



A BIZTONSÁGTUDATOSSÁG OKTATÁSÁNAK ESZKÖZEI A BEVONÓDÁS ÉRDEKÉBEN

TÖRLEY GÁBOR

Eötvös Loránd Tudományegyetem, Informatikai Kar, Budapest, Magyarország
gabor.torley@inf.elte.hu

Összefoglaló

Ma már nagyon sokféle módon lehet átadni ismereteket a biztonságtudatosságról, pl. kiterjesztett / virtuális valóság, web alapú tananyagok, online videók, játékok (online és offline) és „unplugged” módszerek. A cikk kiemeli, hogy azok a módszerek a jobbak, amelyekkel magasabb gondolkodási szintet lehet elérni a Bloom taxonómia szerint. Egy jó tanítási módszer megtalálása és alkalmazása nagyon fontos, mert a tanulók egyre fiatalabb korban találkoznak az Internet veszélyeivel.

Kulcsszavak: Bloom taxonómia, bevonódás, információbiztonság, átadási módok, tanítási módszerek

1. Bevezetés

Livingstone et al (2011) kérdőíves kutatása vizsgálta az alapvető online veszélyeket: pornográfia, zaklatás, szexuális tartalmú üzenetek fogadása, kapcsolat olyan emberekkel, akikkel nem volt találkozás élőben, offline találkozókat online ismerősökkel, potenciálisan ártalmas felhasználók által generált tartalom és személyes adatokkal való visszaélés. Megmutatták, hogy a fiatalabb gyermekek megfelelő készség és meggyőződés nélkül élnek ezen a területen. Ennek ellenére a legtöbb 11-16 éves képes üzeneteket blokkolni azokról, akikkel nem akarnak kapcsolatban lenni, illetve képesek megfelelő tanácsokat találni az internetes biztonsággal kapcsolatban a világhálón. Nagyjából a megkérdezett gyerekek fele képes megváltoztatni az adatvédelmi beállításokat a közösségi hálózaton a profiljukra vonatkozóan, valamint összevetni weboldalakat, hogy megítéljék a minőségüket, hitelességüket, illetve, hogy kéretlen leveleket blokkoljanak. A kutatók azt vallják, hogy szükség van a digitális készségek fejlesztésére, hogy minden gyermek eljusson valamilyen közös minimum tudásszintre és hogy ezt a tudást megkapják a digitálisan izolált és képzetlen gyermekek is.

A 2022-es PISA vizsgálatok eredménye (OECD, 2023) hasonló dolgokat mutatott: a magyar diákok 3 ponttal az OECD átlaga alatt teljesítettek olvasásból/szövegértésből. A magyar tanulók több, mint negyede a 2. szint alatt teljesített. Ezen a szinten a diákok meg tudják határozni a fő gondolatát egy mérsékelt hosszú szövegnek. Az értékelés és a reflektálás mindig is a szövegértés műveltségterület része volt. A digitális szövegértés korszakában az olvasók egyre több és több információval találkoznak, és képesnek kell lenniük arra, hogy el tudják dönteni, hogy mi az, ami megbízható és mi az, ami nem. Ez ugyancsak része az informatikai biztonságtudatosságnak. Ugyanis az alacsony szövegértéssel rendelkező tanulók tudatossága is alacsonyabb lesz.

2. Irodalmi áttekintés

Az 1950-es években kifejlesztett Bloom-féle taxonómia valószínűleg az egyik legjobban ismert és legszélesebb körben használt modell az ember kognitív folyamatainak leírásához. A taxonómia felülvizsgált verzióját 2001-ben publikálták (1. ábra) (Anderson – Krathwohl, 2001).



Bloom-féle taxonómia (eredeti, 1956.)



Bloom-féle taxonómia (felülvizsgált, 2001.)

1. ábra: Bloom-féle taxonómia, eredeti és felülvizsgált (Van Niekerk et al, 2013.)

