



5. MODUL

KIBERBIZTONSÁG ÉS ONLINE BIZTONSÁG



erasmediah.eu



**Co-funded by
the European Union**



5.1 Tananyag

Bevezetés a kiberbiztonság alapjaiba



ERASMEDIAH

Educational Reinforcement Against
the Social Media Hyperconnectivity



**Co-funded by
the European Union**

5.1. lecke

Bevezetés a kiberbiztonság alapjaiba

Célok:

- A kiberbiztonság alapfogalmainak világos megértése, beleértve az olyan kulcsszavakat, mint a fenyegetések, sebezhetőségek és kockázatok.
- Az olyan elterjedt online fenyegetések azonosítása, mint az adathalászat, a rosszindulatú programok, a zsarolóvírusok és a szociális manipulációval kapcsolatos támadások, és azok hatásának megértése.
- A potenciális kiberbiztonsági incidensek azonosítására és kezelésére irányuló proaktív gondolkodásmód előmozdítása.

Fő üzenet(ek):

- Akár magánszemély, kisvállalkozás vagy globális vállalat vagy, az alapvető kiberbiztonsági gyakorlatok ismerete elengedhetetlen a digitális lábnyomod védelme érdekében.
- Az egyszerű megelőző lépések bevezetése jelentős időt, pénzt és stresszt takaríthat meg egy kibertámadás utáni helyreállításhoz képest.



ÓRA TÍPUSA:





Áttekintés

A mai digitális világban a kiberbiztonság alapjainak megértése már nem opcionális – hanem szükségszerűség. Ez a lecke bemutatja a kiberbiztonság alapelveit, a gyakori fenyegetéseket és az online biztonság fokozásának gyakorlati módjait. Együttesen felfedezzük, hogyan védhetjük meg a személyes és professzionális digitális eszközöket, elősegítve a kibertudatosság és -reziliencia kultúráját.

A workshop 4 lépésre tagolódik:

- 1: Bevezetés a kiberbiztonság alapjaiba (15 perc)
- 2: Gyakori kiberfenyegetések azonosítása (10 perc)
- 3: Kiberbiztonsági stratégiák a legjobb gyakorlatokhoz (10 perc)
- 4: Záró reflexió és a legfontosabb tanulságok (5 perc)



