TANÁRI KÉZIKÖNYV

A DIGITÁLIS BIZTONSÁGRÓL

BE@CYBERPRO
Fostering cybersecurity careers

Hogyan segíthetjük a gyerekeket, fiatalokat a digitális eszközök és az internet biztonságos, tudatos és értékteremtő használatában?

A DIGITÁLIS BIZTONSÁGRÓL

TANÁRI KÉZIKÖNYV

Hogyan segíthetjük a gyerekeket, fiatalokat a digitális eszközök és az internet biztonságos, tudatos és értékteremtő használatában?

SZERZŐK:

Dr. Sediviné Balassa Ildikó
Chogyelkáné Babócsy Ildikó
Hartyányi Mária
Kacsur Annamária
Modla Réka
Christina Todorova
Francisco Moyano
Guillermo Pérez-Tomé
Inés López
Javier Fernández Collantes
Luis Fernández
Mary Cleary
María Teresa Villalba de Benito
Milena Andreeva
Pavel Varbanov
Sonia Martínez-Requejo
Stefana Petrova
Vera Poslova

Szakmai szerkesztő: Dr Sediviné Balassa Ildikó, Chogyelkáné Babócsy Ildikó
Olvasószerkesztő: Szabóné Hábel Tímea, Révész Angéla
Tördelőszerkesztő: Bánszki András
Borítóterv: Bánszki András

ISBN SZÁM: 978-615-00-9459-5

Felelős kiadó: SZÁMALK-Szalézi Technikum és Szakgimnázium
Halász József igazgató
PROMPT-H Számítástechnikai, Oktatási, Kereskedelmi és Szolgáltató Kft.
Dr. Lengyel József igazgató

A könyv az Európai Bizottság támogatásával az Erasmus+ programban megvalósított Be@CyberPro, „A Videogame for Fostering Cybersecurity Careers in Schools" (Videójáték az iskolában a kiberbiztonsági pályák iránti érdeklődés előmozdítására) című projekt keretében készült.

Az Európai Unió Erasmus+ programjának társfinanszírozásával

Az Európai Bizottság támogatása ezen kiadvány elkészítéséhez nem jelenti a tartalom jóváhagyását, amely kizárólag a szerzők álláspontját tükrözi, valamint a Bizottság nem tehető felelőssé ezen információk bárminemű felhasználásáért.

Köszönetüket fejezzük ki a projektben együttműködő hazai és külföldi partnereknek: PROMPT-H Számítástechnikai, Oktatási Kft., SZÁMALK-Szalézi Technikum és Szakgimnázium (Magyarország), UNIVERSIDAD EUROPEA DE MADRID, UNIVERSIDAD DE ALCALA, COLEGIO JOYFE SL (Spanyolország), ICS SKILLS , CORK ISTITUTE OF TECHNOLOGY (Írország), ESI CEE EUROPEAN SOFTWARE INSTITUTE CENTER, EASTERN EUROPE 125 SECONDARY SCHOOL (Bulgária).

Köszönet a hazai, kísérleti tanárképzésben résztvevő mentoroknak, Chogyelkáné Babócsy Ildikónak, Hartyányi Máriának, Kacsur Annamáriának és Sediviné Balassa Ildikónak.

Köszönet az online kurzust sikeresen elvégző valamennyi pedagógusnak, kiemelten a munkájukat és tapasztalataikat is megosztó alábbi tanároknak: Olasz-Barabás Brigitta, Fenyvesiné Jászai Lídia, Tóthová Edita, Pappné Szabó Alexandra, Karsai Zita és Teleki József.

Külön köszönet az IT-biztonság és kiberbiztonság női szakértőinek – Zengő Andreának, Bíró Gabriellának, Fülöp Juditnak és dr. Baracsi Katalinnak –, akik segítik a projekt feladatainak hazai megvalósítását, és akiket példaképül állíthattunk a pályaválasztás előtt álló a fiatal lányoknak.

Végül köszönjük az e könyv elkészítésében résztvevő kollégáink együttműködését és munkáját.

Tartalomjegyzék

ELŐSZÓ

Mi is lehetne ma az oktatásban aktuálisabb téma, mint a digitális világban való munka és tanulás, az online térben való eligazodás!? Ez foglalkoztat bennünket tanárokat, a szülőket és a diákokat egyaránt, hiszen senki sem lehet biztos abban, hogy a közeljövőben nem kényszerül-e ismét arra, hogy otthonról, számítógépen a világhálóra csatlakozva végezze a munkáját, vagy éppen tanuljon.

Amikor ezt a könyvet elkezdtük megírni, még nem tudhattunk a COVID-19 által előidézett robbanásszerű változásokról. Nem tudhattuk, hogy netgenerációs tanulóinknak, akik mondhatni, szünet nélkül „lógnak a neten", hamarosan hivatalosan is ezt kell tenniük.

A felkészülés az internet biztonságos használatára eddig is nagyon fontos volt, de a kialakult helyzetben több ennél: elengedhetetlen. Különösen érvényes ez az internetes zaklatásnak leginkább kitett, legsérülékenyebb fiatalok esetében, akiknek a szülők mellett leginkább a tanárok segíthetnek, akikre ebben a kérdésben komoly felelősség hárul.

A középiskolákra és pedagógusaikra várnak a feladatok, hogy tudatosítsák a diákokban, hogy milyen fontos ma az adatvédelem, a számítógépes bűnözés elleni védekezés és a kibertérben való felelős magatartás. Ez volt az a kihívás, amire az Erasmus+ programban támogatott projektben együttműködő spanyol, bolgár, magyar és ír szakemberek egy online tanárképzési program kidolgozásával válaszoltak, és amit ennek a kézikönyvnek a révén most a Számalk-Szalézi Technikum és Szakgimnázium és a PROMPT-H Számítástechnikai Oktatási, Kereskedelmi és Szolgáltató Kft. minden hazai pedagógus számára elektronikus könyv formátumban ingyenesen elérhetővé tesz.

Ezt a kiadványt a hazai közönség és a pedagógusok számára az teszi különösen értékessé, hogy a tudatos internethasználati kompetenciák fejlesztésére részletesen kidolgozott és kipróbált óraterveket tartalmaz, az oktatásban még viszonylag újszerű, de a diákok körében egyre népszerűbb, izgalmas, aktív tanulásra ösztönző szabadulószobás játékokkal. Igaz, hogy egy hagyományos óra előkészítéséhez képest a szabadulószoba megtervezése első alkalommal jelentős többletmunkával jár, ám a diákok visszajelzései alapján megtérült a befektetés. A módszer gyakorlati példákon keresztül való bemutatása kedvet csinálhat, és sokat segíthet minden pedagógusnak abban, hogy az online világ veszélyeit a hagyományosnál hatékonyabb, élményalapú tanítási módszerrel tudatosítsa diákjaikban.

Nagyon tanulságosak annak a közös kutatásnak az eredményei is, amelyben a pedagógusok azt vizsgálták, hogy a diákok milyen mértékben vannak tisztában az internet veszélyeivel. Arra a kérdésre, hogy: „Volt-e negatív élményed az interneten?" a 340 tanulóból 274-en válaszoltak igennel. A viszonylag kis minta ellenére megdöbbentő, hogy a válaszadók 81%-ának már volt része valamilyen negatív élményben (internetes zaklatás, az online jelenléthez kapcsolódó kiközösítés, megfélemlítő üzenetek a közösségi oldalakon stb.).

Ez is mutatja, hogy milyen nagy a szülők és tanárok felelőssége, nemcsak a felvilágosításban, a veszélyek tudatosításában, hanem abban is, hogy motiválják a pályaválasztás előtt álló fiatalokat az informatikai szakmákban való továbbtanulásra. Különösen fontos lenne elérni ezekben a szakmákban valamiféle nemek közötti egyensúlyt, hiszen ma még rendkívül alacsony a nők aránya a kiberbiztonsági területeken.

A könyv elolvasását tisztelettel ajánlom minden pedagógusnak, szakembernek, aki - felismerve a felelősséget - aktívan tenni is szeretne azért, hogy tanulóink, gyermekeink képesek legyenek élni a digitális világ szolgáltatásaival, képesek legyenek munkájukban alkalmazni a legkorszerűbb technológiai megoldásokat úgy, hogy közben tisztában vannak a veszélyekkel, és fel vannak készülve azok elkerülésére.

Dr. Lengyel József igazgató
PROMPT-H Számítástechnikai Oktatási, Kereskedelmi és Szolgáltató Kft.

A NEMZETKÖZI PROJEKTRŐL, ÉS A TANÁRTOVÁBBKÉPZÉSI KURZUSRÓL

A 21. században már egyre gyakrabban találkozhatunk a *DIGITÁLIS BIZTONSÁG* kérdéskörével.

Egyre több iskolában, munkahelyen jelennek meg az internet veszélyei, így ezek megelőzésére is nagyobb hangsúlyt kell fektetnünk, mind cégek, mind az iskolák részről.

Számos nemzetközi és hazai kutatás[1], felmérés igazolja, hogy miközben a technológia rohamosan fejlődik, egyre több szakember hiányzik az informatikai területről. Egyre több feladat hárul a kiberbiztonsággal foglalkozó szakemberekre, és ahogyan más műszaki szakmákban, itt is nagyon alacsony a nők aránya: globális szinten mindössze 10%.

Az oktatási intézmények pedagógusaira és oktatóira várnak azok a feladatok, hogy tudatosítsák a diákokban, hogy milyen fontos ma az adatvédelem, a számítógépes bűnözés elleni védekezés, és a kibertérben való felelős magatartás.

Az is elsősorban a család és az iskolák feladata, hogy a pályaválasztás előtt álló fiatal lányokat arra ösztönözzék, hogy informatikai szakirányban tanuljanak tovább. Ebben szándékozik segíteni a pedagógusoknak és iskoláknak a **„Be@CyberPro - Légy kiberbiztonsági szakértő!" című Erasmus+ projekt, amelynek megvalósításában négy országból összesen kilenc intézmény vett részt.**

Az Európai Unió támogatásával megvalósuló nemzetközi projekt több fontos célt is kitűzött, az alábbiak szerint:

- A projekt alapcélja a nemek közötti aránytalanság csökkentése a kiberbiztonsági iparban, a szektorban működő magáncégek és felsőoktatási intézmények összefogásával, iskolákkal együttműködve.
- A kiberbiztonsági szakmákban rejlő lehetőségek és a sikeres kiberbiztonsági karriert reprezentáló női pályamodellek bemutatása motiválhatja a lányokat az informatikai szakirányú továbbtanulásra.
- A partnerség a kihívásokra való reagáláshoz szükséges problémamegoldó készségek fejlesztésével; online környezetben zajló tanártovábbképzéssel, virtuális valóság alapú játékok fejlesztésével; a nők pozitív szerepének hangsúlyozásával és karrier lehetőségeik bemutatásával segíti az iskolákat, a tanárokat, a tanulókat és a szülőket.

1 A hazai informatikus- és IT-mérnökképzés helyzetének, problémáinak, gátló tényezőinek vizsgálata Összefoglaló tanulmány
https://docplayer.hu/15993204-A-hazai-informatikus-es-it-mernokkepzes-helyzetenek-problemainak-gatlo-tenyezoinek-vizsgalata.html
Európai szintű probléma az informatikusok hiánya
https://ma7.sk/piac/europai-szintu-problema-az-informatikusok-hianya

A projekt eredményei:

- Online tanártovábbképzési program közös fejlesztése és pilot projektek.
- Többnyelvű videojáték készítése a diákok számára, és a játék kipróbálása.
- E-könyvek írása és kiadása:
  - Digitális biztonságról (tanári kézikönyv) - magyar nyelvű kiadvány
  - A kiberbiztonsági szakemberként sikeres női példaképek bemutatása – angol, spanyol, bolgár és magyar nyelvű kiadvány

A tanártovábbképzési kurzusról

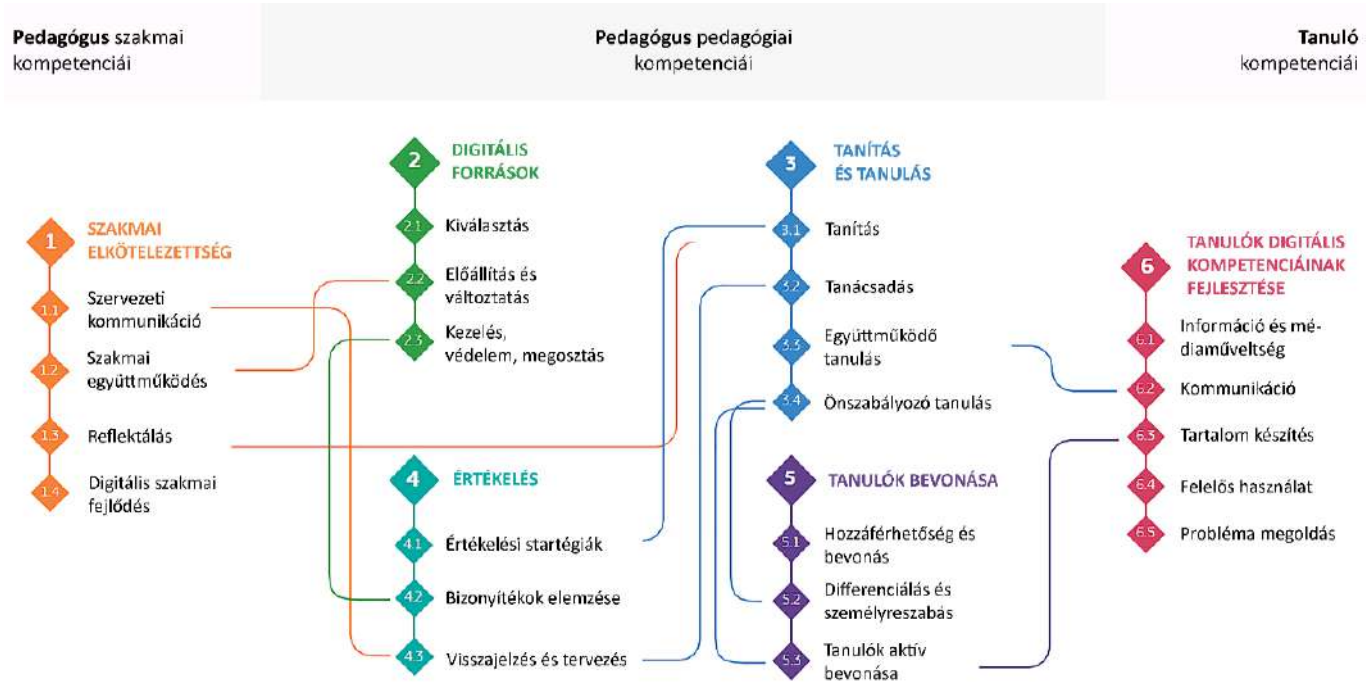
Négy ország partnerintézményeinek szakemberei dolgoztak közösen a **tanártovábbképzési programon,** melyet a **„Digitális biztonság"** témaköreiből állítottak össze, majd a négy nyelven elkészült képzést minden partnerország ki is próbálta, értékelte és hasznosítja. A pilot tanártovábbképző kurzus az egyes témakörök legfontosabb tartalmát foglalta össze, annak érdekében, hogy a pedagógusok és oktatók megfelelő ismeretekkel rendelkezzenek a digitális biztonság megtanításához. A képzés azt a célt is szolgálta, hogy a pedagógusok a tanulókat fel tudják készíteni a tudatos digitális eszközhasználatra, a felelősségteljes magatartásra a kibertérben.

A kurzus tartalmát az Európai digitális kompetencia keretrendszerben (Digcomp és DigCompEdu) meghatározott kompetenciák alapján fejlesztette ki a nemzetközi partnerség. A DigComp, az állampolgárok digitális készségeinek európai keretrendszere a számítógépes biztonságot az öt érintett terület egyikeként határozza meg, összesen 4 kompetenciát rendelve hozzá. A DigCompEdu ezzel szemben 3 kompetenciát határoz meg, az egyiket a digitális erőforrások területén (a digitális erőforrások kezelése, védelme és megosztása), és kettőt a tanulók digitális kompetenciájának elősegítése (a számítógépes problémák felelős felhasználása és megoldása) területén.

Ezen túlmenően a kurzusban helyet kapott egy fejezetrész az internetbiztonsági szakmákról, hogy a tanárok rendelkezzenek a tanulók motiválásához szükséges ismeretekkel. Ez a rész be kívánja bemutatni azt, hogy Európában és hazánkban mely kompetenciák azok, amelyekkel egy kiberbiztonsági szakembernek rendelkeznie kell, továbbá, hogy mely szakmák azok, amelyek tanulása kellő elméleti és gyakorlati tudást ad ahhoz, hogy az IT biztonság, kibervédelem területén - a tanulási folyamat befejezését követően - a fiatalok el tudjanak helyezkedni. A negyedik fejezetrész ahhoz is segítséget kíván nyújtani, hogy a különböző iskolák pályaválasztással foglalkozó tanárai e témában is felkészültek legyenek.

Az oktatók digitális kompetenciáira[2] vonatkozó keretrendszer, a DigCompEdu (Redecker & Punie, 2017) célja, hogy az oktatók kompetenciaszükségleteinek alapvető ismeretét biztosítsa európai szinten, az oktatás minden szakaszában. Amint az alábbi ábrán látható, a DigCompEdu 6 különböző területet határoz meg, összesen 22 kompetenciával. A területeket szakmai, pedagógiai és tanulási kompetenciákra osztják. Ezen kívül hat kompetenciaszintet állít fel, amelyek megegyeznek a nyelvi kompetencia kereteinek szintjeivel (A1-től C2-ig).

2 Digitális kompetencia: a tanárok és diákok számára nélkülözhetetlen 21. századi készség https://www.schooleducationgateway.eu/hu/pub/resources/tutorials/digital-competence-the-vital-.htm



DigCompEdu - Európai oktatási referencia-keretrendszer oktatók számára (Redecker & Punie, 2017)

A tanártovábbképzés célja

A kurzus alapvető célja az volt, hogy a TANÁROK ismerjék meg, illetve meglévő tudásukat gazdagítsák a DigCompEdu által meghatározott 3 kompetenciakörbe tartozó tartalmakkal, amelyek:

- a „digitális erőforrások területe”,
- „a digitális erőforrások kezelése, védelme és megosztása” a diákok digitális kompetenciája fejlesztésének érdekében,
- a „számítógépes problémák felelős felismerése és megoldása”.

A TANÁROK legyenek képesek a tanulóik számára - korosztálytól függően, differenciáltan - az ismereteket továbbadni, és tudatos, felelős és etikus magatartásra megtanítani a fiatalokat. Képesek legyenek továbbá a pályaválasztás során a diákok korrekt tájékoztatására az informatikai szakmákról, beleértve a speciális képzési irányokat is, mint az IT-biztonság és kibervédelem.

A képzésről és a könyvről

Az online képzéseket Moodle környezetben, négy országban, négy nyelven próbáltuk ki. A hazai képzést 2019. decemberben kezdtük el és 2020 májusában fejeztük be. Sajnos, a kurzus idejében arra kényszerültek az iskolák a Covid vírus miatt, hogy bezárjanak. Márciustól az egész országban bevezetésre került a digitális oktatás. Ez meghosszabbította az online kurzust, egyrészt mert a tanár kollégáknak nagyon sok plusz feladatuk volt a digitális oktatásra való gyors áttérés miatt, másrészt a továbbképzésben kapott feladatmegoldások kipróbálása is nehezebbé vált.

A digitális oktatásra való áttérés a gyerekek digitális térben való tartózkodását azonban több mint duplájára emelte,[3] ami a mi felelősségünket is megnövelte. Egyértelművé vált, hogy ki kell adnunk ezt a kézikönyvet, át kell adni a tapasztalatokat, játékokat, kipróbált feladatokat, hogy segíthessünk minden pedagógusnak – rajtuk keresztül a diákoknak is - felkészülni e fontos feladatra.

A könyv első részében a tanárképzés tananyagát olvashatják, rövidítve és kiegészítve magyar nyelvű szakirodalommal (cikkekkel és videókkal). A második fejezetben az egyes témákhoz tartozó feladatokat ismertetjük, és minden fejezetrészhez tartozóan bemutatunk néhány tanári megoldást a legjobbak közül. Az egyéni feladatmegoldásokon kívül két olyan tematikus gyűjteményt is közzéteszünk, melyeket a résztvevő tanárok közösen alkottak meg.

3 A digitális oktatás első tapasztalatai
https://www.mixonline.hu/Cikk.aspx?id=174633
A digitális oktatás tapasztalatai egy szakértő szemével
https://www.dszc.hu/informaciok/hirek/2164-a-digitalis-oktatas-tapasztalatai-egy-szakerto-szemevel

I. FEJEZET: A DIGITÁLIS BIZTONSÁGRÓL

Az alábbi négy elméleti fejezetrészben a következő témákat részletezzük:

1. **modul - A digitális eszközök és tartalom védelme**
2. **modul - A személyes adatok és a magánszféra védelme**
3. **modul - Az egészség, a jólét és a környezet védelme**
4. **modul - Karrier leírások**

Ezek a modulok adták a tanártovábbképzés elméleti alapját minden partnerországban. E könyv keretében a tananyagot egyrészt rövidítettük, másrészt új tartalommal egészítettük ki a hazai szakirodalomra és a témában megjelent szakmai anyagokra építve.

1. MODUL: A DIGITÁLIS ESZKÖZÖK ÉS TARTALOM VÉDELME

BEVEZETŐ

Ebben modulban négy nagy témával foglalkozunk az alábbiak szerint:

- A digitális eszközök védelme
- Kockázatok és veszélyek a digitális környezetben
- A digitális tartalom védelme
- A technológia felelős használata

A négy részben olyan elméleti tananyagot osztunk meg, melyek alapján megtanulhatók a legfontosabb ismeretek, illetve gazdagítható az e témákban már meglévő tudás.

1. A DIGITÁLIS ESZKÖZÖK VÉDELME

Olyan világban élünk, amely folyamatos technológiai változás alatt áll. Új kihívásaival szemben pozitív és felelősségteljes hozzáállásra van szükségünk, amit az idevágó területek megismerésén keresztül szerezhetünk meg.

Tudatában kell lennünk, hogy személyes adataink hanyag kezelése hatással lehet ránk. Ahogyan nem mondjuk el bárkinek életünk minden részletét, ugyanúgy tartsuk magunkat ehhez a digitális életünkben: nem szabad felelőtlen módon szétszórnunk az információinkat anélkül, hogy tudnánk, hogyan fogják végezni, hiszen az információt egy harmadik fél elferdítheti és rosszra használhatja (pl. zsarolásra, csalásra...).

Kezdjük azzal, hogy a készülékeinkben található információra összpontosítunk és arra, hogyan lehet véletlenül kiadni őket, vagyis hogyan kerülhetnek egy harmadik félhez. Bár bonyolult dologról van szó, meg kell ismernünk az adataink védelmének lényeges elemeit, és meg kell tennünk mindent, hogy információink és készülékeink biztonságosan védve legyenek.

1.1 Adatvédelem – operációs rendszerek

Ha egy eszközt, akár számítógépet, akár egy okostelefont vásárolunk, rendszerint a telepített operációs rendszerrel (OS) együtt kapjuk. A fertőzések, támadások, biztonsági sérülések stb. többsége a számítógépnek az internettel való kapcsolódása során történik. Ennek elkerülésére szerintünk az a legjobb módszer, ha az operációs rendszerünket a lehető leggyakrabban frissítjük.

Ha az operációs rendszer automatikus frissítést végez, akkor automatikusan letölti és telepíti a frissítéseket. Ha ez nincs aktiválva vagy helyesen beállítva, látogasson el az operációs rendszer fejlesztői oldalára a legújabb frissítésekhez és nézze meg, hogyan kell aktiválni.

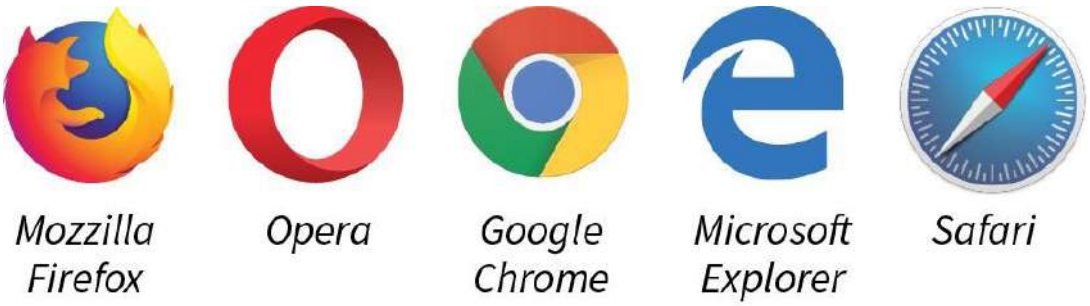
Hogyan?

