GAZDASÁG ÉS PÉNZÜGY • 11. ÉVF. 1. SZ. • 2024. MÁRC. • DOI: 10.33926/GP.2024.1.2

A KIBERBŰNÖZÉS LEGJOBB ELLENSZERE A PÉNZÜGYI MŰVELTSÉG

Kovács Levente – Terták Elemér[1]

ABSZTRAKT

A pénzügyek viharos digitalizációjának nyomán „mellékhatásként" elharapódzott a kiberbűnözés. Emiatt a pénzügyi szolgáltatóknak egyre nagyobb erőfeszítéseket kell tenniük a rájuk bízott értékek védelme és saját reputációjuk megőrzése érdekében. Ezeket az erőfeszítéseket az államok bűnüldöző szervei messzemenően támogatják, hiszen alapfeladataik közé tartozik az állampolgárok vagyoni biztonságának védelme, továbbá a pénzügyi stabilitás megőrzése. Ugyanakkor természetszerűleg a pénzügyi szolgáltatásokat igénybe vevő ügyfelek maguk is felelősséggel tartoznak a saját vagyonuk biztonságáért, kiváltképpen a jelszavaik, számítógépeik és kapcsolataik gondos kezelésével.

Ez az írás elsősorban a pénzügyi műveltség fejlesztésében részt vevő pedagógusok számára készült, hogy egyfelől átfogó képet kapjanak a pénzügyi bűnözés különböző megnyilvánulási formáiról, s az ezek ellen való védekezés lehetséges módjairól is. Másfelől segítséget kíván nyújtani a számukra a pénzügyi műveltség színvonalának az emeléséhez, valamint a célközönség részéről felmerülő kérdések szakszerű megválaszolásához.

JEL-kódok: A20, G2, O30

Kulcsszavak: pénzügyi kultúra, kiberbűnözés, kockázatok, pénzügyi biztonság

1. NÉHÁNY GONDOLAT A KIBERBŰNÖZÉS RELEVANCIÁJÁRÓL

Az elmúlt néhány évtized alatt a digitális átalakulás, beleértve a mobiltelefónia forradalmát is, alapjaiban változtatta meg a pénzügyi szolgáltatások nyújtását szerte a világon (Pásztor–Szijártó, 2016; Poletaeva et al., 2019). E folyamat előrehaladásán nagyot lendített a 2020-ban kitört koronavírus-járvány, mivel egészségvédelmi okokból ugrásszerűen megnőtt a távmunka, a távoktatás, valamint a digitális kereskedelem szerepe, és mindennek természetes következményeként a

1 *Kovács Levente* főtitkár, Magyar Bankszövetség; tanszékvezető egyetemi tanár, Miskolci Egyetem, levelező szerző. E-mail: kovacs.levente@bankszovetseg.hu.
Terták Elemér elnökségi tag, Magyar Közgazdasági Társaság. E-mail: elemertertak@gmail.com.

digitális pénzügyi tranzakciók száma és értéke is. A digitális korszakban az adatok és a pénzügyi nyilvántartások védelme legalább olyan fontosságra tett szert, mint amennyire egykoron a páncéltermek és páncélszekrények nélkülözhetetlenek voltak a pénz, az értékpapírok, valamint az ezekkel kapcsolatos okiratok biztonságos megőrzéséhez. Az egyre hatalmasabb összegű digitális pénzáramlást lebonyolító nemzetközi kibertér óhatatlanul magára vonta a bűnözők figyelmét, és megnövelte az általuk kezdeményezett kibertámadások kockázatát, gyakoriságát, valamint súlyosságát (Terták–Kovács, 2023). A kiberbűnözők elsősorban az adatlopásra és az adathalászatra összpontosítanak, hogy kifoszthassák áldozataik bankszámláit. Ezenkívül csalással és megtévesztéssel, vagy pedig az áldozat eszközeinek megbénításával, zsarolás útján próbálják rábírni áldozataikat nagyobb összegek kifizetésére. Az idén 100 esztendős Nemzetközi Bűnügyi Rendőrségi Szervezet – közismert nevén az Interpol – által a bűnözés globális trendjeiről tavaly közzétett első jelentése szerint a 195 tagország rendőrségeinek közel kétharmada a pénzmosást, az internetes csalást, az adathalászatot és a zsarolóvírusok (ransomware)[2] terjesztését minősítette napjaink legjelentősebb veszélyeinek (NZZ, 2022). Ezek együttesen mind a digitális pénzügyi bűnözés elemei.

Napjaink digitális pénzügyi bűnözése a fehérgalléros bűnözésnek[3] olyan válfaja, ami a csalárd tevékenységek széles körét fedi le (Weisburd et al., 1994), és magába foglal minden olyan, digitális eszközök használatával vagy segítségével elkövetett bűncselekményt, amely pénzügyi vállalkozást vagy pénzpiacot, így például bankokat, fintechcégeket, hitelezőket és természetesen bármely pénztulajdonost érint (Croall, 2009). Az információs és kommunikációs technológiák segítségével végrehajtott pénzügyi bűncselekmények elkövetése azért különösen vonzó a szervezett bűnözői csoportok számára, mivel viszonylag alacsony kockázat mellett magas hasznot tudnak elérni (Lyng, 2005), mégpedig az egész világra kiterjedően. Ehhez hozzájárul, hogy az ilyen bűncselekmények nyomozása magas színvonalú műszaki és pénzügytechnikai ismereteket igénylő feladat, ami megnehezíti a tettesek elkapását. Ez kiváltképpen igaz azokra az internetes csalásokra és egyéb bűncselekményekre, amelyekben több ország is érintett, s ezért csak nemzetközi együttműködéssel deríthetők fel (Katona, 2021).

2 Az úgynevezett zsarolóvírusos támadások során a számítógépeken tárolt adatokat rosszindulatú programok feltelepítésével teszik hozzáférhetetlenné. Az adathalászat hamis webhelyek vagy e-mailek használatával történő adatlopást jelent.

3 Fehérgalléros bűnözés alatt a pénzügyi indíttatású, nem erőszakos vagy közvetlenül nem erőszakos bűncselekményeket szokás érteni, amelyeket szakmabeli ismereteiket és pozíciójukat felhasználva főként a társadalom magasabb végzettségű rétegeihez tartozó, ún. „fehérgalléros" állásban lévők követnek el.

A nemzetközi szinten tevékenykedő, szervezett bűnözői csoportok hasznot húznak a digitális tér biztonságára vonatkozó nemzeti jogszabályok közötti eltérésekből, továbbá abból, hogy részben ebből eredően az egyes országok bűnüldöző hatóságai között gyakran nehézkes az együttműködés (Weisburd et al., 1994). Ennek nem csupán a bűncselekmények jogi definíciója közötti eltérés az oka, hanem az is, hogy a kiberbűnözés esetében a joghatósági eljárások illetékessége országonként eltérő, ráadásul a bevált hagyományos rendőri kapcsolatok helyett sokszor különböző típusú, újonnan létrehozott kibervédelmi szervezeteknek kell egymással együttműködniük. Ezért a hatóságok a jogosultságok egyértelmű tisztázásáig gyakran kénytelenek a nyomozási együttműködést felfüggeszteni. Ezeken a problémákon sokat segített az Európa Tanácsnak a 2001-ben Budapesten elfogadott Számítástechnikai Bűnözésről Szóló Egyezménye, amely a kibertér számos szabályozási hiányossága ellenére világos feladatrendszert szabott meg a csatlakozó államok számára azzal kapcsolatban, hogy nemzeti jogukban miként kezeljék a már akkor elharapódzó kiberbűncselekményeket. Az egyezmény elfogadása óta eltelt több mint két évtized során végbement technikai, jogi és gyakorlati fejleményekre tekintettel azonban indokoltnak tűnik az egyezmény korszerűsítése (Krasznay, 2021). A módosítás szükségességének egyik fontos indokát az időközben megszületett és egyébként valóban nagyon fontos adatvédelmi előírások – az EU-ban a GDPR mozaikszóként közismert, általános adatvédelmi rendelet –, mert rendelkezéseik betartása nem szándékoltan nehezíti a nyomozóhatóságok gyors közös fellépését.

Végül, de nem utolsó sorban fontos felhívni arra a figyelmet, hogy az olyan egyéni és szervezeti sérülékenységek, mint például az áldozatok pénzügyi tudatosságának, kockázatértékelésének és védekezésének a hiányosságai (Dunn, 2007; Walklate, 2017), jócskán megkönnyítik a bűnözők dolgát (Lyng, 2005). Ezt tükrözi a Pénzügyi Békéltető Testületnek (PBT)[4], a fogyasztók és az MNB által felügyelt pénzügyi szolgáltatók közötti pénzügyi tárgyú jogviták békés rendezéséhez lehetőséget nyújtó szervezetnek az a tapasztalata is, hogy a fizetési forgalommal kapcsolatban a szervezet elé kerülő panaszok 77 százalékát azért kellett megszüntetni, mert a tényállás egyértelműen mutatta, hogy a kár bekövetkezéséért a felelősség egyértelműen a gondatlannak bizonyult ügyfelet terheli. Az egyéni védekezés szervezett elősegítése tekintetben nemzetközileg is figyelemre méltó kezdeménye-

4 A Pénzügyi Békéltető Testület a Magyar Nemzeti Bank által működtetett, bíróságon kívüli, vitarendezési fórum, amely 2011. július 1-je óta nyújt lehetőséget a fogyasztók és az MNB által felügyelt pénzügyi szolgáltatók közötti pénzügyi tárgyú fogyasztói jogviták békés rendezéséhez. A testület elsődleges célja, hogy egyezséget hozzon létre a felek között. Ha ez nem lehetséges, akkor kötelezést vagy ajánlást is hozhat, amennyiben szolgáltatói jogsértés történt. A PBT eljárása ingyenes, sem eljárási díjat, sem illetéket nem kell fizetni, és a jogi képviselet sem kötelező.

zés a magyar KiberPajzs projekt.[5] Ennek keretében a kiberbiztonsági kockázatokról és az ellenük való védekezési lehetőségekről összehangolt intenzív kommunikációs kampányokat folytatnak az érintett kormányzati és hatósági intézmények, a piaci szereplők, valamint kommunikációs partnerként a Médiaunió Alapítvány. A védekezéshez szükséges ismeretek széleskörű terjesztésén kívül a projekt elősegítette az illetékes hatóságok és a pénzügyi szektor vállalkozásainak összehangolt fellépését, továbbá a hatékony megelőzési és védekezési stratégiák kialakítását.

