https://doi.org/10.36007/5093.2024.300

A DIGITÁLIS VÉDELEM ALAPJAI KÖZÉPISKOLÁSOKNAK
BASICS OF DIGITAL PROTECTION FOR SECONDARY SCHOOL STUDENTS

Bence Pásztor[1]

ABSTRACT
To get basic information about security is becoming increasingly important in the digital world, especially for secondary school students, who, enter a new phase of their lives, and as a result of that must take on greater independence and responsibility. This publication gives an overview about those essential information security concepts that are needed for secondary school students to recognize and prevent the threats they may face in the online environment. The research introduces some basics of information security concepts to students, such as phishing and the misuse of personal data. Information security knowledge will play a crucial role not only during their secondary school years but later in their professional lives as well, as navigating securely in the digital space is indispensable in the modern world.

KEYWORDS
information security, personal data, secondary school, security concepts, phishing

BEVEZETŐ

A középiskolába való belépéssel a diákok élete alaposan megváltozik, hiszen az általános iskolás évekhez képest a tanulóknak nagyobb önállóságot és felelősséget kell vállalniuk, mint korábban. Nem csak a tanulmányaikra kell figyelniük, hanem új feladatokkal is szembe kell nézniük, amelyek az önállóbb életvitelhez kapcsolódnak. Többek között egyre nagyobb szerepet kapnak a tanulmányaikkal kapcsolatos ügyintézésben, online fizetések lebonyolításában, valamint más online tevékenységek kezelésében.

Az interneten való jelenlét, a korlátozott banki ügyintézés és az oktatási platform használata mind olyan területek, ahol az információbiztonsági ismeretek hiánya súlyos kockázatokat jelenthet. Az adathalászat, a kibertámadások és a pénzügyi csalások valós veszélyeket hordoznak. A középiskolás diákoknak is fokozott figyelmet kell fordítaniuk arra, hogyan tudják megvédeni magukat ezekkel a fenyegetésekkel szemben.

SZAKIRODALMI ÁTTEKINTÉS

Digitális oktatási rendszerek

A középiskolák által használt oktatási platform, mint például az EduPage, alapvető

[1] PaedDr. Pásztor Bence, Selye János Egyetem, Gazdaságtudományi és Informatikai Kar, Informatikai Tanszék, pasztor.bence@student.ujs.sk

fontosságú a tanulók számára, hiszen ezen keresztül intézik a tanulmányi ügyeiket, ahol a rendszer tárolja a tanulmányi eredményeiket, a személyes adataikat, iskolai dokumentumaikat és a tantárgyakhoz kapcsolódó információkat. Az EduPage lehetővé teszi a diákok számára az órarendek, a házi feladatok és az osztályzatok megtekintését, valamint a tanárokkal való kommunikációt. Ezen kívül a platform biztosít hozzáférést az iskolai étlaphoz is, így a diákok és a szüleik egyaránt tájékozódhatnak az étkezési lehetőségekről. A szülők hozzáférhetnek gyermekük osztályzataihoz, hiányzásaihoz és egyéb iskolai eseményekhez, így átfogóbb képet kapva a gyermekük iskolai életéről (EduPage, 2024).

A középiskolás diákok gyakran kapnak Microsoft Office fiókot, amely segíti őket az iskolai feladatok hatékonyabb elvégzésében. A kapott fiókon keresztül hozzáférhetnek az Office programokhoz, mint például a Word, Excel és PowerPoint, valamint online tárhelyet is használhatnak a feladatok és dokumentumok tárolására. Fontos, hogy a felhasználók megfelelően kezeljék a fiókjuk biztonságát (Microsoft, 2024).