Az informatikai biztonságtudatosság növelhető, ha a Bloom-féle taxonómiát alkalmazzuk olyan képzési programok megtervezéséhez, amelyek túlmutatnak az alapvető ismeretfelidézésen, és magasabb szintű kognitív készségeket – például az elemzést, az értékelést és az alkotást – céloznak meg. A kiberbiztonság oktatásának taxonómia szerinti szinteken történő strukturálásával az iskolák hatékonyabb helyi tanterveket alakíthatnak ki, amelyek mélyebb megértést biztosítanak, növelik a diákok motivációját, valamint elősegítik a hosszú távú biztonsági gyakorlatok fenntartását.

A pedagógiai taxonómiák segítenek leírni és kategorizálni azokat a kognitív, érzelmi és egyéb dimenziókat, amelyekben az egyén részt vesz a tanulási folyamatban. Másképpen megfogalmazva, a pedagógiai taxonómiák segítenek abban, hogy „megértsük a megértést”. (Sousa, 2006.)

Az alábbi felsorolás egy rövid leírása a felülvizsgált taxonómia szintjeinek:

- Emlékezik – ez a korábban megtanult tények bemagolását és visszaadását jelenti. A tanuló valószínűleg nem értette meg a tanultakat. Igék, amelyek leírják ezt a szintet: leír, mond, keres
- Megért – Ezen a szinten a megtanult dolgokat fel tudja használni a tanuló problémamegoldás és döntéshozatal során. Igék, cselekvések, amelyek leírják ezt a szintet: megbeszélés, vázlat írása, magyarázat
- Alkalmaz – A harmadik szint az előzőre épül, és hozzáadja azt a képességet, hogy a tanuló fel tudja használni a megtanult anyagot új helyzetekben, minimális irányítás mellett. Igék, amelyek leírják ezt a szintet: felhasznál, szemléltet, megold
- Eleméz – Ez a szint magában foglalja a képességet arra, hogy a tanuló felismerje az összetartozó részeit egy bonyolult rendszernek, és megértse a kapcsolatot a részek és az egész között. Erre példa, amikor a tanuló feloszt egy bonyolultabb fogalmat egyszerűbb komponensekre, hogy jobban megértse a felépítését. Igék, amelyek leírják ezt a szintet: meghatároz, összehasonlít, magyaráz, kategorizál
- Értékel – Amikor a tanuló értékel, akkor rendelkezik azzal a képességgel, hogy megítélje az értékét valaminek, meghatározott kritériumok vagy szabványok alapján. Igék, amelyek leírják ezt a szintet: dönt, rangsorol, értékel, igazol
- Alkot – Ez a legmagasabb szintje a taxonómiának, és arra a képességre utal, hogy a tanuló össze tud rakni különböző részeket, annak érdekében, hogy kitaláljon egy, a tanuló számára új ötletet vagy tervet. Igék, amelyek leírják ezt a szintet: létrehoz, elképzél, (meg)tervez

Az informatikai biztonságtudatosságot (IB) meghatározhatjuk olyan módon, hogy a felhasználó milyen szinten értette meg a fontosságát az informatikai biztonság területén létező jó gyakorlatoknak. Másként fogalmazva az IB helyes, „biztonságos” szokások létrehozását, támogatását, fejlesztését és fenntartását jelenti (Abawajy, 2013.).

Példák az egyes szinteken, a phishing témájára alkalmazva:

- Emlékezés: Alapvető tények felidézése a különböző kiberveszélyekről, például a phishingről vagy a számítógépes vírusokról.
- Megértés: A phishing e-mailekhez kapcsolódó kockázatok és az erős jelszó fontosságának magyarázata.
- Alkalmazás: A megszerzett tudás alkalmazása phishing e-mail helyes azonosításával és megfelelően erős jelszó kiválasztásával egy új e-mail fiókhoz.

- Elemzés: Phising e-mailek, módszerek összehasonlítása, abból a célból, hogy meghatározásra kerüljenek a phising e-mailek közös tulajdonságai.
- Értékelés: Mely phising módszerek a leghatékonyabbak és miért.
- Alkotás: Új biztonsági szabályzat vagy irányelvek kidolgozása egy intézmény számára, a kockázatok és megoldások átfogó megértése alapján.

