ACTA Universitatis, Sectio Paedagogica, Tom. XLVI. *pp. 101–130*

Kenyeres Attila Zoltán

KOMPLEX PEDAGÓGIAI ÉS KUTATÁSI MÓDSZER A FIATALOK MÉDIATUDATOSSÁGÁNAK NÖVELÉSÉRE – A MÉDIA DETEKTÍV FIATALOKNAK PROGRAM JÓGYAKORLATA

Az álhírek, adathalász csalások és hamis nyereményjátékok

Az álhírek létezése egyidős az emberiséggel. Ebben a tanulmányban kifejezetten az interneten és hangsúlyosan a közösségi médiában terjedő álhírek kapcsán kialakítandó médiaműveltségre koncentrálunk. Ezek az álhírek a korábban főképp csak szóban vagy írásban terjedő hamis információkhoz képest egy új, digitális álhírtípust jelenítenek meg. Gaughan úgy definiálja az álhíreket, hogy azok igaz, valós híreknek álcázott valótlan állítások (Gaughan, 2017). Walters úgy véli, hogy az álhír *„a) olyan tartalom, amely híranyagnak mutatja magát, b) objektíve hamis állításokat tesz adott események megtörténtéről, c) lényegét tekintve hamis módon"* (Walters, 2018: 142). Mindezek alapján elmondható, hogy az álhírek *„olyan hírcikkek, amelyek szándékosan és bizonyíthatóan hamisak, és félrevezethetik az olvasókat"* (Allcott – Gentzkow, 2017: 213), amelyeket jellemzően az interneten és a közösségi médiában terjesztenek (Allcott – Gentzkow, 2017). Veszelszki is átveszi ezt a definíciót az álhírek tágabb értelmezéséhez, azonban ő leszűkíti az álhírek körét, hangsúlyozva a pénzügyi haszonszerzésre törekvést és a hiteles újságírás látszatának megteremtését. Az álhírekkel kapcsolatos fogalmak közé sorolja a különböző internetes csalásokat (spamek, adathalászat, hoax, klikkvadászat), a hírparódiát és a propagandát (Veszelszki, 2017). Royster úgy definiálja az álhíreket, mint *„valódi hírek álruhájában online közzétett pontatlan cikkek, amelyek létrehozásakor nem törődnek azzal, hogy igaz-e, vagy sem"* (Royster, 2017: 276). Klein és Wueller már a szándékosságot is kihangsúlyozzák az álhírek kapcsán, amikor az álhíreket úgy definiálják, mint *„hamis tényállítások szándékos vagy tudatos online közzétételét"* (Klein – Wueller, 2017: 6). Az álhíreket Krekó a dezinformáció fogalomkörébe sorolja, amelyet ő szándékos megvezetési céllal alkalmazott manipulációs technikák köreként azonosít (Krekó, 2018). Filipec a dezinformációt hamis információk szisztematikus és szándékos terjesztéseként írja le, amely főként állami szereplők vagy azok leányvállalatai által történik valamely külföldi állammal vagy médiummal szemben. A dezinformáció fő célja a döntéshozók

https://doi.org/10.46436/ActaUnivEszterhazyPaedagogica.2025.101

véleményének befolyásolása (Filipec, 2019). A hamis információk egy része kifejezetten felhasználó készítette tartalom, amellyel kapcsolatban Gelencsér és Szűts azt állapítják meg, hogy az internet és a közösségi média a média történetében addig soha nem látott ideális technikai feltételeket teremtett arra, hogy amatőrök is véleményt nyilváníthassanak, nyilvánosan „okoskodjanak" (Gelencsér – Szűts, 2020), aminek eredménye lehet a téves információk terjedése is.

Az internetalapú újmédia, benne a közösségimédia-eszközök tehát az emberiség történetében még soha nem látott mennyiségben, soha nem látott gyorsasággal képesek korábban elérhetetlen mennyiségű tömegekhez eljuttatni az álhíreket és egyéb félrevezetéseket. Ezek felismerése pedig egyre komplexebb eljárásokat igényel, ahogy átalakul ezek modalitási spektruma. Az infokommunikációs technológia elsőként a nyelvi létmódokat (a beszédet és az írást) duplázta meg, létrehozva ezek internetes alternánsait (a másodlagos szóbeliséget és írásbeliséget), kialakítva a szövegek/műfajok módosult vagy átmeneti mediális változatait, amelyet Balázs intermedialitásnak nevezett (Balázs, 2015). Az átalakulás része a hypertextualitás, a multimedialitás és az interaktivitás megjelenése is (Szűts, 2018). A multimedialitás az álhírek relációjában azt eredményezte, hogy a korábban főként csak szóban és/vagy írásban terjedő, unimodális álhírek helyett és mellett az interneten multimodálissá váltak az álhírek: a szöveg mellett megjelentek a vizuális és hangalapú modalitások is: a videók, a képek és a hangok. Mindez nehezíti a detektálásukat (Nirav Shah – Ganatra, 2022). Az interneten terjedő, immár többféle modalitást is magában foglaló álhírek azonosításához így multimodális megközelítésre van szükség, amely figyelembe veszi és kombinálja a különböző modális kategóriákból származó információkat. A multimodális álhírfelismerési stratégia már figyelembe veszi a szöveget, a társadalmi jellemzőket (például a felhasználók reakciói), a hangot, a videót, a képeket, a hírt közlő forrás és az azt továbbító felhasználó tulajdonságait, valamint a hír hálózati és terjedési jellemzőit is (Comito és mtsai., 2023).

Az álhírekhez hasonlóan az adathalászat sem új jelenség. Volkamer és társai szerint ez egy évszázadok óta alkalmazott, a bizalom megszerzésén és kihasználásán alapuló trükk modern megfelelője: valakinek a megtévesztése valamilyen személyes előny megszerzése érdekében (Volkamer és mtsai., 2017). Az adathalászat e-mailes verziójában olyan rosszindulatú szándékkal küldött e-maileket alkalmaznak az elkövetők, amelyekkel a címzetteket megpróbálják rávenni arra, hogy információkat vagy hozzáférést adjanak meg a feladónak. A feladó általában legitim szervezetnek adja ki magát, és az e-mailt úgy állítja össze, hogy megpróbálja rávenni a felhasználót egy művelet elvégzésére. Ez a művelet magában foglalhatja érzékeny személyes adatok (pl. jelszavak) felfedését és/vagy a számítógéphez vagy hálózathoz való véletlen hozzáférés biztosítását (pl. rosszindulatú szoftverek telepítésével) (Butavicius és mtsai., 2016). Az adathalászat folyamata tehát két fő részből áll: az elkövetők egyrészt pszichológiai befolyásolást (social engineering) alkalmaznak a felhasználók

bizalmának megszerzésére, másrészt mindezt valamilyen technikai eszköz, technikai trükk felhasználásával teszik. A céljuk a felhasználók különböző, magánjellegű adatainak megszerzése. Általában egy kiválasztott szervezet oldalára megtévesztésig hasonlító weboldalra csalják a címzettet, ahol érzékeny személyes adatok megadására bírják (Yang és mtsai., 2022; Butavicius és mtsai., 2022; Basit és mtsai., 2021). Az adathalászatra a nemzetközi szakirodalom – és a hétköznapi nyelv is – a „phishing" kifejezést használja, amely a password (jelszó) és a fishing (halászat) angol szavak összevonásából jött létre, arra utalva, hogy a csalók a felhasználók jelszavait próbálják meg „elhalászni" különféle trükkökkel (Wright és mtsai., 2016). Más szerzők a telefonos csalásokra vezetik vissza a kifejezés eredetét arra utalva, hogy kezdetben az adathalász támadásokat telefonhálózatokon hajtották végre, amelyeket az angolban „Phone Phreaking"-nek neveztek. Emiatt váltotta fel a „Fishing" kifejezést a „Phishing" kifejezés, és lett az első „f" betűből „ph". A phishing a kibertámadások egyik fajtája is lehet. A kibertámadások olyan rosszindulatú digitális platformon történő kísérletek, amelyek célja bizalmas szervezeti vagy személyes adatokat tartalmazó rendszerek feltörése vagy ilyen adatok ellopása, megrongálása (Basit és mtsai., 2021). A megtévesztésen és a bizalom megszerzésén alapuló trükköknek nemcsak a személyes adatok ellopása lehet a célja, hanem a közvetlen pénzszerzés is (Chaudhry és mtsai., 2016). Ezek egyik formája, amikor a feladó a címzett bajba jutott rokonának, barátjának adja ki magát, és pénz átutalását próbálja elérni (Hong 2012), illetve ennek tipikus formáját jelentik a kifejezetten az időseket megcélzó, a köznyelvben „unokázós csalás" néven ismert telefonos átverési kísérletek is. Lehetséges, hogy az elkövető más módon próbál az áldozat bizalmába férkőzni (például társkeresőként), majd a bizalom kiépítése után különböző ürüggyel próbál pénzt kicsalni tőle.

A hamis nyereményjátékok általában a közösségimédia-felületeken terjednek posztok vagy továbbított chatüzenetek formájában. Jellemzően két fajtájuk van: az egyik kategória egy relatíve ártalmatlan átverés, amelynek célja, hogy egy közösségimédia-oldal minél több követőt és/vagy lájkolót szerezzen. Ennek érdekében vagy egy nagy értékű nyereményt (pl. egy értékes autót) kínálnak fel sorsolásra a posztot megosztó közösségi oldalt lájkolók és a posztot tovább osztók között. Sorsolás valójában nem történik, hiszen nyeremény sincs. A másik fajtája, amikor egy létező, megbízható cégnek (például egy üzletlánc) adja ki magát a közösségimédia-oldal az ő nevüket és dizájnjukat felhasználva (pl. egy üzletlánc rajongói oldala), és kínál fel nyereményt az oldalt lájkolók és a posztot megosztók között. Vagy ugyanezen logika mentén egy drága terméket kínál nagyon olcsón, mintha az adott cég leértékelte volna az árut például „készletkisöprés" címén. Egy harmadik kategóriát a kifejezetten adathalász célú hamis nyereményjátékok képeznek. Ebben az esetben is ismert, jónevű cégek és márkák képviselőinek adják ki magukat a csalók, az ő nevüket és dizájnjukat használják fel. Nyereményjátékot hirdetnek a nevükben, a játékban való

részvételhez pedig egy linkre kell kattintani, és innentől már az adathalászat működési mechanizmusai lépnek életbe: vagy egyből érzékeny banki adatokat kell megadni, vagy első körben egy könnyű rejtvényt kell megoldani, vagy válaszolni néhány nagyon könnyű kérdésre (például, hogy ismeri-e az illető az adott céget, szokott-e tőlük vásárolni stb.), majd ezt követően vezeti az áldozatot az adatokat kérő oldalra (függetlenül attól, hogy a kérdésekre helyesen válaszolt-e, vagy sem).

