

37. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Budapest, 2025. április 22–24.
Nemzeti Közszolgálati Egyetem
Hadtudományi és Honvédtisztképző Kar

Ki vagyok én – avagy a személyiséglopás aspektusai a kibertérben

Jelige: *Kettős személyiség*

Pályamunka lezárásának időpontja: 2023. szeptember

2025.



TARTALOM ÉS ÁBRAJEGYZÉK

1.	BEVEZETÉS	4
2.	A KUTATÁS CÉLJA, MÓDSZERTANI HÁTTERE	5
3.	MI A SZEMÉLYISÉGLOPÁS?.....	6
4.	SZEMÉLYES ADATOK KÉRDÉSKÖRE	8
5.	BÜNTETŐJOGI SZABÁLYOZÁS.....	9
6.	A SZEMÉLYAZONOSSÁG-LOPÁS FAJTÁI	12
7.	HOGYAN SZEREZHETŐK MEG A SZEMÉLYES ADATOK?	14
8.	AKTUALITÁS	20
9.	IDENTITÁSLOPÁS MEGELŐZÉS	26
10.	PROFILOZÁS, MINT ADATGYŰJTÉS.....	30
11.	FIGYELMEZTETŐ JELEK	33
12.	HA MÁR MEGTÖRTÉNT A BAJ.....	34
13.	AZ EMBEREK ÉS A BIZTONSÁGTUDATOSSÁG	34
14.	BANKOK BIZTONSÁGA	45
15.	BEFEJEZÉS	50
16.	VONATKOZÓ JOGSZABÁLYOK	51
17.	FELHASZNÁLT IRODALOM.....	52
18.	FÜGGELÉK	HIBA! A KÖNYVJELZŐ NEM LÉTEZIK.
18.1.	ANNOTÁCIÓ.....	HIBA! A KÖNYVJELZŐ NEM LÉTEZIK.

1. ábra FBI 2022-es jelentése	4
2. ábra Példa magyartalan adathalász e-mailre (Forrás: https://biztonsagportal.hu/hogyan-ne-keruljunk-az-adathalaszok-halojaba.html)	16
3. ábra Példa adathalász e-mailre (Forrás: https://pcforum.hu/hirek/24323/vigyazat-emailben-probaljak-kicsalni-az-otp-ugyfeleinek-banki-azonositoit)	17
4. ábra Tiszta asztal (Forrás: https://www.stackfield.com/blog/clean-desk-policy-162)	18
5. ábra Nem tiszta asztal (forrás: https://en.idei.club/40838-clean-desk-policy.html)	18
6. ábra Mediamarkt család	26
7. ábra Biztonságos weboldal	27
8. ábra Sütik további beállításai	31
9. ábra Korosztály felmérése (Forrás: saját szerkesztés)	35
10. ábra Milyen közösségi oldalakat preferálnak az emberek? (Forrás: saját szerkesztés)	35
11. ábra Milyen tartalmakat osztanak meg szívesen a válaszadók? (Forrás: saját szerkesztés)	36
12. ábra A kitöltők milyen jelszót választanak? (Forrás: saját szerkesztés)	37
13. ábra Jelszavak megosztása (Forrás: saját szerkesztés)	38
14. ábra Jelszó feljegyzése (Forrás: saját szerkesztés)	39
15. ábra Személyes adatok megosztása (Forrás: saját szerkesztés)	40
16. ábra Adatvédelmi, adatkezelési ismeretek (Forrás: saját szerkesztés)	41
17. ábra Személyes adatokkal visszaélés tapasztalatok (Forrás: saját szerkesztés)	42
18. ábra Jelzés a hatóságok felé (Forrás: saját szerkesztés)	42
19. ábra A nem jelzés indoka (Forrás: saját szerkesztés)	43
20. ábra Weboldal (Forrás: saját szerkesztés)	44
21. ábra Weboldal (Forrás: saját szerkesztés)	44

1. BEVEZETÉS

Századunk kiemelkedő problémájának ígérkezik a kibertérben elkövetett bűncselekmények széleskörű elterjedése. Ma már az internet világában kevésbé jártas felhasználók is könnyűszerrel válhatnak elkövetővé, ha megfelelő helyen informálódnak. Az egyszerű felhasználók naivitását, vagy éppen figyelmetlenségét kihasználva több milliós összegekhez is hozzájuthatnak. Napjainkban már nem feltétlen eleme az áldozattá válásnak a felhasználó gondatlan magatartása, azonban sok esetben egy egyszerű Google kereséssel meg lehetne előzni a problémát. Személyes tapasztalataim alapján az egyik kiemelkedő problémát a személyazonosság-lopás jelenti. A bankkártya adatokkal történő visszaélések, valamint a más személyében elkészített profillal végrehajtott csalások, illetve az online tértől elrugaszkodva a mobilhálózaton keresztül történő megtévesztések komoly problémát jelentenek. A személyazonosság-lopás (angolul: identity theft) áldozati száma az internethasználók növekedésével párhuzamosan gyarapodik. Olyan mennyiségben, hogy e cselekmények következtében a Szövetségi Nyomozó Iroda (Angolul Federal Bureau of Investigation, rövidítve FBI, az Amerikai Egyesült Államok szövetségi szintű nyomozószervének a 2022-es jelentésében az áldozatok száma alapján szerepel az első tizben.¹

2022 CRIME TYPES

By Victim Count			
Crime Type	Victims	Crime Type	Victims
Phishing	300,497	Government Impersonation	11,554
Personal Data Breach	58,859	Advanced Fee	11,264
Non-Payment/Non-Delivery	51,679	Other	9,966
Extortion	39,416	Overpayment	6,183
Tech Support	32,538	Lottery/Sweepstakes/Inheritance	5,650
Investment	30,529	Data Breach	2,795
Identity Theft	27,922	Crimes Against Children	2,587
Credit Card/Check Fraud	22,985	Ransomware	2,385
BEC	21,832	Threats of Violence	2,224
Spoofing	20,649	IPR/Copyright/Counterfeit	2,183
Confidence/Romance	19,021	SIM Swap	2,026
Employment	14,946	Malware	762
Harassment/Stalking	11,779	Botnet	568
Real Estate	11,727		
Descriptors*			
Cryptocurrency	31,310	Cryptocurrency Wallet	20,781

1. ábra FBI 2022-es jelentése

¹ Federal Bureau of Investigation – Internet Crime Report 2022 (Internet Crime Complaint Center, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf) letöltve: 2023.08.06.

Témaválasztásom indoka abban rejlik, hogy sokszor tapasztalom, hogy a környezetemben élők internetes bűncselekmények áldozatává válnak. Úgy gondolom, a személyiséglopásból eredő cselekmények sokszor veszélyesebbek, azonban számos esetben megelőzhetők. Szeretnék kidolgozni egy bűnmegelőzési projektet, amely során azt vizsgálom, hogy az embereknek mire kell figyelmet fordítaniuk az esetleges áldozattá válás elkerülése érdekében. Dolgozatomban ismertetem a személyazonosság-lopás főbb aspektusait, továbbá lehetséges megoldásokat dolgozok ki az áldozattá válás csökkentése, illetve megelőzése érdekében.

A témaválasztást szintén befolyásoló tényező, hogy mindig is érdekelték a számítógépes, valamint a kibertérben zajló bűncselekmények. E bűncselekmények nyomozása gyakran kihívás elé állítja a nyomozó hatóságokat is. Magyarországon a rendőrség szervei mellett más szerv is foglalkozik a kibertérben elkövetett bűncselekmények eredményes felderítésének elősegítésével. Véleményem szerint a bűncselekmények számának a csökkentéséhez elengedhetetlen a felhasználók tudatosítása, illetve az aktív védelem igénye, valamint a kételkedés a felhasználók részéről.

2. A KUTATÁS CÉLJA, MÓDSZERTANI HÁTTERE

A témát illetően több hipotézist állítottam fel. A hipotézisek igazolására, illetve cáfolására elsősorban kérdőívet készítettem, amit az ismeretségi körömben terjesztettem. A dolgozatomban vizsgáltam, hogy azok a felhasználók, *akik kétfaktoros autentikációt használnak, kevésbé vannak kitéve a személyiséglopás áldozatának.* A kétoldali kommunikáció például a bank és az ügyfél között létfontosságú eleme a biztonságos ügyintézésnek. A többfaktoros hitelesítés lehetővé teszi, hogy egy másodlagos ellenőrzésen menjenek át a kezdeményezések, mielőtt ténylegesen bekövetkezik a hozzájárulás, vagy adatmegosztás. Természetesen, már ezt is ki lehet cselezni, ahogy azt majd az Aktualitás című fejezetben kifejték, viszont lehet ez az a faktor, ami megelőz egy áldozattá válást. A következő felvetésem, hogy *az adatvédelmi, adatkezelési ismeretek iránti magasabb tudatossággal rendelkező emberek jobban képesek megvédeni a személyes adataikat és elkerülni a személyiséglopást.* Nézőpontom szerint, aki adatkezeléssel foglalkozik a munkája során, vagy adatvédelemmel kapcsolatos képzésben vesz részt, jobban ügyel az adatai biztonságára. Erre a következtetésre saját példámon keresztül jutottam. Mivel egyetemi képzésem során volt lehetőségem adatvédelmi ismeretekkel foglalkozni, és az erre vonatkozó jogszabályokat megismerni. A gyakorlati példák megismerése következtében jobban ügyelek arra, hogy mit osztok meg az interneten, illetve kiknek engedélyezek hozzáférést a személyes adataimhoz. Továbbá, felmerül

bennem a kérdés, hogy biztonságos-e nekem ez a cselekvés vagy nem? Milyen következményei lehetnek ennek? E kérdések felmerülését pedig, ezeknek az ismereteknek a megszerzéséhez kötöm.

Időszerű problémának tartom a közösségi médiában való túlzott megosztást, hogy az emberek gyakran az utóhatásokra nem gondolva posztolnak személyes adatokat az interneten. Ebből adódik a következő hipotézisem, így szól: *a közösségi média platformokon és az online fórumokon való magánéleti információk megosztása növeli a személyiséglopás kockázatát.* Ismerősi körökben is tapasztalom, hogy mit sem sejtve megosztják a gyermekek iskolai bizonyítványait, amelyen minden személyes információ rajta van, valamint Facebook-os csoportokban a talált iratokat teszik közzé, elmulasztva a jelenség kockázatának a felmérését.

A személyes adatok közül a legnépszerűbb, amit az elkövetők haszonszerzési célból megszereznek a bankkártya adatok. Ennek eredményeképp, a kvalitatív kutatási módszert alkalmazva, interjút készítettem a bankok témakörben jártas szakemberrel. Interjúalanyom, Weissmüller Gábor a Citibank nyomozati vezetője, illetve Magyar Bankszövetség Csalás Elleni Munkacsoportjának vezetője. Egy iskolai konferencia keretében már volt szerencsém hallani a szakmailag kimagasló előadását, ezért a témaválasztást követően nem volt kérdés, hogy őt fogom felkérni. Érdekelt, hogy a bankoknak milyen biztonsági intézkedései vannak az ügyfelek adatainak a biztonságos kezelésére vonatkozóan.

A kutatásom célja, hogy preventatív tájékoztatást nyújtsak a felhasználóknak.

3. MI A SZEMÉLYISÉGLOPÁS?

Külföldi szakirodalmi meghatározás alapján a személyiséglopásnak nincs egységes definíciója. Több államban különböző kifejezéseket használnak a jelenségre, mint az *identity theft*, *identitätsdiebstahl* vagy az *identity fraud*. Azonban a hangsúly mindegyikben a személyes adatok csalási szándékkal történő felhasználására helyeződik. Lawson és Lawford kanadai szerzőpáros megfogalmazása alapján az identitáslopás nem más, mint „*egy másik személy személyes információinak a jogosulatlan gyűjtése és csalárd módon történő felhasználása*”.² Német meghatározás szerint a személyiséglopás lényege a jogellenes megszerzésen alapul. Ami alapján, csak akkor identitáslopás, ha az adatösszesség alapján az érintett személy

² Philippa Lawson & John Lawford - IDENTITY THEFT: THE NEED FOR BETTER CONSUMER PROTECTION (Public Interest Advocacy Centre 1204 – ONE Nicholas St. Ottawa, Ontario K1N 7B7, November 2003, With Funding from Industry Canada <https://www.piac.ca/wp-content/uploads/2014/11/idtheft.pdf>) letöltve: 2023.08.16.

beazonosítható. Például, ha csak a bankkártyaszámot szerzik meg az nem minősül annak, viszont ha hozzá a nevet és a lejáratát is, az már igen.³

Magyar meghatározások is eltérő kifejezéseket használnak, Hámori Balázs a Bizalom, jóhírnév és identitás az elektronikus piacokon című publikációjában így fogalmaz: „Az *identitáslopás* egy személy adatainak (név, születési év, lakcím, hitelkártya-azonosító, tájszám és más személyes adatok, illegális eltulajdonítása azzal a céllal, hogy azokat különféle tranzakciókban anyagi előnyszerzésre használják az autóbérléstől a bankhitel felvételéig.”⁴ Ezzel ellentétben külföldi minta alapján használt terminológia, a személyiséglopás, amit Haig Zsolt a személyes információs hadviselés kérdéskörébe sorol. Abból kifolyólag, hogy a bűncselekmény következményeként az áldozatok nemcsak anyagi, hanem az emberi méltóság terén is károsodást szenvedhetnek.⁵ A személyazonosság-lopás szókapcsolat Sobán Kinga megfogalmazása szerint olyan kétlépcsős folyamat, amelynek az első lépése a személyes adatok eltulajdonítására irányul, a másodikban pedig az elkövető a személyes információk birtokában a sértettnek álcázva magát visszaélést követ el.⁶ A visszaélés megnyilvánulhat bűncselekmény formájában, illetve egyéb szolgáltatások igénybevételével. Személy szerint úgy gondolom, hogy mindegyik kifejezés helytálló, a személyazonosság-lopás szóhasználat jobban tükrözi a hivatalosabb, illetve büntetőjogi oldalát a cselekménynek, míg a személyiséglopás vagy az identitáslopás inkább tükrözi az emberi oldalát. Ahogy Haig Zsolt is fogalmaz, az emberi méltóság sérülését is magába foglalja. Hiszen a személyiség szó, az egyénre vonatkozó viselkedési, gondolkodási és érzelmi jellemzők együttesét jelenti. Ami számomra tágabb tartalommal bír, mint a személyazonosság. E szó alatt az egyén azonosítására szolgáló információk érthetők, amik leginkább a külső jegyekben mutatkoznak meg, mint például egy anyajegy, vagy a biometrikus adatok, vagy a személyazonosító igazolvány. Dolgozatom során nem teszek különbséget a kifejezések között, hanem egymás szinonimájaként használom őket.

³ Georg Borges, Jörg Schwenk, Carl-Friedrich Stuckenberg, Christoph Wegener - Identitätsdiebstahl und Identitätsmissbrauch im Internet - Rechtliche und technische Aspekte (2011, Springer 11. o.) letöltve: 2023.08.16.

⁴ Hámori Balázs - Bizalom, jóhírnév és identitás az elektronikus piacokon (Közgazdasági Szemle, LI.évf., 2004. szeptember (832-848.o.) letöltve: 2023.08.10.

⁵ Haig Zsolt – Az információs hadviselés kialakulása, katonai értelmezése (HADTUDOMÁNY 21.(1-2.) pp. 12-28. (2011)) letöltve: 2023.08.10.

⁶ Sorbán, Kinga - Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói (Themis: 2015/1. 343–375. o.) letöltve: 2023.08.10.

4. SZEMÉLYES ADATOK KÉRDÉSKÖRE

Magyarország Alaptörvénye alapján mindenkinek joga van a személyes adatai védelméhez. Arról, hogy mi minősül személyes adatnak, a 4/2007 vélemény a személyes adat fogalmáról, így fogalmaz: „*A személyes adat minden olyan információ, amely valamely **azonosított vagy azonosítható élő személlyel** kapcsolatos. Mindazon információk, amelyek összegyűjtése egy bizonyos személy azonosításához vezethet, ugyancsak személyes adatnak minősülnek.*”⁷ Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény „*az érintettre vonatkozó bármely információ*” meghatározást használja. Ami a korábbi megállapításhoz hasonlóan azokat az adatokat tartalmazza, amik alapján egy adott személy egyértelműen beazonosítható. Például név, lakcím, IP-cím, vezetéknev.utónév@vállalkozás.com típusú elektronikus levelezési címek, személyazonosító igazolvány száma, süti (cookie)-azonosító, a telefon hirdetési azonosítója, helymeghatározó adatok, egyedi azonosítását elősegítő, kórház vagy orvos által tárolt adatok.⁸ A törvény az azonosítható természetes személyt az alábbi módon határozza meg: „*az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat, online azonosító vagy a természetes személy fizikai, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;*”. A személyiséglopás alapját képezi más személyes adatainak elsősorban a jogosulatlan megszerzése, majd pedig a felhasználása. Az információk megszerzésének rengeteg módja lehet, amiket a későbbiekben szeretnék kifejteni.

A személyes adok védelmét Európában az Általános Adatvédelmi Rendelet (GDPR: General Data Protection Regulation) biztosítja. A globalizáció következményeként a személyes adatok egyre több forrásból megismerhetők. A Big Data és az adatok értékének köszönhetően az adatvagyonnal történő gazdálkodás központi szerepet játszik manapság. A GDPR célja, az adatvédelmi incidensek, személyiséglopás és személyazonossággal történő visszaélések megakadályozása. Ezt a személyes adatok kezelésének a korlátozásával teszi lehetővé. Az adatkezeléshez jogalap szükséges, így az adatkezelő az alábbi feltételek valamelyikének megléte esetén kezeli jogszerűen az érintett adatait:

⁷ 4/2007 vélemény a személyes adat fogalmáról (https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_hu.pdf) letöltve: 2023.08.16.

⁸ Európai Bizottság válasza – Mit nevezünk személyes adatnak? (https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_hu) letöltve: 2023.08.15.