- **Windows**: A Windows rendszerben az operációs rendszer frissítése nagyon egyszerű: A Start menüpontba lépünk, és beírjuk az „update”-et, mire megjelenik a „Windows Update” opció. Innentől igen egyszerű a dolog, a „Frissítések keresése” gombra kell kattintani. Ugyanabból az ablakból aktiváljuk az Automatikus frissítéseket.
- **MacOS**: Általános szabály, hogy a Mac értesít a rendelkezésre álló új frissítésekről egy „Értesítés” nevű felugró ablakban, amely a letöltéshez és telepítéshez visz minket.
- **Linux**: A Linux frissítése a legújabb verzióra néha magában foglalja a teljes kiosztás újratelepítését. De a Linux csomagokat manuálisan is frissíthetjük a legújabb verzióra.
- **Android**: Android használatakor a Google minden hónap elején értesítést küld az összes regisztrált sebezhetőségről és biztonsági problémáról. Ezzel a bejegyzéssel együtt megjelennek a havi frissítések is.
- **IOS**: Az IOS igazán jól kezeli az automatizált frissítéseket. A „Beállítások / Általános / Szoftver frissítése” menüpontokkal magunk is beállíthatjuk.

Az alkalmazott operációs rendszertől függően előfordulhatnak eltérések az előzőekben említettektől, de a legtöbb eszköz esetében általában ugyanezek a frissítési módok.

1.2 Adatvédelem - webböngészők

A webböngészők jobban ki vannak téve az ilyen fenyegetéseknek, mivel ezeket főleg a neten való keresésre és információforrásként (pl. applikációk) használjuk. Mindegyiküknek megvan a saját sebezhetősége éppúgy, mint az operációs rendszereknek: minél inkább használják őket a felhasználók, annál több támadásnak vannak kitéve.



Forrás: https://www.nkp.hu/tankonyv/informatika_6/lecke_02_005

Mit tehetünk?

A webböngészők „addon”, „plugin” kiterjesztésűek. Tudnunk kell, hogy melyik biztonsággal kapcsolatos segédprogramot használjuk a webböngészőnkhöz, és ezt azután alkalmazzuk is, hogy a lehető legbiztonságosabban mozogjunk a neten.

Böngészőink konfigurációs menüjében lehetőségünk van arra, hogy a „Kiterjesztések” menüpont használatával fokozzuk a biztonságunkat. Minden böngésző rendelkezik saját kiterjesztéssel, és nekünk kötelességünk megtalálni azokat, amelyek megvédhetik a rendszerünket, és amikről úgy véljük, hogy az eszközeink számára a legmegfelelőbbek.

1.3 Adatvédelem - alkalmazások (szoftverek)

Bármilyen típusú alkalmazás telepítési folyamatában két lehetőség áll rendelkezésre: letölthetjük és telepíthetjük azokat megbízható weboldalakról, vagy letölthetjük egy harmadik fél honlapjáról az eredeti fejlesztő által garantált biztonság nélkül. Még ha a számítógépeinken fenn is vannak az ismert és legbiztonságosabb alkalmazások, ne töltsünk le harmadik féltől származó applikációkat!

A mobileszközök esetében a legnépszerűbb webáruházak a Google Play és az Apple Store, ahonnan az Android és az IOS alkalmazások nagy részét letölthetjük. Ezeken a helyeken rendszeresen ellenőrzik az összes alkalmazást, hogy garantálják a biztonságot. A Google a Google Play Protectet használja, hogy védelmet biztosítson a rosszindulatú programok, a kémprogramok vagy bármilyen más, kárt okozó program ellen.

Mit tehetünk?

- Ne telepítsünk alkalmazásokat olyan helyekről, amelyek nem hivatalosak, nem megbízható webáruházak vagy fejlesztői webhelyek.
- Ne telepítsünk olyan alkalmazásokat, amelyek etikai szempontból nem korrektek. (Példa: olyan alkalmazások, amelyek kémkedési, hekkelési stb. funkciókat engedélyeznek).
- Ne telepítsünk olyan illegális szoftvereket vagy játékokat, amik olyan ingyenes szolgáltatásokat, elemeket stb. tesznek hozzáférhetővé, amelyeket egyébként pénzért lehetne megkapni.
- Ne telepítsünk olyan alkalmazásokat, amelyek egyszerű pénznyerési lehetőséget ígérnek.

Egy másik fontos tényező, hogy rendszerint lazák vagyunk az engedélyekkel: átugorjuk vagy elfogadjuk azokat. Gyakori, hogy az ingyenes alkalmazások engedélyt kérnek az eszközünk bizonyos aspektusaira (általában többet, mint amennyire szükségük van), például: **Adatok tárolása**, **Kamera, Névjegyek**, **Mikrofon, SMS, Telefon, Helymeghatározás** stb. vagy engedélyt kérnek a GPS pozíciónknak az alkalmazáshoz való hozzáadásához.

Ezeknek az engedélyeknek mindegyikében veszélyek rejlenek, amelyek akár egyetlen megtekintés után is felugró ablakokat engednek be.

Hogyan?

Mielőtt telepítünk egy alkalmazást, az applikációhoz szükséges összes engedélyt megnézhetjük a webáruházban:

- A saját telefonunkról hozzáférhetünk az engedélyezési beállításhoz az „Alkalmazás” menü „Beállítások” almenüjében, ám ha úgy véljük, hogy az alkalmazáshoz nincs szükség bizonyos jogosultságokra, akkor azokat le is tudjuk tiltani.
- Bármely olyan alkalmazást eltávolíthatunk, amelyet gyanúsnak tartunk, mert működésbeli problémákat okoz (pl. a készülék gyorsan felmelegszik, az akkumulátor élettartama a szokásosnál rövidebb, ismeretlen levonások jelentkeznek a bankszámlánkon stb.).

1.4 Alapvető hitelesítési módszerek

Amikor egy szolgáltatáshoz vagy egy adatunkhoz való hozzáférésre gondolunk feltételezzük, hogy az biztonságos. A hozzáférési engedély általában hitelesítési eljárással jár. Amikor a jelszavainkat kezeljük vagy alkalmazzuk, mindig használjunk bizonyos bevált módszereket.

- Ne használjuk az alapértelmezésben megadott jelszavakat (nagyon elterjedt az elektronikus eszközök használatakor).
- A jelszavaknak erősnek, személytelennek, biztonságosnak kell lenniük, és ne használjuk fel ezeket újra meg újra.
- A jelszavakat rendszeresen módosítani kell.
- Ne használjuk ugyanazt a jelszót különböző szolgáltatásokhoz.
- Ne használjunk jelszó-emlékeztetőt.
- Tippek a biztonságos jelszó létrehozásához
    - Tartalmazzon számokat.
    - Használjunk vegyesen nagybetűket és kisbetűket benne.
    - Tartalmazzon speciális karaktereket Pl.: - *? ! @ # $ / () {} =. ,; :

Miután beléptünk tudnunk kell, hogy veszélyeztethetjük az adatainkat, ha nem tesszük meg a szükséges intézkedéseket. Nézzük meg mit csináljunk, amikor véglegesen vagy ideiglenesen befejezzük a munkafázisunkat:

- Zárjuk be a munkafázisunkat vagy változtassuk meg a felhasználót (abban az esetben, ha a gazdagépnek több fiókja van, vagy egynél több felhasználó használja a böngészőket, webszolgáltatásokat, stb.).
- Ha csak rövid időre hagyjuk el a számítógépet, akkor is zárjuk le a képernyőt, hogy más ne férhessen hozzá a fájljainkhoz vagy az éppen használt alkalmazásainkhoz.
- Annyira jól kell konfigurálnunk az alkalmazásokat, böngészőket, szolgáltatásokat, amennyire csak lehetséges, hogy automatikusan eltávolítsák a helyben tárolt kapcsolati adatainkat a különböző alkalmazásokból (általában az adatvédelmi beállításokban tehetjük meg), vagy ha ez nem lehetséges, akkor töröljük manuálisan.

A jelszavak szokásos használatának egyéb alternatívái:

- Ellenőrzés két lépésben: ez nem egy másik alternatíva a jelszóra, hanem egyfajta megerősítés, amely növeli a biztonságot. Kettős ellenőrzésen alapul: az „amit tudunk” (a jelszó) együtt van az „amik vagyunk”-kal vagy „valami, amink van”-nal. Ez a második tényező többnyire egy szöveges üzenetben (SMS) vagy emailben kapott kód.
- Az ujjlenyomat használata a jelszó alternatívájaként az okostelefonok fejlesztésének köszönhetően jelentősen megnövekedett.
- Egyéb biometrikus adatok, például íriszfelismerés, arcfelismerés, pulzusszám stb.
- Egyedi és ideiglenes jelszó használata. A rendszer véletlenszerű ideiglenes kódot generál, amely szöveges üzenetben (SMS) érkezik minden alkalommal, amikor bejelentkezünk.

Mit jelent a többszintű hitelesítés?

A biztonságos hozzáférés a készülékeinkhez mára már elvárás. Nyilvánvaló, hogy a kontrollálatlan hozzáférés nem a legbiztonságosabb módja annak, hogy az adatainkat megőrizzük vagy megvédjük a manipulációtól. Éppen ezért az operációs rendszerek, az alkalmazások, a felhőtárolók stb. biztonsága egyre hatékonyabbá válik garantálva, hogy annyira biztonságosak legyenek, amennyire csak lehetséges.

A hozzáférés szabályozása több változáson ment keresztül az idők során, ami arra késztette a felhasználókat, hogy új, biztonságosabb jelszavakat hozzanak létre, és **többszintű hitelesítést** használjanak.

A többszintű hitelesítés egy olyan hitelesítési módszer, amely több, mint egy tényezőn alapul: valami, amit a felhasználó ismer (PIN-kód, jelszó), valami, amit a felhasználó birtokol (USB-csatlakozó, koordináta kártya) és valami, ami maga a felhasználó (viselkedés vagy fizikai tulajdonság: ujjlenyomat, írisz, hang vagy arc), esetleg ezek egyes kombinációi.

A közösségi médiában mindig igyekezzünk a lehető legmagasabb szintű biztonságot beállítani. Ha az általunk használt szolgáltatások nem teszik lehetővé ezt a biztonsági módszert, köztes megoldásként mindig használhatunk jelszókezelőt (ingyeneset vagy fizetőset), amely engedi a kétszintű hitelesítést. Ezt nem szabad összekevernünk a kétlépéses ellenőrzéssel.

A két lépéses hitelesítésben az első lépés általában jelszót és egy második tényezőt tartalmaz, például egy jelszógenerátorral (külső vagy belső eszköz) készített véletlen kódot. A szoftveralapú kódgenerátorok egyszer használatos jelszót hoznak létre, amiket asztali vagy mobilalkalmazások használnak.

Forrás: https://szamitastechnikarol.blog.hu/2019/03/24/ket_lepesre_vagy_a_teljes_biztonsagtol

1.5 Tűzfalak szerepe, felépítése

A tűzfal olyan rendszer (lehet hardver vagy szoftver, vagy mindkettő egyidejűleg), amely lehetővé teszi számunkra, hogy megvédjük készülékünket vagy készülékcsoportunkat az internetről származó lehetséges veszélyektől. Megakadályozza a nem-hitelesített hozzáférést, a hitelesítettet viszont engedélyezi.

A tűzfal egyfajta akadályként szerepel a számítógép és a külső hálózatok között. Beállítható az olyan opciók listájából, amelyek lehetővé teszik bizonyos meghatározott portokról származó átvitelek elfogadását, vagy pedig letiltják azokat.

Még ha könnyen használhatónak tűnik is, nem szabad elfelejtenünk, hogy a tűzfal nem minden esetben segíthet. A tűzfal leggyakoribb korlátai a következők:

- a működési ponton kívüli, például az intézményünkből jövő támadások;
- az intézmény felhasználói, akik hozzáférnek a számítógépekhez és rossz szándékuk van (szenzitív adatok, fertőzések másolása, rosszindulatú programok telepítése stb.);
- „emberek félrevezetése”-támadások (pszichológiai manipuláció).

A tűzfal engedélyezi azokat a biztonsági sérüléseket, amelyeket szolgáltatások és protokollok okoznak. Ilyenek például az interneten közzétett szolgáltatások, amelyek beállítását figyelemmel kell kísérni.

Fontos, hogy helyesen végezzük el a tűzfal beállításokat, hogy lehetővé tegyük az olyan alkalmazások, szolgáltatások stb. forgalmát, amelyek megbízhatóak, és kizárjuk a gyanúsakat.

Ami bennünket, tanárokat érdekel, mind egyénileg a munkánkban, mind pedig abban, amit a diákoknak tanítunk az eszközvédelemről, azok a személyes tűzfalak:

- **Windows**: Egy olyan installált tűzfallal jár, ami engedélyezi vagy blokkolja az alkalmazásokat, protokollokat és/vagy portokat.
- **MacOS**: Nagyon hasonló a Windowshoz. ***https://support.apple.com/es-es/HT201642***
- **Linux**: A Linuxnak van egy IPtables nevű tűzfala, amely benne van az operációs rendszerben. Ezzel beállíthatjuk az alapértelmezett szabályokat, szűrhetjük a forgalmat bizonyos portokon keresztül, és blokkolhatjuk egy másik személy IP-jét vagy MAC-jét, valamint a bejövő és kimenő kapcsolatokat.
- **IOS**: Az alapértelmezés szerint az IOS-ban nincs tűzfal. Ahhoz, hogy legyen, egy olyan külső alkalmazást kell telepíteni, amely megkíván egy telepített JailBreak alkalmazást (olyan alkalmazás, amely lehetővé teszi számunkra, hogy adminisztrációs ellenőrzést kapjunk a telefonunk felett).
- **Android**: Nincs alapértelmezett alkalmazása vagy konfigurációja, és az összes portja nyitott. Az IOS-hoz hasonlóan a tűzfal megváltoztatásához telepíteni kell egy rootbeállító alkalmazást. Van néhány kivétel, mint például a ***“Firewall without root”*** (=„Tűzfal root nélkül”)-applikáció, amely, ahogy a neve is jelzi, nem igényel root jogosultságokat.

Fizikai biztonság (külső tárolóeszközök)

A külső eszközök mindig veszélyforrást jelentenek az adataink számára. USB-eszközökön keresztül történő fertőzés akkor következik be, amikor a fertőzött fájlokat a számítógépünkre másoljuk egy USB-ről. A tűzfal nem lép fel ellenük, és néhánynak sikerül elkerülnie a vírusirtó bekapcsolását, mert úgy viselkedik, mintha hardver lenne. Minden, amit a fentiekben említettünk, előfordulhat más külső eszközök, mint például merevlemez, memóriakártyák, stb. esetében is.

Mit tehetünk?

Fontos óvintézkedés, hogy ne telepítsünk talált vagy ellenőrizetlen eszközöket. Ilyen esetekben ugyanis megkockáztatjuk olyan programok háttérben történő telepítését, amelyek károsíthatják vagy ellophatják az adatainkat (USB-hackelés). Legtöbbjük önállóan működik, így amikor bekapcsoljuk az eszközt, a parancsok, melyeket a támadó előre beprogramozott, szabadon garázdálkodnak a készülékben.

Az USB lemezekről való “automatikus lejátszás” tiltása megakadályozhatja néhány ilyen kártékony program működését, bár ez nem minden esetben működik.

Ahhoz, hogy megvédjük a merevlemez-adatokat, az USB-eszközöket, memóriakártyákat stb., titkosítsunk (rendszerint az összes operációs rendszer megadja a lehetőséget a titkosítás alkalmazására), és védjük meg őket az általunk választott jelszóval. Ez jól fog jönni abban az esetben, ha a fizikai eszköz netán elveszne vagy ellopnák.

Hol?

Védhetjük adatainkat a fenyegetettségtől külső eszközökön keresztül is, amelyek a Windows GPO-szabályzatát használják.

Ha az eszköz fertőzött és a víruskereső valós idejű szkennelésre, vírusirtásra és rendszerindítási ellenőrzésre képes, a hatékonysága jobb lesz, mert a víruskereső megakadályozza a fertőzést még azelőtt, hogy az betöltődne a szolgáltatásból vagy a programból, és így megelőzi a károsodást és megkönnyíti annak eltávolítását.

A kivehető eszközök alkalmazásának esetén az USB Disk Security alkalmazás megakadályozhatja az USB-hozzáférését a készülékünkhöz, az USB-kapcsolat vezérlését, az USB-szkennelését, a biztonságos URL-hitelesítést és karanténba teszi a nem biztonságos fájlokat.

1.6 Eszközeink fizikai védelme

Végül, de nem utolsósorban, beszéljünk a digitális készülékeink védelméről. A kioldási mintákba vetett túl nagy bizalom oda vezethet, hogy azt hisszük, nem jelent veszélyt nekünk, ha a mobiltelefonunkhoz mások is hozzáférhetnek. Azonban mindig vannak olyanok, akik, ha meg tudják szerezni a készüléket, képesek hozzáférni az adatokhoz.

Mit tehetünk?

Természetesen ne mutassuk meg senkinek sem a biztonsági rendszerünket, sem a mintázatot, sem a jelszót. Ez kötelező érvényű. Ne engedjük, hogy egy harmadik fél hozzáférjen a telefonunkhoz.

Hol?

Android készülékek esetében, hogy ne kelljen megrajzolni a mintánkat, konfigurálhatjuk azt a Beállítások / Biztonság menüponttal, és így védve leszünk a rossz szándékú emberektől.

Minden eszköz más és más hozzáférési garanciát kínál, ezért az eszközeinket és azok biztonsággal kapcsolatos előnyeit kötelezően meg kellene ismertetni az eszközvásárláskor.

Az alapszabály minden esetben az, hogy ne hagyjuk az eszközöket nyitva, amikor nem tudjuk őket magunkkal vinni, és ne osszuk meg egy harmadik személlyel. Nem bizalmatlanságról van szó, hanem a biztonságra vonatkozó védelemről.

2. KOCKÁZATOK ÉS VESZÉLYEK A DIGITÁLIS KÖRNYEZETBEN

Az Európai Unió azt határozta meg, hogy a jövő európai polgárainak képesnek kell lennie a digitális környezetben előforduló kockázatok és veszélyek felismerésére és meg kell, hogy védje magát tőlük. A cél az, hogy a tudásunk fejlesztésével észre tudjuk venni a problémákat, megoldásukra biztonsági intézkedéseket tudjunk alkalmazni, amelyeket azután megtaníthatunk a diákjainknak.

2.1 Bevezetés a digitális kockázatokba és veszélyekbe

Tekintsük át elsőként azt, hogy a mai digitális környezetben melyek a leggyakoribb veszélyek és biztonsági kockázatok, amelyekkel szembe kell néznünk:

Rosszindulatú programok:

- **Vírus**: rosszindulatú futtatható kód, amely más futtatható fájlokhoz van csatolva és általában helyettesíti azokat. A készülék megfertőzéséhez az kell, hogy valaki megpróbálja futtatni a programot.
- **Féreg**: emberi beavatkozás nélkül sokszorozódik, kihasználva a biztonsági réseket. Nem változtatja meg a programokat, de mivel a RAM memóriában van, gyorsan másolódik át az egyik számítógépről a másikra, és lelassítja a hálózatot, valamint a csatlakoztatott eszközöket.
- **Trójai programok**: legális szoftvernek álcázva rosszindulatú tevékenységet végeznek, hogy a támadó távolról hozzáférjen a fertőzött számítógéphez.
- **Zsaroló programok**: olyan programok, amelyek blokkolják a számítógéphez való hozzáférést addig, amíg váltságdíjat nem fizetnek. Általában féregként (sebezhetőség kiaknázása) vagy trójai programként (letöltött fájl) terjednek.
- **Kémprogram**: Az operációs rendszert módosító szoftver, amely hátsó ajtót hoz létre, hogy lehetővé tegye a készülékben az adminisztrátori jogosultságokhoz való hozzáférést, és közben állandóan rejtve marad a felhasználó elől.
- **Bot:** olyan szoftver, amely automatikusan ismétlődő műveleteket hajt végre, és rosszindulatú műveletek, például szolgáltatás-megtagadási támadások végrehajtására használható.

Email támadások:

- **Kéretlen levelek** (spam): az interneten küldött kéretlen üzenetek, amelyek reklámozás, adathalászat, rosszindulatú programok terjesztése stb. céljából készülnek.
- **Adathalászat** (phishing): legálisnak álcázott csaló emailek.

Böngésző veszélyek:

- **Kémprogramok** (spyware): kémkedés a felhasználó után.
- **Kéretlen reklámprogramok** (adware): hirdetéseket továbbítanak (általában kémprogramokkal).
- **Scareware**: meggyőzi a felhasználót, hogy félelemből egy konkrét cselekvést végezzen.

2.2 Kéretlen email: A spam

A spamek kéretlen üzenetek, amelyeket reklámozással, adathalászattal, kártékony programok terjesztésével stb. küldenek az interneten keresztül. A tanulmányok azt mutatják, hogy a kapott emailek legalább 80% -a spam. Ez komoly nehézséget jelent az internetszolgáltatók számára és nekünk, mint felhasználóknak szintén, mert sok időt pazarlunk el az emailek ellenőrzésére. A spam emailek első lépésként használhatók email címek gyűjtésére a későbbi és veszélyesebb támadások végrehajtásához (adathalászat, rosszindulatú programok, stb.).

A közösségi hálózatok népszerűségével nehezebb megkülönböztetni a törvényes és a csalárd emaileket egymástól.

Forrás: https://piacesprofit.hu/kkv_cegblog/elet-a-spamen-tul-szakertoi-tippek/

Védekezés a spamek ellen

Lássunk néhány alapvető intézkedést, hogy megvédjük magunkat a spamek ellen, és tanítsuk meg a diákjainknak is, hogyan kell védekezniük:

- Legyünk diszkrétek. A biztonság és az adatvédelem egyik alapvető szabálya az, hogy ne adjunk meg több információt, mint amennyire feltétlenül szükség van.
- Használjunk külön email fiókokat a különböző célokra. Például ne adjuk meg a fő email fiókunkat ingyenes szolgáltatásokra vagy fórumokra történő regisztráláskor.
- Tiltsuk le a HTML emaileket, vagy úgy állítsuk be az emaileket, hogy elkerüljük a HTML automatikus megjelenítését, vagy képek és csatolmányok letöltését.
- Állítsuk be az email szoftverünkön a **spamszűrőt**, és mindig frissítsük a víruskeresőnket, telepítsük le a rendszer és az alkalmazások legújabb biztonsági korrekcióit, és aktiváljuk a személyes tűzfalunkat.

2.3 Hamis email: adathalászat

A szélhámosok leginkább az adathalász emaileket használják, és egyre kifinomultabbak, egyre nehezebb felismerni őket. Az emailek adathalászatának fő célja, hogy pénzt szerezzen az áldozatoktól azáltal, hogy megtéveszti őket egy olyan emailben, amelyben általában egy harmadik személynek álcázva (bankként, biztosítótársaságként, fogadóirodaként, közösségi hálózati képviselőként, munkahelyi részlegként, stb.) kérnek bizalmas személyes információkat (pl. bankszámlaszámról, felhasználókról és jelszavakról stb.). Nem csak pénzt vehetnek fel, hanem ellophatják a személyazonosságunkat, vásárolhatnak, sőt kereskedhetnek is az ellopott információkkal.

Forrás: https://www.invitech.hu/techpercek/az-adathalaszat-a-legveszelyesebb-a-munkatarsakra

Tanulságos az alábbi videó, melyet ajánlunk a tananyaghoz: Riasztás, adathalászok

3. A DIGITÁLIS TARTALOM VÉDELME

Digitális eszközeink megóvásának megtanulása során azonosítottuk a különböző „napi használatú szolgáltatásokban" előforduló veszélyeket, például: nyilvános wifi esetén hotspotokban, levelezésben, csevegésekben, stb. Ebben a részben itt az ideje megtanulnunk, hogyan védjük meg a digitális tartalmat a közvetlen behatolóktól, a fizikai adathordozó tönkretevésétől és ellopásától.

Először kezdjük azzal, hogy felidézzük a leggyakoribb információtároló területeket, megértjük, hogy milyen különbségek vannak az információk különféle helyen történő mentésében, és megőrizzük adataink teljességét.

3.1 A digitális tartalom biztonságos tárolása

Lehetőségeink adataink tárolásához:

- notebook számítógép;
- optikai lemezek (cd, dvd, bluray, hd-dvd stb.);
- flash memóriák (pendrive-ok, sd-kártyák stb.);
- mágneses merevlemezek;
- kemény burkolatú merevlemezek;
- távoli szerverek;
- felhőtárhelyek.

