat, mivel ezeket a támadók szeretik kihasználni.
Telepítsük a frissítéseket, lehetőleg amint elérhetőek lesznek.
Használjuk eszközeinket az otthoni privát hálózaton, ha lehetséges, csak szükség esetén csatlakozzunk rájuk hálózaton kívül.
Mindig offline telepítsünk, végezzünk vírusellenőrzéseket.
Biztosítsuk, hogy egy üzemszünet, például a jel zavarásának vagy leállásának köszönhetően ne okozzon egy védtelen állapotot telepítés vagy működés közben.
Gondolkozzunk el, hogy az „okos” funkciók tényleges szükségesek, vagy egy normál eszköz is elég lenne-e (lásd a Nem mind arany, ami… fejezetben)
Tudatosítsuk magunkban a robotökoszisztéma hatását az ember környezetére! Az ember-gép viszony folytonosan változik az IoT eszközök térnyerésével, ezért szükséges az érzékenység a körülöttünk lévő szenzorok adattovábbításával, esetleges adatszivárgásával kapcsolatban. (lásd a Miért nem zártad el az internetet? Avagy a gazdasági kibervédelem bekezdésben)
Ne csak egy védekezési formát használjon! Az eszközhöz képest mérlegelje a szükséges protokollokat. Lehet olyan eset, ahol nem elég csak egy tűzfal és vírusírtó kombó, de olyan is van, hogy felesleges egy vírusírtó. (Egy kisebb szenzoregység esetében ez teljesen lelassítja az ezközt, míg fertőzés esetén csak az újratelepítés segít, így a tűzfal is elég.).
A biztonságvédelem fő viszonyítási pontja mindig az adott adat értéke legyen.
Jó, ha tisztában vagyunk legalább néhány „Intézkedési” tervvel. Tudjuk, hogy szélesebb körű támadás esetén mi az épp aktuális ránk vonatkozó felkérés a felelős szervek részéről!
Legyünk tisztában, hogy a tudatlanság nem mentesít! Ha a mi eszközeinken keresztül támadtak mások, vagy ha mi is érintettek leszünk illegális tevékenységekben tudtunkon kívül, csupán figyelmetlenségből, attól még mi is számon kérhetők, büntethetők vagyunk.

IV. Melléklet – Ábrák a felhasználóknak készült tájékoztató kiadványokhoz és szórólaptervezetek a figyelemfelhívás nagyobb sikeréhez



1. ábra - Okosház kapcsolatait, és azok megvédését szemléltető ábra kézi vázlata. Egy hasonló digitalizált ábra felhasználható az informáló kiadványban és a honlapon is.

A JELSZÓ: ELÉG JÓ?

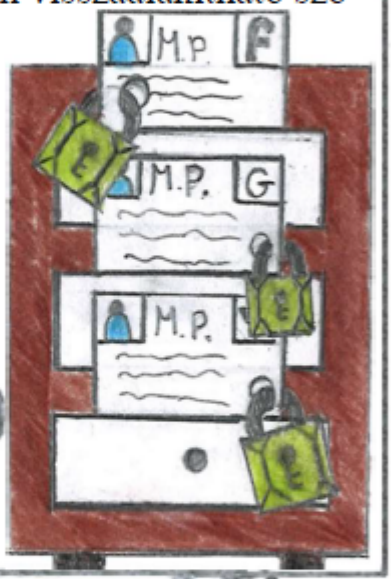
TIPPEK AZ ELÉGSÉGES JELSZÓHOZ

A jó jelszó

Hosszú:	***legalább 8*** karakteres
Tartalmaz:	***kis-, nagybetűt és szám***ot
Személyes adatot:	***nem*** tartalmaz
Változatos:	***rendszeresen megváltoztatják***
Okos:	***nem triviális***an visszaalakítható szó

