ERASMEDIAH – EDUCATIONAL REINFORCEMENT AGAINST THE SOCIAL MEDIA HYPERCONNECTIVITY
PROJECT NUMBER: 2023-1-HU01-KA220-YOU-000161173

5. MODUL
KIBERVÉDELEM ÉS ONLINE BIZTONSÁG

ERASMEDIAH
Educational Reinforcement Against the Social Media Hyperconnectivity

erasmediah.eu

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

5.4 Tananyag

Kiberfenyegetések felismerése és stratégiák a nem megfelelő tartalomnak való kitettség megelőzésére

ERASMEDIAH
Educational Reinforcement Against the Social Media Hyperconnectivity

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Időtartam: 40 perc

5.4. lecke

Kiberfenyegetések felismerése és stratégiák a nem megfelelő tartalomnak való kitettség megelőzésére

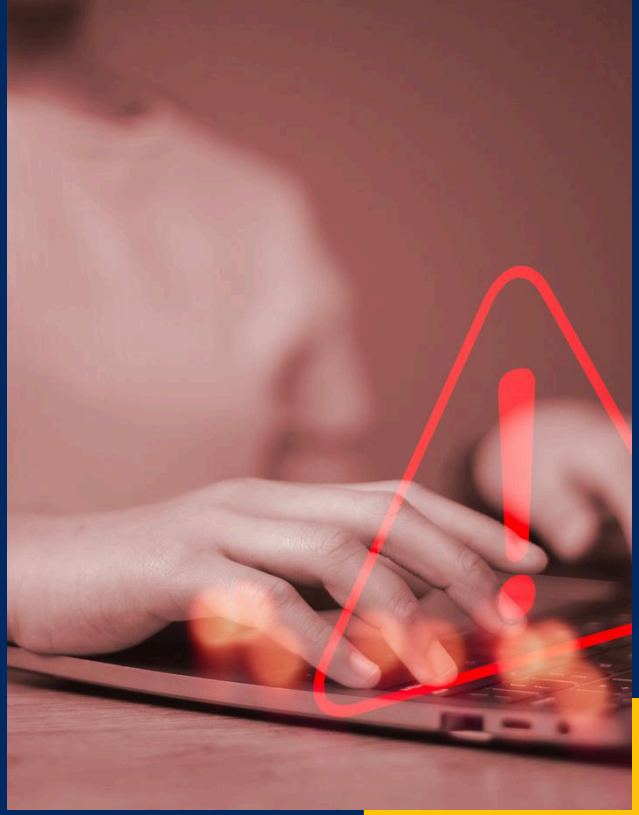
Célok:

- Az olyan elterjedt online kockázatokkal kapcsolatos tudatosság növelése, mint a nem megfelelő tartalmaknak való kitettség, az internetes zaklatás és a szexuális visszaélések elcsábítása, különösen a veszélyeztetett felhasználók, például a gyermekek és a tinédzserek megcélzásával.
- A tanulók felvértezése kritikus készségekkel, hogy felismerhessék a kiberfenyegetések figyelmeztető jeleit, például a gyanús linkeket, a ragadozó online viselkedést és a manipulatív tartalmakat.
- Az online interakciók kezelésében a proaktív szokások ösztönzése a kritikai gondolkodás elősegítésével, a biztonságos digitális terek azonosításával és az online élményekkel kapcsolatos nyílt kommunikáció fenntartásával.

Fő üzenet(ek):

- Az online fenyegetések gyakran ártatlannak tűnő platformok vagy interakciók mögött rejtőznek. A jelek felismerése kulcsfontosságú a biztonság megőrzéséhez.
- Az olyan egyszerű gyakorlatok, mint a tartalomszűrők használata és az erős kommunikáció fenntartása, segíthetnek megelőzni a káros tartalmaknak és a kiberfenyegetéseknek való kitettséget.

ÓRA TÍPUSA:



Áttekintés

A mai hiper-összekapcsolt digitális környezetben a nem megfelelő tartalmaknak és a kiberfenyegetéseknek való kitettség állandó kockázatot jelent. Ez a lecke átfogó képet ad e fenyegetések természetéről és kockázatairól, gyakorlati eszközöket kínál enyhítésükre, valamint stratégiákat a biztonságosabb online interakciók elősegítésére. A lebilincselő gyakorlatok és a gyakorlati tanácsok segítségével a résztvevők felkészültebbek lesznek arra, hogy biztonságosan és felelősségteljesen eligazodjanak a digitális világban.

