DOI: 10.38146/BSZ-AJIA.2025.v73.i5.pp1067-1078

Az információbiztonság-tudatosság fejlesztése

The Improvement of information security awareness

Stranszki Péter
beosztott munkatárs
Információs Hivatal
pstranszki@ih.gov.hu

Nyári Norbert
főosztályvezető-helyettes, doktorandusz
Információs Hivatal
Óbudai Egyetem,
Biztonságtudományi Doktori Iskola
nnyari@ih.gov.hu

Absztrakt

Cél: A publikáció célja, hogy bemutassa az információbiztonság-tudatosság fejlesztésének szükségességét és annak módszereit, valamint az elmúlt évtized legelterjedtebb csalási formáit.
Módszertan: A tanulmány több hazai kutatás és szakcikk feldolgozásával azok szintézisét végzi el.
Megállapítások: Az információbiztonság-tudatosság fejlesztése minden korosztály számára fontos, mivel a lakosság nagy többsége napi szinten kapcsolódik az internethez. Ehhez szükség van a rendszeres oktatásra, valamint az aktuális támadási trendek ismeretére. Fontos, hogy a fejlesztés, oktatás során az online felhasználók elméleti ismeretek mellett a lehető legtöbb, a mindennapi életben is használható gyakorlati ismeretre is szert tegyenek. A figyelemfelkeltéshez szükséges lehet az egyes oktatási módszertani elemek kombinálása is.
Érték: A szerzők szándéka szerint a publikáció segít bemutatni az információtudatosság fejlesztésének fontosságát és szükségességét.

Kulcsszavak: információbiztonság-tudatosság, oktatás, csalások, kiberbiztonság

Abstract

Aim: The purpose of the publication is to present the need for the improvement of information security awareness and its methods, as well as the most common forms of fraud in the last decade.

A szerzők a kéziratot magyar nyelven nyújtották be. Benyújtás: 2024. 09. 02. Átdolgozás: 2024. 12. 16. Elfogadás: 2025. 01. 10.

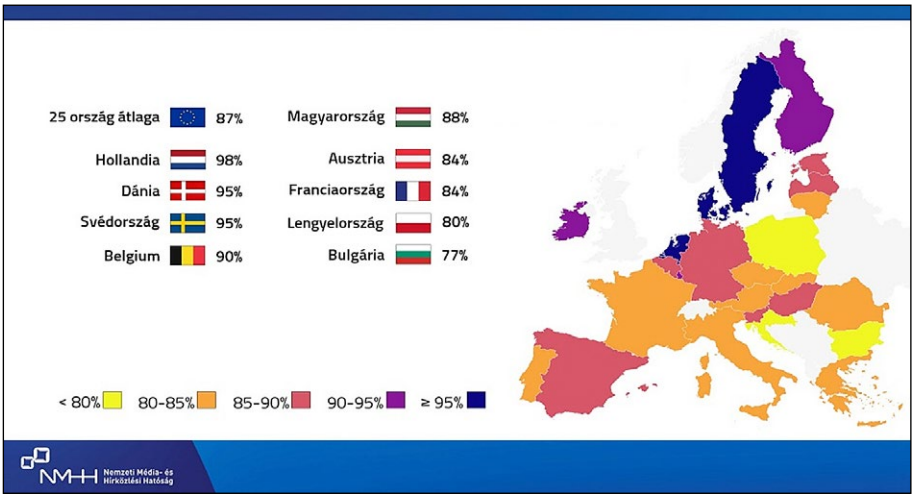
Methodology: The study synthesizes several domestic researches and technical articles.
Findings: The development of information security awareness is important for all age groups, as the majority of the population is connected to the Internet on a daily basis. This requires regular education and knowledge of current attack trends. It is important that in the course of education, in addition to theoretical knowledge, online users also acquire as much practical knowledge as possible that can be used in everyday life. In order to attract attention, it may be necessary to combine individual educational methodological elements.
Value: According to the author's intention, the publication helps to demonstrate the importance and necessity of improvement of information awareness.