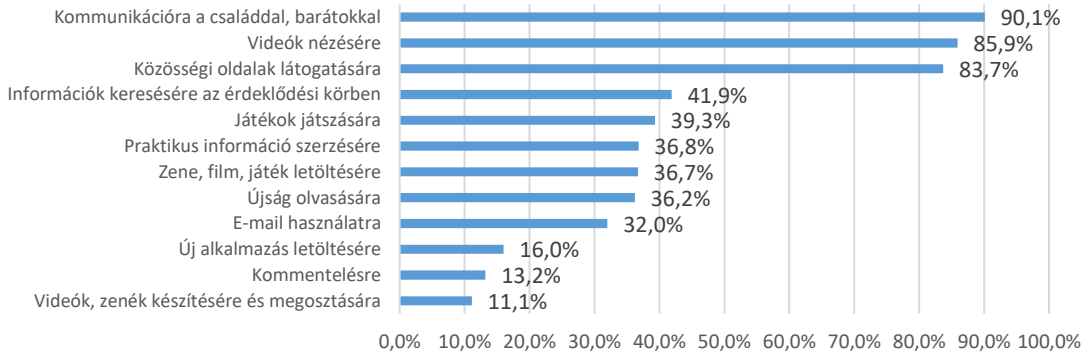
Az ilyen rendszerek biztonságos használata nagyon fontos, mivel a nem megfelelően védett rendszerek könnyen kibertámadások célpontjaivá válhatnak. A megfelelő jelszóhasználat az egyik leglényegesebb biztonsági intézkedés, hiszen a gyenge jelszavak könnyen feltörhetők, amelyek veszélyeztethetik a féltve őrzött adatokat. Ennek érdekében erős jelszavakat kell használni, amelyek biztosítják az adatok nagyobb biztonságát és megakadályozzák az adatokhoz való illetéktelen hozzáférést (Szász & Kiss, 2018).

KUTATÁS MÓDSZERTANA

A Szlovák Köztársaság Oktatási, Tudományos, Kutatási és Sportminisztériuma anyagi támogatásával a "Centrum vedecko-technických informácií SR" 2021 októbere és novembere között egy felmérést végzett, amelyben az általános és középiskolás diákok internethasználati szokásait vizsgálták. A kérdőívet összesen 2565 diák töltötte ki, közülük 1328 általános iskolás és 1237 középiskolás volt. A kutatás eredményeit 2022-ben hozták nyilvánosságra (Janková, 2022).

Az online tevékenységek

A kutatásból azt tudtuk meg, hogy a megkérdezett középiskolás diákoknak mindössze az 1,6%-uk nyilatkozta azt, hogy még nem használta az internetet, a 98,4%-a már használta. A felmérésben továbbá megkérdezték a diákokat, hogy milyen tevékenységeket folytatnak a világhlálón, a válaszokat a következő grafikonon láthatjuk.

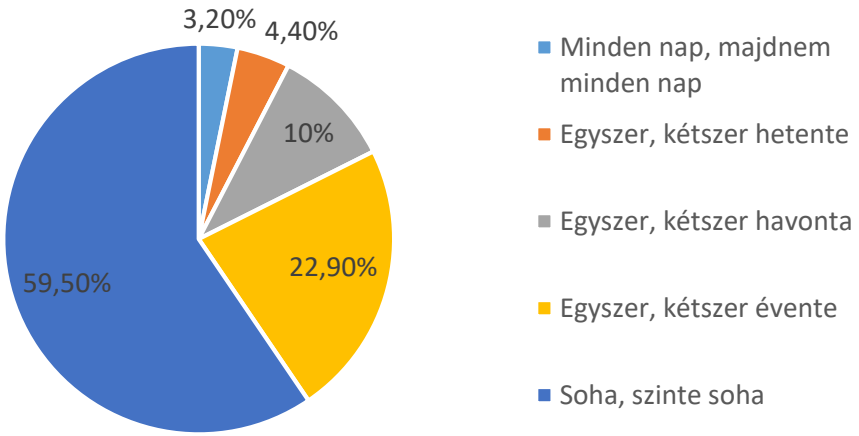


1. ábra: *Az online tevékenységek a középiskolás diákok körében*
Forrás: Saját szerkesztés (Janková, 2022)

A grafikonból kiderül, hogy a legtöbb diák az internetet elsősorban a családdal és barátokkal való kommunikációra használja, amit a videók nézése követ. A harmadik leggyakoribb tevékenység a közösségi oldalak látogatása. A grafikon arra is rávilágít, hogy a tanulók olyan online tevékenységekhez használják az internetet, amelyekhez nélkülözhetetlen a megfelelő információbiztonság ismeret (Janková, 2022).

