



5. MODUL

KIBERVÉDELEM ÉS ONLINE BIZTONSÁG



erasmediah.eu



**Co-funded by
the European Union**



5.6 Tananyag

Gyakorlati eszközök az online biztonsághoz



ERASMEDIAH

Educational Reinforcement Against
the Social Media Hyperconnectivity



**Co-funded by
the European Union**

5.6. lecke

Gyakorlati eszközök az online biztonsághoz

Célok:

- **A résztvevők felvértezése** gyakorlati eszközökkel és technikákkal a gyakori online fenyegetések, többek között az adathalászat, a rosszindulatú programok és a csalások azonosítására és enyhítésére.
- A kiberbiztonsági erőforrások, például jelszókezelők, VPN-ek és biztonságos böngészők használatában való **jártasság fejlesztése**, miközben elősegíti az online adatvédelem kezelésének megértését.
- **A biztonságos és felelős online gyakorlatok előmozdítása** a digitális platformok kritikus értékelésén, a kiberfenyegetések figyelmeztető jeleinek felismerésén és olyan védőszokások elsajátításán keresztül, mint a gyanús tevékenységek jelentése.

Fő üzenet(ek):

- A tudatosság és a felkészültség az elsődleges védelmi vonal. Az online fenyegetések megértése és a megfelelő eszközök birtoklása lehetővé teszi, hogy biztonságosan eligazodjon a digitális világban.
- A biztonságod a kezvedben van. A VPN-ekhez, biztonságos böngészőkhöz és adatvédelmi beállításokhoz hasonló praktikus eszközök segítségével megvédheted személyes adataidat és kézben tarthatod online jelenlétedet.



ÓRA TÍPUSA:





Áttekintés

Az online biztonság nagymértékben függ a személyes adatok védelmére és a digitális fenyegetések megelőzésére tervezett eszközök hatékony használatának képességétől. Ez a lecke a kulcsfontosságú kiberbiztonsági eszközök, például a jelszókezelők, a VPN-ek és az adatvédelmi beállítások praktikus, gyakorlati alkalmazását hangsúlyozza. A résztvevők aktívan felfedezik, hogyan működnek ezek az eszközök, tesztelik funkcióikat, és stratégiákat tanulnak meg a napi digitális rutinokba való beépítésükhöz. Irányított tevékenységek révén magabiztosságot építenek ki ezen eszközök online jelenlétük védelmére és a kockázatokra való gyakorlati megoldásokkal való reagálás terén.

A workshop 4 lépésre tagolódik:

- 1:** Bevezetés az online biztonsági eszközök használatába (10 perc)
- 2:** Gyakorlati eszközismeret (15 perc)
- 3:** Forgatókönyv-alapú kockázatkezelés (10 perc)
- 4:** Záró gondolatok (5 perc)



1. lépés

Bevezetés az online biztonsági eszközök használatába

Találkoztál már valaha gyanús dologgal az interneten? Talán egy furcsa e-maillal, amely a jelszavad visszaállítását kéri, egy ingyenes nyereményt kínáló felugró ablakkal, vagy egy weboldallal, amely túl sok személyes adatot kér? Ezek a helyzetek kockázatosnak tűnhetnek – és gyakran azok is.

A jó hír az, hogy vannak **praktikus eszközök**, amelyekkel megvédeheted magad az ilyen pillanatokban. A workshop végére tudni fogod, hogyan ismerd fel ezeket a kockázatokat, és hogyan használd az olyan eszközöket, mint a jelszókezelők, a VPN-ek és az adatvédelmi beállítások, hogy biztonságban maradj online. Merüljünk el a részletekben, és nézzük meg, hogyan segíthetnek ezek az eszközök!