2. VESZÉLYESEBBÉ VÁLIK-E KORUNKBAN A PÉNZÜGYI BŰNÖZÉS?

A digitális átalakulás korszakában a technológia folyamatos fejlődésével nemcsak a pénzügyi szolgáltatások spektruma szélesedik ki, és növekszik a tranzakciók sebessége, hanem – mint azt már említettük – a pénzügyi bűnözés módszerei is folyamatosan fejlődnek és gyorsan változnak (Szóka, 2021). A bűnözők a világot behálózó interneten keresztül akár nagy távolságból is könnyen hozzáférhetnek a bűnelkövetéshez szükséges adatokhoz, információkhoz és ezek forrásaihoz, emellett egyidejűleg igen nagyszámú áldozatot is könnyen el tudnak érni (Orbán, 2023; Terták–Kovács, 2023). A globalizáció következtében a bűnözők határokon átnyúló tevékenysége is megnövekedett, emellett gyakoribbá vált a különböző országok bűnözőinek összefogása a bűnözés terén. E fejlemények folytán a pénzügyi bűnözés terén is végbement a globalizáció (van Dijk, 1999; Shivaraj, 2023), ami óhatatlanul megnehezíti az általuk elkövetett bűncselekmények eredményes felderítését és megelőzését. További nehezítő körülmény, hogy a bűnözők a nemzetközileg átfogóan nem szabályozott kriptovalutákat használják zsákmányaik elrejtésére és továbbítására (Katona, 2021).

A pénzügyi bűnözés következményei rendkívül károsak mind az egyénekre, mind a vállalkozásokra és egyéb jogi személyekre nézve. A pénzügyi bűncselekmények személyi áldozatai az őket ért pénz- és vagyonvesztésen kívül sokszor maradandó, súlyos érzelmi, pszichológiai és egészségi károsodást is elszenvednek (Davies et al., 2003; Dunn, 2007). A megkárosított vállalkozások pedig nyereségük és/vagy vagyonuk csökkenésén kívül jó üzleti hírnevüket, valamint az ügyfeleiknek – az üzleti tevékenységük folyamatosságához elengedhetetlen – bizalmát is elveszíthetik. A pénzügyi bűnözés elharapódzása mindezen felül alááshatja a lakosságnak a pénzpiacok biztonságos működésbe vetett hitét, ez pedig következményeként felhajtja a pénzügyi szolgáltatások díját, valamint a hitelfelvételek költségeit.

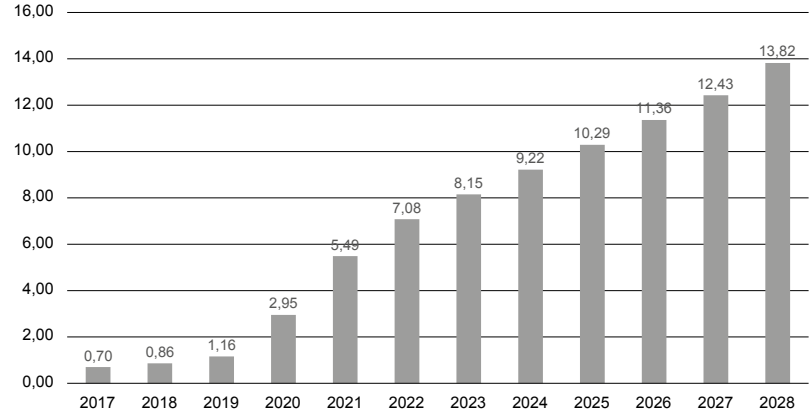
5 A KiberPajzs projekt honlapja: https://kiberpajzs.hu/

A pénzügyi bűnözés azonban nem csupán nemzeti szinten káros: a világgazdaság egészére is negatív hatással van. Így például a pénzmosás révén a bűnözők jelentős összegű pénzeszközöket mozgatnak szerte a világon, így elérhetetlenné teszik ezeket, ha az általuk okozott károk enyhítésére lefoglalni kívánnák a hatóságok. Ezenkívül a nemzetközi méretűvé dagadó csalások és hamisítások meggyengíthetik a nemzeti valutákat, visszavethetik a befektetéseket, és mindezek révén végső soron károsíthatják az egyes országok gazdaságait (van Dijk, 1999).

A globalizált pénzügyi természetű kiberbűncselekményeket természetükből fakadóan nehéz nyomon követni, még inkább az általuk okozott valamennyi kárt megbízható módon számszerűsíteni. Így például meglehetősen nehéz az évente tisztára mosott pénz teljes összegének pontos becslése. Ezért a pénzügyi bűncselekményekre, köztük a pénzmosásra vonatkozó adatok gyakran csak szakértői becsléseken alapulnak. E becslések szerint a pénzügyi bűnözés által okozott károk a globális GDP 3–5 százalékát teszik ki, vagyis a pénzügyi bűnözés akár a világ egyik legjövedelmezőbb szektorának is tekinthető, s ez a körülmény nyilván megnehezíti a vele szemben folytatott harcot. Ezen túlmenően a pénzügyi bűncselekmények az áldozatok által közvetlenül elszenvedett károkon kívül a gazdaság egészének okozhat akár hosszabb időn át gazdasági többletköltségeket a keletkezett károk kiküszöbölése és a kiberbiztonság megerősítése. A súlyos következmények magyarázzák, hogy miért is tesznek a kormányok és a pénzügyi intézmények nagy erőfeszítéseket a pénzügyi bűnözés leküzdésére (van Dijk, 1999).

A kiberbűnözés által okozott károk 2017 óta napjainkig regisztrált és 2028-ig prognosztizált összegét az *1. ábra* mutatja be.

1. ábra
A kiberbűnözés becsült globális költsége (2017–2028), Mrd USD



Forrás: Statista, 2023

A kiberbűnözés folyamatosan növekszik. 2001 óta az online bűncselekmények áldozatainak száma 16-szorosára, a pénzügyi veszteségek pedig több mint 570-szeresére nőttek. Összességében a kiberbűnözés több mint 7 millió áldozatot és legalább 80 ezer milliárd dolláros veszteséget követelt az elmúlt 22 év alatt (AAG IT, 2023). A gyors növekedés fő tényezője a viharos digitalizáció volt: míg 2007-ben, a mobilbankolás forradalmának a hajnalán a világ lakosságának mindössze egyhatoda rendelkezett internetkapcsolattal, addig 2023 közepén az időközben 1,2 milliárd fővel gyarapodott lakosságnak a kétharmada. A prognózisok szerint 2028-ig a pénzügyi vesztességnek „mindössze" 70 százalékos növekedésével kell számolni, ám még ez a „lassuló" ütem is több mint másfélszerese a világ GDP-je ugyanezen időszak alatt várható növekedési ütemének (Surfshark, 2023). A kiberbűnözés intenzitása szoros kapcsolatot mutat a globális fejleményekkel: a 2008. évi nagy globális pénzügyi válságot követően 2009-ben 115 százalékkal nőtt a kiberbűnözés miatti pénzügyi veszteség. 2020-ban, a koronavírus-világjárvány első évében a kiberbűnözés áldozatainak száma 69 százalékkal ugrott meg 2019-hez képest, és ezzel elérte eddigi csúcsát. Az árak emelkedése és az infláció a világ legnagyobb részén 2022-ben tetőzött, amely évben a kiberbűnözés okozta károk közel 30 százalékkal növekedtek az előző évihez képest.

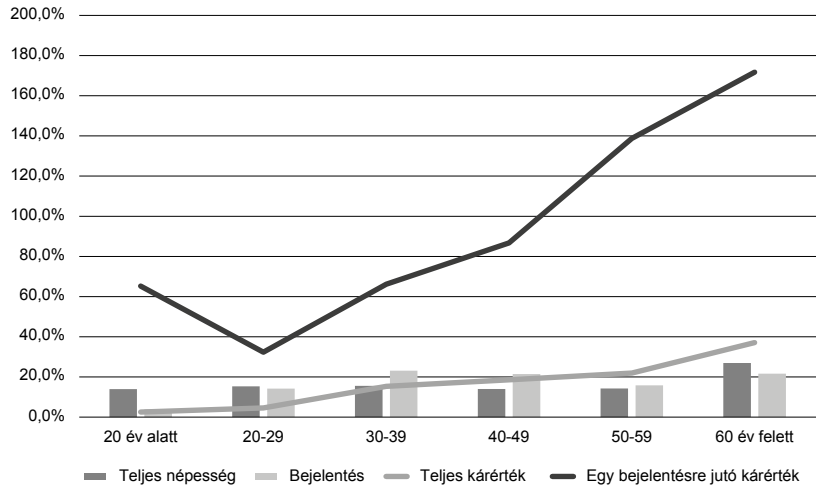
A világszerte elkövetett digitális pénzügyi bűncselekményekről ugyan még nem állnak rendelkezésre minden országból teljes körű, megbízható adatok, ám ennek ellenére a nemzeti bűnügyi statisztikák összehasonlítása révén országonként néha szembeszökő különbségeket is lehet észlelni az egymillió internethasználóra jutó bűncselekmények számában és az egyes bűncselekmény-típusok elkövetési gyakoriságában. A különbségek társadalmi, kulturális és gazdasági tényezőkkel magyarázhatók, de az ezek közötti összefüggéseknek a feltárása még várat magára. Világviszonylatban 2022 folyamán a kiberbűnözésnek az egymillió internetfelhasználóra vetítetten Nagy-Britanniában és az Egyesült Államokban volt a legtöbb áldozata. Viszont ugyanebben az esztendőben az USA-hoz hasonló fejlettségű, azzal szomszédos Kanadában fajlagosan csak egynyolcad annyi károsult volt, mint az USA-ban. Meglepő módon Európában az egymillió internethasználóra jutó kiberbűncselekmények száma csak a töredéke volt az angolszász országokban, illetőleg a többi angol nyelvet beszélő országokban mért értéknek.