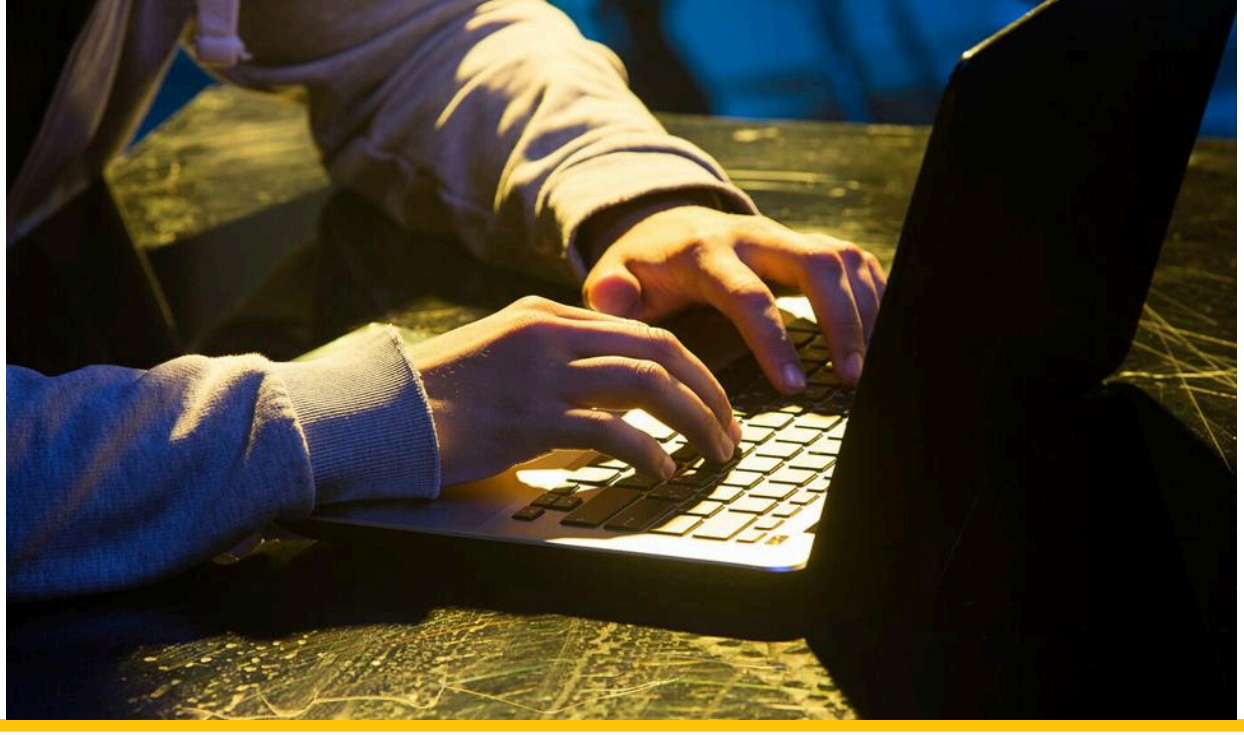
A workshop 4 lépésre tagolódik:

1: A kiberfenyegetések és a nem megfelelő tartalom alapjai (10 perc)

2: Figyelmeztető jelek és kockázatok felismerése (15 perc)

3: Megelőzési és mérséklési megközelítések (10 perc)

4: Reflexió és alkalmazás (5 perc)



1. lépés

A kiberfenyegetések és a nem megfelelő tartalom lényege

Találkoztál már olyannal az interneten, ami kellemetlenül vagy bizonytalanul érintett?
A kiberfenyegetések olyan káros tevékenységek, amelyek online személyeket vagy rendszereket céloznak meg, és céljuk az információk ellopása, károkozás vagy a sebezhetőségek kihasználása.
Példák többek között:

- Cyberbullying: Online platformok használata zaklatásra vagy megfélemlítésre.
- Adathalászat: Megtévesztő üzenetek küldése, hogy rávegyék az embereket személyes adataik kiadására.
- Behálózás: Kapcsolatépítés valakivel online, hogy később kihasználja.

Mi minősül nem megfelelő tartalomnak?

- Káros, explicit vagy bizonyos korosztályok számára nem megfelelő tartalom, például:
- Explicit képek vagy videók.
- Manipulatív vagy behálózó üzenetek.
- Erőszakos vagy gyűlöletkeltő anyagok.

1. lépés

A kiberfenyegetések és a nem megfelelő tartalom lényege

Az ilyen tartalmaknak való kitettség érzelmi stresszt okozhat, károsíthatja a kapcsolatokat, és hosszú távú következményekkel járhat, mint például a személyazonosság-lopás vagy a kizsákmányolás.

Gyakorlat

Most kiscsoportokra oszlunk. Minden csoport kap egy forgatókönyvet elemzésre:

1. forgatókönyv: Kapsz egy e-mailt egy idegentől, aki személyes adatokat kér tőled.

2. forgatókönyv: Gyanús linket látsz egy e-mailben.

3. forgatókönyv: Nem helyénvaló hozzászólásra bukkansz a közösségi médiában.

A feladatotok, hogy a csoportodban válaszolj a kérdésekre:

- Mi a kockázatos ebben a helyzetben?
- Hogyan tudsz biztonságosan reagálni?

Miután a csoportok elkészültek, osszák meg egy közös megbeszélés keretében a következtetéseket.

2. lépés

Figyelmeztető jelek és kockázatok felismerése

Vess egy pillantást az alábbi példákra, és gondold át, hogy láttál-e már hasonlót az interneten. Ötletelés közben csoportosan beszéljétek meg, hogy melyek a leggyakoribb figyelmeztető jelek, és hogyan reagálhattok rájuk.

1. Ismeretlen vagy gyanús feladó

Kapsz egy üzenetet egy ismeretlen személytől, aki személyes adatokat kér, vagy arra kér, hogy kattints egy linkre.

Az e-mail cím szokatlannak tűnik, például "bank123random@mail.com" egy hivatalos cím helyett.