1. lépés

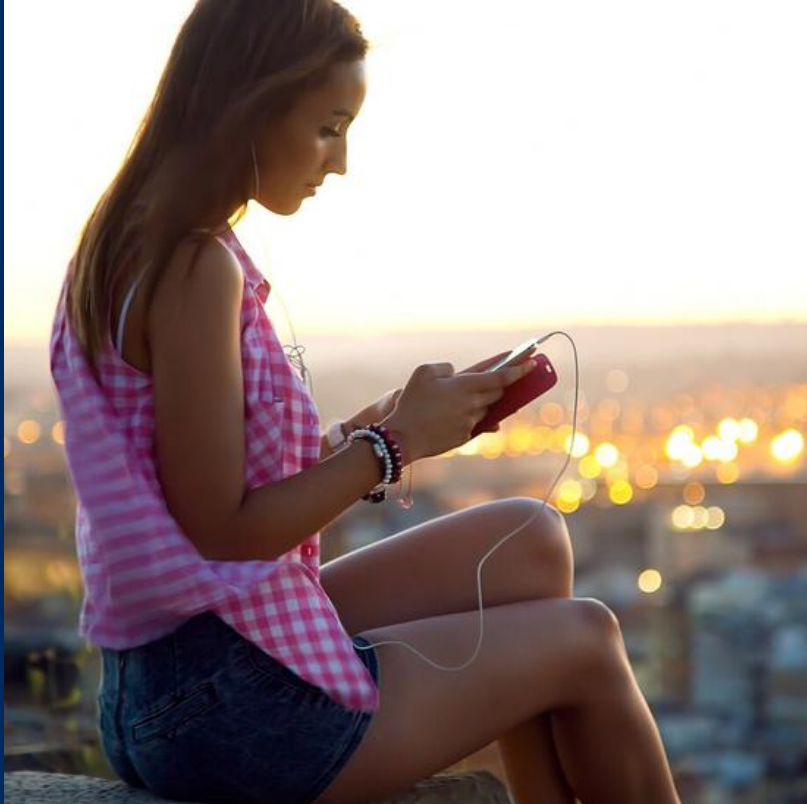
Bevezetés a kiberbiztonság alapjaiba

Kezdjük egy rövid videóval, amely bemutatja a kiberbiztonság fogalmát. Mindennapi életünkben folyamatosan használunk digitális eszközöket, de vajon milyen gyakran állunk meg, hogy elgondolkodjunk azok biztonságán? A kiberbiztonság elengedhetetlen ahhoz, hogy biztonságban tudjuk magunkat és személyes adatainkat a digitális világban. Ma belemerülünk a kiberbiztonság alapjaiba, és megvizsgáljuk, miért olyan fontos.

Nézzük meg együtt ezt a videót

Most, hogy megnéztük a videót, beszéljünk a következőkről:

- Mi tűnt fel neked a kiberbiztonsággal kapcsolatban a videóban?
- Miért gondolod, hogy a kiberbiztonság fontos a mindennapi életünkben?



1. lépés

Bevezetés a kiberbiztonság alapjaiba

A kiberbiztonság nem csak a rendszerek védelméről szól; a saját online viselkedésünk megértéséről is. A digitális eszközökkel való interakciónk módja vagy erősítheti a biztonságunkat, vagy sebezhetővé tehet minket a fenyegetésekkel szemben.

Itt az ideje, hogy egy pillanatra elgondolkodj a digitális életeden.

Írd le a válaszokat a következő kérdésekre:

- Milyen gyakran gondolsz az online tevékenységeid biztonságára?
- Tudsz azonosítani olyan szokásokat, amelyek veszélyeztethetik a személyes adataidat?

Készülj fel a gondolataid megosztására!



2. lépés

Gyakori kiberfenyegetések azonosítása

Nézzük meg közelebbről, hogy milyen típusú kiberfenyegetésekkel találkozhatunk.

Az internet egy hatalmas tér, tele lehetőségekkel, de kockázatokkal is jár. A kiberfenyegetések bárkit, bárhol célba vehetnek, ezért elengedhetetlen megérteni a természetüket és hatásukat. Ebben a lépésben megvizsgáljuk a különféle fenyegetéseket és azt, hogy azok hogyan befolyásolhatnak minket.

Olvasátok el a következő cikket: [Microsoft a kibervédelemről](#)

A cikk kiemeli:

- A különböző típusú kiberfenyegetéseket, beleértve az adathalászatot, a zsarolóvírusokat és a rosszindulatú programokat.
- Hogyan működnek ezek a fenyegetések, és kiket céloznak meg.
- Példákat a károkra, amiket okozhatnak.



2. lépés Gyakori kiberfenyegetések azonosítása

A cikk elolvasása után gondold át a következőket:

- Melyik típusú kiberfenyegetést találta a leginkább aggasztónak, és miért?
- Te vagy egy ismerős tapasztalta már ezeket a fenyegetéseket?
- Mit gondolsz, a fenyegetéseknek a megértése segíthet megelőzni őket?

Írj le egy valós példát vagy forgatókönyvet (lehet elképzelt is), ahol a cikkben említett kiberfenyegetések egyike előfordulhat. Készülj fel arra, hogy megoszd a példádat, és megvitasd a csoporttal!



3. lépés

Kiberbiztonsági stratégiák és legjobb gyakorlatok

Most pedig összpontosítsunk arra, hogyan védhetjük meg magunkat online.

Miközben a kiberfenyegetések folyamatosan fejlődnek, vannak egyszerű és hatékony lépések, amelyeket megtehetünk adataink védelme és a biztonság fenntartása érdekében. A kiberbiztonsági legjobb gyakorlatok alkalmazásával minimalizálhatjuk a kockázatokat és biztonságban maradhatunk digitális életünkben.