Keywords: information security awareness, education, fraud, cyber security

Bevezetés

Az elmúlt tíz évben a 16–74 év közötti lakosság között az internetet használók száma Magyarországon közel másfélszeresére nőtt, manapság a magyar lakosság közel 90%-a használja a világhálót, míg tíz évvel ezelőtt ez a szám még csak 66% volt.

1. számú ábra
A világhálót napi rendszerességgel használók aránya a 16-74 éves korosztályban az egyes uniós országokban



Forrás. URL1.

Az internet elterjedésével nemcsak az elérhető szolgáltatások köre, a megtalálható információk mennyisége, illetve a felhasználók száma sokszorozódott meg, hanem a nagy számok törvénye alapján a felhasználókra leselkedő veszélyek száma és az okozott kár mértéke is. Megjelentek új veszélyforrások, a visszaéléssel foglalkozó személyek, csoportok száma is megnövekedett. A technológia fejlődésével a visszaélések is sokkal kifinomultabbak lettek: míg akár 1–2 évvel ezelőtt egy szöveges üzenetben (például e-mail, sms) érkező szövegről a magyartalansága miatt gyorsan el lehetett dönteni, hogy nem valós adattartalmú, nagy valószínűséggel csalók által kreált irományról van szó, addig ma a mesterséges intelligencia korában tökéletes magyarsággal leírt üzenetben próbálják a csalók az adatainkat, értékeinket megszerezni. Feltörhetik hackerek az e-mail-fiókjainkat, bankszámla-hozzáférésünket, bármilyen előfizetéshez tartozó online fiókunkat, és ellophatják személyes vagy banki adatainkat, elutalhatják pénzünket. Személyes adatainkkal, feltört fiókjainkon keresztül megszemélyesíthetnek minket, megtévesztve ezáltal másokat. Mivel manapság az internetes jelenlét hozzátartozik a mindennapjainkhoz, ezért ezek a támadási lehetőségek bárkit érinthetnek.

Ahhoz, hogy a fent említett támadásokat minél nehezebben és kisebb arányban tudják sikerre vinni, olyan különféle biztonsági megoldásokat kell bevetnünk, mint például biztonsági eszközök, szoftverek használata, illetve védett, zárt kommunikációs rendszerek kialakítása, az egyes rendszerelemek fizikai felügyelete. Egy 2018. évi információbiztonsági szakmai fórumon elhangzott előadás is kifejti, hogy *„egy rendszer annyira sebezhető, mint ahogy a leggyengébb láncszeme”* (Bubán, 2018), és mint minden rendszerben, itt is általában az ember a leggyengébb láncszem. Ezért minden informatikai rendszert használónak el kell sajátítania egy gondolkodásmódot, biztonsági szabályokat, online viselkedési normákat annak érdekében, hogy a manapság nagyrészt elektronikus formában elérhető értékeit (pénz, adatok, dokumentumok, licencek, pótolhatatlan képek stb.) a lehető legnagyobb biztonságban tudhassa. Ezen felül *„mint minden preventív eszköz, az információbiztonság tudatosság képzés hatékonyabb és olcsóbb, mint az incidenst követő korrektív eszközök, eljárások, folyamatok”* (Bubán, 2018).

A biztonságtudatos gondolkodásmód sokféleképpen elsajátítható, akár egy oktatás vagy képzés során, akár egy kampány keretében, vagy egy nagyobb rendezvény során. A közös mindegyik formában az ismeretanyag, a szemléletmód átadásának szándéka. Mindegyik esetben a cél, hogy bemutatásra kerüljenek az aktuális veszélyforrások, azok legjellemzőbb megjelenési formái, valamint a lehetséges következmények felvázolása mellett a helyes reakció.

Fontos tisztában lennünk azzal is, hogy a legfontosabb értékeink közé tartoznak a személyes adataink, amelyeket kizárólag indokolt esetben, a lehető legnagyobb körültekintéssel szabad kiadni.

Továbbá azt is észben kell tartania az online világban tevékenykedőknek, hogy ha megtörténik a baj és információbiztonsági incidens részesévé válnak, milyen lépéseket szükséges megtenniük, kihez fordulhatnak vagy kell fordulniuk a károk enyhítése, a károk kezelése, vagy a további károk megelőzése érdekében.

