Magyar Rendészet 2021/2. 67–82. DOI: 10.32577/mr.2021.2.4

A közösségi média hatása a kiberbűncselekmények elkövetésére

GYARAKI Réka[1]

A közösségi média hatása a bűncselekmények számának elkövetését kedvezőtlenül befolyásolja. Azok a platformok, így az online térben a szórakozásra, ismerkedésre, társkeresésre létrehozott alkalmazások igazi melegágyai azoknak a bűncselekményeknek, amelyeket az online térben, az offline térben vagy ezeket ötvözve követnek el.
A tanulmányban azokat a kiberbűncselekményeket mutatom be, így a csalásokat és az információs rendszer felhasználásával elkövetett csalásokat a felhasználói viselkedések kockázataival összefüggésben, amelyek elkövetéséhez nagymértékben hozzájárulnak a népszerű alkalmazások.

Kulcsszavak: *számítógép, közösségi média, kiberbűnözés, áldozat, csalás, online csalás*

1. Bevezetés

A tanulmány célja az interneten elkövetett csalások mellett annak bemutatása, hogy a személyeknek, pontosabban a felhasználóknak milyen szerepük lehet abban, hogy sértettjei legyenek egy, a kibertérben elkövetett bűncselekménynek.

A kibertérben elkövetett bűncselekmények számát befolyásolja egyrészt az IT-eszközök növekvő száma.[2] Míg 2010-ben a netbook, tablet háztartásonkénti ellátottsága 0,9% volt, addig ez a szám 2019-ben 16,1%-ra nőtt. A laptopok száma esetében ez a szám 16,9%-ról 52,2%-ra nőtt,[3] vagyis egyre több háztartásba jut el az internethasználat lehetősége.

---

[1] Dr. Gyaraki Réka rendőr őrnagy, egyetemi tanársegéd, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Bűnüldözési, Gazdaságvédelmi és Kiberbűnözés Elleni Tanszék; doktori hallgató, Nemzeti Közszolgálati Egyetem Rendészettudományi Doktori Iskola.
Réka Gyaraki Police Major, Assistant Lecturer, University of Public Service Faculty of Law Enforcement, Department of Criminal Investigation, Economy Protection and Cybercrime Prevention; PhD student, University of Public Service Doctoral School of Police Sciences and Law Enforcement.
E-mail: gyaraki.reka@uni-nke.hu, ORCID: https://orcid.org/0000-0002-5733-5974

[2] Nemzeti Média- és Hírközlési Hatóság: *Az elektronikus hírközlési piac fogyasztóinak vizsgálata, 2019 – internetes felmérés.* NMHH, 2020. Online: https://nmhh.hu/cikk/212533/Az_elektronikus_hirkozlesi_piac_fogyasztoinak_vizsgalata_2019__internetes_felmeres

[3] KSH-adatok (a 2020-as számok a tanulmány megírásakor még nem álltak rendelkezésre). KSH: *A háztartások életszínvonala, 2019.* Központi Statisztikai Hivatal.

Az internettel rendelkező háztartások száma egy kutatás szerint *2020. január 1-jén a magyar lakosságot (15–69 évesek között) vizsgálva 87% az, aki legalább havonta egyszer meglátogatja a világhálót. Ez egyes becslések szerint minimum 6 175 500 fő.*[4]

A számok természetesen nem feltétlenül valósak, mivel a kibertérben elkövetett bűncselekmények által okozott károk nem egyértelműen jelennek meg, illetve nem minden deliktumnál mérhetők pénzben. A hatóság tudomására sokszor pedig jóval kevesebb bűncselekmény jut, mivel a sértettek úgy gondolják, hogy a cselekmény nem bűncselekmény, az elkövetési érték elenyésző, vagy nem éri el a szabálysértési értékhatárt, illetve a sértettek szégyellik a sérelmükre elkövetett cselekményt.

A kiberbűncselekmények kutatásában eddig nagyon sokan foglalkoztak az elkövetőkkel, illetve azok személyiségével, valamint a jogellenes cselekménnyel.

A kibertérben sértetteké vált személyekkel kapcsolatban is nem egy kutatás született. A biztonságtudatosság is egyre többször kerül a középpontba, egyre többször lehet tanácsokkal találkozni a televíziós műsorokban, reklámokban, de a közösségi médiának köszönhetően a figyelemfelhívások is egyre gyakrabban megjelennek.

Az alábbiakban bemutatom a kutatásom első részét, a kezdeteket, amit a legegyszerűbben elérhető, megfigyelhető helyen kezdtem meg, a világ legnépszerűbb közösségi oldalán. Ehhez egyrészt a közösségi médiában megtalálható olyan csoportokat, személyeket kerestem meg, akik az interneten keresztül átverés vagy csalás áldozatai lettek, és emiatt megtérült vagy meg nem térült anyagi káruk lett. Ahhoz, hogy a kutatás hipotéziséhez megfelelő képet kapjak, mindenképpen szükség volt arra, hogy az ő online viselkedésüket megismerjem (szubjektív oldal), majd értékeljem, leginkább kiberbiztonsági és bűnüldözési szempontból.

Ugyanakkor kellett egy objektívebb megismerés is. Ehhez segített hozzá a Belügyi Tudományos Tanács által meghirdetett gyakornoki pályázat, amelynek segítségével a Készenléti Rendőrség Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztály munkáját megismerhettem, valamint a nyomozásokba is betekinthettem.

Az alábbi feltevések mentén indultam el: a felhasználók által hagyott digitális nyomokból és az interneten tanúsított viselkedésükből következtetni lehet arra, hogy mekkora eséllyel válnak kiberbűnözők áldozatává (H1), és a kibertérben elkövetett jogellenes cselekmények ugyanazokat az emberi tulajdonságokat használják ki (H2).

A kibertérben elkövetett jogellenes cselekmények vizsgálatakor a sértettekre helyezem a hangsúlyt, leginkább annak feltérképezésére, hogy milyen szerepet játszanak a felhasználók az egyes kiberbűncselekmények során az esetleges áldozattá válásukban, vagy milyen tulajdonságok és a biztonságtudatosság mely részeinek hiánya miatt tehetik ki magukat annak, hogy kiberbűnözők vagy kibertérben ténykedő bűnözők áldozatai legyenek.