Stratégiák a dezinformáció és az álhírek hatásának mérséklésére

A szakirodalomban jellemzően négy stratégiát vázolnak fel a dezinformáció és az álhírek hatásainak csökkentésére:

1. Tényellenőrzési mechanizmusok: például fact checker weboldalak és szolgáltatások működtetése (Bodaghi és mtsai., 2024; Tufchi és mtsai., 2023). Ide tartozik a tényellenőrző videók készítése is (Lu–Shen, 2023).
2. Figyelmeztetések alkalmazása: amikor különböző minősítő és figyelmeztető jelölésekkel, ikonokkal, szöveges figyelmeztetéssel látják el a közösségimédia-posztokat és/vagy azok forrását, amelyek az információ valóságtartalmának átgondolására ösztönöznek (Bryanov – Vziatysheva, 2021; Kim és mtsai., 2023). Kim és társai ezzel kapcsolatban azt állapították meg, hogy a negatív (a hírforrás megbízhatatlanságára utaló) ikonoknak nagyobb hatásuk volt, így ezek feltüntetése csökkentette a cikkek vélt hitelességét, viszont a hírforrás megbízhatóságát jelző pozitív ikonoknak nem volt szignifikáns hatásuk, ezekre a felhasználók kevés figyelmet fordítottak (Kim és mtsai., 2023).
3. Algoritmusalapú stratégiák: különböző automatizált modellek végzik az álhírek felismerését, gépi tanulási és mélytanulási algoritmusokat alkalmazva (Babaei és mtsai., 2022; Nirav Shah – Ganatra, 2022; Pszona és mtsai., 2023; Tufchi és mtsai., 2023; Hosseini és mtsai., 2023; Comito és mtsai., 2023).
4. A felhasználó-központú stratégiák: a legtöbb stratégia a felhasználók médiaműveltségének fejlesztésére irányuló módszereket foglal magában (Luo és mtsai., 2022). Ilyen módszer lehet az úgynevezett oldalirányú (laterális) olvasás készségének elsajátítása is, amely során a felhasználó egy gyors átvizsgálás után elhagy egy (kétes) oldalt, hogy ellenőrizze, mit írnak az információról más megbízható digitális források. Ezzel szemben a vertikális olvasás során az egyén kizárólag a weboldalon belüli hírtartalomra összpontosít (Fendt és mtsai., 2023). Az álhírekkel, dezinformálással és egyéb félrevezetésekkel terhelt digitális környezetben egyre fontosabb a médiaműveltség kialakítása az egyén számára. Ahogy Bulger és Davison fogalmaz: a médiaműveltség az álhírekkel szembeni fellépés súlypontjává vált (Bulger – Davison, 2018).

A médiaműveltség és annak szerepe

A felhasználó-központú stratégiák közül az egyik legelterjedtebb az egyének médiaműveltségének fejlesztése. A médiaműveltség alapkoncepciója abból indul ki, hogy különbség van a létező valóság és annak a médiában történő reprezentációja között (Hobbs – Frost, 2003; Chen és mtsai., 2011; Ashley és mtsai., 2013; Maksl és mtsai., 2015). A médiaműveltség egyik legkorábbi írott definícióját Aufderheide és Firestone adta, akik szerint ez *„az állampolgár képessége az információhoz való hozzáférésre, az információ analizálására és előállítására meghatározott eredmények elérése érdekében"* (Aufderheide – Firestone, 1993: 6).

A médiaműveltséggel foglalkozó szakirodalom többsége a fenti definíciót alapul véve 4 fő készséget sorol fel ennek relációjában: 1. az üzenetekhez való hozzáférés készsége; 2. az üzenetek elemzésének készsége; 3. az üzenetek értékelésének készsége; 4. a médián keresztül továbbított üzenetek létrehozásának készsége (lásd: Hobbs – Frost, 2003; Livingstone, 2004; Duran és mtsai., 2008; Ashley és mtsai., 2013; Ashley és mtsai., 2010; Fleming, 2014; Vraga és mtsai., 2015). Más kutatók ezeken belül egyéb alképességet említenek: ilyen a médium/hírforrás megbízhatóságának, hitelességének értékelése; az információforrás kompetenciaszintjének kiértékelése (Ashley és mtsai., 2010); az elfogultságok érzékelése (Ashley és mtsai., 2010; Koc – Barut, 2016). Ugyancsak fontos a médiatermékek létrejöttét befolyásoló társadalmi, gazdasági és politikai környezet átlátásának képessége (Duran és mtsai., 2008; Ashley és mtsai., 2010; Fleming, 2014; Ashley és mtsai., 2013; Chu – Lee, 2014), valamint a médiatartalommal szembeni kritikai attitűd megléte (Hobbs – Frost, 2003; Mihailidis, 2009; Potter, 2010; Ashley és mtsai., 2010; Maksl és mtsai., 2015; McLean és mtsai., 2016; Bulger – Davison, 2018). Szintén lényeges, hogy az egyén felismerje a médiaüzenetek céljait, a célközönséget, az üzenet nézőpontját, a médiatartalom szerkesztési technikáit, valamint beazonosítsa a hírmédia adásaiból kihagyott információkat is (Hobbs – Frost, 2003; Duran és mtsai., 2008). Fontos tisztában lenni a média „hatalmával" és a médiaüzenetek hatásaival, valamint tudni kell különbséget tenni az irónia a valóság között is (Koc – Barut, 2016). Más kutatók szerint szükséges a médiarendszerrel és a médiatermékekkel szembeni bizonyos szintű szkepticizmus is (Ashley és mtsai., 2010; Maksl és mtsai., 2015). Duran és társai szerint egy médiaműveltséggel rendelkező személy a következő dolgokat érti meg: *„milyen meggyőző üzenetek találhatók a médiában; miért úgy néznek ki, hangzanak és olvashatók a médiaüzenetek, ahogyan; ki hozza létre ezeket az üzeneteket és ki profitál belőlük; mikor hat ránk a média; hol találhatnak alternatív médiát, és hogyan tehetnek valamit aktívan a médiarendszer megváltoztatásáért."* (Duran és mtsai., 2008: 51)

A fenti premisszákból kiindulva Potter szerint a médiaműveltség legfontosabb funkciója, hogy segíti az egyént megvédeni a médiából származó tartalom potenciálisan negatív hatásaitól (Potter, 2010). Mihailidis szerint a médiaműveltség birtokában az egyén felismeri

a média meggyőzésre, manipulációra, befolyásolásra és ellenőrzésre irányuló kísérleteit (Mihailidis, 2009). Lin és társai is ezt hangsúlyozzák, szerintük a kritikus médiafogyasztó képes a manipuláció és az elfogultságok felismerésére (Lin és mtsai., 2013).

A médiaműveltség fogalma a technológia fejlődésével bővül, így a hagyományos (nyomtatott és audiovizuális) médián túl manapság már az internetre és más új médiumokra is kiterjed (Livingstone, 2004). Chen és társai már kifejezetten az internetalapú újmédia kapcsán említik az „újmédia-műveltség" mint alkategória fogalmát, amely a 21. századi médiakörnyezet kihívásaihoz igazodik. Ez a fogalom szerintük 4 komponensből áll: 1. Funkcionális fogyasztás: hozzáférés a médiatartalomhoz, a szöveges jelentés megértése; 2. Kritikus fogyasztás: a médiatartalmak szociokulturális, politikai és gazdasági következményeinek elemzése, kérdések felvetése a médiaüzenetek céljai, mögöttes ideológiái, társadalmi értékei és a hatalom reprezentációja kapcsán; 3. Funkcionális előállítás: az újmédia-tartalmak előállítása különböző médiaplatformokon; 4. Kritikus előállítás: saját meggyőződés közvetítése, megtárgyalás mások elképzeléseivel, a várható hatások mérlegelése (Chen és mtsai., 2011). Lee ugyancsak a digitális újmédia kapcsán tárgyalja a „digitális médiaműveltség" fogalmát, amelynek kifejlesztése segíti az egyént abban, hogy megértse az internetes fenyegetéseket, mint a félretájékoztatás, vagy az olyan kiberbűnözési formákat, mint az adathalászat, illetve jobban ki tudja értékelni az interneten terjedő információkat és azok forrásait (Lee, 2018).

Egyéb médiaműveltségi alkategóriák is léteznek a szakirodalomban:

- számítógépes műveltség: amely a digitális média technikai karakterisztikáira referál, a számítógépes programok használatával kapcsolatos (Chen és mtsai., 2011; Livingstone, 2004);
- információs műveltség: jártasság az internet használatában, az online információk típusainak és formátumainak ismerete, azok kritikai analízise és értékelése, a kritikus online tartalomfogyasztás (Chen és mtsai., 2011; Ashley és mtsai., 2013); más meghatározás szerint az információs műveltség az információ megértésének, megtalálásának, értékelésének és felhasználásának intellektuális keretrendszere (Boh Podgornik és mtsai., 2016; Jones-Jang és mtsai., 2021);
- digitális műveltség: a digitális eszközökön történő feladatvégrehajtás és problémamegoldás készségei (Reddy és mtsai., 2020), minden, az online digitális média és a közösségi média használatához szükséges készség beletartozik ebbe a körbe (Jones-Jang és mtsai., 2021);
- internetműveltség (Livingstone, 2004).

A médiaműveltség tehát egy átfogó, egyfajta „ernyőfogalom", amely többféle műveltséget és készséget magában foglal, több alkategóriája is létezik. Összességében bármilyen

platformról származó médiatartalom kritikus elemzésének, értékelésének, felelősségteljes felhasználásának és előállításának képességét jelenti, amelyhez a médiarendszer és a társadalom működésével kapcsolatos valós ismeretek is társulnak.

A médiaműveltség hatása az álhírek felismerésére

Az egyén médiaműveltségének fejlesztése lehet az egyik legfontosabb pedagógiai módszer az álhírek és egyéb átverések kivédése érdekében. Azonban a kutatások vegyes képet mutatnak a különböző médiaműveltségi képzések gyakorlati hatásossága kapcsán. Jones-Jang és társai 1299 amerikai állampolgár bevonásával végeztek kutatást. Önbevallás alapján mérték meg a résztvevők média-, információs, hír- és digitális műveltségi szintjét, majd 10 darab, közösségi médiából származó posztról készült képernyőmentésről kellett eldönteniük, hogy igazak-e vagy hamisak. A 10 hírből 4 igaz volt, 6 álhír. Az eredményeik szerint egyedül az információs műveltség megléte növelte az álhírek felismerési valószínűségét. A kutatók az önbevalláson alapuló műveltségi skálák hátrányaira is rámutattak, amelyek nem feltétlenül adnak valós képet a résztvevők tényleges álhírfelismerő képességeiről (Jones-Jang és mtsai., 2021). Orhan 157 törökországi egyetemista körében végzett kutatása csak mérsékelt pozitív kapcsolatot tárt fel a magas kritikai gondolkodás és újmédia-műveltségi szint, valamint az álhírek észlelési képessége között. Elsőként a Sosu által kifejlesztett kritikai gondolkodási diszpozíciók skálát (CTDS), valamint az újmédia-műveltségi skálát (NMLS) alkalmazták. Majd a résztvevőknek 6 darab közösségimédia-posztról készült képernyőmentés kapcsán kellett 5 fokozatú Likert-skálán értékelniük a megbízhatóságra vonatkozó állításokat. A 6 képernyőmentésből 3 igaz, 3 hamis hírről szóló poszt volt. Eredményei szerint a kritikai gondolkodásra való hajlam és az újmédia-műveltség megléte jelezte szignifikánsan előre az álhírek közösségi médiában való észlelését a vizsgált egyetemisták között. Ugyanakkor azt tapasztalta, hogy a kritikai gondolkodás nagyobb hatást gyakorolt az álhírek felismerésére, mint az újmédia-műveltség (Orhan, 2023). Fendt és társai a laterális olvasás gyakorlati hatását vizsgálták 312 tanár szakos egyetemista körében. Arra jutottak, hogy a laterális olvasás szignifikáns javulást eredményezett az álhírek felismerésében, ugyanakkor a megbízható hírforrások értékelését nem befolyásolta jelentősen (Fendt és mtsai., 2023). Luo és társai tajvani egyetemisták körében végzett kutatása csak kevés empirikus bizonyítékot talált arra, hogy az újmédia-műveltség pozitív szerepet játszik az álhírek felismerésében. Ugyanakkor a kutatás csak önbevalláson alapult, a kutatók a gyakorlatban nem tesztelték a diákok képességeit (Luo és mtsai., 2022). Appel és Prietzel az analitikus gondolkodás szerepét vizsgálta politikai tartalmú deepfake videók felismerésében. Azt találták, hogy az analitikusan gondolkodók (rendszeresen és automatikusan reflektálnak

a látott információkra) nagyobb valószínűséggel azonosították helyesen a deepfake-eket, mint azok, akik kevésbé reflektívek, inkább intuitívak voltak (Appel and Prietzel, 2022).