Napjaink internetes csalásainak főbb típusai és azok jellemzői

Az internetes csalások sokfélék lehetnek: egy részük a jóhiszeműségünkre alapozva próbálja megszerezni az adatainkat, más esetek pedig a megtévesztésen alapulnak. A közös bennük, hogy az elkövetők minden esetben a valós személyüket elfedve, anonim módon követik el a csalásokat (Herédi, 2022). Sok esetben a csalók pszichikai nyomás alá helyezik az áldozatukat, sürgetik, siettetik, ez által próbálják megakadályozni, hogy végig tudja gondolni, hogy milyen adatokat ad ki. Általánosan elmondható minden csalás típusról, hogy olyan, az áldozat számára nagy előnnyel kecsegtető ajánlatokkal, lehetőségekkel próbálják a csalók rávenni őket az általuk megtervezett viselkedésre, amelyek nehezen visszautasíthatók. Így kihasználják azt az emberi gyengeséget, hogy azt higgye az áldozat, hogy egyszer neki is lehet szerencséje.

A jóhiszeműségre alapozó csalások közül az elmúlt években két jelentősebb számban megjelenő típus fordult elő. Az egyik fajtában, az úgynevezett „unokázós csalások" esetében jellemzően idősebb embereket kerestek meg közeli családtagnak vagy unokának kiadva magukat. Jellemzően pénzt csaltak ki az áldozatoktól a legkülönfélébb kitalált történetekkel. Egy másik jellemző változat volt, hogy a csalók telefonon megkeresték az áldozatot a számlavezető bankja nevében, majd egy éppen a bankszámláján folyamatban levő gyanús utalásról tájékoztatták, amit most még meg tud akadályozni úgy, hogy egy általuk meghatározott – és természetesen általuk kezelt – folyószámlára utalja a pénzét.

A megtévesztésen alapuló csalások során más személynek, cégnek adták ki magukat a csalók, és ezek nevében próbálták megszerezni jellemzően a banki adatokat. Az elmúlt években több bank (például az OTP) nevében kerültek adathalász e-mail üzenetek elektronikus postafiókokba, amelyek tartalmaztak egy olyan linket, ami a bank honlapjára nagyban hasonlító oldalra irányít. Ezen az oldalon a csalók kérik, hogy különböző okok miatt (például fiók kompromittálódása, bankot ért támadás miatti biztonsági okokból) adja meg az ügyfél azokat a banki adatokat, amellyel a valós honlapon be tudnak jelentkezni a felhasználó fiókjába.

Ugyancsak megtévesztésen alapuló támadástípus, hogy a fentihez hasonló folyamatról különböző csomagszállító cégek (például Magyar Posta, Foxpost, DPD) nevében küldenek elektronikus üzenetet, amelyben jelzik, hogy kifizetetlen csomagja van az ügyfélnek, amit az e-mailben lévő linkre kattintva lehet kifizetni.

Szintén jellemző csalási forma volt korábban az áldozat részére küldött hamis értesítő üzenet, ami egy nyereményjátékon elért sikerről szólt, de a nyeremény átvételéhez szükséges még néhány adat megadása, amit az üzenetben lévő linken keresztül lehet megadni.

Korábban jellemző volt és ma is kedveltek az olyan típusú üzenetek, amelyek csatolmányt tartalmaznak, és amint az üzenet címzettje megnyitja ezt a rejtett kódot tartalmazó csatolmányt, egy olyan kártékony program kerül letöltésre a számítógépére vagy a telefonjára, amelyen keresztül a csalók lényegében átveszik az irányítást a gép és a rajta tárolt adatok fölött.