Vitaindító kérdés: „Mit teszel, ha üzenetet kapsz valakitől, akit nem ismersz?”

2. Helyesírási vagy nyelvtani hibák

Az üzenet tele van helyesírási hibákkal vagy furcsa megfogalmazásokkal.

Példa: „A fiókod blokkolva van! Kattints ide a reaktiváláshoz”

Vitaindító kérdés: „Gyanút keltenek-e az üzenetben előforduló hibák? Miért, vagy miért nem?”

2. lépés

Figyelmeztető jelek és kockázatok felismerése

3. Sürgős kérések vagy fenyegetések

Üzenetek, mint például: „Ha 24 órán belül nem fizet, a fiókját deaktiváljuk!” A tartalom megpróbál megijeszteni, vagy gyors cselekvésre kényszeríteni.

Vitaindító kérdés: „Hogyan lehet megkülönböztetni a valódi figyelmeztetést egy átveréstől?”

4. Túl szép, hogy igaz legyen ajánlatok

Hihetetlen jutalmakat ígérő hirdetések: „Nyertél egy vadonatúj iPhone-t! Kattints ide a nyereményed átvételéhez”

Weboldalak, amelyek irreális előnyöket kínálnak kevés erőfeszítéssel.

Vitaindító kérdés: „Miért veszélyesek az ilyen jellegű ajánlatok?”

2. lépés

Figyelmeztető jelek és kockázatok felismerése

5. Ismeretlen linkek vagy mellékletek

Egy nem megbízhatónak tűnő linket kapsz, például: „www.freegift.now”.

Ismeretlen feladóktól származó mellékletek, amelyek vírusokat tartalmazhatnak.

Vitakérdés: „Hogyan ellenőrizhető, hogy egy hivatkozás vagy melléklet biztonságos?”

Feladat:

- A csoportban válasszatok ki egyet ezek közül a figyelmeztető jelek közül, és beszéljétek meg, hogyan kezelnétek a helyzetet.
- A végén minden csoport megosztja meglátásait és ötleteit arról, hogyan kerülhetik el ezeket a kockázatokat a mindennapi online tevékenységek során.

3. lépés

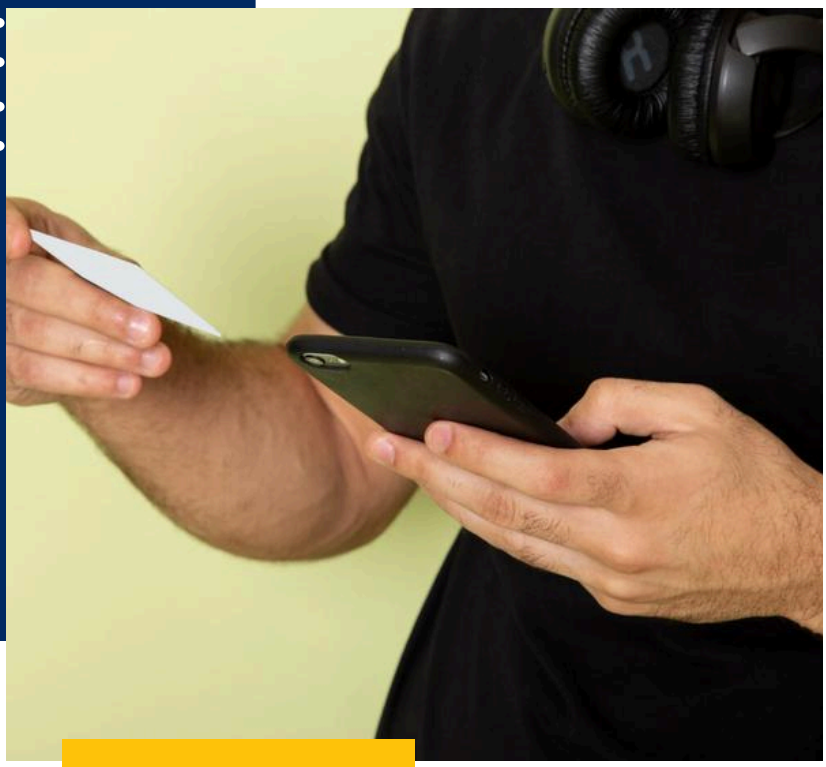
Megelőzési és ártalomcsökkentési megközelítések

Az online biztonság megőrzésének legjobb módja, ha proaktív lépéseket teszünk adataink védelme és a kockázatok megelőzése érdekében, mielőtt azok bekövetkeznének. Fedezzünk fel egyszerű stratégiákat, amelyeket azonnal elkezdhettek használni.

Maradjunk ugyanabban a csoportban. Olvassátok el az alábbi listát azokról az egyszerű dolgokról, amelyeket megtehettek az online kockázatok csökkentése érdekében:

- **Használj erős, egyedi jelszavakat,** és rendszeresen frissítse azokat.
- **Engedélyezd a többtényezős hitelesítést (MFA) a** fontos fiókokhoz.
- **Kerüld a gyanús linkeket és mellékleteket –** mindig ellenőrizd a forrást.
- **Tekintsd át az adatvédelmi beállításokat** a közösségi médiában **é**s az alkalmazásokban, hogy szabályozhassa, kik láthatják az adatait.
- **Tartsa naprakészen a szoftvereket** a biztonsági réseket javítva.