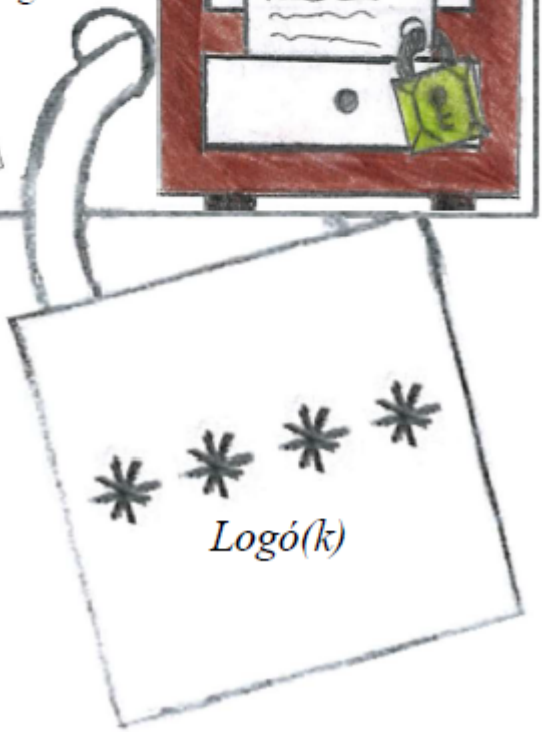
Tanácsok:

- Ne használjunk online jelszógenerátort!
- Ne írjuk le sehova jelszavunkat!
- Jelszavunk ne adjuk meg senkinek!
- Egy jelszót csak egy helyre használjunk!
- Ne használjunk közös jelszavakat!
- Jelszavunk sose jegyeztessük meg programokkal!



Elfelejti jelszavait?

Használjon jelszószéfet!



Tudjon meg ön is többet:

www.megnincsilyenoldal.hu

Szervezetnév

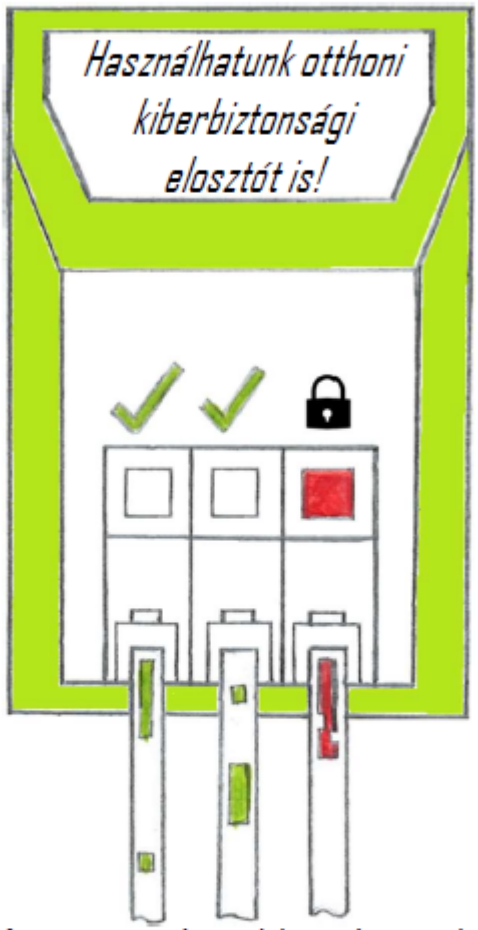
2. ábra - Szórólapterv a megfelelő jelszóhasználatért.