A mesterséges intelligencia (MI) megjelenésével a fenti támadási típusok sokkal kifinomultabbak lettek. Az MI révén eltűnnek az idegen nyelvről fordított szövegek „magyartalanságai", illetve a félrevezető honlapok minősége is „emelkedett", azaz sokkal megtévesztőbbé váltak. Az MI megjelenésével szélesedtek a támadók lehetőségei, mivel az írott szövegen kívül az MI révén a csalók már hangot is tudnak utánozni, létrehozni, így könnyebben el tudják hitetni a nem felkészültekkel, hogy egy ismerőssel, baráttal beszélnek. Internetes kereskedelemmel foglalkozó felületeken az MI megjelenésével viszont már nemcsak az eladók kerülhetnek megszemélyesítésre, hanem akár a vevők is. Ebben az esetben vevőként jelentkeznek a csalók, és a terméket egy csomagküldő szolgálattal történő szállítással kérik. Egy, a csomagküldő szolgálat honlapjához hasonló honlapon különböző adatok megadását kérik, amikkel az eladó bankszámlájához hozzáférnek.

A legfrissebb hírek szerint a csalók már szállásadó oldalak nevével is visszaélnek (URL2). A különféle MI eszközök segítségével nyelvtanilag kifogástalan e-mailek generálásával és küldésével könnyűszerrel el tudják hitetni a potenciális áldozatokkal a megkeresés eredetiségét, valódiságát és hitelességét.

A fent részletezett csalásformák mellett a legelterjedtebbek közé tartoznak napjainkban a hamis befektetési ajánlatok, hamis webáruházi ajánlatok, online térben hirdető eladók árverése, közösségi médián keresztüli adatlopás, hamis szolgáltatói ügyintézés a közösségi médiában (Angler phishing), hamis tranzakciók jóváhagyása, hamis wifi-hálózat létrehozása (Evil twin phishing), vagy meghamisított banki oldalak (URL3).

A figyelemfelhívás fontossága és megjelenési formái

A biztonságtudatos gondolkodás kialakítása nem csak az egyén, de csoport vagy társadalom szinten is megjelenő igény, mivel sok esetben egy kompromittálódott informatikai eszköz nem az elérendő cél. Ezeket a támadók ugródeszkaként,

álcaként használják a tényleges kilétük elfedéséhez, tehát a támadások elleni védekezéssel nemcsak saját adatainkat, hanem a másokkal fenntartott kapcsolatainkat, illetve a kapcsolatok adatainak biztonságát is növeljük. Ebből adódóan fontos, hogy a különböző módon közvetített ismeretek, figyelmeztetések, tanácsok elérjenek a célközönséghez, és hasznosuljanak, azaz a felhasználók tudatosabban használják az internetet, és egyre kisebb arányban legyenek a csalók áldozatai. A másik fontos oka a biztonságtudatos gondolkodás kialakításának, hogy az internetes bűnözés 2025-re globális szinten eléri a 30 milliárd dollárt, ami közel a duplája a 2021-es 17,5 milliárd dollárnak (URL4). Ez az összeg egy alacsonyabb befektetéssel, mint a megelőzés, tudatosságra való felhívás vagy a védelem, csökkenthető.

Egy 2023-ban készült tanulmány keretében egy 220 fős mintán vizsgálták a piaci szegmensben dolgozók információbiztonsági tudatossági szintjét korosztályokra lebontva (Habók, 2024). Bár a kutató nem kifejezetten információbiztonsági szakember, a kutatásban az általa használt módszert több információbiztonsági szaklap is relevánsként értékelte (Habók, 2024).

A kutatásban részt vevők életkoruk összetétele szerint vizsgálva nem követik a Központi Statisztikai Hivatal által hivatalosan közzétett munkaerőpiaci viszonyokat, 90%-a az X (43–58 év), illetve Y (27–42 év) generációból került ki; ez az életkorbeli súlyozás a demográfiai eredményeket befolyásolta a kutatás értékelésekor.

Ebből a kutatásból kiderült, hogy *„az életkor és az információbiztonsági tudatosság közt gyenge negatív korreláció mutatható ki, tehát valamelyest az idősebbek kevésbé teljesítettek jól a kognitív területen”* (a mérőszám 0-hoz közeli negatív értéket mutat, ami enyhe csökkenés).

Minél többször és minél különbözőbb környezetben hallhatók az esetleges veszélyekről szóló figyelmeztetések, illetve a helyes viselkedésformák, annál jobban tudatosul az emberekben, mit kell tenni, ha mégis csalók próbálkoznának adataik, értékeik megszerzésével. Ebből következik, hogy ha különböző információs csatornákat együttesen használva közvetítjük az információbiztonság fontosságát, akkor jobban rögzülnek az átadott információk és jobban beépülnek a gondolkodásmódba.