Tároló segédeszközök

A legtöbb ismerős számunkra. Nagyon gyakran mentünk, mozgatunk és továbbítunk ezekkel a segédeszközökkel, anélkül, hogy teljesen tisztában lennénk a korlátaikkal. Ha megkérdeznénk: „Tárolnánk-e az információinkat csupán egyetlen eszközön, például egy pendrive-on?", indokoltnak tűnik a "NEM" válasz. Ez azért van, mert tudjuk, hogy valami, ami olyan praktikus, mint egy pendrive, elveszhet, eltörhet, megsérülhet, tönkremehet, elavulttá válhat, vagy ellophatják. Mi tehát a legjobb adat tárolási stratégia?

3.2 Az eszközökre vonatkozó adatok titkosítása és jelszavas védelem

A biztonság első szintjén számos lemez és flash memória tartalmaz egy kis szoftvert, amely lehetővé teszi a felhasználó számára, hogy titkosítsa a hardver tartalmát, és egy belső fájlkezelőn keresztül tegye hozzáférhetővé. Ezt a fájlkezelőt is megvédhetjük jelszóval. Könnyen megérthető, hogy milyen hasznos a titkosítás: ha a készülékünket ellopják, az információ nem érhető el mások számára. Ennek az az oka, hogy a fizikai információk elrendezése nem értelmezhető az operációs rendszernek kivéve, ha az eszköz belső fájlkezelője azt korábban már dekódolta. Ennek ellenére az információink biztonsága nem függhet kizárólag ettől.

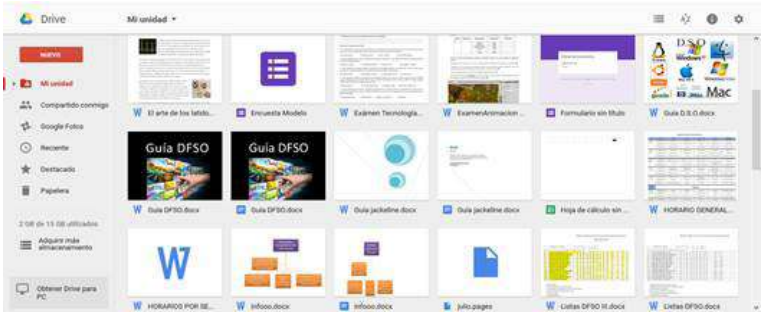
A fájlkezelőkön kívül az operációs rendszernek olyan eszközei is vannak, amelyek képesek a fájlok és mappák titkosítására. A saját fájlok és mappák titkosításához a Windows operációs rendszer esetében itt talál a segítséget: ***https://techwok.hu/2019/05/09/legjobb-ingyenes-titkosito-program***.

Vannak távoli szerverek és szabad hely a felhőben az információk tárolására. Ezeken a helyeken az adataink várakozhatnak, sőt titkosíthatjuk is őket, de felhasználásuk számos lépést igényel ahhoz, hogy információink biztonságban maradjanak. Először is nézzük a különbséget a helyi tárolás és a felhőtárolás között.

3.3 A helyi és a felhőben történő tárolás közötti különbség

Helyi tárolásról akkor beszélünk, amikor a hardvert, ahol az információinkat tároljuk, közvetlenül elérhetjük.

Felhőtárolás akkor történik, amikor az adatainkat egy fizikai adathordozóra küldjük el úgy, hogy mi közvetlenül nem érhetjük el, de programok, alkalmazások vagy webes ügyfelek igen.



A Google Drive felhasználói felülete a felhőben lévő fájlok és mappák kezeléséhez

Tehát a felhő valójában jól szervezett (távoli merevlemezek, szerverek stb.) tárhelyek gyűjteménye, amelyet rajtunk kívülállók kezelnek. A felhasználó számára ez egy interneten keresztül elérhető virtuális tér, amelyben a dokumentumok és a számítógépes programok tárolódnak úgy, hogy az ugyanazon hálózathoz csatlakozó többi felhasználó is hozzájuk férhessen és használhassa azokat.

Információink ezeken a helyeken (szerverfarmok, lemezkészletek stb.) valóságosan ott vannak, és még ha teljes mértékben hozzá is férünk azok kezeléséhez, nem kell aggódnunk annak a fizikai térnek az állapotáért vagy kezeléséért, ahol az adatok találhatók.

Feltehetjük a kérdést, hogy azok a vállalatok, amelyek a felhőtereket kialakítják, ugyanúgy biztonságosak és megbízhatóak-e? Nyilvánvaló, hogy ez sokunkat fog érdekelni. Legalább annyi elvárható, hogy garantálják az ott feltöltött adatok integritását és hozzáférését.

3.4 Mit jelent az összehangolás?

Az összehangolás azt jelenti, hogy a fájlok, amiket a helyi eszközeinkben formálunk, ugyanazokat az állapotokat és változatokat tartják fenn, mint amit a felhőtárolóban találunk. Az összehangolás előnyös, mert az adatok ugyan helyi szintűek (gyors hozzáférés, nincs késleltetés stb.), de felhőben történt biztonsági mentéssel. A felhőszolgáltatók rendszerint tele vannak olyan alkalmazásokkal, amik segítik adataink összehangolását.

Mit kell összehangolni?

Az összehangolásban részt vevő minden helyi környezetnek van egy applikációja - vagy asztali alkalmazása -, amely fenntartja ezt az állapotot a helyi és a felhőszintű fájlok között. Ezeket az alkalmazásokat telepíteni kell az operációs rendszerünkben az összehangolás érdekében. Mindazonáltal magunknak kell megvizsgálnunk, hogy a fájlok megfelelően összehangoltak-e, figyelve az ikonokat (nyilak, ellenőrzések stb.) a tálcán, és azt, hogy az alkalmazás stabil állapotban van-e.

Az olyan asztali alkalmazások, mint például a One Drive, a Google Drive vagy a Dropbox meg tudják mutatni nekünk ezeket a státuszokat. Csak ellenőriznünk kell az igénybe vett szolgáltatás ikonjait, és a rendszerünk legértékesebb fájljait a tálcán.

Forrás: https://www.tmsi.hu/2017/11/27/felhotarolas-jelszo-kezelokhoz-ellene-vagy-mellette

3.5 A biztonsági mentés alapszabályai

A központoknak nemcsak biztonsági rendszerre van szükségük az adatok megőrzéséhez, hanem bizonyos módszerekre is, arra az esetre, ha netán komoly adatvesztés történne. Különböző típusú biztonsági másolatok léteznek, és célszerű tudni, hogy melyik a legjobb számunkra. Négy különböző típusú biztonsági mentés létezik:

- **Teljes biztonsági mentés:** ahogy azt a név is sugallja, az ilyen típusú biztonsági mentés minden adatra kiterjed.
- **Differenciálmentés:** csak azokról a fájlokról készít másolatot, amik az utolsó mentés után készültek. Ezért csak új és/vagy módosított fájlokat tartalmaz.
- **Inkrementális mentés:** az utolsó teljes, differenciált vagy növekményes biztonsági mentés óta módosított összes fájl másolatát menti. A leggyorsabb módszer a biztonsági másolatok készítéséhez.
- **Tükörmentés:** hasonló a teljes biztonsági mentéshez, de itt a fájlokat nem tömörítik, és nem lehet jelszóval védeni. Ezért több helyet foglal el, és kevésbé biztonságos.

3.6 A felhő használata és beállítása

Mindegy, hogy milyen felhőszolgáltatást használunk (Google Drive, One Drive, DropBox, iCloud, Amazon Home Drive, stb.), mindegyik ugyanúgy kezdi a kezelési és beállítások parancssorát.

Először is regisztrálunk egy email fiókot a kívánt felhőszolgáltatásra. Innen vagy jelszóval védett hozzáférést fogunk kapni a felhőhöz, vagy egy két lépésből álló azonosítást. Ez a hely egyenértékű egy olyan gyökérkönyvtárral, ahol a katalógusfát felépíthetjük, és a kívánt fájlokat tárolhatjuk a szolgáltató által kínált helyhatárokon belül.

A Google Drive felhasználói felülete a felhőben lévő fájlok és mappák kezeléséhez

A főbb opciók általában hasonlóak az asztali számítógépek, mobileszközök vagy táblagépek fájlkezelőihez:

- online együttműködési fájlok létrehozása (dokumentumok, táblázatok, prezentációk, rajzok, űrlapok stb.);
- mappák létrehozása;
- a meglévő fájlok vagy mappák feltöltése a helyi tárolóból;
- fájlok és/vagy mappák másolása és áthelyezése;

- fájlok és/vagy mappák törlése;
- a mappastruktúra kezelése és szervezése;
- a fájlok és/vagy mappák információinak lekérdezése;
- fájlverzió-kezelés.

Ide tartoznak a fájlmegosztással és a valós idejű munkákkal kapcsolatos lehetőségek, valamint azoknak a felhasználóknak az információi, akik kölcsönhatásba léptek az egyes mentett elemekkel:

- a fájlok és/vagy mappák engedélyeinek kezelése;
- jogosultság-beállítás és a felhasználók interakciója a fájlokban és/vagy mappákban (megjelenítés, megjegyzések és létrehozás).

Ugyancsak rendelkezünk majd a fiók biztonsági kezelésével, ahol egyedi bejelentkezési lehetőségeket állíthatunk be, és kiválaszthatjuk az azonosítás opcióját is a hitelesítésre.

Ne feledjük, hogy ha egy olyan fiókkal jelentkezünk be, ami hozzáférést biztosít a felhő tárhelyéhez, mindig zárjuk le a munkamenetet, amikor befejezzük a használatát, különösen, ha a munkánkhoz nyilvános eszközt használtunk.

Mindezeket diákjainknak is tudniuk kell, nemcsak azért, mert így megakadályozhatják az információlopást, hanem, mert így megelőzhetik a személyazonosság-lopással kapcsolatos bármilyen internetes zaklatást is.

4. A TECHNOLÓGIA FELELŐS HASZNÁLATA

A felelősségteljes technológia használatot ugyanolyan fontos elsajátítani, mint arra ösztönözni a diákjainkat, hogy egészséges és felelősségteljes szokásokat fejlesszenek ki a tömegtájékoztatási eszközökkel szemben.

Ebben a tananyagrészben áttekintjük a technológiai források használatával kapcsolatos kockázatokat, amelyekkel tanárként szembesülünk, és amelyekkel a diákjainknak is meg kell birkózniuk. Megismerkedünk néhány didaktikai útmutatással is, és hasznos anyagokat nézünk át, hogy beépítsük azokat a tanórába.

Forrás: www.Pixabay.com

4.1 Kockázatmegelőzés és a technológiák felelősségteljes használatának előmozdítása a fiatalok körében

A mai digitális társadalomban, amelyben együtt van jelen a virtuális és a valós környezet, fontos az egyének megfelelő és felelősségteljes bevonása, és hogy tudatában legyenek a technológia kínálta lehetőségeknek és kockázatoknak.

A kompetens és felelősségteljes digitális állampolgárság megteremtése érdekében azonban szükséges képzés indítása, a tudatos technológiahasználatra való felkészítés.

Nem lenne értelme úgy elkerülni a kockázatokat, hogy megtiltjuk, illetve korlátozzuk a fiatalok eszközhasználatát, inkább engedjük, hogy önállóak legyenek, de támogatóként mellettük vagyunk, és képezzük őket.

A felnőtteknek kísérniük és irányítaniuk kell a gyerekeket és a fiatalokat a digitális világban. A felkészítés, a képzés nem korlátozódhat az online védelem technológiáinak és technikáinak ismeretére, hanem ki kell terjednie a virtuális világban a tisztességre és a megfelelő bánásmódra vonatkozó szabályokra is, továbbá az érzelmi oktatásra, amelynek célja az önállóság, az empátia és a kritikus gondolkodás.

Ez a Save the Children szervezet álláspontja (2017.) a felelősségteljes digitális állampolgárság elősegítéséről, a megelőzés iránti elkötelezettségről és a felelősségteljes használat előmozdításáról a pedagógusok és a családok számára adott fontos tanácsokkal és útmutatással.

Csak így lehet kihasználni a technológia által kínált lehetőségeket a hiányosságok csökkentése és az esélyegyenlőség biztosítása érdekében.

Alapvető fontosságú, hogy irányítói szerepet töltsünk be a digitális kompetenciáik fejlesztésében annak érdekében, hogy felelősségteljes digitális állampolgárokká váljanak.

4.2 Technológiák felelős használatának irányelvei az iskolákban

Az oktatási intézmények, akárcsak más szervezetek, figyelembe veszik a technológia használatából eredő kockázatokat. Az iskolai környezetben nagy mennyiségű személyes információt kezelnek, és a munka lényegében kiskorúakra összpontosít, így iskolai szinten szükség van a technológiák felelősségteljes használatára vonatkozó irányelvekre. Ebben a szabályzatban a megelőzési és a felelősségteljes felhasználás előmozdításához szükséges stratégiákat kell kidolgozni, valamint olyan protokollrendszert, amely előírja, hogy milyen lépéseket kell tenni, ha az oktatási közösség bármilyen konfliktushelyzetbe kerül, vagy nem megfelelően használja a technológiát. Ez egyenértékű bármely vállalat biztonsági akciótervével.

Ahhoz, hogy a központ irányelveit meg lehessen alkotni, a következők szükségesek:

- Kezdjük az információ jelenlegi szintjének meghatározásával, és állítsunk fel stratégiai célokat.
- Elemezzük az iskolára általában irányuló potenciális kockázatokat.
- Határozzunk meg követendő, kiberbiztonságilag jó megoldásokat.
- Adjunk meg olyan tervezett intézkedéseket, amelyek szóba jöhetnek a megelőzésben, és amelyek reakcióként is alkalmazhatók problémák esetén.

Fontos szem előtt tartani, hogy a szabályok kidolgozása és alkalmazása az oktatási közösség valamennyi tagjának összehangolt és konszenzuson alapuló munkája kell, hogy legyen a hatékony alkalmazás érdekében.

A központ irányelvei mellett fontos, hogy technikai jellegű megelőző intézkedéseket vezessünk be, például a technológiák használatával:

- A dokumentáció és a személyes adatok archívumának beállítása a jelenlegi adatvédelmi előírásoknak megfelelően.
- A tanárok és a diákok által használt számítógépes berendezések beállítása, amelyek szűrők és víruskeresők használatával garantálják a biztonságot az információszivárgások elkerülése érdekében.
- Az internetkapcsolat beállítása, amely biztosítja a biztonságos hozzáférést a wifi-hálózaton keresztül.

4.3 Hogyan alakítsunk ki tanulói tevékenységeket a technológiák felelős használatának elősegítése érdekében?

A diákjaink digitális társadalomban élnek, és naponta használják a technológiát, megosztják személyes adataikat, hozzáférnek másokéhoz, aktívak a közösségi hálózatokban, és különböző eszközöket használnak tanulmányi és rekreációs célokra.

Ez olyan helyzet, amely előnyöket és kockázatokat is rejt. Ezért a mi feladatunk, hogy tanárként ösztönözzük a technológiák felelősségteljes használatát. Függetlenül attól, hogy számítástechnikai tantárgyak tanárai vagyunk-e vagy sem, szükség van arra, hogy az osztályainkban integráljuk a technológiát az alapvető pedagógiai és technikai elvek alapján, hogy ezzel támogassuk a diákok digitális kompetenciájának fejlődését. Ez szükségszerűen magában foglalja az internetbiztonság és a felelős használat stratégiáinak integrálását is.

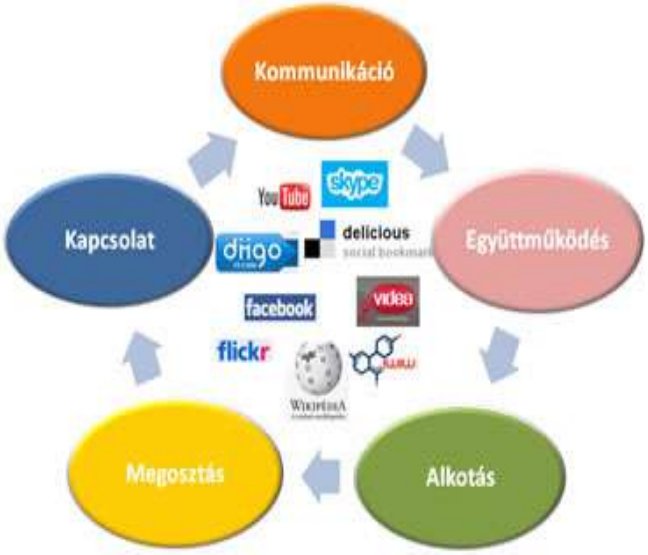
Pedagógiai szinten speciális tevékenységek alakíthatók ki a technológiák kockázatainak és előnyeinek megértéséhez, valamint az eszközök felelősségteljes használatához. Ha azonban nincs erre idő, integrálhatjuk a felelősségteljes felhasználási stratégiákat minden olyan tevékenységben, amely a technológiai erőforrásokkal foglalkozik.

Az alábbiakban bemutatott didaktikai forrásokban példákat találhatunk a hatékony biztonsági stratégiákat tartalmazó, középiskolai oktatásba bevonható konkrét tevékenységekről. Ne feledjük, hogy ezekbe a tevékenységekbe bele kell foglalni a fogalmakat, az eljárásokat és az elvárt viselkedést, hogy megkönnyítsük a diákok számára a technológiák használatát, így lehetőséget adva arra, hogy reflexív módon alkossanak, feltaláljanak és megoszthassanak dolgokat, a csupán fogyasztói felhasználói szerepen túlmenően.

E célból ajánlott olyan, a valós élethez kapcsolódó, tapasztalati helyzeteken alapuló didaktikai módszereket alkalmazni, amelyek elősegítik a tudás aktív elsajátítását, és ezáltal lehetővé teszik a személyes és kollektív elemzést és a visszajelzést. Ne feledjük, hogy mindez középiskolákban és szakgimnáziumokban történik, olyan diákok körében, akiknek már van technológiai hátterük. Következzen néhány didaktikai módszer, amely hasznos lehet a számunkra:

- **Projektalapú tanulás**: Egy olyan reális projekteken alapuló, erősen motiváló kérdésre, feladatra vagy problémára épülő tanítási modell, amely közvetlenül kapcsolódik egy ismert kontextushoz, és amelyen keresztül a diákok együttműködve fejlesztik kompetenciáikat a megoldások keresése során.
- **Esettanulmányok**: Egy sor konkrét esetet mutatnak be tanulmányozáshoz és elemzéshez, amelyek különböző, valós életbeli problémákkal foglalkoznak. A projektalapú tanulástól annyiban különbözik, hogy teljes körű tájékoztatást nyújt az esetről és annak megoldásáról, irányvonalakat szab, szemben a sokkal nyitottabb, projektalapú megközelítéssel, amely a hallgatók részéről nagyobb autonómiát igényel.

- **Együttműködő tanulás:** A diákok koordinált módon, együttesen dolgoznak egy közös cél megvalósítása érdekében, felelősségi körök és egyértelműen meghatározott kölcsönhatási szabályok alapján.
- **Játékalapú tanulás:** Szabadidőn kívüli technikák, elemek és játékdinamikák együtteséből áll, amely növeli a motivációt, és segíti a problémamegoldó magatartást.



Forrás: https://www.sulinet.hu/iktmuhely_2010/ikt_az_oktatasban.html

4.4 Hogyan segíthetjük a diákok szüleit a technológia felelős használatának ösztönzésében?

A családok szerepe elengedhetetlen a digitális társadalom bevezetésében és a technológia felelős használatának előmozdításában. A gyerekek már nagyon korán együtt élnek a különböző technológiai erőforrásokkal, ennek ellenére szükségük van a családjuk támogatására és irányítására önállóságuk és kritikai gondolkodásuk fejlesztése érdekében.

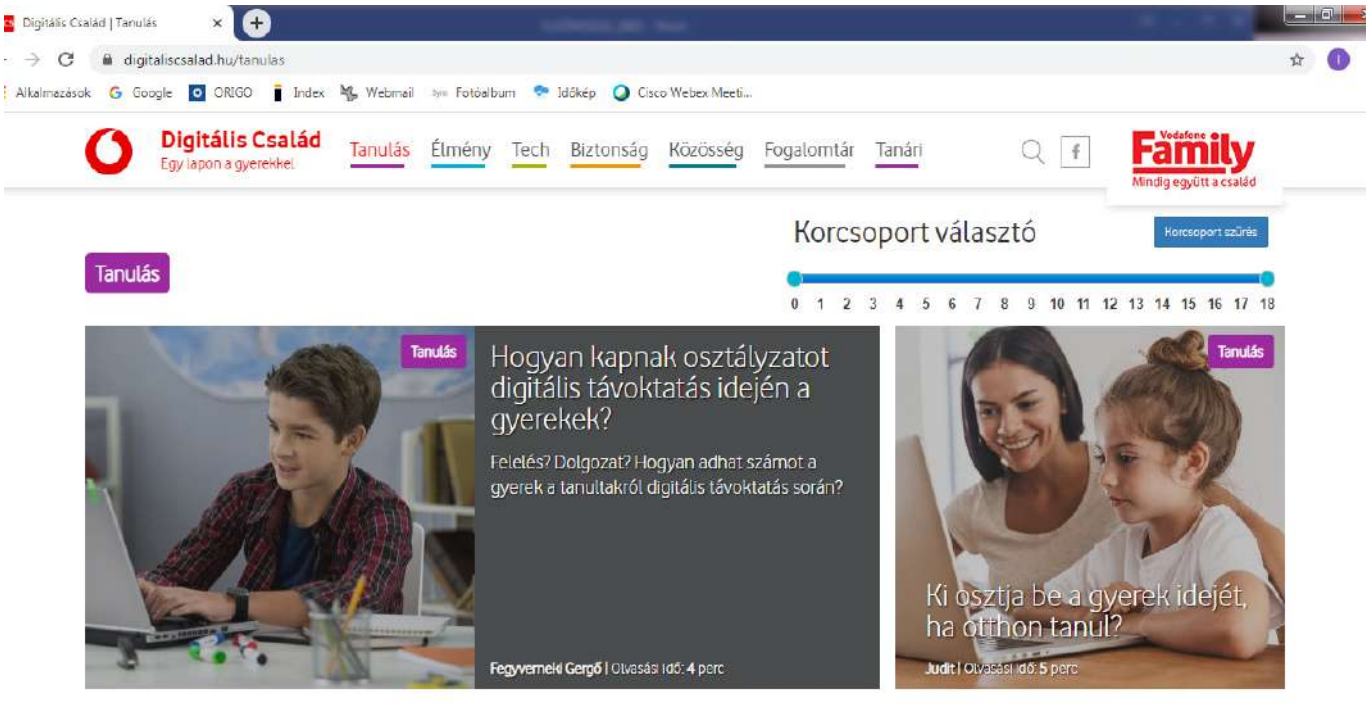
Gyerekkori sajátosságaik következtében: kíváncsiságuk, túlzott bizalmuk és a kísérletezés iránti vágyuk miatt gyakran alábecsülik a kockázatokat, amelyekkel szembesülhetnek. Emiatt itt felsorolunk néhány, a szülőket leginkább érintő szempontot:

- a különböző forrásokhoz (pl. mobiltelefonok, internetes böngészés vagy közösségi hálózatok) való hozzáférés optimális életkora;
- szükséges iránymutatások annak érdekében, hogy gyermekeiket a rendelkezésükre álló erőforrások megfelelő használatára ösztönözzék;
- egészséges egyensúly a technológiai és analóg tevékenységek között a lehetséges függőségi problémák elkerülése érdekében;
- a technológia használatának hatásai a tanulmányi teljesítményre vagy a kognitív funkciókra, például a koncentrációra, a döntéshozatalra vagy a pszichomotoros készségekre.

Tanárként a szerepünk nagyon értékes lehet a családok támogatásában, és mint minden oktatási tevékenységben, az iskola és a család összehangolt fellépése garantálja a sikert. E célból a tanárok és a családok között különböző koordinációs módokat kínálnak a gyermekeknek a felelős technológia etikus használatának elősegítésére:

- Tartsunk folyamatos és kölcsönös kommunikációt a tanári csapat és a családok között annak érdekében, hogy nyomon lehessen követni a viselkedésváltozásokat, amelyek a technológia helytelen használatából adódó problémát jelezhetik. Ezt a kommunikációt a technológiai erőforrások, például mobilalkalmazások segítségével lehet előmozdítani. Mindenesetre ezt a kommunikációt ne tekintsük a tanulók fölötti ellenőrzésnek. A diákokkal való kommunikáció elengedhetetlen, de hangoljuk össze a családokkal.
- Az informális és/vagy formális tevékenységek kifejlesztése az iskolában és az iskolán kívüli technológia felelősségteljes használatának előmozdítására megcélozza mind a kiskorúakat, mind a szüleiket, akik aztán referenciaként fogják használni.
- A szülőknek adjunk olyan útmutatást, amik segíthetnek nekik a döntéseik meghozatalában, és készítsünk iránymutatást a technika helyes használatára otthonra, mint pl. útmutatót, infografikát. Fontos végiggondolni e dokumentumok formátumát, hogy azok könnyen olvashatóak és hasznosak legyenek, valamint hogy annyira segítsék az egyeztetést, amennyire csak lehetséges.
- Összehangoltan járjunk el, amikor gyermekeink helytelenül használják a technológiát, lehetőleg egyénileg, egyeztető és megoldó hozzáállással.