A kiberbiztonság nem igényel haladó technikai készségeket – apró, szándékos tettek is nagy különbséget jelenthetnek a saját és adataid védelmében.



3. lépés

Kiberbiztonsági stratégiák és legjobb gyakorlatok

ÍAlapvető biztonsági szabályok:

- Hozz létre erős, egyedi jelszavakat, és rendszeresen cseréld őket.
- Engedélyezd a többfaktoros hitelesítést (MFA) a fokozott biztonság érdekében.
- Legyen óvatos a linkekkel és mellékletekkel, különösen az ismeretlen forrásból származókkal.
- Tartsd naprakészen a szoftvereket és az eszközöket a sebezhetőségek javítása érdekében.
- Használj biztonságos Wi-Fi-kapcsolatokat, és lehetőség szerint kerüljd a nyilvános hálózatokat.

Feladat: Kiberbiztonsági ellenőrzőlista

1. lépés: Értékeld a jelenlegi szokásaidat

- Gondold át jelenlegi online viselkedésedet és szokásaidat. Vannak olyan területek, ahol veszélynek teheted ki magad?
- Példa: „Ugyanazt a jelszót használom több fiókban is”

2. lépés: Terv létrehozása

- Írj le egy megvalósítható lépést a fent felsorolt kulcsfogalmak mindegyikéhez. Például:
- Erős jelszavak: „Telepítek egy jelszókezelőt a biztonságos jelszavak generálásához és tárolásához” stb.



3. lépés

Kiberbiztonsági stratégiák és legjobb gyakorlatok

3. lépés: Csoportos megosztás

Oszd meg az egyik tervezett tevékenységedet egy partnereddel vagy a csoporttal.

- Beszéljétek meg, hogy ezek a lépések hogyan segíthetnek a digitális biztonságotok javításában.
- Adjatok tippeket vagy javaslatokat egymásnak további, a biztonságot növelő intézkedésekre

Záró reflexiós kérdés:

- Milyen szokást vagy stratégiát kezdhetsz el gyakorolni még ma, hogy azonnal javítsd az online biztonságodat?

4. lépés

Záró gondolatok és tanulságok

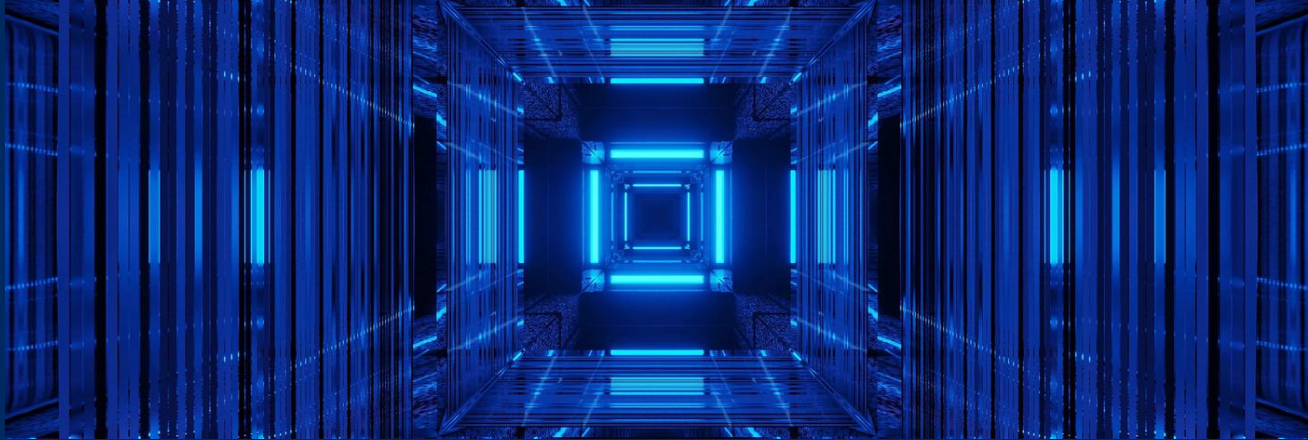
Befejezésül szánjunk egy percet arra, hogy átgondoljuk mindazt, amit ebben a leckében tanultunk, és azt, hogy hogyan tudjuk ezt a tudást a jövőben felhasználni.

