Tinédzserek és internetbiztonság: Gyakorlati útmutató tanároknak és szülőknek

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

Tartalom

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

Bevezető

Az európai polgárok jelentős része számára a kiberbiztonság máig ismeretlen kifejezés. A legfrissebb adatok szerint sokan közülük még a legalapvetőbb kiberbiztonsági előírások betartásának fontosságát sem ismerték fel (Erixon & Lamprecht, 2018; Pupillo, 2018). Becslések szerint például a szakemberek 50% -ának nincs jelszava, PIN-kódja vagy eszközeit védő biometrikus rendszere, 66,6% -uk pedig az adatok titkosításának hiányáról számolt be (Reischuk, 2019). Ebben az összefüggésben érthető, hogy az elmúlt évtizedben az Európai Unió (EU) a határozott megközelítés kidolgozása mellett döntött annak, hogy különböző szinteken megerősítse az internetbiztonságot.
A kiberbiztonság a következőképpen határozható meg: „a kibertér és a kibertér által támogatott rendszerek védelmére használt erőforrások, folyamatok és struktúrák szervezése és összegyűjtése olyan események ellen, amelyek de facto a tényleges tulajdonjogoktól eltérnek" (Craigen, Diakun-Thibault és Purse, 2014) . Konkrétabban, a Nemzetközi Távközlési Unió (ITU) szerint a kiberbiztonság magában foglalja az eszközök, irányelvek, biztonsági koncepciók, biztonsági biztosítékok, iránymutatások, kockázatkezelési megközelítések, cselekvések, képzés, bevált gyakorlatok, biztosíték és technológiák gyűjtését, amelyek felhasználhatók a számítógépes környezet, a szervezet és a felhasználó tulajdonának védelme érdekében (Von Solms & Van Niekerk, 2013).

Az Európai Kiberbiztonsági Ügynökség (ENISA, 2020) szerint a kibertámadások kifinomultabbá, célzottabbá, szélesebb körűvé és észrevétlenebbé válnak. A hivatal szerint az adathalászat, a személyazonosság-lopás és a ransomware száma növekedett, különösen a COVID-19 környezetben, amely táptalajként szolgált az otthonok, a vállalkozások, a kormányok és a kritikus infrastruktúra elleni támadásokhoz (Kohler, 2020; Sterlini, Massacci, Kadenko, Fiebig és van Eeten, 2019; Štitilis, Rotomskis, Laurinaitis, Nadvynychnyy és Khorunzhak, 2020). Ennek eredményeként a kibertámadásokkal járó gazdasági veszteségek elsöprőek a kormányok, ügynökségek és intézmények, vállalkozások és magánszemélyek számára, amely ki vannak téve a megnövekedett kiberfenyegetéseknek (Carrapico & Barrinha, 2018; Lis & Mendel, 2019). Becslések szerint a számítógépes bűnözés évente akár 575 milliárd dollárba is kerül a világgazdaságnak (Sobers, 2019). Az olyan zavarba ejtő technológiák elterjedése, mint például a tárgyak internete, amely manapság több mint 50 milliárd eszközt köt össze, hatalmas mértékben megnövelte a kibertámadás kockázatát (Lis & Mendel, 2019).
Ebben az összefüggésben észszerűnek tűnik megfontolni egy jelentős mértékű befektetést olyan gazdasági és emberi erőforrásokba, amelyek képesek kezelni ezt a helyzetet. Ugyanakkor kevés beavatkozás történik a rendelkezésre álló erőforrások és az emberi befektetés hiányának kezelése érdekében, amelyek enyhítenék ezt a fenyegetést. Becslések szerint 2021-re 3,5 millió betöltetlen kiberbiztonsági pozíció lesz (Ventures, 2017), ezért a szervezeteknek szembe kell nézniük azzal a kihívással, hogy kiberbiztonsági szakembereket és szakértőket toborozzanak egy olyan

munkaerőpiacra, ahol hiányoznak a piaci igények kielégítéséhez megfelelő képességekkel és képzettséggel rendelkező szakemberek (Crumpler & Lewis, 2019). Ezenkívül a kiberbiztonsági ágazatban dolgozó női szakemberek alacsony aránya is súlyosbíthatja a problémát. A legfrissebb adatok szerint az ágazatban foglalkoztatott nők aránya Európában 7% -ra becsülhető, ami messze elmarad attól, amit a jelenlegi piaci igények is megkövetelnek a nemek közötti egyenlőségről (Poster, 2018). A kiberbiztonsági szakmák nemek közötti szakadékának hátterében a nemi sztereotípiák, a diszkrimináció és az erősen férfias munkakörnyezet állhat. (Bagchi-Sen, Rao, Upadhyaya és Chai, 2010; Poster, 2018). A meglévő szakirodalom azt mutatja, hogy a nőknek számos akadálya van az ágazatba lépés és az előrelépés terén; társadalmi, intézményi és személyes kihívások (Bagchi-Sen et al., 2010). A férfiközpontú kultúra fontos szerepet játszik a nők számítástechnikai felsőoktatásban való részvételről szóló döntéseiben (Heaton & McWhinney, 1999). Eszerint a női hallgatók korlátozott segítségnyújtással és mentorálási lehetőségekkel rendelkeznek, és ez szintén döntő szerepet játszik az informatikai munkaerőpiacra való belépésük ösztönzésében (Ahuja, 2002; Parasuraman, Purohit, Godshalk és Beutell, 1996). Az iskolai végzettség, az érdeklődés és a képességek, valamint az informatikai tudás összetűzésbe kerülhet a női identitás különböző aspektusaival, negatívan befolyásolva a nő bizalmát abban, hogy képes lehet siker az ágazatban (Trauth, Quesenberry és Morgan, 2004). Ráadásul a szakmai és családi felelősség egyensúlya megteremtésének nehézsége jelentős akadályt jelent karrierjük előrehaladásában (Armstrong, Riemenschneider, Allen és Reid, 2007). Figyelembe véve, hogy a kiberbiztonság jövője attól függ, hogy képes-e vonzani és megtartani a nőket, prioritásnak kell tekinteni manapság a nők kiberbiztonságban való jelenlétének elősegítését (Poster, 2018). A nehézségek minimalizálása a pálya kezdeti szakaszában, az esélyegyenlőség biztosítása az informatikai karrier elérésében, a nők informatikai karrierjének előmozdítása, valamint a nők technikai és elemző készségei erősíthetik jelenlétüket az informatikai szektorban. Ezek járulhatnak hozzá, hogy több női példakép legyen előttük, akik erre a területre irányítják és ösztönzik a fiatal nőket. (Bagchi-Sen et al., 2010). A fentieket szem előtt tartva a Be@cyberPro egy olyan uniós projekt, amelynek célja a készségek és a nemek közötti különbségek áthidalása a kiberbiztonsági ágazatban képzés, a tanulók ösztönzése, a tanárok felhatalmazása és a szülők bevonása révén. A Be @cyberPro célja a nemek közötti különbségek kezelése a magánszektorba tartozó vállalatokkal és tudományos intézményekkel való együttműködéssel, valamint középiskolákkal és szakiskolákkal való közösen a kiberbiztonsági pályák népszerűsítése érdekében. A projekt elsődleges célcsoportjai a középiskolai tanulók és általában véve a formális szakképzésben résztvevő diákok, különösen a lányok, továbbá a tanárok és a családok. A kiberbiztonsági pályával kapcsolatos információk elérhetőbbé tétele a diákok, a tanárok és a szülők számára több fiatalt befolyásolhat pozitívan, hogy ezt a pályát válassza. Ezenkívül a pozitív női példaképekkel kapcsolatos információkhoz való hozzáférés segíthet arra ösztönözni fiatal lányokat, hogy kövessék a vágyaikat.