Hipotézisem szerint maguk a felhasználók hagyják legtöbbször azokat a digitális nyomokat, elektronikus adatokat, amelyek miatt sértettekké válhatnak a kibertérben,

[4] Internetezők számának alakulása hazánkban. Klenovszki János: *Nőtt az internetpenetráció, már 6 175 500 fő internetezik hazánkban.* NRC, 2020.

vagy azzal összefüggésben az offline világban is, így a biztonságtudatosságnál az ember felhasználói viselkedéselemzésére kell a hangsúlyt fektetni, és nem általánosságban felhívni a figyelmet az internet veszélyeire. A kibertérben tanúsított viselkedés összefüggésben állhat azzal, hogy a felhasználó kiberbűncselekmény áldozatává váljon.

A kiberbűncselekmények a kezdetektől fogva fejlődést mutatnak mind az elkövetők személyében, módszerében, mind pedig a sértettek típusának tekintetében is. Újabb és újabb elkövetési módszerek jelennek meg az internet segítségével, amihez a közösségi média, az online piacterek, a webáruházak, társkereső oldalak stb. elterjedése, népszerűsége hozzájárul.

Az eddig a fizikai térben történő aktivitásunkat, mint a vásárlás, ügyintézés, csekkbefizetések, ismerkedések felváltották az elektronikus kereskedelem nyújtotta kényelmi szolgáltáltatások, a sorban állás helyett az elektronikus ügyintézés előtérbe helyezése.

A felhasználói biztonságtudatosságra jellemző mérték azt mondja meg, hogy egy adott felhasználó esetén, ha egy bizonyos szituációba kerül, milyen valószínűséggel hoz olyan döntést vagy végez olyan tevékenységet, amely a veszély okozta esemény bekövetkezését eredményezi. A másik jellemző tulajdonság arra utal, hogy egy adott felhasználó milyen gyakran kerül olyan szituációba, hogy döntést kelljen hoznia.[5]

A következőkben a kutatásom első lépését mutatom be:

Első körben mindenképpen olyan bűncselekményt választottam, amelyben a sértettek és a tevékenységük jól megfigyelhető, és valószínűsíthető, hogy az online és offline térben történő cselekménye eltérő. Ezért a kutatás során két bűncselekményt vizsgálok, az egyik, amikor a sértettek felhasználóként történő viselkedése a kibertérnek köszönhetően mást fog mutatni, mint a fizikai térben. Ezért esett a választásom az internetes csalásra és az információs rendszer felhasználásával elkövetett csalásra.

Ezen két bűncselekmény esetében vizsgálható a sértettek által megosztott vagy gyakran látogatott internetes tartalom, az infokommunikációs eszközök és az emberi biztonságtudatosság összefüggése, valamint a tudatosság nem léte vagy legalábbis hiánya.

Az áldozatokat a pszichológiában is ismert Big Five modell egyes elemei,[6] valamint a biztonságtudatosság[7] követelményeinek alapján kísérlem meg kategóriákba sorolni. Ez fogja megadni azokat a pontokat, amelyek az egyes kiberbűncselekmény-típusoknak (lásd részletesebben a 3.1. pontnál) meg fogja majd adni a kockázatát.

Az általam kiemelt emberi magatartások és tulajdonságok:

- vizualitás;
- bizalom (becsületesség és jószándék);
- nárcizmus;
- szociábilitás/közösséghez tartozás;

---

[5] Leitold Ferenc: A felhasználói viselkedés, mint információbiztonsági kockázat becslése. In *Networkshop 2019.* Budapest, Hungarnet Egyesület, 2019. 189–197.

[6] Steve G. A. van de Weijer – E. Rutger Leukfeldt: Big five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking,* 20. (2017), 7. 407–412.

[7] Neumann János Számítógép-tudományi Társaság: *IT biztonság közérthetően – Első a (kiber)biztonság!* 2019.

- megfelelni akarás;
- hanyagság, figyelmetlenség;
- magány;
- tudatlanság, tudatosság hiánya;
- külső vagy belső kontroll (felügyelet) hiánya.

Ezeket 0-tól 6-ig a bűncselekményeknél, illetve kibertámadásoknál pontozom. A 0 érték kerül azokhoz a kiberbűncselekményekhez vagy támadásokhoz, amelyeknél a felsorolt tulajdonságok vagy magatartások nem értelmezhetők.

2. A kutatás során alkalmazott módszerek

A UCL *(University College London)* Cyber-munkacsoportja 2010 végén publikált egy jelentést, amelyben a közösségi média szerepét határozták meg a tudományos tevékenység különböző fázisaiban.[8] Ennek a jelentésnek a tartalma megfelelően illeszkedik a kutatásom céljához. A csoport az alábbi részterületeket definiálta a közösségi médiában történő kutatáshoz:

- a kutatási lehetőségek feltérképezése;
- partnerek kezelése;
- pénzügyi támogatás megszerzése;
- szakirodalom áttekintése;
- kutatási adatok gyűjtése;
- az eredmények terjesztése;
- a kutatási folyamat menedzselése.

A kutatás eredményességéhez interjúk és statisztikai adatok elemzése, valamint a közösségi médiában történő megfigyelés útján tapasztaltak járultak hozzá.

Az interjúalanyokat olyan személyek közül választottam ki, akik valamilyen internetes bűncselekmény – többnyire csalás vagy adathalászat – áldozatává váltak. Bár a kutatás még nem fejeződött be, az eddig adott válaszok alapján a megkérdezettek közül 5% volt, akinek a felállított szempontok alapján a kibertérben tanúsított magatartása az átlagos feletti szintet elérte (legalább 3-as értékelést kapott). A megkérdezettek 95%-a viszont sem az általa használt IT-eszközöket, sem a felhasználói viselkedését, sem a biztonsági beállításokat nem az elvárható, minimumkövetelményeknek megfelelően állította be.

Az interjúk során az adott válaszokat egy kockázati skála szerint pontozom 1-től 5-ig terjedő skálán, figyelembe véve az interjúalanyok saját elmondását, valamint a saját észlelést is.

[8] UCL Report: https://search2.ucl.ac.uk/s/search.html?query=2010+social+media&collection=website-meta&profile=_website&tab=websites&submit=Go

De ahogy hangsúlyoztam, a kutatás még jelenleg is folyamatban van, így ezek csak az elsődleges eredmények.

Az egyik legnépszerűbb és legnagyobb létszámú közösségi oldalon, a Facebookon, több károsultakat összefogó oldalakra, csoportokba regisztráltam. Leginkább megfigyeléseket végeztem, természetesen amellett, hogy önkéntes alapon kerestem az interjúalanyokat.