Az egyes bűncselekménytípusok tekintetében világszerte az adathalászatnak volt a legtöbb áldozata, míg az okozott kár nagyságát tekintve a befektetési csalások vezettek. Az adathalászat nagy gyakorisága az internetpenetrációval és nyelvi okokkal magyarázható, ugyanis ez a bűncselekmény legkönnyebben a legtöbb ember által beszélt nyelveken követhető el, ahol egyúttal sok embernek van internetkapcsolata. Nem véletlen tehát, hogy az angol és a kínai nyelvet használó országokban fordul elő a leggyakrabban az adathalászat. A befektetési csalások intenzitása pedig összefüggést mutat az adott országok részvénypiacának a nagy-

ságával, illetve azzal, hogy az adott országok háztartásainak a megtakarításaiban mekkora a részvények és a kötvények hányada.

A kiberbűncselekmények áldozatainak kor szerinti megoszlásában viszont az egyes országok között hasonlóság tapasztalható. Az USA-ban 2022 folyamán az FBI Internetes Bűnügyi Panaszközpontja (Internet Crime Complaint Center – IC3) 800 944 bejelentést kapott. A bejelentett esetek együttes kárértéke 10 300 milliárd dollár volt. A *2. ábra* korcsoportonkénti bontásban mutatja be a kárbejelentések számának és értékének a megoszlását.

2. ábra
Kárbejelentések száma, értéke és megoszlása 2022-ben az USA-ban



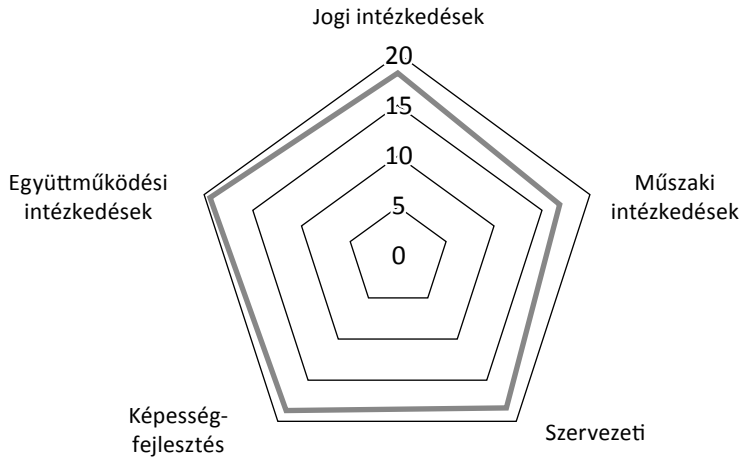
Forrás: IC-3, 2022

Mint az az ábrából jól kivehető, az áldozatoknak valamivel több mint egyötöde 60 év feletti volt, ami némileg alacsonyabb a teljes népességben képviselt részarányuknál, ám az egy bejelentésre jutó kárérték az ő esetükben volt a legmagasabb. A kárbejelentők életkora és az elszenvedett kár nagysága a legtöbb országban – köztük hazánkban is – ehhez hasonló megoszlást mutat. Ennek fő oka feltehetően az, hogy az idősebb korosztályok tagjai kevésbé jártasak a korszerű pénzügyi technikák alkalmazásában. Ez pedig arra figyelmeztet, hogy az idősebb emberek védelmére az átlagosnál nagyobb figyelmet kell fordítani. Szintén tanulságos, hogy a 20 év alattiak korosztályára a bejelentéseknek alig 4 százaléka jutott, ami jóval kisebb a népességben betöltött részarányuknál, viszont az általuk elszenvedett kár fajlagos összege kétszerese volt a 20–29 éves korosztályénak. Ez viszont arra utal, hogy kellő ismeret és jártasság hiányában a kiskorúak szinte vakon

mennek bele súlyos károkkal járó ügyletekbe. Ennek a megelőzése érdekében az iskolai pénzügyi oktatásra változatlanul nagy figyelmet kell fordítani.

A pénzügyi bűnözés kockázatai kapcsán rá kell mutatnunk arra is, hogy az egyes országok felkészültsége a kiberbiztonság megvédésére nem egyforma. A Nemzetközi Távközlési Egyesületnek a kezdeményezése alapján kidolgozták a Globális Kiberbiztonsági Indexet (Cybersecurity Index – GCI). Ez a mérőszám globális szinten öt különböző dimenzióban méri a szervezet 160 tagországának a felkészültségét. A 2020. évre vonatkozóan végzett felmérés szerint az idén közzétett rangsor élén az Egyesült Államok és Nagy-Britannia áll. Az első tíz helyezett között mindössze két EU-tagállam – Észtország és Spanyolország – szerepel. Hazánk a rangsorban a 35. helyezést érte el, amivel a középmezőny felső részén helyezkedik el. A *3. ábra* a magyar minősítést mutatja be (ITU, 2023)

3. ábra
Magyarország kiberbiztonsági indexe



Forrás: ITU (2020)

3. AZ ÁLDOZATOK TIPOLÓGIÁJA

A „fehérgalléros" pénzügyi bűncselekmények áldozatai két nagy kategóriába sorolhatók (Ganzini et al., 1990):

1) Vétlen áldozatok, akiket a bűnözők szokásos kereskedelmi ügyletek keretében tévesztenek meg. Ez utóbbi csoport áldozatai egyaránt lehetnek hitelezők, versenytársak, alkalmazottak és ügyfelek.

2) „Önkéntes" áldozatok, akik többnyire a bűnözők által kilátásba helyezett, csábítóan busásnak és könnyen elérhetőnek tűnő haszon reményében mennek lépre (Dunn, 2007; Croall, 2009; Walklate, 2017).

A különféle fehérgalléros bűncselekménytípusoknál az áldozat és az elkövető közötti kapcsolat jellege általában hasonló: erőszakmentes, közvetett és személytelen; az áldozat személye többnyire teljesen ismeretlen és közömbös is az elkövető számára (von Henting, 1948; Dunn, 2007). Mivel az elkövetéshez igénybe vett digitális csatornákon az elkövető nem ismeri és nem találkozik közvetlenül az áldozatával, ezért a bűntudat sem tartja vissza a bűntett elkövetésétől (Walklate, 2017). Az üzleti világ szubkultúrája egy másik olyan tényező, amely csökkenti a fehérgalléros bűnözés feletti informális társadalmi ellenőrzést. Az üzletemberek ugyanis a haszonszerzésre irányuló erőfeszítést és a vevő „megdolgozását" az üzleti tevékenység természetes részének tekintik, továbbá készek a magasabb nyereség elérése érdekében akár az átlagosnál nagyobb kockázatot is vállalni (Lyng, 2005). Gondolkodásukban ezért fel sem rémlik az áldozattá válás lehetőségének a veszélye; figyelmüket szinte teljesen leköti a remélt nagy haszon (Davies et al., 2003). Az üzleti világ eme „amoralitása" miatt viszont elengedhetetlen, hogy a hatóságok a piac folyamatos felvigyázásával következetesen gátat vessenek annak, hogy a polgárok nyereségvágyuknál fogva könnyűszerrel a fehérgalléros bűnözés áldozatává váljanak (Ganzini et al., 1990). Ez magában foglalja a szükséges jogszabályok megalkotását, hatékony felderítési stratégiák kidolgozását, a következetes bűnüldözést, továbbá a megfelelő büntető szankciók alkalmazását (Shichor et al., 2001). Ezen túlmenően a fogyasztók rendszeres tájékoztatása a megtévesztő üzleti praktikákról és az ezek elkerülését célzó tanácsadás sokat segíthet az embereknek abban, hogy ne váljanak bűnözés áldozatává (Croall, 2009).

Az „önkéntes" áldozatok csoportja eltérő szociodemográfiai profillal rendelkezik, mint a lakosság többi része. A Financial Industry Regulatory Authority[6] a befektetési csalások áldozatairól összegyűjtött adatok statisztikai elemzése alapján több olyan sajátosságot is talált a befektetők személyiségi jellemzőiben és magatartásában, amelyek megnövelték annak a valószínűségét, hogy csalások áldozatává váljanak (FINRA, 2016; Goucher, 2010). Ezek a következők.