Az angol nemzeti alaptanterv (National Curriculum of England, 2013.) két célt határoz meg az információ-technológiával (IT) kapcsolatban. Minden tanuló legyen képes

- értékelni és alkalmazni az IT-t, beleértve új és szokatlan technológiákat, hogy analitikusan megoldjon problémákat,
- arra, hogy felelősségteljes, kompetens, magabiztos és kreatív felhasználója legyen az információs és kommunikációs technológiának (IKT).

Az alábbiakban példákat láthatunk az új magyar kerettantervből (2020) a javasolt tevékenységekre informatikai biztonság témakörében (NAT, 2020):

- Az adatok védelmét biztosító lehetőségek használata az online kommunikációs alkalmazásokban (5-8. évfolyam)
- Az elektronikus kommunikáció gyakorlatában felmerülő problémák, valamint az ezeket megelőző vagy ezekre reagáló biztonságot szavatoló beállítások megismerése, használata (5-8. évfolyam)
- Az adatbázisokra épülő online szolgáltatások, például az e-kereskedelem lehetőségeinek kipróbálása, vita azok biztonságos használatának lehetőségeiről
- A biztonsági beállítások lehetőségeinek elemzése, azok hatása, majd vizsgálata a különböző közösségi médiumok, mint online adatbázisok esetén
- A digitális eszközök biztonságos használatához szükséges lépések megtétele, az eszköz szoftveres karbantartása, vírusvédelme (9-11. évfolyam)

Az angol kerettanterv többször utal a Bloom-féle taxonómia magasabb szintjeire, mint a magyar kerettanterv. Az angol tanterv céljai jobban fókuszálnak a gyakorlati módszerekre, mint a megértésre és a tudásra. Az utóbbira utaló szavak inkább a magyar kerettantervben fordulnak elő. Ez egy filozófiai különbség a két ország tanterve között.

Chou et al (2011) négy kulcsfontosságú internetes biztonsággal kapcsolatos területet határozott meg, amelyeket ismerniük szükséges a tanároknak:

1. Biztonságos kommunikáció. Ez a terület annak megtanítására utal, hogy hogyan tudják a tanulók megvédeni magukat a vírusoktól, hackerektől, kéretlen levelektől (spam) és törvénytelen kereskedelmi ügyletektől, valamint hogyan tartsák biztonságban saját bizalmas információikat.
2. Információs etikett és információk megfelelő felhasználása. Ez a terület azzal foglalkozik, hogy miként lehet azonosítani a rosszindulatú pletykákat, pornográfiát, szexuális kényszerítést, félrevezető reklámokat és más offenzív tartalmat. Ugyancsak lefedi a tiszteletét a szerzői jogoknak és a digitális információk etikus használatát.
3. Biztonság a személyes emberi kapcsolatokban. Ez a terület magában foglalja az összes közösségi interakciót, beleértve az online kapcsolatépítést, személyes találkozásokat az interneten megismert barátokkal, online zaklatást és a digitális etikettet, különösen Web 2.0 korában, ahol a közösségi hálózatok állnak a figyelem középpontjában.
4. Biztonságos számítógép és internet használat. Ez egy vegyes kategória, amely magában foglalja a megfelelő eszközöket és munkakörnyezetet, a szem védelmét, illetve az egészséges testtartást.

A legtöbb gyermek számára Európában (9-16 éves életkor) az okostelefon a leginkább preferált eszköz arra, hogy felcsatlakozzanak a világhálóra. Ez gyakran azt jelenti, hogy gyermekek többsége napi szinten vagy szinte mindig használja az okostelefonját (Smahel et al, 2020).

3. Átadási módok

Mivel az informatikai biztonságtudatosság az a képesség, hogy észrevegyük vagy elkerüljük azokat a viselkedésmódokat, amelyek kompromittálják az informatikai biztonságot, ezért a tanítási módszerek nem alapulhatnak kizárólag a lexikális tudáson. Természetesen a megfelelő szókincs megismerése szükségszerű. Emiatt a frontális átadási módokat szükséges kiegészíteni olyan módon, hogy a tanulók ne csak megértsék az IB szókincsét, hanem hogy magasabb szintű gondolkodást érjenek el a Bloom-féle taxonómia alapján.