A csoportok, bár a károsultakat hivatottak összefogni, kérve, hogy osszák meg tapasztalataikat, történeteiket, sok érdeklődőt is vonzanak. A tagok néhány esetben már saját lehetőségeiket túllépve nyomozásba kezdtek, kiderítve az elkövető tényleges személyazonosságát, lakcímét, munkahelyét és kapcsolatait, akár saját hatáskörben írtak az elkövetőknek vagy támadták a sértettet.

A kutatásom szempontjából nem releváns, de mégis erősen megfigyelhető a cyberbullying jelensége,[9] azaz az internetes zaklatásé, amely korábban a fiatalkorúakra volt jellemző. Ma már azonban azon korosztálynál is megfigyelhető, akik érettebb személyiséggel rendelkeznek, hogy nemcsak nézelődők maradnak ezeken az oldalakon, hanem ítélkeznek és gúnyolódnak másokon, így megjelenik az áldozathibáztatás is, ami akár visszatartó erő is lehet abban, hogy a deliktumok a megfelelő hatóság – rendőrség, Nemzeti Kibervédelmi Intézet – tudomására jussanak.

3. A közösségi média és a kiberbűncselekmények

A közösségi média fogalmát Andreas Kaplan és Michael Haenlein az alábbiakban definiálta: „Az internetes alkalmazások olyan csoportja, amely a web 2.0 ideológiai és technológiai alapjaira épül és ami elősegíti, hogy kialakuljon és átalakuljon a felhasználó által létrehozott tartalom."

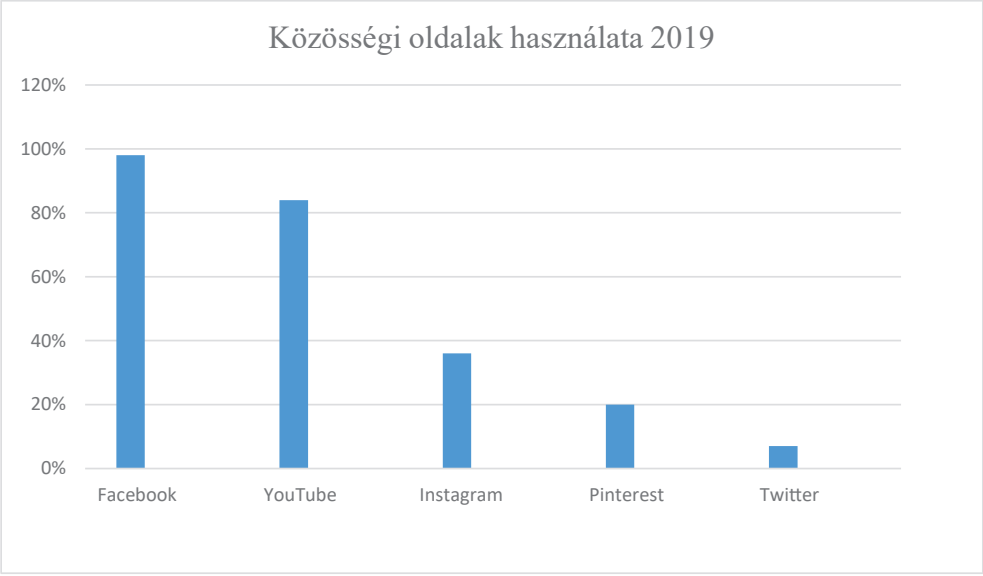
Az alábbi ábra rangsorolja és százalékos elosztásban mutatja a 2019-ben legnépszerűbb közösségi oldalakat, a magyar lakosság körében.[10]

Az egyik legnépszerűbb közösségi oldal a Facebook, amely aktív felhasználóinak száma ma már meghaladja a 2 milliárd főt, és korosztályos elosztását tekintve valamennyiben nagy népszerűségnek örvend.

Az egyik népszerűségét már nemcsak az adja, hogy a rég nem látott vagy távoli ismerősöket megtalálhatjuk rajta, hanem olyan felhasználókkal is találkozhatunk, akiknek hasonló érdeklődési köre van, váratlan élethelyzetben képes tanácsot adni, stb.

[9] Zsila Ágnes – Demetrovics Zsolt: Cyber-viktimizáció és cyber-agresszió. *Médiakutató,* 19. (2018), 1. 21–33.

[10] Az azért szükségesnek érzem hangsúlyozni, hogy az általam megkérdezett alanyok közül csak minden negyedik ismerte ezt a szót, hogy közösségi média vagy social media, esetleg közösségi háló.



1. ábra: NMHH: Az elektronikus hírközlési piac fogyasztóinak vizsgálata. Forrás: Az elektronikus hírközlési piac fogyasztóinak vizsgálata, 2019 – internetes felmérés. NMHH, 2020.

A közösségi média megjelenése óta többször volt támadások kereszttüzében. Az eredeti célja, miszerint az ismerősöket bejelölve, társasági oldalként működik, elveszítette. Mára sokkal inkább egy olyan internetes oldallá vált, amely az anonimitás, a felhasználók szabad véleménynyilvánításának ad teret, ahol az agresszió és a segítségkérés jól megférnek egymás mellett. Az egyes felhasználók politikai, vallási, ideológiai nézeteikhez társakat, közösséget, csoportot találnak.

Szembe menve Bányász Péter megállapításával, miszerint széles skálán mozog a felhasználók adatvédelmi és információbiztonsági tudatossága,[11] a kutatás rámutatott arra, hogy nem a széles skálán történő mozgás az elsődleges probléma, hanem sok esetben az egymásra épülő információbiztonsági ajánlások nem számolnak az érzelem és a vizualitás kihívásaival.

Visszatérve az 1. pontba írt észrevételeimhez, nem elutasítva és nem is teljes mértékben támogatva a közösségi média adta lehetőséget, a kutatásomhoz az egyik legjobb terepnek bizonyult.

[11] Bányász Péter: Social engineering and social media. *Nemzetbiztonsági Szemle,* 6. (2018), 1. 62.

3.1. Kiberbűncselekmények

Az új technológiák a bűnözés új lehetőségeit teremtették meg, ugyanakkor viszonylag kevés új típusú bűncselekményt hoztak létre, sokkal inkább az addigi deliktumokat helyezték át a kibertérbe, vagy a kibertér, számítógép segítségével, új módszerekkel követik el az eddigi hagyományos bűncselekményeket.

