



5. MODUL

KIBERVÉDELEM ÉS ONLINE BIZTONSÁG



erasmediah.eu



**Co-funded by
the European Union**



5.2 Tananyag

Személyes adatok és adatvédelem online



ERASMEDIAH

Educational Reinforcement Against
the Social Media Hyperconnectivity



**Co-funded by
the European Union**

5.2. lecke

Személyes adatok és adatvédelem online

Célok:

- A személyes adatok online megosztásának kockázataira és az azokkal való visszaélés lehetőségére való **figyelemfelhívás**.
- **A tanulók felvértezése** gyakorlati stratégiákkal digitális lábnyomuk kezelésére, beleértve az adatvédelmi beállításokat, a biztonságos kommunikációt és a túlzott megosztás elkerülését.
- **Adatvédelmi incidensek példáinak feltárása**, bemutatva azok egyénekre gyakorolt hatását, és azt, hogy hogyan lehetett volna megelőzni azokat.
- **Proaktív viselkedés ösztönzése** olyan szokások kialakításával, mint az alkalmazásengedélyek áttekintése, a szolgáltatási feltételek megértése és az adatvédelmi eszközök használata.

Fő üzenet(ek):

- Minden online megosztott információ – a fényképektől és lájkoktól kezdve a helyadatokig – kihasználható kiberbűnözők vagy vállalatok által.
- A hozzáférés korlátozásának ismerete az elsődleges védelmi vonal.
- A személyes adatok védelme nem az internet kerüléséről szól; hanem az okos és tudatos cselekvésről. Egyszerű eszközökkel és döntésekkel biztonságban tarthatod az adataidat anélkül, hogy feláldoznád a digitális életedet.



ÓRA TÍPUSA:



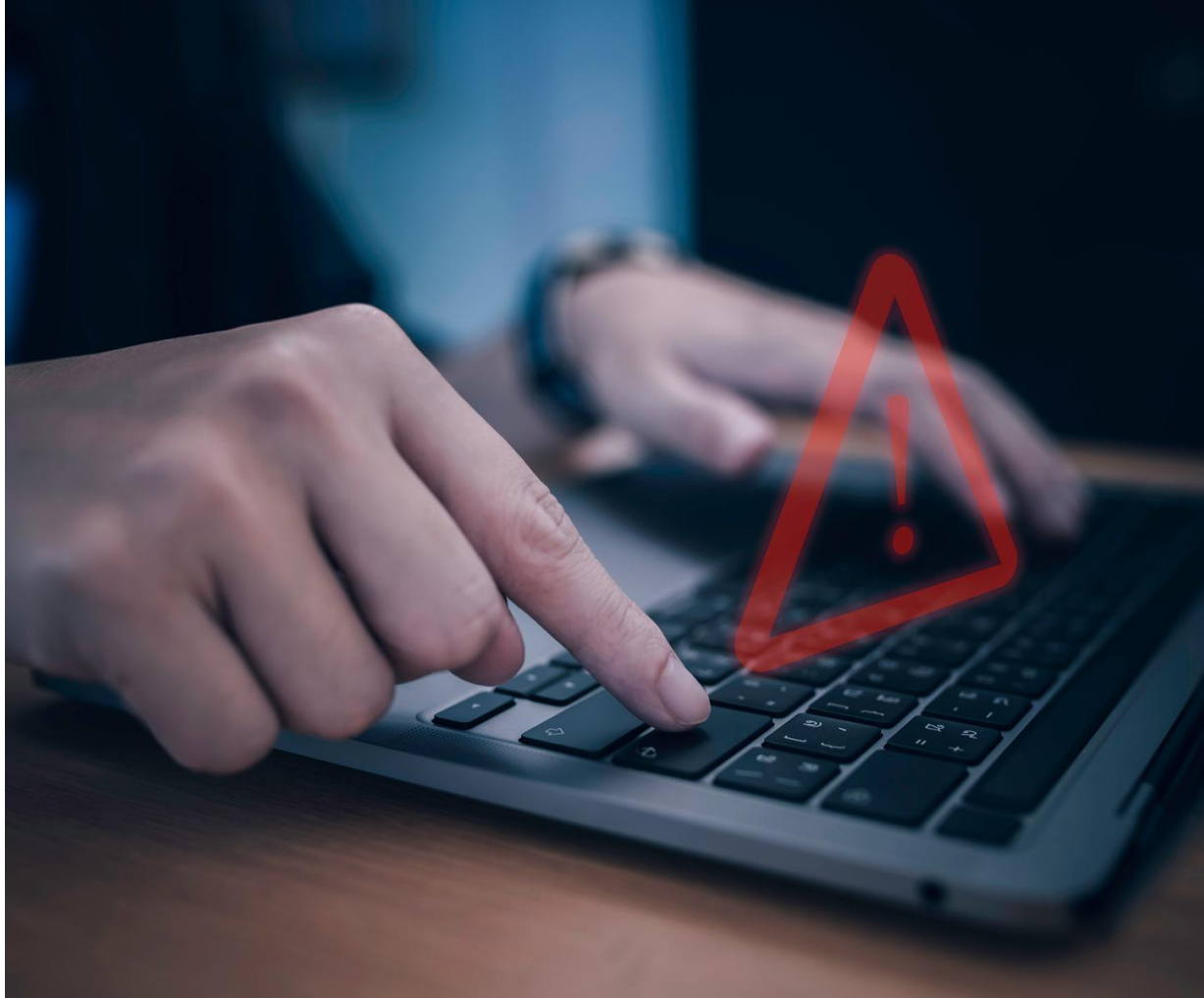


Áttekintés

Mivel életünk nagy része online zajlik, a személyes adatok védelme minden eddiginél fontosabb. Ez a lecke rávilágít arra, miért fontos a magánélet védelme. Megvizsgáljuk, hogy az olyan egyszerű szokások, mint a túlzott megosztás a közösségi médiában vagy az alkalmazások engedélyeinek gondolkodás nélküli elfogadása, hogyan szivárogtathatják ki adataitokat. Ha felismeritek ezeket a kockázatokat és gyakorlati stratégiákat alkalmaztok, elsajátíthatjátok azokat az eszközöket, amelyekkel megvédhetitek digitális identitásotokat és átvehetitek a saját online biztonságotok felett az irányítást.

A workshop 4 lépésre tagolódik:

- 1: Bevezetés az online adatvédelmi kockázatokba (15 perc)
- 2: Valós adatvédelmi incidensek feltárása (10 perc)
- 3: Gyakorlati stratégiák a személyes adatok védelmére (10 perc)
- 4: Záró reflexió és a legfontosabb tanulságok (5 perc)



1. lépés

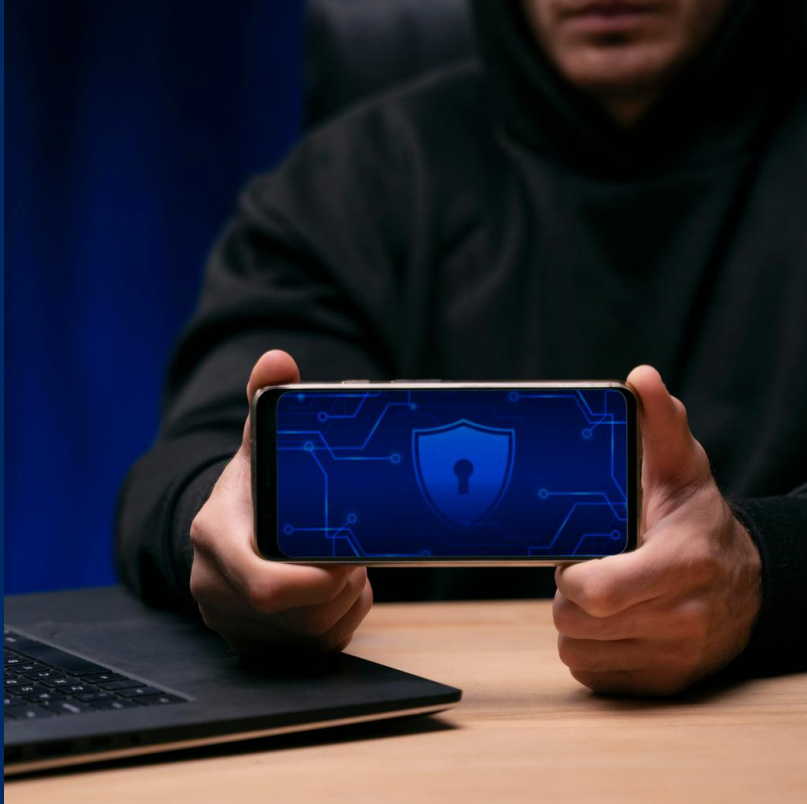
Bevezetés az online adatvédelmi kockázatokba

Letöltöttél már egy új alkalmazást, elfogadtad az engedélyeit, és soha nem gondoltál bele, hogy milyen információkat gyűjt? Amikor az internetet használjuk, személyes adataink – például a tartózkodási helyünk, jelszavaink és böngészési szokásaink – könnyen nyilvánosságra kerülhetnek. Most megvizsgáljuk, milyen adatvédelmi kockázatok léteznek, és hogyan érinthetnek Benneteket.