A kiterjesztett és virtuális valóság (Augmented Reality (AR) / Virtual Reality (VR)) és a számítógépes játékok előnyösek lehetnek, mert valós időben lehet hatékonyan tudást és készségeket átadni, a virtualitás miatt biztonságos a használata, és nagyobb bevonódást tesz lehetővé, mert iskolán kívül is lehet használni.

A szimuláció az egyik legjobb mód arra, hogy valaki megtanulja, hogyan viselkedjen különböző helyzetekben. Egy biztonságos környezetben „el lehet szenvedni” a következményeit a jó és a rossz döntéseknek, és ezáltal megtanulni egy helyes gyakorlatot. Sajnos, ez a módszer nagyon drága, és a környezet, illetve a játékszoftver kifejlesztése is sok erőforrást igényel. Hazánkban, általában az iskoláknak nincs erre anyagi erőforrása.

Az Amerikai Egyesült Államok haditengerészetének posztgraduális iskolája (Naval Postgraduate School) fejlesztett ki egy videojátékot, CyberCIEGE néven (Thompson et al, 2015). Ebben a játékban a játékos egy virtuális világban számítógépeket, hálózatot és embereket irányít. Egy virtuális cég céljai, illetve belső szabályai alapján a játékos fizikai, logikai és humán eszközöket, erőforrásokat, módszereket vehet be abból a célból, hogy megelőzzön egy kibertámadást. Lényegében a CyberCIEGE egy hálózati biztonságot szimuláló eszköz. Különböző helyzetekhez különböző forgatókönyveket hoztak léte, mind egy-egy külön hálózati biztonsággal kapcsolatos fogalom megtanításához, megértéséhez és alkalmazásához. A szoftver legnagyobb célja, hogy megtanítsa a hallgatóknak, hogy miként tudnak olyan rendszert építeni, amely minél kevésbé sérülékeny, illetve minél inkább rugalmas a támadásokkal szemben.

Egy komplex játékszoftver kifejlesztése drága, de léteznek online játékok, amelyekkel a tanuló megtanulhatja az IB különböző aspektusait. Egy jó példa az Anti-Phishing Phil (Sheng et al, 2007). Ezzel a játékkal a tanulók megtanulhatják, hogy melyek azok a linkek, amelyekre biztonsággal tudnak kattintani, és miért. Sajnos, ez a játék már idejétmúlt, mert nincs benne említés a https protokollról, illetve Flashben írták, ezért már böngészőben nem futtatható.

Az Interneten található játékok közül jó példa az Interland. Ez a játék megtanítja a gyerekeknek a digitális állampolgárság és internet biztonság alapjait, hogy magabiztosan fel tudják fedezni az online világot. Öt témában mélyíthetik el ismereteiket a gyerekek a játék használata közben: (1) hírek/információk megosztása (mit szabad megosztani ismerőssel és idegennel, és mit nem); (2) álhírek és fals információk felismerése (hogyan lehet a valódit a hamistól megkülönböztetni); (3) személyes adatok védelme és biztonsága (jelszókezelés); (4) kedves és tiszteletteljes viselkedés (bánjanak úgy másokkal, ahogyan szeretnék, hogy velük bánjanak); (5) tudatosan beszéljenek egy felnőttel, kérjenek segítséget, ha kétségük támad vagy bajba kerülnének.

A Magyar Államvasutak (MÁV) adott ki egy közlekedésbiztonsági játékot Ütközéspont címmel. Bár ez a játék nem a kiberbiztonsággal foglalkozik, mégis a módszereit fel lehet használni. A MÁV játékában egy baleseti helyszínélő munkáját kell elvégeznünk, ahol interaktív módon, illetve a játék által vezetve kell megvizsgálunk a baleset körülményeit, információt gyűjteni, következtetéseket levonni, és a végén egy tesztet kitölteni a megismert információk alapján. Hasonló módon lehet írni egy játékot pl. egy kibertámadás utólagos felderítéséhez.