A csoportban beszéljétek meg, hogy ezek közül melyeket gyakoroljátok már, és melyek megvalósítása lehet nehéz.
Közös megbeszélés:
„Melyik stratégiát tartjátok a leghatékonyabbnak az online biztonság megőrzésére?”



3. lépés

Megelőzési és ártalomcsökkentési megközelítések

„Hogyan emlékeztetheted magad arra, hogy jobb szokásokat alakíts ki, például ellenőrizd az adatvédelmi beállításokat vagy kerüld a kockázatos linkeket?” Az ötletelés után minden csoport megoszt egy **új** stratégiát, amelyet alkalmazni tervez, és néhány szóban elmagyarázza, hogy miért fontos.

Végezetül szánj egy percet arra, hogy elgondolkodj egy konkrét szokáson vagy eszközön, amelynek azonnali alkalmazását elkötelezed magad az online biztonságod javítása érdekében. Írd le egy cetlire, és gondold át, hogyan segíthetsz másoknak is ugyanezen szokások elsajátításában. Tudásod megosztásával biztonságosabb online környezetet teremthetsz nemcsak magad, hanem a barátaid, a családod és a közösséged számára is.

4. lépés

Reflexió és alkalmazás

Most, hogy megismerkedtünk az online kockázatokkal és a megelőzési stratégiákkal, itt az ideje, hogy átgondoljuk, mit tanultunk, és hogyan alkalmazhatjuk azokat a mindennapi digitális életünkben.
Szánj egy percet arra, hogy csendben válaszolj a kérdésre:
„Milyen jelenlegi szokásod van, ami veszélybe sodorhat az interneten?”
Írd le a válaszodat egy post-it cetlire.
Következő lépésként alkossatok párokat egy párral, és osszátok meg a gondolataitokat:

- Magyarázzátok el, melyik kockázatos szokást azonosítottátok, és miért jelenthet problémát.
- Osszátok meg a kockázat enyhítésére tervezett intézkedést vagy eszközt.
- Adjatok egymásnak visszajelzést vagy további ötleteket a terveitek megerősítése érdekében.
- Beszéljétek meg, hogyan alkalmazhatók ezek a stratégiák különböző helyzetekben, például nyilvános Wi-Fi használatakor, személyes adatok megosztásakor, vagy a becsmérlés és az adathalászat elkerülésekor.

Összefoglalás

- A tudatosság az első lépés a védekezés felé.
- A figyelmeztető jelek mindenhol ott vannak, de ha megtanulod felismerni őket és megfelelően reagálni, jelentősen növelheted az online biztonságodat!
- A kiberfenyegetések és a nem megfelelő tartalmak megértése lehetővé teszi a potenciális kockázatok azonosítását és magabiztos reagálását.
- A mindennapi online helyzetekben rejlő kockázatok felismerése lehetővé teszi a gyors cselekvést és a veszélyek elkerülését.
- A tudatosság terjesztésével hozzájárulsz egy biztonságosabb online közösség létrehozásához mindenki számára.

Útmutató trénerek és tanárok számára

Célkitűzés:
A lecke célja, hogy felhívja a figyelmet az online kockázatokra, beleértve a kiberfenyegetéseket és a nem megfelelő tartalmakat, és felvértezze a résztvevőket a biztonságosabb online interakciók elősegítésére szolgáló gyakorlati stratégiákkal. Valós helyzetek elemzésével a résztvevők megtanulják azonosítani a kockázatokat, felismerni a figyelmeztető jeleket, és megelőző intézkedéseket tenni.

Szükséges anyagok:

- Flipchart vagy digitális prezentációs eszköz a kulcsfogalmak felvázolásához
- Tollak és filctollak
- Üres papírlapok jegyzeteléshez vagy feladatok elvégzéséhez
- Hozzáférés olyan eszközökhöz, mint a CyberWise vagy a Malwarebytes Browser Guard (amennyiben bemutatja őket a résztvevőknek)
- Színes post-it jegyzetlapok ötleteléshez

1. lépés: A kiberfenyegetések és a nem megfelelő tartalom alapjai (10 perc)

1. Kezdje a résztvevők kérdésével: „Találkoztak már valaha valami gyanús vagy veszélyes dologgal az interneten?”. Bátorítsa néhányukat, hogy osszák meg tapasztalataikat, vagy adjanak egy rövid példát, például egy gyanús e-mail fogadása vagy egy sértő hozzászólás megtekintése. Ezzel hangsúlyozhatja az online kockázatok megértésének és kezelésének fontosságát.
2. Rövid előadás – ismertesse a főbb kiberfenyegetéseket: adathalászat, behálózás stb. Határozza meg a nem megfelelő tartalmat, beleértve a következőket:

- Explicit anyagok – Káros vagy megrázó képek és videók.
- Ragadozó üzenetek - Manipulatív vagy káros kommunikáció.
- Korhatár-besorolás nélküli tartalom – Bizonyos korosztályok számára nem megfelelő anyag.