Más kutatók olyan kísérletek eredményeit mutatják be, amelyek az előzetes ismeretek és e-mailekkel kapcsolatos tapasztalatok szignifikáns szerepét mutatták ki az adathalász csalások felismerésében (Harrison és mtsai., 2016). Ezek elsősorban számítógépes ismereteket, hálózati biztonsággal kapcsolatos ismereteket, hálózat- és e-mailhasználati tapasztalatokat, a pszichológiai manipulációval kapcsolatos ismereteket jelentenek. Megállapítják, hogy az adathalászattal járó kockázatok csökkentésében fontos beavatkozási eszköz lehet az egyének ismereteinek és tapasztalatának növelése (Yang és mtsai., 2022). Ugyanakkor az erre vonatkozó eddigi kutatások azt találták, hogy a felhasználók adathalászattal kapcsolatos speciális oktatása csak általánosságban és átmenetileg teszi őket gyanakvóbbá. Jackson és munkatársai 27 fő bevonásával végzett kísérletében a résztvevőknek webhelyek valódiságát kellett megítélniük. A résztvevők egyik csoportja részletes tájékoztatást kapott a csalásra utaló jelekről, illetve a böngésző „súgó" fájljában is el kellett olvasniuk a biztonságról szóló részt. Egy másik csoport csak részleges tájékoztatást kapott, illetve kijelöltek egy kontrollcsoportot is. Az eredmények vegyes képet mutattak: a teljes körű képzésben részesült csoport bizonyos webhelyek és csalási formák esetén jobb, mások esetében ugyanakkor rosszabb eredményt ért el a kontrollcsoporthoz képest. A teljes körű képzést kapott csoport tagjai nagyobb valószínűséggel minősítették legitimnek mind a valódi, mind a hamisított oldalakat, amikor a böngésző adathalászatot jelző figyelmeztetése nem jelent meg (Jackson és mtsai., 2007). Anandpara és munkatársai 40 embert vontak be egy adathalászatról szóló képzésbe, majd úgynevezett „adathalász IQ"-tesztet végeztettek velük. Az eredmények szerint az adathalász-oktatás egyetlen mérhető hatása (az „adathalász IQ"-teszt szempontjából) az aggodalom növekedése volt – nem pedig a képességek növekedése. A képzés tehát csak növelte a résztvevők gyanakvását anélkül, hogy fejlesztette volna a képességüket (Anandpara és mtsai., 2007). Harrison és társainak kutatása azt mutatta ki, hogy azok, akik jobban odafigyelnek egy adathalász e-mailre, nem feltétlenül hoznak helyes döntést annak valódiságáról. Ennek oka szerintük, hogy túl sok elemet mérlegelnek. Ezért azt javasolják, hogy az adathalászat elleni erőfeszítések során a felhasználókat arra kell megtanítani, hogy csak néhány kulcsfontosságú elemre figyeljenek az üzenetben. Ilyen például az e-mail valódi feladójának megtalálási módja, illetve a hiperhivatkozások alapos vizsgálata. Bár a helyesírási és nyelvtani hibák is fontos jelek, ezek keresése elvonhatja a figyelmet a fontosabb jelekről (Harrison és mtsai., 2016). Parsons és munkatársai 117 fő bevonásával végzett kísérletükben arra jutottak, hogy azok a résztvevők, akik előzőleg informatikai/technológiai kurzuson vettek részt, összességében rosszabbul teljesítettek az adathalász e-mailek felismerésében. Fontos tanulság lehet a képzési és oktatási programokra nézve, hogy jobban teljesítettek a teszten azok, akiknek előre jelezték, hogy a teszten kifejezetten az adathalászatot felismerő képességeket mérik. A kontrollcsoport, aki erről nem tudott, rosszabbul teljesített

(Parsons és mtsai., 2013). A bemutatott kísérletek tehát vegyes képet mutatnak: egyes kutatók szerint hatékonyak a felhasználók képességeit fejlesztő képzések, más eredmények viszont ennek ellenkezőjét indikálják.

Álhír- és adathalászkvíz mint pedagógiai módszer a Média Detektív Fiataloknak projekt keretében

Az alábbiakban a „Média Detektív Fiataloknak" nevű Erasmus+-program során kidolgozott egyik pedagógiai módszert mutatjuk be a fiatalok médiaműveltségének növelésére annak érdekében, hogy minél inkább képesek legyenek az álhírek, adathalász csalások, hamis nyereményjátékok és egyéb csalások önálló felismerésére a gyakorlatban. A projekt 3 országban: Magyarországon, Romániában és Szlovákiában zajlott 2022 és 2024 között. Ennek során pedagógusoknak és ifjúságsegítőknek tartottunk médiaműveltséget növelő felkészítést, és adtuk át nekik azokat a tananyagokat és pedagógiai módszereket, amelyeket aztán ők a fiataloknak adtak tovább. Az egyik ilyen pedagógiai módszer volt a 20 elemes kvíz, amely egyben kutatást is jelentett, hiszen a diákoknak online kellett kitölteniük, majd háttérváltozós kérdésekre is válaszolniuk kellett. Ezekből fontos kutatási adatokat nyertünk ki, amelyek még elemzésre várnak.

Az álhírek és adathalászat, valamint hamis nyereményjátékok felismerését segítő 20 elemes kvíz összeállításakor több szempontot vettünk figyelembe: egyrészt azokat a kutatási eredményeket, amelyek azt mutatták, hogy az önbevalláson alapuló tesztek nem feltétlenül indikálják megfelelően azt, hogy a résztvevők a valóságban mennyire képesek felismerni az átveréseket (lásd: Jones-Jang és mtsai., 2021). Korábbi kísérleteink alkalmával ugyanezt tapasztaltuk: az önbevalláson alapuló teszteken sok esetben magabiztosnak mutatkozó résztvevők a gyakorlatban nem feltétlenül szerepeltek jól a tesztet követő 10 elemes álhírkvízen. A kvíz összeállításakor Jones-Jang és munkatársainak, valamint Orhannak a módszerét alkalmaztuk, akik az önbevalláson alapuló médiaműveltségi tesztek után konkrét példákat mutattak a résztvevőknek, akiknek dönteniük kellett azok valóságtartalmáról (Jones-Jang és mtsai., 2021; Orhan, 2023). A korábbi tapasztalataink alapján tehát elhagytuk az önbevallásos tesztet, és a diákoknak egy 20 elemes online formában, a Google-kérdőív segítségével készült álhírkvízt kellett kitölteniük, majd válaszolniuk kellett néhány háttérváltozós kérdésre, hogy kutatásban is használni tudjuk a kapott adatokat. Mind a 20 példa valós képernyőmentést mutatott: létező közösségimédia-posztok, e-mailek, honlapok és SMS-ek formájában. Ezek három témakört fogtak át: hamis és valós nyereményjátékok (5 elem), adathalász próbálkozások és valódi üzenetek (10 elem), valamint álhírek és igaz hírek (5 elem). A 20 példa kiválasztásakor arra törekedtünk, hogy a hazai és nemzetközi szakirodalomban az álhírek

és adathalász próbálkozások elemzése során azonosított vizuális, nyelvi és egyéb jelek közül minél több megjelenjen a képernyőmentéseken. A tesztet a részt vevő diákok tanórai keretek között, egy kivetített QR-kód segítségével a mobiltelefonjukon tölthették ki a 3 országban. Ezt követően a foglalkozást vezető pedagógussal vagy ifjúságsegítő szakemberrel immár közösen tekintették meg mind a 20 példát, és beszélték át egyenként, mik voltak az átverésre vagy épp a valódiságra utaló jelek a konkrét esetekben. Ehhez a programban részt vett pedagógusok és ifjúságsegítők egy részletes leírást és útmutatást kaptak a megfigyelendő konkrét jelekről mindegyik képernyőmentéshez. Sok esetben ugyanis ők maguk sem mindig tudták helyesen megítélni a képernyőmentések valódiságát. Az alábbiakban táblázatok formájában, témakörökre lebontva mutatjuk be a 20 képernyőmentés tartalmát, a csalásra vagy valódiságra utaló konkrét jeleket, valamint azok szakirodalmi említéseit.