Online videók is jó eszközök lehetnek, mert megtekinthetőek akár többször is, ahogyan szükség van rá. Egy osztályteremben, de akár a felsőoktatásban/felnőttoktatásban is megfelelő bevezetése lehet az adott témának egy ilyen videó. Ezek a rövidfilmek, filmrészletek segíthetnek együtt érezni a szereplőkkel, megérteni a helyzetüket stb. Fiatalabb korosztálynak szóló videók is elérhetőek, tehát akár a kezdetektől (3-4. osztály) lehet használni ezt az eszközt. Erre nagyszerű példa a Sheeplive projekt.

Eredetileg a „CS Unplugged” egy ingyenes tananyaggyűjtemény az informatika tantárgyhoz, amellyel különböző játékokon (kirakó, kártya), rajzeszközökön és szabadtéri aktivitásokon keresztül lehet különböző témaköröket tanítani, azokat bevezetni. A „CS Unplugged”-módszert olyan módszerként értelmezem, amikor számítógép használata nélkül tanítok informatikát. Ez a módszer akár társas- és szituációs játékokat, színházi nevelést, pszicho drámát is magába foglalhat (Jozifek, 2018).

Informatikai biztonsággal kapcsolatos „számítógép mentes” foglalkozások találhatóak a Code.org oldalon. A legtöbbjük óratervet, tanári videót és a szükséges eszközöket vagy azok leírását tartalmazza. Ezek a foglalkozások akár általános iskolában is felhasználhatóak.

A Common Sense Media elsősorban a Digitális állampolgárság (Digital Citizenship) tananyagán keresztül kínál „unplugged” tevékenységeket, amelyek célja olyan fogalmak oktatása, mint a digitális konfliktusok (digital drama), a számítási gondolkodás és a médiaműveltség. Példaként említhető a Digital Drama Unplugged feladat, amelyben a diákok szerepjáték segítségével dolgoznak fel különböző digitális konfliktushelyzeteket. A tanulók csoportokban dolgoznak, egy megadott segédanyagból származó forgatókönyvet játszanak el, amely egy digitális konfliktusokat tárgyaló videóra épül. A feladat célja, hogy ösztönözze a diákokat a konfliktusok enyhítésére szolgáló stratégiák gyakorlására, valamint az online kommunikáció kihívásainak – például a hangnem félreértelmezése vagy az anonimitás hatása – átgondolására.

A Digital Citizenship tananyaga számos más „offline” tevékenységet is integrál, amelyek különböző digitális állampolgársággal kapcsolatos témákra összpontosítanak. Ezek a feladatok ösztönözhetik a beszélgetést például arról, hogyan befolyásolja a közösségi média használata az érzelmeket, vagy milyen adatvédelmi kockázatokat hordoznak az új technológiák. Emellett magukban foglalhatják helyzetek elemzését annak érdekében, hogy a tanulók jobban megértsék az olyan kérdéseket, mint az online gyűlöletbeszéd, a megerősítési torzítás, valamint a pozitív online kapcsolatok kialakítása.

Társasjátékok (vagy bármilyen közös offline játék) alkalmas az adott téma megértésének segítésére, mert ezek

- képesek bevonni az embereket,
- lehetőséget adnak arra, hogy teszteljünk egy ötletet és kérdezzünk,
- olyan társas környezetet teremtenek, amely elősegíti az interakciót és a téma megbeszélését. (Denning et al, 2013)

Általában ezek a játékok nem igényelnek nagy előkészületeket, illetve nem függenek más erőforrásoktól. Jó példa társasjátékokra a Safer Internet által készített Lájkvadász társasjáték, illetve a Control-Alt-Hack nevű (angol nyelvű) kártyajáték (Denning et al, 2013).