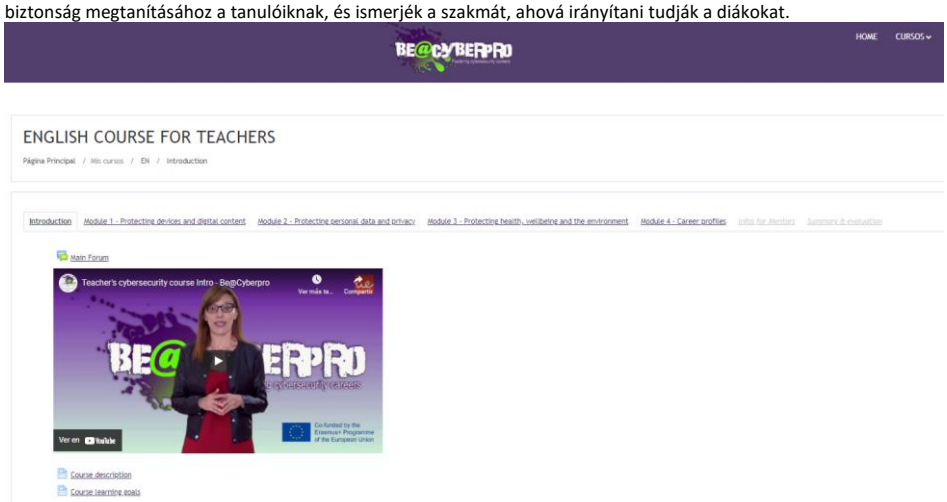
Ennek a könyvnek éppen ez a célja: a projekt legjelentősebb eredményeinek terjesztése a tanárok és a családok körében.

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

MOODLE E-LEARNING KERETRENDSZER

Elkészült egy online tanfolyam a Moodle e-learning rendszerben, amely a tanárok számítógépes biztonságát érintő alapvető tartalmakkal, annak érdekében, hogy a tanárok megfelelő ismeretekkel rendelkezzenek a számítógépes biztonság megtanításához a tanulóiknak, és ismerjék a szakmát, ahová irányítani tudják a diákokat.



1. ábra: Képernyőkép a tanároknak készült kiberbiztonsági tanfolyamból a Moodle platformon

A Moodle egy tanfolyam-kezelő rendszer (CMS), más néven Learning Management System (LMS) vagy virtuális tanulási környezet (VLE). Ez egy ingyenes internetes alkalmazás, amelyet az oktatók hatékony online tanulási platformok létrehozására használhatnak. Nagyon népszerűvé vált az oktatók körében szerte a világon, mivel olyan eszköz, amivel dinamikus weboldalakat hozhatnak létre online a diákjaik számára. A működéshez egy távoli webkiszolgálóra, az egyik saját számítógépre, akár egy webtárhely szolgáltató által üzemeltetett tárhelyre kell telepíteni.

- Egy Moodle projekt középpontjában mindig az áll, hogy a pedagógusoknak a legjobb eszközöket nyújtsa a tanulás irányításához és népszerűsítéséhez, de a Moodle használatának számos módja van: A Moodle olyan funkciókkal rendelkezik, amelyek lehetővé teszik, hogy nagyon nagy körben alkalmazzák és több százezer tanulóra terjedjen ki, illetve általános iskolában vagy tanulási hobbi céljára is használható. Sok intézmény platformként használja teljes online tanfolyamok lebonyolításához, míg mások egyszerűen arra használják, hogy a személyes tanfolyamok egy-egy részét színesebbé tegyék (vegyes oktatás).
- • Sok felhasználó szívesen használja az aktivitási modulokat (például fórumokat, adatbázisokat és wikiket), hogy több síkon együttműködő tanulási közösségeket építsen a téma köré (a szociális konstrukciós hagyomány szerint), míg mások inkább arra használják a Moodle-t, hogy eljuttassanak tartalmakat a tanulók számára (például szabványos SCORM csomagok), és feladatok vagy kvízek segítségével értékeljék a tanulást.

Project number: 2018-1-ES01-KA201-050461

DIDAKTIKAI PROGRAM: Kiberbiztonság a tanárok számára

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

Tartalom

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

Bemutatás

A Be @ CyberPro által készített didaktikai anyagot felhasználhatja az óráin a diákjaival való együttműködésre. A célja a digitális kompetenciájuk fejlesztése és mindenekelőtt a felelősségteljes és tájékozott magatartás kialakítása a kiberbiztonság alapelveivel összhangban. Ez a program lehetőséget kínál, hogy együtt dolgozzon a tanulókkal ezeknek az anyagoknak az alapján. Dolgozhat a teljes tartalommal, illetve kiválaszthat egyes modulokat is.

Ennek a programnak az ajánlott időbeosztása ajánlott időzítése 8 egy órás foglalkozás. 1-3 foglalkozással az egyes modulokhoz vagy tartalomrészekhez. A felnőttképzésben tanulók számára a csoportos korrepetáló foglalkozások tökéletes teret biztosíthatnak ezeknek a didaktikai javaslatoknak a megvalósításához abban az esetben, ha nem oktat kifejezetten a digitális technológiákra összpontosító tárgyakat, bár ezt a programot más tantárgyak esetén is használhatja.

Néhány gyakorlati tanács a kezdéshez

- A tanulókkal folytatott párbeszéd útján mutassa be az összes megvitatandó témát. Tegyen fel nyílt kérdéseket, amelyek lehetővé teszik számukra, hogy megosszák egymással tapasztalataikat és aggályaikat. Néhány egyéb forrás felhasználásával is bemutathat egy témát, például:
- Aktuális hírek
- Filmrészletek
- Az adott korcsoportnak szóló sorozatokból vett részletek
- Valódi esettanulmányi munkák, amelyek megfelelnek a tanulók igényeinek és érdeklődésének. Ne csináljon mindent egyedül. Hívjon meg kiberbiztonsági szakértőket, hogy a tanulók másoktól is hallhassák az igazságot.