3. Tevékenység: Ossza a résztvevőket 3-5 fős csoportokra, és rendelj hozzájuk a három különböző forgatókönyv egyikét.

Csoportok számára szóló utasítások:

- Kockázat elemzése: Beszéljétek meg, mi teszi kockázatossá a forgatókönyvet (pl. ismeretlen feladó, sürgős hangjelzés vagy gyanús link).
- Javasoljanak biztonságos intézkedéseket: keressenej gyakorlati megoldásokat:
  - E-mailek esetén: Kerülje a linkekre kattintást, ellenőrizze a feladót hivatalos csatornákon keresztül, vagy jelentse spamként az e-maileket.
  - Nem megfelelő hozzászólások esetén: Blokkold a felhasználót, jelentsd a hozzászólást, és kerüld a válaszadást.
  - Gyanús linkek esetén: Vigye az egérmutatót az URL fölé az ellenőrzéshez, ne kattintson rá, ha bizonytalan, és konzultáljon megbízható forrással.
- Eredmények megosztása: A csoportok összefoglalják elemzéseiket, és megosztják azokat az osztállyal. Emeljék ki a közös stratégiákat, és vitassák meg azok hatékonyságát.

4. A főbb pontok megerősítésével zárjuk a tevékenységet, összekapcsolva azt az online biztonsággal kapcsolatos, a későbbi lépésekben feltárandó tágabb stratégiákkal.

2. lépés: Figyelmeztető jelek és kockázatok felismerése (15 perc)

1. Mutassa be a résztvevőknek a kiberfenyegetések gyakori figyelmeztető jeleit világos példákon keresztül:

- Gyanús linkek vagy ismeretlen feladók: Ismeretlen személyektől érkező üzenetek linkekkel vagy mellékletekkel (pl. „www.freeprizes.xyz”).
- Helyesírási hibák vagy sürgős igények: Olyan üzenetek, mint például a „Fiókja blokkolva van! Aktiválja újra most”, gyakran rosszul megírva, hogy sürgőssé tegyék.
- Túl szép, hogy igaz legyen ajánlatok: Jutalmak vagy ajánlatok ígérete, például: „Nyertél egy ingyen iPhone-t!”

Vizuális elemeket is használhat, például adathalász kísérletekről készült képernyőképeket, és ösztönözheti a résztvevőket példák megosztására a jobb interakció érdekében.

2. Csoportos gyakorlat elvégzése. Ossza a résztvevőket kis csoportokra, és minden csoportnak adjon egy adott figyelmeztető jelet az elemzéshez (pl. sürgős üzenetek vagy gyanús linkek).

A következő lépéseket kell elvégezniük:

- Az üzenet elemzése: Beszéljék meg, mi teszi a fenyegetést meggyőzővé (pl. sürgősség vagy megtévesztés).
- Megoldási javaslatok: Keressenek válaszokat, például források ellenőrzése, gyanús linkek elkerülése vagy csalások jelentése.
- Foglalják össze az eredményeket: Készítsenek gyakorlati tippeket a kijelölt veszély elkerülésére.

3. A végén minden csoport bemutatja a meglátásait és stratégiáit. Foglalja össze ezeket egy bevált gyakorlatokat tartalmazó, összegzőlistában egy táblán vagy flipcharton. Befejezésül hangsúlyozza az óvatosság, az ellenőrzés és a kritikai gondolkodás fontosságát az online biztonság megőrzésében.

3. lépés: Megelőzési és mérséklési megközelítések (10 perc)

1. Kezdje azzal, hogy hangsúlyozza a személyes adatok védelme és az online kockázatok csökkentése érdekében tett proaktív lépések fontosságát. Mutasson be egy listát azokról az egyszerű intézkedésekről, amelyeket a résztvevők azonnal megtehetnek, például:
Erős, egyedi jelszavak használata és rendszeres frissítése.

- Többtényezős hitelesítés (MFA) engedélyezése kritikus fiókokhoz.
- A gyanús linkek és mellékletek elkerülése a forrásuk ellenőrzésével.
- A közösségi média és alkalmazások adatvédelmi beállításainak áttekintése.
- A szoftverek naprakészen tartása a biztonsági réseket orvosolni.
- Magyarázza el, hogyan csökkenthetik hatékonyan ezek az intézkedések a gyakori online kockázatokat.

2. Maradjon meg a korábbi csoportbontás, és adja át nekika teendők listáját. Kérje meg őket, hogy beszéljék meg és végezzék el a következő feladatokat:
Csoportos megbeszélés:

- Határozzátok meg, mely tevékenységeket gyakorolják már, és melyeket találnak kihívást jelentőnek.
- Vitassátok meg, hogy miért lehet bizonyos stratégiákat nehezebb megvalósítani, és ötleteljetek módszereket ezen kihívások leküzdésére.
- Válaszoljatok a legfontosabb kérdésekre:
- „Szerintetek melyik stratégia a leghatékonyabb az online biztonság megőrzésében?”
- „Hogyan emlékeztetheted magad arra, hogy jobb szokásokat alakíts ki, például rendszeresen ellenőrizd az adatvédelmi beállításaidat vagy kerüld a kockázatos linkeket?”

Új stratégiák megosztása:
Minden csoport kiválaszt egy új stratégiát, amelyet alkalmazni tervez, elmagyarázza, miért fontos, és megosztja a többiekkel.