Első lépésként olvasd el a „Gyakori online adatvédelmi fenyegetések” című fejezetet ebből a [cikkből](#). (A szöveg angol nyelvű, a böngészőbe épített fordítóval érdemes magyar nyelvre váltani.)

Olvasás közben jegyzetelj:

- Melyik az az adatvédelmet fenyegető veszély, amelyet a legzavaróbbnak találsz?
- Indokold a választásodat!



1. lépés

Bevezetés az online adatvédelmi kockázatokba

Miután befejezted az olvasást, beszéljünk meg:

Melyik adatvédelmi fenyegetés lepett meg a legjobban, és miért?

- Szerinted hogyan befolyásolják ezek a fenyegetések a mindennapi életünket?
- Mi történhet, ha figyelmen kívül hagyjuk őket?

Nyugodtan ossz meg egy gyors példát a saját tapasztalataidból – legyen szó akár gyenge jelszavakról, adatkövetésről, vagy bármiről másról, amit láttál vagy hallottál. Ha bizonytalan vagy, mások meghallgatása ötleteket adhat!



2. lépés

Valós adatvédelmi incidensek feltárása

Nézzünk egy valós példát arra, hogy mi történik, ha nem vagyunk óvatosak a személyes adatainkkal online.

Képzeld el:

Sári imádja megosztani az életét a közösségi médiában. Fotókat posztol az új lakásáról, mesél a napi rutinjáról, sőt, még a tartózkodási helyét is megosztja, amikor a kedvenc kávézójában van. Egy nap Sári felfedezi, hogy a bankszámláját kiürítették. Hogyan? Egy kiberbűnöző összerakta a személyes adatait a nyilvános bejegyzéseiből – tartózkodási helyét, életmódbeli szokásait, sőt még a jelszavaira vonatkozó utalásokat is –, hogy hozzáférjen a fiókjaihoz. Mindez a túlzott megosztás miatt!

Most gondold át a következő kérdéseket:

- Mi romlott el? Milyen cselekedetek vagy szokások vezettek az adatvédelmi incidenshez?
- Hogyan lehetett volna megelőzni ezt a helyzetet? Milyen egyszerű változtatások eredményezhettek volna változást?

Írd le a válaszaidat, és készülj fel arra, hogy megoszd azokat a csoporttal.



2. lépés

Valós adatvédelmi incidensek feltárása

Közös megbeszélés:

- Szerinted mi romlott el Sára helyzetében?
- Szerinted miért történnek ilyen könnyen adatvédelmi incidensek?

Végül gondold át egy pillanatra:

- Te vagy egy ismerősöd találkozott már online adatvédelmi problémával? Lehet ez egy gyanús e-mail, egy feltört fiók vagy egy túlzott megosztás a közösségi médiában.
- Hogyan történt, és mi lett a következménye?
- Ha kényelmesen érzed magad, oszd meg a történetedet a csoporttal. Ha nem, az sem baj – már a pusztá meghallgatás is értékes meglátásokhoz juttat.



3. lépés

Gyakorlati stratégiák a személyes adatok védelmére

Most, hogy megvizsgáltuk az adatvédelmi kockázatokat és a valós példákat, összpontosítsunk a gyakorlati lépésekre, amelyekkel megvédhetjük magunkat (adatainkat) online.

Kezdjük egy gyors videóval az adatvédelemről.

Figyelj a megosztott legfontosabb tippekre.

A megtekintést követően írd le 3 konkrét lépést, amelyeket megtehetsz online adatvédelmed javítása érdekében. Gondold át:

- Az adatvédelmi beállítások módosítása a közösségimédia-fiókjaidon.
- Alkalmazásengedélyek áttekintése a telefonodon.
- Légy óvatos azzal, hogy milyen személyes adatokat osztasz meg online, különösen nyilvános platformokon.



3. lépés

Gyakorlati stratégiák a személyes adatok védelmére

Most pedig osszatok meg egy-egy stratégiát, amelyet megvalósítani terveztek. Például:

- „Ma este átnézem az összes alkalmazást a telefonomon, és eltávolítom azokat, amelyeket nem használlok.”
- „Korlátozni fogom, hogy kik láthatják a Facebook/Instagram-bejegyzéseimet, és kikapcsolom a profilom nyilvános láthatóságát.”

Beszéljük meg:

- Mi teszi ezeket az adatvédelmi szokásokat könnyűvé vagy nehezen elsajátíthatóvá?
- Túl könnyen megosztunk információkat online?
- Úgy gondoljuk, hogy az adatvédelmi beállítások és engedélyek beállításai zavaróak vagy időigényesek?
- Miért hagyják figyelmen kívül sokan az egyszerű adatvédelmi gyakorlatokat, még akkor is, ha ismerik a kockázatokat?
- Azért, mert nem hiszik, hogy velük fog ilyen történni?
- Szerinted azért van ez, mert az emberek nincsenek tisztában az eszközökkel vagy a szokásokkal, amelyeket használniuk kellene?