Beszéljen őszintén, a kockázatok minimalizálása vagy enyhítése nélkül, de ne essen túlzásokba. A megelőzés az igazság megismerésével kezdődik.

Ösztönözze a tanulókat kritikus gondolkodásra az információk szembeállításával vagy olyan tevékenységekkel, amelyek során megoszthatják ötleteiket és véleményüket.

• Használjon többféle anyagot. Az általunk javasoltakon kívül továbbiakat találhat az online oktatási terekben, például a https://www.betterinternetforkids.eu/ linken. Európa-szerte működik a Biztonságos Internet központok (SIC) hálózata is, amely általában figyelemfelhívó központot, segélyvonalat, forródrótot és ifjúsági panelt tartalmaz.

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

1. modul - A digitális eszközök és tartalmak védelme

Tanulási célok
• A tanuló legyen képes megkülönböztetni a kockázatok és fenyegetések sokféleségét a digitális környezetben: hamis hírek, zsaroló levelek, adathalászat, spam, udvarlás, szexting, szerzői jogok megsértése stb. • • Tudja, hogyan alkalmazza a biztonsági és védelmi intézkedéseket, és ösztönözzön másokat (társaikat és diákjaikat) azok alkalmazására.

Kompetenciák a DigComp Framework alapján
4.1. Eszközök és digitális tartalomvédelem **Ismeretek:** • 1. Jelentős kockázatok és fenyegetések a digitális környezetekben. • 2. Fejlett védelmi intézkedések a digitális eszközök megóvására: víruskereső, tűzfal, spamszűrők, jelszavak, szoftverfrissítések használata. • 3. Személyes adatok. A védelem szintje az adatok jellege szerint. **Készségek:** • 13. Különböző módszereket tudok alkalmazni az eszközök és a digitális tartalom védelmére, és másokat is erre tudok ösztönözni. • 14. Sokféle kockázatot és fenyegetést tudok megkülönböztetni a digitális környezetben: hamis hírek, zsarolóvírus, adathalászat, spam, ápolás, szexting, szerzői jogok megsértése, ipari kémkedés stb. • 15. Tudom, hogyan kell alkalmazni a biztonsági és védelmi intézkedéseket. • 16. Különböző módszereket alkalmazok a megbízhatóság és az adatvédelem fenntartására.

Tartalom[1]:

1.1. Digitális eszközök védelme

1.2. Kockázatok és fenyegetések a digitális környezetben

1.3. A digitális tartalom védelme

[1] Valamennyi tartalom elérhető a project weboldalán: https://www.beacyberpro.eu/

1.4. A technológia felelős használata

1. foglalkozás Bevezető. Előzetes ismeretek.
• Bevezető beszélgetés." Mik azok az előnyök és kockázatok, amiket már ismerünk, ha okostelefon használunk". • Kérdőív az eszközhasználati szokások megállapítására. • • Ötletgyűjtés a szakszavak válogatására: álhírek, zsarolóvírus, adathalászat, spam, ápolás, szexting, szerzői jogok megsértése, ipari kémkedés stb. • • Problémás helyzetek azonosítása együttműködő csoportokban. Mi a probléma? Mit gondolsz, hogyan lehet megoldani? • A problémás helyzetek megoldása az egész osztály közreműködésével. - Belép az iskola / IES webhelyére, és kap egy üzenetet, amelyben arra kérik, hogy telepítsen egy frissítést a tanári kommunikációs alkalmazáshoz. Ez egy rosszindulatú program. Két hónapja beszélget valakivel az Instagramon, aki nagyon kedves, és arra kéri, hogy találkozzon vele személyesen, de amikor megérkezik a találkozó helyére, nem azt találja, akinek mondta magát. - Kapott egy SMS-t, amelyben megkérték, hogy lépjen be az iskolai fiókjába és adja meg a jelszót, de ezt az üzenetet nem az iskola küldte.
2. foglalkozás **Sextortion[2] - zsarolás intim felvételekkel**
• "A Ceruzákat középre" egy láncjáték, ami nagyon hasznos módja az ismereteket beépítésének, mivel így a diákok egymással kölcsönhatásban veszik át a tanultakat. A 4 fős csapatokban felváltva felolvasnak néhány kérdést, és szóban válaszolnak rájuk. Amikor beszélniük kell, ceruzáikat vagy íróeszközeiket az asztal közepére teszik. Nem írhatnak és nem használhatják a jegyzeteiket ez alatt az idő alatt. Miután befejezték a beszélgetést, és már mindenki tudja, mit kell tennie, itt az ideje, hogy elővegyék az író eszközeiket és elkezdjenek írni. Amikor eljött az írás ideje, nem beszélhetnek az osztálytársaikkal. • A „Ceruzákat középre" csoportok 4 főből állnak, és 4 kérdést kapnak az előző foglalkozás tartalmából. • A munka megkezdéséhez minden tanulónak az asztal közepén kell hagynia ceruzáját / számítógépét; ez azt jelenti a diákok számára, hogy ideje beszélgetni az osztálytársaikkal. Először az 1. tevékenységért felelős személy felolvassa a kérdést vagy a feladatot a csoportjának. Együtt megbeszélik és döntenek a feladat megoldásának legjobb módjáról... Miután ebben megegyeztek, minden diák elveszi a saját ceruzáját / eszközét (jelezve, hogy most csendben marad), és egyenként leírja a csoport által kidolgozott megoldást.

[2] This topic may not be considered as adequate for the curricula of all countries. Please, confer with the school board or a sex educator before addressing it

Miután mindenki befejezte a válaszok leírását, visszateszik a ceruzát / eszközt középre. Ezután a második feladatért felelős személy ismerteti a következő feladatot, megismételve ugyanazt a folyamatot, amíg mindegyiken végig nem mennek.

- A Skam sorozat epizódjának megtekintése (szexzsarolásos eset).
- Sajtóhírek keresése a sajtóban hasonló esetekről.
- Töltsön ki egy ki egy „Döntési fa" sablont egy lehetséges esetről: "Ha egy ismeretlen személy flörtölni próbál veled a közösségi hálózatokon..."

3. foglalkozás

Álhírek

- Indító beszélgetés: Mit tudunk az álhírekről? Osszunk meg olyanokat, amiket ismerünk. Előre gyűjtsünk össze néhány frissebb példát.
- Útmutató az álhírek kiszűréséhez.
- Csoportos tevékenység: "Az igazság őrzői". Több hírt megmutatunk, és a tanulóknak az információk szembeállításával fel kell ismerniük, melyik igaz, és melyik hamis. Itt is követhető A "Ceruzákat középre" kooperatív tevékenység dinamikája.