A fent idézett kutatás során a résztvevők 2/3-a arra a kérdésre, hogy *„Milyen forrásból tájékozódnak információbiztonsági hírekről”*, a *„Podcastot hallgatok a témában”*, *„Konferencia/meetup előadásokat hallgatok”*, *„Cikkeket/Blogbejegyzéseket olvasok”*, illetve *„Egyéb”* válaszlehetőségek közül legalább egyet megjelölt, és csak 1/3-uk jelölte meg a *„Nem foglalkozom a témával”* válaszlehetőséget. Ez azt mutatja, hogy az emberek nagyobb része nyitott az információbiztonság téma iránt, érdeklik az ezzel a témával kapcsolatos információk.

A kutatás szintén rámutatott arra, hogy a megkérdezettek nagyobb része bár érdeklődik a téma iránt, aktívan keveset tesz a szabadidejében azért, hogy az ismereteit ezen a téren bővítse, frissítse.

A fentiekből látszik, hogy igény mutatkozik a téma iránt, de ezt olyan formában kell tálalni, ami nem veszi el az emberek szabadidejét. Mivel a tudás megszerzése és fenntartása mindenki érdeke, olyan ismeretátadási, tudatosítási helyszínt és formát kell keresni, amit támogat a munkáltató és munkaidőben történik.

A legkézenfekvőbb lehetőség a munkahelyi/iskolai oktatások, továbbképzések formája, mivel mind a munkahely, mind az egyén számára hasznos az ott elhangzott információk átadása.

A munkáltató egyik fő érdeke az, hogy a munkavállalók tisztában legyenek a munkahelyen használt informatikai rendszerekkel és az ezekkel kapcsolatos eljárásrendekkel, helyes magatartási formákkal. A különféle továbbképzéseken a munkavállaló számára hasznos információkat kell átadni, amelyek a munkahelyi rendszerek használatán túl más esetekben is előnyére válhatnak. A munkahelyi képzéseket célszerű rendszeresen megszervezni, ezáltal is biztosítva az alkalmat a gyakorlati információk átadásán túl a szabályozási környezet lényeges elemeinek áttekintésére is. Ennek keretében fel lehet hívni a figyelmet az előző oktatási alkalom óta eltelt időszakban tapasztalt hiányosságokra, az előfordult információbiztonsági incidensek kivizsgálása során tett megállapításokra és általánosan a típushibákra és azok javítására.

Emellett iskolai rendszerű képzésben hasznos lehet egy új téma bevezetésekor annak biztonsági aspektusainak bemutatása, átbeszélése. Úgy a munkahelyi továbbképzések, mint az iskolai képzés esetében fontos információátadási mód lehet, ha rövid formában bemutatásra kerülnének az aktuális veszélyek, veszélyforrások, azok megjelenési formái és a lehetséges védekezési metódusok.

Fontos, hogy az információátadás rendszeres legyen, mivel szinte hétről-hétre új veszélyforrások, támadási formák kerülnek napvilágra, amelyekre adott esetben az eddigiektől eltérően kell reagálni. Ennek a formája lehet személyes oktatás, tematikus weboldal, rendszeres hírlevél. Emellett lehet tematikus szakmai napot, kampányt szervezni, ahol a résztvevők akár játékos formában megismerkedhetnek az aktuális támadói és információvédelmi trendekkel, azok különböző megjelenési formáival és a hatékony védekezési módszerekkel.

Sok esetben az elméletben elsajátított tudás gyakorlatban történő alkalmazása nehézségekbe ütközik. Ehhez nyújthatnak segítséget az elméleti ismeretek gyakorlati alkalmazását oktatási céllal tesztelő feladatok. Ennek kiváló példája lehet egy egyetemi előadáson elhangzott szemléltetés, amikor egy nagyvállaltnál az információvédelmi csapat adathalász levelek kiküldését követően megvizsgálta, hogy a címzetti kör mekkora hányada lépett tovább a levélben

kért linken keresztül. A linkre való kattintást követően a címzett azonnal visszajelzést kaphat a cselekedete helytelenítéséről, és bemutatásra kerülnek azok a jelek, amiből megállapíthatta volna, hogy az érkezett elektronikus levél hamis. Ezt kiegészítve egy versennyel, amelynek végén a jól szereplők jutalomban részesülnek, felkeltik a munkatársak érdeklődését.