Hogyan maradhatsz motivált, hogy ragaszkodj ezekhez a szokásokhoz?

Például emlékeztetők beállítása a jelszavak frissítésére vagy a közösségi média beállításainak rendszeres ellenőrzése.

4. lépés

Záró gondolatok és a legfontosabb tanulságok

A workshop lezárásaként szánjunk egy percet arra, hogy átgondoljuk, mit tanultunk, és hogyan tudjuk azokat a mindennapi életünkben alkalmazni.

Kérdezd meg magadtól: Mi az az egy szokás, amit ma megváltoztathatsz az online adatvédelmed javítása érdekében? Ez lehet valami egyszerű, például a helymegosztás kikapcsolása, a közösségi média adatvédelmi beállításainak ellenőrzése, vagy az óvatosabb gondolkodás arról, hogy mit teszel közzé. Most gondold át, hogyan segíthetsz másoknak: Hogyan fogod megosztani a ma tanultakat egy barátoddal, családtagoddal vagy kollégáddal? Már az apró tippek is, például az erős jelszavak fontosságának magyarázata vagy az alkalmazásengedélyek ellenőrzésének bemutatása nagy változást hozhatnak.





Összefoglalás

- **Figyelj oda, hogy mit osztasz meg online:** Az apró részletek, mint például a helyszínek vagy a szokások, rossz kezekbe kerülve könnyen felhasználhatók.
- **Adatvédelmi beállítások áttekintése és módosítása:** Rendszeresen ellenőrizze a közösségi média, az alkalmazásengedélyek és a fiókbeállítások beállításait a szükségtelen adatmegosztás korlátozása érdekében.
- **Korlátozd a nyilvánosan közzétett személyes adatok körét:** Kerüld az olyan érzékeny adatok megosztását a közösségi médiában vagy más platformokon, mint a címek, szokások vagy személyes azonosítók.
- **Légy óvatos az alkalmazásokkal és linkekkel:** Gondold át, mielőtt linkekre kattintasz, alkalmazásokat töltesz le, vagy engedélyeket adsz – csak ellenőrzött forrásokban bízz.
- **Kezdj apró lépésekkel:** Az olyan egyszerű szokások, mint a helymeghatározás kikapcsolása vagy a nyilvános bejegyzések korlátozása, nagy hatással lehetnek a személyes adatok védelmére.



Útmutató tanárok és trénerek számára

Célkitűzés:

A lecke célja, hogy a résztvevők gyakorlati készségeket és ismereteket szerezzenek személyes adataik védelméhez és az online adatvédelem fenntartásához. Interaktív tevékenységek, valós példák és reflektív beszélgetések segítségével a résztvevők azonosítják a gyakori online adatvédelmi kockázatokat, betekintést nyernek az adatvédelmi incidensek hatásaiba, és gyakorlatias stratégiákat dolgoznak ki adataik védelmére. A lecke végére a tanulók tudatosabbnak, felkészültebbnek és elkötelezettebbnek érzik magukat a digitális biztonságukat fokozó szokások elsajátítása iránt.

Szükséges anyagok:

- Internetkapcsolat videó lejátszásához vagy cikkhez
- Projektor és vászon
- Hangszórók
- Hozzáférés az ajánlott kiberbiztonsági eszközökhöz
- Flipchartpapír vagy táblafilcek
- Tollak, ceruzák és jegyzettömbök





1. lépés: Bevezetés az online adatvédelmi kockázatokba (15 perc)

1. Kezdj egy könnyen érthető kérdéssel: „Mikor töltöttél le utoljára egy alkalmazást, fogadtad el az engedélyeit, vagy osztottál meg egy bejegyzést online? Elgondolkodtál már azon, hogy milyen személyes adatokat osztasz meg?”. Magyarázd el, hogy ezek az apró, mindennapi tettek akaratlanul is kiadhatnak olyan privát adatokat, mint a tartózkodási helyed, a böngészési szokásaid vagy a személyes rutinod harmadik felek vagy kiberbűnözők számára.

2. Hangsúlyozd, hogy a személyes adatok védelme elengedhetetlen a mai digitális világban. Emeld ki, hogy a látszólag ártalmatlan viselkedések – mint például egy fénykép megosztása vagy az alkalmazások hozzáféréseinek engedélyezése a névjegyeidhez – nem kívánt következményekkel járhatnak. Használj egy egyszerű hasonlatot: „A személyes adataid olyanok, mint egy kirakós darabjai. Egyetlen darab önmagában ártalmatlannak tűnhet, de másokkal kombinálva sokat elárulhatnak rólad.”