Gondold át online szokásaidat – vannak-e olyan változtatások, amelyekre a mai beszélgetés után úgy érzed, hogy inspirációt szeretnél tenni? Ha igen, mi az első lépés, amit megteszel a kiberbiztonságod javítása érdekében?

Most pedig gondold át, hogyan segíthetünk másokon. Milyen egyszerű tippet vagy szokást osztanál meg ebből a workshopból egy barátoddal vagy kollégáddal, hogy segíts nekik biztonságban maradni az interneten?

Köszönöm mindenkinek az aktív részvételt és a mai hasznos hozzászólásokat!





Összefoglalás

- **A kiberbiztonság mindenkié.** A fenyegetések megértése és a legjobb gyakorlatok alkalmazása segít nekünk biztonságban maradni az interneten.
- **A kis lépések nagy különbséget jelentenek.** Az olyan eszközök, mint a jelszókezelők és a rendszeres frissítések, jelentősen növelhetik a biztonságot.
- **Maradj tájékozott.** A kiberfenyegetések folyamatosan fejlődnek, ezért a legújabb tippek és eszközök használata elengedhetetlen a hosszú távú biztonság érdekében.
- **Légy proaktív.** Minél több biztonságos szokást alakítasz ki, annál biztonságban leszel te – és a körülötted lévők is.



Útmutató tanárok és trénerek számára

Célkitűzés:

A lecke célja, hogy segítsen az oktatóknak és tanároknak felvértezni a fiatalokat alapvető kiberbiztonsági ismeretekkel. Izgalmas beszélgetések, tevékenységek és reflexiók révén a résztvevők megértik a gyakori kiberfenyegetéseket, elsajátítják az online biztonság legjobb gyakorlatait, és megvalósítható terveket készítenek a digitális világban való védekezésre.

Szükséges anyagok:

- Internetkapcsolat videólejátszáshoz vagy cikkek megtekintéséhez
- Projektor és vászon
- Hangszórók
- Hozzáférés az ajánlott kiberbiztonsági eszközökhöz
- Flipchart papír, táblafilcek
- Tollak vagy ceruzák
- Papírlapok





1. lépés: Bevezetés a kiberbiztonság alapjaiba (15 perc)

1. Kezdje egy ismerős példával a résztvevők bevonásával:

„Gondoljatok vissza, mikor használtatok utoljára egy új alkalmazást vagy látogattatok meg egy weboldalt. Elgondolkodtatok már azon, mennyire vannak biztonságban az adataitok?”

2. Emelje ki a kiberbiztonság jelentőségét: Magyarázza el, hogy a kiberbiztonság nem csak az informatikai szakemberek számára fontos; a mai digitális korban mindenki számára kritikus fontosságú készség. Hangsúlyozza, hogy a kiberbiztonság hogyan segít megvédeni a személyes, szakmai és szervezeti információkat.

3. Világosan vázolja fel a foglalkozás céljait.

4. Tevékenység: Videóvetítés és megbeszélés:

- Játssza le a kiberbiztonság alapjairól szóló videót ([nézze meg itt](#)).
- A megtekintés után tegyen fel irányító kérdéseket a résztvevőknek.

5. A videó után vezessen beszélgetést:

- „Mi lepett meg leginkább a kiberbiztonságban?”
- „Szerintetek a kiberbiztonság mindenkinek fontos? Miért, vagy miért nem?”
- „Milyen kockázatokkal jár, ha nem figyelünk oda az online biztonságra?”