A bemutatott screenshot tartalma	**A csalásra vagy valódiságra utaló konkrét jelek**	**Az adott jelek szakirodalmi említései**
1. A Magyar Posta nevében érkezett hamis üzenet, hogy a felhasználót kisorsolták egy nyereményjátékban való részvételre, iPhone-t és Samsung Galaxyt lehet nyerni	Gyanús URL (nem a posta címére mutat)	(Basit és mtsai., 2021; Milletary, 2005; Saberi és mtsai., 2007)
	Fogalmazási és helyesírási hibák	(Downs és mtsai., 2006; Canfield és mtsai., 2016; Furnell, 2007; Baslyman – Chiasson, 2016; Chou és mtsai., 2004; Wash, 2020; Volkamer és mtsai., 2017)
	Váratlanul érkezik, nem volt előzetes regisztráció nyereményjátékban való részvételre	(Wash, 2020; Canfield és mtsai., 2016)
	Nem életszerű, túl értékes nyeremény a „semmiből", vágyat kelt a könnyű megszerzésre	(Milletary, 2005; Harrison és mtsai., 2016)
	Egy megbízható cégnek (ez esetben a Magyar Posta) adják ki magukat, az ő dizájnjukat, jelképeit használva, az ő nevével visszaélve	(Basit és mtsai., 2021; Milletary, 2005; Jagatic és mtsai., 2007; Saberi és mtsai., 2007; Wash, 2020; Liu és mtsai., 2011; Hong, 2012; Chaudhry és mtsai., 2016)
2. A „Penny Market Fans" nevében a Facebookon hirdetett hamis születésnapi nyereményjáték	Egy megbízható cégnek (ez esetben a Penny Market) adják ki magukat, az ő dizájnjukat, jelképeit használva, az ő nevükkel visszaélve	(Basit és mtsai., 2021; Milletary, 2005; Jagatic és mtsai., 2007; Saberi és mtsai., 2007; Wash, 2020; Liu és mtsai., 2011; Hong, 2012)
	Magyartalan megfogalmazás	(Downs és mtsai., 2006; Canfield és mtsai., 2016; Furnell, 2007; Baslyman – Chiasson, 2016; Chou és mtsai., 2004; Wash, 2020; Volkamer és mtsai., 2017)
	Megosztást kér	

A bemutatott screenshot tartalma	**A csalásra vagy valódiságra utaló konkrét jelek**	**Az adott jelek szakirodalmi említései**
2. A „Penny Market Fans" nevében a Facebookon hirdetett hamis születésnapi nyereményjáték	Nincs hivatalos játékszabályzat, nincs róla link, amely a Penny Market hivatalos oldalára mutatna	
	Nem életszerű, könnyű nyereményt ígér (minden kommentelő és az oldalt tovább osztó személy nyer)	(Milletary, 2005; Harrison és mtsai., 2016)
	Hamis közösségimédia-poszt, amelyet csalók készítettek	(Baslyman – Chiasson, 2016)
3. Valódi nyereményjáték a Lidl Magyarország hivatalos Facebook-oldalán	A Lidl hivatalos nyereményoldalán található	(Downs és mtsai., 2006)
	A hivatalos profilt igazoló kék pipa megjelenik a Lidl logója mellett	
	Nem kér megosztást	
	Van hivatalos játékszabályzat a Lidl hivatalos oldalára vivő linkkel (bár rövidített a link, így ez megtévesztő)	
	Életszerű a nyeremény	
4. Hamis nyereményjátékot hirdető poszt az OTP Bank nevében. Mindenki 75 ezer forintot kap, aki kitölti a belinkelt kérdőívet	Egy megbízható cégnek (ez esetben az OTP) adják ki magukat, az ő dizájnjukat, jelképeit használva, az ő nevükkel visszaélve. Valójában a „Bónuszinterjú" nevű Facebook-oldal a hirdető	(Basit és mtsai., 2021; Milletary, 2005; Jagatic és mtsai., 2007; Saberi és mtsai., 2007; Wash, 2020; Liu és mtsai., 2011; Hong, 2012; Chaudhry és mtsai., 2016)
	Nem az OTP hivatalos weblapjára mutat a link, hanem az otp-promo2023. com hamis oldalra	(Basit és mtsai., 2021; Milletary, 2005; Kirda, 2006; Saberi és mtsai., 2007; Chaudhry és mtsai., 2016; Parekh és mtsai., 2018)
	Magyartalan megfogalmazás	(Downs és mtsai., 2006; Canfield és mtsai., 2016; Furnell, 2007; Baslyman – Chiasson, 2016; Chou és mtsai., 2004; Wash, 2020; Volkamer és mtsai., 2017)
	Nem életszerű a nyeremény	(Milletary, 2005; Harrison és mtsai., 2016)
	Hamis közösségimédia-poszt, amelyet csalók készítettek	(Baslyman – Chiasson 2016)

A bemutatott screenshot tartalma	A csalásra vagy valódiságra utaló konkrét jelek	Az adott jelek szakirodalmi említései
5. Valódi nyereményjátékra felhívás e-mailben az Erste Banktól	A feladó e-mail-címe: valóban az Erste Bank hivatalos címéről érkezett	(Downs és mtsai., 2006)
	Linkre kell kattintani – ez önmagában csalásra is utalhat	(Basit és mtsai., 2021; Milletary, 2005; Kirda, 2006; Saberi és mtsai., 2007; Chaudhry és mtsai., 2016; Parekh és mtsai., 2018)
	Az e-mailben küldött link valóban az Erste Bank hivatalos oldalára mutat, ahol ugyancsak megtalálható a felhívás	(Downs és mtsai., 2006)
	Életszerű, nem „csak úgy" jár a nyeremény, meghatározott befektetés indításával lehet bekerülni a sorsolásba	
	Nincsenek helyesírási hibák, magyartalan megfogalmazások, ékezethibák stb.	(Butavicius és mtsai., 2022)
	Névre szóló megszólítás	(Butavicius és mtsai., 2022)

1. táblázat: Hamis és valódi nyereményjátékok (forrás: saját készítés)

A kvízben 5 példa szerepelt a nyereményjátékok kapcsán, ugyanis ezek egy része kevésbé ártalmas átverési típusba tartozik, így ezekből nem szerepeltettünk olyan sok példát. A kvízt nem akartuk 20-nál több elemesre készíteni, hogy a fiatalok türelmét ne tegyük próbára. Az 5 példa között szerepeltek közösségi médiában és e-mailben küldött nyereményjátékok is. Elsősorban a forrás megbízhatóságára utaló jeleket kellett megfigyelni a helyes azonosításhoz. Bár mindegyik példa nyereményjátékot mutat be, az OTP nevében készített poszt egyben adathalász csalás is. Ez is rámutat arra, hogy az egyes kategóriák a gyakorlatban nem feltétlenül különíthetők el egymástól élesen. Az Erste Bank által valós nyereményjátékról kiküldött e-mail bizonyult leginkább „beugratósnak" a beérkezett válaszok alapján. Ezért fontos, hogy a médiaműveltségnek része legyen az is, milyen jelek mutatják azt, hogy egy forrás valódi és megbízható.

A bemutatott screenshot tartalma	**A csalásra vagy valódiságra utaló konkrét jelek**	**Az adott jelek szakirodalmi említései**
1. OTP-s internetbanki belépés valódi, hivatalos oldala	Az URL az OTP valódi honlapjára mutat, „.hu" végződéssel	(Downs és mtsai., 2006)
	„https" kiterjesztéssel indul a link, amely biztonságos kapcsolatra utal, szintén a hitelességet erősíti	(Chou és mtsai., 2004; Dhamija és mtsai., 2006)
2. Csaló érdeklődik Messenger-üzenetben egy interneten meghirdetett termék iránt	Másnak adja ki magát, mint aki valójában (ez esetben egy becsületes vásárlónak)	(Wash, 2020)
	Személyes adatokat kér tőlünk, e-mail-címet – hasonló helyzetben sosem kell megadnia adatokat a terméket hirdető félnek	(Basit és mtsai., 2021; Milletary, 2005; Jagatic és mtsai., 2007; Kirda, 2006; Saberi és mtsai., 2007; Liu és mtsai., 2011; Hong, 2012)
	A szállítás megszervezését ígéri az érdeklődő	
	Magyartalan megfogalmazások, fordítóprogramos üzenetküldés	(Downs és mtsai., 2006; Canfield és mtsai., 2016; Furnell, 2007; Baslyman – Chiasson 2016; Chou és mtsai., 2004; Wash, 2020; Volkamer és mtsai., 2017)
	Hamis üzenet, amelyet csalók küldtek	(Baslyman – Chiasson, 2016)
3. A Netflix nevében küldött SMS, „utolsó figyelmeztetés" a fiók törlése előtt, 24 órán belül meg kell erősíteni az előfizetői adatokat	Másnak adja ki magát, megbízható cég (ez esetben a Netflix) nevével él vissza	(Basit és mtsai., 2021; Milletary, 2005; Jagatic és mtsai., 2007; Saberi és mtsai., 2007; Wash, 2020; Hong, 2012; Chaudhry és mtsai., 2016)
	Érzelmet kelt az üzenet: ránk ijeszt	(Hong, 2012; Volkamer és mtsai., 2017; Wash, 2020)
	Váratlanul érkezik, nem volt előzménye	(Wash, 2020; Canfield és mtsai., 2016; Downs és mtsai., 2006)
	Időbeli sürgetés: érzelmi manipuláció, pszichológiai manipuláció	(Downs és mtsai., 2006; Butavicius és mtsai., 2022; Abroshan és mtsai., 2021; Parsons és mtsai., 2013; Milletary, 2005; Baslyman – Chiasson, 2016; Volkamer és mtsai., 2017)

A bemutatott screenshot tartalma	A csalásra vagy valódiságra utaló konkrét jelek	Az adott jelek szakirodalmi említései
3. A Netflix nevében küldött SMS, „utolsó figyelmeztetés" a fiók törlése előtt, 24 órán belül meg kell erősíteni az előfizetői adatokat	Linkre kell kattintani az üzenetben	(Basit és mtsai., 2021; Milletary, 2005; Kirda, 2006; Saberi és mtsai., 2007; Chaudhry és mtsai., 2016; Parekh és mtsai., 2018)
	A küldött link nem a Netflix hivatalos oldalára mutat	(Basit és mtsai., 2021; Milletary, 2005; Kirda, 2006; Saberi és mtsai., 2007; Chaudhry és mtsai., 2016; Parekh és mtsai., 2018)
	Adategyeztetésre hív fel	(Basit és mtsai., 2021; Milletary, 2005; Kirda, 2006; Saberi és mtsai., 2007; Liu és mtsai., 2011)
	Hamis SMS, amelyet csalók készítettek	(Baslyman – Chiasson, 2016)
4. OTP-s internetbanki belépés csaló oldalra a Jófogás nevű internetes adok-veszek oldalt lemásoló csaló weblapról indulva	Megbízható cégeknek (ez esetben a Jófogás és az OTP) adják ki magukat, az ő dizájnjukat, jelképeiket használva, az ő nevükkel visszaélve. Az OTP dizájnját másolták le, de az oldal nem az OTP-hez tartozik.	(Basit és mtsai., 2021; Milletary, 2005; Kirda, 2006; Saberi és mtsai., 2007; Wash, 2020; Liu és mtsai., 2011; Hong, 2012; Chaudhry és mtsai., 2016)
	Gyanús URL: bár tartalmazza a Jófogás nevét, valójában nem annak oldalára mutat: jofogas-hu. sell-online. info kezdetű a hamis URL, amely valójában nem „.hu" végződésű, de szerepel benne ez a kiterjesztés is megtévesztésképp	(Basit és mtsai., 2021; Downs és mtsai., 2006; Jakobsson és mtsai., 2007; Canfield és mtsai., 2016; Furnell, 2007; Milletary, 2005; Baslyman – Chiasson, 2016; Chou és mtsai., 2004; Wash, 2020; Volkamer és mtsai., 2017; Sheng és mtsai., 2010)
5. Hamis figyelmeztetés e-mailben az Erste Bank nevében az internetes alkalmazás hozzáférésének lejártáról	Egy megbízható cégnek (ez esetben az Erste Bank) adják ki magukat, az ő dizájnjukat, jelképeit használva, az ő nevükkel visszaélve	(Basit és mtsai., 2021; Milletary, 2005; Kirda, 2006; Saberi és mtsai., 2007; Wash, 2020; Liu és mtsai., 2011; Hong, 2012; Chaudhry és mtsai., 2016)
	Hamis e-mail, amelyet csalók küldtek	(Milletary, 2005; Chou és mtsai., 2004; Saberi és mtsai., 2007; Hong, 2012; Abroshan és mtsai., 2021; Butavicius és mtsai., 2016; Canfield és mtsai., 2016; Kirda, 2006; Wu és mtsai., 2006; Downs és mtsai., 2006; Zhang – Ghorbani, 2020; Volkamer és mtsai., 2017; Baslyman and Chiasson, 2016)