Online kockázatok

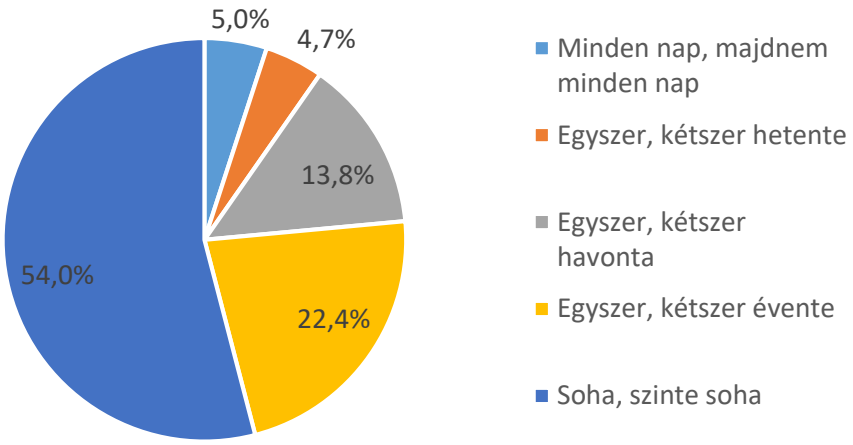
Az online világban a fiatalok számos veszéllyel találkozhatnak. A középiskolás tanulók többsége (85%) tisztában van azzal, hogy az interneten olyan tartalommal vagy viselkedéssel találkozhat, amely idegesítheti vagy felzaklathatja őt. Rendkívül fontos, hogy megfelelő ismereteket szerezzenek az online biztonság terén. Az interneten számos veszély leselkedik a felhasználókra. Ide tartozik például az adathalász támadások, valamint különféle internetes csalások, például hamis webáruházak vagy a pénzt kérő megtévesztő üzenetek és telefonhívások. A következő grafikonon láthatjuk, hogy a középiskolás diákok milyen gyakran találkoznak adathalász e-mailekkel/üzenetekkel.



2. ábra: *Adathalász e-mailek/üzenetek a középiskolás diákok körében*
Forrás: Saját szerkesztés (Janková, 2022)

A grafikon adatai alapján a diákok 3,2%-a nyilatkozta, hogy minden nap vagy majdnem minden nap találkozik adathalász (phishing) e-mailekkel vagy üzenetekkel. További 4,4% hetente 1-2 alkalommal, 10%-uk havonta néhány alkalommal, míg 22,9%-uk évente 1-2 alkalommal szembesül ilyen jellegű fenyegetéssel. Ugyanakkor a diákok többsége, 59,5% soha vagy szinte soha nem találkozott adathalász üzenetekkel.

A következő probléma, amelyet a kutatásban vizsgáltak, az internetes csalás. Ennek eredményei a következő grafikonon látható.



3. ábra: *Internetes csalások a középiskolás diákok körében*
Forrás: Saját szerkesztés (Janková, 2022)

A grafikonon láthassuk, hogy a diákok 5%-a naponta vagy majdnem minden nap találkozik internetes csalással, 4,7% hetente 1-2 alkalommal, 13,8%-uk havonta néhány alkalommal, míg 22,4%-uk évente 1-2 alkalommal tapasztalt ilyen esetet. A diákok 54%-a viszont soha vagy szinte soha nem találkozott internetes csalással (Janková, 2022).

EREDMÉNYEK

Mivel a diákok az internetet számos különböző online tevékenységre használják, ezért kiemelkedően fontos, hogy tisztában legyenek az alapvető információbiztonsági ismeretekkel. Ide tartoznak például a jó jelszó tulajdonságai, a jelszavak biztonságos tárolása és megosztása, a kétfaktoros hitelesítés fontossága, az online fizetés alapvető tudnivalói, a phishing támadások és online csalások felismerése, valamint tudják mi számít személyes adatnak és hogyan kell kezelniük azokat.