6 A Financial Industry Regulatory Authority (FINRA) egy olyan amerikai önszabályzó, nem kormányzati szervezet, amelynek az a feladata, hogy „megvédje a befektetői közösséget a csalásoktól és a rossz gyakorlatoktól". A FINRA 2007 júliusában jött létre. A szervezet jelentős ellenőrzési jogosultsággal rendelkezik a tagvállalatainak, alkalmazottaiknak és az általuk kiszolgált befektetőknek a napi tevékenysége felett. Nem tartozik felelősséggel az általa ellenőrzött iparág iránt, ugyanakkor széles körű hatáskörei nincsenek alávetve a kormányzati szabályozó szervezetekre vonatkozó elszámoltathatósági szabályoknak sem.

- **A befektetési ügynök és/vagy tanácsadó ellenőrzésének az elmulasztása**. A befektetők több mint 80 százaléka nem szokta ellenőrizni, hogy tanácsadója, brókere, közvetítője vagy ügynöke rendelkezik-e megfelelő engedéllyel a tevékenysége folytatására (Harvey et al., 2014).
- **Nem engedélyezett, magas kockázatú pénzügyi termékekbe történő befektetések**. A befektetési csalások ismertté vált áldozatainak közel háromnegyede fektetett be nagy hozamot ígérő, ám magas kockázatú pénzügyi termékbe, míg akik nem váltak áldozattá, azoknak mindössze a fele. A statisztikai vizsgálatok azt is kimutatták, hogy a befektetési csalások áldozatai kétszer akkora valószínűséggel döntenek az átlagosnál magasabb hozamú befektetések mellett, mint a kontrollcsoport (FCA, 2016).
- **Képtelenség a rábeszélés és a keretezés manipulatív taktikáinak felismerésére.** Minden ötödik befektető képtelen felismerni, hogy mikor próbálják különböző manipulatív módszerekkel a befektetési döntését befolyásolni (Langenderfer–Shimp, 2001; Petty–Cacioppo, 1981).
- **Túlzott önbizalom/önhittség a befektetési döntések meghozatalakor és/vagy a befektetési tanácsadó kiválasztása során**. A befektetési csalások ismertté vált áldozatai és a csalást nem szenvedettek csoportja befektetési szerkezetének az összehasonlítása azt mutatta, hogy a csalások áldozatai jóval nagyobb – a kontrollcsoporthoz képest több mint kétszeres – arányban fektettek be olyan termékekbe, amelyeket ismerőseik vagy munkatársaik ajánlása alapján saját maguk választottak ki (Fattah, 1991). A befektetési csalások áldozatai általában túlzottan is bíztak a saját ítélőképességükben, döntéseiket a megérzéseik és ösztöneik vezérelték, és ezekre nagyobb mértékben is hagyatkoztak, mint a többiek (Harvey et al., 2014).

4. A PÉNZÜGYI BŰNCSELEKMÉNYEK TÍPUSAI

A pénzügyi bűncselekmények két nagy csoportra oszthatók: az úgynevezett „szabályozott" pénzügyi bűncselekményekre és a „nem szabályozott" bűncselekményekre. A szabályozott pénzügyi bűncselekmények a jogszabályokban foglalt előírások előre megfontolt és szándékos megsértését jelentik, beleértve a pénzügyi és banki tevékenységekre vonatkozó szabályokat is. Az úgynevezett „nem szabályozott" pénzügyi bűncselekmények mindenekelőtt csalást és más megtévesztést foglalnak magukban (Alexander–Seymour, 1998).

4.1. Szabályozott pénzügyi bűncselekmények

A szabályozott pénzügyi bűncselekmények közé tartozik a bennfentes kereskedés, a (tiltott) piacbefolyásolás, a pénzmosás, a vesztegetés, a sikkasztás, a kiberbűnözés, az adóelkerülés, a pénzhamisítás stb. (NZZ, 2022). Ezek a bűncselekmények a pénzügyi piacok és intézmények védelmét szolgáló jogszabályok és előírások szándékos megsértését jelentik. A szabályozott pénzügyi bűncselekmények elkövetői többnyire olyan személyek, akik vezetői vagy döntéshozói pozíciót töltenek be, vagy akik hozzáférnek bennfentes információkhoz. Lajtár (2019) szerint az ilyen bűncselekmények jellemzően a következők.

- **Vesztegetés**: valamilyen összegű pénz fizetése vagy egyéb előny felajánlása egy adott személy vagy szervezet döntéseinek a befolyásolására.
- **Bennfentes kereskedés**: bizalmas vagy bennfentes információk felhasználása értékpapírok, pénzügyi termékek vételére vagy eladására saját vagy harmadik fél számára történő előnyszerzés céljából.
- **Sikkasztás**: valakinek a gondjaira bízott pénzeszközöknek vagy vagyontárgyaknak jogtalan eltulajdonítása, vagy azzal sajátjaként történő rendelkezés.
- **Adóelkerülés**: olyan cselekmény, amely révén jövedelmek, vagyonok, valamint az ezekre vonatkozó információk eltitkolásával lehetővé válik az adófizetési kötelezettség elkerülése.
- **Kiberbűnözés**: számítógép/számítástechnikai eszköz vagy internet használatával adatok hozzáférhetősége, sértetlensége és titkossága ellen elkövetett bűncselekmények, ideértve a zsarolóvírusok telepítését, továbbá a számítástechnikai adatok tartalmával kapcsolatos és a szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények.
- **Hamisítás**: eredeti közokirat, bankjegy vagy értékpapír megváltoztatása vagy utánzása, az ezeken szereplő adatok megváltoztatása vagy törlése, továbbá a megváltoztatott vagy utánzott okiratok felhasználása vagyoni előny megszerzése érdekében.
- **Pénzmosás**: minden olyan tevékenységet és pénzügyi műveletet felölel, amely a bűncselekmények elkövetéséből származó pénzeszközök valós forrásának leplezésére és legális eredetűvé történő átalakítására irányul.

A pénzmosás kapcsán meg kell említeni, hogy a digitális bankolást kínáló, fizikai fiókkal nem rendelkező, egyre népszerűbbé váló virtuális pénzintézetek – az úgynevezett neobankok – elterjedése nem szándékoltan ugyan, ám mégis növeli a pénzügyi csalások és pénzmosási bűncselekmények elkövetésének a kockázatát (Pásztor, 2018). A közelmúltban ugyanis több tagállamban a különféle csalástípusokkal kapcsolatos nyomozások során a digitális fizetések pénzmosási célú felhasználását figyelték meg. A neobankok által alkalmazott virtuális

IBAN-számlaszámok[7] (vIBAN) használata ugyan kétségtelenül gyors nemzetközi fizetéseket tesz lehetővé, amit az ügyfelek nagyra értékelnek, azonban elfedik a számlatulajdonos tartózkodási országát, valamint megnehezítik a gyanús tranzakciók észlelését, a gyanús tranzakciók lenyomozásában pedig egy további lépést tesznek szükségessé.

4.2. Nem szabályozott pénzügyi bűncselekmények

A nem szabályozott pénzügyi bűncselekmények közé tartoznak mindenekelőtt a személyazonosság-lopás, a csalás, a pénzügyi csalások, valamint a megtévesztés egyéb formái. Ezek a bűncselekmények jellemzően félrevezető adatokkal vagy információkkal való visszaélésekkel járnak pénzügyi haszonszerzés céljából. A nem szabályozott pénzügyi bűncselekmények általában a következőket foglalják magukban (Langenderfer–Shimp, 2001):

- **Személyazonosság-lopás**: valaki személyes és érzékeny adatainak csalással vagy megtévesztéssel történő megszerzése és jogosulatlan felhasználása anyagi haszonszerzés céljából.
- **Csalás**: más tévedésbe ejtése vagy tévedésben tartása hamis állítások vagy valótlan adatok megadása révén jogtalan haszonszerzés céljából. Ennek jellegzetes válfajai:
  - **Pénzügyi csalások**: magánszemélyek vagy vállalkozások becsapására irányuló kísérletek hamis okok, befektetések vagy szolgáltatások felajánlásával.
  - **Hitelkártyacsalás**: ellopott hitelkártyaadatok felhasználása áruk és szolgáltatások vásárlására.
  - **Befektetési csalás**: megtévesztő taktikák alkalmazása magánszemélyek vagy vállalkozások rábírására, hogy pénzt fektessenek be csalárd rendszerekbe.
  - **Banki csalás**: hamisított vagy megtévesztő dokumentumok felhasználása pénzeszközöknek banktól vagy más pénzügyi intézménytől való megszerzésére.
  - **Online csalás**: hamis vagy megtévesztő dokumentumok felhasználása áruk vagy szolgáltatások online megszerzésére.

7 Az IBAN (International Bank Account Number) az Európai Unióban és a világ más államaiban is bevezetett egységes felépítésű nemzetközi bankszámlaszám.

- **Adathalászat**: kísérletek bizalmas információk megszerzésére, például felhasználónevekre, jelszavakra és hitelkártyaadatokra úgy, hogy a csaló hivatalos szerv vagy ismert szolgáltató munkatársának adja ki magát.