- az érintett egyértelmű, megerősített cselekedettel hozzájárulását adta személyes adatainak kezeléséhez; (Ez történhet önkéntes írásbeli, elektronikus vagy szóbeli nyilatkozattal.)
- az adatkezelés szerződéses kötelezettség teljesítéséhez szükséges
- az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges (uniós vagy nemzeti jogszabályok alapján);
- az adatkezelés közérdekű feladat végrehajtásához szükséges (uniós vagy nemzeti jogszabályok alapján);
- az adatkezelés egy személy létfontosságú érdekeinek védelme miatt szükséges;
- az adatkezelés az adatkezelő jogos érdekeinek érvényesítéséhez szükséges (de ekkor ellenőrizni kell, hogy az adatkezelés során az érintettek alapvető jogai nem sérülnek-e súlyosan)⁹

5. BÜNTETŐJOGI SZABÁLYOZÁS

Az Egyesült Államokban az identitáslopás rendkívül gyakori bűnözési forma. Ebből kifolyólag az USA volt az első ország a világon, amely meghatározta és szigorú jogi keretek között kezelte a személyazonosság lopását, mint különálló deliktumot. Ezt a jogi változást 1998-ban hajtották végre az Identity Theft and Assumption Deterrence Act nevű törvény módosításával. A törvényt módosítás elsődleges célja a tényállás büntetőjogi következményeinek a biztosítása, beleértve az anyagi károkozástól a személyiségi jogi sérelmek okozásának büntetését.¹⁰ A kodifikált törvénykönyv 18. fejezetének 1028. § (7) befejezete alapján *„aki, tudatosan, törvényes felhatalmazás nélkül átadja, birtokolja vagy használja egy másik személy azonosítására szolgáló eszközt azzal a szándékkal, hogy olyan jogellenes tevékenységet kövessen el, vagy abban segédkezzon, vagy azzal összefüggésben, amely a szövetségi törvények megsértésének minősül, vagy amely bármely alkalmazandó állami vagy helyi törvény szerint bűncselekménynek minősül.”*¹¹ Ugyanezen törvény szerint az azonosítás alatt bármely név vagy szám önállóan vagy más információval együtt alkalmas az egyén beazonosítására. Például név, társadalombiztosítási szám, születési idő, hivatalos állam, vagy kormány által kibocsátott vezetői engedély, adóazonosító szám, egyedi biometrikus adat (ujjlenyomat, hangnyomat,

⁹ Európai Bizottság – Mikor kezelhetők személyes adatok? (https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-can-personal-data-be-processed_hu) letöltve: 2023.08.12.

¹⁰ SAMAHA, Joel - Criminal law. Ninth edition. Thomson Wadsworth Publisher, USA, Belmont. 2008. 393.o.

¹¹ 18 U.S. Code § 1028 - Fraud and related activity in connection with identification documents, authentication features, and information (<https://www.law.cornell.edu/uscode/text/18/1028>) letöltve: 2023.08.12.

retina- vagy írisz kép, vagy más fizikai ismertetőjegy), egyedi elektronikus azonosítószám, lakcím, irányítószám, telekommunikációs azonosító információja vagy azonosító eszköze. Annak ellenére, hogy a deliktum neve az identitáslopás (identity theft) a törvény e deliktum alatt nem bünteti a megszerzést, csakis a birtoklást, használatot, illetve az átadást. Az ilyen jellegű információk gyűjtése számítógépes csalásnak minősül. A büntetési tételt tekintve a személyiséglopás akár harmincévi szabadságvesztéssel járhat abban az esetben, ha terrorizmussal összefüggő bűncselekmény keretében történik. Ez elrettentésként jelenik meg, mivel gyakran választott módszer a terrorizmus finanszírozására. A büntetés kiszabásánál figyelembe veszik az áldozatok számát, az elkövetés módját, továbbá, hogy milyen kárt szenvedett a sértett (mind anyagi, mind az emberi méltóságot sértő).¹²

A magyar Büntető Törvénykönyv nem nevesíti a személyiséglopást külön deliktumként, hanem több bűncselekmény megvalósulhat e kifejezés alatt. Úgy gondolom, ez annak is köszönhető, hogy jelenleg a meglévő tényállások többnyire lefedik a személyazonosság-lopás egyes mozzanatait. A fentiekben említett elméletből kiindulva, hogy az identitáslopás egy kétlépcsős folyamat, az első a személyes adatok megszerzésére irányul. Ez a cselekmény megvalósulhat a tiltott adatszerzés formájában: *„Aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából elektronikus hírközlőhálózat –ideértve az információs rendszert is –útján másnak továbbított vagy azon tárolt adatot kifürkész, és az észlelteket technikai eszközzel rögzíti”*¹³ A kifürkészés szó ebben az esetben magában rejti az elektronikus úton történő megismerést, az információs rendszerek segítségével kivitelezhető. E tevékenység bármilyen technológiával történhet (pl. adathalászat, keylogger). Az adatok megszerzésének nem feltétlenül kell a kibertérben történnie a személyiséglopás esetében, egy egyszerű fizikai térben elkövetett lopással is megvalósítható a cselekmény, azonban én dolgozatomban a számítógépes környezet veszélyeire szeretnék fókuszálni.

Az adatok megszerzését követően a visszaélésszerű felhasználáson van a hangsúly. Ez a cselekmény a személyes adattal visszaélés deliktumával követhető el. Ami így szól: *„Aki a személyes adatok védelméről vagy kezeléséről szóló törvényi vagy az Európai Unió kötelező jogi aktusában meghatározott rendelkezések megszegésével haszonszerzési célból vagy jelentős érdeksérelem okozva a) jogosulatlanul vagy a céltól eltérően személyes adatot kezel...”* A

¹² 18 U.S. Code § 1028 - Fraud and related activity in connection with identification documents, authentication features, and information (<https://www.law.cornell.edu/uscode/text/18/1028>) letöltve: 2023.08.12.

¹³ 2012. évi C. törvény a Büntető Törvénykönyvről 422.§. (1) e)

bűncselekmény megvalósulásának elengedhetetlen eleme a célzat, tehát a haszonszerzési céllal történő felhasználás vagy az érdeksérelem okozása a sértettnek. A jelentős érdeksérelem egy társadalmi típusú sértő eredmény, akkor megállapítható, ha az ügy összes körülményét figyelembe véve a sértett szakmai elismerése vagy erkölcsi megbecsülése csorbát szenved.¹⁴ (Például: vagyoni hátrány, munkahely elvesztése, családi kapcsolatokat befolyásoló hátrány) Az adatkezelés fogalmát a korábban említett 2011.évi CXII. törvény határozza meg a következőképpen: *„adatkezelés: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése”*

A következő bűncselekmény, ami a visszaélést tükrözi az információs rendszer vagy adat megsértése, ami a következőképpen szól: *„Aki információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával jogosulatlanul belép, vagy a belépési jogosultsága keretei túllépve vagy azt megsértve bent marad”*¹⁵ Ez a tényállás magába foglalhatja egy közösségi média profilba történő belépést, amihez előzetesen az elkövető megszerezte a jelszót és azt jogosulatlanul felhasználta. A jelszó megszerzése többféle módon is megtörténhet, amiket a későbbiekben részletesen kifejték.

Véleményem szerint a leggyakoribb bűncselekmény típus, aminek az internet világa teret enged az a csalás. Ma már szinte mindenkinek van legalább egy olyan ismerőse, aki csalás áldozata volt már. A csalás a Btk. szerint a következőképpen hangzik: *„Aki jogtalan haszonszerzés végett más tévedésbe ejt, vagy tévedésben tart, és ezzel kárt okoz, csalást követ el.”*¹⁶ A tényállás elengedhetetlen eleme az eredmény, tehát a kár bekövetkezése, valamint a célzat, a jogtalan haszonszerzés. A törvény külön meghatározza a bűncselekmény értékhatárait. A tévedésbe ejtés, téves tévképzetet jelent, valótlan dolog való tényként történő feltüntetése (pl. hazugság) vagy valós tény elferdítése, elhomályosítása, melynek hatására a sértett tévedésbe kerül. A tévedésben tartás, pedig a sértett meglévő tévedésének el nem oszlatása, vagy

¹⁴ Dr. Bátki Pál – Jelentős érdeksérelem jelentése a büntetőjogban (2020. <https://batki.info/jelentos-erdekseirelem-jelentese-a-buntetojogban/>) letöltve: 2023.08.17.

¹⁵ 2012. évi C. törvény a Büntető Törvénykönyvről 423.§. (1)

¹⁶ 2012. évi C. törvény a Büntető Törvénykönyvről 373.§. (1)

megegyezése. A csalás nehézsége a hatóságok szemszögéből, hogy az áldozat önként adja át a vagyonát, vagy enged hozzáférést a személyes adataihoz, mivel ő nem tudja, hogy ez nem az ő érdekeit szolgálja.

A „sima” csalás speciális esete az információs rendszer felhasználásával elkövetett csalás: *„Aki jogtalan haszonszerzés végett információs rendszerbe adatot bevisz, az abban kezelt adatot megváltoztatja, törli, vagy hozzáférhetetlenné teszi, illetve egyéb művelet végzésével az információs rendszer működését befolyásolja, és ezzel kárt okoz.”* A törvény meghatározza az információs rendszer definícióját is. Erre a bűncselekményre hozok példát a későbbiekben.

6. A SZEMÉLYAZONOSSÁG-LOPÁS FAJTÁI

A személyiséglopást a jogirodalomban az alapján különböztethetjük meg, hogy a bűncselekmény mi ellen irányul, így lehet személyes vagy üzleti. Az előbbi esetében a cselekmény az egyén személyes adatainak megszerzésére irányul csalárd szándékkal. A cél olyan jogellenes tevékenység végzése, mint áruk vételezése, bűnözői aktivitások elősegítése, illetve különböző szolgáltatások jogosulatlan igénybevétele. Az elkövetési tárgy leggyakrabban a sértett neve, telefonszáma, lakcíme személyazonosító igazolvány száma, bankkártya adatai és ahhoz tartozó PIN-kód, elektronikus levelezési címe, édesanyja neve, továbbá a biometrikus adatai. Ezzel szemben az üzleti személyiséglopás cégek és pénzintézetek ellen irányulnak. Az elkövető elsődleges célja az anyagi haszonszerzés, illetve a vagyoni hátrány okozása. Ebben az esetben a cég neve, telefonszáma, elektronikus levelezési címe, védjegye, bankszámlaszáma, illetve azonosítószáma lehet a megszerzendő adatkör.¹⁷

Vannak olyan esetek, amikor két vagy több személy hozzájárul ahhoz, hogy egymás személyazonosságát használják. Ezt identitásdelegálásnak nevezik.¹⁸ Például, amikor a házaspárok engedélyt adnak egymásnak a bankkártyájuk használatára.

Másik kategorizálás alapján a személyiséglopás fajtái az alábbiak:

- vagyoni,
- bűnügyi,
- egészségügyi,
- szintetikus,

¹⁷ HOFFMAN-MCGINLEY: Identity theft: A Reference Handbook i. m. 3-5.o

¹⁸ KOOPS, Bert Jaap – LEENES, Ronald et. al.: A typology of identity-related crime. Conceptual, technical and legal issues. In: Information, Communication & Society. 2009/1. 8. o.

- gyermekidentitás-lopás¹⁹

Az első és egyben a legjellemzőbb kategória esetében a bűnöző célja a vagyoni haszonszerzés és a személyes adatok körén belül elsősorban a bankkártya, illetve bankszámla adatok megszerzése. Gyakori elkövetési mód, hogy az elkövető eladja a megszerzett adatokat.

A bűnügyi identitáslopás következtében a delikvens a lopott személyazonosító igazolvánnyal személyiséglopás áldozatának adja ki magát, amikor a rendőrség igazoltatja, vagy elfogja bűncselekmény miatt. Így a bűnöző a valódi személyazonosságát elrejtí és helyette, az ártatlan személy (identitáslopás sértette) ellen indíthatnak büntetőeljárást. Ebben az esetben az áldozat csak az idézés során szembesül a nevét érintő cselekményekről. A magyar joggyakorlatban a 2/2004 BJE határozat rendelkezése alapján, ha az elkövető más személynek adja ki magát, és ebből kifolyólag nem releváns adat kerül az eljáró hatóságok által kiállított közokiratba, a Btk. 268.§ hamis vád büntette mellett a Btk.342.§ (1) bekezdés c) pontja szerinti „intellektuális” közokirat-hamisítás büntetét is elköveti.²⁰ Az intellektuális közokirat-hamisítás során az elkövető a közokirat kiállítására jogosult szerv megtévesztésével közreműködik abban, hogy az adott szerv valótlan adatot foglaljon közokiratba anélkül, hogy tudna az adat igaztalan mivoltáról. Ilyenkor valós közokirat jön létre, a benne foglalt nem valós adatokkal. A határozat arra vonatkozóan is rendelkezik, hogy ha valaki, a személyazonosságának igazolására más nevére szóló valódi közokiratot is felhasznál, akkor az előző esetben felsorolt bűncselekmények mellett a Btk.342.§ (1) bekezdés b) pontjának harmadik fordulatába ütköző közokirat-hamisítás büntetéseért is felel.²¹

Az egészségügyi személyiséglopás egyre növekvő probléma világszerte. Ebben az esetben támadások a kórházakat, egyéb egészségügyi szolgáltatók servereit célozza, a páciensek társadalombiztosítási számának megszerzése érdekében. Az elkövetők motivációja lehet a magáncélú felhasználás, valamint az adatok továbbadása.

A következő csoport a szintetikus személyazonosság-lopás, amely során az elkövető valós információt/információkat kombinál egy másik létező vagy nem létező személy adataival, így hoz létre egy mesterkélt személyt.

¹⁹ MANAP, Nazura Abdul – RAHIM, Anita Abdul – TAJI, Hossein: Cyberspace Identity Theft: The Conceptual Framework. In: Mediterranean Journal of Social Sciences. Vol 6. No. 4. 2015. 600–602. o. letöltve: 2023.08.20.

²⁰ 2/2004. számú BJE határozat

²¹ 2/2004. számú BJE határozat

A gyermekidentitás-lopás a szintetikus alfaja, ebben az esetben a bűnözők gyermekek, és fiatakorúak társadalombiztosítási számának megszerzését tűzik ki célul. Megtörténhet, hogy a sértett csak 8 éves korában nyitja meg az első bankszámláját, azonban addigra már adóssága van a társadalombiztosítási számához kötve.

Egy különálló kategóriának számít az identitásklónozás, amely során a tettes minél több információt, lehetőség szerint személyazonosító adatot kísérel meg begyűjteni, majd felhasználni. Az elkövető tényszerűen leklónozza az áldozatot, és a lemásolt személyt fogja alakítani egy másik országban. Ilyenkor a klónozó személy célja, hogy az eredeti, saját identitását álcázza.²²

7. HOGYAN SZEREZHETŐK MEG A SZEMÉLYES ADATOK?

A személyes adatok megszerzésének rengeteg lehetséges módja van. Ma már olyan kidolgozott, megtévesztő metódusokat gondolnak ki az elkövetők, amiknek akár az informatikában jártasabb felhasználók is bedőlhetnek. Véleményem szerint, a legkönnyebben megelőzhető módja az adatszivárgásnak, ha maga a felhasználó nem oszt meg magáról személyes adatot. A közösségi média platformok, mint a Facebook, Instagram, Twitter stb. lehetővé teszik a felhasználóknak, hogy különféle tartalmakat osszanak meg. Sokszor egy ártatlan poszt, amit egy szülő posztol, például a gyermeke bizonyítványáról, vezethet az adatok szivárgásához. A szülő célja ezzel nem az adatok közzététele, hanem a büszkeségének megosztása az ismerősökkel. Ennek ellenére sok felhasználó nem ügyel arra, hogy kiknek osztja meg az adott fényképet, hanem akár nyilvánosan is látható lehet. A Facebook lehetőségeihez mérten be lehet állítani, hogy egy tartalmat az ismerősöknek, ismerősök ismerőseinek is megosztjuk, vagy nyilvános hozzáférést biztosítunk hozzá. Továbbá, az is előfordulhat, hogy egy családi vacsoráról készített kép sarkába belóg egy hivatalos ügyintézéshez szükséges papír, amin személyes adatok vannak vagy egy szelfi háttérben található kiolvasható információk, amelyekkel bárki visszaélhet. Előfordulhat az is, hogy az emberek találnak egy pénztárcát, amiben személyazonosító igazolvány van, vagy bármilyen más irat, amin személyes adatok vannak, és jószándékból, hogy megtalálják a tulajdonost, feltöltik a közösségi oldalra. Sokan nincsenek tisztában azzal, hogy ezzel sértik más személy személyes adatait, illetve nem tudják adott esetben a helyes eljárást, hogy be kell vinni a találás helye szerint illetékes jegyzőnek

²² MANAP, Nazura Abdul – RAHIM, Anita Abdul – TAJI, Hossein: Cyberspace Identity Theft: The Conceptual Framework. In: Mediterranean Journal of Social Sciences. Vol 6. No. 4. 2015. 600–602. o. letöltve: 2023.08.20.

vagy okmányirodának.²³ Az internet világának köszönhetően megjelent egy jelenség, amit túlzott megosztásnak (angolul: oversharing) nevezünk. Ez azt jelenti, hogy valaki túl sok személyes információt oszt meg magáról a közösségi oldalakon. Arra, hogy mi számít túl soknak nincsen objektív mérce, kortól, kultúrától és tartalomtípustól függően eltérő lehet, viszont legegyszerűbben úgy lehet meghatározni, hogy az a szint, ami már a megosztó követőit zavarja, a mennyiségük, vagy jellegük miatt.²⁴

Szintén probléma lehet a szemétkébe dobott papírok, dokumentumok, melyek személyes adatokat tartalmaznak.

Az egyik leggyakoribb adatszerzési technika az adathalászat. E tevékenység célja bizalmas információk eltulajdonítása, vagy megkárosítása olyan módon, hogy a klienseket csalárd módszerekkel személyes adatok, jelszavak hitel- és bankkártyaszámok megadására veszik rá.²⁵ Ezt legegyszerűbben a megtévesztés technikájával tudják végrehajtani. A csalók megbízható forrásnak mutatják magukat, és a felhasználó a véleménye szerint megbízható oldalnak fedi fel az adatait. Az adathalászatnak több különböző típusa van. Véleményem szerint a legelterjedtebb az elektronikus levelezési rendszeren keresztül küldött támadás, amely során hamis hivatkozásokkal, linkekkel próbálják rábírni a felhasználókat, hogy elküldjék a személyes adataikat. Sok esetben fiókszolgáltatónak adják ki magukat, mint a Google vagy Microsoft, vagy akár egy munkatársnak, régi ismerősnek. Számos változata létezik már ennek az adatnyerésnek. Sokszor adategyeztetés szükségességére hivatkozva kérnek adatokat, vagy nyereményjáték formájában. Ezekben az esetekben a felhasználónak magának kell megadni az adatait, amelyeket a megtévesztésük következtében szolgáltatnak. Olyan eset is gyakorinak számít, hogy a linkeken keresztül vagy e-mail mellékletekkel kártékony programokat telepítenek a kliens eszközére, amely kiolvashatja az azon tárolt személyes adatokat, vagy éppen ők mondják, hogy támadást észleltek a kliens gépén és kijavítják a problémát az adatokért cserébe. Sokan nem is gondolnak bele, hogy egy kattintással eladják az adataikat, hiszen ez akár csak évek múlva járhat következményekkel, nem feltétlen azonnal. Az említett hivatkozások nemcsak elektronikus levelezéseken keresztül juthatnak el a felhasználókhoz, hanem a közösségi média platformokon, SMS-ben és telefonos hívások révén is. A támadásoknak sok esetben nincs konkrét célpontja, hanem több személynek is elküldik ugyanazt a levelet és vagy bejön, vagy nem alapon próbálkoznak az adatok megszerzésére. Ez

²³ 2013. évi V. törvény a Polgári Törvénykönyvről 5.55.§

²⁴ Lexiq – Oversharing (<https://lexiq.hu/oversharing>) letöltve: 2023.08.20.