A jó jelszó tulajdonságai

A megfelelő jelszó kiválasztása és használata alapvető fontosságú a középiskolás tanulóknak az adataik megőrzése és védelme érdekében. Egy erős jelszó nehezebbé teszi az illetéktelen hozzáférést a különböző fiókokhoz, illetve hatékonyabban véd a kibertámadásokkal szemben. Az alábbiakban összefoglaljuk, hogy milyen szabályokat kell figyelembe venni egy megfelelő jelszó megalkotása során:

- **Hosszúság**: Egy biztonságos jelszó legalább 12 karakter hosszú legyen. Minél hosszabb egy jelszó, annál nehezebb feltörni, mivel a lehetséges kombinációk száma jelentősen nő.
- **Komplexitás**: A jelszónak tartalmaznia kell nagy- és kisbetűket, számokat, valamint speciális karaktereket (például @, #, $, %). Ez növeli a variációk számát, és megnehezíti a jelszó feltörését különféle módszerekkel, például brute-force támadásokkal.
- **Ne legyen könnyen kitalálható**: Kerüljék a személyes információk használatát, mint például a név, születési dátum, vagy a közismert, gyakran használt jelszavak (például 12345678 vagy jelszó). Az ilyen egyszerű jelszavak könnyen feltörhetők vagy kitalálhatók, különösen a célzott támadások esetén.
- **Ne használjuk ugyanazt a jelszót több helyen**: Fontos, hogy minden rendszerhez különböző jelszót használjanak. Ha egy jelszót több helyen is használnak és egyetlen rendszert is feltörnek, az a többi fiók biztonságát is veszélyezteti.
- **Rendszeres jelszóváltoztatás**: Ajánlott bizonyos időközönként, például 3-6 havonta, jelszót változtatni (Microsoft).

Az adatok védelme érdekében fontos betartani ezeket a szabályokat. Sok rendszer pedig csak akkor engedélyezi a jelszó létrehozását, ha a szabályokat megfelelően követtük.

A jelszavak tárolása és megosztása

Az erős jelszavak létrehozása csak az első lépés a középiskolás tanulóknak az adataik védelmében, továbbá nagyon fontos az is, hogy a jelszavaikat biztonságosan tárolják. Nem szabad azt a hibát elkövetniük, hogy ezeket a féltve őrzött adatokat jegyzetekben vagy szöveges dokumentumokban tárolják, mivel ez számos kockázattal jár. Ha ezekhez a fájlokhoz vagy jegyzetekhez illetéktelenek hozzáférnek, a jelszavak könnyen kiszivároghatnak, és ezáltal az adatok veszélybe kerülnek.

A biztonságos jelszótárolás legjobb módja egy **jelszókezelő program** használata. Ezek a programok titkosítják a jelszavakat, így azok biztonságosan tárolhatók egyetlen mesterjelszó alatt. A felhasználónak csak egy jelszót kell megjegyeznie, amíg a többi jelszót a jelszókezelő védi és kezeli. Emellett a jelszókezelők általában képesek erős, bonyolult jelszavak generálására is, így a felhasználónak nem kell aggódnia a jelszó komplexitásának megtervezése miatt (Hatzivasilis, 2020).

A jelszavak megosztása is komoly kockázatokat rejt. Soha nem szabad megosztani a jelszavakat másokkal, még akkor sem, ha a kérdező megbízhatónak tűnik. Gyakran előfordulnak **phishing támadások**, amelyek során a támadó megbízhatónak látszó e-mailekkel, üzenetekkel próbálja megszerezni a jelszavakat. Az ilyen támadások célja, hogy a felhasználókat megtévesszék, és

arra késztessék őket, hogy önként adják át a jelszavaikat vagy egyéb érzékeny adataikat. Éppen ezért fontos a tudatosság és az óvatosság minden esetben (KnowBe4, 2021).

A kétfaktoros hitelesítés (2FA)

A középiskolás diákoknak érdemes használniuk a kétfaktoros hitelesítést, hogy biztonságosabban tárolhassák az adataikat. A kétfaktoros hitelesítés egy olyan biztonsági módszer, amely két különböző hitelesítési tényezőt használ a fiókokhoz vagy rendszerekhez való hozzáférés biztosítására. Ez egy extra védelmi réteget jelent, amely jóval nagyobb biztonságot nyújt, mint a pusztán jelszavas védelem. A 2FA bevezetése különösen fontos lehet olyan rendszereknél, ahol érzékeny adatokat kezelnek, például az EduPage rendszerben, online banki fiókoknál vagy e-mail fiókok esetében.