Mi különbözteti meg a számítógépes bűnözéseket a hagyományos bűncselekményektől? Nyilvánvaló, hogy az egyik különbség a számítógép és az IT-eszközök használata és terjedése, de a technológia önmagában nem elegendő a bűncselekmények különböző területei közötti differenciák megkülönböztetéséhez. Korábban a bűnözőknek nem volt szükségük számítógépre vagy kibertérre például a csalás elkövetéséhez, a gyermekpornográfia és a szellemi tulajdon forgalmazásához, a személyazonosság ellopásához, vagy a magánélet megsértését is el tudták követni. Mindezen tevékenységek léteztek már azt megelőzően is, mielőtt a 4. ipari forradalom berobbant volna. A Britannica enciklopédia meghatározása szerint, a kiberbűnözés vagy számítástechnikai bűnözés, különös tekintettel az internetre, a jelenlegi bűnözői magatartás kiterjesztését jelenti néhány új, illegális tevékenység mellett.

A kiberbűncselekmények alábbi két típusba sorolását alkalmaztam a kutatás során:[12]

A kiber(tér)függő bűncselekmények *(cyber-dependent crime)* McGuire és Dowling tanulmánya szerint azok a „tiszta" kiberbűncselekmények, „amelyeket csak számítógép, számítógépes hálózatok vagy más információs kommunikációs technológia (IKT) segítségével lehet elkövetni". A „cyber-dependent crime" magában foglalja a hackinget, a vírusok és a rosszindulatú programok terjesztését, illetve a DDoS támadásokat.[13]

A kiber(tér) által támogatott bűncselekmények *(cyber-enabled crime)* azok a „hagyományos bűncselekmények", amelyek nagyságát vagy elérhetőségét növelhetik számítógépek, számítógépes hálózatok vagy más információs kommunikációs technológiák (ICT) felhasználásával. Ilyen típusú bűncselekmények a pénzügyi csalások, az adathalászat (phising), a pharming, amely az adathalászathoz hasonló, adatok megszerzésére irányuló bűncselekmény és a zsarolás.[14]

A kettős felosztáshoz igazodva a jellemző kiberbűncselekményeket besoroltam – természetesen felhasználva a külföldi szakirodalomban is megjelölt altípusokat.

---

[12] A kiberbűncselekmények felosztására rengeteg rendszer született, de a kutatáshoz ezt az elosztást használom, ez alapján sorolom be a Btk. egyes bűncselekményeit.

[13] Mike McGuire – Samantha Dowling: *Cyber crime: A review of the evidence. Research Report 75, Chapter 1: Cyber- dependent crimes.* Home Office, 2013.

[14] CPS: *Cybercrime-prosecution guidance.* The Crown" Prosecution Service (CPS), Tech. Rep, 2019.

4. A csalás színtere a 4. ipari forradalom korában

Az internet megjelenésével a kibertér vált a csalás elkövetésének új helyszínévé, köszönhetően annak is, hogy a felhasználók száma folyamatosan nő, az információs rendszerek pedig egyre inkább kielégíteni igyekeznek a rohanó és fejlődő világunkat. A vásárlást megkönnyítendő az elérhető hirdetési oldalak bárhol és bármikor hozzáférhetők, nem beszélve a közösségi médiában jelen lévő marketplace-ekről, a hirdetési és licitálási csoportokról, ahol a lakó- vagy munkahelyünknek megfelelő vagy földrajzilag közel lévő adásvételi csoportokba regisztrálnak a felhasználók.

Erős eltérés mutatkozik a valós (fizikai) térben és a kibertérben történő bűncselekmények között az elkövetés módszere tekintetében. Amíg az olyan helyek esetében, mint a bevásárló- és szórakozóhelyek az elkövető (tettes) és az áldozat valószínűleg személyesen találkoznak, mivel nagyszámú ember látogat bizonyos helyeket, például bevásárlóközpontokat, ahol a bűnözők könnyen megtalálhatják a potenciális áldozataikat, ezáltal nagyobb eséllyel válik valaki bűncselekmény áldozatává, vagy éri bármilyen atrocitás, mint a kevésbé látogatott, kevesebb embert vonzó helyszíneken. Így a felismerés, a személyes kontakt vagy a videókamerák működése miatt nagyobb az esélye a felderítésnek, ám a kibertérben történő elkövetés esetében ritkán vagy egyáltalán nem találkozik az elkövető és áldozat, hiszen az egymás közötti adásvétel, segítségnyújtás a virtuális piacon történik.

Amíg a fizikai térben a potenciális áldozatkiválasztásnál nagymértékben hozzájárul a tömegen kívül a felelőtlen viselkedés (pénztárca jól látható és felügyelet nélkül történő elhelyezése), a nagy tömegben figyelemelvonásra alkalmas tevékenység stb., addig a virtuális térben a felelőtlen viselkedés teljesen mást takar, hiszen még a legnagyobb körültekintés mellett is előfordulhat, hogy bűnöző áldozatává válik valaki.

Számos oka lehet annak, hogy miért követnek el bűnözők a kibertérrel összefüggő bűncselekményeket:

- gyors pénzszerzés reményében;
- az online tevékenységüknek alacsony a határköltsége a globális hozzáférés miatt;
- a bűnüldöző szervek általi felderítés sokszor kevésbé hatékony és sok esetben költségesebb is;
- a hivatalos nyomozás és a büntetőeljárás lefolytatása lassabb és ritkább a közös nemzetközi együttműködés és jogszabályi közelítés;
- nehéz azonosítani az elkövetők személyét és a tartózkodási helyüket;
- a nemzetközi kereskedelem és kapcsolattartás egyre elterjedtebb, ennek következtében az elkövetés is könnyen megtörténhet;
- a bűncselekmény sokszor vagy legalábbis hosszú ideig látenciában marad.

A felsoroltakon kívül még számos okot lehetne megadni, így országonként a társadalmi, szociális és oktatási, (biztonság) tudatosítási eltéréseket, ahogy a technika, technológia fejlődését, a gazdasági fejlettséget stb., ami megkönnyíti az áldozattá válást.

Az e-mail megjelenése előtt a csalóknak minden lehetséges áldozattal külön-külön kellett kapcsolatba lépniük postai úton, faxon, telefonon vagy közvetlen, személyes kapcsolaton keresztül. E módszerek esetében azonkívül, hogy sokszor fölösleges pénz- és energiabefektetést igényeltek, nehezebb is volt az áldozat kiválasztása.