3. lépés: Megelőzési és mérséklési megközelítések (10 perc)

3. A tevékenység zárásaként kérje meg a résztvevőket, hogy egyénileg gondolják át egy olyan szokásukat vagy eszközüket, amelynek azonnali használatára elkötelezik magukat online biztonságuk javítása érdekében. Kérje meg őket, hogy írják le egy post-it cetlire. Bátorítsa a résztvevőket, hogy gondolják át, hogyan oszthatják meg ezt a szokást barátaikkal, családjukkal vagy kollégáikkal, hogy közösen előmozdítsák a biztonságosabb online környezet kialakítását.

4. lépés: Reflexió és alkalmazás (5 perc)

1. Egyéni reflexió:
Kérdezd meg a tanulókat: „Milyen online szokást változtathatsz meg a biztonságod javítása érdekében?”

- A résztvevők post-it cetlikre írják fel válaszaikat.

2. Páros megbeszélés:

- Párosítssa a résztvevőket, hogy megosszátok a céljaikat, és javasoljatok megvalósítható lépéseke**t.**

3. Összefoglalás:

- Zárja egy motivációs gondolattal. Ez lehet például: „Az online viselkedésedben bekövetkező apró változások nagy különbséget jelenthetnek a saját és a közösséged biztonságában”.

Főbb tanulságok:

A résztvevőknek a foglalkozás után világos ismeretekkel kell rendelkezniük arról, hogyan azonosítsák a kiberfenyegetéseket és a nem megfelelő tartalmakat, például az adathalász kísérleteket, a manipulatív üzeneteket vagy a gyanús linkeket. Hangsúlyozza a gyakorlati biztonsági stratégiák fontosságát, mint például az erős jelszavak használata, a többtényezős hitelesítés engedélyezése és az adatvédelmi beállítások testreszabása a személyes adatok védelme érdekében.

Kérje meg a résztvevőket, hogy proaktív gondolkodásmódot tanúsítsanak a kritikai gondolkodás elősegítésével és az online kockázatokról folytatott nyílt beszélgetések fenntartásával. Erősítsék meg ezeket az elveket rendszeres gyakorlással és a tudás másokkal való megosztásával, hullámhatást keltve, amely biztonságosabb online szokásokat népszerűsít a közösségeikben.

Utánkövetés és otthoni tevékenységek:

- Kérje meg a résztvevőket, hogy:
- Tekintsék át a személyes közösségi média beállításaikat.
- Próbálják ki olyan tesztelőeszközök, mint például a Malwarebytes Browser Guard vagy a tartalomszűrők használatát.
- Osszák meg meg az egyik megtanult stratégiát egy barátoddal vagy családtagoddal.

Tippek tanároknak:

Keltse fel az érdeklődést valós példák és világos vizuális elemek használatával, amelyek elmagyarázzák az online kockázatokat és a gyakorlati biztonsági stratégiákat. Ösztönözze az interaktív beszélgetéseket, hogy a résztvevők könnyebben megértsék az anyagot. A gyakorlati tevékenységek, mint például a biztonsági útmutatók készítése, segítenek megszilárdítani a fogalmakat. Tartson fenn támogató és nyitott környezetet, ahol a kérdéseket szívesen fogadják, és hangsúlyozza a biztonságos online szokások hosszú távú előnyeit. Erősítse meg a kulcsfontosságú tanulságokat utólagos feladatokkal vagy csoportos reflexiókkal, hogy a résztvevők megőrizzék és alkalmazzák a tanultakat.

Eszközök

CyberWise

A CyberWise egy oktatási platform, amely eszközöket, forrásokat és útmutatókat kínál az egyének, különösen a szülők, az oktatók és a diákok online biztonságának megértéséhez. Modulokat kínál a kiberfenyegetések, például az adathalászat, a kiberzaklatás és a nem megfelelő tartalom felismeréséről, valamint stratégiákat kínál a kockázatok enyhítésére.

www.cyberwise.org

Malwarebytes böngészővédő

Ez egy ingyenes böngészőbővítmény, amely megvédi a felhasználókat az adathalászattól, átverésektől, rosszindulatú programoktól és a nem megfelelő tartalmaktól. Aktívan blokkolja a káros webhelyeket és hirdetéseket, így biztonságosabb böngészést biztosít minden felhasználó számára, nem csak a gyermekek számára.

www.malwarebytes.com

Hivatkozások

- CyberWise. (n.d.). Retrieved from https://www.cyberwise.org
- Dalby, J. (2021, January 15). How to Avoid Inappropriate Content. Gabb Now. Retrieved from https://gabb.com/blog/how-to-avoid-inappropriate-content
- Fadziso, T., Thaduri, U., Ballamudi, V., Desamsetti, H. (2023, September 25). Evolution of the Cyber Security Threat: An Overview of the Scale of Cyber Threat. Retrieved from https://figshare.com/ndownloader/files/42443952
- Lynch, M. (2024, April 5). 19 simple ways to block inappropriate content. The Tech Edvocate. Retrieved from https://www.thetechedvocate.org/19-simple-ways-to-block-inappropriate-content
- Mallick, R. (2024, February 21). Navigating the Cyber security Landscape: A Comprehensive Review of Cyber-Attacks, Emerging Trends, and Recent Developments. Retrieved from https://www.researchgate.net/publication/378343830
- Malwarebytes Browser Guard. (n.d.). Retrieved from https://www.malwarebytes.com/browserguard
- Roy, R. (2021, August 23). What Is a Cyber Threat? Definition, Types, Hunting, Best Practices, and Examples. Retrieved from https://www.spiceworks.com/it-security/vulnerability-management/articles/what-is-cyber-threat
- Singh, J. (n.d.). 10 Types of Cyber Security Threats and Solutions. Retrieved from https://cybersecuritykings.com/10-types-of-cyber-security-threats-and-solutions