1. lépés

Bevezetés az online biztonsági eszközök használatába

Íme három egyszerű eszköz, amelyekkel sokkal biztonságosabbá teheted az online életedet:

- **Jelszókezelők:** Ezek segítenek erős, egyedi jelszavak létrehozásában és tárolásában, így nem kell mindegyiket megjegyezni.
- **VPN-ek (virtuális magánhálózatok):** Ezek védik az online tevékenységeidet, különösen a nyilvános Wi-Fi-hálózatokon, azáltal, hogy biztonságossá teszik a kapcsolatodat.
- **Böngésző adatvédelmi beállításai:** Ezekkel szabályozhatod, hogy milyen információkat gyűjthetnek rólad a webhelyek, például a tartózkodási helyedet vagy a böngészési szokásaidat.

Ma ezekre az eszközökre fogunk összpontosítani, mert hatalmas különbséget jelenthetnek az online biztonság megőrzésében.

Gondolj vissza arra, amikor utoljára valami olyasmivel találkoztál az interneten, ami nem tűnt elfogadhatónak – például egy megbízhatatlan weboldallal. Hogyan kezelted? Figyelman kívül hagytad, tovább vizsgáltad az ügyet, vagy talán rákattintottál?

Közös, bevezető beszélgetés:

- Milyen online fenyegetéseket vagy kockázatokat észleltél korábban?
- Milyen eszközöket vagy stratégiákat használsz már az online biztonságod megőrzése érdekében?
- Szánjunk néhány percet arra, hogy csoportként megosszuk az ötleteinket. Ne aggódj, ha ezt még nem tapasztaltad meg első kézből – a társaid történetei új gondolatokat ébreszthetnek.



2. lépés

Gyakorlati eszközök felfedezése

Most itt az ideje, hogy belevágjunk és felfedezzük, hogyan tehetik egyszerű eszközök biztonságosabbá online jelenlétedet. Ebben a feladatban kipróbálhatod a böngésző adatvédelmi beállításait, és tesztelheted jelszólétrehozási képességeidet a Jelszómérő segítségével. Kezdjük is!

1. rész: Böngésző adatvédelmi beállításai

A böngésződ szabályozhatja, hogy a weboldalak mennyi információt gyűjtsenek rólad. Ellenőrizzük és módosítsuk az adatvédelmi beállításaidat:

- Nyisd meg böngésződ adatvédelmi beállításait (keresd meg a „Beállítások” menüpontot, majd lépj az „Adatvédelem” vagy a „Biztonság” menüpontra).
- Tekintsd át ezeket a kulcsfontosságú területeket:
 - **Nyomon követés:** Be van kapcsolva?
 - **Sütik:** Le vannak tiltva a harmadik féltől származó sütik?
 - **Engedélyek:** Mely webhelyek férhetnek hozzá a tartózkodási helyedhez, kamerádhoz vagy mikrofonodhoz?



2. lépés

Gyakorlati eszközök felfedezése

3. Végezd el a szükséges módosításokat: Kapcsod be azokat az adatvédelmi beállításokat, amelyekről úgy gondolod, hogy segítenek megvédeni az adataidat.

Például:

- Blokkold a nyomon követő sütiket.
- Tiltsd le a helymegosztást azoknál a webhelyeknél, amelyekben nem bízik meg.

Gyors visszatekintés: Mi lepett meg a jelenlegi beállításaidal kapcsolatban? Változtattál valamin?

2. rész: Jelszó erősségének tesztelése a Jelszómérővel

Egy erős jelszó létrehozása az egyik legegyszerűbb módja a fiókok védelmének. Most nézzük meg, mennyire biztonságosak a jelszavaid:

1. Nyisd meg a jelszóerősség-mérőt.
2. Gondolj egy új jelszóra (ne használj olyat, ami már megvan!).



2. lépés

Gyakorlati eszközök felfedezése

3. Írd be a jelszót a PasswordMeter-be, és nézd meg a visszajelzést:

- Mennyire erős a jelszavad?
- Milyen javaslatokat ad arra, hogy erősebbé tegye?

4. Kísérletezz a jelszavad megváltoztatásával a visszajelzések alapján (pl. adj hozzá szimbólumokat, tedd hosszabbá, vagy keverd a kis- és nagybetűket). Figyeld, hogyan javul az eredmény!

Gyors visszatekintés: Mennyire volt könnyű vagy nehéz erős jelszót létrehozni? Mi az az egy dolog, amit a jövőben másképp fogsz csinálni a jelszavak beállításakor?