OKOSESZKÖZÖK VÉDELME

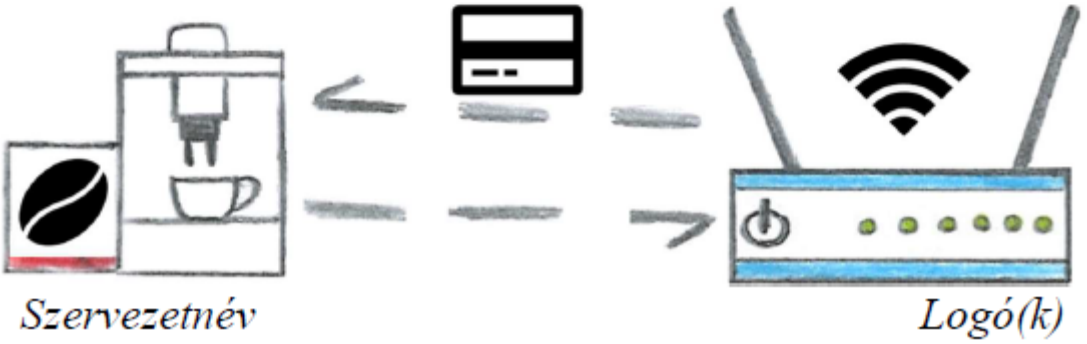
Ön használ okoseszközöket az otthonában? Eszközei megfelelően védettek?
Okos Oszkár biztos ebben. Legyen olyan, mint Oszkár!

Okos Oszkár tanácsai:

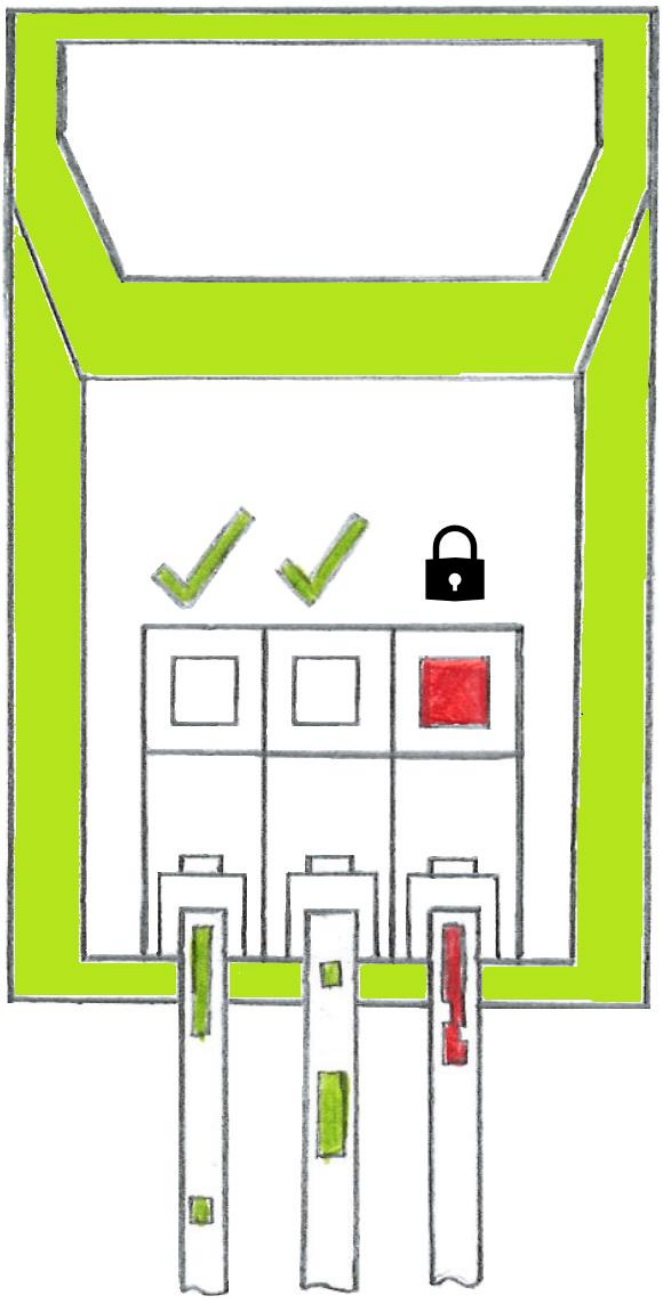
Az okoseszközök fontos adatokat is közölnek egymással *(pl. bankkártyaadataink)*, ezért:



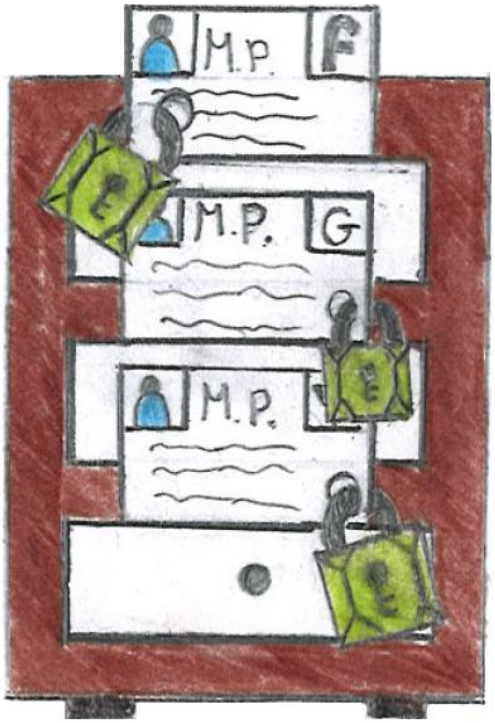
- ***Erős jelszavak***at használjunk!
- ***Erős titkosítást*** válasszunk otthoni Wi-Fi hálózatunknak! pl. WPA2
- Új és használt eszközöket is ***csak ellenőrzött forrásból vásároljunk***! Így adatainkat azok nem szivárogtatják ki, ami meggyengíti az eszközeink védelmét!
- OS-t csak offline ***telepítsünk***!
- Eszközeinket ***ne csatlakoztassuk közvetlenül*** az internetre!
- Mindig ***módosítsuk*** az új eszköz biztonságvédelmi ***beállításait***!
- ***Tiltsuk le eszközünkön a távoli hozzáférést***, ha nem szükséges!
- ***Tiltsuk le a nem használt funkciókat***, így nehezebben leszünk támadhatók!



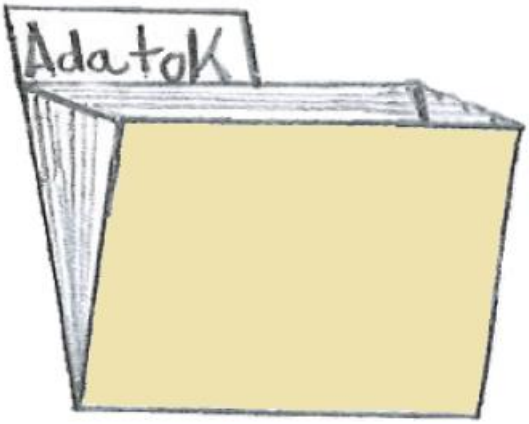
3. ábra - Szórólapterv a megfelelő eszközvédelemért