KVÍZ

1. Mi az adathalász kísérlet legfontosabb jele?
A. Üzenet fogadása egy korábban ismeretlen, de ellenőrzött fióktól
B. Linkek, képek vagy mellékletek nélküli e-mail
C. Azonnali cselekvésre felszólító, gyakran nyelvtani hibákkal tarkított e-mail
D. Ismert feladótól érkező üzenet, amelyben rutinszerű információkat kérnek

2. Milyen viselkedés növelheti a kiberfenyegetések kockázatát?
A. Eszközök és alkalmazások rendszeres frissítése
B. E-mailekben található linkekre kattintás a feladó ellenőrzése nélkül
C. Kétfaktoros hitelesítés használata online fiókokhoz
D. A közösségi média adatvédelmi beállításainak havonta egyszeri ellenőrzése

3. Melyik szokás segít elkerülni a kiberfenyegetések áldozatává válást?
A. Jelszókezelő használata egyedi jelszavak létrehozásához és tárolásához
B. Minden engedély elfogadása alkalmazások telepítésekor a kényelem érdekében
C. Jelszavak megosztása megbízható barátokkal vagy családtagokkal, hogy legyen tartalékuk arra az esetre, ha elfelejtené őket
D. A böngésző biztonsági figyelmeztetéseinek figyelmen kívül hagyása