A tevékenység végére javítani fogod a böngésződ adatvédelmi beállításait, és megtanultad, hogyan kell erősebb jelszavakat létrehozni!



3. lépés

Forgatókönyv-alapú kockázatkezelés

Miután áttekintettünk néhány gyakorlati eszközt, nézzük meg, hogyan alkalmazhatók ezek valós helyzetekben. Kis csoportokban fogtok dolgozni a forgatókönyvek elemzésén, a kockázatok azonosításán, és azon, hogyan kezeljétek azokat a tárgyalt eszközök segítségével.

Olvasd el a csoportodnak adott forgatókönyvet. Íme néhány példa:

- 1. Kapsz egy e-mailt, amiben értesítenek, hogy nyertél egy díjat, de a link gyanúsnak tűnik. Mit tehetsz?*
- 2. Egy közösségi média alkalmazás telepítéskor hozzáférést kér a tartózkodási helyedhez, a kamerádhoz és a mikrofonodhoz. Engedélyezned kellene?*
- 3. Nyilvános Wi-Fi-t használsz egy kávézóban, és egy ismeretlen weboldalra kérnek bejelentkezni. Hogyan maradhatsz biztonságban?*

Beszéljétek meg a csoportoddal a forgatókönyv kockázatait. Kérdezzétek meg magatoktól:

- Mi baj történhet, ha nem cselekszel körültekintően?
- Miért érződik ez a helyzet veszélyesnek?

Döntsétek el, hogyan tudnál gyakorlati eszközöket használni a kockázat kezelésére. Például:

- A böngésző adatvédelmi beállításával blokkolhatod a felesleges engedélyeket.
- Kerüld a gyanús linkekre kattintást, és ellenőrizze az e-maileket adathalászati jelek után.
- Kapcsolj be egy VPN-t a nyilvános Wi-Fi-kapcsolatod biztonságosabbá tételéhez.



3. lépés

Forgatókönyv-alapú kockázatkezelés

Néhány perc elteltével minden csoport megosztja a következőket:

- *Milyen kockázatokat észlelt a forgatókönyvben*
- *Milyen eszközöket vagy lépéseket használt a biztonsága érdekében*

Gondold át: Hogyan segíthetnek ezek az eszközök a saját online tevékenységeidben?

Az olyan praktikus eszközök, mint a böngésző adatvédelmi beállításai, a VPN-ek és az adathalászat-észlelés, a kockázatos helyzeteket kezelhetővé tehetik. Rendszeres használatuk sokkal könnyebbé teszi az online biztonság megőrzését!

Gondoljuk át, mit tanultunk, és hogyan tudjuk ezeket felhasználni az online biztonságunk megőrzése érdekében.

1. lépés: Gondolkodj el

Gondolkozz el ezeken a kérdéseken:

- Melyik eszköz (pl. böngésző adatvédelmi beállításai, VPN-ek, jelszókezelők) volt a leghasznosabb számodra? Miért?
- Hogyan változott az online biztonságról alkotott véleményed ezen eszközök használata után?

2. lépés: Tervezd meg a következő lépést

- Írj le egy lépést, amit meg fogsz tenni az online biztonságod javítása érdekében.
- Mit fogsz tenni? (Például: „Jelszókezelővel fogok erős jelszavakat létrehozni.”)
- Mikor fogod megtenni? (pl.: „A hét végére.”).

A gyakorlati eszközök jelentik az első lépést – maradj következetes, hogy online biztonságod erős maradjon!





Összefoglalás

- A böngésző adatvédelmi beállításai, a jelszókezelők és a VPN-ek egyszerű, de hatékony eszközök az online biztonság fokozásához.
- Aktívan kezeld, hogy milyen információkat osztasz meg online az adatvédelmi beállítások módosításával és a szükségtelen engedélyek korlátozásával.
- Rendszeresen frissítsd az adatvédelmi beállításait, hozzon létre biztonságos jelszavakat, és tekintsd át az alkalmazások engedélyeit, hogy az online biztonság a digitális életének rutin részévé váljon.
- Maradj proaktív – az eszközök kritikai gondolkodással és tájékozottsággal való kombinálásával felkészülhetsz a folyamatosan változó online fenyegetésekre.
- Próbáld meg más praktikus online eszközöket is kipróbálni, hogy megértsd és javítsd digitális biztonságodat – minél több eszközt tudsz használni, annál jobban növelheted a biztonságodat!