2. modul – A személyes adatok és a magánszféra védelme

Tanulási célok

- • Alkalmazzon különböző stratégiákat a digitális technológiák használatából eredő fizikai és pszichológiai kockázatok megelőzésére, és ösztönözzön másokat (tanár társait és tanulókat) ezek alkalmazására.
- Legyen képes megkülönböztetni a digitális technológiák használatából fakadó nemkívánatos környezeti hatások széles körét, és gondolkodjon el arról, hogyan lehet ezt a hatást minimalizálni.
- Segítsen másoknak (tanár társainak és diákjainak) a befogadás és / vagy a jólét fejlesztése szempontjából hasznos technológiai erőforrások alkalmazásában.

Kompetenciák a DigComp Framework alapján

Digitális identitás kezelése

Készségek:

• S1. A különböző digitális identitások kritikus használata, az egyes kontextusokban vagy helyzetekben a legmegfelelőbb kiválasztása. • S2. Digitális identitásomat megválasztom és kezelem az általam készített dokumentumokban és adatokban. • • S3. Különböző módszereket használok digitális identitásom védelmére és annak ellenőrzésére, hogy megfelelően működnek-e.
4.2. A személyes adatok és a magánszféra megóvása a digitális környezetben **Ismeretek:** • 1. A személyes adatok vagy információk helytelen védelméből eredő kockázatok. • 2. Egyszerű eszközök és módszerek a személyes adatok és információk védelméhez. • 3. Az adatvédelmi irányelvek alapvető szempontjai és tényei. • 4 A személyes adatok és tartalomvédelem eszközei és stratégiái (középszint). • 5 Technológiai erőforrások az adatvédelemhez. **Készségek:** • K13. Különböző módszereket és eszközöket használok és alkalmazok adataim védelmére, és szükség esetén képes vagyok segíteni másoknak. • K14. Korlátozom a másokkal megosztott információkat és adatokat; Ellenőrzem az adatok és információk nyilvános megjelenését, és szükség esetén segítek másoknak. • K15. Tisztában vagyok az általam használt szolgáltatások adatvédelmi irányelveinek különbségeivel, és az érdekeimnek leginkább megfelelő szolgáltatást választom, vállalva és felügyelve annak kockázatait. • K16. Segítek tanítványaimnak abban, hogyan védhetik meg digitális identitásukat és kezelhetik digitális lábnyomukat.

Tartalom[3]:

2.1. lecke	A személyes adatok és a személyes információ védelme
2.2. lecke	Az információ és a személyes adatok és adatok online védelmére szolgáló eszközök és módszerek
2.3. lecke	Az információ és a személyes adatok és adatok offline védelmére szolgáló eszközök és módszerek
2.4. lecke	A magánszféra védelmének irányelvei és a digitális fair play

[3] Minden tartalom elérhető a projekt weboldalán: https://www.beacyberpro.eu/

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

1. foglalkozás Bevezető. Előzetes ismeretek
• Indító beszélgetés: Tudjuk, hogy milyen személyes adatok nem oszthatók meg engedély nélkül? Hogyan védhetjük meg a személyes adatainkat? • Megoldunk néhány problémás helyzetet, kooperatív csoportokban. Kövesse a „Ceruzákat középre” kooperatív tevékenység menetét! - Valaki lefényképezi, hogy elesel az utcán, és a barátaid fel akarják tölteni a Tik Tok-ra. - Egy barátod a nyárról a tengerparton készített képeket tett közzé az Instagramon, és te bikiniben vagy. - Egy személy elkezdett követni téged az Instagramon, és megjegyzéseket fűz a fotóidhoz, azt állítva, hogy ismer, de nem tudod, kicsoda. • Áttekintjük a közösen használt közösségi hálózatok adatvédelmi irányelveit. Hogy épülnek fel? Mi lenne a legbiztonságosabb módszer? Mit jelent ez?
2. foglalkozás **Az adataim és én**
• "Fejösszedugás” - csoportos tevékenység az előző foglalkozáson tanultak felidézésére. 1. Négytagú csoportok jönnek létre és számokat kapnak. 2. A tanár feltesz egy kérdést, és a diákok egyenként gondolkodnak a válaszon: Hogyan akadályozhatod meg barátaidat abban, hogy olyan információkat osszanak meg, amelyeket nem szeretnél közzétenni? 3. Mindegyik csoportban csoportos beszélgetést tartanak, "összedugják a fejüket". (Innen ered a tevékenység neve). 4. Néhány perc múlva a tanár 1-től 4-ig választ egy számot, és az ennek megfelelő tanuló a csapata nevében válaszol a kérdésre. • Íme néhány eszköz és módszer az információ online és offline védelméhez: # 1 Tűzfal # 2 Antivírus szoftver # 3 Hozzon létre erős jelszavakat # 4 Ne ossz meg mindent a közösségi médiában Egészítsd ki a „Döntési fát” és " Gondolkodj el azon, amit megosztasz. ".

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

3. modul – Az egészség, a jóllét és a környezet védelme

Tanulási célok
• Tiszteletben tartani az általam a tanulók körében megosztott és a virtuális tanulási környezetekben beágyazott forrásanyagok szerzői jogait, licenszeit és használati korlátozásait. • Lépéseket tenni a digitálisan megosztott bizalmas adatok és információk védelmére, és ösztönözni a tanulókat, hogy tegyék ugyanezt a dolgozataikkal.

Kompetenciák a DigComp Framework alapján
4.3.1. A digitális technológiák etikus és egészséges használata **Ismeretek** • Ismeri a technológiák hosszan tartó alkalmazásának hatását • Ismeri a technológiák addiktív aspektusait • Ismeri a számítógépek és az elektronikus eszközök környezeti hatásait, és azt, hogy miként tudja ezeket mérsékelni egyes alkatrészek újrahasznosításával • Meg tudja határozni, hogy rendelkezésre állnak-e megfelelő és biztonságos digitális eszközök, amelyek hatékonyak és költséghatékonyak más eszközökhöz képest **Készségek:** • K11. Különböző stratégiákat tudok alkalmazni a digitális technológiák használatából eredő fizikai és pszichológiai kockázatok megelőzésére, és másokat is el tud igazítani azok alkalmazásában. • K12. Képes vagyok felismerni a digitális technológiák használatából fakadó nem kívánt környezeti hatások széles körét, és át tudom gondolni, hogyan lehet ezeket minimalizálni. • K13. Másokat is tudok ösztönözni a társadalmi befogadás és / vagy a jólét fejlesztése szempontjából hasznos technológiai források felhasználására.
4.4. A környezet védelme **Készségek:** • K14. Különböző módokat tudok mutatni arra, hogyan lehet a környezetet megóvni a digitális technológiákból és azok használatából eredő hatásoktól.