Az online tér kínálta lehetőségek megkönnyítették, hogy a csalásra fogékony áldozatokkal való kapcsolatfelvétel esélyei javuljanak, aminek érdekében a csaló előzetesen kutatást tud végezni az általa megcélozott jellemzőkről a különböző közösségi médiumok, online csoportok vagy társkereső oldalak segítségével.[15]

4.1. Megtévesztések informatikai környezetben

A megtévesztések vagy csalás jellegű számítógépes bűncselekmények felosztását a szakirodalom az alábbi két csoportba sorolja:

Az első csoportba tartoznak azok, ahol ténylegesen észlelhető a pénzügyi károkozás. Az elkövető motivációja a pénzszerzés az információszerzéssel szemben. (*Money Seeking Frauds* – például nigériai levelek, hamis termékek, nyereményre irányuló levelek stb.)

A második csoportban a jogellenes cselekmény a személyes adatok megszerzésére irányul, ami mellett a támadó célja lehet a pénzszerzés. Az így megszerzett személyes adatok felhasználásával követnek el bűncselekményt, (*Personal Information Seeking Frauds* – malware, hamis weboldalak és e-mailek stb.).[16]

Zárójelben megemlítve beszélhetünk még egy harmadik csoportról is, ami már nem annyira a klasszikus csalás jegyeit hordozza magán, mégis a nemzetközi szakirodalmat tekintve csalásként *(fraud)* definiálják. Ehhez azok a jogellenes cselekmények tartoznak, amelyek – hasonlóan a második esethez – szintén személyes adatok megszerzésére irányulnak, de nem feltétlenül pénzszerzés vagy anyagi károkozás a cél. Az elkövető kizárólag a sértett személyes adatait (például a fényképét, nevét) szerzi meg és él vele vissza (például személyiséglopás) közösségi vagy úgynevezett „randizós" oldalakon történő ismerkedés céljából, aminek motivációja leginkább szexuális visszaélés. Bár a magyar büntetőjog a csalások egyes típusainál nem tesz különbséget, mégis a külföldi szakirodalomban ezek más és más elnevezéssel jelennek meg, és annak ellenére, hogy mindegyiknél teljesül a törvényi tényállás: „aki jogtalan haszonszerzés végett mást tévedésben ejt, vagy tévedésben tart", csalást követ el, mégis az áldozatok és az átverések módszere eltérő.

Bár valamennyi online csalás elkövetése során a klasszikus csalási tényállási elemek megvalósulnak, mégis áldozati oldalról vizsgálva a tényeket éles ellentéteket mutat az elkövetési magatartások, míg az elkövetők sokszor a fent említett típusokat kombinálva követik el a bűncselekményüket.

---

[15] CISA: *Recognizing and Avoiding Email Scams.* Cybersecurity & Infrastructure Security Agency.

[16] Roderick S. Graham – Shawn K. Smith: *Cybercrime and digital deviance.* New York, Routledge, 2019. 92–93.

5. A pénzszerzések illegális módja a kibertérben

A csalások kibertérben történő elterjedésének és hihetetlen fejlődésének magyarázata jobbára az e-kereskedelem népszerűségéhez köthető. A közösségi médiában is megtalálható marketplace-en (internetes piactéren) olyan termékeket hirdetnek meg cégek, termelők, kézművesek, magánszemélyek kedvezőnek tűnő áron, amelyek népszerűek vagy nehezen hozzáférhetők.

A legjobban mutatja a kibertérben lévő gazdasági bűncselekmények súlyosságát az Amerikai Egyesült Államokban működő *Internet Crime Complaint Centre* (IC3), amely 2017-ben több mint 301 ezer panaszt vizsgált különböző számítógépes bűncselekményekkel és gyermekpornográfiával kapcsolatban.[17]

A kibertérben történő gazdasági és kereskedelmi műveletek jellemzői szorosan összefüggnek a számítógépes bűncselekmények jellemzőivel is, mint az anonimitás, a nemzetközi jelleg és a gyorsaság, amelyek a legális és az illegális tevékenységek folytatásánál ugyanolyan fontos szempontok.

Az internet az egyik leggyorsabb eszköze többek között a kommunikációnak, az információmegosztásoknak és -továbbításoknak, az elektronikus ügyintézésnek vagy az elektronikus kereskedelemnek, amely történhet mind úgynevezett webboltokban vagy a piactéren, ahol egymás között zajlik a legális és akár illegális termékek, szolgáltatások kereskedelme. Az emberek közötti ismerkedés is egyre gyakrabban kezdődik az online térben, felhasználva a közösségi oldalak adta lehetőségeket, amelyek társas, üzleti (kereskedelmi), vallási vagy egyéb csoporthoz tartozás, mint például valami vagy valaki iránti rajongás, vagy épp ellenszenv miatt jöttek létre.

Szabó Máté megállapítása szerint „egy egyén sorsát egyre inkább az határozza meg, hogy mit árul el róla a személyiségprofilja, mit tartanak róla nyilván, és nem a fizikai valóság, amellyel a személyiségprofil sok esetben nem egyezik”.[18]

A McAffee kiberbiztonsággal foglalkozó vállalatnak a közelmúltban megjelent *A kiberbűnözés gazdasági hatása* című jelentésének egyik legjelentősebb aspektusa szerint a számítógépes kémkedés, a szellemi tulajdon (IP) számítógépes lopása és az üzleti adatok bizalmas jellegének hangsúlyozása jelenti az egyik legkardinálisabb problémát. A Stratégiai és Nemzetközi Tanulmányok Központjának (CSIS) és a McAfee jelentése szerint a kiberbűnözés a globális gazdaságnak évente 600 milliárd dollárba kerül, vagyis a globális GDP 0,8%-ába, és az internetes kémkedés a károk 25%-át teszi ki, ami több, mint a számítógépes bűnözés bármely más kategóriája. Ezenkívül a jelentés azt állítja, hogy „az internetkapcsolat hatalmas teret nyitott a számítógépes bűnözéshez, és az IP-lopások jóval meghaladják a kormányok érdeklődésének hagyományos területeit, például a katonai technológiákat”.

---

[17] Majid Yar – Kevin F Steinmetz: *Cybercrime and society.* 3rd Edition, Sage, 2019.