Útmutató tanárok és trénerek számára

Célkitűzés:

Ez a lecke arra összpontosít, hogy a résztvevők elsajátítsák az alapvető online biztonsági eszközök használatához szükséges gyakorlati készségeket. Egyéni és csoportos gyakorlatok és beszélgetések révén képessé válnak a gyakori online fenyegetések azonosítására és kezelésére, digitális védelmük megerősítésére olyan erőforrásokkal, mint a jelszókezelők, VPN-ek és adatvédelmi beállítások, valamint a biztonságosabb szokások beépítésére a mindennapi online tevékenységeikbe.

Szükséges anyagok:

- Internet-hozzáférés tesztelési eszközökhöz (pl. VPN-ek, jelszókezelők)
- Laptopok, tabletek vagy okostelefonok gyakorlati feladatokhoz
- Fehér tábla vagy flipchart ötleteléshez és összefoglaló megbeszélésekhez
- Üres papírlapok jegyzeteléshez
- Tollak, ceruzák vagy színes filctollak





1. lépés: Bevezetés az online biztonsági eszközökbe (10 perc)

1. Kezdeként tegyen fel egy ismerős kérdést a résztvevőknek: „Találkoztál már valaha gyanús dologgal az interneten, például egy furcsa e-maillal, egy nyereményt kínáló felugró ablakkal vagy egy túl sok személyes adatot kérő weboldallal?” Röviden magyarázza el, hogy ezek a helyzetek kockázatosnak tűnhetnek, és gyakran azok is, de vannak gyakorlati eszközök a kezelésükre.
2. Mutassa be a foglalkozás fókuszát három alapvető eszközre: jelszókezelőkre, VPN-ekre és böngésző adatvédelmi beállításokra. Emelje ki fontosságukat azzal, hogy elmagyarázza, hogy a jelszókezelők segítenek erős, egyedi jelszavak létrehozásában és tárolásában, a VPN-ek biztonságos online tevékenységeket biztosítanak nyilvános Wi-Fi-n, és a böngésző adatvédelmi beállításai szabályozzák, hogy a webhelyek milyen információkat gyűjthetnek, például a tartózkodási helyet vagy a böngészési szokásokat.
3. Ösztönözze a résztvevőket, hogy reflektáljanak saját online kockázatokkal kapcsolatos tapasztalataikra a következő kérdéssel: „Gondoljon vissza, mikor találkozott utoljára valami gyanús dologgal az interneten. Hogyan kezelte?”
4. Vezessen be egy rövid beszélgetést olyan kérdésekkel, mint például: „Milyen online fenyegetéseket észleltetek?” és „Milyen eszközöket vagy stratégiákat használtál már a biztonságod megőrzése érdekében?” Kérje meg a résztvevőket, hogy osszák meg történeteiket vagy ötleteiket, hangsúlyozva, hogy az egymástól való tanulás új felismeréseket szülhet.
5. Befejezésül hangsúlyozza ezen eszközök fontosságát az online kockázatok kezelésében, a következő kijelentéssel: „Jelszókezelők, VPN-ek és adatvédelmi beállítások használatával magabiztosan navigálhatsz a digitális világban, miközben véded személyes adataidat.” Tartsd a beszélgetést interaktívnak és támogatónak, biztosítva, hogy a résztvevők bátorítva érezzék magukat gondolataik megosztására és a csoporttól való tanulásra.





2. lépés: Gyakorlati eszközök felfedezése (15 perc)

1. Kezdje a tevékenység céljának ismertetésével: olyan gyakorlati eszközök felfedezése, amelyek a böngésző adatvédelmi beállításain és a jelszóerősség-teszteléseken keresztül fokozzák az online biztonságot.