4. ábra – Cybersecurity HUB

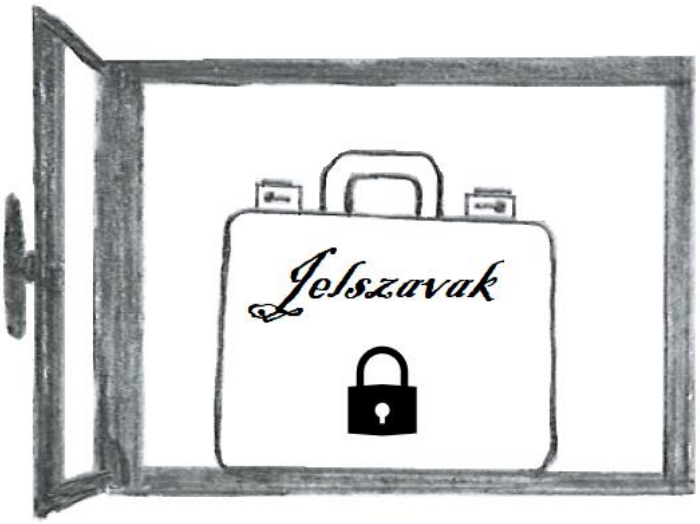


5. ábra - Fiókvédelem

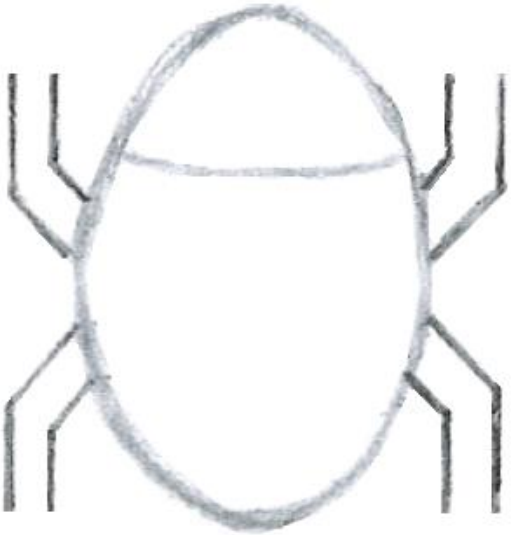


6. ábra - Adatok

7. ábra – Okoseszköz kommunikáció