[18] Szabó Máté: *Az információs hatalom alkotmányos korlátai.* Doktori értekezés. Budapest, Eötvös Loránd Tudományegyetem, 2011.

5.1. Romantikus csalások[19]

A romantikuslevél-csalások a nigériai csalásokhoz hasonlóak. E-mailben vagy a közösségi oldalakon többnyire egyedülálló személyekkel a csaló felveszi a kapcsolatot. A csalók többnyire olyan személyként mutatkoznak be, aki felé egyébként is megvan az emberek bizalma, köztudottan magas fizetése van: így orvos, katona vagy egy olajfúró tornyon dolgozó személy, aki először óvatosan közelítve, majd később egyre jobban biztosítva áldozatát az érzelmeiről, esetleg házasság ígéretével kecsegtetve, pénzt kér. Többnyire kis összeget először, majd ezt követően a hazautazásra, egészségügyi költségek kifizetésére, vízumért vagy más hivatalos okmányért felszámolt díj megfizetése miatt egyre több és több összeget kér. A teljesített kifizetések után pedig a közösségi oldalán a profilját megszünteti, vagy megváltoztatja a nevét, és folytatja tovább a pénzszerzést. Az áldozatok leginkább heteroszexuális, idősebb nők, de ugyanúgy megtalálják a homoszexuális férfiakat és nőket is az elkövetők.[20]

A közösségi médiának köszönhetően több interjút készítettem olyan áldozatokkal, akik romantikus csalók áldozatai lettek.

Az áldozatok 93%-ban nők, akik közül 76% idősebb vagy korosodó felhasználó, akiket az elkövetők megkárosítottak.

Az elkövetők valamennyien orvosnak, mérnöknek, katonának adták ki magukat, akik valamelyik nemzetközi szervezet megbízásából idegen országban dolgoznak. Ezekkel a történetekkel, valamint a megnyerő (lopott) fényképükkel és a folyamatos érdeklődésükkel nagyon gyorsan beférkőztek az áldozataik bizalmába.

Az egyik áldozat úgy fogalmazott: „olyan volt, amilyennek látni akartam, azt mondta, amit hallani akartam".

Az elkövetők nagyon gyorsan a sértettek bizalmába férkőztek, ahol beteg gyerekükre vagy ki nem fizetett munkabérükre hivatkozva magas összegeket kértek. Ezeket az összegeket részben bitcoinban vagy Western Unionon keresztül, esetleg az áldozatok saját bankszámláján keresztül, fizették ki, sok esetben több alkalommal is, nem egy esetben több tízmillió forintot utaltak át a csalóknak.

5.2. A C2C csalások és a B2C

A C2C *(Customer to Customer)* az interneten terjedő csalások olyan formája, amely a fogyasztók közötti kereskedelem elnevezése és amelyben a fogyasztó a fogyasztóval áll üzleti, kereskedelmi kapcsolatban, például a second hand oldalakon, vásárok

[19] Symantec: *BEC scams remain a billion-dollar enterprise, targeting 6K businesses monthly.* 2019. Online: www.symantec.com/blogs/threat-intelligence/bec-scams-trends-and-themes-2019

[20] Monica Whitty – Tom Buchanan: The online romance scam: A serious cybercrime. *Cyberpsychology, Behavior and Social Networking,* 15. (2012), 3. 181–183.

hirdetésével, egyéni eladásokkal.[21] A fogyasztó és fogyasztó közötti kereskedelmi kapcsolat helyszínei sokszor szintén a közösségi oldalak, ahol a megunt, kinőtt termékek, cikkek kereskedelme sokkal gyorsabban történhet meg, mint a már eddig is ismert népszerű oldalakon, hiszen sok esetben egy adott márkára, termékre, célcsoportra specializálódva hoznak létre zárt vagy nyílt adásvételi csoportokat. Bár sokszor a csoportok adminisztrátorai, az oldal kezelői a csalók kiszűrésére különböző feltételeket szabnak az abba való belépésre, de leginkább visszajelzésekből, kommentekből, posztokból értesülnek a csalásokról, csalárd üzletelésekről.

Jellemző, hogy a kifizetett termékek, szolgáltatások nem érkeznek meg a vásárlóhoz, nem eredeti terméket árulnak, amelyről nem minden esetben tájékoztatják a vásárlókat (az utóbbi időben a „jellegű" kifejezés utalhat arra, hogy nem eredeti).

A C2C csalások esetében a klasszikus csalás bűncselekményének tényállása mellett, számos más bűncselekmény is megvalósulhat, mint a személyes adattal visszaélés vagy az információs rendszer felhasználásával elkövetett csalás.

A B2C kereskedelem a *Business to Customer* tevékenység, azaz a C2C kereskedelemmel ellentétben, a vállalkozás értékesíti a fogyasztónak, vevőnek a szolgáltatást vagy terméket. A csalás megvalósulhat az értékesített áru minőségével, mennyiségével, az árával kapcsolatban, illetve az online fizetés esetén a bankkártya vagy az ügyfél adatainak megszerzését követően a kifizetett árut, terméket vagy szolgáltatást a megrendelő nem kapja meg, vagy nem abban a minőségben, mint ahogyan hirdetik.

Jellemző, hogy a weboldalon a cég elérhetősége, telephelye, székhelye nincs feltüntetve. Sajnos gyakori, hogy a vásárló a weboldalon szereplő cégnek nem néz utána, vagy az utánvétes vásárlás helyett, akár azért, mert nem adnak rá lehetőséget, akár mert számára kényelmesebb az utalás, a bankkártyaadatait megadja.[22]

Sokszor jellemző, hogy amennyiben a vevő számára elhanyagolható pénzt bukott a sikertelen vásárlás során, nem tesz meg semmit annak érdekében, hogy azt hivatalos útra terelje.

Ahogyan a bevezetőben is említettem, a közösségi médiában a károsultak által létrehozott csoportokba belépve kértem a sértetteket az interjú elkészítésére. Annak ellenére, hogy a csoporttagok az adott, sokszor zárt csoporton belül aktívak, a hozzászólásukban, illetve az általuk írt posztokban részletesen leírták, hogyan és milyen módon váltak áldozattá, a felkérésemre csak nagyon kevesen jelentkeztek.