Ezeket a csalástípusokat a legváltozatosabb módszerekkel igyekeznek a bűnözők elkövetni. Néhány jellegzetes elkövetési módszer:

- **„Keszonos" módszer**, amelynek keretében a csalók a kiszemelt áldozataikat erős pszichológiai nyomásnak alávetve próbálják meg rávenni arra, hogy nem létező, csekély értékű vagy magas kockázatú részvényekbe, kötvényekbe fektessenek be, vagy utalják át pénzüket az általuk megadott, „biztonságosnak" mondott számlára. Ehhez a bűnözők gyakran hamis dokumentumokat és szakértői véleményeket is felhasználnak, és áldozataikat szinte mindig időnyomás alá helyezik. (NZZ. 2022).
- **Ponzi-sémák**, amelyekben a csalók rövid időn belül a piacinál jóval magasabb hozam elérését ígérve csábítják magukhoz a befektetőket. A haszon maximalizálása érdekében a kezdeti befektetők számára a későbbi befektetőktől szerzett pénzeszközökből teljesítik az ígért magas hozamok kifizetését, akik ezért kezdeti elégedettségük révén szándék nélkül ugyan, de ismeretségi körükben „reklámozzák" a sémába való befektetést. Akik a séma felfutása után fektettek be, üres kézzel maradnak, mert ilyenkor a csaló eltűnik a pénzeszközökkel, amelyeket pénzmosás révén juttat ki külföldre (FCA, 2016).
- **Piramisjáték**, más néven hálózati értékesítés (pl. network marketing), ami sokban hasonlít a Ponzi-sémához. A kezdeti befektetők azonban ennél a módszernél aktív szereplőkké válnak, akiknek új befektetőket kell toborozniuk a beígért magas jutalék megszerzéséhez. Ennél a módszernél is azok bukják a legtöbbet, akik a séma felfutása után fektettek be.

Ezeknél a csalási módszereknél a bűnözők a legkülönfélébb kommunikációs csatornákat, például telefonhívásokat, internetet, közösségi médiát, tömeges levelezést, televíziós vagy rádiós reklámokat vesznek igénybe, hogy minél több potenciális áldozatot érhessenek el (Shichor et al., 2001). A felsorolt csatornák révén ugyanis a potenciális áldozatok nagy számát lehet gyorsan és egyszerűen, ráadásul alacsony ráfordítással elérni. Egy jellegzetes példája a csalásnak az, amikor egy bűnözői csoport tagjai magukat rendőrnek vagy banki munkatársnak adják ki, és telefonon veszik fel a kapcsolatot a kiszemelt áldozataikkal azzal az ürügygyel, hogy figyelmeztessék őket a számlájukat, befektetésüket vagy akár pénzintézetüket érintő csalás veszélyére. Az áldozataikat arra biztatják, hogy megtakarításaikat biztonságosnak mondott letéti számlákra utalják át, amelyekről aztán leemelik a befolyt pénzt (USDJ, 2015).

A befektetési csalások esetében utólag többnyire az szokott kiderülni, hogy az áldozatnak eladott értékpapírok bóvlik, vagy valóságosan nem is léteztek. Bár

a felkínált értékpapírok valódiságáról a becsapott vevők különösebb erőfeszítés nélkül maguk is meggyőződhettek volna, de ettől a kilátásba helyezett haszon káprázata miatt többnyire eltekintenek (Alexander–Seymour, 1998).

A kiberbűnözés a legutóbbi időben a „Vásárolj most, fizess később" (Buy Now Pay Later, BNPL) finanszírozás, más néven eladáshelyi részletfizetési hitel területén jelent meg. A bűnözők kihasználják a BNPL-ügyletek jóváhagyási folyamatának jelenlegi gyengeségeit. Mivel a BNPL-szolgáltatás keretében nem történik valóságos hitelbírálat, ezért a bűnözők gyakran átjutnak a csak algoritmikus alapokon nyugvó ellenőrzésen, és személyazonosság-lopás révén létező felhasználói fiókokat használnak fel az eltulajdonítani kívánt áruk megrendeléséhez.

A csalások terén a legújabb kockázati tényezőt a gépi tanulás, a mesterséges intelligencia (Ml) és a deepfake[8] technológiájának gyakorlatilag mindenfajta pénzügyi bűncselekmény elkövetéséhez történő felhasználása jelenti. Az Ml-alapú chatbotok[9], például a ChatGPT[10] kiváltképpen könnyen használhatók fel az online csalási sémákban. Az úgynevezett deepfake technológia pedig segíthet a távoli beléptetési védelem kijátszásában.

5. A PÉNZÜGYI BŰNCSELEKMÉNYEK ELKÖVETÉSÉNEK A MOTIVÁCIÓI

Bár magától értetődőnek tűnik, hogy a pénzügyi bűncselekmények indítéka az anyagi haszonszerzés, ez mégsem tekinthető kizárólagos motivációnak. Számos esetben derült ki ugyanis, hogy az elkövetők egy részét nem a haszonszerzés, hanem a szakmai kíváncsiság és kalandvágy, vagy valamilyen sérelem megtorlására, illetőleg személyes bosszúra irányuló vágy hajtotta tetteiknek az elkövetésében. Emellett egyes államok államérdekből, terrorista szervezetek és bűnszervezetek pedig politikai célok érdekében indítanak kibertámadást a védett infrastruktú-

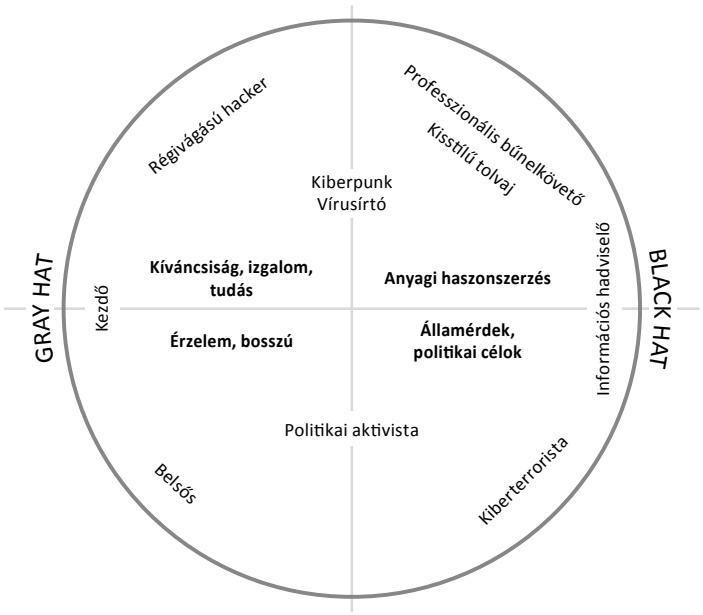
8 A deepfake olyan hitelesnek tűnő videóklip, amely valós emberek arcvonásait felhasználva mesterséges intelligencia segítségével nem létező személyek képmását jeleníti meg, vagy valódi személyeket a valóságban meg nem történt események szereplőiként jelenít meg.

9 A chatbot egy olyan szoftveralkalmazás, amely emberi erőforrás bevonása nélkül képes ügyfelekkel történő kommunikációra. A chatbotrendszereket úgy tervezték, hogy meggyőzően szimulálják azt, ahogyan egy ember viselkedne beszélgetőpartnerként. Bár a szó klasszikus értelmében nem tekinthetők mesterséges intelligenciának, a mai technikai szinten már emberi közreműködés nélkül képesek olyan feladatok megoldására, mint például az online rendelések felvétele.

10 A ChatGPT (GPT=Generative Pre-trained Transformer) egy olyan nyelvi modell, amely képes valós idejű kommunikációra az emberekkel, mivel lehetővé teszi a természetes nyelv feldolgozását, és logikailag megfelelő szöveges válaszokat generál a felhasználók kérdéseire vagy kéréseire.

rák – közük a pénzügyi szektor – ellen. Az információs rendszerek megsértésének lehetséges motivációit a *4. ábra* mutatja be.

4. ábra
Az informatikai bűnözés motivációs hálója



Forrás: Varga Á., 2022

A hacker kifejezés alatt eredetileg olyan számítástechnikai szakembert értettek, aki az informatikai rendszerek működését a hétköznapinál jóval magasabb szinten látja át, s képes a rendszer határain túllépni olyan módon, hogy azzal akár többet hozzon ki az adott rendszerből, mint amennyit a rendszer fejlesztői eredetileg elgondoltak. Minthogy időközben a bűnözői körökben is megjelentek olyan számítástechnikai ismeretekkel bíró személyek, akik képesek egy adott rendszerbe „betörni" (azt illetéktelenül használni), s képesek onnan a maguk vagy mások számára információt eltulajdonítani, ezért a „hackelés" kifejezés fokozatosan negatív értelemet kapott. Az eredetileg pozitív indíttatásúnak tekintett hackerkultúra így több egymás mellett párhuzamosan létező szubkultúrára vált szét. Ezek egyikét a „crackerek" alkotják: e csoport tagjai olyan elkövetők, akik szakismeretüket rosszindulatú tevékenységekre, rongálásra használják. De megmaradtak a tisztességesebb hackerek is. Köztük a greyhat hackereknek (más néven szürke kalapos hackereknek) nevezett olyan személyek, aki bár megsértik az etikai normákat vagy elveket, de a blackhat hackereknek (fekete kalapos hackereknek)

tulajdonított rosszindulatú szándékok nélkül. A szürke kalapos hackerek a középutat jelentik egyfelől a fehér kalapos hackerek (etikus hacker – ethical hackerek), másfelől a fekete kalapos hackerek között, akik rosszindulatúan aknázzák ki az emberek gyengeségeit és a rendszerek sebezhetőségét anyagi haszon szerzése érdekében. (Varga Á., 2022).

6. PÉNZÜGYI BŰNCSELEKMÉNYEK SZANKCIONÁLÁSA

A pénzügyi bűncselekmények érthető okokból súlyos bűncselekményeknek minősülnek, elkövetésükért komoly büntetés szabható ki. A bűncselekmény súlyosságától függően szankcióként szabadságvesztés, vagyonelkobzás és/vagy pénzbírság jár. Ezenkívül a pénzügyi bűncselekmények elkövetésében bűnösnek talált személyek személyes és szakmai jó hírneve is sérülhet, továbbá a pénzügyi és más bizalmi foglalkozástól való végleges vagy határozott idejű eltiltással sújthatók (US DoJ, 2015).