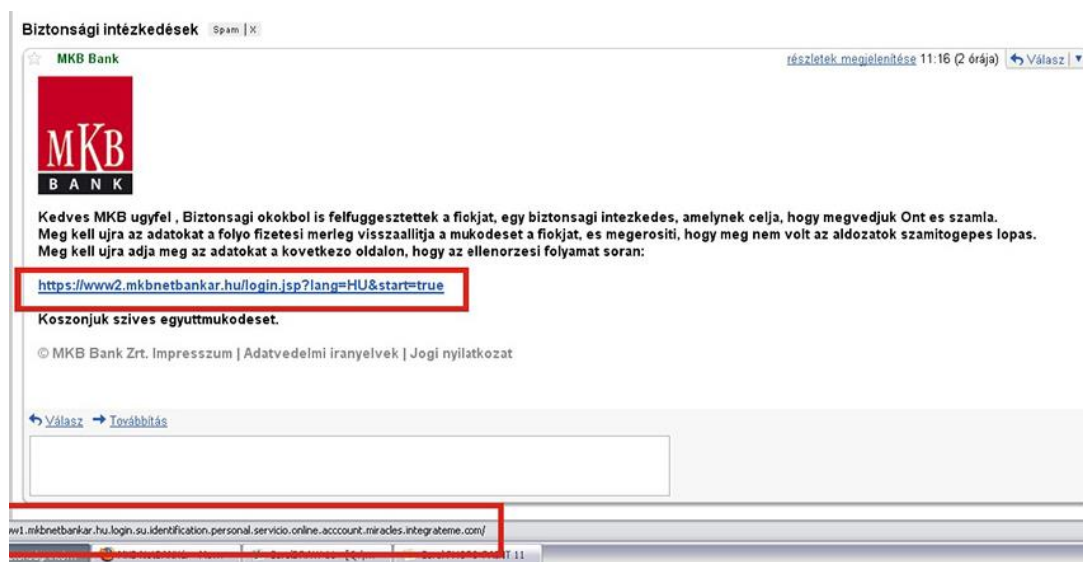
²⁵ Microsoft – Mi az az adathalászat (<https://www.microsoft.com/hu-hu/security/business/security-101/what-is-phishing>) letöltve: 2023.08.25.

gyakran botok használatával valósul meg. Ennek ellenére, irányulhat kitűzött célpont ellen is, és a személy munkájáról, közösségi életéről összegyűjtött információkat felhasználva próbálnak személyes adatokat kicsalni. A viselkedésüket, szokásaikat kifigyelve az aktuális élethelyzetükhöz igazítva tudják véghezvinni a sikeres adatszerzést. E támadások személyre szabott jellege miatt hatékonyak a kiberbiztonsági intézkedések kijátszásában.

„Bálnavadászat” kifejezéssel illetik az üzleti vezető, illetve híresség ellen intézett támadásokat. Ilyenkor az elkövető rendkívül alapos kutatás során kifigyeli, hogy mikor alkalmas a pillanat a bizalmas adatok eltulajdonítására.²⁶

Személy szerint úgy gondolom, hogy a legjellemzőbb adat, amit előszeretettel szereznek meg a tulajdonostól, az a bankkártya, bankszámla és pénzhez köthető információk. Azok a támadások, melyek nem konkrét egyén ellen irányulnak előbb kapcsolódnak a pénzintézethez köthető adatokhoz. Meghatározott személy ellen úgy vélem, más szándéka is lehet a támadónak, nem feltétlenül az anyagi kár. Természetesen a szándék nemcsak emberi méltóság sérelmére terjedhet ki ebben az esetben sem, hiszen a rosszakarás az anyagi kárban is megjelenhet.

Az adathalászatnak különböző taktikái lehetnek, melyek célja az emberek megtévesztése. Régebben jellemző volt, hogy egy adathalász e-mail nyelvezete elég magyartalan volt, illetve nem volt igényesen megfogalmazva.

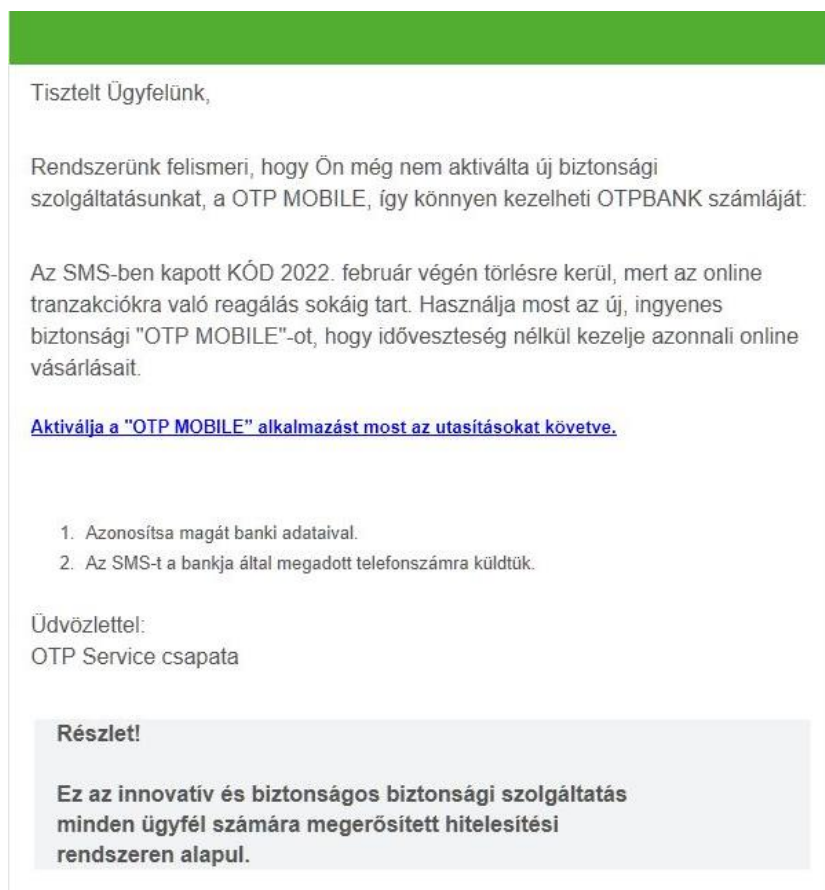


2. ábra Példa magyartalan adathalász e-mailre (Forrás: <https://biztonsagportal.hu/hogyan-ne-keruljunk-az-adathalaszok-halojaba.html>)

²⁶ Microsoft — Adathalászati trendek és technikák (<https://learn.microsoft.com/hu-hu/microsoft-365/security/intelligence/phishing-trends?view=o365-worldwide>) letöltve: 2023.08.25.

A képen látható, hogy ékezet nélkül, sok esetben értelmetlen mondatokkal teli levelet fogalmaztak az adathalászok.

Ma már a különféle fordító programok segítségével hitelesebbnek tűnő üzeneteket lehet írni. Emellett a technológia fejlődése, illetve a támadók leleményessége lehetővé teszi, hogy a szolgáltatókat szinte teljesen leutánozzák. Például, egy bank által kiállított számla, ahol a bank fejléce, a tartalom és minden ugyanazon a helyen helyezkedik el, mint egy eredeti számlán.



3. ábra Példa adathalász e-mailre (Forrás: <https://pcforum.hu/hirek/24323/vigyazat-emailben-probaljak-kicsalni-az-otp-ugyfeleinek-banki-azonositoit>)

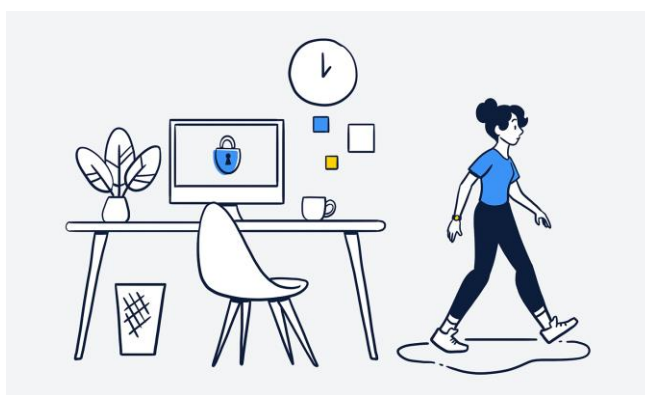
Párhuzamosan az online ügyintézés fejlődésével, egyre bátrabban használjuk az online történő azonosítást, ami rendkívül elősegíti, mind az ügyintézők, mind az ügyfelek munkáját. Ennek ellenére, a bankkártyadatokon túl a személyazonosító igazolvány lefényképezését, vagy kamerán keresztül történő bemutatását is kérhetik az elkövetők. A közösségi média profil elsajátítása során is fény derülhet olyan adatokra, amiket szívesen felhasználnak a támadók, például szülőnek, gyorsabb ügyintézéshez elküldött fotó egy személyes adatokat tartalmazó iratról, vagy dokumentumról.

Az áldozattá váláshoz hozzájárul, hogy a megtévesztő üzenetekre sokszor a felhasználók nem számítanak és bizalommal nyitják meg az elektronikus postaládájukba érkező tartalmakat. További ok, amiért az emberek bedőlnek az adathalászatnak a cselekvési kényszer. A felhasználó úgy érzi, cselekednie kell, példának okán, ha számlatartozásról érkezik e-mail gondolkodás nélkül megnyitja, hogy miről lehet szó.²⁷ Ehhez az is hozzájárul, hogy rohanó világban élünk. A nyomás és a szükség érzete alatt, sokszor elmulasztjuk azt, hogy megálljunk és átgondoljuk a dolgokat. Valóban kéri a bank azonosítás céljából a személyazonosító igazolványról egy fényképet? Nem feltétlen. Az érzelmi manipuláció eszközével a meglévő bizalom kijátszásával használják a sürgősség érzetét, például egy veszélyben lévő rokon nevében kérnek adatokat. A félelem és az aggodalom érzése az agyat megbénítva kényszeríti a felhasználót cselekedetre.

A különböző személyes információkat tartalmazó fiókokhoz való hozzáférés egyik módja a jelszavak megszerzése. A könnyű jelszó használata, például a gyermekünk neve, kutyánk neve, születési évünk, házassági évforduló nem szerencsés, ha védeni szeretnénk a fiókjainkat. Egy személyről információgyűjtéssel, például a közösségi média profilok elemzésével, vagy egyéb nyílt forrású információk megszerzésével az elkövetők tudomására juthatnak ezek az adatok és kikövetkeztetheti a jelszavát a személynek. Tapasztalhatjuk, hogy sok irodában kis cetlikre, naptárra különböző jelszavak vannak feljegyezve, de akár otthoni környezetben is. Ennek ellenére a cégeknek egyértelműen az ISO 27001 szabvány alapján a tiszta asztal politikát (angolul: clean desk policy) kellene alkalmazni az információk illetéktelen kézbe kerülésének megakadályozása érdekében. Ez azt jelenti, hogy a munkavállalók olyan módon hagyják ott az íróasztalukat, hogy azon semmilyen érzékeny adatokat tartalmazó dokumentum, irat nincs. Ezeket biztonságos helyre kell helyezni.



5. ábra Nem tiszta asztal (forrás: <https://en.idei.club/40838-clean-desk-policy.html>)



4. ábra Tiszta asztal (Forrás: <https://www.stackfield.com/blog/clean-desk-policy-162>)

²⁷ Microsoft – Mi az az adathalászat (<https://www.microsoft.com/hu-hu/security/business/security-101/what-is-phishing>) letöltve: 2023.08.25.

A jelszavakat adatvédelmi incidensek következtében a szolgáltatóktól, illetve vállalatoktól is ellophatják. Azonban népszerű a korábban már ismertetett mód, a megtévesztés, hogy az elkövető az adott szolgáltatónak adja ki magát, és így próbálja kicsalni az ügyféltől a jelszót. A következő támadási forma a brute force, azaz próbálgatásos jelszó feltörés. Ebben a szituációban a hacker az összes lehetséges kombinációt végigjátszva próbálja megfejteni a jelszót. E támadás egyik fajtája a szótár alapú, amely a legtöbbször alkalmazott jelszavakkal kezdi kimeríteni a próbálkozásokat, mint az angol „password” szó, vagy az 123456 számsor, vagy olyan adatbázisokat alkalmaznak, amelyek szimpla kulcsszavak, vagy már előzőleg kiszivárogtatott jelszavak. Döntő többségében az ilyen egyszerű jelszavak feltörése 10 másodpercet vesz igénybe, azonban egy bonyolult jelszó feltöréséhez akár 3000 év is szükséges lehet.²⁸ Az identitáslopás megelőzése című fejezetben kifejtem, hogy milyen követelmények szükségesek egy erős jelszóhoz.

A személyes adatok megkaparintásához használt módszer ezenfelül, amikor kártékony applikációkat, programokat töltenek le a felhasználókkal, valamint zsarolóvírusok útján is szerezhetnek információkat. Az ilyen jellegű vírusok zárolják a felhasználó eszközét vagy titkosíthatja az azon lévő adatokat, információkért cserébe.

Az elkövetők segítségére lehetnek különféle kémprogramok, kémszoftverek, amelyen célja, hogy a megfertőzött számítógépről megszerezzék a személyes adatokat. A felhasználó tudta nélkül a kémprogram összegyűjti az érdeklődési körre, böngészésre jellemző információkat és ezeket kielemezve kereshetnek meg a támadók ajánlatokkal, vagy bűncselekmény elkövetésére is felhasználhatják ezeket az információkat. További program a keylogger, ami billentyűzet-leütést figyelő alkalmazásokat jelent. Minden információ, adat, jelszó, amit begépel az ember a számítógépbe, illetve mobiltelefonba azt megjegyzi. Az ATM automaták esetében bankkártyákhoz tartozó PIN kódokat is szerezhetnek meg ilyen módon az elkövetők.

Természetesen az érzékeny adatok megszerzését fizikai térben elkövetett lopással is elkövethető, azonban én a dolgozatomban az online tér veszélyeire szeretném felhívni a figyelmet.

²⁸ Pénzcentrum – Megdöbbentően sok jelszó kerül rossz kezekbe: légy résen, így kerülheted el a kellemetlen meglepetést 2023 (<https://www.penzcentrum.hu/tech/20230531/megdobbentoen-sok-jelszo-kerul-rossz-kezekbe-legy-resen-igy-kerulheted-el-a-kellemetlen-meglepetest-1137602>) letöltve: 2023.09.02.

8. AKTUALITÁS

A napjainkban a legelterjedtebb Magyarországon elkövetett, személyiséglopással összefüggésbe hozható bűncselekményeknek két kategóriája van.

Az első, talán „kevésbé veszélyes” fajtája az adathalász email-ek, ezen belül is a bankkártyaadatok célzatos megszerzésére irányuló, hamis tartalmú levelek.

A témában egyáltalán nem jártas, laikus ember is hallhatott már az ún. Vinted-es, Jófogásos, Facebook Marketplace-es vagy Foxpost-os csalásokról, hiszen szerencsére a médiában is egyre több szerepet kap. A fent megnevezett csalások lényege a következő. Egy teljesen ártatlan személy a leírt weboldalak egyikén eladásra kínálja valamely saját dolgát, például egy babakocsit, fotelt, televíziót. Erre a hirdetésre jelentkezik az ismeretlen személy magyar vagy más nemzetiségű profillal. Főként chatszolgáltatáson keresztül, elektronikusan beszélget az eladóval, azonban néha előfordul az is, hogy mobiltelefonon keresztül, szóban is megnyilvánul.

Az ismeretlen vásárló elkezd az eladásra kínált termék iránt érdeklődni, sőt, sok esetben még alkudozni is próbál, majd eldönti, hogy meg szeretné vásárolni azt, és megbeszéli az eladóval, hogy valamely magyarországi csomagküldő (pl. Foxpost, GLS) szolgáltatás útján szeretné, ha a fizetés és a szállítás teljesítve lenne. Amennyiben az eladó ebbe belemegy (az esetek többségében igen), akkor a vásárló egy, a fenti szolgáltatások hivatalos levelére megtévesztésig hasonló email-t küld az eladónak, amelyben a mit sem sejtő eladó egy linkre kattint, ahol a megnyíló webhely kéri a bankkártyaadatait. Természetesen ez kitöltésre kerül, hiszen az email teljesen valósnak tűnik, és ez más, megbízható webáruházaknál is egy bevett fizetési módszer.

A bankkártyaadatok kitöltése után az ismeretlen vásárló azt írja/mondja az eladónak, hogy kapni fog egy SMS-ben vagy email-ben érkező kódot, amelyet meg kell adnia neki, hogy a csomagküldő szolgálat a rendelést teljesíteni tudja. Másik módszer, hogy a kód beírására történő lehetőség több esetben már abba a webhelybe bele van építve, amelyben előzetesen a bankkártyaadatait megadja az eladó. Miután ezek végrehajtásra kerültek, a vásárló szól, hogy órákon belül utalja az összeget a hirdető által megadott bankkártyaadatok alapján. A vásárló ezen felül egy magyarországi pontos címet is megad, ahova a hirdető elküldheti a terméket a kifizetés ellenében. Persze ez is kizárólag a bizalom növelésére irányul.

Eladónk tehát teljességgel abban a tudatban hagyja ott a számítógépet vagy teszi le a telefont, hogy az általa megadott bankkártyaadatok arra szolgálnak, hogy a vevő a csomagküldő szolgáltatáson keresztül a fizetést teljesíteni tudja.

Ezután percek, de lehet, hogy akár órák telnek el, nem történik semmi, nem érkezik meg a megbeszélrt összeg az eladó számlájára.