A következő WEB-lap cikkeit minden szülő számára ajánljuk[4]:



4 További ajánlásokat találnak a II. fejezet 2.1 részében közzétett „TEMATIKUS GYŰJTEMÉNYBEN”

4.5 A technológia pozitív felhasználása

Fontosnak tartjuk kiemelni a technológiák néhány pozitív felhasználását. Megismerhetjük hogyan ösztönözhetjük a technológiák felelősségteljes használatát a diákjainkkal, képesek leszünk tanárként kiaknázni az oktatási és szociális előnyöket is.

A web 2.0 alkalmazások kifejlesztésével az internet nemcsak egy nagyszerű könyvtár lett, hanem óriási lehetőség is az internetes felhasználóknak. Ily módon nem vagyunk többé passzív befogadói az információnak, a tanulóink rendelkezésére állnak az ötleteik, projektjeik és munkájuk megoldására és másokkal való megosztására. A technológia által kínált oktatási lehetőség pl. a következő lehet:

- Hozzanak létre egy olyan webhelyet, amelyet a tanulók egy adott témakörrel töltenek meg.
- Végezzenek a diákok egy tudományos kutatást és próbáljuk meg közzétenni a Wikipédiában.
- Kezdeményezzenek egy olyan online projektet, amelyben a diákok közösségi vezetőkként működnek értékes információkat terjesztve.

A mobil technológia bővítése lehetővé tette az azonnali hozzáférést gyorsan és kényelmesen, és növelte a szocializációs és kommunikációs lehetőségeket. Közösségi hálózatokon keresztül bármikor és bárhol kommunikálhatunk más emberekkel, megoszthatunk ötleteket és véleményeket. Ez lehetővé tesz számunkra néhány érdekes felhasználást az oktatásban:

- Kérjük meg a tanulókat, hogy készítsenek interjút egy adott témával foglalkozó szakértővel. Ehhez meg kell keresniük ezeket a szakértőket a hálózaton, kommunikálni velük, és kérniük kell az együttműködésüket ahhoz, hogy személyes vagy online interjút készítsenek.
- Kezdeményezzünk dinamikus kommunikációt a diákokkal olyan közösségi hálózatokon keresztül, mint a Twitter, hogy ösztönözzük a kíváncsiságukat és kutatásukat a témában.

A technológia szórakozásra is jó: az interaktív és játékos alkotóelemek vonzóvá teszik a diákok számára. A figyelmüket és érdeklődésüket megragadó eszközök ismerete és használata nagyban segít motivációjuk előmozdításában. A legfontosabb az, hogy tudjuk, hogyan kell kihasználni őket a tanulási és oktatási folyamat javára. Íme egy ötlet ehhez !

- Készítsünk „szabaduló szoba" játékot a tanulókkal együtt és próbáljuk ki azt. [5] (Legyen a téma a „Digitális biztonság"!).

Használjuk ki a tanulók tanulásában és integrált fejlődésében mindazt, amit a technológiák kínálnak. A gyakran használt technológiák kedvező előnyöket kínálnak mind magunknak, mind a diákjainknak.

5 E könyv II. fejezetében találhatnak a tanárok által készített minták között is megfelelőt, melyet csak kipróbálni kell

ÖSSZEFOGLALÁS

Ebben a fejezetben elkezdtük a technológiák életünkre gyakorolt hatásának elemzését, tágabb, szociológiai szemléletet is mutatva működésükről és hatásukról.

Eszközeink és adataink biztonsága sok tényezőtől függ. Ha szoftverünket minden szinten frissítettük: operációs rendszert, böngészőket, alkalmazásszoftvereket stb., és ha telepítettünk addonokat és erre szolgáló szoftvert, a védelmünk mindig garantált lesz. Ugyanúgy, ahogy a hozzáférési módszereink biztosítását megoldjuk, a csatlakozási adatok védelme is nehezebbé teszi az adataink elvesztését, lopását vagy sérülését / megsemmisítését. A jó tűzfal használata megakadályozza a rossz szándékú behatolók hozzáférését, valamint azt, hogy a kimenő információk a hálózatba jussanak.

Különösen fontos megemlíteni a józan észt és az információt abban az esetben, amikor a kapcsolati adatok védelmét a lehető legmagasabb szintű hitelesítéssel és a szükséges adatvédelemmel látjuk el.

A külső eszközök esetében nagyon fontos gondolni az adatok titkosítására, a véletlen veszteségekre vagy a lopásra, és megint csak hagyatkozzunk a józan eszünkre, ne pedig a promóciókra, esetleg ismeretlen eredetű eszközökre. Eszközeink sebezhetőek, ezért használjuk a tudásunkat, hogy a lehető legjobban megvédjük őket.

Néhány pozitív hatást elemeztünk, mint például a kommunikáció megkönnyítését és az információk egyszerű és gyors megosztását, ami lehetővé teszi az időbeli és térbeli korlátok feloldását. Más, kevésbé pozitív hatásokat is elemeztünk, mint például az információk manipulálása vagy a digitális jogsértés jelensége.

Elemeztük az iskolák szerepét egy olyan szabályrendszer meghatározásában, amely előnyben részesíti a technológia felelősségteljes használatát a lehetséges visszaélésekből eredő kockázatok elkerülése érdekében. Néhány javaslatot is felülvizsgáltunk, kiemelve azt, hogy a diákok alkalmazkodjanak az adatvédelmi jogszabályokhoz, mint pl. saját adataik védelme, a közösségi hálózatokon megosztott információk, vagy a mobileszközök használatának kezelése.

Az anyagban néhány szükséges útmutatót javasoltunk arra, hogy a diákokat a technológia felelősségteljes használatára ösztönözzük, valamint néhány tanácsot adtunk a családoknak, hogy segítsünk nekik a tantermen kívüli munka megerősítésében. Példák, az osztályteremben való alkalmazáshoz használt didaktikai anyagok és egyéb, nem iskolai környezetben végzett hasznos tevékenységek kerültek bemutatásra annak érdekében, hogy hatékonyan és összehangoltan előmozdítsuk azt, hogy a serdülők felelősen használják a számukra elérhető technológiai erőforrásokat.

Végezetül néhány ismeretszerzési, módszertani javaslattal zártunk: miként is aktivizáljuk és motiváljuk diákjainkat arra, hogy minél többet tudjanak a digitális biztonságról és felkészüljenek a felelősségteljes magatartásra a digitális „országúton” való biztonságos közlekedésre.

SZAKIRODALOM

1. Digitális eszközök használata oktatásban és nevelésben: ***https://www.digitalhungary.hu/e-volution/Digitalis-eszkozok-hasznalata-az-oktatasban-es-a-nevelesben/9050/***
2. ***Nákovics L. A biztonságos internetezés trükkjei: https://techwok.hu/2018/03/07/biztonsagos-internetezes-trukkjei/***
3. Biztonságos Internet Nap 2020. ***https://moderniskola.hu/2020/02/biztonsagos-internet-nap-2020-egyutt-egy-jobb-internetert/***
4. Hogyan legyenek a gyerekek és a tanárok biztonságban a digitális oktatás ideje alatt is? ***https://www.eset.com/hu/hirek/hogyan-legyenek-a-gyerekek-es-a-tanarok-biztonsagban-a-digitalis-oktatas-ideje-alatt-2020/***
5. A saját fájlok és mappák titkosításához a Windows operációs rendszer esetében itt talál a segítséget: ***https://techwok.hu/2019/05/09/legjobb-ingyenes-titkosito-program/***.
6. Bender, William (2014). Penso, ed. Aprendizagem Baseada em Projetos: educação diferenciada para o século XXI (en portugués). Porto Alegre, Brasil. p. 15. ISBN 978-85-8429-001-7.
7. Cañón, R., Grande, M. y Ferrero, E. (2018) Ciberacoso: revisión de la literatura educativa en español. Revista Latinoamericana de tecnología educativa. Vol. 17 Núm. 2 (2018). Recuperado de: ***https://doi.org/10.17398/1695-288X.17.2.87***
8. Comisión Europea. (2012). Comunicación de la comisión al parlamento europeo, al consejo, al comité económico y social europeo y al comité de las regiones. Estrategia europea en favor de una Internet más adecuada para los niños. OPOCE. Retrieved from ***https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52012DC0196&from=EN***
9. Hoffman, D.L, Novak, T.P. y Schlosser, A. E. (2001) The evolution of the digital divide: Examining the relationship of race to Internet access and usage over time. En Compaine, B. Digital Divide. Cambridge, Massachussets: The MIT Press
10. Save the Children. (2017). Acceso a las nuevas tecnologías de los menores de edad. Lekérve: ***https://www.savethechildren.es/sites/default/files/imce/acceso_internet_menores_edad_1.pdf***
11. Vuorikari, R., Punie, Y., Carretero Gómez, S., & Van Den Brande, G. (2016). DigComp 2.0: The Digital Competence Framework for Citizens. Update Phase 1: the Conceptual Reference Model. - European Commission. ***https://doi.org/10.2791/11517***

VIDEÓ

1. Riasztás, adathalászok: ***https://www.youtube.com/watch?v=XfyNmro0RUU***

2. MODUL: A SZEMÉLYES ADATOK ÉS A MAGÁNSZFÉRA VÉDELME

BEVEZETŐ

A technika térhódításával az ember mindennapi élete megváltozott: online intézhetjük a vásárlást és a pénzügyeinket, kapcsolatot tudunk tartani a rokonaikkal és a barátainkkal, az interneten foglalhatjuk le az utazásainkat, egészségügyi kartonjainkat digitálisan tárolják - személyes adataink ott vannak mindenütt az interneten nap mint nap létrehozott profiljainkban. A 2020-as világjárvány okozta globális karantén ezt az állapotot még jobban felerősítette: a digitális technika nagyban segítette emberek millióit abban, hogy életüket kicsit másképpen, de folytatni tudják otthonaikból, online.

A digitálisan felszerelt társadalom természetesen számos előnnyel jár. Ma már szoftveres megoldások segítik a termelékenységet, és – például a bürokrácia csökkentésével - lehetővé teszik számunkra, hogy több időt szenteljünk a saját jóllétünknek. Ez az előrelépés az adatokat és az információkat az életvitelünk és a gazdaság számára létfontosságúvá, rosszindulatú egyének számára pedig kívánatossá teszi. A technológia szenzációs fejlődésével párhuzamosan drámaian, napról napra emelkedik a technológiát használó internetes bűncselekmények száma, aminek borzasztó pénzügyi és pszichológiai következményei vannak. A kiberbiztonsági vállalatok feltételezései szerint a károk összege az egész világon még 2021. előtt eléri majd éves szinten a 6 milliárd dollárt, szemben a 2015-ös 3 milliárd dollárral. Az internetes bűnözők rugalmasnak, alkalmazkodónak, tanulékonynak bizonyultak, gyorsan elkezdik alkalmazni az új technológiákat ezen a sajnos nagyon jövedelmező és meglehetősen könnyű kriminológiai területen. Az átlagos felhasználók többsége még az alapvető óvintézkedéseket sem teszi meg, hogy megvédje magát tőlük, sőt, gyakran még a megfelelő internethigiénia sincs meg bennük: érzékeny adatokat és információkat szivárogtatnak ki magukról pusztán hanyagságból, nemtörődömségből. Ezzel pedig könnyű célpontokká válnak a kiberbűnözők számára.

Könyvünk ezen fejezete emiatt kiemelten foglalkozik az adatvédelemmel, illetve azokkal a tudni- és tennivalókkal, amiket Önnek magánemberként és tanárként ismernie, illetve diákjai számára tanítania is kell.

1. A SZEMÉLYES ADATOK ÉS A SZEMÉLYES INFORMÁCIÓ VÉDELME

1.1 Törvényi szabályozás[6]

A magánszféra és a saját adatok felett gyakorolt jog az Európai Unió alapszabályainak fontos alapelvei, amik ránk, az EU pedagógusaira is érvényesek: védenünk kell a tanulóinkat, valamint saját adataikhoz, magánszférájukhoz való jogaikat, ahogyan ez az Emberi Jogokról Szóló Európai Egyezmény[7] alapvető megállapításai között is szerepel. A GDPR[8], számos további alapelvet és szabályt állít fel az adatvédelemmel kapcsolatban.

6 A jogi szabályozással e modul 4. részében és a 3. modul 5. részében részletesen foglalkozunk.
7 https://en.wikipedia.org/wiki/European_Convention_on_Human_Rights
8 DIGITÁLIS ADATVÉDELMI SZABÁLYZAT - A Magyar Köztársaság Országgyűlése Magyarország európai uniós jogharmonizációs kötelezettségeinek teljesítése érdekében megalkotta az információs Önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényt. Az iskolák 2018-ban készítették el a „Digitális adatvédelmi szabályzatukat, mely az Európai Unió és a Tanács által elfogadott, a személyes adatok védelméről és az ilyen adatok szabad áramlásáról szóló rendeletében, más néven általános adatvédelmi rendeletben (General Data Protection Regulation, rövidítve: GDPR) foglaltak betartásával készült.

A Szabályzat 5. cikkelye (1)(f) kötelezővé teszi, hogy a "személyes adatokat olyan módon kell kezelni, ami biztosítja a személyes adat megfelelő védelmét, beleértve a törvénytelen vagy törvénysértő továbbadás elleni védelmet és a véletlen elvesztés elleni védelmet, az adatok tönkretétele vagy sérülése elleni védelmet, megfelelő technikai és szervezési intézkedések alkalmazása révén (egységesség és megbízhatóság)." Ezeknek a szabályoknak a be nem tartása jelentős bírságot von maga után.

A 83. cikkely (5)(a) leszögezi, hogy a „személyes adatok kezelése alapelveinek megsértése a legmagasabb szintű adminisztratív büntetés tárgyát képezi". Ez 20 millió euróig terjedő, vagy a teljes éves forgalom 4%-át kitevő bírságot jelenthet.

A GDPR egyik alapszabálya, hogy a személyes adatokat "megfelelő technikai és szervezeti intézkedések" megvalósításával, biztonságos módon lehessen elérni. Ez azt jelenti, hogy az Ön iskolájának is ki kell neveznie egy adatvédelmi biztost[9], aki gondoskodik arról, hogy az iskola minden alkalmazottja tisztában legyen az ott tárolt személyes adatok biztonságát érintő folyamatokkal. Önnek, mint az iskola alkalmazottjának, szintén be kell tartania a törvényi előírásokat, és felelősséget kell vállalnia a személyes adatok helytelen kezelése esetén. Ennek értelmében jól kell ismernie néhány alapvető internetbiztonsági szabályt, például a titkosítást. Ebben a fejezetben bemutatunk néhány, a személyes információ és a magánszféra védelmére szolgáló eszközt, remélve, hogy hasznosítani tudja majd őket, ha biztonsági javaslatokra lenne szüksége.

A személyes adatok adatszolgáltatásával, feldolgozásával, az adatok megszerzésével és tárolásával kapcsolatban Önnek, mint az iskola alkalmazottjának szem előtt kell tartania az adatszolgáltatásra vonatkozó főbb törvényi előírásokat, mint például a méltányos és törvényes kezelés, indokolt korlátozás, adatminimalizálás és adatvisszatartás. A törvény alapján végzett feldolgozás már önmagában biztosítja, hogy ezeket a szabályokat betartják (pl. adatok típusa, tárolási periódus és megfelelő biztosítékok). A személyes adatok feldolgozásának megkezdése előtt értesíteni kell az érintetteket a feldolgozásról, annak célját, a begyűjtött adatok típusát, a befogadókat és az adatvédelmi jogokat érintően[10]. Végül, de nem utolsósorban, jogilag az adatok kiszivárgása vagy az adatok nem felhatalmazott félnek való véletlenszerű átadása esetén az Ön iskolájának haladéktalanul, legkésőbb az eset felfedezését követő 72 órán belül értesítenie kell erről az érintett személyeket és az Adatvédelmi Hatóságot.

1.2 Etikai álláspontok

Ebben a fejezetben etikai szempontból vizsgáljuk meg, miért fontos a személyes adatok védelme. Manapság, különösen, ha olyan technikával és szoftverrel támogatott tanulásról van szó, amihez különféle információk és adatok megadása szükséges, a személyes és érzékeny adatok[11] begyűjtése korlátlan mértékben elvégezhető.

9 Magyarországon 2018 óta kötelező készíteni és betartani az iskoláknak adatvédelmi szabályzatot. https://www.accessnow.org/cms/assets/uploads/2018/09/GDPR-User-Guide-Digital-Hun.pdf

10 https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection/what-are-main-aspects-general-data-protection-regulation-gdpr-public-administration-should-be-aware_en

11 lásd a modul 4-es leckéjét

Lehetséges, hogy Ön is használ valamilyen szoftvert a tanításhoz, vagy netán az iskola, ahol dolgozik, több felületet is használ a tanulók előmenetelének közlésére az érintett személyekkel, például helyi hivatalokkal vagy szülőkkel. Az is előfordulhat, hogy Ön szeretne online megosztani különböző kutatásokat a diákjai körében, vagy a tanulók fényképeit, konferenciákra készített dolgozatait osztaná meg a kollégákkal. Képzelje magát a tanulók helyébe, és gondolja végig, mit érezne, ha például a munkáját, vagy a személyes adatait valaki a belegyezése nélkül tenné közzé. Ez megadhatja a választ arra, miért fontos az etikus és belegyezésen alapuló adatgyűjtés, feldolgozás és elemzés, valamint az adatok biztonságos tárolása és kezelése.

Valószínűsíthetően ebben semmi újdonság nincs az Ön számára: az Ön iskolájának etikai bizottsága vagy jogi osztálya biztosan számos gyakorlat révén garantálja, hogy Ön is betartja az adatgyűjtéssel kapcsolatos törvényi és etikai előírásokat. Az etikus adatgyűjtés nem új téma, különösen a tudományos kutatások világában, jóllehet az internetbiztonság, mint az etikus adatgyűjtés területe relatíve új, és néha nemtörődömségből a szőnyeg alá söprik. Fontos, hogy megértsük: minden, amit digitálisan tárolnak, kezelnek, vagy megosztanak, sérülékenynek számít, kockázatokra érzékeny, és további védelemre van szüksége, mivel az adatszivárgás hatásai és következményei óriásiak, veszélyesek, és a törvény által büntetendők. Mi pedig szinte mindent digitálisan tárolunk, ahogyan az iskolákban használt szoftver is teszi. Ami azt jelenti, hogy minél több digitális rendszert vonunk be a tanítási gyakorlatba és a tanulók iskolai életébe, annál összetettebb etikai problémák és kihívások keletkeznek ezekkel kapcsolatban[12].

Míg egészében véve az adatvédelem minden olyan adatot érint, amely azonosítható egyéntől vagy egyénektől származik, vannak más adatok is, amelyek érdekesek lehetnek egy harmadik fél számára. Azt már nagyon is jól tudjuk, hogy a személyes adatokkal hogyan lehet többféle okból is rosszindulatúan visszaélni. Csakhogy a különféle szoftvertermékek minőségi adatokat szolgáltatnak, amelyek képesek feltárni a tanulók viselkedésével kapcsolatos információkat, amit tovább lehetne értékesíteni, kiszivárogtatni, vagy hivatalosan megosztani az alkalmazott szoftver adatvédelmi szabályozásának megfelelően, például azért, hogy személyre szabott hirdetések célpontjaivá váljanak, és így valaki más hasznot húzzon belőlük. Ez az etikus adatkezelés egyik internetbiztonsági vonatkozása, amivel nem árt tisztában lennie, és tudnia kell, hogy ha ilyen adatgyűjtés történik, akkor az adatok az EU vonatkozó adatvédelmi szabályai alá tartoznak[13].

Tanárként a tanuló adatait, amelyeket Ön vagy az Ön által az osztályban tanulási célokra használt szoftver összegyűjt, elemez, használ vagy megoszt, erkölcsi tartalomnak kell tekinteni, ami a diákok identitását, biztonságát és jólétét érinti - mind fizikai, mind érzelmi vonatkozásban. Az is az Ön kötelessége, hogy elvégezze és biztosítsa az átláthatóságot, amikor a tanulók személyes adatairól és arról van szó, ahogyan ezeket begyűjtik, kezelik, megosztják, elemzik és tárolják. Ide tartozik Ön is, amikor képeket vagy a tanulók által készített dolgozatokat oszt meg egy konferencián.

Az adatok etikus kezelése érdekében az internetbiztonság szempontjából azt javasoljuk Önnek, hogy tájékoztassa a tanulókat és szüleiket arról, hogy az Ön által használt szoftver milyen adatokat és hogyan gyűjt, ezeket miként elemzi, illetve, hogy milyen célból és mennyi ideig tárolja.

12 https://nki.gov.hu.
13 Regulation (Eu) 2016/679 Of The European Parliament And Of The Council, 2016.

Tegyen meg mindent, ami lehetséges, annak érdekében, hogy megfeleljen az iskolája tanulói adatok védelmével kapcsolatos internetbiztonsági szabályzatának. Titkosítson mindent, amit tud, legyen tudatában annak, hogy az Ön által használt készülékek mennyire védettek fizikailag és szoftveres oldalról. Gondolja át, miket oszt meg, hol, kikkel, hogyan, és hogy szükség van-e erre, és kerülje a titkosítatlan személyes adatok megosztását. Ennek a fejezetnek a 2. és a 3. részében részletesen ismertetünk néhány olyan eszközt, amiket alkalmazhat a személyes adatok védelmére mind online, mind offline.

Ragaszkodjon ahhoz, hogy az iskolájának strukturált internetbiztonsági szabályzata legyen, ha eddig még nem alkották volna meg. Függetlenül attól, hogy Ön számítástechnika tanár, zenetanár, vagy az iskola adminisztrációs területén tevékenykedik, valószínűsíthetően adatokkal dolgozik, és tisztában van az adatok nem biztonságos kezelésének etikai következményeivel, ezért fel kell szólalnia az egységes szabályozásért, ami biztosítja a közös internetbiztonsági alapot, amelyre Ön és a kollégái támaszkodhatnak. Ösztönözze az iskolavezetést, hogy szervezzenek tanári workshopokat, ahol többet megtanulhatnak arról, hogyan lehet megvédeni az információt, és ahol kérdéseket is feltehetnek. Keressen további képzési és tanulási lehetőségeket saját maga és a kollégái számára, és hangoztassa ezek fontosságát!

Végül, de nem utolsósorban, amennyiben lehetséges, vonja be a tanulókat és szüleiket is a személyes adatok etikai vonatkozásaival kapcsolatos párbeszédbe.

Figyelmeztesse a tanulókat, hogy soha ne osszanak meg felesleges személyes információt magukról, vagy a családjukról és barátaikról.

Segítsen nekik, hogy megismerkedjenek azokkal az eszközökkel, amelyek megvédik az adataikat, vagy kapcsolja össze őket egy olyan kollégájával, aki meg tudja ezt tenni, ha Ön nem érzi magát elég jártasnak a számítástechnikában. Ösztönözze őket arra, hogy több információt keressenek, és dolgozzanak annak érdekében, hogy többet tudjanak meg: szervezzen tanórán kívüli tevékenységeket a tanulóknak, hívjon meg vendégelőadókat, lépjen kapcsolatba olyan internetbiztonsági szakemberekkel, akikhez a tanulók fordulhatnak.

Az etikai alapelvek széles körű, összetett és nagyon bonyolult dilemmák, amiket elsődlegesen figyelembe kell vennünk, amikor adat- és magánszféra védelemről van szó az iskolákban. Tanárként kiemelkedően fontos, hogy megvédjük a diákjainkat és saját magunkat, annak érdekében, hogy megőrizhessük a tanári szakma jó hírét, és biztosítsuk a sérülékeny felek biztonságát, amit leginkább az adatok feltörése és kiszivárogtatása veszélyeztethet.

1.3 Az adatok és a személyiség ellopásának ára

Az internetes bűnözés a szégyenből, valamint a boldogságnál és haragnál is erőteljesebben átélt érzelemből, a megaláztatásból[14] táplálkozik. A témával való ismerkedéshez négy videó megnézését javasoljuk: az első ***egy TED beszélgetés Monica Lewinskyvel***, "A szégyen ára" címmel, amely az internetes zaklatás témájával és a közösségi megaláztatással foglalkozik.

A következő videó ***(„Az internetes bűnözés nem a számítógépekről szól, hanem a viselkedésről")*** szintén egy TED beszélgetés Adam Andersonnal arról, hogy az internetbiztonság nem csupán hat a pszichikumunkra, de a pszichológiát használja arra, hogy hatást gyakoroljon ránk.

14 Otten, 2013

A harmadik videóval ***(„A hihetetlen léleklátó felfedi titkát")*** arra szeretnénk rámutatni, hogy napi rendszerességgel mennyi információt osztunk meg magunkról online.