3. Tevékenység – cikkolvasás és reflexió

Osszd meg vagy nyomtasd ki ki a Mi az online adatvédelem? cikk „Gyakori online adatvédelmi fenyegetések” című részét.

Kérd meg a résztvevőket, hogy:

- Határozzák meg, hogy melyik adatvédelmi fenyegetést tartják a leginkább aggasztónak.
- Gondolják át, miért tűnik ez a fenyegetés különösen veszélyesnek vagy meglepőnek.
- Bátorítsa őket, hogy jegyezzenek fel rövid gondolatokat a csoportos megbeszélésre való felkészülés érdekében.





1. lépés: Bevezetés az online adatvédelmi kockázatokba (15 perc)

4. Vezessen le egy rövid beszélgetést a következő témakörök segítségével:

- „Melyik adatvédelmi fenyegetés tűnt fel a leginkább, és miért?”
- „Hogyan befolyásolják ezek a kockázatok az online viselkedését vagy szokásait?”

Kérjen meg néhány résztvevőt, hogy osszák meg gondolataikat, megerősítve azt, hogy ezen kockázatok tudatosítása az első lépés a személyes adatok jobb védelme felé.

5. Összefoglalás – foglalja össze a beszélgetés fő pontját (például: Az adatvédelmi kockázatok felismerésével átveszi az irányítást online jelenléte felett. A tudatosság lehetővé teszi, hogy okosabb döntéseket hozzon azzal kapcsolatban, hogy mit oszt meg és hogyan lép interakcióba online).





2. lépés: Valós adatvédelmi incidensek feltárása (10 perc)

1. Kezdeként osszon meg egy ismerős és hatásos forgatókönyvet, amely bemutatja, hogyan vezethet súlyos adatvédelmi incidensekhez az online túlzott megosztás.

Magyarázza el a résztvevőknek, hogy ez a történet nem egyedi. Sokan tudtukon kívül személyes adatokat osztanak meg, amelyeket a kiberbűnözők vagy rosszindulatú egyének felhasználhatnak a nyomon követésére, a fiókjaikba való betörésre, vagy akár a személyazonosságuk ellopására. Hangsúlyozza, hogy az adatvédelmi incidensek gyakran apró, látszólag ártalmatlan információkkal kezdődnek.

2. Mutasson be egy rövid írásos forgatókönyvet a résztvevőknek, amely Sári történetén vagy egy hasonló hipotetikus helyzeten alapul:

Példa egy másik forgatókönyvre:

„Alex letöltött egy ingyenes mobilalkalmazást anélkül, hogy elolvasta volna az engedélyeket. Az alkalmazás hozzáfért a tárolási helyéhez, a névjegyeihez és a médiafájljaihoz. Röviddel ezután furcsa üzeneteket vett észre, amelyeket a barátai kaptak. Kiderült, hogy az alkalmazás gyűjtötte az adatait, és spam üzeneteket küldött a fiókját használva.”





2. lépés: Valós adatvédelmi incidensek feltárása (10 perc)

3. A szituáció elemzése:

- Egyénileg vagy kis csoportokban dolgozva elemezzék a helyzetet.
- Mi romlott el? Milyen cselekedetek vagy viselkedések okozták az incidenst?
- Hogyan lehetett volna ezt megelőzni? Határozzon meg egyszerű lépéseket vagy szokásokat a személyes adatok védelme érdekében.
- Írják le röviden a gondolataikat.

4. A résztvevők osszák meg gondolataikat az alábbiak szerint:

- „Tapasztalt már Ön vagy valamelyik ismerőse hasonló problémával, például adathalászattal, hackeléssel vagy túlzott megosztással?”
- „Miért osztanak meg az emberek annyi személyes információt anélkül, hogy mérlegelnék a kockázatokat?”
- Lehetséges okok:
 - Alkalmazások vagy platformok megbízhatósága.
 - Nem tudatosítva a következményeket.
 - Zavaró adatvédelmi beállítások.

Ösztönözze a tapasztalatok vagy meglátások nyílt, támogató megosztását.





3. lépés: Gyakorlati stratégiák a személyes adatok védelmére (10 perc)

1. Videóvetítés Mutasd be az Adatvédelem című videót. Ösztönözze a résztvevőket, hogy fordítsanak nagy figyelmet a videóban megosztott gyakorlati, végrehajtható stratégiákra. Hangsúlyozza ki, hogy ezek a tippek könnyen megvalósíthatók, de jelentősen javíthatják az online adatvédelmet.