1. lépés: Bevezetés a kiberbiztonság alapjaiba (15 perc)

6. Személyes reflexió: Kérje meg a résztvevőket, hogy szánjanak néhány percet gondolataik leírására:

- „Milyen gyakran gondolsz át online tevékenységeinek biztonságát?”
- „Meg tudsz nevezni egy vagy két olyan szokást, amely veszélyeztetheti a személyes adataidat?”
- „Mit gondolsz, milyen változtatásokkal javíthatnád online biztonságodat?”

7. A résztvevők kiscsoportban osszák meg gondolataikat:

- 1. lehetőség: Ossz meg egy olyan szokást, amelyet kockázatosnak tartasz, és kérj tanácsot a csoportodtól, hogyan lehetne javítani rajta.
- 2. lehetőség: Beszéljétek meg, hogy tapasztalatok-e vagy hallottatok-e már kiberfenyegetésről, és hogyan kezelték azt.

Ha a résztvevők nem szeretnék csoportokban megosztani a tapasztalataikat, engedje meg nekik, hogy leírjanak egy változtatást, amelynek megvalósítására vállalkoznak, és névtelenül nyújtsák be a csoportvezetőnek későbbi megbeszélés céljából.





2. lépés: Gyakori kiberfenyegetések azonosítása (10 perc)

1. Ossza meg a résztvevőkkel a Microsoft kiberbiztonsággal kapcsolatos összefoglaló cikkének [linkjét](#), vagy a szöveg nyomtatott változatát.

2. Adjon a résztvevőknek 5 percet, hogy elolvassák és feljegyezzék a leginkább aggasztónak talált veszélyeket, azok működésére és lehetséges hatására összpontosítva.

3. Megbeszélés:

Csoportos beszélgetés lebonyolítása:

- „Melyik kiberfenyegetést tartjátok a legaggasztóbbnak, és miért?”
- „Te vagy valamelyik ismerősöd tapasztalta már ezeket a fenyegetéseket? Mi történt?”

4. Szükség esetén egészítse ki a mondottakat

A beszélgetés gazdagítása érdekében emeljen ki statisztikákat vagy példákat, például adathalász e-maileket vagy zsarolóvírus-támadásokat. Ezekkel érdemes előre felkészülni.

5. Forgatókönyvek írása:

Kérje meg a résztvevőket, hogy írjanak egy rövid, valós vagy hipotetikus példát, amely egy kiberfenyegetéssel kapcsolatos, például:

- **Adathalászat:** „Egy család e-mail rávett valakit, hogy ossza meg a fiókbejelentkezési adatait”
- **Kártevő:** „Egy gyanús linkre kattintva vírust töltöttek le, ami zárolta a fájlokat”

6. Mutassák be a forgatókönyveket a csoportban, és vezessen beszélgetést a következőkről:

- „Mi romlott el a forgatókönyvben?”
- „Hogyan lehetett volna elkerülni a helyzetet?”
- „Milyen megelőző intézkedések segíthettek volna?”

7. Opcionálisan kiegészítheti a beszélgetést azzal, hogy kiemeli a valós megelőző stratégiákat az egyes fenyegetéstípusokra.





3. lépés: Kiberbiztonsági stratégiák a legjobb gyakorlatokhoz (10 perc)

1. A legjobb gyakorlatok áttekintése:

Mutasson be egyszerű, hatékony stratégiákat:

- Használj erős, egyedi jelszavakat.
- Többtenyezős hitelesítés (MFA) engedélyezése.
- Kerüld a gyanús linkeket és mellékleteket.
- Tartsd naprakészen a szoftvereket és az eszközöket.
- Használj biztonságos Wi-Fi-t vagy VPN-t.

Használjon valós példákat vagy rövid bemutatókat az egyes stratégiák hatásának bemutatására.