A pénzügyi bűncselekmények tetteseit a büntetőjogi felelősségen kívül polgári jogi felelősség is terheli. E felelősség alapján sújthatók az elmarasztalt tettesek a jogalap nélkül elért haszon elvonásával, kártérítési kötelezettséggel, továbbá a beszüntetési és leállási végzéssel. Ez utóbbi szankciókat általában azért szabják ki, hogy megakadályozzák az elmarasztalt egyéneket vagy szervezeteket abban, hogy a jövőben ismételten pénzügyi bűncselekményeket követhessenek el.

Mint az a leírtakból is következik, a kiberbűnözésnek jelentős társadalmi hatásai vannak, legyen szó akár adathalász tevékenységről vagy az egyének anyagi biztonságát és vagyonát károsító csalásról. Minthogy a folyamatos technikai fejlődés újabb és újabb veszélyhelyzeteket hoz felszínre, s szüntelenül új elkövetési felületek és módszerek jelennek meg, ezekre a büntetőjognak és a polgári jognak egyaránt reagálnia kell. A hazai jogi szakértők többségének a véleménye szerint mindazonáltal a hatályos magyar büntető törvénykönyv (Btk.) releváns tényállásai – ezen belül az információs rendszer felhasználásával elkövetett csalásokkal foglalkozó 375. §, továbbá a tiltott adatszerzéssel foglalkozó 422. §, az információs rendszer vagy adat megsértésére vonatkozó 423. §, valamint az információs rendszer védelmét biztosító technikai intézkedés kijátszásáról szóló 424. § – egyelőre megfelelően fedik le az online térben elkövetett bűncselekményeket, vagyis a tényállások bővítése csak a kiberbűnözés markánsan új formáinak megjelenése esetén lenne indokolt (Grund, 2021).

A büntetőjog és a polgári jog eszközei csupán egy részét alkotják azoknak az intézkedéseknek, amelyek a kibertér védelmének megteremtését és biztonságának megőrzését hivatottak szolgálni. A kiberbűnözés elleni védekezésben a jogalkotáson, a jogalkalmazáson és a jogérvényesítésen túl is kiemelt szerepe van az állam-

nak. Ez teendők egész sorát jelenti a megfelelő műszaki szabványok és előírások megalkotásától, valamint az informatikai és számítástechnikai termékek és szolgáltatások forgalomba hozatalának az engedélyezésétől kezdve az állami infrastruktúrák rendszerei védelmének biztosításán, a bűnüldözés és a jogalkalmazás felkészítésén át egészen az állampolgárok tájékoztatásig és oktatásáig.

A kiberbiztonságot megteremtő eszközrendszer nélkülözhetetlenül fontos része ugyanis maga a biztonságot kívánó és elváró egyének felkészültsége és hozzáállása is. A körültekintő internethasználat és a kiberbiztonság megőrzésére való törekvés a jelszavak és a számítástechnikai eszközök védelmén kívül abban is megnyilvánul, hogy mindig bejelentésre kerülnek-e a megkísérelt és a végrehajtott támadások. Az egyéni felhasználók bejelentései ugyanis nagymértékben hozzájárulhatnak a társadalom nagyobb fokú tudatosságához és az eredményesebb társadalmi szintű védekezéshez.

A kiberbiztonság megteremtése terén nem hanyagolható el a nemzetközi dimenzió sem. A legtöbb nemzetnek eltérő büntetőszabályai vannak az egyes kiberbűncselekményeket illetően, s a kulturális különbségekből meg a hagyományokból adódóan nem is minden cselekmény vált ki széles körben azonos reakciót. Ezért az olyan nemzetközi cselekmények esetében, amelyek szabályozása államonként nagymértékben eltér, bonyolultabbá válik a joghatósági problémák kezelése, a nyomozási hatáskörök megosztása, továbbá lassul az információcsere. A kiberbűnözés globális jellege miatt azonban elengedhetetlen az egyes országok illetékes szervei közötti nagy fokú együttműködés, a szabályozás harmonizációja és a tudományos eredmények megosztása, annál is inkább, mert a világ államainak nagy része a jogi és intézményi különbségek ellenére nagyon hasonló kihívásokkal küzd, ráadásul sokszor azonos elkövetőkkel szemben, ezért más államok és az illetékes szervei közötti jogi megállapodások és a rendszeres tapasztalatcsere hasznosnak bizonyulhatnak az együttműködésben részt vevő valamennyi nemzet számára.

7. GYAKORI KÉRDÉSEK ÉS VÁLASZOK A PÉNZÜGYI BŰNCSELEKMÉNYEKKEL KAPCSOLATBAN

Mint azt már kifejtettük, a pénzügyi bűncselekmények általában összetettek, a reájuk vonatkozó jogi és szabályozási környezet részben a körülmények változása miatt sem mindig egyértelmű (FINRA, 2016). E bizonytalanságok miatt is a pénzügyi műveltség színvonalának emelésére irányuló oktatás keretében a részvevők részéről óhatatlanul sok, többnyire hasonló tisztázást igénylő kérdés szokott felmerülni. Az oktatói munka segítése céljából ezért a továbbiakban néhány, a pénzügyi bűnözéssel kapcsolatban felmerülő kérdésre adunk rövid választ.

K1. Mit tehetek, hogy megvédjem magam a pénzügyi bűnözéstől?

Tapasztalatok szerint a kiberbűnözés és a csalás elleni védekezésében *a leggyengébb láncszem legtöbbször maga a felhasználó.* Ahhoz tehát, hogy bárki eredményesen megvédhesse magát a pénzügyi bűnözés okozta károk ellen, elengedhetetlen, hogy tisztában legyen a lehetséges kockázatokkal, továbbá minden lehetséges intézkedést is megtegyen önmaga védelmére. Ez magában foglalja az adathalász kísérletekre való odafigyelést, az olyan sémákba történő befektetések elkerülését, amelyek kondíciói túl szépnek tűnnek ahhoz, hogy igazak is legyenek, továbbá óvatosságot és körültekintést a személyes adatok bármilyen formában történő megosztásában is.

Néhány olyan jellemző, ami feltehetően befektetési csalásra vagy megtévesztésre utal, és ezért óvatosságra kell intenie mindenkit:

- **Gyorsan elérhető, garantált magas hozam ígérete.** A magas hozam a valóságban mindig magas kockázattal párosul, ami azt jelenti, hogy a befektető akár a teljes befektetését is elbukhatja. A magas kockázat tudatos vállalása különbözteti meg a befektetést a megtakarítástól, mely utóbbinál a hozam előre ismert és garantált, ám általában alacsony (FCA, 2016; FINRA, 2016).
- **Összetett (bonyolult) pénzügyi termékek.** A pénzügyi termékek nagy komplexitása vagy a komplex befektetési stratégia korántsem előfeltétele vagy garanciája az átlag feletti hozam elérésének. Ha nem érthető vagy nem átlátható a felajánlott konstrukció működése, különösen jelentősebb árfolyam- vagy kamatszintváltozás esetén, akkor jobb eltekinteni a befektetéstől, még akkor is, ha az ügylet történetesen nem ütközik jogszabályi korlátba. A nagy hozamot ígérő, tipikus termékek közé tartoznak a tőkeáttételes (leverage) és származtatott (derivatív) instrumentumok, mint például az online kereskedési platformokon történő, elsősorban FX (forex, deviza) és CFD (contract for differences), különbözetre vonatkozó pénzügyi megállapodások. Ezek az ügylettípusok ugyan nem tiltottak, de csak azok számára alkalmasak, akik képesek akár nagy vesztességet is gond nélkül „elviselni". A magas tőkeáttétel ugyanis azt jelenti, hogy a szolgáltatók által meghatározott letéti összeggel (margin) olyan ügyleteket lehet kötni, ahol az ügyletérték az elhelyezett letét összegének tízszeresét vagy akár százszorosát is elérheti. A tőkeáttétel mértékének növelése magasabb hozamot ígér, azonban minden tőkeáttételes ügylet magában hordozza a veszteség megsokszorozódásának lehetőségét, amivel a befektetők sajnos sokszor későn szembesülnek.
- **Befektetés eszközlése szerződések és egyéb dokumentumok nélkül.** Ha egy tanácsadó/ügynök pusztán szóbeli tájékoztatással, ígéretekkel akarja ügyfelét rávenni egy befektetésre, akkor a káprázatos ígéretek és a szép szavak mögött nagy valószínűséggel nincs más, mint csalás. Minden országban törvényi

kötelezettség, hogy a befektető részletes írásbeli tájékoztatást – ún. prospektust – kapjon a felkínált befektetési lehetőség műszaki, gazdasági és jogi sajátosságairól, kockázatairól, valamint a befektetést előkészítő vagy menedzselő szervezetekről és személyekről.

- **Időben állandó hozam ígérete**. Gyanúsnak tekintendő minden olyan befektetési ajánlat, ami az ígéretek szerint csak a befektetett összeg gyarapodását eredményezi, és még válság bekövetkezése esetén sem veszít értékéből. A való életben ugyanis még a legkonzervatívabb befektetéseknél is bekövetkezhet értékcsökkenés.
- **Időnyomás és korlátozott befektetési lehetőség**. A befektetési csalók jellegzetes értékesítési technikája, hogy az általuk kínált kecsegtető befektetési lehetőséggel csak rövid ideig lehet élni, ezzel nyomást gyakorolnak a döntés gyors meghozatalára, megelőzve ezáltal az alapos megfontolás és az utánajárás lehetőségét.