Tartalom[4]:

[4] Minden tartalom elérhető a projekt weboldalán: https://www.beacyberpro.eu/

3.1. lecke A fizikai egészség védelme a technológia használata közben

3.2. lecke A pszichológiai jólét védelme a digitális környezetben

3.3. lecke Digitális technológiák a társadalmi jólét és a beilleszkedés támogatására

3.4. lecke A környezet megóvása

3.5. lecke Az internetbiztonság európai és országonkénti jogi szabályozása

1. foglalkozás
• Indító beszélgetés: Technológia és egészség: Befolyásolja-e a technológiai eszközök használata a testi és lelki egészséget? A meglévő ismeretek feltérképezése és tanácsadás zajlik. • Felmérés a technológia használatával és az egészséggel kapcsolatos szokásaikról. • Csoportos dramatizálási gyakorlat a fizikai egészséget és / vagy a pszichés jólétet javító vagy romboló magatartás bemutatására a technológia használatával (gyenge ergonómia, rossz megvilágítás, valakinek a mellőzése stb.) kapcsolatban. • Csoportos tevékenység: „Forgó papír” a munkamenet során tanultak összefoglalására. • A tanár felkéri a csapatokat, hogy végezzenek el egy tevékenységet (összegezzenek, írjanak esszét, készítsenek listát stb.). Először minden csapatból kijelölnek egy tanulót, aki a papírlapra leír valamit, ami aztán az összes csapattárs között végigmegy. Amíg az egyik tanuló ír, a többieknek figyelniük kell arra, amit ír, segíteniük kell, tanácsot kell adniuk és motiválniuk kell őket. Miután valaki befejezte a saját részét, átadja a papírlapot a következő csapattársnak, és ugyanaz a művelet megismétlődik, amíg a csapat összes tagja nem végzett.

4. modul - Karrierleírások

Tanulási célok
• Kommunikáljon a tanulókkal a digitális technológiák iránti pozitív hozzáállással, tudatosítva bennük a lehetséges kockázatokat és korlátokat, ugyanakkor bizalmat keltve abban, hogy képesek lesznek kezelni ezeket a technológiák előnyeinek kiaknázása érdekében, és ösztönözve őket ezek kreatív használatára és kritikus értékelésre. • Dolgozzon ki pedagógiai stratégiákat a digitális eszközök és a tanulók által közzétett digitális tartalom nem biztonságos használatának megelőzésére, azonosítására és kezelésére. • Dolgozzon ki stratégiákat annak elősegítésére, hogy a tanulók megvédjék személyes adataikat és digitális identitásukat a digitális környezetben. • A digitális technológiák segítségével dolgozzon ki stratégiákat annak a tanulói magatartásnak a megelőzésére, felismerésére, amelyek negatívan befolyásolják egészségüket és jólétüket.

Tartalom[5]:

4.1.lecke Karrierleírások

1. foglalkozás
• Indító beszélgetés: Ismersz-e valakit, aki a kiberbiztonsági szektorban dolgozik? • Szakemberekkel készített interjúk e-book bemutatása. • Beszélgetés a bemutatott könyvről. Mi volt a legmeglepőbb? • Egyéni tevékenység: "Ha a kiberbiztonságban dolgoznék, szeretnék ..." és „mit kérdeznél valakitől, aki kiberbiztonságban dolgozik”?
2. foglalkozás
• Női kiberbiztonsági szakértők felkeresése (személyes vagy szinkron online). Meséljenek a tapasztalataikról! • Kezdeményezünk vitát az előző foglalkozás egyéni tevékenysége és a vendégek előadása során felmerült kérdések alapján. • Közös prezentációt készítünk a modul következtetéseinek levonására.

[5] Minden tartalom elérhető a projekt weboldalán: https://www.beacyberpro.eu/

KIBERVÉDELEM SZÜLŐKNEK

Útmutató bevált gyakorlatokhoz

Commented [EJG2]: include images, photos in the ebook

Project number: 2018-1-ES01-KA201-050461

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

Bemutatás

Ennek az útmutatónak az a célja, hogy segítse a szülőket abban, hogy gyermekeik megértsék a kibervédelem alapelveit az online biztonság érdekében, valamint abban, hogy tájékozottak legyenek a felelősségteljes online magatartás kialakításában.

Együtt jobban:

- élvezhetik az internetet
- megelőzhetik a kockázatokat
- észrevehetik a problémákat és azokat kezelhetik.

Néhány gyakorlati tippet adunk a szülői közvetítéshez abban, hogy gyermekeik online-biztonságát elősegítsék.

Néhány gyakorlati tanács mielőtt hozzáfogna

Folytasson nyílt és ítéletmentes párbeszédet gyermekeivel. Tegyen fel olyan nyílt kérdéseket, amelyek lehetővé teszik számukra tapasztalataik és aggályaik megosztását. Nem lesz mindig könnyű, és nem is lesznek mindig fogékonyak a párbeszédre. Találjon időt arra, hogy a beszélgetés szabadon folyjon.

Használhat néhány más forrást a beszélgetés indításához, például:

- aktuális híreket
- filmrészleteket
- korosztályuknak szóló tévéműsorból vagy sorozatból való részleteket

Nem kell mindent saját magának csinálnia. Ha úgy érzi, hogy gyermekének valamilyen problémája lenne, konzultáljon iskolai oktatójával, hogy közösen megbeszélt terv alapján tudjon cselekedni.

Őszintén beszéljen a gyermekével, anélkül, hogy elbagatellizálná vagy enyhítené a veszélyeket, ugyanakkor ne nagyítsa fel azokat. A megelőzés a tudással kezdődik.

Segítse elő kritikus gondolkodásukat úgy, hogy információkat állítson szembe vagy olyan feladatot végezzenek, amelyben megoszthatják az ötleteiket és véleményüket

Igazodjon a gyermek értelmi és érettségi szintjéhez.

Itt találhat néhány gyakorlati tippet ahhoz, hogy hogyan foglalkozzon a különféle online-biztonsági ügyekkel.

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

1. A digitális eszközök és tartalmak védelme

Célkitűzések

- Alakítson ki egy pozitív hozzáállást a digitális eszközökhöz. Hívja fel a figyelmet a lehetséges kockázatokra és korlátokra, ugyanakkor teremtsen bizalmat annak kezelésében, hogyan használhassa ki a technológia előnyeit. Ösztönözze a biztonságos és felelősségteljes kreatív felhasználást.
- Legyen képes a digitális környezetben lévő kockázatok és veszélyek sokféleségének megkülönböztetésére, például: álhírek, gyermekek megkörnyékezése, szexting, szülői túlposztolás (sharenting) stb. (Lásd az útmutató végén található Fontosabb kifejezések), és arra is, hogy hogyan lehet ezek ellen védekezni.
- Ismerje meg, hogyan alkalmazza a biztonsági és védelmi intézkedéseket, és irányítsa a gyermekét azok alkalmazására.