És végül, de nem utolsó sorban ***egy magyar példa arra***, hogyan változtathatja meg néhány nap alatt akár az egész életünket, ha nem figyelünk személyes adataink védelmére.

Most pedig vizsgáljuk meg közelebbről, miért is fontos mindannyiunk számára, hogy megfelelően megismerkedjünk az adatbiztonság kérdéseivel.

Ahogy a legutolsó videóban is láthattuk, kis híján a „kamucég" ügyvezetői igazgatójaként vitte el a rendőr az adatlopás áldozatát – aki önként adta meg adatait egy nyereményjáték kapcsán. Ilyen eset velünk is előfordulhat, ha nem vagyunk kellően elővigyázatosak: amikor megmutatjuk számgyertyás születésnapi tortánkat a közösségi oldalakon, ahol valódi nevünkkel regisztráltunk, máris két érzékeny adatot adtunk ki kezünkből. Ha történetesen édesanyánkkal való kapcsolatunk is jelölve van az oldalon, és ő a lánykori nevével (is) szerepel, máris olyan adatokat lophatnak el tőlünk, amelyekkel könnyedén személyazonosság-lopást, vagy identitáscsalást követhetnek el. A Javelin Stratégia & Kutatás adatai szerint csak az USA-ban 2017-ben 16.7 millióan váltak azonosítási csalás áldozatává, de sajnos Magyarország is a „top 7-ben van a világon az emailben kapott kártevők számát tekintve[15]". Az adatfeltörési esetek és az azonosítólopási jelentések emelkedő tendenciát mutatnak. A kiberbűnözők egyre több összetett sémát alkalmaznak, de – mint láthattuk - gyakran maguk az áldozatok azok, akik nem teszik meg a szükséges óvintézkedéseket a saját védelmük érdekében, legalább az alapvető internetbiztonsági szabályok betartásával.

És ha még be is tartják az internetes higiénia alapkövetelményeit, szerencsétlen módon mégis érhet bárkit személyiséglopás, aminek messzemenő következményei lehetnek az áldozatokra.

Az Egyesült Államok Igazságügyi Minisztériumának (DOJ) 2014-ben átdolgozott tanulmányában az áll, hogy az USA-ban évente 17.6 millió ember szembesül a személyiséglopás valamelyik formájával. Ez olyan tevékenységekre vonatkozik, mint például a törvénytelen számlanyitás személyes adatok ellopásával, de nem veszi figyelembe azokat az eseteket, amelyek az internetes zsarolással kapcsolatosak, amikor az áldozatot addig bántalmazzák, amíg nem fizet azért, hogy visszaadják az ellopott információt, bár arra nincs garancia, hogy nem szivárogtathatták-e ki máshová, és nem használhatták-e fel más rosszindulatú felek egyéb célokra.

Az USA Igazságügyi Minisztériumának jelentése szerint "A személyiséglopás gazdasági hatása közvetett és közvetlen pénzügyi veszteségből tevődik össze. A személyiséglopásnak tulajdonítható teljes veszteség nagyobb része közvetlen, és azt a pénzösszeget jelenti, amit az elkövető a sértettől megszerez annak számlaadatai vagy személyes adatai helytelen használatával, beleszámítva a megszerzett áruk, szolgáltatások vagy készpénz értékét. Közvetett veszteségnek számít minden egyéb költség, amivel a személyiséglopás jár, mint például a jogi bírságok, visszaküldött számlák és más egyéb költségek (pl. posta, telefonhívások, közjegyzői díjak). A közvetlen és közvetett veszteségek nem feltétlenül jelennek meg a sértett személyes veszteségeként, mivel a közvetett vagy közvetlen veszteségeket részben vagy teljesen megtéríthetik az áldozatoknak."

15 https://nki.gov.hu

A pénzügyi szempontok mellett az adatkiszivárogtatás áldozatává válásának ára lehet folyamatos megaláztatás, a munkahely és a család elvesztése, és sok más egyéb is. A Személyiséglopást Kutató Központ felméréséből kiderül, hogy a megkérdezett áldozatok 69%-a félti a személyes és a pénzügyi biztonságát, 65%-uk dühöt, haragot vagy megalázottságot érez. Alvászavarokról vagy álmatlanságról 40%-uk számolt be. Ezek az érzések a jelentés szerint az idővel erősödtek, amikor az áldozatok nem tudták önállóan megoldani a problémát. Fontos kiemelni továbbá azt a tényt is, hogy a személyiséglopás áldozata felelősségre vonható azokért a bűncselekményekért, amiket a tolvaj az ő nevében végez el[16].

Ami még ezeknél is ijesztőbb a Javelin Strategy jelentésében, hogy a gyerekek egyre inkább válnak azonosítási csalás áldozataivá. Míg az USA-ban a gyerekek régóta a társadalmi azonosító jellel való visszaélés és hitelkártya csalás célpontjai voltak, úgy tűnik, hogy ez a jelenség tovább fokozódik. A biztonságtechnikai cég felmérése szerint 2017-ben több mint 1 millió gyerek azonosítóját lopták el. Emiatt is különösen fontos, hogy az iskola megfeleljen a biztonsági előírásoknak, a lehetséges adatkiszivárgás pedig jelentős büntetést vonhat maga után. A korábban is említett GDPR 83. (5) (a) cikkelye leszögezi, hogy a személyes adatok feldolgozása alapelveinek megsértése a legmagasabb szintű adminisztratív bírságok hatálya alá tartozik. Ez 20 millió euróig vagy a teljes éves árbevétel 4%-áig terjedő büntetést jelenthet, attól függően, hogy melyik a magasabb összeg. Ez újfent munkahelyek elvesztéséhez, negatív megítéléshez, pénzügyi veszteséghez és válsághelyzethez vezet.

A megfelelő adatkezelési eljárások követése alapvető a pénzügyi, dologi, fizikai és erkölcsi károk elkerülésére. A saját személyes adatainak védelme mindenkinek a saját joga, ugyanakkor felelősséggel is jár: felelősek vagyunk legalább az alapvető lépések megtételéért, amivel megvédhetjük magunkat és magánszféránkat, és megmenekülhetünk az adatvesztés okozta tragédiától[17].

Összefoglalás

Mivel mindennapi életvitelünk, társadalmi és oktatási rendszereink egyre jobban kötődnek az elektronikus adatokhoz és számítógépes hálózatokhoz, a személyes adatok egyre nagyobb óceánja tárolódik az interneten. Ezzel a magánszféra megsértésének veszélye fenyegeti az egyes embereket, és az iskolákra nézve azt jelentheti, hogy potenciálisan óriási felelősséget kell vállalniuk, abban az esetben, ha adatbiztonsági feltörés következik be intézményünkben.

Az internetes támadások és feltörések egyre gyakoribbá válnak, ami növekedő veszteségeket okoz. Ennek feltartóztatása érdekében minden eddiginél nagyobb figyelmet kap az internetes biztonság és a digitális személyes adatok védelme: az ITRC 2018-as jelentése[18] szerint az adatfeltörés leggyakrabban használt módszere a hekkelés volt, összesen 482 adatfeltöréssel, ami 17 millió nyilvántartást érintett.

Az adatvédelem és az internetbiztonság problémáiról nagyon fontos beszélni, annak érdekében, hogy a jövő mindannyiunk számára biztonságosabb legyen.

16 https://mediakutato.hu/cikk/2017_04_tel/01_a_digitalis_identitas.pdf
17 A témáról tovább olvashat:
https://www.bjs.gov/content/pub/pdf/vit14.pdf
https://www.idtheftcenter.org/images/surveys_studies/Aftermath2013.pdf
https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity
18 https://www.idtheftcenter.org/2018-data-breaches/

Kérjük, tekintse át ennek a fejezetnek a forrásanyagait is, hogy több információt találjon az adatok és a magánélet védelmének problémájával és fontosságával kapcsolatban. Helytakarékossági okokból a hivatkozásokat egy könyvjelző-alkalmazásban gyűjtöttük össze. A webmix bal oldalán a magyar nyelvű forrásokat és szakirodalmat találja, míg a jobb oldalon az idegen nyelvű honlapokra kattintva tájékozódhat tovább a témában: ***https://www.symbaloo.com/mix/adatvedelem.***

2. AZ INFORMÁCIÓ ÉS A SZEMÉLYES ADATOK VÉDELMÉRE SZOLGÁLÓ ONLINE ESZKÖZÖK ÉS MÓDSZEREK

2.1 Jelszavak

2.1.1 Alapelvek

Tudjuk, hogy egyszerű jelszavakat létrehozni digitális öngyilkosság. A gyermek nevének használata az email jelszóhoz olyasmi, amit ma már senki sem tesz, azonban a jelszó alapjai az idő múlásával megváltoztak, és azt, amit néhány évvel ezelőtt kifinomult jelszónak tartottak, manapság már nem lehet a biztonságos kategóriába sorolni.

Néhány évvel ezelőtt a hosszú jelszavakat biztonságosabbnak ítélték meg, mint a rövid jelszavakat. Melyik jelszót tartaná biztonságosabbnak az alábbiak közül?

1. 7D * K2 # c
vagy
2. abcdefghijklmnopqqq

Nemcsak a jelszó hosszáról van szó, hanem figyelembe kell vennie annak minőségét is, mivel a jelszó-feltörő algoritmusok olyan mintákat keresnek, mint például a fenti második példában van, és sokkal könnyebb feltörni a második jelszót, mint az elsőt.

A magas entrópiájú jelszavak létrehozása nem könnyű, ugyanakkor a legtöbb jelszókezelő felajánlja egy biztonságos jelszó létrehozását az Ön számára, hogy megfeleljen a használni kívánt szolgáltatás feltételeinek. Azonban legyen óvatos, amikor egy alkalmazás használatával választ erős jelszót, és csak hivatalos szoftvert használjon, ne pedig egy véletlenszerű online eszközt, ami a „biztonságos jelszó létrehozása" Google-keresésben jelent meg.

Mutatunk egy példát egy harmadik típusú jelszóra:

3. mycatisgreenandilovepizza.

A helyzet az, hogy a jelszó-feltörők félelmetesen jól ki tudnak találni teljes szavakat és hétköznapi kifejezéseket, és a feltörő minőségétől és a processzor sebességétől függően ez a jelszó kevesebb, mint 30 perc alatt bedőlhet. A jelszó megalkotáskor azt kell feltételeznie, hogy olyan dolgok, mint a gyermeke neve vagy a kedvenc zenéje, a város, ahol él, és még sok más tény is ismert Önnel kapcsolatban. A pszichológiai befolyásolás nagyon érdekes és egyre nagyobb elismerést szerző téma az internetbiztonságban, és sajnos számos új módot teremt a jelszavak feltörésére is.

Ezt a jelenséget heurisztikus támadásnak nevezik – mivel az Ön jelszava valamilyen személyes dolgához kapcsolódhat, amely valószínűleg online is megjelenik.

A heurisztikus társadalmi kutatáson alapuló támadás egy másik típusa az emberi viselkedésre irányuló heurisztikus támadás. Ez akkor vált elterjedtté, amikor a platformok arra kötelezték a felhasználókat, hogy a választott jelszavakhoz nagybetűt, számot és szimbólumot adjanak meg. A „heckerek" vagy a feltörő szoftverek algoritmusa először azt fogja feltételezni, hogy a szükséges szimbólumokat, nagybetűket és számokat a jelszó elejére vagy végére helyezi, hogy megfeleljen a platform követelményeinek.

Ezért például a „P @ ssword1" nem jelent sokkal erősebb jelszót, a „passwordpassword"-nél egy rosszindulatú fél számára. Az internetbiztonságnak és a kiberbűnözésnek is sok köze van az emberi pszichológia megismeréséhez és a kiszolgáltatott viselkedési minták felismeréséhez, tehát ne essen ilyen csapdába!

2.1.2 Változtassa gyakran a jelszavát!

Javasoljuk, hogy néhány havonta változtassa meg a jelszavát. Természetesen sokkal fontosabb, hogy biztonságosan és titokban tartsa a jelszavát, és ne használja több webhelyen, de a jelszavak megváltoztatása önmagában sem egy rossz szokás.

Néhány szolgáltatás, például az AWS, emlékezteti Önt, ha egy ideje nem változtatta meg a jelszavát, és felszólítja, hogy tegye meg. Az ilyen típusú kötelezettséghez azonban feltétlenül szükség van egy jelszókezelőre, amit néhányan kockázatosnak tartanak, mivel az ilyen, „kényszer" a jelszó gyakori megváltoztatására kockázatos viselkedéshez vezethet, például egy jelszóval használhat több szolgáltatást, vagy a jelszavakat a telefonján, vagy ami még rosszabb, papíron tárolja. Javasoljuk, hogy csak akkor frissítse a jelszavait, ha biztonságos módon tudja tárolni őket.

2.1.3 Többtényezős azonosítás

A többtényezős hitelesítés megköveteli, hogy a felhasználó két vagy több különálló módszert használjon személyazonosságának ellenőrzésére, és ha az egyik lépés sikertelen, akkor a felhasználónak nem engedik meg, hogy a szolgáltatást használja. Ez általában egy jelszó, amelyet valami más követ, például egy kóddal ellátott szöveg, vagy automatikus telefonhívással történő azonosítás, biometria, biztonsági tokenek, email ellenőrzések és így tovább. Ez jó módszer például egy fontos profil, e-bank profil vagy email fiók védelmére.

2.1.4 Ne használja fel újra!

A könnyen kitalálható jelszónál is rosszabb eset a jelszó újbóli felhasználása. A jelszavak újbóli felhasználása meleg fogadtatást jelent minden rosszindulatú fél számára, amelyik egynél több profilhoz kíván hozzáférni, mégpedig a következők miatt: a legtöbb ember egy vagy két emailt használ a személyes célokra használt szolgáltatásra történő regisztráláskor. Képzelje el, hogy regisztrálva van az „F" weboldalra ugyanazzal az email címmel és jelszóval, amelyet a „G" weboldalon használ. A hekkerek hozzáférést kapnak az „F" webhelyhez, amely tárolja a jelszavakat és SHA1 titkosítással védi őket, ami csak egy kicsit nehezíti meg jobban a hekkerek számára, hogy elolvassák, mintha egyszerű szövegről lenne szó.

A hekker látja az emailt, visszafejtette a jelszavát, és kíváncsi lesz arra, hogy létrehozott-e másik profilt ugyanazzal az email címmel a „G" webhelyen. Találja ki, melyik jelszót próbálja ki először! A hekkerek számára plusz „bónusz", ha ugyanazt a jelszót használja az email fiók védelmére – Ön pedig akkor nagyon-nagyon kellemetlen helyzetbe kerül.

Ha különböző jelszavakat használ minden profiljához, és ha az „F" webhely valamilyen módon ki is adja a jelszavát, akkor az elszenvedett károk elkülönülnek a többi webhelytől, és nem terjednek ki az Ön által használt egyéb szolgáltatásokra is.

2.1.5 Jelszókezelők

A jelszókezelők nagyszerűen használható eszközök, mivel megkönnyítik az összes jelszó és profil megjegyzését. A jelszókezelő egy szolgáltatás, amely tárolja a jelszavait, felhasználóneveit és egyéb releváns információkat. Nagyon sok jó, ingyenes szolgáltatás használható. Úgy működnek, hogy általában az összes jelszót egy fő jelszóval védik, és amikor a fő jelszót beírja, akkor hozzáférhet a jelszó-tárolóhoz. Mivel azonban a jelszókezelők tárolják az összes jelszót és profilt, nagyon „szaftos" támadási célponttá válhatnak. Ezért javasoljuk, hogy megbízható jelszókezelőt használjon, továbbá legyen kétszer olyan óvatos a linkek megnyitásakor, és tanulja meg, hogyan ellenőrizheti a tanúsítványokat. A hamis tanúsítvánnyal rendelkező hamis webhely, amely megpróbálja megszerezni a jelszavait, pontosan ugyanúgy fog kinézni, mint a legitim.

Tudnia kell, hogyan lehet beazonosítani az adathalász webhelyeket, erről bővebben a „Biztonságos webhelyek és hálózatok" című fejezetben olvashat.

2.2 Digitális személyiség

A digitális személyiség fogalmát általában egy adott személyről, társaságról vagy szervezetről ismert információ digitális ábrázolásaként definiálják. Vagyis a digitális személyiség alkotórésze minden olyan információ vagy kijelentés, amelyet Ön online készített magának, vagy valaki más állít elő, Önre hivatkozva. Ilyen állítás lehet például, hogy egy bizonyos helyen dolgozik, az iskola valószínűleg feltüntette a nevét munkavállalóként az iskola webhelyén, vagy például a LinkedIn oldalán Ön is megemlítette az iskolához való kapcsolódását. Egy fénykép, videó vagy hangfelvétel szintén kinyilatkoztatásnak tekinthető a kiberbiztonság szempontjából - kijelenti, hogy néz ki, vagy megmutatja a környéküket. Az állítás lehet egy egyszerű írásbeli nyilatkozat is, amelyet a Facebook-on tesz közzé, például „Ma boldog vagyok". Internetbiztonsági szempontból a kinyilatkoztatás ennél valamivel bonyolultabb lehet technikailag.

Az internetbiztonság a kinyilvánítást azonosság-nyilvántartásként ismeri el, amely egyértelműen egy vagy több jellemzőt tulajdonít az identitásnak. Ez az azonosító bejegyzés lehet akár a felhasználónév. Az olyan kinyilatkoztatást, amely egyazon identitásban egynél több attribútumot állít fel, hitelesítő adatnak nevezik - például felhasználónév és jelszó vagy nem technikai értelemben az egyetemi oklevelet is hitelesítő adatnak tekinthetjük, mivel egy összetett kinyilvánítás-bejegyzést jelent, többszörös attribútumokkal, például név, születési idő, elöljáró neve, stb.

Miért fontos ez? Minden, az Ön által vagy valaki más által tett kinyilatkoztatás összekapcsolódik, és digitális identitást alkot, amely Önre vonatkozik. Az online világban, hasonlóan az igazihoz, az azonosító adatokat adatbázisokban tárolják, és gyakran összehasonlítják vagy összevegyítik más adatokkal, amelyeket további felhasználás céljából határozatlan ideig tárolnak.

Az Önnel kapcsolatban online közzétett biteket és információkat harmadik felek gyűjtik, és ezeket az adatokat különféle módon használják - például a digitális személyazonosságához kapcsolódó böngészési adatok felhasználhatók a böngészési élmény javítására úgy, hogy az az Önnek megfelelő hirdetéseket kínálja fel. Ez nem feltétlenül rossz, de az lehet. Minden, amit Ön, vagy valaki más oszt meg Önről, és az Ön személyiségéhez köthető, magában foglalja a digitális identitást, és ez kiszivároghat, vagy felhasználható gazdasági, pszichológiai vagy egyéb kellemetlen módon.

Nem megijeszteni akarjuk, csak éberségre szólítjuk fel, arra vonatkozóan, hogy milyen információkat küld, hol, milyen módon és milyen célokra. Ezenkívül a internetbiztonság területén bemutatjuk, hogy a digitális identitás nemcsak kinyilatkoztatásokból áll, hanem például a felhasználó által generált viselkedésből, az online jelenlét során előállított adatokból, vagy az Ön által használt platformon megosztott adatokból is. Ez azt jelenti, hogy nemcsak akkor kell vigyáznia, amikor valamit online közzétesz, hanem arra is ügyelnie kell, hogyan viselkedik online, milyen helyeket látogat, és mit csinál ott. Például, ha egy szolgáltatást online vesz igénybe, akkor titkosítási azonosítót kaphat, amely a digitális személyisége egy részét tartalmazza. Az online tevékenységet érintő összes ilyen azonosító nemcsak arra szolgál, hogy azonosítsa Önt az interneten, hanem arra is, hogy biztosítsa a megtagadást, az engedélyezést, a hitelesítést stb. - az online azonosítás abban rejlik, ami az online lét lényege, és amiért használjuk. Ez azt jelenti, hogy az online világnak vannak olyan mechanizmusai, amelyek bizonyos mértékig biztosítják, hogy Ön az, így viszont igaz az is, hogy ha Ön oszt meg valamit, akkor nehéz lesz letagadnia.

Az internetbiztonságban a digitális identitás kapcsán a név (nym) kifejezést használjuk[19]. A nymek olyan identitások, amelyeket a felhasználó kap, amikor más felekkel lép kapcsolatba, vagy ahol a felhasználó cselekedeteit szoftvertermék, platform vagy valami más rögzíti. Az általános nym az álnév, amelyet gyakran Ön ad magának. A nymek összekapcsolhatók Önnel vagy létrehozhatók az Ön számára egy értelmes összefüggésben, például a Facebook-profiljához, de lehetnek olyasmik is, amik csak egy adott alkalmazás vagy online tranzakció kapcsán jönnek létre. Az értelmetlen nymeket kötetleneknek nevezzük, amelyek egyszerűen csak egy alkalmazásspecifikus azonosítót jelentenek, amely nem feltétlenül tárja fel a tényleges személyazonosságot. Azonban a részleges identitások, például a Facebook-profil, többet fedhetnek fel Önről, és pontosan feltárhatják az identitásra jellemző dolgokat-: a születésnapot vagy valami mást. Ez nagyon fontos, mivel a részleges identitásokat a különböző szolgáltatások gyakran összekötik, és egy adott embernek tulajdonítják.

19 ***https://regi.tankonyvtar.hu/hu/tartalom/tamop425/0046_informatikai_biztonsag_es_kriptografia/ch11.html#id521337***

Valószínűleg Ön is zsonglőrködik a különböző identitásokkal. Van szakmai digitális identitása, személyes digitális identitása, osztálytermi digitális identitása, sport digitális identitása, és még sok más. Ezeket nevezzük tartalomfüggő identitásoknak, és nagyszerű, hogy az online világ egy olyan összetett környezet, amely ezt is lehetővé teszi, így létrehozhat tartalmat, megoszthatja azt konkrét célcsoportokkal, és interakcióba léphet különböző érintett felekkel. Teljesen úgy, mint a való életben, ahol másképpen beszél egy macskával, és másképpen a főnökével. Eltérően az analóg világtól, különösen gyorsan lehet digitális kapcsolatokat kialakítani, amelyekre a hosszú távú memória a jellemző. Vagyis az adatok nagyon gyorsan mozognak, nagy részüket hosszú ideig tárolják, nagyon jó eséllyel bizonyítva az adatok eredetét. Ez megköveteli, hogy éber legyen a személyes biztonság, a magánélet, a bizalom kérdéseit illetően, és figyeljen azokra a kockázatokra, amik abban rejlenek, hogy a szükségesnél több információ kerül ki.

Amikor csak lehetséges, használjon különféle eszközöket a különböző identitási szerepekhez!

Nem arra gondolunk, hogy minden meglátogatott webhelyhez másik számítógépet kell használnia. Azt azonban javasoljuk, hogy ne használja a személyi számítógépét munkához. A személyi számítógép sérülékenysége az adatok szivárgását eredményezheti, amelyek a munka identitásához és az ottani információkhoz kapcsolódnak, és fordítva. Munkaeszközének a Facebook-profilja megtekintésére történő használata feltárhatja a személyes információkat.

Amikor csak lehetséges, használjon különféle fiókokat a különböző identitási szerepekhez!

Ennek egyik példája lehet a munkahelyi email használata a személyes kommunikációra, ami határozottan nem ajánlott, ahogyan a személyes emailfiók munkához történő használata sem. A különféle webhelyeken a személyes emailjével regisztrálhat, ami felfedi az esetleges többi digitális identitását. Ügyeljen arra, hogy szigorúan őrizze a magánszféráját.

Helyezze biztonságba a dokumentumait – online és offline is!

Biztosítsa be az esetleges személyes adatait bármilyen lehetséges módon. Tömörítsen, titkosítson és védjen jelszóval minden olyan dolgot, amelyet nem akar kiszivárogtatni, és ne feledjen el figyelni rá, mit és hová tölt fel.

Erősítse a jelszavait!

Megállapodtunk abban, hogy a jelszó nem biztonságos, ha többféle profil védelmére használja. Védje digitális személyazonosságát erős jelszavak használatával, ne használjon egy jelszót egynél több fiókhoz, különösen akkor, ha több digitális identitással is rendelkezik. Természetesen igaz, hogy egy feltörés nagyon sokukra hatással lehet, de a lehetséges károkat minimálisra csökkentheti erős jelszavak használatával és azzal, ha csak biztonságos helyeken hoz létre profilokat. Ehhez szükség van egy jelszókezelőre.

Csak annyit osszon meg, amennyit muszáj!