2. Biztonsági eszközök: Ha lehetséges, mutassa be vagy magyarázza el a Last Pass vagy a Bitfender alkalmazását (az Eszközök pontban, a 21. oldalon talál róluk információt)

3. Tevékenység: kiberbiztonsági ellenőrzőlista:

- Osszon ki egy egyszerű ellenőrzőlista-sablont, amelyen a felsorolt stratégiák szerepelnek.
- Kérje meg a résztvevőket, hogy írjanak le egy-egy megvalósítható lépést mindegyikhez. Példa: „Engedélyezni fogom az MFA-t az e-mailjeimben.”
- Ösztönözze a résztvevőket, hogy az egyszerű, azonnali cselekvésekre összpontosítsanak, és szükség esetén segíts tisztázni a lépéseket.

4. Csoportos megosztás:

- A résztvevők megosztanak egy-egy lépést, amit meg szeretnének tenni.
- Adjon gyors visszajelzést, és ösztönözze a párbeszédet a változások előnyeiről.
- Bátorítsa a résztvevőket, hogy rendszeresen nézzék át az ellenőrzőlistájukat szokásaik frissítése érdekében.





4. lépés: Záró reflexió és a legfontosabb tanulságok (5 perc)

1. A tanultak megerősítése és alkalmazása érdekében kérdezze meg a résztvevőket:

- „Milyen szokást tervezel ma megváltoztatni vagy elsajátítani?”
- „Hogyan fogod megosztani másokkal a tanultakat?”

2. Csoportos megosztás:

Kérjen meg önként jelentkezőket, hogy osszák meg gondolataikat vagy egy fontos tanulságot.

3. Záró üzenet:

Emlékeztesse a résztvevőket: „A kiberbiztonság mindenki felelőssége. Apró, tudatos lépések is nagy változást hozhatnak az online biztonság megőrzésében.”

Köszönöm mindenkinek az aktív részvételt, és buzdítom őket az azonnali cselekvésre.

Főbb tanulságok:

Hangsúlyozza a résztvevőknek, hogy a kiberbiztonság egy olyan készség, amelyre mindenkinek szüksége van, függetlenül a technikai szakértelmüktől. Használja a lecke főbb pontjait annak kiemelésére, hogy a gyakori fenyegetések megértése és a megelőző intézkedések, például az erős jelszavak használata vagy az MFA engedélyezése hogyan csökkenthetik drámaian az online kockázatokat. Ösztönözze a résztvevőket arra, hogy proaktív gondolkodásmódot tanúsítsanak egyszerű, elérhető célok kitűzésével online szokásaik javítása érdekében. Erősítse meg ezeket a tanulságokat további beszélgetések vagy tevékenységek révén, amelyek újra átgondolják ezeket a koncepciókat, biztosítva, hogy a résztvevők továbbra is éberek és motiváltak maradjanak az erős kiberbiztonsági gyakorlatok fenntartása érdekében.





Utánkövetés és otthoni tevékenységek

- Bátorítsa a résztvevőket, hogy gyakorolják a tanultakat online tevékenységeik nyomon követésével a következő héten.
- Azonosíthatják azokat a területeket, ahol a legsebezhetőbbnek érzik magukat, és minden nap egy új kiberbiztonsági stratégiát alkalmazhatnak.
- Ezenkívül javasold, hogy próbáljanak ki olyan eszközöket otthon, mint a LastPass vagy a Bitdefender, és osszák meg tapasztalataikat a csoporttal egy utólagos foglalkozáson.

Tippek tanároknak:

- **Integrálja a kiberbiztonsági témákat** a mindennapi beszélgetésekbe vagy órákba valós példák segítségével, amelyek kapcsolódnak a diákok tapasztalataihoz, például a közösségi média biztonságához vagy a gyakori csalásokhoz. Használjon interaktív módszereket, például csoportos beszélgetéseket vagy szerepjáték-forgatókönyveket, hogy a téma lebilincselő és gyakorlatias legyen.
- **Rendszeresen ellenőrizze a haladást, és nyújtson támogatást az erős kiberbiztonsági szokások kialakításának fontosságának megerősítéséhez.**