A bemutatott screenshot tartalma	**A csalásra vagy valódiságra utaló konkrét jelek**	**Az adott jelek szakirodalmi említései**
5. Hamis figyelmeztetés e-mailben az Erste Bank nevében az internetes alkalmazás hozzáférésének lejártáról	Személytelen megszólítás, nem névre szólóan	(Butavicius és mtsai., 2022; Parsons és mtsai., 2013; Sheng és mtsai., 2010; Canfield és mtsai., 2016)
	Nyelvi hibák: magyartalan megfogalmazás, ékezethibák, tegeződés/magázódás váltakozása	(Downs és mtsai., 2006; Canfield és mtsai., 2016; Furnell, 2007; Baslyman and Chiasson, 2016; Chou és mtsai., 2004; Wash, 2020; Volkamer és mtsai., 2017)
	Linkre kell kattintani, amely nem az Erste hivatalos weblapjára mutat (ez a konkrét screenshoton nem látszott)	(Basit és mtsai., 2021; Milletary, 2005; Kirda, 2006; Saberi és mtsai., 2007; Chaudhry és mtsai., 2016; Parekh és mtsai., 2018)
6. Valódi fizetési felszólítás e-mailben az MVM Next online ügyfélszolgálatától lejáró gázszámla ügyében	A feladó e-mail-címe: az MVM hivatalos e-mail-címéről érkezett	(Downs és mtsai., 2006)
	Személytelen megszólítás – ez önmagában átverésre is utalhat	(Butavicius és mtsai., 2022; Parsons és mtsai., 2013; Sheng és mtsai., 2010; Canfield és mtsai., 2016)
	Linkre kell kattintani – ez önmagában átverésre is utalhat	(Basit és mtsai., 2021; Milletary, 2005; Kirda, 2006; Saberi és mtsai., 2007; Chaudhry és mtsai., 2016; Parekh és mtsai., 2018)
	A bankkártyás fizetési lehetőségről küldött link az MVM hivatalos oldalára mutat	(Downs és mtsai., 2006; Sheng és mtsai., 2010)
	Nincs helyesírási hiba, elírás, ékezethiba, magyartalan megfogalmazás	(Butavicius és mtsai., 2022)
	Valós adatok (konkrét szerződésszám, felhasználói azonosító) – bár csalók is megszerezhetik ezeket az adatokat, de a konkrét adatok a hitelességet erősítik	(Downs és mtsai., 2006)
	Nincs fenyegetés, sürgetés, érzelemkeltés	(Sheng és mtsai., 2010)

A bemutatott screenshot tartalma	A csalásra vagy valódiságra utaló konkrét jelek	Az adott jelek szakirodalmi említései
7. Valódi figyelmeztetés e-mailben a Facebook Messengerben szokatlan aktivitásról (angol nyelven)	A Facebook hivatalos e-mail-céméről érkezett az értesítés	(Downs és mtsai., 2006)
	Névre szólóan	(Downs és mtsai., 2006; Butavicius és mtsai., 2022)
	A szokatlan bejelentkezés pontos időpontja és helyszíne is meg van adva (a részletesség a hitelességet erősíti)	(Downs és mtsai., 2006)
	Nem sürget, nem ijesztget, nem fenyeget	(Sheng és mtsai., 2010)
	Linkre kell kattintani – ez önmagában átverésre is utalhat	(Basit és mtsai., 2021; Milletary, 2005; Kirda, 2006; Saberi és mtsai., 2007; Chaudhry és mtsai., 2016; Parekh és mtsai., 2018)
	A link a Facebook hivatalos oldalára mutat	(Downs és mtsai., 2006)
	Az értesítés a Facebook alkalmazásban is megjelent (ez nem látszik a screenshoton)	
8. Hamis emlékeztető e-mail az MVM nevében lejáró földgázszámláról	A feladó e-mail-címe nem az MVM hivatalos címe, hanem egy francia e-mail-cím	(Milletary, 2005; Chou és mtsai., 2004; Saberi és mtsai., 2007; Hong, 2012; Abroshan és mtsai., 2021; Butavicius és mtsai., 2016; Canfield és mtsai., 2016; Kirda, 2006; Wu és mtsai., 2006; Downs és mtsai., 2006; Zhang – Ghorbani, 2020; Volkamer és mtsai., 2017; Baslyman and Chiasson, 2016)
	Egy megbízható cégnek (ez esetben az MVM) adják ki magukat, az ő dizájnjukat, jelképeit használva, az ő nevükkel visszaélve	(Basit és mtsai., 2021; Milletary, 2005; Jagatic és mtsai., 2007; Saberi és mtsai., 2007; Wash, 2020; Liu és mtsai., 2011; Hong, 2012)
	Ékezethibák	(Milletary, 2005)
	Formai hiba: nagybetűk indokolatlan használata a tárgyban, ami nem jellemző hivatalos e-mailekben	(Wash, 2020)
	Linkre kell kattintani	(Basit és mtsai., 2021; Milletary, 2005; Kirda, 2006; Saberi és mtsai., 2007; Chaudhry és mtsai., 2016; Parekh és mtsai., 2018)

A bemutatott screenshot tartalma	**A csalásra vagy valódiságra utaló konkrét jelek**	**Az adott jelek szakirodalmi említései**
8. Hamis emlékeztető e-mail az MVM nevében lejáró földgázszámláról	A link valójában nem az MVM hivatalos oldalára mutat	(Basit és mtsai., 2021; Milletary, 2005; Kirda, 2006; Saberi és mtsai., 2007; Parekh és mtsai., 2018)
	Nincs semmilyen megszólítás az e-mailben	(Butavicius és mtsai., 2022; Parsons és mtsai., 2013; Sheng és mtsai., 2010; Canfield és mtsai., 2016)
	Hamis e-mail, amelyet csalók készítettek	(Baslyman – Chiasson, 2016; Abroshan és mtsai., 2021)
9. Valódi figyelmeztetés e-mailben a Netflix-fiók használatáról (angol nyelven)	A Netflix hivatalos e-mail-céméről érkezett	(Downs és mtsai., 2006)
	Névre szóló megszólítás	(Downs és mtsai., 2006; Butavicius és mtsai., 2022)
	Konkrét adatok: a Netflix-fiókba történt bejelentkezés pontos időpontja és helyszíne	(Downs és mtsai., 2006)
	Nem fenyeget, nem sürget, nem ijesztget, csak egy tényszerű értesítést tartalmaz	(Sheng és mtsai., 2010)
	Nem kell linkre kattintani	(Downs és mtsai., 2006)
10. Valódi értesítés SMS-ben a Bookline-tól, hogy a megrendelt könyv átvehető az egri Libri áruházban	Személytelen megszólítás, ráadásul rövidítést alkalmazva (T. Vasarlonk) – ez átverésre utal	(Butavicius és mtsai., 2022; Parsons és mtsai., 2013; Sheng és mtsai., 2010; Canfield és mtsai., 2016)
	Ékezetek teljes hiánya – átverésre utal	(Milletary, 2005; Wash, 2020)
	Magyar telefonszámról érkezett – a valódiság irányába mutat	(Downs és mtsai., 2006)
	Nincs link, amire kattintani kell – valódiság irányába mutat	(Downs és mtsai., 2006)
	Konkrét áruházat jelöl meg, és konkrét dátumot, ameddig ott át lehet venni a könyvet – valódiságra utal	(Downs és mtsai., 2006)
	Tényleg történt könyvrendelés (ez nem derül ki a screenshotból)	

2. táblázat: Adathalász és valós üzenetek (forrás: saját készítés)

Mivel abból indultunk ki, hogy az adathalász próbálkozások jelentik az egyén számára közvetlenül a legnagyobb veszélyt (például a pénze vagy érzékeny adatai azonnali ellopásával), ezért ebből a kategóriából szerepelt a legtöbb példa a kvízben, ez alkotta a leghangsúlyosabb csoportot. Külön kategóriát képezett az interneten eladásra kínált termékekre specializálódott csalások esete, amelyet leginkább akkor lehet felismerni, ha valaki már találkozott a trükkel. A legtöbb példa esetében a feladó címe és az URL voltak a lebuktató jelek – összhangban Harrison és társainak megállapításaival (Harrison és mtsai., 2016). A Facebook és a Bookline által küldött valós üzenetek bizonyultak a leginkább „beugratósnak" a beérkezett válaszok alapján ebben a kategóriában. Ez is azt indikálja, mennyire fontos a médiaműveltség fejlesztése során az is, milyen jelek mutatják egy forrás és üzenet valódiságát.

A bemutatott screenshot tartalma	**A csalásra vagy valódiságra utaló konkrét jelek**	**Az adott jelek szakirodalmi említései**
1. Közösségimédia-poszt egy autón csak 24 órán át megpihenő, majd maguktól békésen továbbálló méhkasról, akiket békén kell hagyni, és cukros vizet kell nekik adni. A történetet egy „bizonyító erejű" fotó is illusztrálja. A fotó valódi, a brit sajtóban jelent meg, csakhogy a sztori egészen más: valójában a méhkirálynő beszorult az autóba, azért gyűltek oda a méhek.	Megható történet, érzelmeket kelt	(Veszelszki, 2017)
	A közzétevő médium nem a hírmédiára jellemző etikai és szerkesztési normákat és elveket alkalmazza, homályos, ellenőrizhetetlen tulajdonú oldal	(Royster, 2017; Lazer és mtsai., 2018; Bajomi-Lázár, 2023; Walters, 2018)
	Spirituális szavak használata a posztban	(Veszelszki – Falyuna, 2019)
	Megosztást kér	
	A megható történet csak a közösségi médiában terjed, nem jelent meg más, megbízható hírforrásokban, de méhekkel foglalkozó szervezetek hivatalos oldalain sem	(Lazer és mtsai., 2018; Weideman, 2018; Gerbaudo, 2018; Gordon, 2018; Tandoc és mtsai., 2018; Bajomi-Lázár, 2023; Guess és mtsai., 2018; Allcott – Gentzkow, 2017; Klein – Wueller, 2017; Zhang – Ghorbani, 2020)
	Átkeretezett jelentéstartalmú fotót tartalmaz – a fotó valódi, de nem azt ábrázolja, amit a kitalált történet elmesél	(Klein and Wueller, 2017)
2. Hamis cikk látszólag az index.hu oldalon arról, hogy Harsányi Leventét beperelte a Magyar Nemzeti Bank	Gyanús URL: az URL valójában nem az index.hu oldalára mutat	(Basit és mtsai., 2021; Downs és mtsai., 2006; Jakobsson és mtsai., 2007; Canfield és mtsai., 2016; Furnell, 2007; Milletary, 2005; Baslyman and Chiasson, 2016; Chou és mtsai., 2004; Wash, 2020; Volkamer és mtsai., 2017; Sheng és mtsai., 2010)