Nem kerülhető el, hogy sok információt osszon meg, amikor bejelentkezik egy bizonyos szolgáltatásba, amelyre a normál életéhez szüksége van. Ne osszon meg túl sokat, különösen, ha nincs rá szükség – és ez a közösségi médiában is érvényes: ne feledje, hogy ami egyszer online volt, az online is marad. Mielőtt megosztana valamit, kétszer is gondolja meg, hogy boldog lenne-e, ha a baráti körén kívül más is látja. Ugyanígy tartózkodjon attól, hogy túl sok információt osszon meg az Önnel kapcsolatban álló emberekről - például a házastársáról, a gyermekéről stb., például arról, hogy hol dolgoznak, hova járnak iskolába, és így tovább. Ha pedig olyasvalamit akar megosztani, ami felfedi a tanulók személyazonosságát, akkor kifejezetten hozzájárulást kell kérnie mind tőlük, mind a szüleiktől - a törvény szerint.

Maradjon éber és képezze magát!

Kövesse nyomon online hitelkártya-nyilvántartását, telefonszámláját, számítógépét és a barátai online magatartását. Cselekedjen, ha olyasmit lát, ami zavarja, tegyen fel kérdéseket és kérjen válaszokat. Kövesse a böngészők viselkedését, a betöltési sebességet, a számítógép sebességét, és jelentős változás esetén tegyen intézkedéseket, például telepítse újra, készítsen biztonsági másolatot az adatokról, futtasson vírusvédelmi ellenőrzést, tegye a fiókjait biztonságossá. Ügyeljen az online szokásaira és a kiberbiztonsági higiénére, és tartsa magát ezekhez.

A digitális identitások kezeléséhez nem kell teljesen megváltoztatnia az életét, azonban ha eddig még nem követte ezeket az alapvető tanácsokat, azt javasoljuk, hogy induljon ki belőlük, és kezdje el kialakítani saját szokásait. Nagyon sok kockázatot rejt a személyazonosság-lopás és az identitáson alapuló zaklatás, és még a legegyszerűbb beavatkozások is jelentős segítséget jelentenek**.**

2.3 Kommunikáció emailben

Ebben a fejezetben alapvető tippeket adunk az email kommunikáció biztonságossá tételéhez. Tudnia kell azonban, hogy a kommunikáció e fajtája sok figyelmet igényel, és egyetlen védelmi eszköz sem helyettesítheti a személyes odafigyelést és az éber gondolkodásmódot.

Email szolgáltató

Az első tipp az email kommunikáció biztonságossá tételéhez az, hogy okosan választjuk ki az email szolgáltatót. Ez nyilvánvalónak tűnhet, de sok felhasználó, különösen az idősebbek, akik még az internet hajnalán hozták létre az email fiókjukat, továbbra is régi és kidolgozatlan email szolgáltatókat használhatnak, mert annak idején ezek voltak a legkönnyebben használhatók, széles körben elterjedtek és hozzáférhetők. Érthető, hogy ha valakinek hosszú ideje van egy email címe, akkor aligha szeretné megváltoztatni. Azonban minden olyan védelmi lépés, amelyet a saját érdekében tehet az emailen keresztül zajló kommunikáció során, nagyban függ attól, hogy az email szolgáltató biztonsági gyakorlata naprakész-e, márpedig a számos kisebb email szolgáltató valószínűleg nem fog annyi energiát fektetni a biztonságba, mint a nagyobbak.

Ha fontolóra veszi az email szolgáltatója lecserélését, vagy egy új email fiók létrehozását, amelyet elsődleges fiókként kíván használni, azt javasoljuk, hogy végezzen kutatást, és szánjon rá egy kis időt, hogy megismerje a szóba jöhető email szolgáltatók adatvédelmi szabályzatát, valamint ügyeljen arra is, hogy jól működő spamszűrő képessége legyen, és támogassa a végpontok közötti titkosítást, vagy legalább a szállítási protokoll titkosításának valamilyen módját. Bár ez nyilvánvalónak tűnhet, vannak még olyan kis, helyi email szolgáltatók, amelyek nem kínálják ezeket, és a személyes kommunikáció így könnyen felfedhető.

A web alapú ügyfelek többsége TLS-t használ az üzenetek titkosításához, ami sajnos némi buktatóval is jár[20]. A végpontok közötti titkosítás sokkal biztonságosabb kommunikációs módszer, de egyetlen felhasználó számára nehéz beállítani. A vállalkozások viszont képesek lehetnek a végpontok közötti titkosítás értelmes kiaknázására. Ha egyszerűen csak a személyes postaládájának biztonságát szeretné biztosítani, érdemes víruskeresőt telepíteni, jelszókezelőt használni, és az alábbi tippeket alkalmazni. Javasoljuk, hogy válasszon olyan email szolgáltatókat, amelyek több tényezővel történő hitelesítést kínálnak, és ahol tovább javíthatják a biztonsági beállításokat.

Egyéni szűrők

A legtöbb email szolgáltató lehetővé teszi egyéni szűrők beállítását, amelyek a spamszűrő mellett veszik fel a küzdelmet a nem kívánt üzenetek ellen. Beállíthatja az email fiókját úgy, hogy kiszűrje a bizonyos szavakat tartalmazó üzeneteket, amiket a csalók vagy a spamküldők használnak.

Antivírus

Hasznos lehet az adathalász csalások ellen egy antivírus program telepítése. Egyes vírusvédelmi szoftverek átvizsgálják a nyitóoldalakat, és figyelmeztetnek, ha megpróbálja ezeket megnyitni. A vírusvédelmi programok az adathalász URL-ek óriási adatbázisából dolgoznak, és először megpróbálják ezzel a listával egyeztetni a megnyitni kívánt weboldalt. Ha egyezést érzékelnek, figyelmeztetést küldenek. Egyes vírusvédelmi szoftverek elemzik a webhelyek szövegében és tartalmában felbukkanó figyelmeztető jeleket, és jeleznek, ha probléma van. Ez a két szolgáltatás különösen akkor hasznos, ha véletlenül rákattint egy adathalász linkre.

Természetesen a legtöbb víruskereső szoftvernek is van vállalati verziója, amely lehetővé teszi az email szerver védelmét. Személyes szinten azonban akár egy ingyenes víruskereső szoftver telepítése is elősegítheti az emailek ellenőrzését, és megakadályozhatja a kockázatos weboldalak megnyitását.

A fiók védelme

Javasoljuk, hogy személyes levelezéséhez és elsődleges email fiókjához olyan szolgáltatót használjon, amely több szintű hitelesítést kínál, és erős entrópiával rendelkező jelszavakat állít be. Használhat jelszókezelőt, de legyen óvatos; valamint feltétlenül állítson be egy biztonsági email címet, ahonnan helyreállíthatja az előzőt, ha valami történik.

Azt is javasoljuk, hogy naponta ellenőrizze a személyes postafiókját, hogy gyorsan felismerje, ha valami furcsa zajlik – például, ha hirtelen nem tudja elérni a postafiókot, ha a spam emailek száma növekszik, vagy bármilyen furcsa tevékenységet észlel, és azonnal intézkedjen.

20 „A TLS protokoll kliens/szerver alapú alkalmazások számára lehetővé teszi a biztonságos kommunikációt, elhárítva a lehallgathatóságot és az esetleges hamisítást. Ha a szerver és a kliens is TLS-t használnak, kapcsolódnak egy handshake procedúrán keresztül végigmenve. Ezalatt a kliens és a szerver bizonyos paraméterek összehangolásával biztonságos kapcsolatot létesít egymás közt.” (https://hu.wikipedia.org/wiki/Transport_Layer_Security)

Különítse el a személyes és a munkahelyi fiókot

Mint fentebb említettük, kerülje ugyanazon cím használatát a személyes, és a formális, vagy munkával kapcsolatos kommunikációhoz. Az iskola rendszergazdája valószínűleg erőfeszítéseket tett azért, hogy elég jól bebiztosítsa a munkahelyi emaileket, ezért ne használja a személyes emailjét érzékeny, vagy munkával kapcsolatos információcseréhez.

Ezenkívül mivel valószínűleg a személyes email címét használja több szolgáltatásra és weboldalra történő regisztrációhoz, ezért tekintse azt sérülékenynek, és csak a személyes kapcsolataival ossza meg. Ne illessze be az email címét, sem a munka, sem a személyes weboldalak szövegeibe, illetve az online elérhető prezentációkba vagy más dokumentumokba.

Gyakran nincs más választása, mint hogy egy email címet linkeljen egy weboldalon. Használjon email tisztítási eszközöket és beépülő modulokat, amelyek a legtöbb tartalomkezelő rendszer számára ingyenesen elérhetők, mint például a Drupal vagy a Wordpress. Ezek az eszközök az összezavarás módszerével generálnak egy közvetlen levélküldő linket, amely megzavarja a legtöbb spamet, de továbbra is működik a szokásos böngészőkben, mivel úgy tűnik, hogy ezeknek a spambotoknak a többsége nem rendelkezik teljes HTML-elemzővel, és a legtöbb nem végez JavaScriptet. Ha nem érzi úgy, hogy össze kell zavarnia az emaileket a weboldalakon, akkor legalább azt megteheti, hogy a „@" -ot „at" -ra és a „." -ot „dot" -ra cseréli. Ez a címet továbbra is olvashatóvá teszi, de megzavarja a spambotokat.

A prezentációkban vagy dokumentumokban képként is megadhatja az email címét, amely valószínűleg megakadályozza, hogy a spambotok begyűjtsék azokat.

Fontolja meg, mielőtt elküldi

Végül, de nem utolsósorban, mindig gondolja át, mielőtt elküldene valamit, különösen, ha érzékeny információkat tartalmaz. Még abban az esetben is, ha bízik az email címzettjében, ezt az emailt megküldhetik másoknak, vagy más módon is kikerülhet a tartalom. Javasoljuk, hogy a fentebb említettek szerint csak titkosított információkat küldjön el, és ossza meg a titkosítási kulcsot személyesen vagy más módon (a titkosítási kulcsot ne ugyanabban az emailben küldje) a fogadó féllel.

Legyen megfontolt az emailek továbbításakor, és védje meg a fogadó email címét. Ha tömeges emailt küld olyan embereknek, akik nem ismerik egymást, akkor a BCC-t (titkos másolatot) használja a To vagy a CC helyett. A másolat másodpéldányt jelent, vagyis akinek a neve megjelenik a Másolat fejléc után, másolatot kap az üzenetről. A másolat fejléce a fogadott üzenet fejlécében is megjelenik, így az email címek láthatók mindenki számára. A BCC a nem látható másodpéldányt jelenti, amely hasonló a másolathoz, azzal a különbséggel, hogy a mezőben megadott címzettek email címe nem jelenik meg a kapott üzenet fejlécében, és a Címzett vagy a Másolat mezőben szereplő címzettek nem fogják tudni, hogy mik ezek a címek.

2.4 Biztonságos webhelyek és hálózatok

Az egyik legfontosabb online tevékenység, a saját ötleteink és gondolataink közlése és megosztása mellett a tartalom böngészése. Ez az információs korszak - függetlenül attól, hogy megosztunk vagy fogadunk információt - az internet révén jön létre. Ezért az internetes biztonság két fontos szempontját kell figyelembe venni, amikor kilépünk az online világba: milyen hálózatokhoz csatlakozunk, és milyen webhelyekre, platformokra látogatunk.

Fontos, hogy felismerjük a nem biztonságos weboldalt, és megfigyeléseinknek megfelelően változtassunk a viselkedésen, ugyanakkor fontos, hogy tudjuk értékelni, hogy a hálózat elég biztonságos-e a csatlakozáshoz, és mi az, amit soha ne tegyünk egy ismeretlen hálózaton.

Ebben a fejezetben arról adunk áttekintést, hogy miből áll egy biztonságos hálózat, és mit szabad, illetve mit nem szabad benne megtennünk.

Amikor nem biztonságos hálózatokról beszélünk, gyakran olyan hotspotokra utalunk, amelyeket nem ismerünk, de amelyekhez tudunk kapcsolódni. Ilyen hálózatok lehetnek a kávéházi hálózatok, az ingyenes wifi (vezeték nélküli) hálózatok. Lehet, hogy nincsenek különleges bejelentkezési követelményeik vagy szűrési folyamat, és sok ember használhatja őket. Valószínűleg mindannyian használtunk már ingyenes wifit: valójában nagyra értékeljük azt a tényt, hogy bemehetünk egy bevásárlóközpontba vagy repülőtérre, és csupán néhány kattintással a létesítmény wifihálózatán keresztül csatlakozhatunk az internethez. A nem biztonságos wifi az Ön számára azt jelenti, hogy a hálózat használata közben nincs biztonságban. Ha csatlakozik ehhez a hálózathoz, és valakik rosszindulatú szándékkal vannak jelen ugyanazon a hálózaton, akkor nagyon keveset lehet tenni, hogy megállítsuk őket: elfoghatják az Ön forgalmát, láthatják, amit csinál és kileshetik, esetleg még azokat a jelszavakat is megismerhetik, amelyeket megad.

Természetesen van sok olyan hotspot, amely megköveteli a hitelesítő adatok valamilyen formájának megadását, és / vagy megjelenik egy „Általános Szerződési Feltételek" oldal, amelyre kattintani kell, mielőtt hozzáférhet a hálózathoz, de ez szinte nem más, mint egy üdvözlő oldal, és nem azt jelenti, hogy biztonságban vagyunk. Bizonyos helyeknek lehetnek napi jelszavai, de ez nem jelenti azt, hogy a biztonsági intézkedéseik szigorúak - a következő fejezetben ezt is bővebben tárgyaljuk -, de nem csupán a jelszavak jelentik az egyetlen óvintézkedést, amelyet a hálózat biztonságához meg kell tennie.

És mindig lesz valami, ami lehallgathatja, amit Ön forgalmaz – bár valószínűleg nem, de mint internetbiztonsági szakembereknek, mindig arra kell gondolnunk, hogy van az életünkben egy kávéházban unatkozó ember, aki beleüti az orrát mások online dolgába, vagy saját „ingyenes wifit" hoz létre, hogy megnézhesse, ki mit csinál online. Ezért lássunk néhány általánosan követendő magatartási szabályt.

Ha lehetséges, kerülje az ingyenes wifi-hálózatok használatát!

A személyes adatait és a magánéletét veszélyeztetve csak akkor használjon nyilvános wifi-hálózatokat, amikor sürgősen (halaszthatatlanul) szüksége van rá. Ne használja csak azért, mert unatkozik, vagy meg kell rendelnie azt az egy dolgot online. Ezek a hálózatok valóban nem biztonságosak.

Ha mindenképpen használnia kell, akkor feltétlenül csatlakozzon a megfelelő hálózathoz!

Számos, technikailag hozzáértő ember, ha unatkozna a kávézóban, saját „ingyenes wifit" vagy „ingyenes kávéházi wifit" állítana be, hogy megtévesszen, és ha bejelentkezünk, megnézhesse, hogy milyen információt szedhet ki belőlünk. Mindig kérdezze meg annak a helynek a személyzetét, ahol tartózkodik, mi a neve a hely nyitott hálózatának, netán mutassa meg a készüléken lévő hálózatok nevét, és kérje meg őket, hogy erősítsék meg, melyik az övék. Ha szállodában tartózkodik, kérdezze kifejezetten a recepciót, vagy ha lehetséges, még jobb, ha a saját mobil adataival csatlakozik, vagy hotspotot hoz létre a többi eszközének – megéri ez a befektetés.

Ne használjon olyan szolgáltatást, amely megköveteli a jelszavai megadását!

Ilyenkor kétszeres a veszély. Egyrészt vannak olyan szoftvereszközök, amelyek felhasználhatók a billentyűzet tevékenységeinek rögzítésére, tehát alapvetően elárulja nekik a jelszavát. Másrészről, a szabad hálózatokon könnyen létrehozhat valaki egy hamis webhelyet, amely nagyban hasonlíthat arra a valódi webhelyre, amit használ, és megtéveszti, hogy beírja a belépési adatait.

Ne dolgozzon semmilyen érzékeny információval, ha nyilvános hálózatba jelentkezik be!

Főleg ne írja be a hitelkártya adatait, ne rendeljen online dolgokat, mindenképpen kerülje az online banki tevékenységeket. Hagyja ezeket későbbre, és ne éljen a lehetőséggel - nem tudhatja, ki csatlakozik még ugyanahhoz a hálózathoz, aki visszaélhet személyes adataival.

HTTPS

Ha egy szervezet biztonságos, titkosítást használó webhelyet akar létrehozni, be kell szereznie egy webhely vagy gazdagép tanúsítványt. Két elem jelzi, hogy egy webhely titkosítást használ: 1) zárt lakat, amely a böngészőtől függően a böngészőablak alján vagy a tetején található a cím és a keresési mezők között, valamint 2) egy URL, amely https: -el kezdődik, nem pedig „http:"-vel. Szoktassa hozzá magát, hogy bármikor, amikor fenn van az interneten, megnézi a weboldal címsorát és nevét. Ha közvetlenül a cím előtt a „https" felirat látható, ez azt jelenti, hogy a webhely titkosítva van, tehát az adatait nem lehet kiolvasni továbbítás közben. Ha csak a „http" látszik, akkor az a webhely nem biztonságos. Észrevehet egy kis „lakat" szimbólumot is a webcím előtt. A HTTPS-t a biztonságos kommunikációhoz használják, a kommunikációs protokoll titkosítva van.

A HTTPS fő motivációja a megtekintett weboldal hitelesítése, valamint a kicserélt adatok magánszférájának és integritásának védelme az áthaladás során. Véd a harmadik fél támadásaitól. Az ügyfél és a szerver közötti kommunikáció kétirányú titkosítása megvédi az adatokat a lehallgatástól és a kommunikáció meghamisításától. A gyakorlatban ez ésszerű biztosítékot nyújt arra, hogy kommunikálni tudjunk azzal a webhellyel, amelyikkel éppen szándékozunk, támadó beavatkozások nélkül[21].

Ellenőrizze a webhelyek tanúsítványát!

Elküldés előtt ellenőriznie kell a meglátogatott webhelyek tanúsítványait, valamint azt, hogy hová küldi az adatait. A megbízható tanúsítványok biztonságos kapcsolatok létrehozására szolgálnak egy kiszolgálóval az interneten keresztül. A tanúsítvány elengedhetetlen egy rosszindulatú fél megkerüléséhez, amely véletlenül egy célkiszolgálóra vezető útvonalon van, és úgy viselkedik, mintha a cél lenne. Az ilyen forgatókönyvet általában közbeeső támadásnak hívják. Az ügyfél a hitelesítésszolgáltató (CA) tanúsítvánnyal hitelesíti a kiszolgálói tanúsítványon szereplő CA-aláírást a biztonságos kapcsolat indítása előtt, az engedélyezések részeként. Az kliens szoftverek - például a böngészők - általában tartalmaznak megbízható CA-tanúsítványokat, mivel sok felhasználónak kell megbíznia a kliens szoftverben. A rosszindulatú vagy a veszélyeztetett kliens átugorhatja valamelyik biztonsági ellenőrzést, és megtéveszthet a felhasználókat.

21 https://en.wikipedia.org/wiki/HTTPS

Ha egy weboldal érvényes tanúsítvánnyal rendelkezik, ez azt jelenti, hogy egy tanúsító hatóság lépéseket tett annak ellenőrzésére, hogy a webcím valóban az adott szervezethez tartozik-e. Amikor beír egy URL-t, vagy egy biztonságos webhelyre mutató linket követ, a böngésző ellenőrzi a tanúsítványt a következő jellemzőkkel kapcsolatban:

- a webhely címe megegyezik a tanúsítványban szereplő címmel
- a tanúsítványt egy tanúsító hatóság írja alá, amelyet a böngésző „megbízható" hatóságként ismer fel.

Ha a böngésző problémát észlel, akkor megjeleníthet egy párbeszédpanelt, amelyik közli, hogy hiba történt a webhely-tanúsítvánnyal. Ez akkor fordulhat elő, ha a tanúsítvány regisztrált neve nem egyezik a webhely nevével, ha Ön azt választotta, hogy nem bízik a tanúsítványt kiállító társaságban, vagy ha a tanúsítvány lejárt. Ilyen esetekben rendszerint felajánlják Önnek a lehetőséget a tanúsítvány megvizsgálására, melyet követően elfogadhatja a tanúsítványt (csak az adott látogatásra vagy örökre), vagy nem fogadja el. Ha nem biztos benne, hogy a tanúsítvány érvényes-e, vagy megkérdőjelezi a webhely biztonságát, ne adjon meg személyes adatokat. Még ha az információ titkosítva van is, mindenképpen olvassa el a szervezet adatvédelmi irányelveit, hogy megtudja, mi történik ezekkel az információkkal.

Az adott weboldal tanúsítványának ellenőrzésekor ügyeljen

- a tanúsítvány kiállítójára,
- a tanúsítvány érvényességi idejére és arra, hogy
- kinek a nevére szól a tanúsítvány.

Ha bármilyen kétsége merül fel, végezzen egy Google-keresést, és tudjon meg többet a hitelesítés érvényességéről, vagy arról, hogy a tanúsítványt kiállító cég tulajdonában van-e a webhely - ha ellentmondás van a tanúsítványon szereplő szervezet és aközött, amelyiknek a nevére szól a tanúsítvány, és a webhely tulajdonosáról vagy a tanúsítvány kiállítójáról az interneten elérhető információ között, azt javasoljuk, hogy gondolja át a weboldal használatát[22].

Összefoglalás

Az internetbiztonság alatt gyakran az internetet és az online teret is értik, a fogalom azonban nemcsak összetett, de szorosan kapcsolódik az alapvető emberi jogokhoz is, mint például a személyes adatok és a magánélet védelme, az érzékeny adatok védelme, a véleménynyilvánítás szabadsága, a biztonsághoz való jog, és a béke értékei. Az internetbiztonság a rendszerek és az emberek védelmét jelenti, és a szakirodalomban többnyire az embereket azonosítják az internetbiztonság leggyengébb pontjaként, mivel az adott műszaki megoldások a helytelen emberi beavatkozás miatt mondhatnak csődöt[23].

Hogyan védjük meg az embereket az online térben, és hogyan akadályozzuk meg az internetes támadásokat abban, hogy megzavarják a társadalom számára nélkülözhetetlen szolgáltatások biztosítását, amikor az emberi hibákon alapuló internetbiztonsági sérülékenység olyan gyakori?

22 További információ:
https://www.thesslstore.com/knowledgebase/ssl-support/how-to-check-a-certificates-expiration-date-chrome/
https://schub.io/blog/2019/04/08/very-precarious-narrative.html

23 Gratian, Bandi, Cukier, Dykstra és Ginther , 2017

Az internet lehetővé teszi a felhasználók számára, hogy hatalmas mennyiségű adatot gyűjtsenek, tároljanak, dolgozzanak fel és továbbítsanak, beleértve a védett és érzékeny üzleti, tranzakciós és személyes adatokat is - hogyan védjük meg mindezt, és egyáltalán, a mi feladatunk-e, hogy megvédjük? Az internetbiztonság megosztott felelősséget jelent. Ahogy a digitális kibertér és a fizikai tér közelebb kerülnek egymáshoz, a kibertérben jelentkező kockázatok és fenyegetések egyre inkább befolyásolják a fizikai teret és az egyének életvitelét[24], és mindannyiunknak felelősséget kell vállalnunk abban, hogy legalább alapszinten elkezdjünk gondoskodni a saját online védelmünkről. Ebben a leckében áttekintettünk néhány alapvető tudnivalót az online biztonság megőrzéséről, valamint hasznos tippeket, ötleteket és megelőző intézkedéseket javasoltunk az olvasó számára az otthoni beavatkozáshoz. A következő részében folytatjuk az Ön személyes adatai és magánszférája offline védelmének bemutatását, valamint azokat az alapelveket, amelyek arra irányulnak, hogy megvédjük magunkat és a családunkat, amennyire csak lehetséges.

Tanárként felelősséggel tartozunk azért, hogy az internetbiztonsággal és az online magatartással kapcsolatos, működő gyakorlatokat megismertessük a tanulókkal. Jól tudjuk, hogy a diákok sok időt töltenek online, ezért arra biztatjuk Önt, hogy indítson el egy beszélgetést a biztonságos online magatartásról és a bevált gyakorlatokról. Osszon meg mindent, amit tud, és tanuljon a diákoktól, miközben megvitatják az internetbiztonság témáját, és különböző szempontokból áttekintik a potenciális sebezhetőségeket és fenyegetéseket - ez eredményez majd nagyobb mérvű változást.

3. AZ INFORMÁCIÓ ÉS A SZEMÉLYES ADATOK VÉDELMÉRE SZOLGÁLÓ OFFLINE ESZKÖZÖK ÉS MÓDSZEREK

Bevezető

Úgy gondoljuk, mindenkinek ismernie kellene az alapvető szabályokat, amikkel megvédhetők az általa használt eszközök, hálózatok és a szoftvertermékek személyes adatai. A személyesen használt eszközök védelme többnyire túlmutat csupán a saját magánszféra védelmén: lehetnek érzékeny adataink vagy információink a munkával kapcsolatban az otthoni számítógépeinken is, például azon javíthatjuk a házi feladatokat vagy ellenőrizhetjük a tanulók projektjeit, tárolhatjuk a jövő havi iskolai kirándulás résztvevőinek névsorát, vagy a munkánkhoz szükséges dokumentumokat mentjük le. Ha nem védjük megfelelően a személyes eszközeinket, az az érzékeny adatok kikerüléséhez, sérüléséhez vezethet.