9. ábra - Jelszószéf

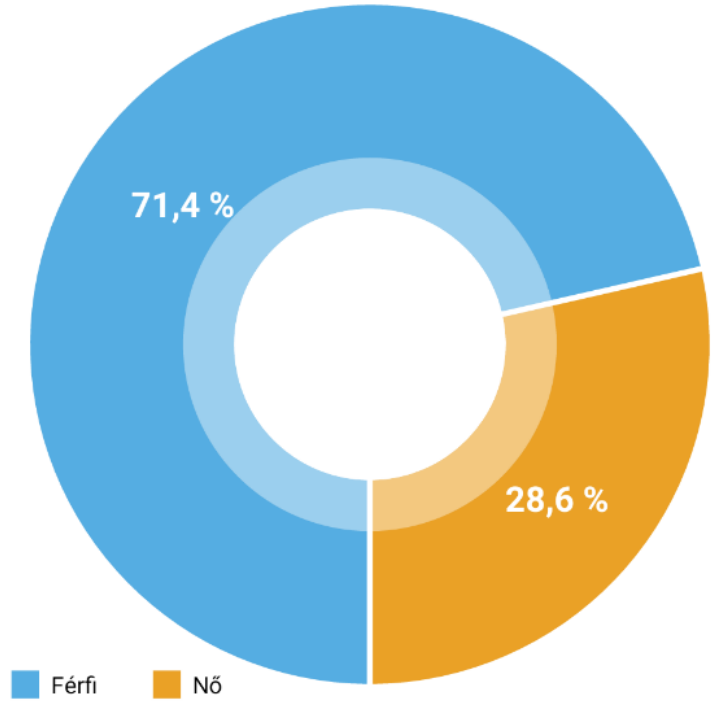


8. ábra - Vírus

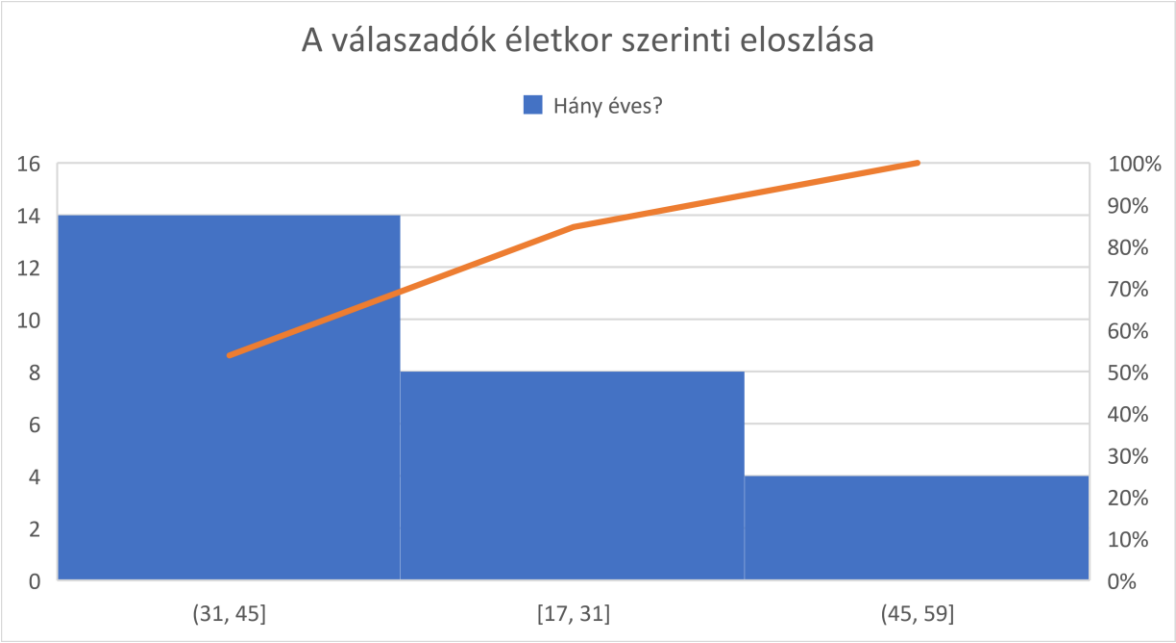
4. – 10. ábra: Ábrák és ábratervezetek az ismertető kiadványhoz