Online tesztek jó eszközök a megértés mérésére. Fontos azonban, hogy ezek a kérdőívek gyakorlati kérdéseket tartalmazzanak, amelyek egy-egy helyzetre mutatnak. Nagyon jó példa erre a „Phishing Quiz by Jigsaw”. Ez a teszt elkéri a tanuló nevét és e-mailcímét (amit nem fogja eltárolni), hogy a teszt és a szituációk még személyesebbek legyenek. Az összes feladat nagyon gyakorlatias, és minden válasz után a tanulók bővebben olvashatnak az adott feladat által említett szituációról.

1. táblázat: Összefoglaló táblázat az eszközökről

Eszköz neve	Bloom-taxonómia szintje
Kiterjesztett és virtuális valóság	alkalmazás (3. szint) – elemzés (4. szint)
Szimuláció	alkalmazás (3. szint) – értékelés (5. szint)
Játék (számítógépen, okoseszközön)	alkalmazás (3. szint) – alkotás (6. szint)
Videók, filmek (online, offline)	alkalmazás (3. szint) – elemzés (4. szint)
Társasjáték	alkalmazás (3. szint) – értékelés (5. szint)
CS unplugged-eszközök	alkalmazás (3. szint) – elemzés (4. szint)
Online tesztek	alkalmazás (3. szint) – értékelés (5. szint)

4. Összefoglalás

Összefoglalva elmondható, hogy a fentebb tárgyalt eszközök és módszerek elérik legalább a Bloom-féle taxonómia harmadik szintjét (alkalmazás), illetve a különböző féle játékok lehetőséget adnak az elemzésre és az értékelésre is. A taxonómia legmagasabb szintjét a CyberCIEGE szoftverrel tudja elérni a hallgató, amikor már eljut oda a tanulmányiban, hogy ő maga hozzá létre a virtuális cég belső szabályait, és az ehhez kapcsolódó forgatókönyveket. Természetesen nem elhanyagolható a megfelelő szókinccs és elméleti tudás átadása, amelyek ismerete és megértése nélkül nem lehetne a taxonómia magasabb szintjeire eljutni. Viszont csupán az ismeretre és a megértésre nem lehet alapozni.

Nagyon fontos, hogy olyan módszert találjunk és alkalmazzunk, amely fiatalabb gyermekeknél is használható, mert nagy többségük kerül szembe veszélyes helyzetekkel a világhálón és a közösségi médiában. „Eszközökre” van szükségük, hogy el tudják dönteni, mi biztonságos és mi nem. A „CS Unplugged” foglalkozásokkal meg lehet tanítani ezeket a fogalmakat, akár kisiskolás kortól.

A játékokkal (offline is), való tanítás/tanulás segít a tanulóknak abban, hogy teszteljék az ismereteiket, de nem csupán a fogalmak ismeretét, hanem azok valóságos alkalmazását is.

Kutatásom következő lépése egy olyan kiberbiztonsági tanterv kialakítása az új magyar kerettanterv alapján, amely a fenti módszereken alapul, valamint egy egyetemi kurzus létrehozása a kiberbiztonság tanítási módszereiről tanárszakos hallgatók számára.