Az információbiztonság-tudatosság oktatását már abban az életkorban el kell kezdeni, amikor az első alkalommal a felhasználó kezébe kerül egy informatikai eszköz. Mivel egy 2020-as kutatás szerint a gyermekek már 9–10 éves korban is több órát töltöttek online (Meggyesfalvi, 2023), ezért az oktatást, a biztonságtudatosságra való nevelést a lehető leghamarabb el kell kezdeni. Már az első alkalmakkor el kell mondani, hogy mit szabad, mit nem szabad, bár amíg az eszköz nem csatlakozik az internetre, addig legfeljebb a rendelkezésre állás sérülhet, illetve adatvesztés történhet. Már ekkor tudatosítani kell a gyermekekben, hogy az informatikai eszközök használatának lehetnek veszélyei, és ezért oda kell figyelniük, hogy mit, hogyan csinálnak. Egy hálózatba kapcsolt informatikai eszköz használatbavételekor azonban már sok mindenre fel kell hívni a figyelmet. A manapság használatos szoftverek, applikációk gyakran tartalmaznak vásárlási lehetőséget, mint például reklámmentességet, vagy plusz előnyöket, illetve kérhetik különböző adatainkat regisztráció, illetve az eszközünk követése céljából. Erre a gyerek 8–10 éves korától kerülhet sor. Ekkor – kortól és érettségtől függően – először csak azt kell megtanulnia, hogy csak azt csinálhat, amit a szülő megenged, később azt is, hogy mikor milyen adatok adhatók meg, amivel még nem élhetnek vissza esetleges eltulajdonításuk esetén. Nagyobb, 12–14 éves kortól már megtanítható, hogy mely szoftverek tekinthetők biztonságosnak, milyen típusú alkalmazások használatát kell kerülni. Ezzel párhuzamosan már el lehet mondani, hogy az interneten milyen lehetséges támadásokkal találkozhatnak, ezeknek mik a főbb jellemzőik, és mit kell csinálniuk, ha találkoznak velük.

Szintén fontos, hogy amennyiben a gyerekek közvetlen környezetében történik egy, az információbiztonságot befolyásoló esemény, akkor arról a megfelelő körben beszélni kell, el kell magyarázni a történteket, az elkövetett hibákat, fel kell hívni a figyelmet a figyelmeztető jelekre, és át kell beszélni a helyes viselkedést.

Az iskoláskorú fiatalok számára történő információátadás egy lehetséges formája a gamifikáció, amelynek során az információ játékos formában (akár applikáció, akár fizikai játék) kerül átadásra. Egy 2021-es tanulmány megállapította, hogy a gamifikációs módszer *„képes biztosítani a hatékony tudástranszfert és a megszerzett tudás magabiztos alkalmazását, ezáltal pozitív irányban befolyásolja a felhasználók biztonságtudatosságát”* (Legárd, 2021). Azonban csak kiegészítő oktatási módszerként használva érhető el a kívánt pozitív hatást. Ahhoz,

hogy ezzel a módszerrel eredményre jussunk, megfelelően kell meghatározni az átadni kívánt információk körét, jól kell felépíteni a játékos feladatokat, ezáltal folyamatosan fenntartva a fiatalok érdeklődését.

Hozzá kell tenni azonban, hogy a fiatalok iskolában történő tanítása során is jól meg kell választanunk a tananyagot. Egy 2021-es tanulmány keretében készített kutatás rámutatott arra, hogy a tanulók alig több mint fele egyáltalán nincs, vagy csak részben van tisztában a böngészőprogramok biztonságával (52%), és kevesebb mint fele az elektronikus tanulási környezet biztonságával (48%) és az internetre kapcsolódás biztonságával (47%) (Bottyán, 2021). Tehát elmondható, hogy a kutatásban részt vett tanulók közel 50%-a úgy használja az internet szolgáltatásait, hogy nincs tisztában azzal, hogy biztonságos módon teszi-e, amit tesz, mindent megtett-e annak érdekében, hogy ne legyen egy támadás áldozata.