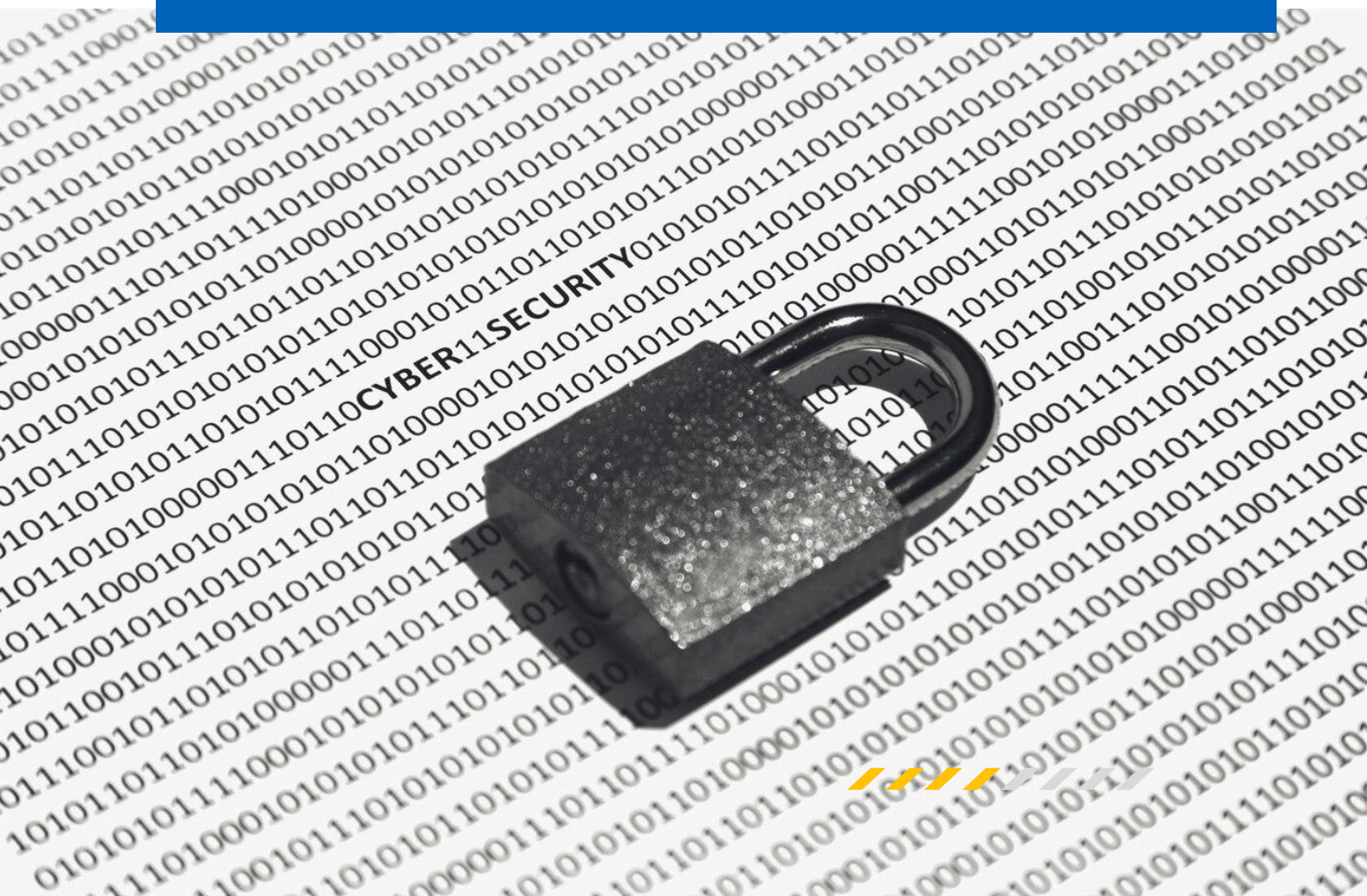
KVÍZ

4. Mitől gyanús és potenciálisan káros egy link?
A. HTTPS titkosítást használ
B. Átirányít egy másik webhelyre
C. Szokatlan karaktereket vagy domaineket tartalmaz
D. Egy barátja osztotta meg közvetlen üzenetben

5. Melyik stratégia a leghatékonyabb a nem megfelelő tartalomnak való kitettség megelőzésére?
A. Az online interakciók minimalizálása
B. Az összes értesítés kikapcsolása az eszközein
C. Kizárólag a víruskereső szoftverre hagyatkozás
D. Tartalomszűrők használata és az adatvédelmi beállítások módosítása

Megoldások

1. kérdés: C
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

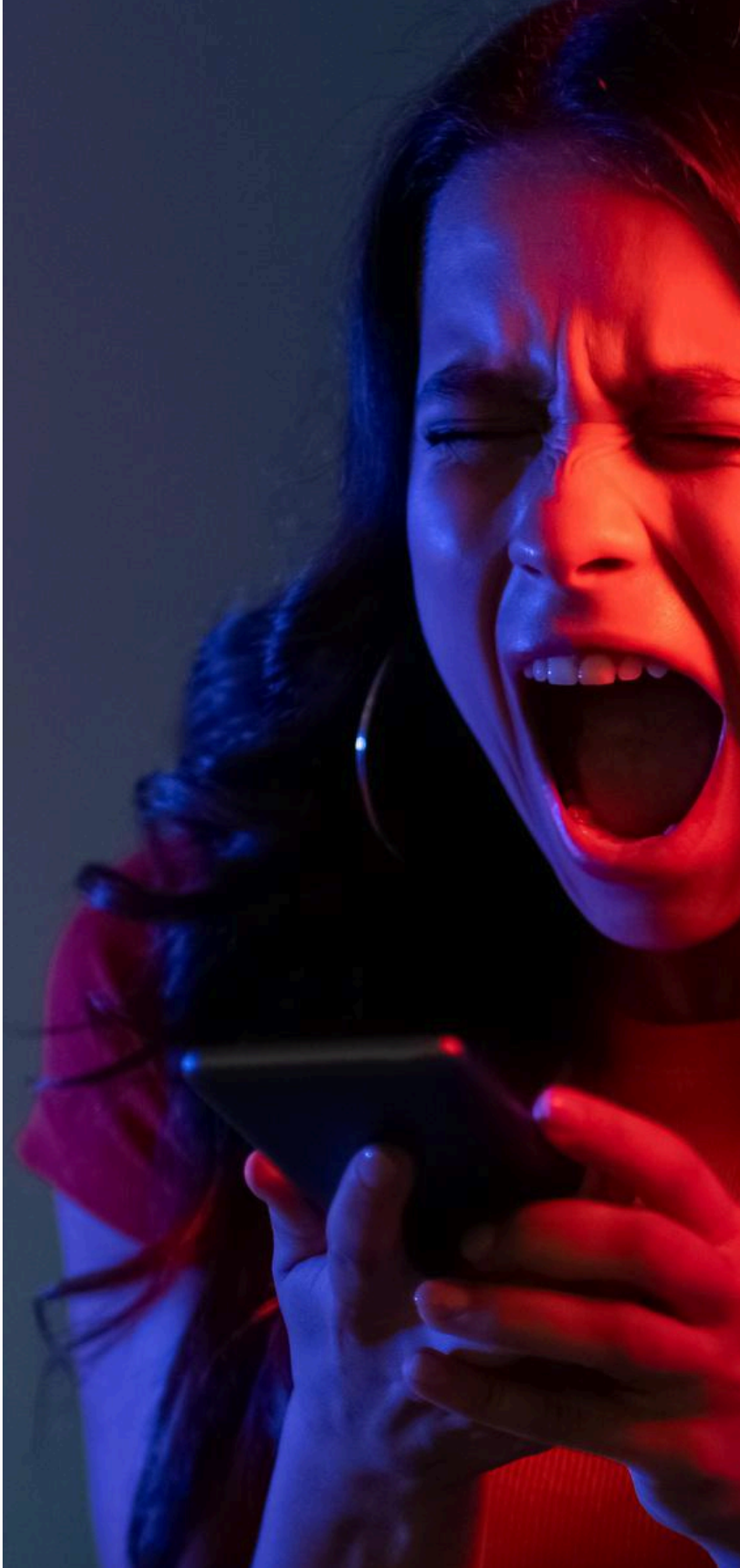
LABC

CWEP Centrum Wspierania Edukacji i Przedsiębiorczości

EDU yayıncılık

ASSERTED KNOWLEDGE THE ICT EQUALISERS

Inno Hub Valencia



Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.