Lehetséges, hogy Önt még sosem érte hekker támadás, és az internetbiztonsági szokásai vagy ezeknek a hiánya még sosem vezetett információszivárgáshoz, de miért kellene vállalnia ennek a kockázatát? Ebben a fejezetben bemutatunk néhányat az alapvető higiéniai szabályok közül, amelyek a személyes adatok és információ biztonságosabbá tételére vonatkoznak. Ezek olyan szokások, amiket Ön is beiktathat a magánéletébe és a munkájába is, hiszen, bár az iskolai környezet védelme és az iskolai eszközökről való gondoskodás a rendszer-adminisztrátorokra tartozik, alkalmazott lévén az Ön tevékenysége az, ami biztosítja, hogy az óvintézkedéseik a kívánt eredménnyel járjanak.

24 Európai Bizottság, 2016

Az internetbiztonság megosztott felelősséggel jár. Nemcsak az iskola egyik kis részlegének a feladata, hogy megóvja Önt és a diákokat. A jó internetbiztonsági szokások követése általában véve megerősíti a saját, a családja és a munkakörnyezete internetbiztonsági helyzetét, és ezeknek az irányelveknek a követésével akár magasabb szintre is emelheti az Ön körül lévő emberek tudatosságát. Az eszközeink védtelenül hagyása pont olyan, mint amikor nem zárjuk be a lakás ajtaját – persze, biztos, hogy senki nem jönne be, de mégiscsak az lenne a legjobb, ha bezárná az ajtót, nem? Ugyanez érvényes az internetbiztonságra is.

3.1 Alapvető szabályok

Az internetes higiénia egyik nagyon fontos szabálya, hogy odafigyeljen a szoftverre, amit a számítógépére telepít. Kizárólag hivatalos szoftvert telepítsen, és törődjön annak naprakészen tartásával, mivel a frissítéssel, amit a szoftverkarbantartás során állít be, megszabadulhat a szoftver ismert sérülékenységeitől. Ha lehetséges, automatizálva és időzítve végezze a frissítéseket. Ugyanez vonatkozik az operációs rendszer frissítésére is: ezek a frissítések azért jöttek létre, mert olyan fontos biztonsági utakat tartalmaznak, amelyek megvédik Önt a legutolsó ismert gyengeségektől, elutasításukkal kockázatoknak teszi ki az eszközt. Ugyanez érvényes az Ön által használt okoskészülékek esetében is. Javasoljuk továbbá, hogy távolítsa el azokat a szoftvereket, amiket már nem használ és nem is kíván használni, hiszen amit nem használ, annak a rendszeres karbantartásával sem törődik. Kifejezetten azt ajánljuk, **hogy törődjön megfelelően azokkal az eszközökkel is, amiket nem használ**, ugyanis rengeteg információ nyerhető ki belőlük. Miután biztonságosan eltárolta az adatokat, amik a régi készülékén voltak, fertőtlenítenie és mágnesesen meg kell tisztítania a lemezt, vagy, ha szeretné eladni például a régi laptopját vagy mobilját, keressen megfelelő szoftvereszközöket (a WikiHow-nak például remek ***oktató anyaga*** van a témában), amikkel teljesen megtisztíthatja őket. Ugyanebből az okból azt javasoljuk, hogy kapcsolja ki a fájl-és médiamegosztást, ha nem használja őket.

Fontos továbbá, hogy **vírusirtó szoftvert is** telepítsen a számítógépére. A legtöbb vírusirtó szoftvernek vannak böngésző bővítményei, és hasznára lehetnek az internet biztonságossá tételében is. Győződjön meg róla, hogy a tűzfala be van kapcsolva és megfelelően van beállítva.

Valaki más számítógépét csak akkor használja, ha muszáj, és akkor is legyen megfontolt, ha USB kulcsot akar használni az információ hordozására, mivel a kártevőket könnyen átviheti a külső tároló eszközökkel. Használjon inkognitó böngészőket[25], és lépjen ki az összes saját profiljából, ha megnyitotta őket. Ne mentsen el soha jelszavakat mások eszközén, és soha ne töltsön fel (vagy le) személyes adatokat és magáninformációt olyan eszközre, ami nem az Öné!

25 Az inkognitóban való böngészés vagy privát böngészés bevett gyakorlat arra, hogy minél kevesebb nyomot hagyjunk magunk után az internetezés során. A privát módban történő böngészés általános a legtöbb korszerű webböngészőben, és úgy működik, hogy letiltja az összes böngészési előzményt és az adatok tárolását a cookie-ban és a webes gyorsítótárakban. Így lehetővé teszi az Ön számára, hogy olyan személyként böngésszen a neten, aki majdnem semmilyen nyomot nem hagy az online tevékenységéről. Az inkognitó módban való böngészés hagyhat ugyanakkor nyomokat a merevlemezen és az eszköz memóriájában, így azokra is ügyelnie kell.
https://www.digitalcitizen.life/keyboard-shortcuts-incognito-private-browsing-inprivate
https://en.wikipedia.org/wiki/Private_browsing

Adatai védelme szempontjából a **biztonsági mentés** is lényeges kérdéskör. A biztonsági szakemberek azt ajánlják, hogy legalább 3 biztonsági mentést készítsen a fontos adatokról: egyet a saját eszközére, egyet a felhőbe és egyet offline, egy védett külső meghajtóra. Egy, a biztonsági szakemberek körében jól ismert szólás szerint egy mentés nem mentés! Rendszeresen ellenőrizze a mentett adatok sértetlenségét és hozzáférhetőségét, és titkosítsa a biztonsági mentéseket – használjon erős jelszavakat és megbízható eszközöket! Végül, de nem utolsósorban, ha biztonsági mentésről van szó, javasoljuk, hogy ne tartson minden tojást ugyanabban a kosárban, vagyis ne legyen minden biztonsági másolat ugyanabban a tárolóban vagy ugyanazon a helyen (nyilvánvalóan ez a külső meghajtón végzett offline biztonsági mentésre vonatkozik).

Az Ön és a tanulói magánszféráját illető fontos probléma a **földrajzi címkézés (geotagging) is**. A közösségi hálózati alkalmazásokkal most bárhonnan fel lehet már tölteni képeket, amikor készítjük őket. Ez problémás lehet, mert sok telefon beágyazza a képfájlba a helymeghatározást is (ami a tartózkodási helyére utal), így bárki minimális tudással is megkeresheti, hol tartózkodott, amikor a képet készítette. Néhány közösségi oldal eltünteti a földrajzi címkéket a fénykép feltöltésekor, de erre nincs garancia. Kapcsolja ki ezt a funkciót az okostelefonján, hogy megőrizze a saját és a tanulói magánszféráját!

A számítógépére mentett fotók, rajzok és videók szintén tartalmaznak személyes adatokat: például egy arckép is annak számít. Továbbá más adatok, mint a helyszín vagy dátum, a rögzítés ideje vagy mások (EXIF média adatok) is elmentődnek a digitális képek esetében. Még ijesztőbb módon a nagy felbontású felvételek bekapcsolhatják a lefotózott személy biometrikus azonosítását[26]. Végül, de nem utolsósorban, általános érvényű tanácsként azt javasoljuk, hogy **tanulja meg használni a virtuális berendezéseket**!

Ha nincs elég jártassága a műszaki dolgokban, a virtuális tér és a virtuális gépek nagyon ijesztőnek és elvontaknak tűnhetnek. Természetesen nem kell mindenkinek ezt az utat választania, de úgy véljük, nagyon hasznos, és internetbiztonsági szakemberekként nagyon sokan alkalmazzuk. A virtualizáció egyszerűen csak egyik vagy másik operációs rendszer futtatását jelenti, így, ha Önnek hagyományos Windowsa van, telepíthet rá vendég operációs rendszert, például a Linuxot vagy ismét a Windowst. Ez nagyon jó szolgálatot tehet, hiszen úgy is konfigurálhatja a vendég operációs rendszert, hogy ne kapcsolódjon az alap operációs rendszerrel, így amit a virtuális gépén csinál, nem veszélyezteti a normál operációs rendszert. Ha például rizikós weboldalt akar megnyitni, megteheti a virtuális gépe segítségével. A virtuális gép egy lépésnyire van az Ön operációs rendszerétől, és meg fogja védeni, így, ha bármilyen kártevő támadás éri a virtuális gépet, egyszerűen megszabadulhat tőle és létrehozhat egy másikat – így a számítógépe biztonságos marad. Ugyanez érvényes, ha nem a saját USB kulcsait használja: megnyithatja őket a virtuális gépével, és ha valamilyen rosszindulatú kód jönne a külső eszközből, nem kell megijednie.

Ezzel a videóval a legjobb elkezdeni, mivel egy kezdőknek szóló útmutatást ad a VirtualBox telepítéséről (ez egy általánosan alkalmazott szoftver virtuális gép létrehozására) egy Windows gépre, és bemutatja egy Ubuntu virtuális gép konfigurálását és futtatását. ***Ez a további videó*** viszont jobban bevezet a VirtualBox alkalmazásába, és abba, hogyan kell telepíteni, futtatni és alkalmazni. Ha jobban kedveli az írott szöveget és leírást, ***ez az útmutató*** segíteni fogja a virtuális gép felállításában és működtetésében.

26 https://us.norton.com/internetsecurity-how-to-how-to-remove-gps-and-other-metadata-locations-from-photos.html
https://www.makeuseof.com/tag/3-ways-to-remove-exif-metadata-from-photos-and-why-you-might-want-to/

3.2 Az eszközeihez való hozzáférés védelme

Nem a megszokott fontossági sorrendet követve elsőként arra hívnánk fel a figyelmét, hogy nem mindegy, hol tartja a számítógépét. Természetesen tudjuk, hogy ha a munkahelyi gépéről vagy laptopjáról van szó, a legvalószínűbb, hogy az irodájában tartja vagy a laptoptáskában, amivel beviheti magával az osztályterembe. A PC-ket nyilván nem lehet túl sokat ide-oda rakosgatni, ennek ellenére azt javasoljuk, hogy tegyen meg egyéb óvintézkedést is: például ne feledkezzen meg az alapvető szabályról, hogy minden esetben zárja le a számítógépét, ha 2 percnél hosszabb ideig van távol, és kapcsolja ki, amikor elhagyja az irodát, feltéve, hogy nincs éppen ütemezett karbantartás. A laptopok esetében azt ajánljuk, hogy legyen még óvatosabb!

Ha magával hozza, vagy hazaviszi a laptopját, ügyeljen rá, hogy nehogy valaki ellopja, és hogy a rajta tárolt adatok biztonságban legyenek. Ez azt jelenti, hogy minden titkosítva van, minden fiókból kilépett, és a szállított információt valahol máshol is eltárolta, így csak az okozhat aggodalmat, hogy egy új géphez jusson, aminek a konfigurálása és a személyre szabott beállítása így csak 2-3 órát vesz igénybe.

Ha a laptopját az iskolai irodájában hagyja, mindig lépjen ki és csukja le, ha 20 percnél tovább nem ér a billentyűzethez (egyébként elég, ha csak lezárja). Ezzel lényegében megvédi a leskelődéstől és attól, hogy valamilyen ital ráboruljon. Amennyiben 4-5 órán keresztül nem foglalkozik, vele, javasoljuk, hogy zárja le, csukja be, és tegye is el (egy szekrénybe, vagy bárhová, ami nem az íróasztal teteje). Ez az óvintézkedés nem a lopás ellen irányul, hanem inkább a leskelődés és illetéktelen hozzáférés ellen.

Már felhívtuk a figyelmét, hogy amíg távol van, zárolja a számítógépet. Nagyon egyszerű, és millió bajtól kíméli meg, ha a számítógépét jelszóval védi, ahogy kellene is. Ezzel a lépéssel csökkenti annak az esélyét, hogy a fiókját valaki használja, ha belépve hagyja ott a számítógépet egy időre. Hogy ez a lezárás hatékony legyen, meg kell győződnie arról, hogy a számítógépe úgy van beállítva, hogy ébredés után jelszót kérjen. A számítógép lezáráshoz nézze meg ezt az ***anyagot***, ami lépésről lépésre bemutatja a tennivalókat a Windows és a Macintosh felhasználóknak.

Jó ötlet egy automatikus inaktiváló kijelentkezés alkalmazása is az eszközön, ha még nem lenne rajta ilyen. Az automatikus kijelentkezés alapvetően mindig a segítségére van, ha sürgősen el kell mennie valahová, és elfelejtette lezárni a számítógépét. A Windows 10 úgy, mint más operációs rendszerek is, automatikusan lezárja a képernyőt, ha a rendszer egy ideje üresjáratban van. Az üresjárat idejét Ön határozhatja meg, lehet akár egy perc, de lehet egy óra is, vagy még hosszabb. ***Ebből a videóból*** megtanulhatja, hogyan konfigurálhatja ezt a beállítást a Windowsban, ha még nem tudná. Ha elfelejti lezárni a képernyőt, vagy úgy érzi, hogy a jelszava kiderült, megváltoztathatja a jelszót, majd azt követően távolból is ki tud lépni a Windows 10-ből. A videó több részlettel is szolgál a témában, de a kilépés csak akkor segít, ha az eszköz jelszóval védett.

Így eljutunk a következő ponthoz: alapvetően fontos, hogy az eszközét jelszóval védje! Van egy kissé cinikus, de igaz mondás a jelszavakkal kapcsolatban: hogy olyanok, mint az alsónemű, nem szabad őket senki mással megosztani, és gyakran kell őket cserélni. Hozzátehetjük továbbá, hogy nem szabad ugyanazt a jelszót több célra felhasználni, és kerülni kell a „könnyű" jelszavakat. Tudjuk, hogy sok fiókja van, ahogy nekünk is. De vannak ingyenes jelszókezelők, amiket egyszerű használni, és biztonságosabbak, mint egy papírra írni a jelszavakat (amit soha nem szabad tennie), vagy egy jelszót használni több weboldalon is, mivel néhány weboldal adatai olykor kikerülnek.

A jelszavak alacsony védettségűek, nyilvánvalóak és titkosítatlanok lehetnek, vagy kiszivároghatnak. Ha a hekkerek ismerik az Ön felhasználónevét (ami nagyon gyakran az email címe) és a jelszavát, megpróbálhatnak betörni a többi lehetséges fiókjába is. Ez a helyzet nagyon kellemetlen az Ön számára, mert kizáródhat a saját felhasználói fiókjaiból, és pénzügyi, érzelmi károkat szenvedhet, vagy más jellegű sérülések érik – tehát ne kockáztasson! A jelszókezelők gyakran ajánlanak fel olyan funkciókat, mint a biztonságos jelszó generálás vagy emlékeztető a jelszó megváltoztatására, ha már jó ideje nem tette meg.

Néha a munkánk arra késztet minket, hogy valaki mással osszuk meg az eszközünket. Ezt igazából egyáltalán nem ajánljuk, de ha muszáj megtennie, tegye meg legalább az alapvető óvintézkedést, hogy **minden felhasználónak külön fiókot hoz létre, különböző felhasználói jogosultságokkal**. Két oktatóanyag[27] hivatott Önt segíteni ebben, ha még nem hozott volna létre különböző felhasználói fiókokat. Az ilyen helyzetekben azt javasoljuk, hogy titkosítson és mentsen le mindent, és minél kevesebb dolgot tároljon rajta – alapvetően munkaállomásként használja az eszközt, és mindent tegyen azonnal külső helyre. Általában véve a legkisebb Jogosultságok elvének (PoLP) követését javasoljuk Önnek. Ez előírja, hogy amennyiben Ön el tudja végezni a munkáját anélkül, hogy igénybe venné az adminisztrátor vagy a root jogosultságot, ne adminisztrátorként lépjen be. A legmagasabb jogosultsággal rendelkező felhasználóként való bejelentkezéskor a rendszer sérülékennyé válik, ami az egész rendszer vagy eszköz veszélyeztetéséhez, a teljes merevlemez átformázásához, vagy egy új felhasználói fiók létrehozásához vezethet a rendszergazdai hozzáféréssel. Ha karbantartási műveleteket végez az eszközön vagy új szoftvert installál, letöröl egy régit, vagy frissítéseket végez, jelentkezzen be adminisztrátorként, de legyen nagyon óvatos, és amit csak lehet, végezzen el offline.

Szeretnénk itt ráirányítani a figyelmét az okostelefonjára és más mobil eszközökre is, amikkel esetleg rendelkezik. Az okos mobileszközökhöz való hozzáférés biztonságossá tétele fontos a személyes adatok és a magánszféra védelmében, de azért is, mert a munkához kapcsolódó személyes adatok biztonsági szintje is magasabb lesz. Bejelentkezhet, hogy megnézze a munkával kapcsolatos e-maljeit, vagy tarthat dokumentumokat a telefonján, be lehet jelentkezve egy felhőszolgáltatásba, ahol tárolja a mentéseit vagy a munkához kapcsolódó információit.

Mint a modul előző leckéjében tettük, most is kifejezetten javasoljuk, hogy kerülje el a munkával kapcsolatos információ saját eszközön való tárolását, bár ez néha fontos lehet a munkavégzés szempontjából, amikor távol van a gépétől, vagy éppen mozgásban van.

Ebben a fejezetben részletesebben tárgyaljuk az eszközeihez való hozzáférés biztonságossá tételét, különös tekintettel a személyes okoseszközökre. Kezdetnek, ha eddig nem használt volna képernyőzárat, tegye meg mostantól. A képernyőzár beállítása kötelező: biztonsági okokból, egyszerűen csak azért, hogy ne tudja feloldani a képernyőt, amikor az eszköz a zsebében van, vagy, hogy a gyerek ne tudjon véletlenül kitörölni valamit. Az okoseszköze hozzáférése biztonságossá tételére a készüléktől függően számos lehetőség elérhető. A leggyakoribb, hogy legalább egy minta vagy jelszó segítségével lehet kioldani a képernyőt.

27 https://www.windowscentral.com/how-manage-user-accounts-settings-windows-10
https://en.wikipedia.org/wiki/Salt_(cryptography)
https://support.microsoft.com/en-us/help/4026923/windows-10-create-a-local-user-or-administrator-account
https://www.lifewire.com/create-user-account-in-windows-7-3506832

Néhány okoseszközön van ujjlenyomat-olvasó, ami nagyon jó megoldás, ha nem akarja, hogy másvalaki használja a telefonját vagy a tabletét. Több okból is azt javasoljuk, hogy inkább jelszót használjon, mint mintát. Elsősorban, mivel elég egyszerű mintákat találunk ki a készülékeink feloldására, így másnak is könnyű lehet kitalálni, hogy Ön milyen mintát használ. Másodszor, mikor egy mintát alkalmaz, az ujja nyomot hagy a képernyőn, így látszódik a minta. A telefon képernyőjének gyakori megtisztítása nem valószínű, hogy eltünteti az árulkodó jeleket, mivel valószínűleg közben Ön is feloldja a telefont. Ezek a jelek könnyen láthatóvá válnak az eszköz képernyőjén, ha egy bizonyos szögben és megvilágításban nézi. Ennek elkerülésére azt ajánljuk, hogy inkább állítson be egy nem hétköznapi jelszót.

Mint a laptopnak vagy a PC-nek, az okoseszköznek is **automatikusan le kell zárnia a képernyőt**, ha üresjáratban van. Ezzel biztosítja, hogy ha Ön az asztalán vagy az osztályteremben hagyja az eszközt, a legtöbb felhasználó nem tudja nézegetni a telefonját.

Egy másik opció, amit jó, ha telepít, a **Keresd meg az eszközt** – beállítás.

BiljaST től a pixabay-ről (Forrás:www.pixabay.com)

Az Android eszközök számára a Google kínálja ezt a szolgáltatást, de vannak hasonlók az áruházban más operációs rendszert használó okoseszközök számára is, például a Find my Iphone (Keresd meg az Iphonomat) az Apple felhasználóknak. Ezzel az alkalmazással nyomon követheti az eszközét, felhívhatja, üzenetet küldhet rá, ami megjelenik a képernyőjén, vagy a távolból visszaállíthatja, ha nincs rá esélye, hogy visszakapja. Ezt az alkalmazást akkor is használhatja, ha előtte nem telepítette, bár, ha vannak a telefonján a munkához kapcsolódó vagy személyes információk, arra biztatjuk, hogy amint lehet, ismerkedjen meg azokkal a lehetőségekkel, amiket ez a beállítás tartalmaz. Ha kiderül, hogy elvesztette az eszközét, ennek az applikációnak a segítségével gyorsan meg tudja határozni a helyét, és a telefon zárolásával bebiztosíthatja, hogy a személyes adatai védettek legyenek, beállíthat egy helyreállító üzenetet, vagy a távolból adatokat törölhet. Ha a telefonját ellopták, és még nem állított be rajta képernyő zárat, a tolvaj újra indíthatja, még mielőtt Ön megpróbálni lokalizálni, és ezzel megakadályozhatja, hogy visszaszerezze a készülékét.

3.3 Titkosítás

Nem beszélhetünk az információ és a személyes adatok védelméről anélkül, hogy megemlítenénk a titkosítást. Itt most csak néhány alapszabályt ismétlünk át a titkosítással kapcsolatban, és a személyes adatok és a magánszféra védelmének egyik javasolt eszközeként említjük meg, mivel a titkosítás témáját részleteiben az első fejezet tartalmazza (Digitális tartalom védelme).

Még ha nem is használja tudatosan a titkosítást, valószínűleg alkalmazza valamilyen módon, például megnyit https-sel kezdődő weboldalakat. A legtöbb banki és pénzügyi alkalmazás például használja, ahogyan néhány csevegő alkalmazás, mint a Viber vagy a WhatsApp is. A HTTPS-ben a kommunikációs protokoll titkosítva van a Transport Layer Security (TLS), vagy elődje, a Secure Sockets Layer (SSL) segítségével. A titkosítás úgy történik, hogy az általános adatokat matematikai egyenletek és titkosítási eszközök segítségével átalakítja biztonsági kódokká az üzenetek titkosítása és dekódolása érdekében. Így megnehezíti, hogy valaki más elolvassa az üzeneteit, vagy lehallgassa a beszélgetéseit vagy a tranzakcióit.

Van egy mondás az informatikában, mi szerint táncolnod úgy kell, mintha nem látná senki, titkosítanod pedig úgy, mintha mindenki látná. Mi kifejezetten azt ajánljuk, hogy mindent titkosítson, amiről nem akarja, hogy illetéktelen személyek is lássák. A titkosítás alapvetően kétféle adatot véd: a nyugalomban lévő adatot és az átvitel közben lévő adatot. A nyugalomban lévő adat például a merevlemezen lévő adatokat jelenti, és a védelem azt biztosítja, hogy ha a laptopját ellopják, az adatokat ne tudják kiolvasni. Az átvitel közben lévő adatok esetében (amelyek egy felhőszolgáltatás segítségével, emailen, vagy böngészők között cserélődnek), a titkosítás abban segít, hogy az átvitel közben ne lehessen az adatait kiolvasni.

TheDigitalArtist a pixabay-ről (Forrás: www.pixabay.com)

Vannak ingyenes és megbízható eszközök az adatai titkosítására mind a számítógépen, mind az okoseszközökön, mint például a kiváló, nyílt forráskódú ***VeraCrypt***. A felhasználástól függően több opció lehetséges:

A legalapvetőbb a számítógép merevlemeze és az itt található adatok védelmére a teljes lemez titkosítása (FDE). Ez azt jelenti, hogy minden olyan adat, ami a számítógépén, egy külső merevlemezen vagy memóriakártyán van, automatikusan titkosított.

Ugyancsak titkosíthat külön mappákat, megosztott lemezt és fájlokat is. Ez időigényesebb ugyan, de jó megoldás, ha például a mappa, amit titkosítani szeretne, nem marad majd az eredeti helyén – például, amikor Ön feltölt egy adatot a felhőszerverre. Nagyon hasznos az információ biztonsági mentésére, és arra, hogy máshol is biztonságosan tárolja, ne csak a merevlemezen.

A felhőszolgáltatással szinkronizálandó adatokat előre is titkosíthatja, amivel olvashatatlanná teszi a felhő számára, és bárkinek, aki azt meghekkelheti. Ebben az esetben a számítógépen tárolt, nem titkosított fájlok sebezhetőnek számítanak.

A titkosításnak más fajtái is vannak, az email titkosításra például a céltól célig (E2E) titkosítás, ami lezárja az üzeneteket, úgy, hogy csak a feladó és a címzett tudja elolvasni, a webes kapcsolatok titkosítása (HTTPS), vagy a mail szerverek titkosítása (Biztonságos/Többcélú Internet Mail Kiterjesztések S/MIME).