A csalás áldozatául esett és interjút vállalt személyek 100%-ban nők, akik közül sokaknak a termék árának olcsósága nem tűnt fel, vagy épp elfogadták az „eladó" magyarázatát. A családi helyzetük, kisgyermek miatt, vagy azért, mert az áhított terméket a lakóhelyüktől nagyon távol tudták volna megtekinteni, személyesen átvenni,

---

[21] Nagy Zoltán András: A csalás jellegű cselekmények az e-kereskedelem körében. In Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika.* Budapest–Pécs, MTA TK Jogtudományi Intézet – Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2019. 148–168.

[22] Symantec: *BEC scams remain a billion-dollar enterprise, targeting 6K businesses monthly.* 2019. Online: www.symantec.com/blogs/threat-intelligence/bec-scams-trends-and-themes-2019

inkább a postai vagy csomagküldő szolgáltatást választva, előre utalva szerették volna megkapni.

Az elkövetőknek kedvezett a 2020-ban megjelent Covid-19, aminek következtében hazánkban 2020 márciusától korlátozásokat vezettek be. A sértettek a pandémiától való félelem miatt kevésbé preferálták a személyes átvételt, illetve hetekig el tudták fogadni az olyan típusú kifogásokat, amelyek karanténra vagy kórházi kezelésre hivatkozva csúsztak.

6. Információs rendszer felhasználásával elkövetett csalás

A hatályos büntetőjogi szabályozás alapján az követi el az információs rendszer felhasználásával elkövetett csalást, „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 bűncselekmény által védett jogi tárgyak a számítástechnikai rendszer integritásához fűződő jogi érdekek, a vagyoni viszonyok és az elektronikus készpénz-helyettesítő fizetési eszközök forgalmának a biztonsága.

A bűncselekmény elkövetési tárgya egyrészt az információs rendszer, maga a számítógépes adat, program, illetve másrészt a hamis, a hamisított, illetve jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszköz.[23]

Továbbra is virágkorukat élik az adathalász e-mailek, telefonhívások, amelyeket vállalatok, pénzintézetek, áram-, víz- és gázszolgáltatók, telefontársaságok nevében küldenek ki, és amelyekbe személyes adatokat, bankkártyaadatokat stb. kérnek, megszerezve ezáltal jelszavakat, PIN-kódokat. Az adathalász támadásokat *social engineering* technikának tartják, hiszen az emberi bizalomra építenek, és az elektronikus levelek tartalma és a telefonhívások is úgy tűnnek, mintha ténylegesen legitim szervezettől, vállalkozástól érkeztek volna, ezzel is erősítve a bizalmat irántuk.[24]

Utóbbi időben már nemcsak választ várnak egy e-mailre, hanem egy linkre kattintva kérik a megerősítést, vagy azon keresztül kell az adatokat megadni, így lopják el az adatokat vagy telepítik a rosszindulatú kódot. Míg korábban a hatóságok arra figyelmeztettek, hogy a felhasználók ilyen esetben jobban figyeljenek, hogy a link a https-en keresztül érhető-e el, addig most már ez a biztonságosnak nevezhető forma sem garancia arra, hogy nem adathalász linkre irányítja-e át a címzetteket.

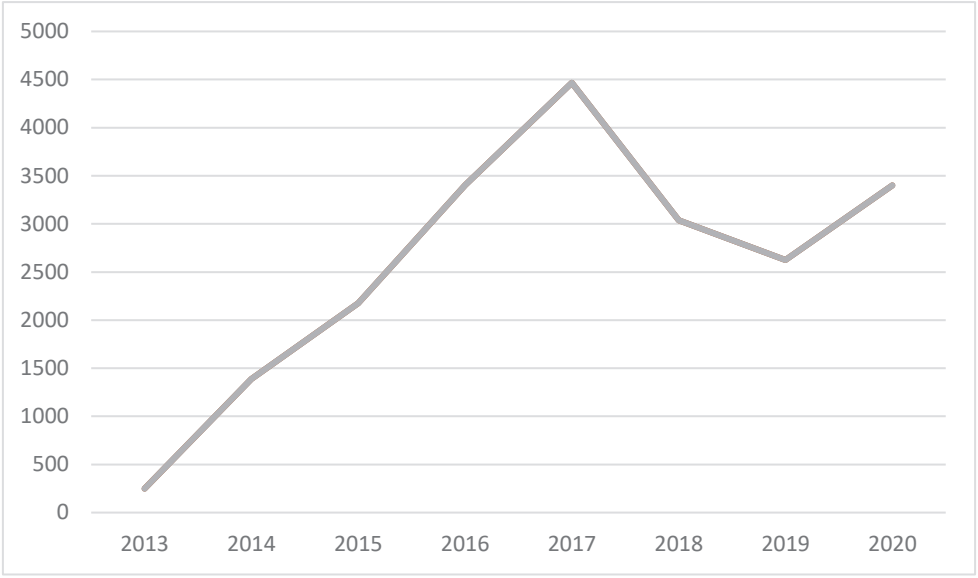
A közösségi média, illetve az ahhoz kapcsolódó üzenetküldő rendszerek és a felhasználók viselkedése, félelme attól, hogy ismerős vagy ismeretlen emberek kibeszélik őket, megszégyenülnek, az adathalász támadások újabb területei lettek. Ismeretlen személyek üzenetküldő szolgáltatáson keresztül felhívják az áldozatok figyelmét arra, hogy „kibeszélik" őket, és „olyan" fényképeket osztanak meg róluk a hátuk mögött egy

[23] Gyaraki Réka: *A számítógépes bűnözés nyomozásának problémái*. Doktori értekezés, Pécs, Pécsi Tudományegyetem, 2019.

[24] IOCTA Report 2019.

csoportban, amelyet az üzenetben küldött linken meg tudnak nézni. Természetesen ezek a linkek semmiféle zárt csoportba nem kalauzolják el a felhasználót, hanem azok félelmükért az adataikkal fizetnek.

Az információs rendszer felhasználásával elkövetett bűncselekmények számának alakulása az ENyÜBS alapján az alábbiak szerint alakult:



2. ábra: Információs rendszer felhasználásával elkövetett csalások 2013–2020. Forrás: https://bsr.bm.hu/Document

7. Konklúzió

A szakemberek és kiberbiztonsággal foglalkozó szervezetek amellett, hogy folyamatosan jelen vannak, és reagálnak az újabb és újabb veszélyekre, promóciós felületként is használják ezeket az oldalakat.