Mit tehet Ön?

BIZALOM

- Be Legyen óvatos azzal, ahogyan reagál, ha a gyerekei azt mondják, hogy problémájuk van. Ez nem a hibáztatás ideje, hanem a közös megoldásé.

SEGÍTSÉGNYÚJTÁS

- Irányítsa gyermekét a technika megfelelő használatában. Megállapodhatnak néhány felelősségteljes használatra vonatkozó irányelvben, vagy akár írhatnak egy „szerződést”, amelyet látható helyre tesznek ki otthon.
- Legyen követendő példa.
- Osszanak meg együtt online tevékenységeket. Ez nem azt jelenti, hogy betolakodunk az online térbe, és lájkolunk mindent, amit közzétesznek, hanem inkább azt, hogy együtt töltik az időt online kereséssel.

FELÜGYELET

- Legyen naprakész gyermeke online jelenlétével: melyek azok az alkalmazások, amelyeket a legjobban használnak, és melyek azok a közösségi hálózatok, amelyeken profiljuk van.
- Igénybe veheti az olyan szülői felügyeleti alkalmazásokat, mint pl. a Qustodio, a SecureKids vagy a Parental Click, a nembiztonságos webhelyekhez való hozzáférés korlátozásához.
- Tartsa rajta a szemét a nem megfelelő tartalmakon: az olyan tartalmakon, amelyek kockázatos vagy negatív viselkedésre ösztönöznek, vagy az olyanokon, amelyek nem megfelelőek a gyermek korához képest.

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

2. A személyi adatok és a magánszféra védelme

Célkitűzések

- Alkalmazzon különböző stratégiákat a digitális technológiák használatából eredő fizikai és pszichológiai kockázatok megelőzésére, és irányítsa a gyermekeket azok alkalmazására.
- Legyen képes megkülönböztetni a digitális technológiák használatából fakadó nem kívánt környezeti hatások széles körét, és gondolja át, hogyan lehet ezt a hatást minimalizálni.
- Mutasson utat az integráció és/vagy a jóllét fejlesztéséhez hasznos technológiai erőforrások felhasználásához.

Mit tehet Ön?

BIZALOM

- Teremtsen olyan légkört, amelyben nyugodtan tud beszélni az Ön jelenlétéről az interneten, a kapott és a megosztott információkról.

SEGÍTSÉGNYÚJTÁS

- Készítsenek együtt erős jelszavakat az eszközök védelme érdekében.
- Tekintsék át együtt a hálózati eszközök és szolgáltatások konfigurációs lehetőségeit, és legyenek óvatosak azzal, hogy milyen információt osztanak meg.
- Legyen követendő példa.

FELÜGYELET

- A PEGI magatartási kódex életkor szerint osztályozza az alkalmazásokat. Tekintse át azokat az alkalmazásokat, amelyekhez a gyermekek hozzáférhetnek, hogy elkerüljék a nem megfelelőek használatát.
- Ha az alkalmazás korlátozott felhasználóval rendelkezik (lépjen a Speciális beállítások> Felhasználók vagy Fiókok menüpontba, és kövesse a lépéseket), korlátozza azokat az alkalmazásokat vagy fájlokat, amelyekhez a gyermekek hozzáférnek, s ha szükséges, akkor szülői felügyelet alkalmazásával.

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

3. Az egészség, jóllét és környezet védelme

Célkitűzések

- Dolgozzon ki stratégiákat a gyermekek egészségét és jóllétét negatívan befolyásoló magatartások megelőzésére, azonosítására és azokra való reagálásra a digitális technológiák segítségével.

Mit tehet Ön?

BIZALOM

- Beszéljen nyíltan a technológia nem megfelelő használatának az egészségre, a jólétre vagy a környezetre gyakorolt káros hatásairól. Ennek érdekében kössön megállapodást a helyes használatról otthon és az otthonon kívül. Ennek a megállapodásnak tartalmaznia kell a hálózathoz való csatlakozás időpontját és helyét is, mert a túlzott használat befolyásolhatja az alvást, a társas kapcsolatokat vagy a tanulmányokat.
- Bízzon benne, hogy gyermeke betartja ezt a megállapodást, és ne váljon szigorú csendőrré.

SEGÍTSÉGNYÚJTÁS

- Legyen követendő példa.
- Ha gyermekének problémája van, és más kiskorúak is érintettek, vegye fel a kapcsolatot szüleivel vagy gondviselőivel, hogy közös megoldást találjanak.

FELÜGYELET

- Figyelje gyermeke viselkedését, és győződjön meg arról, hogy betartják-e a technológia megfelelő használatáról szóló megállapodást anélkül, hogy megsértenék a magánéletét.
- Húzzon meg határokat, hogy megelőzze a technológiákon keresztüli visszaélések esélyeit. Például a megállapodás egyértelművé teszi, hogy nem megengedett gúnyolódni valakivel, akit beleegyezése nélkül vettek fel videóra, valamint azt, hogy meg kell védenie a magánéletét.

Fontosabb kifejezések

- **Álhírek** (*fake news*): szándékosan publikált átverések, melynek célja a propaganda terjesztés és félrevezetés
- **Online zaklató** (*cyberbully*): A neten gyakran anonim módon, arctalanul tesz bántó megjegyzéseket különböző közösségi oldalakon, vagy egy általa készített előnytelen fotót, esetleg montázst oszt meg a zaklatás elszenvedőjéről.

- **Online csábítás** (*grooming*): a gyermekkel szexuális céllal történő kapcsolatfelvétel
- **PEGI** (*Pan European Game Information* azaz *Egységes Európai Játékinformációs Rendszer):* elektronikus játékokhoz használt korhatár és tartalom besorolási rendszer Európában
- **Szexting** (*sexting*): szexuális tartalmú, erotikus, meztelen vagy félig meztelen képek és videók küldése a mobiltelefonról a másik mobiljára vagy email címére
- **Szülői túlposztolás** (*sharenting*): Olyan viselkedést jelöl, mely során a szülők képeket és információkat osztanak meg gyerekeikről a közösségi hálón, a gyerek engedélye nélkül.