2. Ossa fel a tevékenységet két részre a strukturált megközelítés biztosítása érdekében.

1. rész: Böngésző adatvédelmi beállításai (8 perc)

1. Vezesse a résztvevőket a böngészőjük adatvédelmi beállításainak megnyitásához (navigálj a „Beállítások” vagy a „Beállítások” menüpontra, majd keresd meg az „Adatvédelem” vagy a „Biztonság” lehetőséget). Kérje meg őket, hogy tekintsék át a legfontosabb területeket:

- **Nyomon követés megelőzése:** Győződjön meg arról, hogy engedélyezve van.
- **Sütik:** Ellenőrizze, hogy nincsenek-e letiltva harmadik féltől származó sütik.
- **Engedélyek:** Tekintse át, hogy mely webhelyek férhetnek hozzá a tartózkodási helyükhöz, kamerájukhoz vagy mikrofonjukhoz.

2. Ösztönözze a résztvevőket, hogy végezzenek módosításokat, például blokkolják a követő sütiket vagy tiltsák le a szükségtelen helymegosztást.

3. Utána egy gyors reflexióra ösztönözzön: „Mi lepett meg a jelenlegi beállításaidkal kapcsolatban? Végrehajtottál-e változtatásokat?” Ez segít a résztvevőknek összekapcsolni felfedezéseiket ezen eszközök értékével.

2. rész: Jelszóerősség-tesztelés (5 perc)

1. Irányítsa a résztvevőket a PasswordMeter oldalára. Kérje meg őket, hogy hozzanak létre egy új jelszót (ne olyat, amit jelenleg használnak), és teszteljék az erősségét.

2. Bátorítsa őket, hogy elemezzék a visszajelzéseket, és kísérletezzenek változtatásokkal, például szimbólumok hozzáadásával, kis- és nagybetűk keverésével vagy a szöveg hosszának növelésével, hogy lássák, hogyan javul az eredmény.

3. Zárásként gondoljal át: „Mennyire volt könnyű vagy nehéz erős jelszót létrehozni? Mi az az egy dolog, amit a jövőben másképp fogsz csinálni a jelszavak beállításakor?”

4. A tevékenységet a gyakorlati értékének megerősítésével zárjuk.

5. Tartsa a foglalkozást gyakorlatias és izgalmas módon, és szükség szerint nyújtson útmutatást, miközben a résztvevők felfedezik és alkalmazzák ezeket az eszközöket.



3. lépés: Forgatókönyv-alapú kockázatkezelés (10 perc)

1. Ez a tevékenység segít a résztvevőknek az online biztonsági eszközök valós élethelyzetekben történő alkalmazásában. Oszd a résztvevőket kis csoportokra, és jelölj ki mindegyik csoportnak egy forgatókönyvet, például:

- Egy gyanús e-mail nyereseményre utaló linkkel.
- Egy közösségi média alkalmazás túlzott engedélyeket kér.
- Nyilvános Wi-Fi használata esetén ismeretlen bejelentkezési ablak jelenik meg.

2. Kérje meg a csoportokat a kockázatok megvitatására, figyelembe véve a következőket:

- „Mi baj történhet, ha nem cselekszel körültekintően?”
- „Miért érződik ez a helyzet veszélyesnek?”

3. Kérd meg őket, hogy határozzák meg, hogyan kezelhetik a kockázatot olyan eszközökkel, mint a böngésző adatvédelmi beállításai, az adathalász linkek elkerülése vagy a VPN engedélyezése.

4. Ezt követően minden csoport megosztja egymással az általuk azonosított kockázatokat és az azok kezelésére használt eszközöket.

5. Befejezésül emelje ki a következőket: „Az olyan eszközök, mint az adatvédelmi beállítások, a VPN-ek és az adathalászat-észlelés, megkönnyítik az online kockázatok kezelését. Ezen eszközök rendszeres használata erősíti az online biztonságot.” Tartsa a foglalkozást fókuszban, és ösztönözze a gyakorlatias, cselekvésre ösztönző meglátásokat.