A kétfaktoros hitelesítés során a felhasználónak nem elég csak a jelszót megadnia, a rendszer egy második hitelesítési tényezőt is kér. Ez lehet például egy **SMS-ben küldött kód**, egy **mobilalkalmazás által generált időalapú kód** vagy hangalapú hitelesítés. A lényeg, hogy a hozzáféréshez két különböző, egymástól független azonosítóra van szükség.

A 2FA sokkal biztonságosabbá teszi a hozzáférést, mivel ha valaki megszerzi a felhasználó jelszavát – például egy adathalász támadás során, még mindig szüksége lesz a második hitelesítési tényezőre, hogy beléphessen a fiókba. Például, ha a felhasználó SMS-ben kap egy kódot, a támadónak hozzáférést kellene szereznie a felhasználó telefonjához is, hogy be tudjon lépni.

Ezen kívül a 2FA **megnehezíti az automatizált támadásokat**, például a brute-force támadásokat, amelyek során a támadók véletlenszerűen próbálnak ki jelszavakat, hogy hozzáférést nyerjenek a fiókokhoz. A második faktor miatt egy sikeres jelszó kitalálása önmagában nem elegendő, így a támadások kevésbé hatékonyak (Microsoft, 2024, b).

Az online fizetés alapvető tudnivalói

A diákok gyakran fizetnek online különféle webshopokban. Az online vásárlások során azonban kiemelten fontos ügyelni az adataik biztonságára. Néhány tipp, hogyan tehetik ezt meg:

- **Biztonságos webhelyek használata**: a tanulóknak mindig ellenőrizniük kell, hogy az általuk használt webhely TLS tanúsítvánnyal rendelkezik (a webcím „https://”-sel kezdődik). Ez biztosítja, hogy a kapcsolat titkosított, és a személyes adatok, beleértve a bankkártya-adatokat, védettek (CIB Bank Zrt., 2024).

- **Ne használjanak nyilvános Wi-Fi hálózatokat**: a nyilvános Wi-Fi hálózatokon végzett tranzakciók kockázatosak lehetnek, mivel a támadók könnyen hozzáférhetnek az átvitt adatokhoz. Amennyiben mégis szükséges nyilvános hálózatot használni, javasolt egy VPN (Virtual Private Network) szolgáltatás alkalmazása, amely titkosítja az adatforgalmat (Mastercard, 2024).

- **Bankkártya adatainak védelme**: inkább ne mentsük el bankkártya adatainkat online felületeken, hacsak nem vagyunk biztosak benne, hogy a weboldal teljes mértékben megbízható és biztonságos (Csaladinet, 2022). Ezenkívül ajánlott a banki tranzakciók értesítéseit aktiválni, hogy azonnal értesüljünk minden szokatlan vagy gyanús tevékenységről (K&H, 2018).

Phishing és online csalások

A diákok gyakran célpontjai a phishing támadásoknak és az online csalásoknak. Ezek során a támadók általában e-mailek, SMS-ek vagy közösségi média üzenetek útján próbálják megszerezni a tanulók személyes adatait. Ha egy üzenet ismeretlen vagy megbízhatatlan forrásból származik, és személyes adatokat kérnek benne (pl. jelszavak, bankkártya adatok), azt azonnal gyanúval kell kezelni. A tanulóknak tisztában kell lenniük azzal, hogy a hivatalos intézmények soha nem kérnek érzékeny adatokat e-mailben vagy üzenetben.

Az adathalász e-mailek felismerhetők, mert gyakran sürgető és fenyegető hangvételűek. Például olyan üzeneteket kaphatnak, amelyek azt állítják, hogy „zárolják a fiókot", ha nem adják meg az adataikat azonnal. Ha ilyen e-mailt kapnak, azonnal töröljék, és soha ne válaszoljanak rá (IBM, 2024).

Személyes adatok kezelése

A középiskolás diákok életében a közösségi média gyakran fontos szerepet játszik, azonban rendkívül fontos odafigyelni arra, hogy milyen információkat osztanak meg ezeken a felületeken (EU Kids Online, 2020). A személyes adataik védelme nagyon fontos, mivel ezek az információk könnyen visszaélésekre adhatnak lehetőséget. Például, ha nyilvánosan megosztják a lakcímüket, a telefonszámukat vagy az e-mail címüket, akkor ezek az adatok könnyen rossz kezekbe kerülhetnek. Az ilyen adatokkal való visszaélés különféle problémákat okozhat, ezért érdemes ezeket az információkat csak szükség esetén és biztonságos módon megosztani (European Commission, 2024).