Project number: 2018-1-ES01-KA201-050461

Co-funded by the
Erasmus+ Programme
of the European Union

DIDAKTIKAI PROGRAM

A Be@cyberpro videójátékhoz

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

Mi a Be@CyberPro?
A Be@CyberPro egy olyan projekt, amelynek célja a készségek és a nemek közötti különbségek áthidalása a kibervédelmi szektorban, a hallgatók ösztönzése, a tanárok felhatalmazása és a szülők bevonása révén. A Be@CyberPro egy magával ragadó többnyelvű tapasztalat-játék, amelyet különböző kibervédelmi problémák feltárására és kibervédelmi szakmák bemutatására használnak. Ez egy interaktív, online digitális játék, amely lehetővé teszi, hogy a különböző hátterű és különböző felszerelésekkel rendelkező tanulók is képesek legyenek játszani vele.

Játékidő: A játékmenetet - minden szintet magában foglalva - 40 perc és 1 óra közötti időtartamra tervezték, azaz egy rendes iskolai tanóra időtartamára.

Játék cselekménye: A játék szerepjáték-stílust követ, ahol a játékosok egy fiktív környezetben a szereplők személyébe lépve játszanak. A főszereplőnek, egy középiskolába járó lánynak különféle kiberbiztonsággal és az ezzel foglalkozó szakmákkal kapcsolatos feladatokat kell megoldania, hogy segítsen barátainak és iskolatársainak.

Hogyan kell a videójátékot játszani?

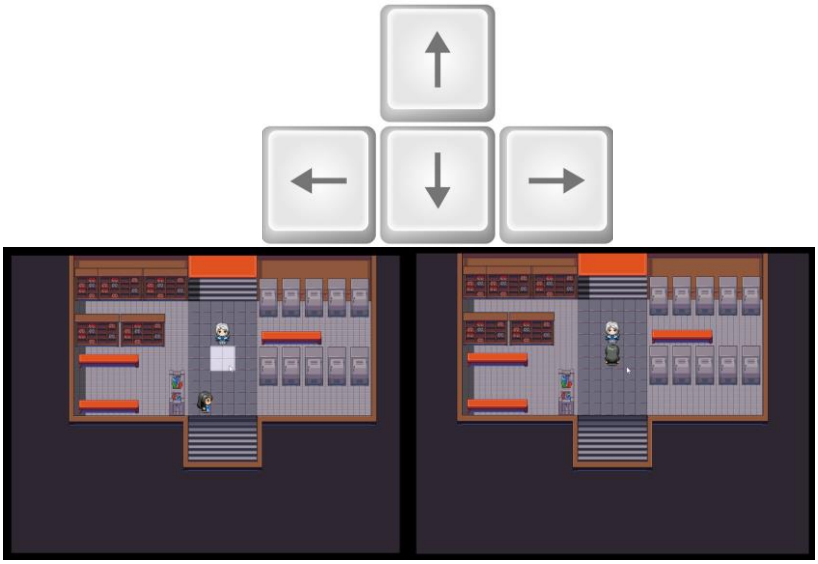
- Használja a megadott linket a játékhoz.
- Megjelenik a játék indítási menüje a következő opciókkal: Új játék, Folytassa és Opciók.

- Először kattintson az Új játék feliratra az egérrel vagy az érintőpaddal!
- Amikor a képernyő betöltődik, kattintson bárhová az egérrel / érintőlappal a szereplők közötti beszélgetések megkezdéséhez.

Project number: 2018-1-ES01-KA201-050461

Co-funded by the
Erasmus+ Programme
of the European Union

- Használja a billentyűzet nyilait, vagy kattintson egy területre a karakter mozgatásához.



- Beszélgetéshez léptesse a főszereplőt a játékban szereplő karakterekhez.

Project number: 2018-1-ES01-KA201-050461

Co-funded by the
Erasmus+ Programme
of the European Union

- Kattintson a képernyő bármely pontjára a beszélgetések folytatásához.
- Kattintson az előugró ablakokra az egérrel, vagy nyomja meg az Enter billentyűt a válasz kiválasztásához.

- Az ajtók megközelítésével különböző helyiségekbe mehet.

Project number: 2018-1-ES01-KA201-050461

Co-funded by the
Erasmus+ Programme
of the European Union

- Az Esc gombot bármikor megnyomhatja az Opciók menü megtekintéséhez.

- Kövesse a játék szereplőinek utasításait, hogy a feladatokat el tudja végezni, és hogy megismerkedjen a kibervédelemmel.

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

A videójáték linkje: A játék bármilyen készülékkel elérhető a következő linken
http://telprojectgames.com/CyberPro/v0.4/index.html

Függelék: Be@CyberPro Képes forgatókönyv (Storyboard**):**
https://drive.google.com/file/d/18HWpPqragp9Pstp7hgEsAmtg97Af2W8i/view?usp=sharing

Mielőtt bemutatná a játékot az osztályának

Íme, néhány javaslat arra vonatkozóan, hogyan használhatja a játékot az osztályteremben:

1. Játssza le a játékot, ismerje meg a játékot érintő vezérlőket, a történetet és a tanulási tartalmat!

2. Fontolja meg a szülők bevonását! Az egyik javasolt mód a szülő bevonására az lenne, ha levelet küldene a tanulókkal, vagy más módon kommunikálná játékalapú tanulási tervét és annak előnyeit a szülőknek. Ezzel elkerülheti azt a félreértést, ami abból adódhat, hogy a tanuló azt meséli otthon, hogy a tanulók csak játszanak a tanórán.

3. Szánjon időt az osztályon belüli következetes játékra! Annak érdekében, hogy a tanulók elegendő játékidőt élvezzenek a Be@CyberPro videójátékkal, hogy kihasználhassák annak előnyeit, próbálja meg:
    - A játékidő mint kijelölt tevékenység szerepeljen az óratervben,
    - Használja a játékot a tanuláshoz kezdő vagy befejező tevékenységként. A játékot a kibervédelem megismerésének kezdőpontjaként használva lehetővé válik, hogy a hallgatók levonhassák saját következtetéseiket a kiberbiztonság fontosságáról, még mielőtt a tudásszakértő a koncepciót részletesen elmagyarázná és megerősítené.
    - Hozzon létre egy sor tanulási lépést, amelyek közül az egyik a játék.

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

A feladat-állomások () bemutatása a hallgatók számára

A feladat-állomás arra való, hogy a hallgatók az óra alatt egyénileg, párban vagy kis csoportokban játszhassák a játékot.

Szánjon időt arra, hogy kifejezetten bemutassa az osztálynak az új feladat-állomásokat, és megvitassa az állomások használatához kapcsolódó szabályokat.