A bemutatott screenshot tartalma	**A csalásra vagy valódiságra utaló konkrét jelek**	**Az adott jelek szakirodalmi említései**
2. Hamis cikk látszólag az index.hu oldalon arról, hogy Harsányi Leventét beperelte a Magyar Nemzeti Bank	Az index.hu dizájnját másolták le a csalók	(Kirda, 2006; Abroshan és mtsai., 2021; Chou és mtsai., 2004; Volkamer és mtsai., 2017)
	Valódi, legitim, megbízható szerkesztőség által közölt hírnek mutatja magát	(Walters, 2018; Weideman, 2018; Pennycook–Rand, 2021; Bryanov – Vziatysheva, 2021; Apuke – Omar, 2021; Lazer és mtsai., 2018; Zhang – Ghorbani, 2020; Gaughan, 2017)
	Elírások vannak a címben	(Veszelszki, 2017)
	A szenzációs történet csak a közösségi médiában terjed, nem jelent meg valójában egyetlen megbízható hírforrásban sem, így a valódi index.hu oldalon sem	(Lazer és mtsai., 2018; Weideman, 2018; Gerbaudo, 2018; Gordon, 2018; Tandoc és mtsai., 2018; Bajomi-Lázár, 2023; Guess és mtsai., 2018; Allcott – Gentzkow, 2017; Klein – Wueller, 2017; Zhang – Ghorbani, 2020)
3. Közösségimédia-poszt arról, hogy a néhai Robin Williams a filmforgatásain kikötötte, hogy hajléktalanokat is alkalmazni kell. Így összesen 1520 hajléktalant segített visszatérni a munka világába. A történetet egy „bizonyító erejű" fotó illusztrálja, amelyen Robin Williams látható az utcán – egy akár hajléktalannak is nézhető idős ember társaságában.	Érzelmeket kelt, túlságosan megható a történet, „túl szép ahhoz, hogy igaz legyen"	(Veszelszki, 2017)
	A közzétevő médium nem a hírmédiára jellemző etikai és szerkesztési normákat és elveket alkalmazza, homályos, ellenőrizhetetlen tulajdonú oldal	(Royster, 2017; Lazer és mtsai., 2018; Bajomi-Lázár, 2023; Walters, 2018)
	Hírességről és/vagy vitatott közéleti eseményről szól	(Klein – Wueller, 2017)
	A szívhez szóló legenda csak közösségimédia-oldalakon terjed, nem jelent meg egyetlen megbízható hírforrásban sem, sem a filmgyártó cégek nem említették, de Robin Williams sem tett említést róla életében.	(Lazer és mtsai., 2018; Weideman, 2018; Gerbaudo, 2018; Gordon, 2018; Tandoc és mtsai., 2018; Bajomi-Lázár, 2023; Guess és mtsai., 2018; Allcott – Gentzkow, 2017; Klein – Wueller, 2017; Zhang – Ghorbani, 2020)
	Hazai és nemzetközi tényellenőrző oldalak is cáfolták a valódiságát.	
	Átkeretezett jelentéstartamú fotót tartalmaz – a fotó valódi lehet, de nem azt mutatja, amiről az írás szól	(Klein–Wueller, 2017)

A bemutatott screenshot tartalma	A csalásra vagy valódiságra utaló konkrét jelek	Az adott jelek szakirodalmi említései
4. Egy közösségimédia-poszt, amely egy álhírt tartalmazó linket oszt meg. A hír szerint Majka „kíméletlenül helyre tette a magyar embereknek beszóló" Pataky Attilát.	Érzelmekre ható, indulatokat és felháborodást keltő hír	(Veszelszki, 2017)
	Más médium nevére emlékeztető URL: a TV2 nevével él vissza, miközben nem a hivatalos „tv2.hu", hanem a „tv-friss.com" nevű álhíroldal	(Basit és mtsai., 2021; Downs és mtsai., 2006; Jakobsson és mtsai., 2007; Canfield és mtsai., 2016; Furnell, 2007; Milletary, 2005; Baslyman – Chiasson 2016; Chou és mtsai., 2004; Wash, 2020; Volkamer és mtsai., 2017; Sheng és mtsai., 2010)
	A közzétevő médium nem a hírmédiára jellemző etikai és szerkesztési normákat és elveket alkalmazza, homályos, ellenőrizhetetlen tulajdonú oldal	(Royster, 2017; Lazer és mtsai., 2018; Bajomi-Lázár, 2023; Walters, 2018)
	Hírességről és/vagy vitatott közéleti eseményről szól	(Klein – Wueller, 2017)
	Bár a hír érdekes és szenzációs, az főképp a közösségi médiában terjed, arról nem számolnak be megbízható és nagy múltú hírforrások	(Lazer és mtsai., 2018; Weideman, 2018; Gerbaudo, 2018; Gordon, 2018; Tandoc és mtsai., 2018; Bajomi-Lázár, 2023; Guess és mtsai., 2018; Allcott – Gentzkow, 2017; Klein – Wueller, 2017; Zhang – Ghorbani, 2020)
	Valódi, legitim, megbízható szerkesztőség által közölt hírnek mutatja magát	(Walters, 2018; Weideman, 2018; Pennycook – Rand, 2021; Bryanov and Vziatysheva, 2021; Apuke and Omar, 2021; Lazer és mtsai., 2018; Zhang – Ghorbani, 2020; Gaughan, 2017)
5. Az index.hu valódi cikke arról, hogy Curtis keményen odaszólt Majkának	A közzétevő forrás: az index.hu megbízható, nagy múltú hazai hírforrás	(Downs és mtsai., 2006)
	A hírt más, megbízható források is közölték	
	Az érintett sztárok hivatalos közösségimédia-oldalain is megjelent	
	Nem annyira érzelemkeltő	

3. táblázat: Álhírek és valódi hírek (forrás: saját készítés)

Ebben a kategóriában is 5 elem szerepelt. Itt az érzelemkeltés (például Robin Williams, Pataky Attila és Majka esetében), valamint a segíteni akarás vágyának kihasználása (a méhek megsegítése) volt az átverések lényege, ezt kellett tetten érnie magán a felhasználónak. A Harsányi Leventéről készült álhír pedig egyben adathalász csalás is volt, mert a cikkben egy hamis befektetést ígérnek, amelyben pénz átutalását kezdeményezik. Ez is mutatja, hogy nem mindig lehet egymástól élesen elkülöníteni a különböző csalási kategóriákat – ez esetben az adathalászat álhírrel párosult. Az elsődleges lebuktató jel az Index nevében készült csalás esetén az URL volt.

Összefoglalás

Ebben a tanulmányban egy három országot átölelő nemzetközi projekt során alkalmazott, médiaműveltséget fejlesztő komplex pedagógiai és kutatási módszert mutattunk be egy 20 elemes kvíz formájában az álhírek, adathalász csalások és hamis nyereményjátékok felismerésére. Az online, mobiltelefonról kitölthető kvíz teljesítése után a foglalkozást vezető pedagógus vagy ifjúságsegítő szakember segítségével közösen beszélik meg a megoldást. A 20 képernyőmentés összeállásakor arra törekedtünk, hogy azok minél szélesebb körben fogják át azokat a jeleket, amelyeket a hazai és nemzetközi szakirodalomban azonosítottak az álhírek és egyéb csalások esetében. A teszt előzetes eredményei arra is rámutatnak, hogy a médiatudatossági foglalkozások során nagy hangsúlyt kell helyezni nemcsak a csalások és átverések jeleinek bemutatására, hanem arra is, milyen jelek mutatják azt, hogy valódi hírekkel, valós és hiteles forrásból származó üzenetekkel van dolgunk.

Felhasznált szakirodalom:

Abroshan, Hossein – Devos, Jan – Poels, Geert – Laermans, Eric (2021): Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process. *IEEE Access* **2021.** 9. sz. 44928–44949. https://doi.org/10.1109/ACCESS.2021.3066383

Allcott, Hunt – Gentzkow, Matthew (2017): Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives* **31**. 2. sz 211–236. https://doi.org/10.1257/jep.31.2.211

Anandpara, Vivek – Dingman, Andrew – Jakobsson, Markus – Liu, Debin – Roinestad, Heather (2007): Phishing IQ Tests Measure Fear, Not Ability. In: Dietrich, Sven –

Dhamija, Rachna (szerk.): *Financial Cryptography and Data Security*, vol. 4886. Berlin, Heidelberg: Springer Berlin Heidelberg (Lecture Notes in Computer Science). 362–366. https://doi.org/10.1007/978-3-540-77366-5_33

Appel, Markus – Prietzel, Fabian (2022): The detection of political deepfakes. *Journal of Computer-Mediated Communication* **27**. 4**.** sz Article zmac008. https://doi.org/10.1093/jcmc/zmac008

Apuke, Oberiri Destiny – Omar, Bahiyah (2021): Fake news and COVID-19: modelling the predictors of fake news sharing among social media users. *Telematics and informatics* **2021**. 56. sz. 101475. https://doi.org/10.1016/j.tele.2020.101475

Ashley, Seth – Maksl, Adam – Craft, Stephanie (2013): Developing a News Media Literacy Scale. *Journalism & Mass Communication Educator* **68.** 1. sz 7–21. https://doi.org/10.1177/1077695812469802

Ashley, Seth – Poepsel, Mark – Willis, Erin (2010): Media Literacy and News Credibility: Does knowledge of media ownership increase skepticism in news consumers? *JMLE.* https://doi.org/10.23860/jmle-2-1-3

Aufderheide, Patricia – Firestone, Charles M. (1993): *Media Literacy A Report of The National Leadership Conference on Media Literacy*. Washington D.C.: The Aspen Institute Communications and Society.