Szerencsésebb esetben a mit sem sejtő hirdetőnek be van kapcsolva az SMS értesítő szolgáltatás a banki tranzakciók tekintetében, vagy a telefonján lévő applikáció szól, ha valamilyen terhelést vagy jóváírást kap a számlájára az adott személy.

Azonban sajnos sok sértett ezt nem használja, és csak jóval később, az internetbankjába belépve vagy a bankfiókjától kapott nyomtatott tranzakciós lista alapján látja, mi is történik a számláján, miközben ő mindennapi életét éli.

Tegyük fel, hogy a fent leírt példában szereplő eladónak nincs SMS vagy applikációs szolgáltatása. Miután a beszélgetés az ismeretlen vevővel lefolytatásra került, eltelik a megbeszélrt óraszám, így az eladó megnézi az internetbankon keresztül, hogy megérkezett-e a kívánt összeg. Ekkor szembesül azzal, hogy nem csak a pénz nem érkezett meg, de a számlájáról a bankkártyája segítségével több százezer- vagy millióforintnyi pénzt vettek fel egy ATM automatából az ország bármely részén.

Amennyiben rendelkezik SMS vagy applikációs értesítéssel, akkor sem változik sokat a dolog, mivel a fent említett pénzfelvétel pár perc vagy akár másodperc alatt végbemegy egészen addig, amíg az a napi limitet – amennyiben van ilyen beállítva – el nem éri. A tranzakciók közleményében minden esetben az „Apple Pay” szó szerepel.

Fentieket a laikus eladó szemszögéből taglaltam, most pedig lássuk, mi történik a valóságban, és nézzük meg azt is, miként lehet elkerülni az ilyen csalásokkor való áldozattá válást.

Az ismeretlen vevő egy viszonylag vagy teljesen frissen kreált profillal keresi fel a hirdetőt, ami – Facebook esetében – könnyen ellenőrizhető a profil megtekintése során. Ez az első dolog, ami gyanúba keverheti az elkövetőt, azonban több webáruháznál a profil létrehozása dátumának megismerésére nincs lehetőség.

A vevő növelni kezdi az eladó bizalmát azzal, hogy „elbeszélget” vele, alkudozik, kedvesen ír/szól hozzá. Egy olyan árban egyeznek meg, ami az eladónak mindenképp teljességgel megfelelő.

Viszont itt kezdődik a csavar a történetben. A vevő egy hamis email címről küldi az adott csomagküldő szolgálat levelére megtévesztésig hasonlító email-t, a benne szereplő link pedig nem arra szolgál, hogy azon keresztül a vevő teljesítse a kifizetést, hanem arra, hogy az adathalász linken keresztül az elkövető megszerezze a sértett bankkártyaadatit. A fent említett

SMS-ben vagy email-ben kapott kód ahhoz kell, hogy az elkövető az Apple márkájú mobilkészülékén a bankkártyaadatok megadását követően a bankkártyát elektronikus úton hozzá tudja rendelni az Apple Pay nevű, kizárólag az iPhone típusú készülékeken használható elektronikus fizetési rendszerhez. Manapság országunkban nagyon sok olyan bankautomata fellelhető, amelybe történő belépéshez nem szükséges a bankkártya fizikai behelyezése, elég, ha a bankkártyánkat, vagy a mobilunkon fellelhető NFC rendszer (érintéses műveleteket lehetővé tevő szolgáltatás pl. fizetéshez vagy a telefon töltéséhez) használatával a mobiltelefonunk hátulját hozzáérintjük az automata erre kialakított részéhez. Előbbi módon ugyan be kell írunk a bankkártyánkhoz tartozó 4 jegyű kódot, azonban utóbbinál ez a jelszó egy általunk, az applikációba történő regisztrációkor megadott kód, amely nem kell, hogy egyezzen a bankkártyánk 4 jegyű jelszavával.

Az ismeretlen elkövető tehát a bankkártyánkat az előzetesen általunk megadott adatok és SMS vagy email-es kód segítségével hozzárendeli az Apple Pay fizetési rendszerhez, ezután egy tetszőleges bankautomatához lépve érintéses módon, az általa korábban választott applikációs jelszó megadásával belép a bankunkba, és kedvére emel le összegeket róla.

Fentiek olvasása során látható, hogy az Apple Pay fizetési rendszer nagyon sok biztonsági kockázati kérdést vet fel, azonban ennek ellenére is, a bankok ezt a módszert úgy veszik, mintha saját magunk hajtották volna végre a tranzakciót, hiszen nem csak a bankkártyaadatainkat adtuk meg az Apple Pay-nek, de még a biztonsági kódot is, amit elvileg csak mi magunk ismerhetnénk meg, és ez a kód elengedhetetlen az Apple Pay-hez történő bankkártya regisztrációhoz. A sértett azonban ezt nem sejtette, hiszen azt gondolta az elkövető vagy a hamis weboldal tájékoztatása alapján, hogy a kód csak a csomagküldő szolgáltatás használatához kell. Az elektronikus pénz készpénz formájában leemelésre kerül, a bankok pedig fentiek miatt elzárkóznak a kártérítéstől, a tranzakciót pedig visszafordítani sem tudják, hiszen a pénz nem elutalva, hanem felvéve lett a sértett bankszámlájáról.

A rendőrség egyedül a megtévesztéshez használt profilban megadott személyes adatok, esetleges IP-címek megkeresések útján történő megismerésében vagy a bankautomatába beépített biztonsági kamera felvételeire hagyatkozhat, azonban az ilyen jellegű bűncselekmények nyomozása nagyon nehéz tekintettel a különböző VPN szolgáltatókra és az automaták kamerájának egyszerű eltakarására.

Fentiek a személyiséglopás témakörébe tartoznak, hiszen az ismeretlen elkövető a sértettől szerzett bankkártyaadatok (így név, kártyaszám, lejárat dátum, CVC kód) megszerzésével a sértett nevében végez pénzügyi műveleteket annak számláját használva.

Hogyan tudjuk megelőzni az ilyen jellegű átveréseket? Első körben minden esetben nézzük meg az adott vásárlói profilt, amennyiben lehetséges, akkor azt, hogy mikor kreálták a fiókot vagy milyen értékelésekkel rendelkezik. Amennyiben ennek során különösebb gyanúra okot adó körülményt nem találunk, minden esetben nézzük meg azt a levelezési címet, amelyről az ismeretlen vevő a Foxpost-os vagy egyéb más csomagküldési szolgáltatásra megtevéstésig hasonló email-t küldi. Ez a cím minden esetben el fog térni az eredeti szolgáltató hivatalos e-mail címétől, ha csak egy karakterben is. Próbáljuk kerülni azokat a weboldalakokat, ahol a bankkártyadataink megadása szükséges a fizetéshez. A kapott biztonsági kódot soha ne adjuk ki harmadik személy részére. Amennyiben nem vagyunk biztosak magunkban, ne legyünk restek segítséget, tanácsot kérni hozzáértő ismerősünktől, barátunktól, családtagunktól.

A másik, sokkal inkább veszélyes személyiséglopással összefüggésbe hozható elkövetési módszer az ún. Anydesk-es csalás. Erről is hallhatott már a laikus is, hiszen a kettő nagy aktuális módszer közül erről beszélnek többen a médiában. Azonban még ennek ellenére is a mai napig nagyon sokan esnek áldozatul ennek az átverésnek. Legegyszerűbben egy konkrét ismerősöm által tapasztalt példán keresztül tudom szemléltetni az ilyen csalások kockázatait és következményeit. Az anonimitás megőrzése érdekében egy általam választott, nem releváns keresztnévvel utalok a sértettre.

Péter egy idős bácsi, régóta tesz félre elektronikusan pénzt különböző helyeken, így például állampapírszámlán és összesen 2 db bankszámlán. Célja az, hogy halálakor az unokáinak egy nagyobb összeggel tudjon segíteni életük elkezdéséhez. Már egy jelentős összeg, 19.000.000 forint összegyűlt ezeken a számlákon.

Egy teljesen átlagos napon érkezik egy hívás Péter mobiltelefonjára egy ismeretlen, Telekom-os hívószámról. Egy hivatalosan és határozottan beszélő hölgy mutatkozik be neki, aki közli, hogy ő az OTP Bankbiztonsági Osztály munkatársa, és azért telefonál, mert a központban gyanús tranzakciókat észleltek a bankszámláján, amelyek kivizsgálásában és megállításában szeretne segítséget nyújtani. Az ismeretlen hölgy Annaként mutatkozik be, gyorsan beszél, Péternek ideje sincs átgondolni a helyzetet, megijed, és bármit megtenne, hogy a sok-sok év alatt felhalmozott pénzének ne essen baja.

Anna közli, hogy egy ún. Anydesk alkalmazást kell a számítógépére, és egy Ruskdesk nevű alkalmazást pedig a telefonjára letöltenie. Péter fél, már idős, nem ért a számítástechnikához, gyorsan megteszi, amire kéri. Anna mindkét alkalmazás vonatkozásában elkéri azt a biztonsági kódot, amit Péter lát, ez kell ahhoz, hogy teljes hozzáférést adjon a készülékeihez. Ezt Anna nyíltan közli is, azt mondja, hogy ez kell ahhoz, hogy a számláin lévő pénzt biztosítani tudják. A kód megadását követően Anna és esetleges társai teljes hozzáférést kapnak Péter számítógépéhez és mobiltelefonjához, minden, amelyet azon belül végrehajtanak olyan, mintha Péter saját maga csinálta volna.

Péter jelszavai előzetesen elmentésre kerültek, hogy gyorsan és egyszerűen be tudjon lépni a netbankjába.

Miután Anna megkapta a kívánt hozzáférést a géphez, elkezd azon dolgozni. A sértettel eközben folyamatos telefonos összeköttetésben van. Olyan dolgokat mond és csinál, amelyek elterelik a gyanút valódi szándékairól. Miután Anna egy kis ideig folyamatosan semmitmondó dolgokat kérdez, csinál a gépen, mindenhez előzetes engedélyt kér, egyszer csak arra kéri Pétert, hogy kapcsolja ki a monitort. Péter ekkor már teljességgel megbízik Annába, csodálkozik a kedvességén, profizmusán, határozottságán és aranyos hangján. Anna nem akarhat mást, csak segíteni, megteszem. Gondolja Péter, majd kikapcsolja a monitorját.

Amint Anna meggyőződik róla, hogy Péter megtette, amit kért, a következőket hajtja végre. A 2 db bankszámlán található kb. 10.000.000 forintot átutalja egy ismeretlen, K&H Bank-nál vezetett számlára, az állampapírban lévő kb. 9.000.000 forintot átváltja, kiutalja a sértett számlájára, majd ezt is tovább utalja az ismeretlen számlaszámra. Eközben természetesen folyamatosan szóval tartja telefonon keresztül a sértettet. Az utalások után személyi kölcsön felvételét kezdi meg 10.000.000 forint összegben. Amennyiben a bankok bármilyen mobilra SMS-ben vagy e-mail-en érkező engedélyt, kódot kérnek, a telefonra letöltött Ruskdesk alkalmazás segítségével azokat is azonnal meg tudja adni.

Péternek valamilyen oknál fogva kissé gyanússá kezd válni, hogy a monitor sokáig ki van kapcsolva, így visszakapcsolja azt. Amit ekkor lát, az minden ember rémálma. Az évekig, mondhatni, hogy egész élete során összekuporgatott, a családjának félretett pénze odalett. Azonnal bontja a vonalat, kikapcsolja a számítógépet, így az Anydesk program működése is leáll. Azonban telefonját nem kapcsolja ki, a Ruskdesk alkalmazás miatt a mobilja továbbra is az ismeretlen elkövetők irányítása alatt áll. Csak órákkal később, unokája megérkezése, tájékoztatása után kapcsolják le kényszerleállítással a feltelepített alkalmazást, de ez már nem

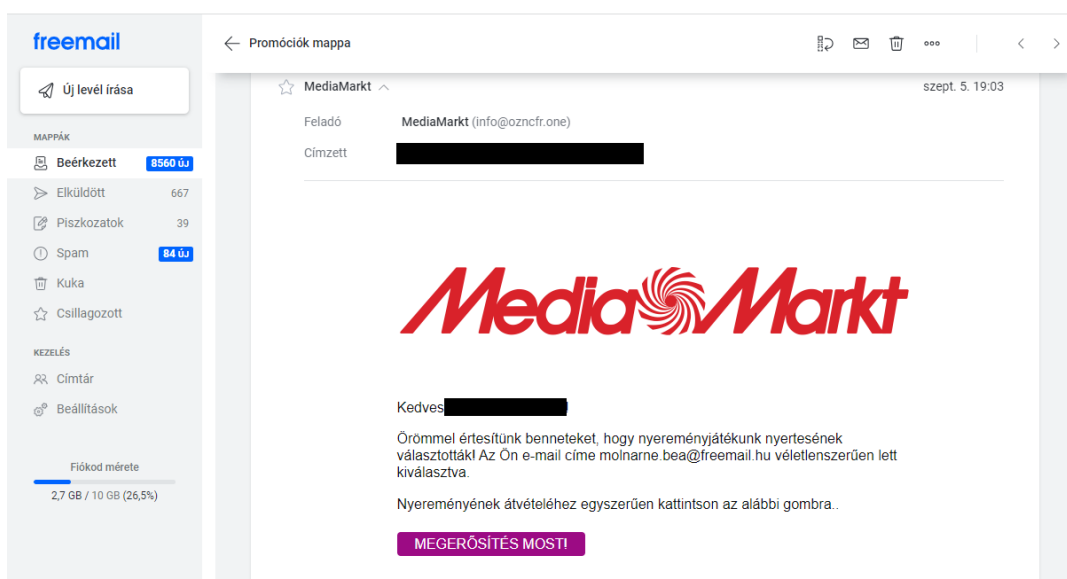
segít. A félretett 19.000.000 forint egy ismeretlen, magyar számlaszámra került át, ahonnan azonnal tovább utalásra került egy külföldi cég számlájára. A pénzmozgás nehezen, vagy egyáltalán nem nyomon követhető. A bank nem tud felelősséget vállalni, hiszen a tranzakciókat a sértett „saját maga” hajtotta végre. A magyar rendőrség az elkövetők által használt VPN szolgáltatások miatt a telefonszámokat és az Anydesk, Ruskdesk programot nem, vagy csak hatalmas nehézségek és idő árán tudják visszakövetni, ekkor sem garantált sikerrel.

Vajon hogyan tudta volna Péter megelőzni azt, hogy egy ilyen csalás áldozatává legyen? Első sorban ismernie kellett volna, hogy a hivatalos banki ügyintézők milyen adatokat kérhetnek és kérnek egy-egy ilyen telefonhívás kapcsán. A bankok sosem kérnek bankkártya vagy bankszámla adatokat, sosem kérik, hogy programokat telepítsünk fel. Amennyiben tényleges gyanús tranzakciókat észlelnék, automatikusan letiltják a számlát és értesítik az ügyfelet, de egyéb személyes vagy különleges adatot nem kérnek tőlük. Előfordulhat, hogyha mi fordulunk bankunkhoz problémával, akkor azonosítás céljából kérnek információt, de akkor sem bankkártya adatokat. Ha viszont már megvan a baj, és hozzáférést adtunk az ismeretlen elkövetőknek az eszközeinkhez, talán egy kis gondolkodási időt adhat az, ha nem mentjük el a jelszavainkat a telefonon, vagy a számítógépen. Nem írjuk fel jegyzetbe a jelszavainkat sem, hanem megjegyezzük azokat, és minden esetben újból beírjuk, amikor például a netbankunkba akarunk belépni. A jelszó sok karakterből álló, minden weblapon különböző, kis- és nagybetűkből, számokból összetevődő legyen. Az elkövetők az esetek túlnyomó többségében nem professzionális hackerek, nem fognak tudni belépni sem a gépünkbe, sem az internetes fiókjainkba, ha mi magunk meg nem adjuk nekik az ahhoz szükséges kódjainkat. Amit Péter mindenféleképpen jól csinált, az az, hogy nem egy helyen tartotta ezt a nagy mennyiségű összeget. Mindig egyszerre több számlán, módon tartjuk a megtakarításainkat. Jó módszer lehet, ha félretett pénzünk egy kisebb részét a bankszámlánkon, nagyobb részét pedig például értékpapírszámlán és/vagy más devizában (euró, dollár) tároljuk. Ezzel a módszerrel marad a mindennapokra felhasználható forintunk is, azonban mégsem értéktelenedik el a mostani inflációs környezetben a megspórolt pénzünk. Ami a legfontosabb pedig, hogy ennyivel nehezebb lesz a csalóknak hozzáférni a megtakarításainkhoz. Büntetőjogilag ez a két bűncselekmény az információs rendszer felhasználásával elkövetett csalás tényállását meríti ki.

9. IDENTITÁSLOPÁS MEGELŐZÉS

Nézőpontom szerint a személyiséglopás megelőzésének a kulcsa a felhasználók tudatosításában rejlik. Ebből kifolyólag szánom dolgozatomat prevenciós célokra, illetve a kutatásom során készítettem egy weboldalt, amit a kérdőívem végére csatoltam. Számos esetben a felhasználó figyelmetlensége, nem kellő mértékű elővigyázatossága okozza a problémát. Szeretnék ismertetni néhány hasznos tanácsot arra vonatkozóan, hogy hogyan lehet elkerülni az áldozattá válást a kibertérben.

Az egyik legfontosabb lépés a biztonságos hálózat, illetve internetkapcsolat használata. Ezalatt értve a nyilvános Wi-Fi hálózatok kerülését, valamint a VPN szolgáltatások alkalmazását. A virtuális magán hálózat (VPN) biztonságos kapcsolatot teremt a készülék és az internet között. Az ismeretlen eredetű linkeket is célszerű kerülni, valamint az e-mailben kapott kétes eredetű üzeneteket ajánlott figyelmen kívül hagyni. Az elektronikus levelezés esetén intő jelnek minősülhet az idegenszerű nyelvezet, valamint maga az e-mail cím, amiről az üzenet érkezett. Példának okán, a napokban egy kedves ismerősimtől kaptam egy üzenetet, hogy az alábbi mail csalás-e.



6. ábra Mediamarkt csalás

A képen látható, hogy az e-mail cím így szól info@oznfr.one. A Google-ben az e-mail címre rákeresve semmilyen összefüggést nem találtam a MediaMarkttal összefüggésben, illetve az üzlet weboldalán sem volt ez az elektronikus levelezési cím feltüntetve. Jól megfigyelhető, hogy még a logóját is használják az áruháznak. A „Megerősítés most!” felirat, tartalmazza a linket, ahol valószínűsíthető, hogy személyes adatokat kérnek (lakcímet, bankkártyaadatot).