4. lépés: Záró reflexiók (5 perc)

1. A foglalkozás zárásaként vezesse végig a résztvevőket egy reflexív gyakorlaton, amely segít megszilárdítani a tanultakat. Kezdje azzal, hogy megkéri őket, hogy gondolják át a következőket:

- „Melyik eszköz (pl. böngésző adatvédelmi beállításai, VPN-ek, jelszókezelők) volt a leghasznosabb az Ön számára? Miért?”
- „Hogyan változott az online biztonságról alkotott véleményed ezeknek az eszközöknek a használata után?”

2. Bátorítsa a résztvevőket, hogy röviden osszák meg gondolataikat, ezzel is támogató környezetet teremtve a beszélgetéshez.

3. Ezután kérje meg őket, hogy tervezzenek meg egy konkrét intézkedést online biztonságuk fokozása érdekében, például:

- „Mit fogsz tenni?” (pl. „Jelszókezelővel fogok erős jelszavakat létrehozni.”)
- „Mikor fogod megcsinálni?” (pl. „A hét végére.”)

4. Zárásként hangsúlyozd a következetesség fontosságát, és emlékeztess a résztvevőket: „A gyakorlati eszközök jelentik az első lépést – maradj következetes, hogy online biztonságod erős maradjon!” A hangnem legyen motiváló, és összefoglalja arra, hogy a tanulságokat a mindennapi online gyakorlatban alkalmazd.

Főbb tanulságok:

A lecke elvégzése után a résztvevők világos képet kapnak arról, hogyan használhatják az olyan alapvető eszközöket, mint a jelszókezelők, a VPN-ek és a böngésző adatvédelmi beállításai az online biztonságuk fokozása érdekében. Megtanulják azonosítani a gyakori fenyegetéseket, például az adatkövetést, és proaktív lépéseket tenni személyes adataik védelme érdekében. Azáltal, hogy ezeket az eszközöket és stratégiákat beépítik a napi rutinjukba, magabiztosan tudnak majd eligazodni a digitális világban, minimalizálva a potenciális fenyegetéseket. Ahhoz, hogy ezeket a tanulságokat hatékonyan kommunikáljuk, könnyen értelmezhető forgatókönyveket és világos példákat kell használnunk, hogy bemutassuk ezen eszközök valós hatását a mindennapi online biztonságra.



Utánkövetés és otthoni tevékenységek:

Ösztönözze a résztvevőket, hogy alaposabban vizsgálják meg jelenlegi online gyakorlataikat a böngésző adatvédelmi beállításainak áttekintésével és módosításával, jelszavaik erősségének tesztelésével olyan eszközökkel, mint a PasswordMeter, és a VPN funkciók felfedezésével. Kérje meg őket, hogy értékeljék a gyakran használt alkalmazások engedélyeit, figyeljék meg a lehetséges kockázatokat, és alkalmazzanak biztonságosabb alternatívákat. Végül kérje meg a résztvevőket, hogy osszanak meg egy újonnan tanult biztonsági tippet egy barátjukkal vagy családtagjukkal, megerősítve ezzel tudásukat és terjesztve a digitális biztonsággal kapcsolatos tudatosságot.

Tippek tanároknak:

Gyakorlati, valós példákkal és más interaktív feladatokkal mutathatod be, hogyan használhatók hatékonyan az olyan eszközök, mint a jelszókezelők, a VPN-ek és az adatvédelmi beállítások az online biztonság fokozására. Mutasd meg a résztvevőknek lépésről lépésre, hogyan navigálhatnak és konfigurálhatják ezeket az eszközöket, hogy a foglalkozás gyakorlatias és gyakorlatias legyen. Teremts nyílt és támogató környezetet, ahol a résztvevők kényelmesen érzik magukat, megbeszélhetik az online fenyegetésekkel kapcsolatos tapasztalataikat és kérdéseket tehetnek fel. Hangsúlyozd ki ezen eszközök rendszeres használatának és a mindennapi online rutinokba való integrálásának fontosságát a következetes és proaktív digitális védelem biztosítása érdekében.