ÖSSZEFOGLALÁS

Az információbiztonság napjainkban különösen fontos, mivel a mindennapi tevékenységeink egyre inkább összefonódik a digitális világgal. A középiskolás diákok gyakran böngésznek a világhálón, különböző közösségi oldalakon kommunikálnak egymással és általában bankkártyával is rendelkeznek. Nagyon fontos, hogy a diákok megértsék, hogyan tudnak erős jelszót választani, miért hasznos egy jelszókezelő program, és mi az a kétfaktoros hitelesítés, amely extra védelmet nyújt a fiókjaikhoz. Emellett fontos, hogy felismerjék a csalókat, például a phishing támadásokat, amikor valaki hamis üzenetekkel próbálja megszerezni a személyes adataikat vagy jelszavaikat. Ezek az alapvető ismeretek segítenek nekik biztonságban maradni az online világban. A felsorolt ismeretek nemcsak a tanulmányaik során, hanem később a munka világában is kiemelkedően fontos lesz számukra, hiszen a digitális térben való biztonságos eligazodás elengedhetetlen a mai világban.

FELHASZNÁLT IRODALOM

Folyóiratcikk

Hatzivasilis, G. (2020). Password Management: How Secure Is Your Login Process? In Model-driven Simulation and Training Environments for Cybersecurity (s. 157-175).

Szász Antónia, Kiss Gábor, „Jelszóvisszafejtő programok oktatási célú felhasználása és hatásuk az információbiztonsági tudatosságra", Információs Társadalom XVIII, 3–4. szám (2018): 82–104. https://dx.doi.org/10.22503/inftars.XVIII.2018.3-4.4

Jelentés

Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S.,and Hasebrink, U. (2020). EU Kids Online 2020: Survey results from 19 countries. EU Kids Online. https://doi.org/10.21953/lse.47fdeqj01ofo

Janková, M. (2022). Vybrané výsledky z výskumu zameraného na používanie internetu, online aktivity a potencionálne riziká z pohľadu žiakov základných a stredných škôl. Bratislava: Centrum vedecko-technických informácií SR.

Weboldal

CIB Bank Zrt. (2024). Elérhető az interneten: A BIZTONSÁGOS KÁRTYÁS FIZETÉSRŐL: https://www.cib.hu/Maganszemelyek/biztonsagi_tanacsok/internetes_kartyas_fizetes.html

Csaladinet. (2022). Elérhető az interneten: El merjük menteni banki adatainkat a böngészőben?: https://www.csaladinet.hu/hirek/tb_ellatasok-penzugyek/csaladi_penzugyek/31622/el_merjuk_menteni_banki_adatainkat_a_bongeszoben

EduPage. (2024). Elérhető az interneten: https://present.edupage.org/

European Commission. (2024). Elérhető az interneten: What is personal data?: https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en

IBM. (2024. 5. 17.). Elérhető az interneten: What is phishing?: https://www.ibm.com/topics/phishing

KnowBe4, „Phishing," [Online]. Elérhető az interneten: https://www.phishing.org/what-is-phishing. [Hozzáférés dátuma: 2024. 8. 30.]

K&H. (2018). Elérhető az interneten: mindent tudni akarsz, ami a bankszámládon történik?: https://www.kh.hu/cikkek/bankszamla-mobilinfo

Mastercard. (2024). Elérhető az interneten: Tippek a biztonságos online vásárláshoz: https://www.mastercard.hu/hu-hu/te-es-a-mastercard/fizetesi-modok/netes-vasarlas/biztonsagos-online-vasarlas.html

Microsoft. Elérhető az interneten: Create and use strong passwords: https://support.microsoft.com/en-us/windows/create-and-use-strong-passwords-

c5cebb49-8c53-4f5e-2bc4-fe357ca048eb

Microsoft. (2024). Elérhető az interneten: Office 365 Education: https://www.microsoft.com/en-us/education/products/office

Microsoft. (2024, b). Elérhető az interneten: What is two-factor authentication?: https://www.microsoft.com/en-ie/security/business/security-101/what-is-two-factor-authentication-2fa