Ha szolgáltató nevében érkezett levél, érdemes leellenőrizni a hivatalos oldalon megadott elérhetőséggel egyezik-e, akár egy pont eltérés is lehet. A kormányzati szervek által használt gov.hu domain, könnyen összetéveszhető lehet a q-val írt qov.hu-oz.

A hívásokon keresztül történő azonosításnál kerüljük a személyes adatok közlését, kivéve, ha mi kezdeményezzük a hívást, a hivatalos telefonszámra.

A számítógépes hálózatokban a tűzfal használata is megvédheti az eszközünket a kártékony tartalmaktól, mivel blokkolja, vagy éppen engedélyezi a hálózati forgalmat. Fő célja, hogy védje a számítógépeket és a hálózatokat a veszélyes, ártó jellegű támadásoktól, amik következtében átvehetik az irányítást az eszközünk felett. Tehát a hálózati biztonságot szolgálja ez a szoftver- vagy harver-alapú rendszer. A legtöbb operációs rendszer alapjáraton rendelkezik beépített tűzfallal, viszont ezekre csak az alapvető funkcionalitás vonatkozik, amely sebezhetőségét már a potenciális támadók már ki tudják cselezni. Ebből kifolyólag a tűzfal védelmét szükséges megerősíteni vírusirtó programmal.²⁹ Úgy gondolom, hogy a lehetséges károk megelőzése érdekében előnyös megbízható és alapos vírusírtót alkalmazni, annak ellenére, hogy ezek sokszor nem ingyenesek. Felmerül a kérdés, hogy az adatainkkal szeretnénk fizetni a bűnözőknek viselve az egész életünkre kiható következményeket, vagy inkább a problémák megelőzéséért fizetünk. Természetesen, fellelhetők ingyenes alkalmazások is, azonban azok kevesebb szolgáltatást nyújthatnak, mint egy fizetős verzió. A keresőmotorokban egyszerű kereséssel a feltételeinknek megfelelő programot kiválaszthatjuk.

A program, alkalmazás letöltésekkel kapcsolatban fontos kritérium, hogy megbízható oldalról történjen a letöltés, a legjobb megoldás, ha az eredeti hivatalos oldalról kezdeményezzük a telepítést. Így kevesebb eséllyel futunk bele a kártékony program telepítésébe. A weboldalak biztonságának ellenőrzése is célszerű. A weboldalak URL-címe az SSL (Secure Sockets Layer) protokollal kezdődik: https://. A https-ből az „s” a securityt, tehát a biztonságot jelenti. A legtöbb böngésző jelzi, hogy az adott oldal biztonságos-e (https) vagy nem biztonságos (http).

A leggyakoribb kereső szolgáltatás esetében, a Google-n alapjáraton, egy biztonságos weboldalon ezt láthatjuk:



7. ábra Biztonságos weboldal

²⁹ ESET Progress. Protected. – Tűzfal (<https://www.eset.com/hu/tuzfal/>) letöltve: 2023.08.30.

A következő preventatív mód az erős jelszó használata. Legyen szó az e-mail fiókról, közösségi média oldalról, vagy ügyfélkapu belépésről, mindig ügyeljünk arra, hogy lehetőség szerint több különböző jelszót használjunk, és próbáljuk meg megjegyezni őket. A korábban szemléltetett példából kiindulva nem szerencsés a telefon jegyzetébe beírt kódot sem használni, kivéve, ha az megfelelő eljárással titkosítva van. Több jelszó biztonságos használatát elősegíti a jelszószev használata, amihez egy jelszót kell csak megjegyeznünk. Véleményem szerint rengeteg ember preferálja a rövid, könnyen megjegyezhető jelszavakat, mint a gyermekük neve, kisállatuk neve, születési dátumok, házassági évforduló. Ezek nem minden esetben célszerűek. Felmerül a kérdés, hogy mi bizonyul erős jelszónak? Minél hosszabb, minimum 12 karakterből álló jelszavakat ajánlott használni, amik tartalmazznak vegyesen kis és nagybetűket, számokat, illetve ha van rá lehetőség speciális karaktereket. Egy témával kapcsolatos előadáson volt lehetőségem részt venni, ahol közölték, hogy a legtöbb jelszó így néz ki, ami kimeríti az alap feltételeket: „Mágiarakás74”. Ez a szókapcsolat 12 karakterből áll, tartalmaz kis- és nagybetűt, és számokat is. Ez sem minősül teljesen biztonságos jelszónak, hiszen kiszámítható, hogy az emberek többsége a nagybetűt a szó elejére teszi, a számokat pedig a végére. Ugyanezt a szót lehet máshogy is használni: „m4g14_r4ká3:74” Ez már több karakterből áll és tartalmaz speciális karaktert is. A betűket lehet számokkal is helyettesíteni. Létezik egy oldal, a security.org³⁰ ahol le lehet ellenőrizni, hogy egy jelszó milyen erősségű, természetesen egy használatunkban lévő jelszavunkat ne írjuk be, de hasonló karakterlánccal meg lehet nézni, hogy az adott jelszót egy gépnek mennyi időbe kerülne feltörni. Az oldal szerint a „Mágiarakás74” jelszót 3 trillió évbe kerül feltörni. Nézzünk egy kitalált karaktert, Julcsit. Julcsinak van egy Facebook fiókja, ahol fel van tüntetve a születésnapja, születési évvel együtt. A lány jelszava az általam kreált jelszó, amit 3 trillió évbe kerülni megfejtetni. Julcsi 1974-ben született, Instagramon az alábbi néven van fent: julsika74. Julcsi gyakran posztol szeretett háziállatáról Mágiarakásról, a cicáról. Ennyi információ alapján egy kis keresgéléssel, akár 5 percbe is telhet Julcsi jelszavának a feltörése. A másik jelszó „m4g14_r4ká3:74” feltörése a weboldal szerint 7 trillió évbe kerülne egy számítógépnek, és a nyílt forrású információszerzésből sem feltétlen lehet kitalálni.

Szintén fontos kiberbiztonsági kérdés a többfaktoros autentikáció. Az erős jelszóhasználat mellett ez is növeli az adataink biztonságát. Ebben az esetben a hagyományos felhasználónév-jelszó páros kiegészül egy azonosítással, hogy biztos a tulajdonos ül az okos eszköz előtt. Ez lehet akár biometrikus azonosító (ujjlenyomat, Face ID) vagy PIN-kód, vagy SMS-ben kapott

³⁰ <https://www.security.org/how-secure-is-my-password/>

megerősítő kód. Egy jól működő rendszerben a második faktor csak egyszer használható egyidejű jelszó, angolul: one time password, OTP. Az OTP-nek van lejárat ideje is, hogy mennyi időn belül lehet felhasználni. A jelszóséf mellé is ajánlott kétlépcsős azonosítást alkalmazni, hogy egy jelszó feltörésével ne juthassanak a többihez. A kétlépcsős hitelesítés bekapcsolható több nagyobb szolgáltatónál is, mint a Google, Microsoft vagy a Facebook, de vannak erre is külön alkalmazások. A banki tranzakcióknál, főleg az online vásárlások esetében is érdemes bekapcsolni azt a funkciót, hogy kérjen az alkalmazás előzetes engedélyt a felhasználótól.

A személyes adatok védelmét biztosító intézkedés lehet még, ha odafigyelünk, hogy mi kerül a szemetesünkbe. Biztos jó néhány emberrel előfordult már, hogy akár egy 10 évvel korábbi orvosi leletet, vagy egy számlát, vagy személyes adatot tartalmazó dokumentumot kidobott a kukába anélkül, hogy a rajta lévő adatokat megsemmisítette volna. Nem gondolva a következményekre, ha azokat az információkat megszerzi valaki. Az adatkezeléssel foglalkozó szervezetnél ez előírás, hogy darálóval vagy más módon megsemmisítsék a már nem szükséges érzékeny iratokat. Ezt úgy gondolom, hogy a magánéletünkben is fontos lenne alkalmazni.

A bankszámlakivonatok rendszeres ellenőrzése is célszerű lehet, hiszen ha számunkra ismeretlen tranzakciót találunk érdemes a bankkártyát minél előbb letölteni. A legtöbb banknál igénybe vehető szolgáltatás, hogy SMS-ben értesítsenek minket a vásárlásokról, viszont ez plusz költségekkel járhat. A netbank alkalmazások is megfelelőek a tranzakciók nyomon követésére.

10. PROFILOZÁS, MINT ADATGYŰJTÉS

A rengeteg adat keletkezésének hátterében létjogosultságú kérdéskör az adatok megfelelő kezelése, és hogy milyen adatokhoz kik férhetnek hozzá az interneten. Minden szolgáltatónak érdeke, hogy olyan dolgokat hirdessen a felhasználónak, ami iránt érdeklődik. A legtöbb ingyenesen használt szolgáltatás, mint a Google vagy Facebook elemzi az adatainkat, tehát ezekkel fizetünk érte. Előfordulhat, hogy amikor két személy például rózsaszín ágynemű vásárlásáról beszélget, bedobja hirdetésbe. Ebben az esetben nem hallgat le minket a készülékünk, hanem előzetes cselekvés megelőzte a hirdetést. Például előzetesen látott már rózsaszín ágyneműről képet, percekig nézegette majd kedvelte, vagy éppen keresgélt is már, hogy venni szeretne. A jövőre vonatkozó hirdetések hátterében bonyolult algoritmusok és a mesterséges intelligencia áll. Az interneten keletkeztetett adatoknak nyomuk marad. Véleményem szerint sok emberrel előfordult már, hogy egy weboldalt nézegetve zavarta, hogy valami belelóg a képbe, de amint rákattint az „Elfogadom” szóra, máris teljes képernyőn olvasgathatta az adott hírt. Számos felhasználó nem is tudja, hogy ilyen esetben mihez járul hozzá. Az általános adatvédelmi rendelet alapján az adatkezeléshez történő beleegyezésnek minősül, ha a felhasználó egy *„internetes oldal megtekintése során bejelöl egy erre vonatkozó négyzetet, hiszen az információs társadalommal összefüggő szolgáltatások igénybevétele során erre vonatkozó technikai beállításokat hajt végre, valamint bármely egyéb olyan nyilatkozat vagy cselekedet is, amely az adott összefüggésben az érintett hozzájárulását személyes adatainak tervezett kezeléséhez egyértelműen jelzi. A hallgatás, az előre bejelölt négyzet vagy a nem cselekvés ezért nem minősül hozzájárulásnak.”*³¹ A rendelkezést figyelembe véve az előre bejelölt négyzet nem minősül hozzájárulásnak, de ha előre be van jelölve a négyzet és a személy rákattint az elfogadásra, azzal már megvalósul a technikai beállítás, amely az engedélyezést szolgálja.

³¹ AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) (32) bekezdés letöltve: 2023.09.03.

A cookie-k, magyarul süti elfogadása engedélyt ad a webhelynek, hogy adatokat tároljon a felkeresett oldalakra látogató kliens készülékén. Így lehetséges, hogy egy korábban látogatott oldalon nem szükséges újra bejelentkezni a felhasználónévvel, hanem már bejelentkezve tölti be a weboldalt. Mindemellett a süti statisztikai adatokat is gyűjtenek a felhasználó böngészési szokásairól.³² A süti nem engedélyezése, illetve csak a szükséges cookie-k elfogadása plusz energiát vesz igénybe, hiszen sok oldalon nincs lehetőség az összes süti elutasítására, hanem a figyelmesebb felhasználó egyesével végig kattintja őket. Természetesen ezek mennyisége sem mindegy, személy szerint, ha gyorsan el szeretnék olvasni egy cikket, és már két perce a sütit kapcsolgatom, lehetséges, hogy inkább bezárom az oldalt és más forrásból próbálok informálódni. Az Origo oldalán lettem figyelmes arra, hogy a cookie-k adatkezelési beállításainál a különböző kategóriáknál a „Beleegyezés” alatt szerepel a „Jogos érdek”, ami alapjáraton be van kapcsolva.

8. ábra Süti további beállításai

A GDPR alapján jogszerű az adatkezelés, ha „az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé, különösen, ha az érintett gyermek.”³³

³² Európai Bizottság hivatalos honlapja: Cookie-k használata (https://commission.europa.eu/cookies-policy_hu) letöltve: 2023.09.03.

³³ AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet) 6.cikk (1) bekezdés f) pontja letöltve: 2023.09.03.

Felmerült bennem a kérdés, hogy mi az a jogos érdek, és ha nem egyezek bele, azt miért engedélyezi a weboldal automatikusan? Természetesen ez is kikapcsolható. A kérdőjel ikonra kattintva megtudtam, hogy a jogos érdek azt jelenti, hogy léteznek olyan szolgáltatók, amelyek nem kérik az egyén hozzájárulását, de jogos érdekeik alapján mégis felhasználják a felhasználó személyes adatait. Jogos érdeknek minősülhet az adatvédelmi rendelet alapján, ha az érintett az adatkezelő ügyfele vagy annak alkalmazásában áll. Továbbá, csalások megelőzése céljából, vagy üzletszerzési célból, valamint közhatalmi szervek, kiber-, informatikai-, vagy hálózatbiztonsági célból, az feltétlenül szükséges és arányos. Az adatkezelőnek egy háromlépcsős tesztet kell végrehajtania, amit érdekmérlegelési tesztnek neveznek. Ez abból áll, hogy az adatkezelő azonosítja a jogos érdekét, majd megállapítja az érintett érdekét, illetve jogalapját, majd súlyozza a két ellenpontot és megállapítja, hogy az eredmény alapján jogosult-e a személyes adatok kezelésére. Dr. Papp Anna Katalin nagyon jó példával szemlélteti a helyzetet: ha online ételrendelés esetén házhozszállítással rendel egy magánszemély, és nem tiltakozik a cég további megkeresése ellen, akkor a szolgáltató jogszerűen küldhet neki ajánlatokat az ételekről, kuponokat, addig, amíg az érintett az adatai kezelése ellen nem tiltakozik.³⁴ Visszatérve a hírközlési portálra, szeretnék kiemelni néhány esetet, amikhez hozzájárul egy személy a süтик elfogadásával. Az egyik a személyre szabott hirdetési profil megalkotása, ebben az esetben a felhasználó tevékenységét, érdeklődési körét, demográfiai adatait és földrajzi elhelyezkedését vizsgálva, valamint, hogy milyen weboldalakat, alkalmazásokat keresett fel létrehoznak egy személyre szabott felhasználói profil, amit reklámozáshoz használnak fel. A szolgáltatókra vonatkozó beállítások fül alatt további süतिकet találhatunk, ahol a jogos érdek szintén hozzájárulás nélkül alapvetően engedélyezve van. Itt már a tárolási idő is fel van tüntetve, ami különböző külföldi marketing cégek (harmadik felek), adattárolási időtartamát határozza meg. Itt a 90 napos határidőtől kezdve 1825 napos határidőig kezelhetik az adatokat. Vannak olyan szolgáltatók is feltüntetve, akik nem használnak cookiekat, vagy más típusú tárhelyet használnak. Nem is gondolná az ember, hogy „Az összes elfogadása” gombra kattintva, mennyi szolgáltatónak engedélyezi az adatai kezelését. A reggeli kávézás közben olvasott hír, a weboldalon töltött idő és tevékenység kész adatvagyon a cégek számára.

³⁴ dr. Papp Anna Katalin – Kinek az érdeke az erősebb? A jogos érdek, mint jogalap a GDPR tükrében (2018, Jogászvilág <https://jogaszvilag.hu/szakma/kinek-az-erdeke-az-erosebb-a-jogos-erdek-mint-jogalap-a-gdpr-tukreben/>) letöltve: 2023.09.03.

11. FIGYELMEZTETŐ JELEK

Ahogy azt már korábban ismertettem, a megszerzett személyes adatok különböző módon kerülhetnek felhasználásra, mint például tranzakciók kezdeményezése, online vásárlások, vagy hitel igénylése. Vannak különböző jelek, amik utalhatnak arra, hogy az illető személyazonosságát felhasználják. Előfordulhat, hogy ha ezt valaki időben realizálja, megakadályozhatja, hogy akár nagyobb anyagi, vagy más jellegű kára keletkezzen. Az egyik ilyen intő jel, ha indokolatlan tranzakciókat kezdeményeztek a bankszámláról. Gyakran az elkövetők kisebb próbavásárlásokkal ellenőrzik egy bankkártya érvényességét. Az ilyen gyanús összegek után egyszerre érdemes felvenni a kapcsolatot a bankkal, vagy tiltani a bankkártyát, amit sok esetben már a netbankban/applikációban is lehetséges. Gyanús jel lehet a letiltott fiók, hiszen a bejelentkezési adatok megszerzését követően a támadó első dolga a jelszó megváltoztatása lesz, hogy ne férjen hozzá a tulajdonos. Abban az esetben, ha szokatlan tevékenységet észlelünk a fiókunkban, vagy értesítést kapunk ismeretlen helyről való bejelentkezésről, azonnal változtassunk jelszót, és ha lehetséges éljünk a „kijelentkezés minden eszközről” funkcióval. Időszakonként az elmentett cookie-kat is érdemes törölni a böngészőnkéből. Az elkövető célja, hogy kizárják az áldozatot a digitális identitásából. Megtörténhet, hogy mobilszolgáltatónál tesznek kísérletet, és a telefonszámot egy másik eszközre irányítják, és kicserélik a SIM-et. Ez jelentős kockázatokkal járhat, hiszen SMS-ben kapott hitelesítő kódokhoz hozzáférhetnek. Ilyen esetben is célszerű felkeresni a bankot, és a mobilszolgáltatót. Magyarországon népszerű támadási forma volt korábbi években a hamis adóvisszatérítésről szóló értesítések. A bűnözők SMS-ben, e-mailen, vagy telefonon keresztül keresték meg a potenciális áldozatokat, hogy a bankkártyaadataikat megszerezzék. A Nemzeti Adó- és Vámhivatal adott is ki figyelmeztetést ezzel kapcsolatban, és felhívta az állampolgárok figyelmét, hogy a NAV-nak bankszámlaszámra, illetve postacímre intézi a visszatérítéseket.³⁵ A személyes adatokkal olyan formában is visszaélhet az elkövető, hogy orvosi ellátást vesz igénybe annak a nevében, akitől a személyazonosságot megszerezte, így az anyagi költségek az áldozatra hárulnak. Ez olyan országokban népszerűbb, ahol a túlnyomórészt magánegészségügyi szolgáltatások állnak rendelkezésre. Ehhez kapcsolódhatnak a különböző adósságok, amikbe az elkövető keveri a személyt, hogy minden anyagi befizetést a személyazonosság tulajdonosára terhel. Így ha valaki, adósságtartozásról kap értesítést, úgy

³⁵ ESET Progress. Protected. – 5 figyelmeztető jel, amely arra utal, hogy személyazonosság-lopás áldozataivá váltunk (<https://www.eset.com/hu/hirek/szemelyazonossag-lopas-jelei-2022/>) letöltve: 2023.09.03.

hogy ő nem tud róla, mindenképp szükséges felvenni a kapcsolatot a szolgáltatóval, illetve a rendőrséggel.