IRODALOMJEGYZÉK

- Abawajy, J. (2013): User preference of cyber security awareness delivery methods, *Behaviour & Information Technology*, 33:3, 237-248, DOI: 10.1080/0144929X.2012.708787
- Anderson, Lorin W. és Krathwohl, D. R. (2001, szerk.) *A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives, Complete Edition*. Longman
- Anti-phising game videó, <https://videos.proofpoint.com/watch/yYyo3hfmcnXRjpRPCQJCVH> [2025. 11. 13.]
- Chou, C. és Peng, H. (2011): Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience, *The Internet and Higher Education*, Volume 14, Issue 1, 44-53, ISSN 1096-7516
- Control-Alt-Hack társasjáték <https://www.controlalthack.com/> [2025. 11. 13.]
- CS Fundamentals Unplugged Lessons, <https://code.org/curriculum/unplugged> [2025. 11. 13.]
- CS Unplugged <https://csunplugged.org/en/> [2025. 11. 13.]
- Common Sense Education: Digital Drama Unplugged <https://www.common sense.org/education/digital-citizenship/lesson/digital-drama-unplugged> [2025. 11. 15.]
- Common Sense Education: Digital Citizenship Curriculum <https://www.common sense.org/education/digital-citizenship> [2025. 11. 15.]
- Denning, T., Lerner, A., Shostack, A. és Kohno, T. (2013): Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education. *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (CCS '13)*. Association for Computing Machinery, New York, NY, USA, 915–928.
DOI: <https://doi.org/10.1145/2508859.2516753>
- Jigsaw Phishing Quiz, <https://phishingquiz.withgoogle.com/> [2025. 11. 13.]
- Jozifek, Zs, (2018, szerk.) *Benne vagy? A színházi nevelés alkalmazási lehetőségei a bullyinggal kapcsolatos tudatosság növelésére*, Nyitott Kör Egyesület, Budapest
- Livingstone, Sonia, Haddon, Leslie, Görzig, Anke és Ólafsson, Kjartan (2011): *Risks and safety on the internet: the perspective of European children: summary*. EU Kids Online, Deliverable D4, EU Kids Online Network, London, UK.
- MÁV közlekedésbiztonsági játéka: Ütközéspont <https://utkozespont.hu/> [2025. 11. 13.]
- Interland játék, https://beinternetawesome.withgoogle.com/hu_hu/interland/ [2025. 11. 13.]
- Lájkvadász társasjáték <https://moderniskola.hu/2021/01/nemsokara-itt-a-biztonsagos-internet-nap/> [2025. 11. 13.]
- Magyar kerettanterv (2020): https://www.oktatas.hu/koznevelés/kerettantervek/2020_nat [2025. 11. 13.]
- OECD (2023): *PISA 2022 Results (Volume I): The State of Learning and Equity in Education*, PISA, OECD Publishing, Paris, <https://doi.org/10.1787/53f23881-en>
- Sheeplive <https://sheeplive.eu/> [2025. 11. 13.]
- Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L., Hong, J. és Nunge E. (2007): Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish. *Proceedings of the 2007 Symposium On Usable Privacy and Security*, Pittsburgh, PA, July 18-20

- Smahel, David, Machackova, Hana, Mascheroni, Giovanna, Dedkova, Lenka, Staksrud, Elizabeth, Ólafsson, Kjatar, Livingstone, Sonia és Hasebrink, Uwe (2020): *EU Kids Online 2020: Survey results from 19 countries*. EU Kids Online Doi: 10.21953/lse.47fdeqj01ofo
- Sousa, David A. (2006): *How the brain learns*. 3rd ed. Corwin Press
- The national curriculum of England: Computing (2013)
<https://www.gov.uk/government/publications/national-curriculum-in-england-computing-programmes-of-study/national-curriculum-in-england-computing-programmes-of-study>
[2025. 11. 13.]
- Thompson, M. F. és Irvine, C. E. (2015): CyberCIEGE: A Video Game for Constructive Cyber Security Education, *Call Signs, a publication of the United States Naval Aerospace Experimental Psychology Society*, Volume 6, Issue 2, Fall
- Van Niekerk, J. és Von Solms, R. (2013): Using Bloom's Taxonomy for Information Security Education. In. Dodge, R. C. és Fatcher, L. (szerk.) *Information Assurance and Security Education and Training*. WISE 2013, WISE 2011, WISE 2009. IFIP Advances in Information and Communication Technology, vol 406. Springer, Berlin, Heidelberg, (2013)

TOOLS FOR SECURITY AWARENESS EDUCATION TO ENHANCE ENGAGEMENT

Abstract

Nowadays, there are many ways to deliver knowledge about security awareness, such as augmented/virtual reality, web-based materials, online videos, games (both online and offline), and “unplugged” methods. The article suggests that the most effective methods are those that can achieve higher levels of thinking according to Bloom's taxonomy. Finding and applying a good teaching method is very important, since learners are exposed to the dangers of the Internet at an increasingly younger age.

Keywords: *Bloom's taxonomy, engagement, information security, delivery methods, teaching methods*