Eszközök

LastPass



A LastPass egy hatékony jelszókezelő eszköz, amelyet a kiberbiztonság fokozására terveztek azért, hogy erős, egyedi jelszavakat generál és biztonságosan tárol minden online fiókhoz. Kiküszöböli a több összetett jelszó megjegyzésének szükségességét azért, hogy egy titkosított digitális trezorban tárolja őket, amelyhez csak egy fő jelszóval lehet hozzáférni.

www.lastpass.com

Bitdefender



A Bitdefender egy fejlett kiberbiztonsági eszköz, amely átfogó védelmet nyújt a rosszindulatú programok, az adathalászat, a zsarolóvírusok és más online fenyegetések ellen. A robusztus víruskereső szoftvert intelligens adathalászat elleni intézkedésekkel ötvözi, így többrétegű biztonságot nyújt személyes és professzionális használatra.

www.bitdefender.com



Hivatkozások

- Bitdefender. (n.d.). Retrieved from <https://www.bitdefender.com>
- Cisco Networking Academy. (n.d.). Cybersecurity Essentials. Cisco Networking Academy: Learn Cybersecurity, Python & More. Retrieved from <https://www.netacad.com/courses/cybersecurity-essentials?courseLang=en-US>
- IBM. (2024, March 25). Types of cyberthreats. Retrieved from <https://www.ibm.com/think/topics/cyberthreats-types>
- 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>
- LastPass. (n.d.). Retrieved from <https://www.lastpass.com>
- Simplilearn. (2020, June 10). What Is Cyber Security | How It Works? | Cyber Security In 7 Minutes | Cyber Security | Simplilearn. [Video]. YouTube. <https://youtu.be/inWWhr5tnEA?si=3XP97c0H4JmHxWSo>





KVÍZ

1. Mi a kiberbiztonság egyik fő célja?

- A. Annak biztosítása, hogy senki ne férhessen hozzá engedély nélkül az internethez
- B. A vállalkozások számára a felhasználói tevékenységek megfigyelésének lehetővé tétele
- C. Digitális eszközök védelme a kockázatok és sebezhetőségek kezelésével
- D. Ismeretlen feladóktól érkező összes e-mail blokkolása

2. Az alábbiak közül melyik mutatja be a többtényezős hitelesítés (MFA) használatát?

- A. Bejelentkezés biztonsági kérdés megválaszolásával
- B. E-mail jelszó és egy biztonsági mentési e-mail cím használata a helyreállításhoz
- C. Jelszó kombinálása a telefonra küldött ideiglenes kóddal
- D. Jelszavak mentése titkosított fájlba a számítógépen

3. Miben különbözik az adathalászat más online fenyegetésektől?

- A. Felhasználói beavatkozás nélküli, közvetlen rendszerbe való betörést foglal magában.
- B. Megtévesztő taktikákat alkalmaz, hogy a felhasználókat bizalmas információk megosztására bírja.
- C. Fizikai eszközökön, például USB-meghajtókon keresztül terjed.
- D. Kizárólag úgy működik, hogy rosszindulatú programokat telepít a számítógépre





KVÍZ

4. Hogyan javítja a szoftverfrissítés a kiberbiztonságot?
- A. Javítja az alkalmazások tervezését és használhatóságát.
 - B. Csökkenti a feladatok végrehajtását zavaró hibák esélyét.
 - C. Bezárja a biztonsági réseket, amelyeket a támadók kihasználhatnak.
 - D. Jobb kompatibilitást tesz lehetővé a régebbi hardverekkel.
5. Miért előnyös jelszókezelőt használni?
- A. Biztosítja, hogy minden jelszava biztonsági mentésre kerüljön egy megosztott szerveren.
 - B. Automatikusan kijelentkezteti Önt egy beállított idő elteltével.
 - C. Komplex jelszavakat hoz létre és biztonságosan tárol minden fiókhoz.
 - D. Értesít, ha valaki engedély nélkül hozzáfér az e-mailjeidhez