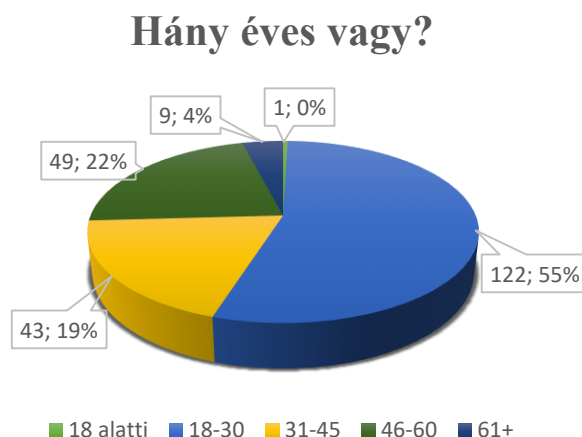
12. HA MÁR MEGTÖRTÉNT A BAJ

Felvetődik a kérdés, hogy ha valaki tapasztalja, hogy visszaéltek a személyes adataival, vagy bármely más előbbiekben ismertetett bűncselekmény áldozata lett mi a teendő. Először is dokumentálni kell mindent, ami történt, és bejelentést tenni a rendőrségnél. A szolgáltatót, rokonokat, közeli hozzátartozókat, illetve a munkatársakat értesíteni, ha az áldozat fiókjával még mindig az elkövető rendelkezik. Több forrásból tiltani a fiókot, amit megszereztek. Közösségi hálózati fiók esetén panaszt szükséges benyújtani az állambiztonsági erőknél és szerveknél (FCSE). Bizonyítékkal a hamis profilról és a visszaélésre vonatkozó információkkal együtt. Feltéve, hogy egy személynek a személyes adatait az engedélye nélkül közzétették a Nemzeti Média- és Hírközlési Hatóság internet hotline nevű portjához ajánlott fordulni.

13. AZ EMBEREK ÉS A BIZTONSÁGTUDATOSSÁG

Kutatásom során készítettem egy kérdőívet, amit az ismeretségi körömben osztottam meg, elsősorban a közösségi média platformokon. Úgy gondolom, hogy minden felhasználó, aki internetezik, potenciális áldozata lehet a kibertérben elkövethető bűncselekményeknek. A felmérésben a kérdéseimet a korábban ismertetett hipotéziseimre alapoztam. A kérdőívre összesen 224 kitöltés érkezett. Abból kiindulva, hogy az adatok megszerzésének leggyakoribb módja ismeretlen hivatkozások, linkek megnyitásából ered, készítettem egy weboldalt, amit a kérdőív végére egy linkkel csatoltam. Kíváncsi voltam, hogy hány személy nyitja meg az oldalt, amihez azt írtam, hogy „A válasz rögzítéséhez kattintson az alábbi linkre”. Természetesen a kitöltők, a hivatkozás megnyitása nélkül is véglegesítették a válaszádat. A weboldalon egy felhívást követően, hogy ez bármilyen link lehetne, ajánlásokat fogalmazok meg az áldozattá válás megelőzése érdekében. A weboldalt a kérdőív elemzésének a végén csatolom.

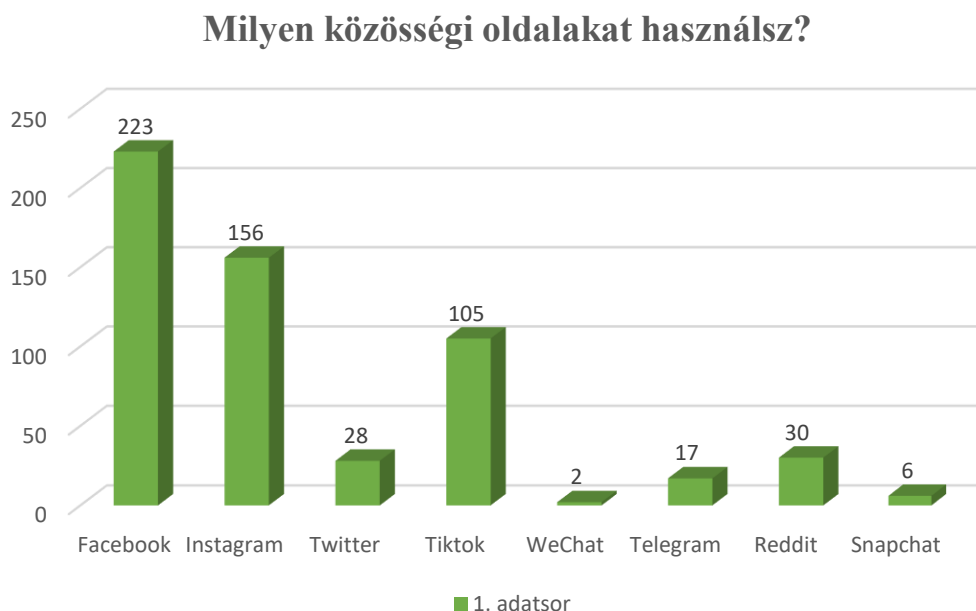
Az első kérdésem a korosztály felmérésére irányult, amit az alábbi módon osztottam fel:



9. ábra Korosztály felmérése (Forrás: saját szerkesztés)

A kitöltők több mint fele, 122 személy 18 és 30 közötti, 43 személy 31 és 45 közötti, 46 és 80 közötti 49 személy, 61 vagy ennél idősebb 9 személy, és 18 év alatti pedig 1 kitöltő.

A következő kérdés arra irányul, hogy ki milyen közösségi platformokat használ. Úgy gondolom, hogy a közösségi oldalakból is rengeteg adat figyelhető meg egy személyről. Például születési adat, párkapcsolat, lakhely, tartózkodási hely, szokások. Ezeket tanulmányozva lehet egy profilt alkotni a személyről, ami megkönnyítheti a személyiségének a felvételét.



10. ábra Milyen közösségi oldalakat preferálnak az emberek? (Forrás: saját szerkesztés)

Egy kitöltőt leszámítva, mindenki használja a Facebookot, 156 személy az Instagramot, és 105 személy a Tiktokot. Véleményem szerint ez a három legnépszerűbb alkalmazás napjainkban,

legalábbis a saját korosztályomban. Természetesen, e platformok használata nem feltétlen jelenti a tartalommegosztást is, hiszen lehet úgy is nézni a közösségi médiát, hogy mi nem osztunk meg semmit, vagy privát a fiókunk, és csak az ismerőseink láthatják. Ennek ellenére, bekerülhet egy-egy nem valós személyt ábrázoló profil az ismerősi körbe, vagy valós személyt ábrázoló, de hamis profil. Többen is használják még a Telegramot, mindössze 17 személy, és a Redditet, 30 személy.

Érdekelt, hogy ki milyen tartalmat oszt meg szívesen a közösségi médiában.

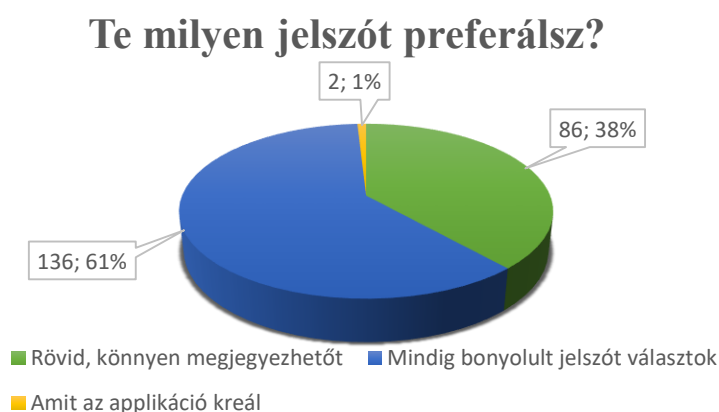


11. ábra Milyen tartalmakat osztanak meg szívesen a válaszadók? (Forrás: saját szerkesztés)

Személy szerint pozitívnak élem meg, hogy 72 személy semmit nem oszt meg magáról a közösségiken. Így biztosan elkerülhető, hogy onnan gyűjtsenek adatokat róluk. A legtöbb jelölés, a szeretteikkel való közös képek megosztására érkezett. Itt gondolhatunk család, barátokra, vagy háziállatokra. Ezekre az információkra már lehet építkezni a bűncselekmények kapcsán. Például, ha rokonnak kiadva kérnek személyes adatokat, vagy szeretett személy testi épségével zsarolva, vagy a korábbi példa alapján, a jelszó feltöréséhez is segítséget nyújthat. 52 válaszadó az élete nagy változásait osztja meg. A válasz mögé példákat is soroltam, mint a házasság, új munkahely, költözés. A munkahely megosztása is kockázatot jelenthet, hiszen munkatársnak is kiadhatja magát az elkövető, vagy utána nézhet a munkahely elérhetőségének és egy hasonló e-mailt kreálva, küldhet levelet a potenciális áldozatnak, aki az eltérést nem észlelve, akár egy egész munkahelyi hálózatot megfertőzhet. Az aktuális programját, hangulátát 41 kitöltő osztja meg. Ebből lehet következtetni a szokásokra, viselkedésre, illetve, hogy mit

szeret, és mit nem szeret az illető. 25 személy posztol olyan tartalmat, ami büszkévé teszi, mint a gyermeke bizonyítványa, nyelvvizsga bizonyítvány. Ezek mind tartalmazznak személyes adatot. Az ismerőseim közül is gyakran látom a bizonyítványokról készített fényképeket, anélkül, hogy a személyes adatok ki lennének takarva. További gyakori elért eredmény a vezetői engedély megszerzése, amit szintén sokan közzétesznek. Következő kategória a hasznos tanácsok, jó receptek, 5 minute crafts videók megosztása, amit 19 személy publikál szívesen. A válaszok között szerepelt még a munkahely reklámozás, vicces tartalmak, különféle programok, programajánlók, mások által megosztott hírek. Volt, aki azt válaszolta, hogy kifejezetten figyel, hogy nyilvánosan semmi személyeset ne tegyen közzé. A 72 személyből, aki azt válaszolta, hogy semmilyen tartalmat nem oszt meg, összesen 10 válaszadó személyes adataival éltek már vissza korábban, vagy gondolja úgy, hogy visszaéltek az adataival. Ez a válaszadók 13,8%-a. Ezzel szemben, kigyűjtöttem azokat a személyeket, akik magukról osztanak meg túlnyomórészt információkat. A 128 személyből, 17 személy érzékeli úgy, hogy vált már személyes adattal visszaélés áldozatává, ami a kitöltők szintén 13,2%-a. Az arányok között minimális eltérés figyelhető meg, amiből úgy gondolom, hogy biztos következtetést nehéz levonni. Ennek ellenére, az eredmények azt bizonyítják, hogy nincs összefüggés aközött, hogy az emberek hamarabb válnak áldozattá amiatt, hogy személyes dolgokat posztolnak a közösségi médiában. Valószínűnek tartom, hogy ez az eredmény annak is köszönhető, hogy viszonylag kevés kitöltőszám érkezett a kérdőívemre. Továbbá lehetséges, hogy azok a személyek, akiknek az adatait felhasználva visszaélést követtek el, más forrásból szerezték meg az adataikat, vagy sokan még nem realizálták, hogy adatszivárgás történt esetükben. Korábban már érzékeltettem, hogy az adatok megszerzését követően a felhasználás akár évek múltával is bekövetkezhet.

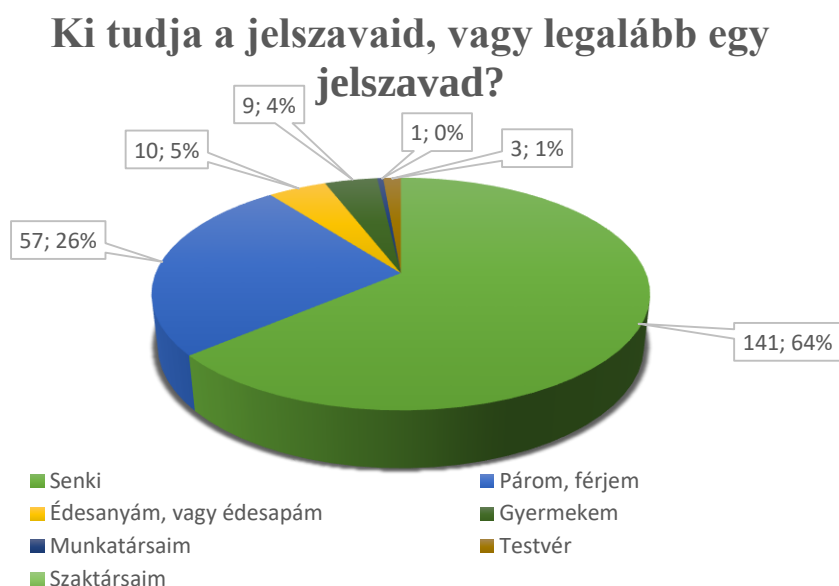
Soron lévő témakör a jelszóválasztást érinti, hogy milyen jelszót preferálnak a felhasználók.



12. ábra A kitöltők milyen jelszót választanak? (Forrás: saját szerkesztés)

Összesen 136 személy, a kitöltők több mint fele válaszolta azt, hogy minden esetben bonyolult jelszót választanak. Ennek ellenére, nagyon sokan, 86 személy dönt a rövid, könnyen megjegyezhető jelszó mellett. 2 személy választja az applikáció által felajánlott jelszót, ezek általában egy bonyolult karaktorsorból állnak, véleményem szerint ez a legbiztonságosabb, viszont ezeket nagyon nehéz lenne megjegyezni, ezért szükséges feljegyezni, ami szintén kockázatot jelenthet.

Ebből adódik a következő kérdés, hogy kik ismerik a felhasználók jelszavait, vagy legalább egy jelszavukat.

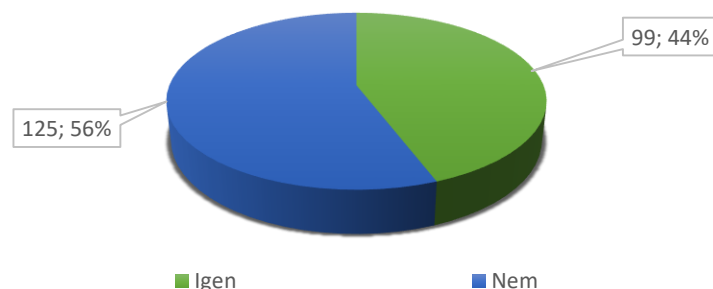


13. ábra Jelszavak megosztása (Forrás: saját szerkesztés)

A kitöltők túlnyomórészt (141 válaszadó) nem osztják meg senkivel sem a jelszavaikat, viszont 37,1% igen. E személyek jelszavát leginkább a családtagok tudják, mint a férj, feleség, gyermekek. Viszont akad olyan személy is, akinek a munkatársai, vagy a szaktársai. Úgy gondolom, családon belül kevés az esélye annak, hogy bárki visszaéljen az adatokkal, viszont ha egy felhasználói fiókba egy családtag megadja például a bankkártya adatokat és onnan szerzi meg az elkövető, abban a szituációban már nem jó, hogy bárki hozzáfért a fiókhoz.

A jelszavak megjegyzése gyakran okozhat problémát, főleg ha különböző jelszavakat használ az ember különféle platformokon, ami ajánlatos. Ilyenkor gyakran csak fogunk egy cetlit a közelben és feljegyezzük a jelszót, azonban ennek is lehetnek kockázatai.

Felírod általában a jelszavad valahova?



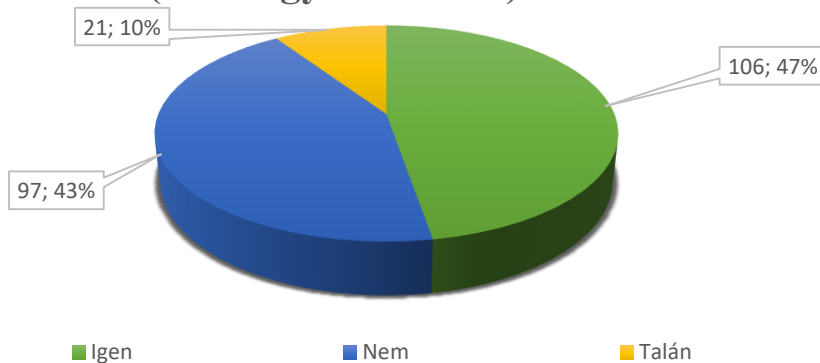
14. ábra Jelszó feljegyzése (Forrás: saját szerkesztés)

A megkérdezettek 55,8%-a nem írja fel sehova sem a jelszavát, hanem memorizálja. Ebből adódóan 44,2% minden esetben felírja. Azok a személyek, akik igennel válaszoltak erre a kérdésre megjelent a következő kérdés, hogy hova írják fel a jelszavukat. A kitöltők 48,5%-a mobiltelefonba jegyzi fel, 39,2% papír alapon tárolja a jelszavát. Különböző helyekre felírva, mint jegyzetömb, füzet, notesz. Van, aki a számítógéphez közel tárolja a papírt, amire fel van jegyezve a jelszó, vagy naptárba írja fel, azonban akad, aki zárható fiókban, vagy egyéb módon otthon elrejtve védi a jelszavát. A telefon rejtett jegyzete is egy opció, amit alkalmaz néhány kitöltő. Létezik olyan is, aki e-mail címben alkotott mappába tárolja őket, vagy számítógépen szöveges dokumentumban, más fájlkiterjesztéssel álcázva. A 99 személyből 6 ember alkalmaz jelszószéfet, vagy kulcstartót.