Mielőtt nekiállnának, világosan magyarázza el a feladat-állomások használata közben várható viselkedést és annak következményeit, ha ezeket az elvárásokat nem teljesíti. Ezután mutassa be hallgatóinak az új feladat-állomást a következő lépések megtervezésével:

- *Ha lehetséges*, használjon egy időzítőt, amelyet a hallgatók láthatnak és hallhatnak, hogy nyomon tudják követni a tanulási állomásokon töltött időt.
- Magyarázza el a tanulóknak, mivel fogja felhívni a figyelmüket, amíg a tanulási állomáson vannak.
- Részletesen magyarázza el a kiválasztott tevékenység célját, amit el fognak végezni – „Ezt kell megtanulnod ezen a tanulási állomáson."
- Csak annyit mutasson be, hogy a tanulók megértsék és komfortosan érezzék magukat az egyes tevékenységek végzésekor. Mutassa meg, hogyan rakjanak rendet az éppen használt állomáson, és terelje oda a következő tanulót, amikor az időzítő kikapcsol.

A videójáték használata az osztályteremben

1. Mutassa be röviden a témát, és magyarázza el a tanulóknak a játék céljait és történetét a játék előtt.
2. A játék előtt vezessen be egy gyors tudásalapot. Kérdezze meg a tanulókat, hogy hallottak-e a kiberbiztonságról vagy, hogy korábban volt-e már problémájuk a kiberbiztonsággal.
3. Hagyja, hogy a tanulók lejátsszák az első szintet, és kérjék meg őket, hogy szüneteltessék a játékot, miután befejezték.
4. Miután mindenki befejezte az első szintet, tartson egy rövid tájékoztatót és beszélje meg velük az eddig tanultakat. Néhány javasolt pont a megvitatáshoz:
    - Mit tanultak a hallgatók ebből a szintből?
    - Mit gondolnak, mit tanultak meg eddig?
    - Volt-e valakinek hasonló tapasztalata?
    - Volt-e valakinek nehézsége az anyag megértésével?
    - Motiváltak-e a diákok a játék folytatására?
5. Mondja meg a tanulóknak, hogy folytassák a játékot ugyanezen felépítés alapján (játékszint, majd vitapontok).
6. Amikor a tanulók befejezték a játékot, ossza ki nekik a játék értékelő kérdőívét (azaz online kérdőívet).
7. A megbeszélésekből és a visszajelzésekből összegyűjtött adatok felhasználásával újabb tanórát készíthet. Különösen figyeljen a felmerült közös problémákra!

Támogatott tanulás

A játékalapú tanulás használatával, valamint a célok, szabályok, feladatok és az interakció a tanórákba való beépítésével a hallgatókat jobban be lehet vonni az órába és a tanulási eredményeket is lehet növelni. A következő irányvonalak segíthetnek (Cojocariua, Boghiana, 2014):

- Építsen érzelmi kapcsolatot a tanulással és a tantárgyi anyaggal
- Adjon alkalmat a visszajelzésre és a gyakorlásra
- Testreszabható az egyénre szabott tanításhoz

Project number: 2018-1-ES01-KA201-050461

A digitális játékok tanulási eszközökként, motiválóként és a kíváncsiság felkeltésére használhatók az infokommunikációs technológia oktatási alkalmazásának részeként. Ennek eredményeként a tantermi játékokban széles körű megállapodás született a diákok tanulásának és teljesítményének optimalizálásának hatékony eszközeként a mindennapi oktatási gyakorlatban. A tanulók elkötelezettsége és a digitális játékok használata közbeni információfogyasztása közötti pozitív kapcsolatot az elmúlt években különféle független tanulmányok igazolták (Papadakis, 2018

Project number: 2018-1-ES01-KA201-050461

Co-funded by the Erasmus+ Programme of the European Union

AZ ONLINE JÁTÉK LINKJE

A játék bármilyen készülékkel elérhető a következő linken:
http://telprojectgames.com/CyberPro/Test/index.html

A PROJEKT WEBOLDALA

https://www.beacyberpro.eu/

SZAKIRODALOM

Ahuja, M. K. (2002). Women in the information technology profession: A literature review, synthesis and research agenda. *European Journal of Information Systems*, *11*(1), 20-34.

Armstrong, D. J., Riemenschneider, C. K., Allen, M. W., & Reid, M. F. (2007). Advancement, voluntary turnover and women in IT: A cognitive study of work–family conflict. *Information & Management*, *44*(2), 142-153.

Bagchi-Sen, S., Rao, H. R., Upadhyaya, S. J., & Chai, S. (2010). Women in cybersecurity: A study of career advancement. *IT professional*, *12*(1), 24-31.

Cojocariu, V. M., & Boghian, I. (2014). Teaching the relevance of game-based learning to preschool and primary teachers. *Procedia-Social and Behavioral Sciences*, *142*, 640-646.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10).

Crumpler, W., & Lewis, J. A. (2019). *Cybersecurity Workforce Gap*. Center for Strategic and International Studies (CSIS).

ENISA (The European Union Agency for Cybersecurity) (2020). *ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected*. https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends.

Erixon, F., & Lamprecht, P. (2018). The next steps for the digital single market: From where do we start. *ECIPE Policy Brief*, *2*, 2018.

Heaton, C. A. N., & McWhinney, G. (1999). Women in management: the case of MBA graduates. *Women in Management Review*.

Kohler, K. (2020). Estonia's National Cybersecurity & Cyberdefense Posture.

Lis, P., & Mendel, J. (2019). Cyberattacks on critical infrastructure: An economic perspective. *Economics and Business Review*, *5*(2).

Papadakis, S. (2018). Evaluating pre-service teachers' acceptance of mobile devices with regards to their age and gender: a case study in Greece. *International Journal of Mobile Learning and Organisation*, *12*(4), 336-352.

Parasuraman, S., Purohit, Y. S., Godshalk, V. M., & Beutell, N. J. (1996). Work and family variables, entrepreneurial career success, and psychological well-being. *Journal of vocational behavior*, *48*(3), 275-300.

Poster, W. R. (2018). Cybersecurity needs women.

Pupillo, L. (2018). EU Cybersecurity and the Paradox of Progress. *CEPS Policy Insight*, (2018/06).

Reischuk, R. (2019). *Let's Encrypt: Cybersecurity disruptieren*.

Sobers, R. (2019). must-know cybersecurity statistics for 2019. *Varonis.*

Sterlini, P., Massacci, F., Kadenko, N., Fiebig, T., & van Eeten, M. (2019). Governance Challenges for European Cybersecurity Policies: Stakeholder Views. *IEEE Security & Privacy*, *18*(1), 46-54.

Štitilis, D., Rotomskis, I., Laurinaitis, M., Nadvynychnyy, S., & Khorunzhak, N. (2020). National Cyber Security Strategies: Management, Unification and Assessment.

Trauth, E. M., Quesenberry, J. L., & Morgan, A. J. (2004, April). Understanding the under representation of women in IT: Toward a theory of individual differences. In *Proceedings of the 2004 SIGMIS conference on Computer personnel research: Careers, culture, and ethics in a networked environment* (pp. 114-119).
Ventures, 2017

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102.