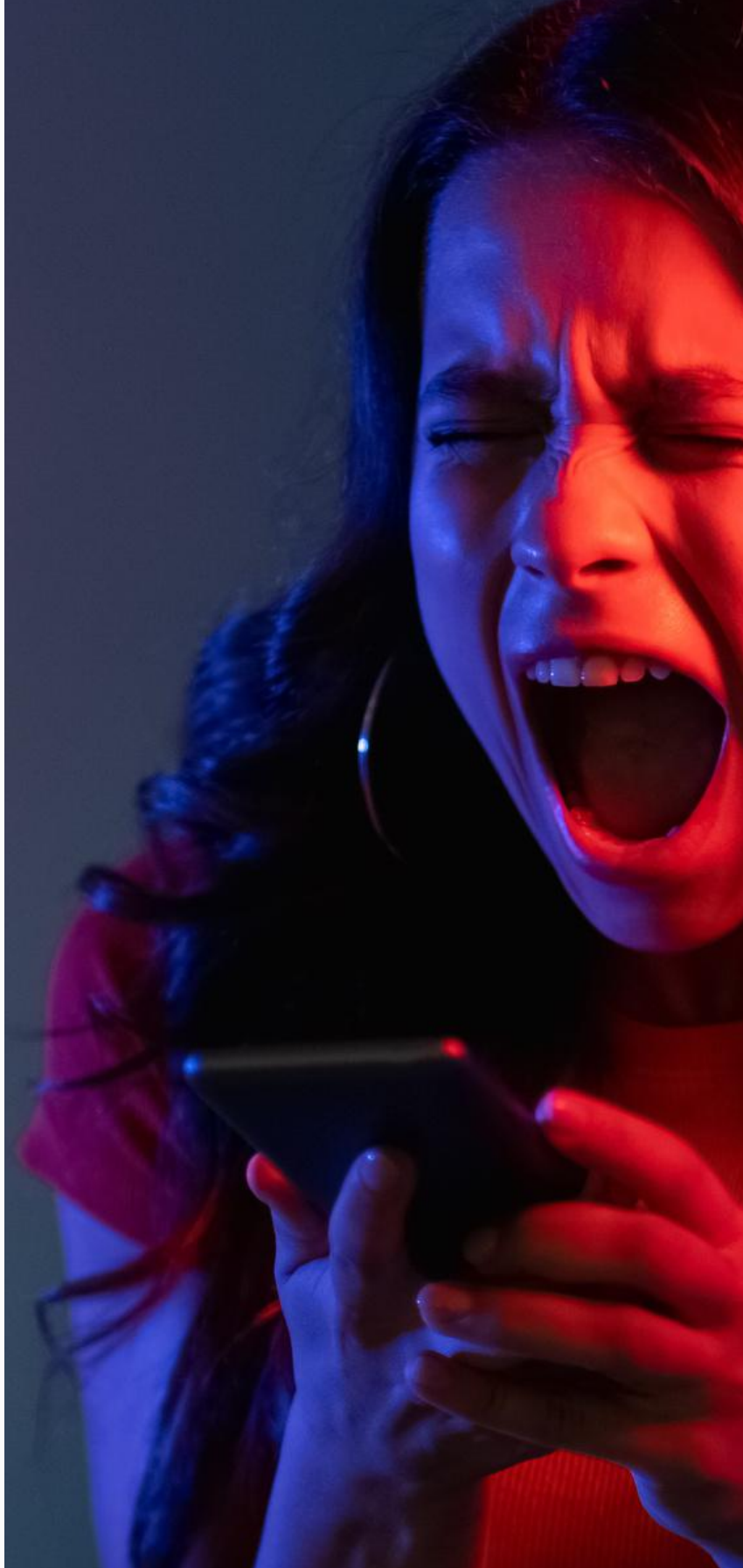
Megoldások

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





Centrum Wspierania
Edukacji
i Przedsiębiorczości



Co-funded by
the European Union