Az Y-generáció információbiztonsági tudatosságával kapcsolatban készült egy tanulmány (Bak & Kelemen-Erdős, 2022), amely felmérte az Y-generáció tudásszintjét. A tanulmány eredménye azt mutatta, hogy a vizsgált „*alanyok annak ellenére, hogy eltérő mértékben és mélységben rendelkeznek információkkal a különböző kibertámadásokról, azok módjáról, következményeiről, valamint azok kiváltó okairól, könnyelműen bánnak saját és személyes adataik védelmével”*, valamint a *„biztonságtudatosságuk nem megfelelő szintű”* (Bak & Kelemen-Erdős, 2022).

Az iskolai oktatás, illetve a gamifikációs módszer elsősorban a fiatalokra alkalmazható, külön kell szólni az idősebb, 60 feletti korosztályról, akik „megélték” az internet elterjedését, fejlődését. Ennek a korosztálynak sokszor nagy problémát okoz, hogy általában nem kaptak semmilyen tájékoztatást, képzést nem csak az internet használatával, de az egyes szoftverek, alkalmazások használatával kapcsolatos biztonsági kérdésekről sem. Mivel az elmúlt tíz évben a bevezetésben található 1. számú ábrán bemutatott módon nőtt az internet használata, általában csak arra fordítottak a felhasználók figyelmet, hogy megtanulják az éppen aktuálisan használt szoftverek kezelését. Mindezek mellett ez a korosztály nehezen tudja elképzelni, hogy léteznek olyan veszélyek is, amelyeket közvetlenül nem látnak, illetve hallanak. Többnyire „vakon” megbíznak egy használt szoftver alap biztonsági beállításaiban, és mivel nem látják a támadókat, nem ismerik a különböző támadási módszereket, ezért nem vagy csak nehezen tudják elképzelni, hogy ők is az internetes csalások célpontjaivá válhatnak. Viszont éppen azért, mivel nem vagy csak nagyon kis mértékben mernek a megszokott felhasználási módtól eltérni, ezért általában feltűnik, ha valami nem a szokásos módon történik, és az ilyen esetekben nem mernek kilépni az addigi felhasználás komfortzónájából.

Ma már egyre több kezdeményezés található az interneten, amelyek célja a tájékoztatás, az edukáció, a felhasználók figyelmének felhívása az online tér biztonságot veszélyeztető kockázataira. A Nemzeti Kibervédelmi Intézet honlapján található Tudásközponton túl állami, részben pénzügyi, részben rendvédelmi szervek összefogásával működik a KiberPajzs, de független pénzügyi szolgáltatók, mint a Mastercard vagy Wise is rendelkeznek kiberbiztonsági honlappal. Ezen portálok célja, hogy röviden és közérthetően összefoglalja az internetes csalások legfőbb jellemzőit, és egyben tanácsot ad, hogy hogyan lehet kivédeni ezeket. Ezek az oldalak, információgyűjtemények kitűnően hasznosíthatók oktatások alapjaként, kiegészítéseként, vagy tájékozódásképpen.

Összefoglalás

Az internet elterjedésével megnőtt a különböző online csalások száma, illetve a csalások által okozott kár nagysága. Véleményünk szerint a hatékony védekezéshez szükséges, hogy ismerjük a lehetséges támadási formákat, illetve azok legfőbb jellemzőit. A cikkben röviden bemutatásra került, hogy miért fontos az információbiztonság-tudatosság, és felsorolásra kerültek napjaink legelterjedtebb internetes csalási formái, valamint azok jellemző megjelenési, végrehajtási formái.