Babaei, Mahmoudreza – Kulshrestha, Juhi – Chakraborty, Abhijnan – Redmiles, Elissa M. – Cha, Meeyoung – Gummadi, Krishna P. (2022): Analyzing Biases in Perception of Truth in News Stories and Their Implications for Fact Checking. *IEEE Transactions on Computational Social Systems* **9.** 3. sz. 839–850. https://doi.org/10.1109/TCSS.2021.3096038

Bajomi-Lázár, Péter (2023): Álhírek és igaz hírek. Definíciós kérdések. In: Özge Çakır-Somlyai (szerk.): *Az álhírek elleni küzdelem – Szöveggyűjtemény*, 2–11. 2024. 03.24-i megtekintés https://mertek.eu/wp-content/uploads/2023/03/Szoveggyujtemeny.pdf

Balázs, Géza (2015): Netfolklór – intermedialitás és terjedés. *Replika* 2015. *1-2.* sz. 171–185. 2024. 03. 24-i megtekintés: https://www.replika.hu/system/files/archivum/90-91_10_balazs.pdf

Basit, Abdul – Zafar , Maham – Liu, Xuan – Javed, Abdul Rehman – Jalil, Zunera – Kifayat, Kashif (2021): A comprehensive survey of AI-enabled phishing attacks detection techniques. *Telecommunication systems* **76.** 1. sz. 139–154. https://doi.org/10.1007/s11235-020-00733-2

Baslyman, Malak – Chiasson, (2016): „Smells Phishy?": An educational game about online phishing scams. In: *2016 APWG Symposium on Electronic Crime Research (eCrime)*. Toronto, ON, Canada, 2016. 06. 01. – 2016. 06. 03: IEEE. 1–11. https://doi.org/10.1109/ECRIME.2016.7487946

Bodaghi, Arezo – Schmitt, Ketra A. – Watine, Pierre – Fung, Benjamin C. M. (2024): A Literature Review on Detecting, Verifying, and Mitigating Online Misinformation. *IEEE Transactions on Computational Social Systems,* 1–27. https://doi.org/10.1109/TCSS.2023.3289031

Boh Podgornik, Bojana – Dolničar, Danica – Šorgo, Andrej – Bartol, Tomaž (2016): Development, testing, and validation of an information literacy test (ILT) for higher education. *Asso for Info Science & Tech* **67. *10***. sz. 2420–2436. https://doi.org/10.1002/asi.23586

Bryanov, Kirill – Vziatysheva, Victoria (2021): Determinants of individuals' belief in fake news: A scoping review determinants of belief in fake news. *PloS one* 16. 6. sz. e0253717. https://doi.org/10.1371/journal.pone.0253717

Bulger, Monica – Davison, Patrick (2018): The Promises, Challenges, and Futures of Media Literacy. *JMLE* **10**. 1. sz. 1–21. https://doi.org/10.23860/JMLE-2018-10-1-1

Butavicius, Marcus – Parsons, Kathryn – Pattinson, Malcolm – McCormac, Agata (2016): Breaching the Human Firewall: Social engineering in Phishing and Spear-Phishing Emails. Cornell University. 2024. 03. 24-i megtekintés: https://arxiv.org/ftp/arxiv/papers/1606/1606.00887.pdf

Butavicius, Marcus – Taib, Ronnie – Han, Simon J. (2022): Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails. *Computers & Security* **2022**. 123. sz. 102937. https://doi.org/10.1016/j.cose.2022.102937

Canfield, Casey Inez – Fischhoff, Baruch – Davis, Alex (2016): Quantifying Phishing Susceptibility for Detection and Behavior Decisions. Human Factors **58**. 8. sz. 1158–1172. https://doi.org/10.1177/0018720816665025

Chaudhry, Junaid Ahsenali – Chaudhry, Shafique Ahmad – Rittenhouse, Robert G. (2016): Phishing Attacks and Defenses. *IJSIA* **10**. 1. sz. 247–256. https://doi.org/10.14257/ijsia.2016.10.1.23

Chen, Der-Thanq – Wu, Jing – Wang, Yu-mei (2011): Unpacking new media literacy. *Journal on Systemics, Cybernetics and Informatics* **9**. 2. sz. 84–88. 2024. 03. 24-i megtekintés: https://www.iiisci.org/journal/PDV/sci/pdfs/ol508kr.pdf

Chou, Neil – Ledesma, Robert – Teraguchi, Yuka – Mitchell, John C. (2004): Client-side defense against web-based identity theft. 2024. 03. 24-i megtekintés: https://crypto.stanford.edu/SpoofGuard/webspoof.pdf

Chu, Donna – Lee, Alice Y. L. (2014): Media Education Initiatives by Media Organizations. *Journalism & Mass Communication Educator* **69**. 2. sz. 127–145. https://doi.org/10.1177/1077695813517884

Comito, Carmela – Caroprese, Luciano – Zumpano, Ester (2023): Multimodal fake news detection on social media: a survey of deep learning techniques. *Social Network Analysis and Mining* **13**. 1. sz. https://doi.org/10.1007/s13278-023-01104-w

Dhamija, Rachna – Tygar, J. D. – Hearst, Marti (2006): Why phishing works. In: Grinter, Rebecca – Rodden, Thomas – Aoki, Paul – Cutrell, Ed – Jeffries, Robin – Olson, Gary (szerk.): *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. CHI06: CHI 2006 Conference on Human Factors in Computing Systems*. Montréal Québec Canada, 22 04 2006 27 04 2006. New York, NY, USA: ACM. 581–590. https://doi.org/10.1145/1124772.1124861

Downs, Julie S. – Holbrook, Mandy B. – Cranor, Lorrie Faith (2006): Decision strategies and susceptibility to phishing. In: Cranor, Lorrie Faith (szerk.): *Proceedings of the second symposium on Usable privacy and security - SOUPS '06. the second symposium*. Pittsburgh, Pennsylvania, 2006. 07. 12. – 2006. 07. 14. New York, New York, USA: ACM Press, 79. https://doi.org/10.1145/1143120.1143131

Duran, Robert L. – Yousman, Bill – Walsh, Kaitlin M. – Longshore, Melanie A. (2008): Holistic Media Education: An Assessment of the Effectiveness of a College Course in Media Literacy. *Communication Quarterly* **56**. 1. sz. 49–68. https://doi.org/10.1080/01463370701839198

Fendt, Marvin – Nistor, Nicolae – Scheibenzuber, Christian – Artmann, Benedikt (2023): Sourcing against misinformation: Effects of a scalable lateral reading training based on cognitive apprenticeship. *Computers in Human Behavior* **2023**. 146. sz. 107820. https://doi.org/10.1016/j.chb.2023.107820

Filipec, Ondrej (2019): Building An Information Resilient Society: An Organic Approach. *CCS Journal* 11. 1. sz. 1–26. https://doi.org/10.5130/ccs.v11.i1.6065

Fleming, Jennifer (2014): Media Literacy, News Literacy, or News Appreciation? A Case Study of the News Literacy Program at Stony Brook University. *Journalism & Mass Communication Educator* 69. **2**. 146–165. https://doi.org/10.1177/1077695813517885

Furnell, Steven (2007): Phishing: can we spot the signs? *Computer Fraud & Security* **2007**. 3. sz. 10–15. https://doi.org/10.1016/S1361-3723(07)70035-0

Gaughan, Anthony J. (2017): Illiberal Democracy: The Toxic Mix of Fake News, Hyperpolarization, and Partisan Election Administration. *Duke Journal of Constitutional Law & Public Policy* **13**. 3. sz. 57–139. 2024. 03. 24-i megtekintés: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1130&context=djclpp

Gelencsér, Péter – Szűts, Zoltán (2020): A társadalmi nyilvánosság webkettes szerkezetváltozása. *Jel-Kép*. **9**. 2. sz. 38–51. 2024. 03. 24-i megtekintés: https://communicatio.hu/jelkep/2020/2/JelKep_2020_2_Gerencser_Peter__Szuts_Zoltan.pdf https://doi.org/10.20520/JEL-KEP.2020.2.39

Gerbaudo, Paulo (2018): Fake News and All-Too-Real Emotions: Surveying the Social Media Battlefield. *Brown Journal of World Affairs* **25.** 1. sz. 1–16. 2024. 03. 24-i megtekintés: https://bjwa.brown.edu/25-1/fake-news-and-all-too-real-emotions-surveying-the-social-media-battlefield/

Gordon, Mordechai (2018): Lying in Politics: Fake News, Alternative Facts, and the Challenges for Deliberative Civics Education. *Educational Theory* **68.** 1. sz. 49–64. https://doi.org/10.1111/edth.12288

Guess, Andrew – Nyhan, Brendan – Reifler, Jason (2018): Selective Exposure to Misinformation: Evidence from the consumption of fake news during the 2016 U.S. presidential campaign. 2024. 03. 24-i megtekintés: https://about.fb.com/wp-content/uploads/2018/01/fake-news-2016.pdf

Harrison, Brynne – Svetieva, Elena – Vishwanath, Arun (2016): Individual processing of phishing emails. *Online Information Review* **40.** 2. sz. 265–281. https://doi.org/10.1108/OIR-04-2015-0106

Hobbs, Renee – Frost, Richard (2003): Measuring the acquisition of media-literacy skills. *Reading Research Quarterly* **38.** 3. sz. 330–355. DOI: 10.1598/RRQ.38.3.2. https://doi.org/10.1598/RRQ.38.3.2

Hong, Jason (2012): The state of phishing attacks. *Commun. ACM* 55. 1. sz. 74–81. https://doi.org/10.1145/2063176.2063197

Hosseini, Marjan – Javadian Sabet, Alireza – He, Suining – Aguiar, Derek (2023): Interpretable fake news detection with topic and deep variational models. *Online Social Networks and Media* **2023.** 36. sz. 100249. https://doi.org/10.1016/j.osnem.2023.100249

Jackson, Collin – Simon, Daniel R. – Tan, Desney S. – Barth, Adam (2007): An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks. In: Dietrich, Sven – Dhamija, Rachna (szerk.): *Financial Cryptography and Data Security*. 11th International Conference, FC 2007, and First International Workshop on Usable Security, USEC 2007, Scarborough, Trinidad/Tobago, February 12–16., 2007. Revised Selected Papers: Springer, 281–293. https://doi.org/10.1007/978-3-540-77366-5_27

Jagatic, Tom N. – Johnson, Nathaniel A. – Jakobsson, Markus – Menczer, Filippo (2007): Social phishing. *Commun. ACM* **50.** 10. sz. 94–100. https://doi.org/10.1145/1290958.1290968

Jakobsson, Markus – Tsow, Alex – Shah, Ankur – Blevis, Eli – Lim, Youn-Kyung (2007): What Instills Trust? A Qualitative Study of Phishing. In: Dietrich, Sven – Dhamija, Rachna (szerk.): *Financial Cryptography and Data Security*. 11th International Conference, FC 2007, and First International Workshop on Usable Security, USEC

2007, Scarborough, Trinidad/Tobago, February 12–16., 2007. Revised Selected Papers: Springer, 356–361. https://doi.org/10.1007/978-3-540-77366-5_32

Jones-Jang, S. Mo – Mortensen, Tara – Liu, Jingjing (2021): Does Media Literacy Help Identification of Fake News? Information Literacy Helps, but Other Literacies Don't. *American Behavioral Scientist* **65.** 2. sz. 371–388. https://doi.org/10.1177/0002764219869406

Kim, Antino – Moravec, Patricia L. – Dennis, Alan R. (2023): When do details matter? News source evaluation summaries and details against misinformation on social media. *International Journal of Information Management* **2023**. 72. 102666. https://doi.org/10.1016/j.ijinfomgt.2023.102666

Kirda, E. (2006): Protecting Users against Phishing Attacks. *The Computer Journal* **49.** 5. 554–561. https://doi.org/10.1093/comjnl/bxh169

Klein, David – Wueller, Joshua R. (2017): Fake News: A Legal Perspective. *Journal of Internet Law* **20.** 10. sz. 5–13. 2024. 03. 24-i megtekintés: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2958790

Koc, Mustafa – Barut, Esra (2016): Development and validation of New Media Literacy Scale (NMLS) for university students. *Computers in Human Behavior* **2016.** 63. 834–843. https://doi.org/10.1016/j.chb.2016.06.035

Krekó, Péter (2018): *Tömegparanoia. Az összeesküvés-elméletek és álhírek szociálpszichológiája*. Budapest: Atheneum Kiadó.