A kérdőívben arra is kíváncsi voltam, hogy azok a felhasználók, akik kétfaktoros hitelesítést használnak, kevésbé vannak kitéve a személyiséglopás áldozatának. Ebből kifolyólag feltettem a kérdést, hogy használnak-e kétfaktoros hitelesítést. A válaszadók 45,1%-a igen, 27,7%-a ahol csak lehetősége van használ, és 27,7%-a nem használ egyáltalán. Azon személyek közül, akik nem használnak semmilyen többfaktoros autentikációt (61 személyből) 2 személlyel történt már olyan, hogy visszaéltek a személyes adataikkal, és 3 ember válaszolt talánnal. Akik használnak, illetve ahol csak lehet, ott használnak, 163 személy közül 13-an jelezték, hogy történt már velük személyes adatokkal való visszaélés, és 9 személlyel talán. Az arányokat összehasonlítva, akik nem használnak kétfaktoros azonosítást 8%-a élt már át személyes adatokkal történő visszaélést, és akik használnak 13%. Tehát a hipotézisem nem igazolódott be, hogy kevésbé esnek áldozatul, akik használnak. Úgy gondolom ez annak köszönhető, hogy az adatok rengeteg forrásból kikerülhetnek és a megkérdezettek esetében más megelőzési mód lenne az irányadó.

A következő állítás arra vonatkozott, hogy volt-e már rá példa, hogy elküldték valakinek a személyazonosító igazolvány számát, vagy a születési adatokat.

**Történt már veled olyan, hogy elküldted valakinek
a személyigazolvány számodat, születési adataidat?
(akár ügyintézéshez)**

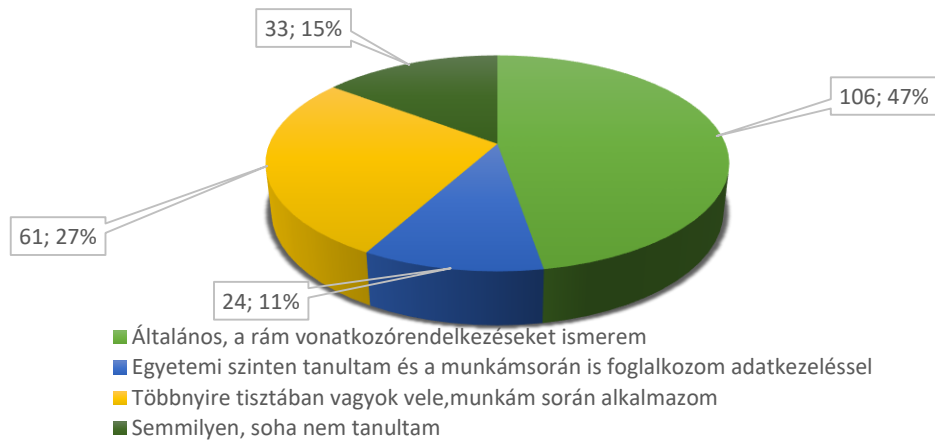


15. ábra Személyes adatok megosztása (Forrás: saját szerkesztés)

A megkérdezettek közül 106 személy, majdnem a kitöltők fele küldte már el a személyes adatait, és 21 személy talánnal válaszolt. 97 személlyel nem fordult még elő ilyen. Úgy gondolom, hogy az emberek sokszor nem is gondolnák, hogy ezzel kockázatot vállalnak, illetve, hogy történhet olyan esemény, amely során más is hozzáfér azokhoz az adatokhoz, nemcsak a célszemély. Igaz, hogy ez az ügyintézés nagyban felgyorsítja, viszont kockázatos.

Fontosnak tartottam megérdeklődni, hogy a kitöltők milyen adatkezelési, adatvédelmi ismeretekkel rendelkeznek, hiszen hipotézisem alapján minél magasabb tudással rendelkezik egy személy ilyen téren, annál kevésbé válik áldozattá.

Milyen adatvédelmi, adatkezelési ismeretekkel rendelkezel?

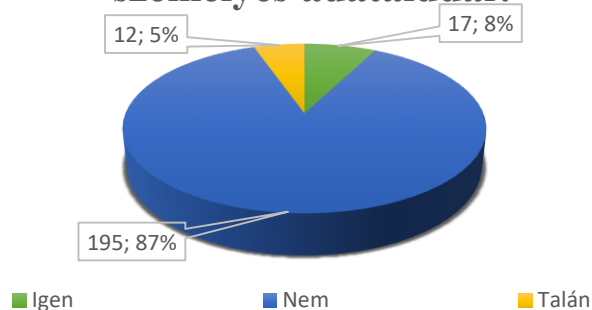


16. ábra Adatvédelmi, adatkezelési ismeretek (Forrás: saját szerkesztés)

A kitöltők 47,3%-a válaszolta, hogy az általános, rá vonatkozó rendelkezésekkel tisztában van, 27,2% többnyire tisztában van vele, a munkája során foglalkozik adatkezeléssel, 14,7% semmilyen ismeretekkel nem rendelkezik soha nem is tanulta, és 10,7% egyetemi szinten tanulta/tanulja és a munkája során is foglalkozik adatkezeléssel. Összehasonlítottam, hogy a háttértudáshoz mérve, milyen mértékben váltak már áldozattá a megkérdezettek. Azon személyek, akik az általános, személyükre vonatkozó rendelkezésekkel tisztában vannak, a 106 személyből 14-en jelölték, hogy éltek már vissza az adataikkal, vagy van rá lehetőség, hogy ez megtörtént. (13%) 61 személy közül, akik többnyire tisztában vannak a rendelkezésekkel, és a munkájuk során is alkalmazzák, 5 személy jelezte a visszaélést. (8%) Egyetemi szintű ismeretanyaggal rendelkező személyek közül a 24 egyénből 3-mal fordult már elő ilyen eset. (12%) 33 személy, akik semmilyen ismeretekkel nem rendelkeznek és soha nem is foglalkoztak vele, 7 személy adataival történt visszaélés. (21%) Az utóbbi kategóriában a többihez képest gyakrabban fordult elő incidens, mint akik tisztában vannak a rendelkezésekkel. Érdekesnek bizonyul, hogy az egyetemi szinten tanult személyek közül is 12% jelzett már hasonló esetet. Véleményem szerint ez abból adódhat, hogy aki egyetemi szinten tanulja, lehet, hogy még nem dolgozik benne, így kevesebb tapasztalattal rendelkeznek, mint azok a személyek, akik már aktívan dolgoznak benne. Tehát a felvetésem, mi alapján minél magasabb tudatossággal rendelkező emberek jobban képesek megvédeni a személyes adataikat és elkerülni a személyiséglopást csak részben teljesült. A magasabb tudatosságot én a végzettséggel hoztam párhuzamba, a személyes tapasztalat helyett.

A felvetéseim igazolására vagy cáfolására feltettem a kérdést, hogy történt-e már a kitöltővel, hogy visszaéltek a személyes adataikkal.

Történt már veled olyan, hogy visszaéltek a személyes adataiddal?

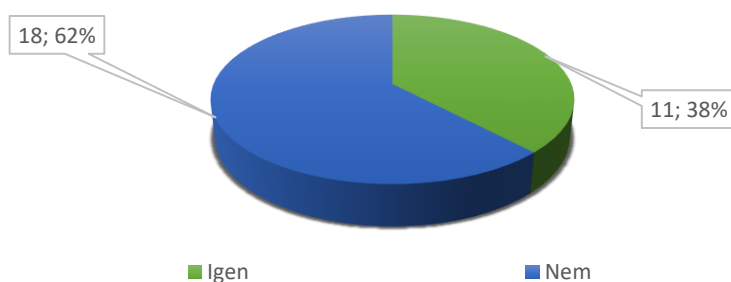


17. ábra Személyes adatokkal visszaélés tapasztalatok (Forrás: saját szerkesztés)

A válaszadók 87%-a azt jelölte, hogy nem történt vele ilyen, viszont 12 személy nem biztos benne, és 17 személynek éltek már vissza a személyes adataival.

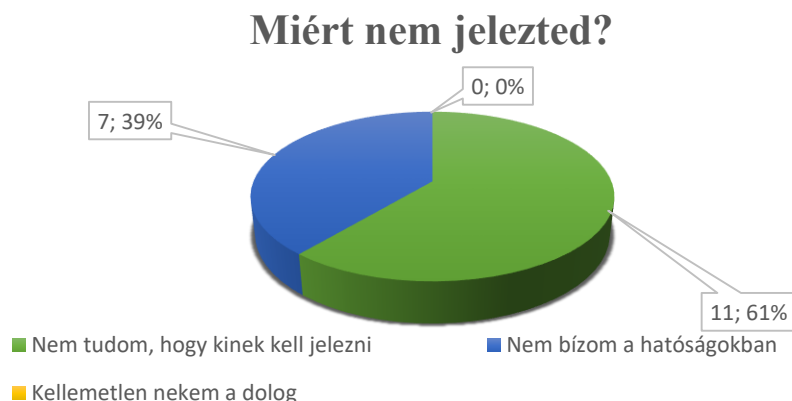
Tapasztalataim alapján a kibertérben előforduló bűncselekmények látenciában maradnak, ebből kifolyólag felmerült bennem a kérdés, hogy jelezték-e az incidenst a hatóságok felé, illetve ha nem, akkor mi az oka annak. Véleményem szerint sokan szégyellik, hogy ilyen eset megtörténhet velük, vagy éppen nem tudják mi a teendő.

Jelezted a hatóságok felé?



18. ábra Jelzés a hatóságok felé (Forrás: saját szerkesztés)

Többen nem jelezték a hatóságok felé, mint ahányan jelezték. Összesen a 29 személyből 18-an nem jelezték és 11-en igen.



19. ábra A nem jelzés indoka (Forrás: saját szerkesztés)

A többség abból az okból nem jelezte, mert nem bízik a hatóságokban. Véleményem szerint, ez adódhat egy-egy negatív tapasztalat miatt vagy ismerősöktől hallott információkból, valamint a sztereotípiákból. Dolgozatom ennek a kérdésnek a vizsgálatára nem terjed ki. 7 személy nem tudja, hogy ebben a szituációban mi a teendő és kinek kell jelezni. A médiában több figyelmet kellene szentelni arra, hogy ilyen jellegű információkról tájékoztassák az embereket, illetve szükséges lenne, hogy az emberekben is kialakuljon az igény arra, hogy utána járjanak, és nem hagyják annyiban az esetet.

A felmérés utolsó témaköre az emberek biztonsági intézkedéseinek felderítésére irányul, hogy használnak-e vírusírtót, illetve mely eszközeiken. A válaszadók 47,8%-a használ, 32,1% csak a számítógépen, vagy laptopon, 17,4% egyáltalán nem használ, és 1,8% egyedül a mobiltelefonján működtet vírusírtót.

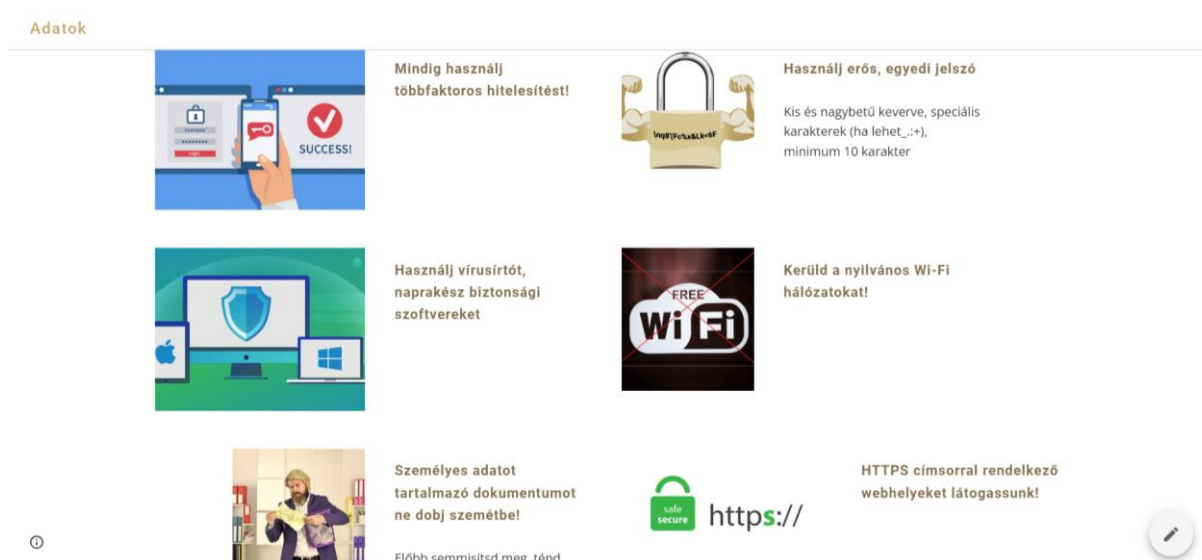
A weboldalak biztonságára vonatkozóan, 117 személy ellenőrzi, hogy a weboldal biztonságos-e, míg 63 személy talán ellenőrzi, és 44 személy egyáltalán nem, vállalva a kockázatot.

A záró kérdésem arra irányult, hogy megnyitják-e a válaszadók az ismeretlen eredetű linkeket. 88,4% válaszolt nemmel, és 8,9% talánnal, valamint 2,7% igennel. Ez azért is érdekes, mert a kérdőívem végére csatolt linket összesen 126 személy nyitotta meg. Természetesen, hozzájárul, hogy segítőszándákkal nyitották meg a hivatkozást, hogy befejezzék a kérdőívet, valamint, hogy ismerős vagyok, aki pont ezzel a témával foglalkozik. Ennek ellenére, ez a megtévesztés lényege, hogy akár egy ismerősnek kiadva is kérhetnek adatokat az elkövetők. A link pedig egy Google Sites-nak kinéző link, amit lehet variálni, hogy milyen módon nézzen ki. Személy szerint egy ingyenes weboldal készítő alkalmaztam, és a linket is eredetben hagytam meg: <https://sites.google.com/view/szemelyiseglopas/f%C5%91oldal>.



20. ábra Weboldal (Forrás: saját szerkesztés)

A weboldalt megnyitva, egy figyelmeztető üzenet áll, hogy ez a link is bármilyen jellegű lehetett volna, és a kitöltő könnyen válhatott volna áldozattá. Lejjebb görgetve pedig megfogalmaztam pár hasznos tanácsot, az áldozattá válás megelőzése érdekében.



21. ábra Weboldal (Forrás: saját szerkesztés)

A korábbi években volt rá példa, hogy a csalók Google Űrlapokon keresztül próbáltak adatokat szerezni a kliensektől. A népszerű szolgáltató űrlapjai azért is jó választás, mert ingyenesen készíthető egy Google fiókkal, könnyedén szerkeszthető, a magas felhasználói számnak köszönhetően a köztudatban megbízhatónak van elkönyvelve, valamint a titkosításának köszönhetően a védekezők nehezen tudják ellenőrizni. Az űrlapokon keresztül kértek az

elkövetők személyes adatokat, illetve a bejelentkezéshez hasonló felületet készítettek a belépési információk megszerzése érdekében.³⁶

14. BANKOK BIZTONSÁGA

A bűnelkövetők elsődleges célja a haszonszerzésre irányul, ami a személyiséglopás keretein belül a banki adatok megszerzésével teljesül. Az információkat saját felhasználásra, vagy továbbadásra is alkalmazhatják. A minőségi kutatási módszer alkalmazásával a Citibank nyomozati vezetőjét, Weissmüller Gábort kértem meg, hogy készítsen velem interjút a témát illetően.

Az első kérdésem arra irányult, hogy a bankok milyen biztonsági intézkedéseket tesznek annak érdekében, hogy az ügyfelek adatai ne kerülhessenek ki?

Gábor elmondása szerint ez egy nagyon komplex rendszer. Elsősorban strukturálisan meg kell különböztetni a papír alapú adattárolást, illetve a digitálisat, mivel máshogy biztosítják a biztonságot. Az adatokhoz való hozzáférést a klasszifikáció alapján szabályozzák. Az archivált adatokra is más kezelési mód vonatkozik, mint azokra, amik használatban vannak. Az alkalmazásban lévőt, hozzáférhetővé kell tenni bizonyos köröknek, akik megfelelő szintű jogosultsággal rendelkeznek. A klasszifikációs csomagoknak külön felelősei vannak, és külön szabályzatok vonatkoznak a kezelésre. Ezek az osztályozási szintek a Citibank esetében bizalmas, szigorúan bizalmas, és nyílt információkból tevődik össze. Az adott személy beazonosítására vonatkozó adatok bizalmasnak minősülnek és nem lehet őket nyílt adatbázisban tárolni. A csomagokon belül is vannak klasszifikációk, hogy azokban milyen adatokat őriznek. Továbbá, áttekintés szükséges, hogy a munkaköröknek megfelelő jogosultságuk és hozzáférésük legyen. A Citibanknál fizikailag is el vannak határolva azok a munkavállalók, akik nyílt adatkezelők, illetve akik klasszifikáltak, és a két épület között nincs átjárás adat és hálózati szinten. Pontos meghatározás szükséges, hogy kinek van betekintése az adattartalmakba. A bank nemzetközi mivoltából adódóan, azt is meg kell határozni, mely adatoknál szükséges, hogy nemzetközi forgalomba legyenek. E bank esetében majdnem minden adat, mivel az olcsóbb struktúra miatt nem minden egy országban összpontosul, hanem a kiszolgáló osztályok (service centerek) más-más földrajzi helyen vannak. Például van Budapesten is. Ebből kiindulva, a magyar adatokat meg kell osztani külföldi várossal, mert

³⁶ Birkás Péter – Így élnek vissza a csalók a Google űrlapokkal (2021, <https://24.hu/tech/2021/10/04/sophos-kutatas-google-urlopok-csalok-kibertamadas-adathalaszat/>) letöltve: 2023.09.10.

lehet, hogy csak ott foglalkoznak olyan könyvelési szinttel, ami elengedhetetlen. Az operációs központok bizonyos feladatokat látnak el, annak érdekében, hogy kiszolgálják a hozzájuk bekötött országokat. Az adat, amint átlépi a határt más adatkezelési jogszabályokat is figyelembe kell venni. A technológiai szempontból értelmezett biztonságot illetően is megkülönböztetjük a papíralapú és digitális kategóriákat. Az első tekintetében elsősorban a fizikai védelemre vonatkozó szabályoknak szükséges megfelelni, hogy ne érhesse tűz, víz stb. amiben az információk megsemmisülhetnek. Egy része ezeknek az archívumoknak kereshető, és a fontosabban digitalizálva is vannak. Ebben az esetben is irányadó a szintek szerinti jogosultság. A digitális adatvédelem már komplexebb és nehezebb kérdéskör. Elektronikus levelezésre tekintettel, egy olyan levél, amiben az ügyfél adatokat ír le klasszifikálnia kell magának a feladónak. A név már ügyféladatnak minősül, ahogy a csatolmány is. A rendszer ezt átvizsgálja, és ha kihágás történne, akkor azt közvetíti a vezetőnek. Az e-mail küldésre jellemző még, hogy csak azonos minősítési szintűnek lehet levelet küldeni, ha magasabb szintű jogosultság kellene, akkor annyi üzenetet kap meg, hogy XY levelet akart küldeni számára. A Citibanknál a belső kommunikáció és az ügyféllel történő interakció is védett. Az országokat átívelő információcsere nyílt hálózaton keresztül történik, viszont ez a folyamat magas szintű enkriptálás keretében valósul meg. A kibervédelmi csapatok 0-tól 24 órában, tehát megállás nélkül figyelik a rendszerek intaktságát, ezen belül a támadásokat, és a próbálkozásokat a rendszer megtörésére. Általában hackerek célja, hogy pénzt szerezzenek abból, hogy bejutnak egy rendszerbe, vagy hírnevet akarnak szerezni belőle. A kiberbiztonsági igazgatóságon belül egy osztály az eseményekkel foglalkozik, míg a másik a fejlesztésekkel. Rendszeresen próbára teszik a saját biztonsági rendszereiket, például etikus hacker felbérelésével tesztelik mennyire megdönthető a rendszer. A Citibank a belső adatkezelésre is jelentős figyelmet fordít. A weboldalukon keresztül biztosítják a kapcsolatot az ügyfelekkel, de reklámfelületeken keresztül is hirdetik magukat, aminek keretében már felajánlanak kitöltendő tartalmakat. Ebben az esetben is biztosítaniuk, hogy az adatok kontamináció nélkül visszajussanak a rendszerükbe. Tehát már itt foglalkoznak az adatok tisztaságával, egy sima reklámkampány berkein belül. Az új termékeknek, okos eszközöknek, számítógépeknek egy átvilágításon kell átesniük, amely a hardver és a szoftver sérülékenységét vizsgálja, hogy használatba kerülhessenek. Amennyiben ez nem megfelelő értéket mutat, nem jön létre az üzletkötés, vagy módosításokat kell végrehajtani annak érdekében.