Eszközök

Get Safe Online



Egy átfogó weboldal, amely ingyenes és egyszerű tanácsokat kínál az online biztonsággal kapcsolatos témák széles skáláján. Gyakorlati útmutatókat tartalmaz a személyes adatok védelméről, a csalások elkerüléséről és a biztonságos online kommunikációról. A tartalom felhasználóbarát és minimális technikai ismeretekkel rendelkezők számára készült.

www.getsafeonline.org

The Password Meter



Egy ingyenes eszköz, amely kiértékeli a jelszavak erősségét, és tippeket ad a fejlesztésükhöz. A tanulók kísérletezhetnek jelszavak létrehozásával, és azonnali visszajelzést kaphatnak biztonsági szintjükről, így interaktív módon megérthetik az erős jelszavak fontosságát.

passwordmeter.com



Hivatkozások

- Alice. (2022, October 3). 5 Tools That Help Keep People Safe Online. Ryadel. Retrieved from <https://www.ryadel.com/en/5-privacy-data-protection-security-tools>
- Get Safe Online. (n.d.). Retrieved from <https://www.getsafeonline.org>
- Goodwall Team. (2022, March 24). 7 Best Online Safety Tools and Privacy Settings to Keep Yourself Protected. Retrieved from <https://www.goodwall.io/blog/online-safety-tools-and-privacy-settings>
- Lakhwani, S. (2024, June 19). Fundamentals of Cybersecurity [2024 Beginner's Guide]. upGrad KnowledgeHut Blog. Retrieved from <https://www.knowledgehut.com/blog/security/cyber-security-fundamentals>
- The Password Meter. (n.d.). Retrieved from <https://passwordmeter.com>
- Vodafone. (n.d.). Using online safety and wellbeing tools. Retrieved from <https://www.vodafone.co.uk/help-and-information/nspcc-phone-safety-toolkit/03-how-to-online-safety-tools>





KVÍZ

1. Mi a virtuális magánhálózat (VPN) egyik fő funkciója?
 - A. Automatikus vírusvédelem biztosítása
 - B. Az internet sebességének növelése
 - C. Felugró hirdetések megakadályozása minden webhelyen
 - D. Online tevékenységek titkosítása, különösen nyilvános Wi-Fi-hálózatokon

2. Milyen viselkedés veszélyeztetheti az online biztonságodat?
 - A. Erős, egyedi jelszavak használata minden fiókhoz
 - B. A böngésző adatvédelmi beállításainak rendszeres módosítása
 - C. Jelszókezelő használata a bejelentkezési adatok tárolására
 - D. Kéretlen e-mailekben található összes linkre kattintás

3. Hogyan érdemes javítani a böngésző adatvédelmi beállításait?
 - A. Az alapértelmezett beállítások használata módosítások nélkül
 - B. A követő sütik blokkolása és a szükségtelen engedélyek letiltása
 - C. Sütik kikapcsolása az összes webhelyen
 - D. Az összes webhely hozzáféréseinek engedélyezése a tartózkodási helyéhez





KVÍZ

4. Mi a böngésző adatvédelmi beállításainak célja?
- A. A felhasználó böngészési élményének felgyorsítása
 - B. A felhasználói jelszavak biztonságos tárolása
 - C. Annak szabályozása, hogy a webhelyek milyen információkat gyűjthetnek a felhasználóról
 - D. Felugró hirdetések megakadályozása minden webhelyen
5. Hogyan javíthatod a jelszavad erősségét?
- A. Szimbólumok beillesztésével, a kis- és nagybetűk keverésével és a hossz növelésével
 - B. Könnyen megjegyezhető, gyakori kifejezések használatával
 - C. Számok és speciális karakterek használatának kerülésével
 - D. Ugyanazon jelszó ismételt tesztelésével