2. Tevékenység – „Személyes adatvédelmi terv”

Kérje meg a résztvevőket, hogy írjanak le három lépést, amit online adatvédelmük védelme érdekében tesznek.

Bátorítsa őket, hogy fontolják meg:

- A közösségi média adatvédelmi beállításainak módosítása.
- Alkalmazásengedélyek áttekintése az eszközeiken.
- Odafigyelnek arra, hogy mit tesznek közzé nyilvánosan.

3. Csoportos megbeszélés:

Kérje meg a résztvevőket, hogy osszanak meg egy olyan tevékenységet, amelyet a csoporttal terveznek megvalósítani.

A következő témakörök segítségével irányítsa a beszélgetést:

- „Melyik stratégiát tartja a legkönnyebbnek ma elkezdni, és miért?”
- „Milyen kihívásokkal szembesülhetsz, miközben megpróbálsz elsajátítani ezeket a szokásokat?”
- „Hogyan tudjuk leküzdeni a gyakori akadályokat, például azt, hogy elfelejtjük módosítani a beállításokat, vagy hogy zavarónak találjuk az adatvédelmi eszközöket?”

Bátorítsa a csoportot, hogy adjanak gyakorlati tippeket, vagy osszák meg személyes tapasztalataikat arról, hogyan küzdöttek le hasonló kihívásokat. Hangsúlyozza ki, hogy a következetes apró lépések jelentős javuláshoz vezethetnek az online adatvédelem terén.

4. Ezenkívül megkérheti a résztvevőket, hogy gondolják át, hogyan oszthatnák meg ezeket a stratégiákat a barátaikkal vagy a családjukkal.





4. lépés Záró reflexió és a legfontosabb tanulságok:

1. Kérje meg a résztvevőket, hogy gondolják át a következőket:

- „Mi az az egy szokás, amit mától kezdve megváltoztatsz az online adatvédelem javítása érdekében?”
- „Hogyan fogod megosztani a tanultakat a barátaiddal vagy a családdoddal?”

2. Erősítse meg a lecke főbb pontjait:

- Az apró változtatások, mint például a beállítások módosítása vagy a megosztás korlátozása, nagy hatással bírnak.
- Az adataid védelme biztosítja a digitális identitásod feletti kontrollt.

3. Zárja a foglalkozást egy zárómonddal. Például: „A személyes adatai értékesek. Tegyen apró, okos lépéseket a védelme érdekében, és így biztonságban marad online.”

Főbb tanulságok:

- A lecke végére a résztvevőknek világosan meg kell érteniük, hogy **az online adatvédelem a tudatossággal és a kis, gyakorlatias lépésekkel kezdődik.**
- Az egyszerű változtatások, mint például **az alkalmazásengedélyek módosítása, a közösségi média adatvédelmi beállításainak áttekintése és a nyilvánosan megosztott tartalmak tudatosítása, jelentősen csökkenthetik a kockázatokat.**
- Ösztönözze a résztvevőket, hogy **vegyék át az irányítást digitális viselkedésük felett** olyan szokások kialakításával, mint az adataikhoz való hozzáférés kilétének ellenőrzése és a gyanús linkekkel vagy üzenetekkel szembeni óvatosság.
- Erősítse meg azt az elképzelést, hogy **a személyes adatok védelme lehetővé teszi az egyének számára, hogy megőrizzék digitális identitásuk és biztonságuk feletti ellenőrzést.**





Utánkövetés és otthoni tevékenységek

- Kérje meg a résztvevőket, hogy a következő napokban **legalább egy, a foglalkozás során azonosított adatvédelmi intézkedést hajtsanak végre.**
- Ez magában foglalhatja egy közösségi média platform adatvédelmi beállításainak áttekintését, a nem használt alkalmazások törlését, vagy adatvédelmi tippek megosztását barátaikkal vagy családtagjaikkal. Javasold nekik, hogy dokumentálják a haladásukat, és gondolkodjanak el azon, hogy ezek a változtatások hogyan segítik őket abban, hogy biztonságosabban érezzék magukat online.
- Ezenkívül biztassa a résztvevőket **olyan eszközök felfedezésére, mint a DuckDuckGo** (egy privát keresőmotor) **vagy a Google Privacy Checkup**, hogy megtudják, milyen könnyen javíthatják online biztonságukat.
- Fontolja meg egy utólagos megbeszélés megszervezését, ahol a résztvevők megoszthatják tapasztalataikat és megbeszélhetik a felmerült kihívásokat.

Tippek tanároknak:

Javasoljuk, hogy valós példákat is építsenek be a beszélgetésbe, hogy az online adatvédelem fogalma érthető legyen.