Interjúalanyom kérdésemre elmondta, hogy ő a bűncselekmények megelőzését sokkal inkább látja a rendszer biztonságossá tételében, mint az ügyfelek tudatosításában. Tapasztalatai alapján

nehéz oktatni az ügyfeleket, ami elől a Citi nem zárkózik el, viszont nem lát benne fejlődést. Véleménye szerint a bombabiztos programok, érintkezési felületek átadása a garancia, hogy elfogadható szintre szorítsák vissza a visszaélések számát. A technológia olyan gyorsan változik, hogy nagyon nehéz vele lépést tartani, tehát mire az ügyfél megérti a szóban forgó technológiát, amivel átverték, arra már száz újabb, másik lesz. Ebből adódóan nagy lett a távolság az ügyfél tudása, illetve a számítógépek tudása között. Úgy gondolja, hogy az átlagembertől alaptól nem várható el, és nem is kell, hogy ilyen magas tudással rendelkezzen, elég, ha a bank olyan programot biztosít, amit nem lehet meghackelni. Ennek hátulütője, hogy egy visszaélés esetén, ha a bank be tudja bizonyítani, hogy az ügyfél gondatlanul járt el a saját személyes adatainak kezelésével a bank nem vállal felelősséget.

Gábor a kérdésemre elmondta, hogy az ügyfélnek úgy kellene kezelni az okos eszközeit, mint a lakását. Belátni, hogy a számítógép, mobiltelefon egy ajtó, amit be kell zárni, hiszen az autót sem hagyjuk sehol lezárás nélkül. A kulcs pedig a különböző programok, amikkel védhetők a készülékeink. Az ingyenes programok sem feltétlen elegendőek, de még rosszabb, ha semmilyen védelmet nem alkalmaznak. A bank a piaci versenyképesség miatt nem teheti meg, hogy ajánl egy programot. Ez a feladat az ügyfélre hárul. Az ő reszortja, hogy megtalálja a számára megfelelőt, szükség esetén szakember bevonásával. Ezzel párhuzamosan a bank több anyagi energiát fordít az ismeretlen jellegű támadások banki oldalról történő megfogására. A technológia fejlődésével a bankok alkalmaznak egy okos rendszert, ami elemzi az ügyfél banki magatartását, hogy milyen kimenő, bejövő pénzforgalma van, a kapcsolatait, mikre költ. Ez abból a szempontból fontos, hogy ha eltérő viselkedést fedeznek fel, akkor felveszik a kapcsolatot az ügyféllel, hogy ő kezdeményezte-e az adott tranzakciót, vagy automatikusan megállítják. Hiszen ritka, ha valaki az összes pénzét elutalja egy nap alatt, viszont, ha házat vásárol, akkor előfordulhat. Ebből fakadóan a bank arra kéri az ügyfeleit, hogy ha külföldre utaznak, vagy egy kiugró összegű tranzakciót terveznek, minden esetben tájékoztassák a bankot. A szolgáltatónak jó modellt kell felállítania, aminek feltétele, hogy naprakész rendszerekkel dolgozzon, és a technológia fejlődést nyomon kövesse. Arra a kérdésemre, hogy a keleti országokkal összekapcsolt tranzakciók gyanúsabbak-e, mint amiket Európán belül indítanak, azt a választ kaptam, hogy már egyre többen utaznak oda üzleti, vagy nyaralás célból, de mégis szokatlanabb, de van rá példa, hogy Dél-Amerikához, vagy Romániához, vagy Ukrajnához köthetők a gyanús pénzmozgások. Sokat számít egy csalás esetén az órabeli különbségek. Ma már fél óra alatt végrehajtanak nemzetközi tranzakción keresztül futó csalásokat, míg régen napokba teltek. Természetesen, ehhez a gyorsasághoz a bankok is

próbálnak felzárkózni, gyanús tranzakció esetében, felveszik a kapcsolatot a célbankkal és a pénzt megállítják. Gyakori probléma, hogy itthon az átlagos munkaidő végén indítanak egy tranzakciót, ami Ázsiába például a munkakezdésre érkezik meg, és már van is lehetősége az elkövetőnek eltűnni a pénzzel, mert mire nálunk megkezdődik az intézkedés ott már másik napszak van. A Citi globális mivoltának köszönhetően, ahogy mennek a napszakok, mindig van egy service center a világon, amelyik működik és tud intézkedni. Például, ha Magyarország 5-kor elengedi az ügyet, Shanghai folytatja.

A bank esetében az adatkezelésre és az üzleti biztonságra vannak kidolgozva folyamatok. Feltéve, hogy a bank rendszerébe bejut a támadó, azt a részt azonnal izolálni kell a többitől, hogy a „fertőzés” ne terjedjen tovább. Ilyenkor a bank az elsődleges intézkedést a rekonstrukcióra helyezi, hogy egy másik hasonló rendszerrel pótolják a megfertőződöttet. A terheléses támadások általában egy helyen, egy országban, egy városban egy rendszert próbálnak túlterhelni, ha ez sikerül, és nem kapcsolják le a hálózatról, akkor dominószerűen próbálják bedönteni a többi rendszert is sorban. Ebben a szituációban, előfordul, hogy leállítják azt a rendszert, lekapcsolják a többiről és kármentesítik. Azonosítják, hogy milyen csatornáktól jön a támadás, megnézik tűntek-e el adatok, és felméri, milyen károk keletkeztek, vagy szükség van-e tisztításra.

Felmerült bennem a kérdés, hogy mikor értesítik az ügyfeleket, támadás esetén. Gábor azt válaszolta, hogy nagyon biztosnak kell lenni abban, hogy az ügyfelek adatait akarták megszerezni, mivel a kár megállítása az elsődleges, aztán a rekonstrukció, majd a nyomozás. A támadás iránya a nyomozási szakaszban derül ki, ami több hónapig is eltarthat. Szükséges egy nyomozati struktúra felállítása, technológiai háttértudás, majd egy hagyományos nyomozáshoz hasonlóan neveket fognak kapni és lesz egy célszemély. Rendkívül fejlett monitorozó programokat használnak akár a helyszínek felderítésére. Csalás esetében, ha kísérleti szakban fogják meg, hogy a pénz még nem hagyta el a bankot sikerrel jártak, ha a tranzakció megvalósult az elkövető járt sikerrel. Vagyonvisszaszerző tevékenységet is végeznek 50%-os sikerességi aránnyal.

A nyomozó hatóságokkal jó kapcsolatot ápolnak, viszont néhány esetben a nyomozók tájékozatlanok azzal kapcsolatban, hogy a bank rendszerei hogyan működnek, milyen adatokat tárolnak, ezért nem tudják a jó kérdéseket feltenni, vagy túl sokat kérdeznek, vagy nem kérdeznek. Természetesen, a bank segítőkész ebben az esetben is.

Feltettem a kérdést, hogy összességében az ügyfeleknek mikre kellene odafigyelniük a saját adataik biztonsága érdekében. A válasz arra irányult, hogy védjék az eszközeiket, kérjenek meg szakembert, ha szükséges, és legyenek tájékozódtak a legújabb csalási trendekkel kapcsolatban. Tartsák tisztán a gépeiket, banki adataikat frissítsék, és csak a bankkal álljanak szóba. Gábor szavaival élve *„legyenek türelmesebbek, ne siessenek a tranzakciók végrehajtásával, hiszen pénzről van szó és a pénzügyi dolgok mindig alapos gondolkodást igényelnek”*.

Számomra rendkívül pozitív élmény volt az interjú, hiszen egy teljesen más nézetből ismerhettem meg a bank biztonságát. Azt gondoltam, hogy a bűncselekmények visszaszorítása az emberek tudatosításában rejlik, viszont interjúalanyomnak teljesen igaza van abban, hogy egy átlagembertől a technikai tudás nem várható el, hanem a banknak a felelőssége, hogy egy teljesen biztonságos rendszert biztosítson. Ennek ellenére, a prevencióhoz az ügyfelek is szükségesek. A tájékozódás egy hatalmas előny a támadásokkal szemben. Személyes tapasztalataim alapján az emberek nem menthetetlenek csak minél több forrásból kell elérni őket, hogy amit látnak, tudatosuljon. Példának okán, már pozitívumnak élem meg, hogy ismerőseim ahelyett, hogy egy e-mailen keresztül kapott linkre kattintanának, kikérik a véleményemet, hogy ez vajon csalás-e. Nem kell nekik feltétlen felismerni, hogy az-e vagy nem, csak kérdezzenek, nézzenek utána, és már megelőzhető a baj.

15. BEFEJEZÉS

A kutatásom eredményeit tekintve, úgy érzem rengeteget tanultam a választott témát illetően. A kutatásom kimenetele többnyire cáfolta a hipotéziseimet, vagy csak részben igazolta. Úgy gondolom, hogy ez annak is köszönhető, hogy akiknek visszaéltek már a személyes adataikkal, sok esetben ők sem tudják, hogy honnan, milyen forrásból szereztek meg az információkat. Emellett, a személyiséglopás, illetve adatszivárgás realizálása akár évek múltán is bekövetkezhet. Természetesen, az is előfordulhat, hogy hazánkban ez mégsem olyan gyakori, mint gondoltam. Ennek ellenére, az információs rendszer felhasználásával elkövetett csalások száma rendkívül gyorsan növekszik, ami inkább a bankkártya adatokkal való visszaéléseket mutatja. Úgy gondolom, hogy mindkét kategória megelőzése rendkívül fontos célt szolgál a mai társadalomban. A jövőben mindenképp szeretném kibővíteni e kutatásomat a csalások vizsgálatára is. Az emberek kibertudatosságra nevelése továbbra is célom. Ebből kifolyólag osztottam meg a kérdőívem végén a weboldalt, amit kibővített formában nyilvánossá teszek. Véleményem szerint, nem szükséges, hogy egy személy informatikus legyen, vagy kiberbiztonsági, kibervédelmi szakember, elég, ha olyan emberi tulajdonság jelen van az életében, amikor leül az okos eszköz elé, mint a kételkedés. Ez természetesen nem a félelmet jelenti, például minden elektronikus levélről, ami érkezik, hanem, hogy megforduljon a fejükbe, hogy mi van ha; mi történhet ha... Ösztönös legyen az, hogy ismeretlen weboldalnak vásárlás előtt utána néz a vásárló, vagy ha online más személytől vásárol, akkor a profilt ellenőrzi, hogy valódi-e, vagy kérdezzenek meg egy ismerőst, aki érthet hozzá. A kérdőívemet megosztottam egy „Internetes csalások” című csoportban, ahol egy személy kételkedett a kérdőív valódiságában, és azt gondolta, hogy „kamu”. Ezt a reakciót teljesen pozitívnak éltem meg, hiszen benne felmerült a gyanú már a kérdőív kapcsán is. Ahogy interjúalanyom is kiemelte, a vírusirtó programoknak is nagy szerepe van a védelemben, hiszen a technológia fejlődésével, már nem feltétlen szükséges kattintás a káros tartalmak megnyitásához, hanem lehetséges, hogy a gép bekapcsolásával, a böngészőprogram betöltésével, egy reklámfelület megfertőzi a rendszert. Ennek köszönhetően gondolom azt, hogy ebben az esetben a kételkedés nem negatív tulajdonság, hanem erény.

16. VONATKOZÓ JOGSZABÁLYOK

4/2007 vélemény a személyes adat fogalmáról

18 U.S. Code § 1028 - Fraud and related activity in connection with identification documents, authentication features, and information

2012. évi C. törvény a Büntető Törvénykönyvről

2/2004. számú BJE határozat

2013. évi V. törvény a Polgári Törvénykönyvről 5.55.§

AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2016. április 27-i (EU) 2016/679 RENDELETE a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről (általános adatvédelmi rendelet)

2001. évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről (Ekertv.)

2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról 187/2015. (VII. 13.) Korm. rendelet; az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról

17. FELHASZNÁLT IRODALOM

Birkás Péter – Így élnek vissza a csalók a Google űrlapokkal (2021, <https://24.hu/tech/2021/10/04/sophos-kutatas-google-urlapok-csalok-kibertamadas-adathalaszat/>)

Dawer Saeed, Razi Iqbal, Hafiz Husnain Raza Sherazi, Usman Ghani Khan: Evaluating Near-Field Communication tag security for identity theft prevention (2019)

Dinah Payne and Pamela A. Kennett-Hensel: Combatting Identity Theft: A Proposed Ethical Policy Statement and Best Practices (Business and Society Review 22:3 393—420, 2017)

Dr. Bátki Pál – Jelentős érdeksérelem jelentése a büntetőjogban (2020. <https://batki.info/jelentos-erdekselem-jelentese-a-buntetojogban/>)

dr. Papp Anna Katalin – Kinek az érdeke az erősebb? A jogos érdek, mint jogalap a GDPR tükrében (2018, Jogászvilág <https://jogaszvilag.hu/szakma/kinek-az-erdeke-az-erosebb-a-jogos-erdek-mint-jogalap-a-gdpr-tukreben/>)

ESET Progress. Protected. – 5 figyelmeztető jel, amely arra utal, hogy személyazonosság-lopás áldozataivá váltunk

ESET Progress. Protected. – Tűzfal (<https://www.eset.com/hu/tuzfal/>)

Európai Bizottság – Mikor kezelhetők személyes adatok? (https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-can-personal-data-be-processed_hu)

Európai Bizottság hivatalos honlapja: Cookie-k használata (https://commission.europa.eu/cookies-policy_hu)

Európai Bizottság válasza – Mit nevezünk személyes adatnak? (https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_hu)

Federal Bureau of Investigation – Internet Crime Report 2022 (Internet Crime Complaint Center, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf)

Georg Borges, Jörg Schwenk, Carl-Friedrich Stuckenberg, Christoph Wegener - Identitätsdiebstahl und Identitätsmissbrauch im Internet - Rechtliche und technische Aspekte (2011, Springer 11. o.)

Gyaraki Réka: A közösségi média hatása a kiberbűncselekmények elkövetésére (Magyar Rendészet 2021/2 67-82.)

Haig Zsolt – Az információs hadviselés kialakulása, katonai értelmezése (HADTUDOMÁNY 21.(1-2.) pp. 12-28. (2011))

Hámori Balázs - Bizalom, jóhírnév és identitás az elektronikus piacokon (Közgazdasági Szemle, LI.évf., 2004. szeptember (832-848.o.)

HOFFMAN-MCGINLEY: Identity theft: A Reference Handbook i. m. 3-5.o

KOOPS, Bert Jaap – LEENES, Ronald et. al.: A typology of identity-related crime. Conceptual, technical and legal issues. In: Information, Communication & Society. 2009/1. 8. o.

Jim Zaiss, Razieh Nokhbeh Zaeem, and K. Suzanne Barber: Identity Threat Assessment and Prediction (The Journal of Consumer Affairs, Spring 2019: 58-70)

Lexiq – Oversharing (<https://lexiq.hu/oversharing>)

MANAP, Nazura Abdul – RAHIM, Anita Abdul – TAJI, Hossein: Cyberspace Identity Theft: The Conceptual Framework. In: Mediterranean Journal of Social Sciences. Vol 6. No. 4. 2015. 600–602. o.

Microsoft – Adathalászati trendek és technikák (<https://learn.microsoft.com/hu-hu/microsoft-365/security/intelligence/phishing-trends?view=o365-worldwide>)

Microsoft – Mi az az adathalászat (<https://www.microsoft.com/hu-hu/security/business/security-101/what-is-phishing>)

Pénzcentrum – Megdöböntően sok jelszó kerül rossz kezekbe: légy résen, így kerülheted el a kellemetlen meglepetést 2023
(<https://www.penzcentrum.hu/tech/20230531/megdobbentoen-sok-jelszo-kerul-rossz-kezekbe-legy-resen-igy-kerulheted-el-a-kellemetlen-meglepetest-1137602>)

Philippa Lawson & John Lawford - IDENTITY THEFT: THE NEED FOR BETTER CONSUMER PROTECTION (Public Interest Advocacy Centre 1204 – ONE Nicholas St. Ottawa, Ontario K1N 7B7, November 2003, With Funding from Industry Canada <https://www.piac.ca/wp-content/uploads/2014/11/idtheft.pdf>)

SAMAH, Joel - Criminal law. Ninth edition. Thomson Wadsworth Publisher, USA, Belmont. 2008. 393.o.

Sorbán, Kinga - Az informatikai bűncselekmények elleni fellépés nemzetközi dimenziói (Themis: 2015/1. 343–375. o.)

Tóth Dávid: Személyiséglopás az interneten. Büntetőjogi szemle, 2020/1. 113-119