Lazer, David M. J. – Baum, Matthew A. – Benkler, Yochai – Berinsky, Adam J. – Greenhill, Kelly M. – Menczer, Filippo (2018): The science of fake news – Addressing fake news requires a multidisciplinary effort. *Science* **359**. 6380. sz. 1094–1096. 2024. 03. 24-i megtekintés: https://scholar.harvard.edu/files/mbaum/files/science_of_fake_news.pdf https://doi.org/10.1126/science.aao2998

Lee, Nicole M. (2018): Fake news, phishing, and fraud: a call for research on digital media literacy education beyond the classroom. *Communication Education* **67.** 4. sz. 460–466. https://doi.org/10.1080/03634523.2018.1503313

Lin, Tzu-Bin – Li, Jen-Yi – Deng, Feng – Lee, Ling (2013): Understanding new media literacy: An explorative theoretical framework. *Journal of Educational Technology & Society* **16.** 4. sz. 160–170. 2024. 03. 24-i megtekintés: https://www.jstor.org/stable/pdf/jeductechsoci.16.4.160.pdf?casa_token=ei6IvlLDoIkAAAAA:PLs5zp6tYc2A8vuufyoapZqAB0BCKLAgccQcFwHs_6pcYp6WoO0X1sQzYvYyWQIzNV78bJgFxagNSkunkFlTdtrG1G4taESKDrF05Ue_W57Czsku3A

Liu, Gang – Xiang, Guang – Pendleton, Bryan A. – Hong, Jason I. – Liu, Wenyin (2011): Smartening the crowds. In: Cranor, Lorrie Faith (szerk.): *Proceedings of the Seventh Symposium on Usable Privacy and Security*. SOUPS ,11: Symposium On Usable Privacy

and Security. Pittsburgh Pennsylvania, 20 07 2011 22 07 2011. New York, NY, USA: ACM, 1–13. https://doi.org/10.1145/2078827.2078838

Livingstone, Sonia (2004): Media Literacy and the Challenge of New Information and Communication Technologies. *The Communication Review* 7. 1. sz. 3–14. 2024. 03. 24-i megtekintés: https://www.academia.edu/1039663/Media_Literacy_and_the_Challenge_of_New_Information_and_Communication_Technologies https://doi.org/10.1080/10714420490280152

Lu, Yingdan – Shen, Cuihua (2023): Unpacking Multimodal Fact-Checking: Features and Engagement of Fact-Checking Videos on Chinese TikTok (Douyin). *Social Media + Society* **9.** 1. sz. 205630512211504. https://doi.org/10.1177/20563051221150406

Luo, Yi Fang – Yang, Shu Ching – Kang, Seokmin (2022): New media literacy and news trustworthiness: An application of importance–performance analysis. *Computers & Education* **2022.** 185. sz. 104529. https://doi.org/10.1016/j.compedu.2022.104529

Maksl, Adam – Ashley, Seth – Craft, Stephanie (2015): Measuring News Media Literacy. *JMLE*. **6.** 3. sz. https://doi.org/10.23860/jmle-6-3-3

McLean, Siân A. – Paxton, Susan J. – Wertheim, Eleanor H. (2016): The measurement of media literacy in eating disorder risk factor research: psychometric properties of six measures. *Journal of eating disorders* **2016.** 4. 30. https://doi.org/10.1186/s40337-016-0116-0

Mihailidis, Paul (2009): Beyond Cynicism: Media Education and Civic Learning Outcomes in the University. *International Journal of Learning and Media* **1.** 3. sz. 19–31. 2025. 02. 16-i megtekintés: https://shorturl.at/WFOAJ https://doi.org/10.1162/ijlm_a_00027

Milletary, Jason (2005): Technical Trends in Phishing Attacks. 2024. 03. 24-i megtekintés: https://insights.sei.cmu.edu/library/technical-trends-in-phishing-attacks/

Nirav Shah, Minal – Ganatra, Amit (2022): A systematic literature review and existing challenges toward fake news detection models. *Social Network Analysis and Mining* **12.** 1. sz. 168. https://doi.org/10.1007/s13278-022-00995-5

Orhan, Ali (2023): Fake news detection on social media: the predictive role of university students' critical thinking dispositions and new media literacy. *Smart Learning Environments* **10.** 1. sz. https://doi.org/10.1186/s40561-023-00248-8

Parekh, Shraddha – Parikh, Dhwanil – Kotak, Srushti – Sankhe, Smita (2018): A New Method for Detection of Phishing Websites: URL Detection. *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*. Coimbatore, 2018. 04. 20. – 2018. 04. 21: IEEE. 949–952. https://doi.org/10.1109/ICICCT.2018.8473085

Parsons, Kathryn – McCormac, Agata – Pattinson, Malcolm – Butavicius, Marcus – Jerram, Cate (2013): Phishing for the Truth: A Scenario-Based Experiment of Users'

Behavioural Response to Emails. In Janczewski, Lech J. – Wolfe, Henry B. – Shenoi, Sujeet (szerk.): *Security and Privacy Protection in Information Processing Systems*, 405. sz. Berlin, Heidelberg: Springer Berlin Heidelberg (IFIP Advances in Information and Communication Technology), 366–378. https://doi.org/10.1007/978-3-642-39218-4_27

Pennycook, Gordon – Rand, David G. (2021): The Psychology of Fake News. *Trends in cognitive sciences* **25**. 5. sz. 388–402. https://doi.org/10.1016/j.tics.2021.02.007

Potter, W. James (2010): The State of Media Literacy. *Journal of Broadcasting & Electronic Media* **54.** 4. sz. 675–696. https://doi.org/10.1080/08838151.2011.521462

Pszona, Maria – Janicka, Maria – Wojdyga, Grzegorz – Wawer, Aleksander (2023): Towards universal methods for fake news detection. *Natural Language Engineering* **29.** 4. sz. 1004–1042. https://doi.org/10.1017/S1351324922000456

Reddy, Pritika – Sharma, Bibhya – Chaudhary, Kaylash (2020): Digital Literacy. International Journal of Technoethics **11**. 2. sz. 65–94. https://doi.org/10.4018/IJT.20200701.oa1

Royster, Lee K. (2017): Fake News: Potential Solutions To The Online Epidemic. *North Carolina Law Review* **96.** 1. sz. 270–296. 2024. 03. 24-i megtekintés: https://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=5718&context=nclr

Saberi, Alireza – Vahidi, Mojtaba – Bidgoli, Behrouz Minaei (2007): Learn to Detect Phishing Scams Using Learning and Ensemble Methods. In: *2007 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology – Workshops*. Silicon Valley, CA, USA, 2007. 11. 05. – 2007. 11. 12: IEEE. 311–314. https://doi.org/10.1109/WI-IATW.2007.79

Sheng, Steve – Holbrook, Mandy – Kumaraguru, Ponnurangam – Cranor, Lorrie Faith – Downs, Julie (2010): Who falls for phish? In: Mynatt, Elizabeth – Fitzpatrick, Geraldine – Hudson, Scott – Edwards, Keith – Rodden, Tom (szerk.): *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI ,10: CHI Conference on Human Factors in Computing Systems. Atlanta Georgia USA, 10 04 2010 15 04 2010. New York, NY, USA: ACM, 373–382. https://doi.org/10.1145/1753326.1753383

Szűts, Zoltán (2018) *Online. Az internetes kommunikáció és média története, elmélete és jelenségei*. Budapest, Wolters Kluwer.

Tandoc, Edson C. – Lim, Zheng Wei – Ling, Richard (2018): Defining "Fake News". *Digital Journalism* **6.** 2. sz. 137–153. https://doi.org/10.1080/21670811.2017.1360143

Tufchi, Shivani – Yadav, Ashima – Ahmed, Tanveer (2023): A comprehensive survey of multimodal fake news detection techniques: advances, challenges, and opportunities. *International Journal of Multimedia Information Retrieval* **12.** 2. sz. https://doi.org/10.1007/s13735-023-00296-3

Veszelszki, Ágnes (2017): Az álhírek extra- és intralingvális jellemzői. *Századvég* **84.** 51–82. 2024. 03. 24-i megtekintés: https://www.researchgate.net/publication/318990136_Veszelszki_Agnes_2017_Az_alhirek_extra-_es_intralingvalis_jellemzoi_Szazadveg_84_51-82

Veszelszki, Ágnes – Falyuna, Nóra (2019): Az áltudományosság leleplezése érveléstechnikai-nyelvészeti eszközökkel. *Médiakutató* **20**. 3. sz. 39–51. 2024. 03. 24-i megtekintés: https://www.mediakutato.hu/cikk/2019_03_osz/03_az_altudomanyossag_leleplezese.pdf

Volkamer, Melanie – Renaud, Karen – Reinheimer, Benjamin – Kunz, Alexandra (2017): User experiences of TORPEDO: TOoltip-poweRed Phishing Email DetectiOn. *Computers & Security* **71**. 100–113. https://doi.org/10.1016/j.cose.2017.02.004

Vraga, Emily – Tully, Melissa – Kotcher, John – Smithson, Anne-Bennett – Broeckelman-Post, Melissa (2015): A Multi-Dimensional Approach to Measuring News Media Literacy. *JMLE*. **7.** 3. sz. https://doi.org/10.23860/jmle-7-3-4

Walters, Ryan M. (2018): How to Tell a Fake: Fighting Back against Fake News on the Front Lines of Social Media. *Texas Review of Law & Politics* **23.** 1. sz. 111–179. 2024. 03. 24-i megtekintés: https://drive.google.com/file/d/1NX5OzXzmQri27BxrDk9D5mnjhqfQW42v/view

Wash, Rick (2020): How Experts Detect Phishing Scam Emails. *Proc. ACM Hum.-Comput. Interact.* **4** (CSCW2) 1–28. https://doi.org/10.1145/3415231

Weideman, Melius (2018): Fake News: The role of search engines and website content. In: Halilagić, Dženita – Knežević, Ratko – Cavanagh, Jerald – Kirby, Padraig (szerk.): *Proceedings - International Scientific Conference „Western Balkan Information Literacy" Alternative facts, Fake News, getting to the truth with Information Literacy 21-22 June 2018 Bihac*. Ireland: Limerick Institute of Technology, 26–35.

Wright, Adam – Aaron, Skye – Bates, David W. (2016): The Big Phish: Cyberattacks Against U.S. Healthcare Systems. *Journal of general internal medicine* **31**. 10. sz. 1115–1118. https://doi.org/10.1007/s11606-016-3741-z

Wu, Min – Miller, Robert C. – Garfinkel, Simson L. (2006): Do security toolbars actually prevent phishing attacks? In: Grinter, Rebecca – Rodden, Thomas – Aoki, Paul – Cutrell, Ed – Jeffries, Robin – Olson, Gary (szerk.): *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. CHI 2006. Montréal Québec Canada, 22 04 2006 27 04 2006. New York, NY, USA: ACM, 601–610. https://doi.org/10.1145/1124772.1124863

Yang, Rundong – Zheng, Kangfeng – Wu, Bin – Di, Li – Wang, Zhe – Wang, Xiujuan (2022): Predicting User Susceptibility to Phishing Based on Multidimensional Features. *Computational intelligence and neuroscience* **2022.** 7058972. https://doi.org/10.1155/2022/7058972

Zhang, Xichen – Ghorbani, Ali A. (2020): An overview of online fake news: Characterization, detection, and discussion. *Information Processing & Management* **57.** 2. sz. 102025. https://doi.org/10.1016/j.ipm.2019.03.004