10. ábra – csillag

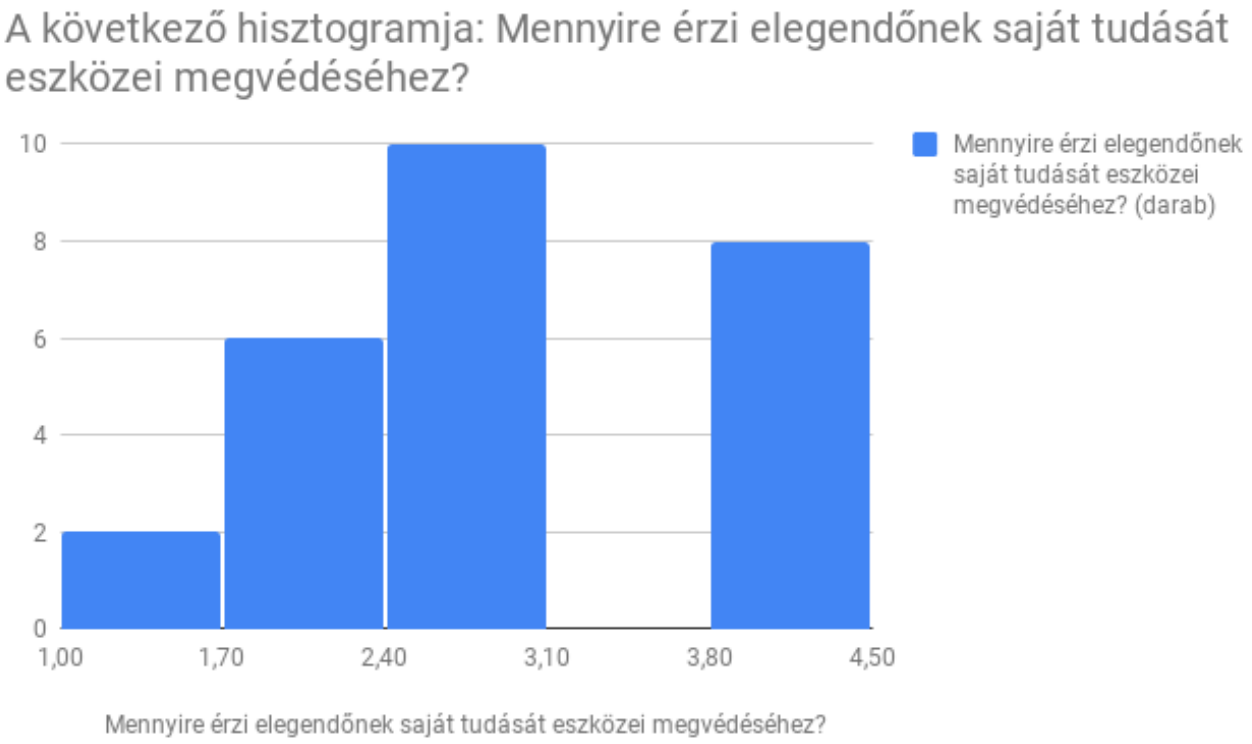
V. Melléklet – Néhány kutatási eredmény



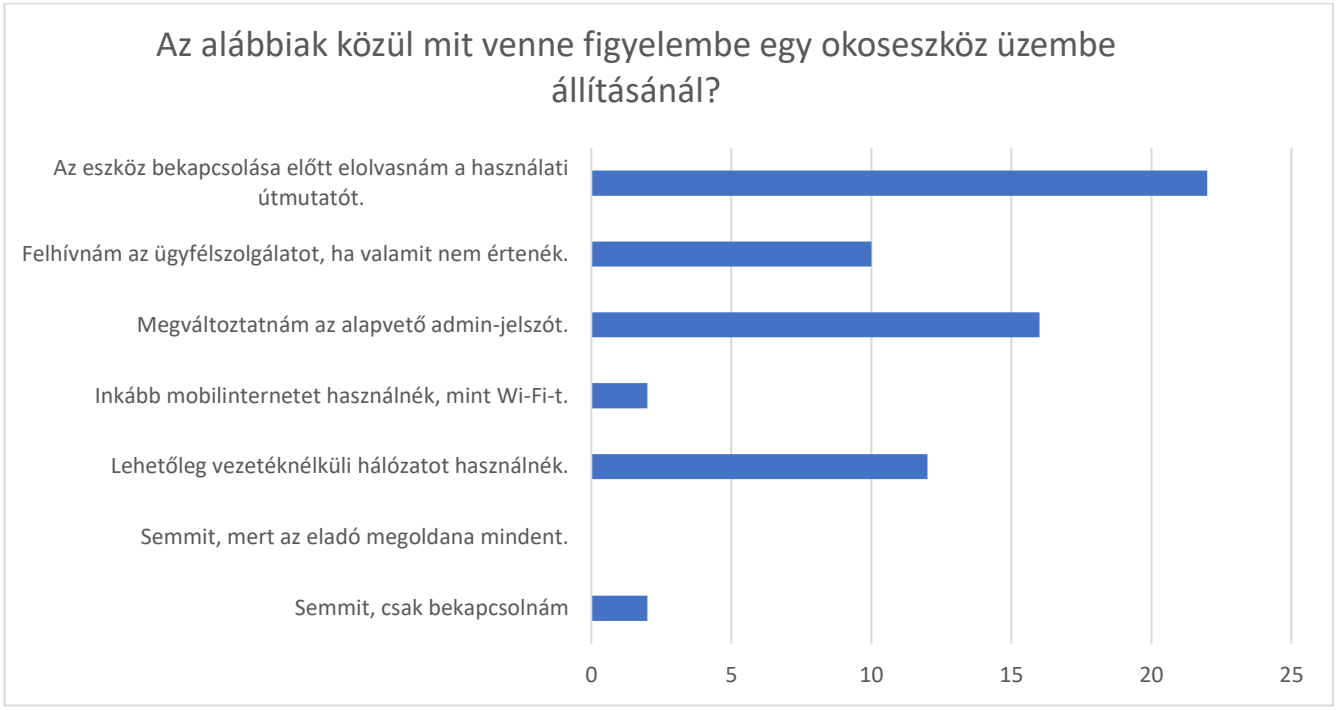
11. ábra - Nemek eloszlása a válaszolók között