K2. Hogyan kerülhető el, hogy kiberbűnözők áldozatává váljak?

- Mindenekelőtt állandó figyelmet kell fordítani a pénzügyi tranzakciók lebonyolítására használt számítógép, mobiltelefon meg a pénzügyi applikációk jelszavainak a védelmére, továbbá a jelszavakat rendszeres időközönként cserélni is kell. Csak a rendszeres jelszócserével lehet elejét venni annak, hogy az adatbázisok feltörésével megszerzett jelszavakkal rendszeresen jogosulatlanul hatolhassanak be a saját rendszerbe, illetve az esetleg megszerzett jelszavakkal vissza lehessen élni. Az ügyfél által választható jelszavakat pedig úgy indokolt kialakítani, hogy nehéz legyen azokat feltörni. Ennek célszerű módja az, ha a saját jelszót legalább nyolc számjegyből, kis- és nagybetűből és különleges jelből véletlenszerű sorrendben állítjuk elő. Születési dátum, a vezetéknév, illetve ezek jelszóként használt kombinációi, vagy egyszerű számsorok használata viszont elkerülendő, ugyanis ezek gyakorlatilag rövid idő alatt feltörhetők.
- A számítógép és a mobiltelefon alapszoftvereit, köztük az operációs rendszer tűzfal- és vírusirtó programjait rendszeresen frissíteni kell, megnehezítve ezzel idegen személyek behatolását a rendszerbe.
- Pénzügyi applikációt alkalmazni vagy a bankszámlára belépni olyankor, amikor nyilvános – tehát más által is használt – WIFI-hálózaton keresztül valósul meg a csatlakozás az internetre, mindenképpen elkerülendő, mert ilyenkor a bizalmas adatok könnyűszerrel elérhetők idegenek számára is.
- Az internetes vásárlásokhoz célszerű külön bankkártyát igényelni, amin legfeljebb annyi fedezet álljon rendelkezésre, amennyi a vásárlásokhoz szükséges. Rendkívül kockázatos olyan bankkártya adatait megadni ismeretlen webshopoknak, amelyeken megtakarításunk teljes összege elérhető.

- Óvatosnak kell lenni, ha ismeretlen személy próbálja meg telefonon vagy e-mailben felvenni velünk a kapcsolatot. A pénzügyi szolgáltatók és professzionális komoly webhelyek csak a beléptető applikációjukban kérik a jelszó megadását, de személyesen soha; ezért semmilyen ürügy alatt sem szabad megadni azokat még akkor sem, ha azt valamilyen kár megelőzésére hivatkozva kérik. Ismeretlen feladó által ajánlott vagy küldött szoftvert sem szabad szakember általi előzetes biztonsági vizsgálat nélkül feltelepíteni. Ezek ugyanis sokszor olyan trójai vírust telepítenek a számítógépre vagy a mobiltelefonra, amelyek lehetővé teszik jelszavaink ellopását, vagy elérhetetlenné teszik a számítógépen vagy a mobiltelefonon tárolt adatok és programok elérését. Azt is nagyon alaposan meg kell gondolni, hogy a közösségi portálokon kivel milyen információkat osztunk meg, illetve azt, hogy mely webáruháztól történik a rendelés. Ismeretlen webáruházból lehetőleg csak utánvéttel szabad vásárolni.
- Olyan e-mailek vagy SMS-ek, amelyek nagy összegű váratlan nyereményről, illetve ismeretlen személytől származó, nagy örökségről értesítenek, de amelyek felvételéhez bizonyos költségeket előre át kell utalni, vagy saját banki adatokat kell megadni, többnyire csalás kísérletét jelzik, ezért azokra nem szabad válaszolni. Mivel az adathalász e-maileket – még ha azok magyar nyelven érkeznek is – többnyire olyan külföldi bűnözők küldik, akik nem tudnak magyarul, ezért a mail szövegét valamilyen fordítóprogram segítségével ültetik át magyarra. Emiatt pedig érdemes figyelmet szentelni a kapott mailek nyelvezetére is, mert a szokatlan fordulatok és a helyesírási hibák a csalási szándékot valószínűsítik.

K3. Hová fordulhatok digitális visszaélés esetén?

Magyarországon az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény az állami és önkormányzati szervezetek információs rendszerei védelmére a Nemzetbiztonsági Szakszolgálatot (NBSZ) jelölte ki, amelynek szervezetén belül létrehozták a Nemzeti Kibervédelmi Intézetet (NKI).

Milyen esetekben nyújthat segítséget az NKI?

- vírusfertőzés az otthoni elektronikus eszközökön;
- adathalász üzenetek vagy adathalász weboldal észlelése;
- sérülékenység észlelése egy kormányzati weboldalon.

K4. Mit tehetek, ha kiberbűncselekmény áldozatává váltam?

Ha az óvintézkedések ellenére sikerült a bűnözőknek kárt okoznia, akkor nagyon fontos, hogy a bűncselekményt mielőbb bejelentsük a rendőrségen, továbbá – amennyiben a károkozás a bankszámlán, vagy értékpapírszámlán történt – a számlavezető pénzintézetnél is.

A bejelentést a legközelebbi rendőri szervnél kell tenni, mégpedig a megkárosítás észlelése után haladéktalanul, az időnek ugyanis kiemelt jelentősége van a tettes(ek) lefülelése, valamint a kár megtérülése szempontjából.

K5. Internetes csalás elkövetése esetén milyen feltételek mellett köteles a bank a számlatulajdonost kártalanítani?

- Ha a jóvá nem hagyott fizetési művelet teljesítéséért a fizetéskezdeményezési szolgáltatást végző pénzforgalmi szolgáltató a felelős, akkor a fizetési számlát vezető pénzforgalmi szolgáltató a számlatulajdonost – annak kérésére – haladéktalanul kártalanítja a fizető félnek visszatérített összegek következtében elszenvedett veszteségekért és kifizetett összegekért, ideértve a jóvá nem hagyott fizetési művelet összegét is. Ez esetben a fizetéskezdeményezési szolgáltatást végző pénzforgalmi szolgáltatónak kell bizonyítania, hogy – a saját felelősségi körén belül – a fizetési művelet hitelesítése és pontos rögzítése megtörtént, valamint teljesítését az általa nyújtott pénzforgalmi szolgáltatás műszaki hibája vagy üzemzavara nem akadályozta.
- További pénzügyi kártérítést a fizető fél és a pénzforgalmi szolgáltató, vagy adott esetben a fizető fél és a fizetéskezdeményezési szolgáltatást végző pénzforgalmi szolgáltató között létrejött szerződésre alkalmazandó joggal összhangban lehet megállapítani.

K6. Számíthatunk-e kártérítésre a terhünkre elkövetett pénzügyi bűncselekmények tetteseitől?

A bűncselekmény súlyosságától függően a jogkövetkezmények is súlyosak lehetnek. Ez magában foglalhat hosszú szabadságvesztést, nagy összegű pénzbírságot és vagyonelkobzást. Ugyanakkor korántsem biztos, hogy az elkövetőt sikerül elkapni, miként az sem bizonyos, hogy akár eredményes büntetőeljárás keretében sikerül az okozott kár megtérítését elérni. Ilyen esetben megfontolható polgári peres eljárás keretében az elkövetőt kötelezni az okozott kár megtérítésére és sérelemdíj fizetésére is, feltéve persze, hogy az elkövető rendelkezik valamilyen vagyonnal és az igénybe vehető kártérítésre. Az említett bizonytalanságokra tekintettel megfontolandó, hogy a kiberbűnözés által okozható károkra biztosítást is lehet kötni.

A kiberbiztosítás a cascobiztosításhoz hasonló elven működik. Ha egy kiberincidens bekövetkezik, és a számítógépes rendszer leáll vagy megsemmisül, akkor sérülhetnek a vállalkozás eszközei, bevételkiesést szenvedhet el, jelentős mértékű nem várt költséggel vagy bírsággal kell szembenéznie, és nem utolsó sorban az incidens során másnak okozott kárért is helyt kell állnia. Példa erre egy zsarolóvírus bejutása a számítástechnikai rendszerbe, aminek következtében értékes ügyféladatok kerülhetnek illetéktelen kezekbe. Az adatvédelmi felelősség (GDPR) kapcsán egyértelmű, hogy a probléma elsősorban nem informatikai jellegű, hanem gazdasági természetű.

A kiberfelelősség-biztosítás, más néven kiberbiztosítás olyan biztosítási kötvény, amelyet egyéni vállalkozók vagy vállalkozások vásárolnak, hogy megvédjék magukat a kibertámadások által okozott pénzügyi károktól. A biztosítás a helyreállítás pénzügyi szempontjaira összpontosítva segít csökkenteni a kibertámadásból eredő üzleti zavarok hatását. A kiberfelelősség-biztosítás segít fedezni továbbá a szervezetnél a kibertámadás miatt felmerülő különféle költségeket, például az adat-helyreállítással, a jogi segítségnyújtással és az ügyfelek visszaszerzésével kapcsolatos költségeket (Sebők, 2022).