Használjanak olyan forgatókönyveket, mint a túlzott közösségi média megosztás, adatvédelmi incidensek vagy alkalmazásengedélyek, hogy bemutassák, milyen apró szokásoknak lehetnek nagy következményei.

Teremtsenek támogató teret a résztvevők számára, hogy ítélezés nélkül megosszák tapasztalataikat.

A figyelem folyamatos fenntartása érdekében építsenek be rövid, gyakorlati feladatokat az órákba, például bemutatva, hogyan módosíthatók az adatvédelmi beállítások, vagy hogyan ismerhetők fel a gyanús linkek. Rendszeresen térjenek vissza a témára az adatvédelmi tudatosság fenntartása érdekében, és ösztönözzék a diákokat arra, hogy adataik védelmét egész életen át tartó szokásként lássák.





Eszközök

DuckDuckGo



A DuckDuckGo egy adatvédelemre összpontosító keresőmotor, amely nem követi nyomon a keresési előzményeket, és nem gyűjt személyes adatokat. Biztosítja, hogy a keresések privátak maradjanak, és segít minimalizálni a böngészés közben hátrahagyott digitális lábnyomot.

duckduckgo.com

Google Adatvédelmi Áttekintés



A Google Adatvédelmi Ellenőrző egy beépített eszköz, amely segít a Google-fiókbeállítások kezelésében. Lehetővé teszi, hogy áttekintse és módosítsa, milyen személyes adatokat gyűjtenek, kik láthatják a tevékenységeit, és mely alkalmazások férhetnek hozzá az adataihoz.

myaccount.google.com/privacycheckup



Hivatkozások

- DuckDuckGo (n.d.). Retrieved from <https://duckduckgo.com>
- Farrier, E. (2024, August 21). A guide to protecting your personal information. Retrieved from <https://lifelock.norton.com/learn/internet-security/ways-to-help-protect-your-personal-information-online>
- Glover, E. (2024, January 24). What Is Online Privacy?. Built In. Retrieved from <https://builtin.com/articles/what-is-online-privacy>
- Google Privacy Checkup (n.d.). Retrieved from <https://myaccount.google.com/privacycheckup>
- Negrean, R. (n.d.). 10 Tips for Protecting Online Privacy: Strategies for Digital Security. Privacy Tutor. Retrieved from <https://privacytutor.net/10-tips-for-protecting-online-privacy>
- Tech Implement Infra Pvt Ltd. (2024, December 8). Essential Tips on Protecting Personal and Professional Data Online. [Video]. YouTube. <https://youtu.be/6WQzMAAd6mJs?si=cq1NFnjxu7i8NRk5>
- Webb, M. (2023, November 26). How to Protect Your Online Privacy: 7 Best Practices to Implement Today. Techopedia. Retrieved from <https://www.techopedia.com/how-to/how-to-protect-your-privacy-online>





KVÍZ

1. Milyen egyszerű lépést tehet a személyes adatok online visszaéléseinek korlátozása érdekében?
 - A. Kerülje teljesen a közösségi média fiókok létrehozását.
 - B. Kapcsolja ki az összes értesítést az eszközein.
 - C. Fogadja el az alkalmazásengedélyeket ellenőrzés nélkül.
 - D. Rendszeresen módosítsa a közösségi média adatvédelmi beállításait.
2. Az alábbiak közül melyik példa a túlzott megosztásra, ami személyazonosság-lopáshoz vezethet?
 - A. Nyaralási fotó megosztása csak közeli barátokkal
 - B. Tartózkodási helyed és napi rutinod nyilvános közzététele
 - C. Háziállataid fotóinak küldése privát üzenetben
 - D. Hangulatjelek használata online a hangulatod leírására
3. Hogyan javíthatja az alkalmazásengedélyek felülvizsgálata az online adatvédelmet?
 - A. Lehetővé teszi az alkalmazások szükségtelen személyes adatokhoz való hozzáféréseinek korlátozását.
 - B. Az engedélyellenőrzések kihagyásával gyorsabban letöltheti az alkalmazásokat.
 - C. Biztosítja, hogy az eszközén lévő összes alkalmazás automatikusan frissüljön.
 - D. Lehetővé teszi az alkalmazások zökkenőmentesebb futtatását az eszközödön





KVÍZ

4. Miért nem védik sokan személyes adataikat online?

- A. Az adatvédelmi eszközök nem érhetőek el a hétköznapi felhasználók számára.
- B. Az emberek megbíznak a vállalatokban, hogy adataik biztonságban vannak.
- C. Az adatvédelmi beállításokat és eszközöket gyakran figyelmen kívül hagyják, vagy zavarónak tartják.
- D. A legtöbb ember úgy gondolja, hogy nincsenek védendő személyes adataik.