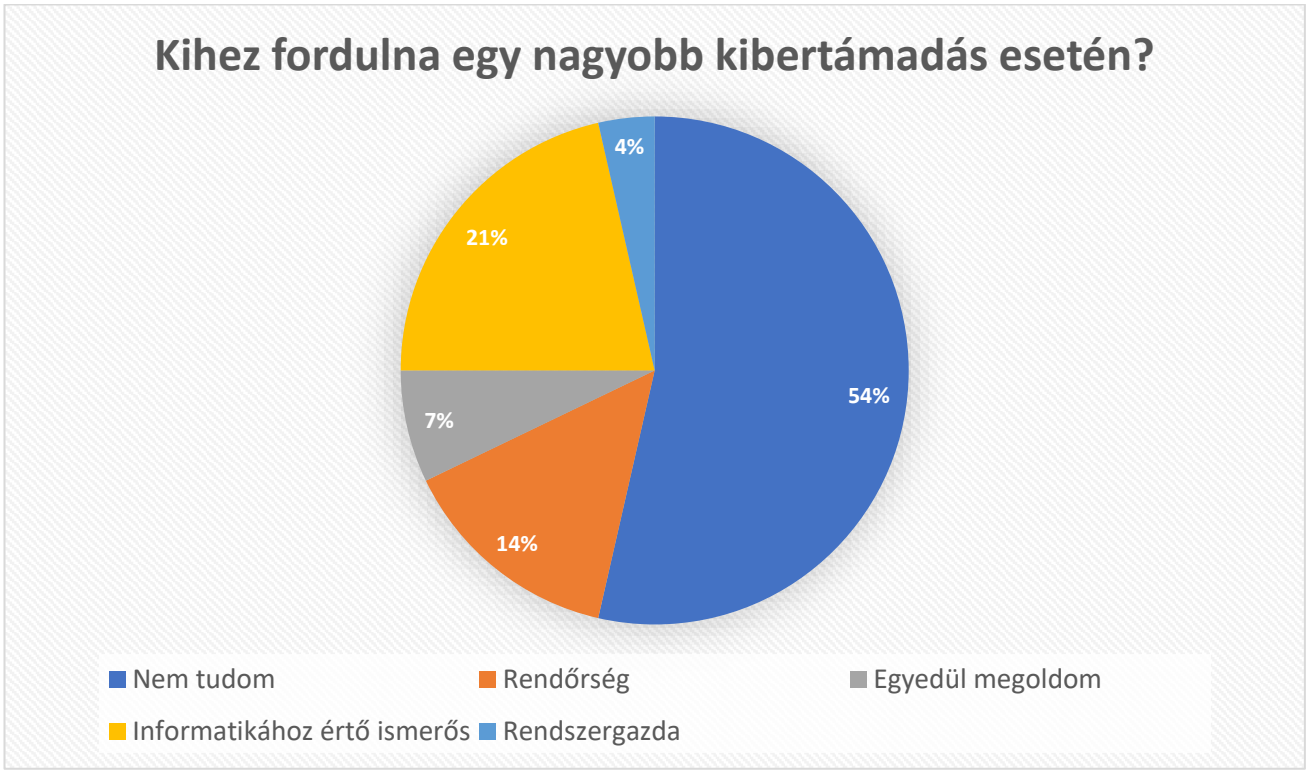
12. ábra - A válaszolók életkor szerinti Pareto-diagramja



13. ábra - Az emberek nem annyira biztosak a tudásukba, ha az okoseszközökről van szó.



14. ábra - Az emberek nem figyelnek a kommunikációs platformok sebezhetőségére.



15. ábra - Az emberek többsége nem tudja, hogy kihez forduljon, vagy azt hogy kihez kéne fordulnia.