Az interjúk során nem ok nélkül választottam azt a módszert, hogy beszélgessek a sértettekkel, egyetlen esetben sem ismerték azokat az intézeteket, szervezeteket, amelyek legalább havi rendszerességgel, kampányszerűen hívják fel a veszélyre poszterekkel, videókkal, podcastekkel a megelőzésre a figyelmet.

Amíg a vállalatok, szervezetek az informatikai biztonsági szabályzattal (röviden: IBSZ), annak oktatásával és betartatásával próbálják az informatikai rendszerüket megvédeni, addig az otthoni felhasználók védtelenek, ők legfeljebb a saját maguk által felállított gondolatok vagy más tapasztalatok alapján tudnak védelmet felállítani a kibertérben, ami nem terjed ki a személyes adataik védelmére.

Az interjúkészítésnél az önként jelentkezők száma kevés, annak ellenére, hogy a virtuális térben, a közösségi médiában részletesen beszámolnak arról, hogy mi történt velük, ezért a kutatás időtartamát 2021. augusztus 31-ig határoztam meg.

Az értékelhető adatok közül jól látszik, hogy az áldozatokká vált felhasználóknál erős szerep jutott többek között a vizualitásnak, a közösséghez tartozásnak és a más véleményének, de viselkedésük nem terjed ki a tudatosságra, következetességre és a körültekintésre.

A kiberbűncselekmények megelőzése nem csak a nyomozóhatóság feladata, hiszen a felhasználó tehet a legtöbbet annak megakadályozása érdekében, hogy egyes esetekben sértetté váljon.

A kevésbé biztonságtudatos személyek szemével vizsgálva a megelőzésre, tudatosításra nevelésre, figyelemfelhívásra szolgáló promóciós anyagokat elmondható, hogy azok csak kampányszerűen láthatók, rövid leírásúak.

IRODALOMJEGYZÉK

Bányász Péter: Social engineering and social media. *Nemzetbiztonsági Szemle,* 6. (2018), 1. 59–77.

CISA: *Recognizing and Avoiding Email Scams.* Cybersecurity & Infrastructure Security Agency. Online: www.us-cert.gov/sites/default/files/publications/emailscams_0905.pdf

CPS: *Cybercrime-prosecution guidance.* The Crown" Prosecution Service (CPS), 2019. Online: www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance

Graham, Roderick S. – Shawn K. Smith: *Cybercrime and digital deviance.* New York, Routledge, 2019. Online: https://doi.org/10.4324/9781351238090

Gyaraki Réka: *A számítógépes bűnözés nyomozásának problémái.* Doktori értekezés, Pécs, Pécsi Tudományegyetem, 2019.

IOCTA 2019 Report

Cross, J. P.: *Identity theft protection. How to prevent identity theft and credit card fraud.* New York, LCPublifish, 2014.

Klenovszki János: *Nőtt az internetpenetráció, már 6 175 500 fő internetezik hazánkban.* NRC, 2020. Online: https://nrc.hu/news/internetpenetracio-2/

KSH: *A háztartások életszínvonala, 2019.* Központi Statisztikai Hivatal. Online: www.ksh.hu/docs/hun/xftp/idoszaki/hazteletszinv/2019/index.html

Leitold Ferenc: A felhasználói viselkedés, mint információbiztonsági kockázat becslése. In *Networkshop 2019.* Budapest, Hungarnet Egyesület, 2019. 189–197. Online: https://doi.org/10.31915/NWS.2019.24

McGuire, Mike – Samantha Dowling: *Cyber crime: A review of the evidence. Research Report 75, Chapter 1: Cyber- dependent crimes.* Home Office, 2013. Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246751/horr75-chap1.pdf

Nagy Zoltán András: A csalás jellegű cselekmények az e-kereskedelem körében. In Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika.* Budapest–Pécs, MTA TK Jogtudományi Intézet – Pécsi Tudományegyetem Állam- és Jogtudományi Kar, 2019. 148–168. Online: https://jog.tk.mta.hu/uploads/files/08_buntetojog_informatika_NAGYZA.pdf

Nemzeti Média- és Hírközlési Hatóság: *Az elektronikus hírközlési piac fogyasztóinak vizsgálata, 2019 – internetes felmérés.* NMHH, 2020. Online: https://nmhh.hu/cikk/212533/Az_elektronikus_hirkozlesi_piac_fogyasztoinak_vizsgalata_2019__internetes_felmeres

Neumann János Számítógép-tudományi Társaság: *IT biztonság közérthetően – Első a (kiber)biztonság!* 2019. Online: https://njszt.hu/hu/news/2019-09-30/it-biztonsag-kozerthetoen-elso-kiberbiztonsag
Rendészettudományi Szaklexikon. Online: https://nkerepo.uni-nke.hu/
Symantec: *BEC scams remain a billion-dollar enterprise, targeting 6K businesses monthly.* 2019. Online: www.symantec.com/blogs/threat-intelligence/bec-scams-trends-and-themes-2019
Szabó Máté: *Az információs hatalom alkotmányos korlátai.* Doktori értekezés, Budapest, Eötvös Loránd Tudományegyetem, 2011.
Weijer, Steve G. A. van de – E. Rutger Leukfeldt: Big Five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking,* 20. (2017), 7. 407–412. Online: https://doi.org/10.1089/cyber.2017.0028
Whitty, Monica – Tom Buchanan: The online romance scam: A serious cybercrime. *Cyberpsychology, Behavior and Social Networking,* 15. (2012), 3. 181–183. Online: https://doi.org/10.1089/cyber.2011.0352
Yar, Majid– Kevin F Steinmetz: *Cybercrime and society.* 3rd Edition, Sage, 2019.
Zsila Ágnes – Demetrovics Zsolt: Cyber-viktimizáció és cyber-agresszió. *Médiakutató,* 19. (2018), 1. 21–33.

Internetes forrás

https://search2.ucl.ac.uk/s/search.html?query=2010+social+media&collection=website-meta&profile=_website&tab=websites&submit=Go

ABSTRACT

The Impact of Social Media on Cybercrime
Réka GYARAKI

The impact of social media adversely affects the number of crimes committed. Platforms, such as applications created for entertainment, dating, dating in the online space are real hotbeds of crimes that are committed either online or offline, or a combination of these.
In this study I present cybercrimes in relation to the risks of user behaviour, such as fraud and information system fraud; popular applications greatly contribute to these offences.

Keywords: *computer, social media, cybercrime, victim, fraud, online fraud*