5. Milyen jó szokást érdemes kialakítani a személyes adatok védelme érdekében?

- A. Ugyanazon jelszó használata a kényelem kedvéért
- B. Az alkalmazások folyamatos tartózkodási helyének nyomon követésének engedélyezése
- C. A szolgáltatási szerződések feltételeinek figyelmen kívül hagyása
- D. Óvatosság a bizalmas információk nyilvános platformokon történő megosztásával kapcsolatban





Megoldások

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





ERASMEDIAH

Educational Reinforcement Against
the Social Media Hyperconnectivity



Lélekben Otthon
Közhasznú Alapítvány

AdM
Archivio della Memoria

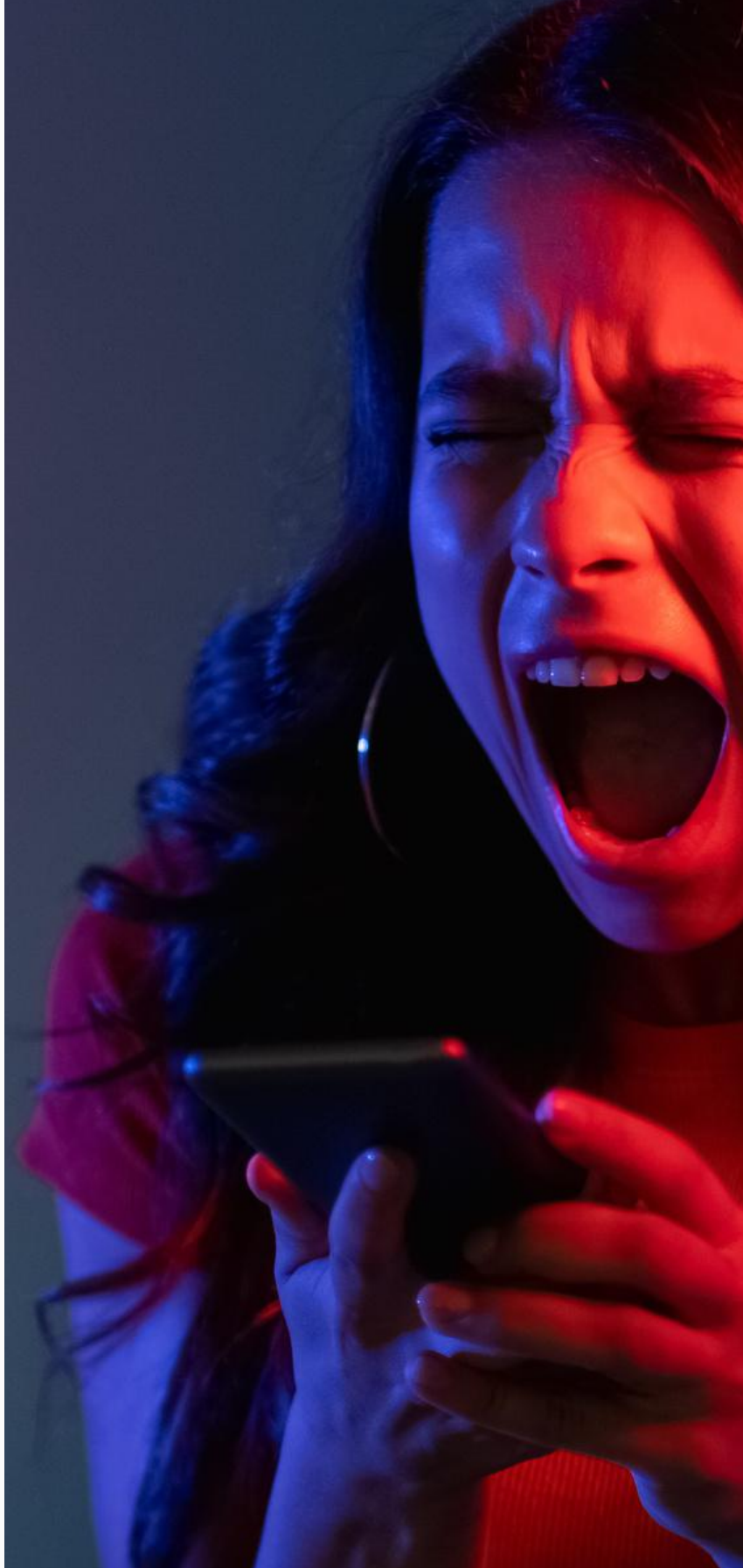


Centrum Wspierania
Edukacji
i Przedsiębiorczości

EDU
yayincılık



@Inno Hub
Valencia



**Co-funded by
the European Union**