Megoldások

- 1. kérdés: D
- 2. kérdés: D
- 3. kérdés: B
- 4. kérdés: C
- 5. kérdés: A





ERASMEDIAH

Educational Reinforcement Against
the Social Media Hyperconnectivity



Lélekben Otthon
Közhasznú Alapítvány

AdM
Archivio della Memoria



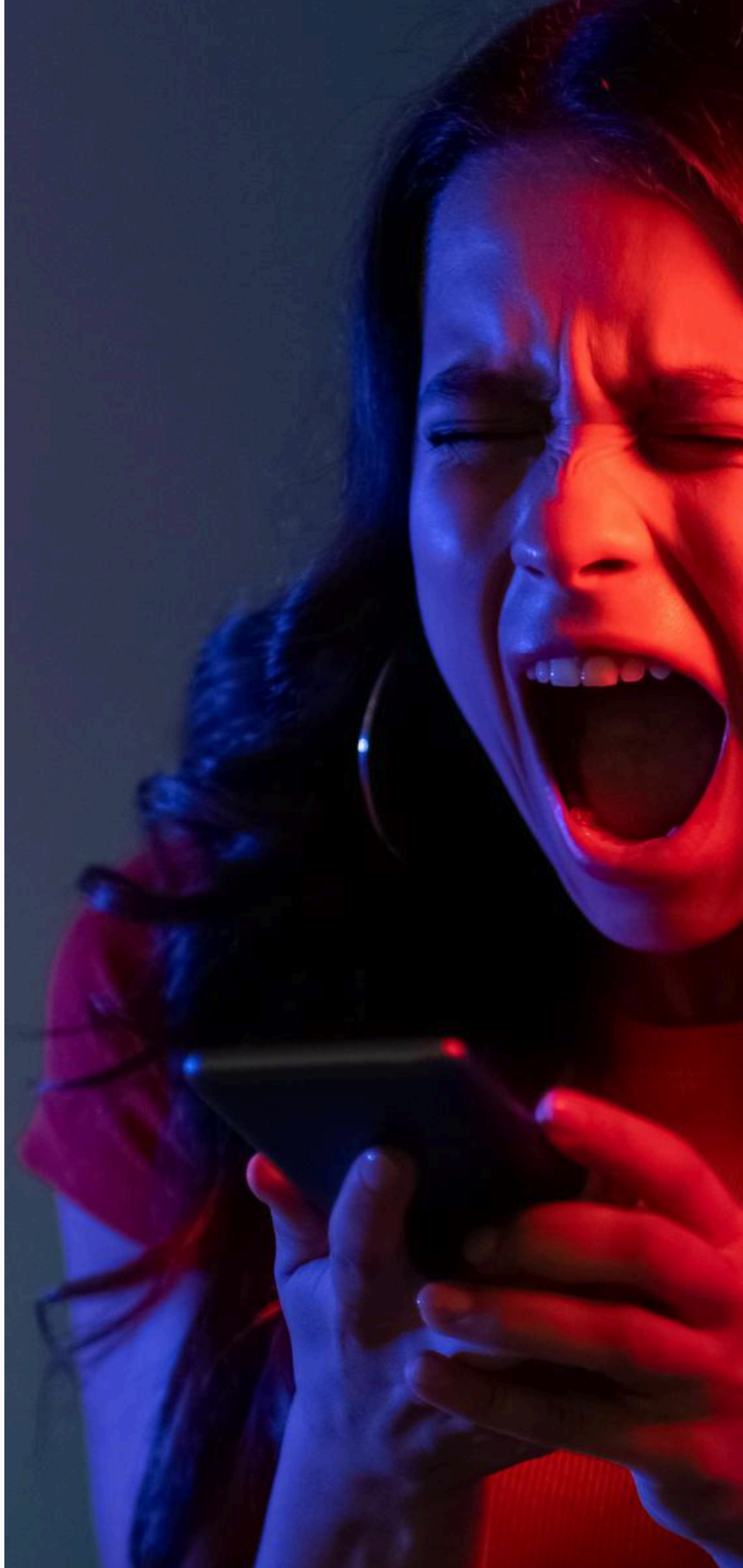
Centrum Wspierania
Edukacji
i Przedsiębiorczości

EDU
yayıncılık



ASSERTED KNOWLEDGE
THE ICT EQUALISERS

@  **Inno Hub**
Valencia



**Co-funded by
the European Union**