Mint minden rendszerben, az információbiztonság-tudatosság rendszerében is az ember a leggyengébb láncszem. Több tanulmány eredményeit felhasználva levezetésre került, hogy az egyes korosztályok milyen információbiztonsági tudással rendelkeznek, illetve milyen forrásokat használnak az információbiztonsággal kapcsolatos hírek beszerzésére. Meglátásunk szerint a tudásszintet különböző módszerekkel, figyelemfelhívásokkal lehet fejleszteni, naprakészen tartani; gondolunk itt az elméleti oktatás különböző formái mellett azok gyakorlatba történő átültetésére, és az ismeretátadás sikerességének tesztelésére.

Azonban tény, hogy mindegyik korosztály más, és másképpen lehet megszólítani, de mindenképpen szükséges a saját és a környezetünk védelme érdekében.

Általánosságként elmondható, hogy az információbiztonság-tudatos gondolkodás kialakítása, az információk naprakészen tartása minden online felhasználó számára fontos.

Felhasznált irodalom

Bak G., & Kelemen-Erdős A. (2022). Információbiztonság-tudatosság az Y generáció szemszögéből, kvalitatív megközelítés alapján. *Had-mérnök*, *17*(4), 81–95. https://doi.org/10.32567/hm.2022.3.6

Bottyán L. (2021). Információbiztonsági tudatosság az iskolákban. *PTE BTK NTI Dolgozatok*, 9, 25–39. https://doi.org/10.15170/PTE.BTK.NTI.DOL.2021-09

Bubán M. (2018). Információbiztonság-tudatosság fejlesztése. *EIVOK 2018 – VI. Erdélyi Informatikai Oktatási Konferencia*, 1–6. https://www.hte.hu/documents/10180/4581406/EIVOK_6_BM_Információbiztonsági_tudatosság.pdf

Habók L. (2024). Az információbiztonsági tudatosság mérése-értékelése Bloom-taxonómiával. *Pannon Digitális Pedagógia*, *5*(1), 18–44. https://doi.org/10.56665/PADIPE.2023.3.2

Herédi I. (2022). A kiberbűncselekmények felderítésének nehézségei. *Belügyi Szemle*, *70*(1), 47–65. https://doi.org/10.38146/BSZ.2022.1.3

Legárd I. (2021). Az információbiztonsági tudatosság fejlesztési lehetősége egy gamifikált applikáció segítségével. *Polgári Szemle*, *17*(4), 358–373. https://doi.org/10.24307/psz.2021.0726

Meggyesfalvi B. (2023). Kockázati tényezők a digitális térben. *Belügyi Szemle*, *71*(12), 45–63. https://doi.org/10.38146/BSZ.2023.12.3

A cikkben szereplő online hivatkozások

URL1: *Internethasználat: az első tíz között Magyarország az Európai Unióban.* https://nmhh.hu/cikk/248501/Internethasznalat_az_elso_tiz_kozott_Magyarorszag_az_Europai_Unioban

URL2: *A szálláshelykereső oldalakon is visszaélnek a kiberbűnözők.* https://kiberpajzs.hu/hirek/a-szallashelykereso-oldalakon-is-visszaelnek-a-kiberbunozok-figyelmeztetes

URL3: *Csalástípusok.* https://kiberpajzs.hu/csalastipusok

URL4: *2023 Cybersecurity Almanac: 100 Facts, Figures, Predictions, And Statistics.* https://cybersecurityventures.com/cybersecurity-almanac-2023/

A cikk APA szabály szerinti hivatkozása

Stranszki P., & Nyári N. (2025). Az információbiztonság-tudatosság fejlesztése. *Belügyi Szemle*, *73*(5), 1067–1078. https://doi.org/10.38146/BSZ-AJIA.2025.v73.i5.pp1067-1078

Nyilatkozatok

Összeférhetetlenség

A szerzők nem jelentettek összeférhetetlenséget.

Finanszírozás

A szerzők nem kaptak pénzügyi támogatást a kutatáshoz, a szerzőséghez és/vagy a cikk publikálásához.

Etikai nyilatkozat

Jelen cikkhez nem kapcsolódik adatkészlet.

Nyílt hozzáférésről szóló tájékoztatás

Levelező szerző

A cikk levelező szerzője Nyári Norbert, aki a nnyari@ih.gov.hu e-mail címen érhető el.