8. ÖSSZEGZÉS ÉS KÖVETKEZTETÉSEK

E tanulmány didaktikai szándékból született, azzal a céllal, hogy olvasói előtt feltárja a kiberbűnözés fő kockázatait és jellegzetességeit. Áttekintette a kiberbűnözés megjelenésének és elterjedésének elsődleges okait, valamint főbb statisztikai adatait. Bemutatta azokat az személyiségtípusokat, akik a leginkább kitettek a kibertérben jelentkező pénzügyi kockázatoknak/csalásoknak, egyszersmind rendszerezte a pénzügyi bűncselekmények főbb típusait. Ezt követően ahhoz kívánt érdemi segítséget nyújtani, hogy felismerhetővé váljon a pénzügyi csalás veszélye. Az áttekintéssel és a rendszerezéssel az elsődleges célunk a pénzügyi tudatosság fejlesztésével foglalkozó személyek kiberbűnözéssel kapcsolatos ismereteinek az elmélyítése volt. A szerzők reménye szerint a cikk hozzájárulhat ahhoz, hogy a jövőben jobban lehessen azonosítani az online térben leselkedő veszélyeket, meghozni a védekezés legfontosabb intézkedéseit, illetve felhívni a figyelmet a pénzügyek digitalizációja következtében megjelenő új kockázatokra is. Az aktív „felhasználói" részvétel a kiberbűnözés elleni küzdelemben nem maradhat eseti jellegű, hanem folyamatos szerepvállalást igényel. Ennek az a fő oka, hogy a szabályozói környezet sok esetben csak késéssel tudja érdemben követni a digitális pénzügyek területén zajló változásokat, miközben a bűnözők sokszor akár több lépéssel is a szabályozói környezet és a hatóságok előtt járhatnak. Ezért sem lehet elégszer hangsúlyozni, hogy az erős kiberbiztonság megteremtésének nélkülöz-

hetetlen, egyszersmind elengedhetetlen feltétele a felhasználók aktív egyéni szerepvállalása; az ahhoz szükséges felkészültséget pedig a pénzügyi tudatosság és ismeretek növelésével érhetik el.

HIVATKOZÁSOK

AAG (2023): The Latest 2023 Cyber Crime Statistics (updated December 2023), https://aag-it.com/the-latest-cyber-crime-statistics/ (letöltve: 2023.12.06.).

Alexander, E. – Seymour, A. (1998): *Roles, Rights, and Responsibilities: A Handbook for Fraud Victims Participating in the Federal Criminal Justice System*. Washington: Police Executive Forum.

Croall, H. (2009): White collar crime, consumers and victimisation. *Crime, Law and Social Change*, 51(1), 127–146.

Davies, P. – Francis, P. – Jupp, V. (eds.) (2003): *Victimology: Theory, Research and Policy*. New York: Palgrave Macmillan.

Katona, Cs. (2021): Kiberbűnözés Magyarországon, avagy hová forduljon digitális bűncselekmény esetén? *Arsboni*, 2021.11.02., https://arsboni.hu/kiberbunozes-magyarorszagon-avagy-hova-forduljon-digitalis-buncselekmeny-eseten/ (letöltve: 2023.12.09.).

Van Dijk, J. J. M. (1999): Introducing victimology. In: van Dijk, J. J. M. – van Kaam, R. G. H. – Wemmers, J. (eds.) (1999): *Caring for crime victims*. Monsey: Criminal Justice Press, 1–12.

Dunn, P. (2007): Matching service delivery to need. In: Walklate, S. (ed.): *Handbook of Victims and Victimology*. Abingdon, UK: Routledge, 255–281.

Fattah, E. A. (1991): *Understanding criminal victimisation*. Scarborough: Prentice Hall Canada.

Financial Conduct Authority (FCA) (2016): Over 55s at heightened risk of fraud, says FCA. Press Release, https://www.fca.org.uk/news/press-releases/over-55s-heightened-risk-fraud-says-fca (letöltve: 2023.12.04.).

Financial Industry Regulatory Authority (FINRA) (2016): FINRA risk meter. https://www.finra.org/investors/tools-and-calculators (letöltve: 2023.09.14.).

Ganzini, L. – McFarland, B. – Bloom, J. (1990): Victims of fraud: Comparing victims of white collar and violent crime. *Bull Am. Acad. Psychiatry Law*, 18(1), 55–63.

Goucher, W. (2010): Becoming a cybercrime victim. *Computer Fraud and Security*, 10, 16–18.

Grund, B. (2021): A kibertér bűncselekményeiről és a kiberbűnözés hazai gyakorlatáról. *MTA Law Working Papers*, 21, https://docplayer.hu/235743259-A-kiberter-buncselekmenyeirol-es-a-kiberbunozes-hazai-gyakorlatarol.html.

Harvey, S. – Kerr, J. – Keeble, J. – McNaughton Nicholls, C. (2014): Understanding victims of financial crime: A qualitative study with people affected by investment fraud. NatCen, Financial Conduct Authority. http://www.fca.org.uk/static/documents/research/qual-study-understanding-victims-investment-fraud.pdf (letöltve: 2023.10.16.)

Von Hentig, H. (1948): *The criminal and his victim*. New Haven: Yale University Press.

ITU (2023): Global Cybersecurity Index 2020, https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Krasznay, Cs. (2021): Húsz év a globális kiberbűnözés elleni küzdelemben – A Budapesti Egyezmény értékelése. *Külügyi Szemle*, 1, https://www.academia.edu/49598305/H%C3%BAsz_%C3%A9v_a_glob%C3%A1lis_kiberb%C5%B1n%C3%B6z%C3%A9s_elleni_k%C3%BCzdelemben_A_Budapesti_Egyezm%C3%A9ny_%C3%A9rt%C3%A9kel%C3%A9se.

Lajtár, I. (2019): A kiberbűnözésről. *Ügyészek Lapja,* 1, https://ugyeszeklapja.hu/?p=774.

Langenderfer, J. – Shimp, T. A. (2001): Consumer vulnerability to scams, swindles, and fraud: A new theory of visceral influences on persuasion. *Psychology & Marketing*, 18(7), 763–783. https://doi.org/10.1002/mar.1029

Lyng, S. (2005): Edgework and the risk-taking experience. In: Lyng, S. (ed.) (2005): *Edgework: The sociology of risk-taking* New York and London: Routledge,17–49.

Neue Zürcher Zeitung (NZZ) (2022): Interpol sieht Finanz-Straftaten und Cyberkriminalität als weltweit grösste Bedrohungen an. https://www.nzz.ch/panorama/interpol-sieht-finanz-straftaten-und-cyberkriminalitaet-als-weltweit-groesste-bedrohungen-an-ld.1708027 (letöltve: 2023.09.04.).

Orbán, A. (2023) Közszolgálati Online Lexikon. Nemzeti Közszolgálati Egyetem, https://lexikon.uni-nke.hu/szocikk/szamitogepes-bunozes/ (letöltve: 2023.10.20.).

Poletaeva, V. – Perepelitsa, D. – Arhangelskaya, T. – Zaripov, I. – Pásztor, Sz. (2019): The research task of banks and authorized government institution interests in manufacturing companies' investment projects congruence. *International Journal of Mechanical Engineering and Technology*, 10(2), 1603–1609.

Pásztor, Sz. (2018): Future of Commercial Banks – Survival or Failure? *Izvestiya*, Mezhdunarodnyy teoreticheskiy i nauchno-prakticheskiy zhurnal 23(4), 71–88.

Pásztor, Sz. – Szijártó, N. (2016): Internal Devaluation and its Macroeconomic Consequences in the EU Periphery. *International Trade and Trade Policy*, 4(8), 6–23.

Petty, R. E. – Cacioppo, J. T. (1981): *Attitudes and Persuasion: classic and Contemporary Approaches*. W.C. Brown Company Publishers.

Sebők, A. (2022): Kiberbiztosítás: Ezért van rá szüksége. MWT Solutions, 22.10.08., https://mwtsolutions.eu/hu/cikk/kiberbiztositas-ezert-van-ra-szuksege/.

Shichor, D. – Shechrest, D. K. – Doocy, J. (2001): Victims of investment fraud. In: Pontell, H. N. – Shichor, D. (eds.) (2001): *Contemporary issues in crime and criminal justice: Essay in honour of Gilbert Geis*. Upper Saddle River: Prentice Hall, 81–96.

Shivaraj, S. (2023): Financial-crime: Understanding its Growth, Threat and Effects. *The Dope*, 2023.03.03., https://thedope.news/financial-crime-understanding-its-growth-threat-and-effects (letöltve: 2023.12.01.).

Statista (2023): Estimated cost of cybercrime worldwide 2017-2028 (in trillion U.S. dollars) https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwid.

Surfshark (2023): Cybercrime statistics. https://surfshark.com/research/data-breach-impact/statistics (letöltve: 2023.12.06.).

Szóka, K. (2021): A pénzügyi kultúra és tudatosság meghatározása és magyarországi helyzete. *Economica*, 12(3-4), https://doi.org/10.47282/economica/2021/12/3-4/10417.

Terták, E. – Kovács, L. (2023): Fókuszban a pénzügyi biztonság kibertérben is – Pénz7, *Gazdaság és Pénzügy*, 10(1), 5–20., http://real.mtak.hu/163412/1/005-020TertakKovacs.pdf.

United States Department of Justice (US DoJ) (2015): Financial fraud crime victims. https://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud (letöltve: 2023.11.11.).

Varga, Á. (2022): Az információs rendszerek megsértésének esetei, motivációi és szabályozási perspektívái, https://www.hte.hu/documents/10180/4737479/Az_informacios_rendszerek_megsertesenek_esetei_motivacioi_es_szabalyozasi_perspektivai.pdf

Walklate, S. (2017): *Handbook of Victims and Victimology*. 2nd Edition, New York,London: Routledge.

Weisburd, D. – Wheeler, S. – Waring, E. – Bode, N. (1994): *Crimes of the Middle Classes: White Collar Offenders in the Federal Courts* (Yale Studies on White-Collar Crime Series): New Haven: Yale University Press.