3.4 Az adatok biztonságos törlése

Ez az információ aligha új Önnek, de amikor töröl egy információt a számítógépéről, az nem tűnik el teljesen. Legtöbbször, amikor fájlokat töröl, megszabadul a fájlrendszerben az azokhoz vezető hivatkozásoktól, míg a fájl maga továbbra is létezik a lemezen. Ha merevlemez meghajtót használ egy fájl törlésére, a mesterfájl index egyszerűen csak úgy jelöli meg, mintha a lomtárba tartozna, nem a mappába. A valódi adat érintetlenül marad, amíg felül nem írjuk a helyét a meghajtón. Mivel a tárterület bármekkora lehet, ez eltarthat egy darabig, ha a tartós állapotú meghajtót (SSD) használja, amely folyamatosan átrendezik a fájlokat, hogy optimalizálja a tárhelyet, így az információ a végén felül lesz írva, de az is lehet, hogy nem.

A Windowsra ez különösen érvényes, mivel a fájlok, amiket a Windows „törölt", általában visszaállíthatóan megmaradnak a merevlemezen, vagyis a törölt adatok visszaállíthatók, ami különösen traumatikus lehet, ha személyes vagy érzékeny adatokról van szó, amiket nem szeretne visszaállítani, például, amikor eladja az eszközt, vagy ha valami igen személyeset töltött le egy nyilvánosan használt számítógépen. A jó hír, hogy léteznek olyan ingyenesen elérhető szoftvereszközök, amelyekkel biztonságosan törölhet fájlokat, így azok nem lesznek visszaállíthatók. Ilyenek az Eraser, Blank and Secure és sokan mások[28].

Az adatok biztonságos törlésére szolgáló applikációk többsége hasznos, ha egy USB-t szeretne megtisztítani (a formázást is választhatja, amit mi is javaslunk), mivel ugyanazok a problémák előfordulnak a külső memóriaeszközök esetében is, ha egyszerűen csak ráklikkel a Delete gombra az USB-n lévő fájloknál. A Windows és a McOS operációs rendszerek tartalmaznak beépített formázási opciót, ami képes mindent kitörölni a külső tárolóeszközről, és a memóriaeszköz „formátum" opciójára történő jobb kattintással hozzáférhető. Arról feltétlenül győződjön meg, hogy tévedésből nem a belső merevlemezt formázza-e meg, amikor az USB eszközt vagy egy SD-kártyát formatál – ezt a hibát könnyű elkövetni, és utána már nincs visszaút. Ez a ***comparitech.com*** -ról származó oktatóanyag segítségére lesz a külső memóriaeszközök megformázásának folyamatában, és javasol néhány szoftvereszközt is a fájlok biztonságos eltávolítására.

28 http://eraser.heidi.ie/
http://www.pendriveapps.com/freeraser-portable-file-shredder/
https://www.usenix.org/legacy/events/fast11/tech/full_papers/Wei.pdf
https://www.makeuseof.com/tag/7-terms-need-know-buying-new-ssd/

3.5 Iratmegsemmisítés

Az iratmegsemmisítés olyan fizikai dokumentumok eltüntetése, amelyek érzékeny vagy személyes információt tartalmaznak, ezért más felekhez való eljutásuk veszélyes lenne. Biztonságos és gazdaságos megoldás arra, hogy a már szükségtelenné vált dokumentumokat ne olvashassák el illetéktelenek. Mindannyian hallottunk már olyasmiről, hogy cégek érzékeny adatokat tartalmazó iratokat dobtak ki, amiket később megtalált valaki. Ennek nagyon komoly jogi következményei lehetnek, pénzügyi veszteségeket és az érzékeny adatok nyilvánosságra kerülését eredményezheti.

Ez a helyzet kétségkívül minden érintettre nézve nagyon kellemetlen. A régi iratok egyszerű kidobása nem garantálja a biztonságnak azt a fokát, ami megfelelő a tanulók magánszférájának vagy az iskola bizalmas feljegyzéseinek védelmére. A fizikai dokumentumok biztonságos kidobását törvény írja elő, ezért, ha az iskola nem rendelkezik iratmegsemmisítővel (azzal a készülékkel, amibe bele kell helyezni a papírt, és csíkokra vágja vagy ledarálja), vesse fel a témát az iskolavezetésnek.

Stux-tól a pixabay-ról (Forrás: www.pixabay.com)

Ha foglalkoznak egy iratmegsemmisítő beszerzésével, azt javasoljuk, olyat vásároljanak, ami más dokumentumok, például cd-k felaprítására is alkalmas. Így biztosítható, hogy az elavult információnak még a digitális másolatai is megfelelően lesznek eltüntetve és nem lesznek felfedhetők. Ezek a megsemmisítők hosszú távon valószínűleg még több időt takarítanak meg Önnek, mivel közülük sokan rendelkeznek azzal a képességgel, hogy megsemmisítsék a gémkapoccsal vagy más módon összefűzött iratokat is, ami lerövidíti az iratok megsemmisítésének előkészítésére fordítandó időt.

A papír alapú dokumentumoktól való megszabadulásnak van még egy hatékony, de időigényes módja: egy több élű olló beszerzése. Ez jó megoldás lehet, ha az iskola nem akar saját iratmegsemmisítőt vásárolni, vagy előfizetni ilyen szolgáltatásra, Ön viszont szeretné biztosítani, hogy legalább a saját maga előállított és megsemmisítésre szánt iratokat megfelelően meg tudja semmisíteni.

Amikor otthon szabadul meg a felesleges iratoktól, jó szolgálatot tehet egy több élű olló, feltéve, ha rendszerint nem állít elő otthon túl sok dokumentumot. Az emberek a felaprított iratokat újrahasznosítják állatok almozására (hörcsögök, tengerimalacok és más rágcsálók számára), eltüzelik a kandallóban, vagy, ha a dokumentumok nem túl titkosak, csomagolóanyagként is szolgálhatnak. Összeaprítva papírhulladékként elhelyezhetők és újrahasznosíthatók.

3.6 Wifi hálózatok védelme

Volt már rá példa, hogy letartóztattak pár ártalatlan internetfelhasználót gyermekpornográfia feltöltéséért vagy fenyegető emailek küldéséért, míg a valóságban az történt, hogy a postafiókjaikat hekkerek törték fel az otthonaikban lévő, védelem nélküli wifi hálózatokon keresztül. Az iskolában a rendszeradminisztrátor feladata, hogy gondoskodjon erről, ám ha otthonról dolgozik, tudnia kell, hogy a gyengén védett wifi hálózaton keresztül külső felek is hozzáférhetnek a személyes információihoz.

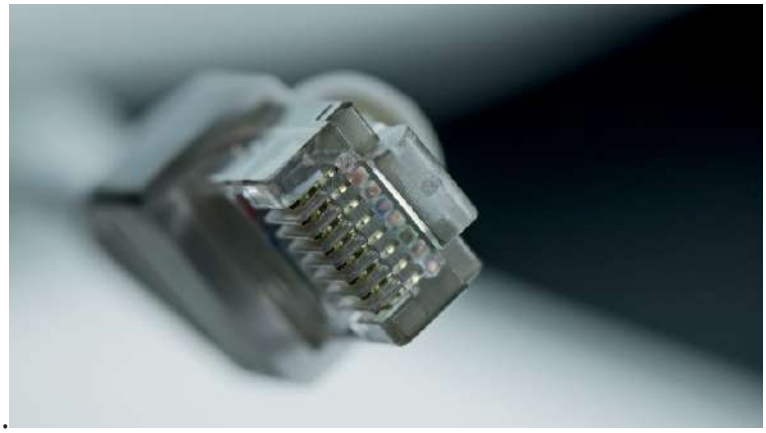
Ez nagyon ijesztően hangzik, és valóban az is, bár van néhány egyszerű lépés, amit megtehet azért, hogy az otthoni hálózata egy kicsit biztonságosabb legyen, és hogy a szomszédok ne tudják lopni a wifijét vagy, ami még rosszabb, hogy az internetes bűnözők ne tudják kihasználni a biztonsági hiányosságokat és átvenni az uralmat a készülékei fölött, ellopni a személyes adatait, vagy bűncselekményeket elkövetni az Ön nevében. A legfontosabb, amit tudnia kell, hogy egyáltalán nem eszköztelen, és hogy már az alapvető biztonsági lépések is hatalmas változást jelentenek, ha az Ön védelméről van szó.

Az első, amit meg kell tennie, hogy az otthoni routerén **változtassa meg az alapértelmezett jelszót**, ha még nem tette volna meg. Ne adjon meg hétköznapi jelszót, ami könnyedén feltörhető! Időről időre változtassa meg a jelszavát, különösen akkor, ha úgy érzi, hogy megváltozott a kapcsolat minősége, vagy ha folyamatosan villog a DATA LED jel a routeren, akkor is, amikor a családban éppen senki nem használja az internetet. A jelszó megváltoztatható a router beállításainak paneljéről, az alábbiakban megvitatjuk azt is, hogyan. Eközben szórakoztathatja magát a különböző hálózati eszközök alapértelmezett felhasználóneveinek és jelszavainak ***listájával***. Ha talál valamit, ami egyezik az Önével, azonnal módosítani kell. Soha ne futtasson nyitott (jelszóval nem védett) kapcsolatot!

A jelszó beállításakor győződjön meg róla, hogy a WPA2 opciót jelöli be, ahogyan a fejezet előző részében tárgyaltuk. Felfrissítheti továbbá a WPA2, a WPA és a WEP különbségeiről szerzett ismereteit ***ezzel a kiváló cikkel*** a How-To Geek-től. A WEP titkosítással védett jelszavakat könnyebb erővel feltörni, mint a WPA2-vel titkosítottakat. Nem biztos, hogy a hekkerek ellenőrzik az otthoni wifi hálózatok sérülékenységét, de sose lehet tudni, és semmi oka nincs, hogy ne használja az erősebb WPA protokolt, kivéve, ha készüléke nem olyan régi, hogy nem támogatja a WPA2-t. Ugyanez érvényes a WPS (wifi védelem beállítás) beállítására is. A WPS egy rövid PIN-szám beírását ajánlja fel Önnek egy jóval bonyolultabb jelszó helyett. A PIN-számokat azonban könnyű feltörni, és míg számos router kizárja a támadót meghatározott számú sikertelen próbálkozás után, nem áll ellen a kifinomultabb WPS támadásoknak. Egyszerűbb ennek elejét venni, és a jelszót választani.

Amennyiben az SSID (vagy az Ön wifi hálózatának a neve) még az alapértelmezettre van állítva, azonnal felfedi a berendezést, amit Ön használ, vagy legalábbis a gondatlanságot, amivel a vezeték nélküli rendszer karbantartását kezeli. Természetesen ne olyanra változtassa, amivel felfedi a kilétét a szomszédok vagy az utcán járó ismeretlenek előtt.

Még egy dolgot tudnia kell: **hogy hogyan férhet hozzá a vezeték nélküli router beállításokhoz.** Rendszerint a 192.168.1.1 beírásával a webböngészőbe és az SSID, illetve a jelszó megadásával lesz lehetősége hozzáférni a router beállításaihoz. Ha ez nem működik, nézze meg a router felhasználói kézikönyvét (ennek online is meg kell lennie, ha Ön esetleg nem tartotta meg a papír alapú használati útmutatót vagy a router dobozát: ***Cisco***, ***Linksys***, ***Netgear***, ***Apple AirPort***, ***D-Link***, ***TP-LINK***.



Fotocitizentől, a pixabay-ről (Forrás: www.pixabay.com)

További tippek, amik hasznára lehetnek az otthoni hálózata megvédéséhez:

- **Kapcsoljon le mindent, amire nincs szüksége!** Ha a routerének van távoli irányítási vagy **távoli felügyeleti** opciója, valószínűleg nem fogja használni ezeket, ezért gondoskodjon róla, hogy le legyenek állítva. Ha nem használ otthonról **FTP** szervereket, kapcsolja ki az opciót! Ha szükség lesz rá, később újra bekapcsolhatja. Ha nem SSH-zik haza, nem akar a routerhez a **Telneten** keresztül kapcsolódni, ügyeljen rá, hogy kikapcsolja ezeket. Szükség esetén ezek is visszavonhatók.
- Vegye fontolóra az UPnP leállítását, ha nem játszik, vagy nem használ torrent szolgáltatásokat. Nézze meg ezt a ***weboldalt***, ami kifejezetten az UPnP támadásokról szól! Még akkor is kikapcsolhatja az **UPnP**-t, ha játszik, vagy torrentkövetőt használ, és manuálisan továbbíthatja a portokat. A portok manuális továbbításáról ***itt*** talál információt.
- Ha vannak okoseszközei vagy megadja az Önhöz látogató vendégeknek a hálózati hozzáférést, gondoljon rá, hogy létrehoz számukra egy **külön hálózatot**. Ez egy biztonsági szempontból célszerű funkció. Azt jelenti, hogy a routere létrehoz egy második SSID-t a vendégek részére, vagy az IoT-eszközöknek, és minden, a vendéghálózathoz csatlakozó eszköz elkülönül az elsődleges hálózaton lévő eszközöktől. Továbbá beállíthatja, mit fognak látni a vendégek az elsődleges hálózatból, és mit nem. A kevésbé biztonságos eszközeit is ehhez a hálózathoz csatlakoztathatja. A hálózatot elkülönítheti külön **SSID**-kkel és **VLAN**-okkal is - további információ ***itt*** és ***itt*** (aczlan kommentje).
- Mialatt vakációzik, vagy hosszabb ideig távol van az otthonától, **kapcsolja ki a routert!** Amíg nincs otthon, úgysem fog rákapcsolódni, és ne hagyja bekapcsolva, ha nincs rá szüksége.

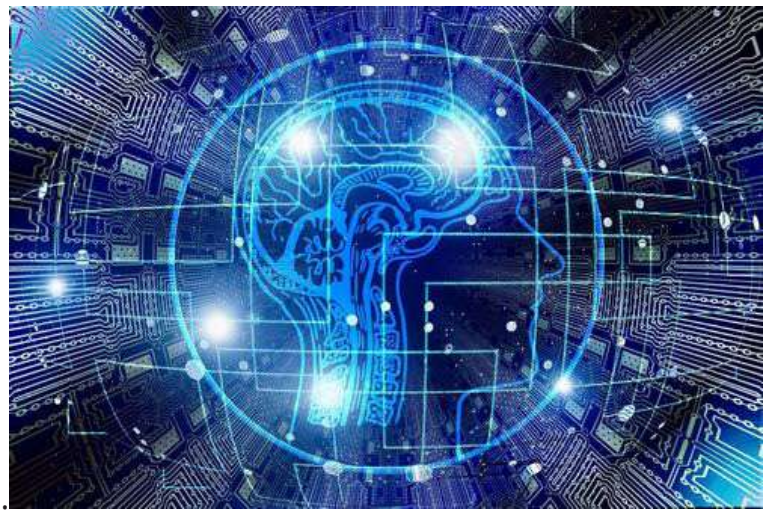
3.7 Megfigyelés és ellenőrzés

A biztonsági megfigyelés és ellenőrzés rendkívül specifikus, de széles körű téma az internetbiztonságban. Itt nem fogjuk részletesen tárgyalni, ahogyan az iparági szintű gyakorlatokat sem. Ezzel a témával szeretnénk felhívni a figyelmet arra a tényre, hogy a jó szintű biztonság fenntartása olyan folyamat, amely figyelemfelkeltést, szokásformálást, éberséget és folyamatos fejlesztést és figyelmet igényel.

Javasoljuk, hogy minden héten ütemezze be a biztonsági gyakorlatai áttekintését, szánjon időt biztonsági másolatok készítésére, az elavult szoftverek és adatok törlésére és az eszközök karbantartására. Minden olyan gyakorlat, amely a személyes adatok és információ védelmére ajánlott, mind az interneten, mind az offline állapotban, folyamatos törődést igényel, és míg némelyikük egy kattintásos feladat, a legtöbbjük megköveteli, hogy újra és újra rájuk nézzen és karbantartsa őket.

A szoftverfrissítés nem tart tovább 15 percnél, ha rendszeresen elvégzi. Az asztal tisztítása vagy karbantartása ugyancsak pár perces erőfeszítést igényel. Az iratok megsemmisítése és a dokumentumok biztonságos törlése a számítógépéről egyre kevesebb időt kíván a kezdeti ráfordítást és erőfeszítéseket követően, és idővel egyre kevesebbet vesz ki Önből. Az információ titkosítása törvényi kötelezettség: szánjon rá időt, hogy ennek eleget tegyen.

Mobileszközeinek védelme sok idegeskedéstől és aggódástól kíméli meg, ezért tanácsos róla gondoskodni. Ügyeljen rá, hogy ezeket a gyakorlatokat a családja körében is elterjessze, és a gyerekeit is a tudatos internetbiztonság és a digitális felelősségvállalás gyakorlatainak megfelelően vértezze fel, hogy ne kelljen a könnyen elkerülhető problémákkal találkozniuk, és ne kelljen feltennie magának a kérdést: „Miért is nem tettem meg?” Biztosítjuk róla, hogy megéri.



Geraltól a pixabay-ről (Forrás: www.pixabay.com)

Összefoglalás

A személyes információ és adatok védelme, ahogyan a tanulók személyes adatainak védelme is, olyan lépés, amit törvényileg, morálisan és érzelmi okokból is meg kell tennie, hogy biztonságosnak érezze a mindennapi életét. Egyetlen eszköz védettségében sem lehetünk 100%-ban biztosak, de a jó internetbiztonsági szokások sokat számítanak és segítenek megőrizni a lelki nyugalmunkat.

Ebben a fejezetben bepillantottunk az adatok offline védelmének és az otthoni hálózatok megvédésének alapjaiba. Az alapszintű tippek és internetbiztonsági gyakorlatok hasznosak lesznek, amikor elkezdi őket használni, ha még nem ismerte volna őket. A titkosítás védelmet és biztonságot jelent a tárolt adatok tekintetében. A fizikai és digitális fájlok biztonsági megfontolásból történő áthelyezése megváltoztatja a gondolkodását az információt illetően, és kétségtelenül segítséget nyújt majd abban, hogyan szervezze meg a fizikai és digitális életterét. A saját otthoni hálózata megvédésének megtanulása révén értékelni fogja az Ön és családja által létrehozott és védett adatokat, és példát mutat majd arra, hogy miért fontos számunkra a személyes adatok és a magánéletünk védelme.

Ezeknek a biztonsági szokásoknak az elsajátítása segít majd a teljes internetbiztonsági tudatosság kialakításában, és abban, hogy magabiztosabbá váljon és kissé jobban megismerje az Ön által nap mint nap alkalmazott technológiát. A legfontosabb, hogy ezek a szokások lehetővé teszik, hogy példát mutasson, átadja tudását az Ön körül lévő embereknek, tanácsokkal segítse a diákjait és bemutassa a digitális identitás és a magánélet védelmének fontosságát.

Linkek, hivatkozások és további információ
https://www.symbaloo.com/mix/vedelmibeallitasok

4. A MAGÁNSZFÉRA VÉDELMÉNEK SZABÁLYAI ÉS A DIGITÁLIS FAIR PLAY

Bevezető

Ennek a fejezetnek a célja, hogy megismertesse Önt az engedélyekkel, szerzői jogokkal és azok típusaival, valamint a GDPR általános kritériumai közül a tanításra vonatkozókkal.

Szó lesz arról, hogyan kezelje a saját digitális entitását, hogyan védje azt meg azokban az adatokban és dokumentumokban, amiket a tanítási gyakorlata során készít, az általános engedélytípusokról, valamint a magánszféra védelméhez kapcsolódó szabályok alapvető tényeiről, illetve arról, hogyan tudja ezeket az ismereteket alkalmazni a tananyagok összeállításában és versenyelőnyként felhasználni az érdeklődési körének, az igényeinek és a tanítási céljainak megfelelően.

Fernando Arcostól a Pexelsről (Forrás: www.pexels.com)

4.1 Szerzői tulajdon és szerzői jog

A tanulóknak szóló oktatási segédanyagok összeállítása és képek, videók, szövegek velük való megosztása nemcsak minden oktató iskolai tevékenységének, hanem magánéletének is része. A források könnyű és gyors online hozzáférése lehetővé teszi, hogy egyedi és vonzó tanulási tartalmakat hozzunk létre. Ugyanakkor elengedhetetlen, hogy a pedagógusok és a diákok egyaránt szilárd alapot kapjanak a jogaik és felelősségeik megértéséhez, valamint a mindennapi munka során alkalmazott tartalomkészítés és -tulajdonlás jogaival és felelősségeivel kapcsolatban.

Az online anyagok jogszerű készítésével és felhasználásával járó felelősségek megtanítása mind magunknak, mind a tanulóinknak nemcsak törvényesség szempontjából fontos: a diákokat a tanítás során a szakma életébe bevezető oktatóknak képesnek kell lenniük arra, hogy mintaként szerepeljenek és mintául szolgáljanak diákjaik számára arról, hogy a **szerzői jogok és a plágium** hogyan és miért lett része az életüknek.

Kezdetnek tekintse meg az alábbi videókat:

- ***Szerzői jogok & Jogkövető használati útmutató tanároknak***
- ***A plágium megismerése & szerzői jog***

- ***http://respectforcopyright.org/***
- ***https://www.commonsense.org/education/lesson/copyrights-and-wrongs-9-12***
- ***https://creativecommons.org/about/***
- ***https://www.teachingcopyright.org/***
- ***https://blog.hubspot.com/marketing/free-content-marketing-tools-list***
- ***https://mediacommons.psu.edu/free-media-library/***
- ***http://www.techsavvyed.net/archives/1997***
- ***https://buffer.com/library/free-images***
- ***https://www.blogtyrant.com/376-super-useful-royalty-free-creative-commons-and-public-domain-websites/***
- ***https://resignal.com/blog/30-free-image-websites-creative-commons-royalty-free/***
- ***https://www.sitepoint.com/creative-commons-sources/***

4.2 Licenctípusok

A jó hír, hogy számos anyag, forrás és média áll az Ön és tanulói rendelkezésére tanítási célú felhasználásra, most ezeket fogjuk bemutatni.

Az első fontos fogalom a **nyilvános** tárgykör. Ez a kézzelfogható tárgyak kategóriája, amelyet oktatási célokra használhat anélkül, hogy fizetnie kellene a használatukért, vagy engedélyt kellene kérnie azok terjesztésére. Ha egy mű a nyilvános tárgykörbe esik, akkor nem tartozik a szerzői jog hatálya alá, vagy a szerzők jogai a tartalom felett lejártak. Ilyenek például a klasszszikus műalkotások, amelyeket a múlt század második évtizede előtt hoztak létre.

Egy másik fontos fogalom Önnek, mint oktatónak, a **Creative Commons Licence**[29] (szó szerinti fordításban kreatív közjavak, rövidítve gyakran használják a CC License elnevezést is). Ez egy nyílt szerzői jogi licenc, ami azt jelenti, hogy a tartalomkészítő ingyenesen engedélyezi a tartalom használatát, bizonyos feltételek mellett. A Kreatív Közjavak licencről (beleértve a képkereséseket, az ingyenes tartalommal rendelkező forrásokat, amiket vegyíthet és újra felhasználhat) bővebben a Creative Commons webhelyen[30] olvashat. Ez a weboldal minden oktató számára tökéletes nyersanyag, ahol ingyenes médiaforrásokat és ingyenes tartalmú linkeket kínál.

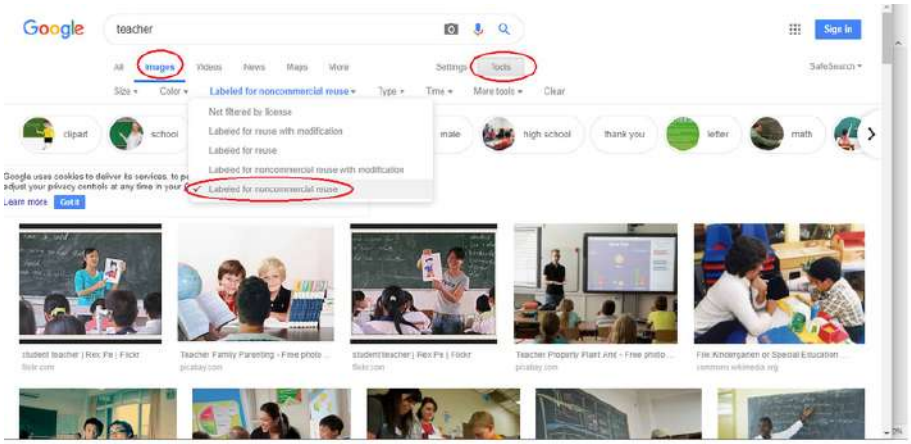
Az ingyenes tartalom ugyanakkor nem jelenti a tartalom korlátlan felhasználását. Önnek, mint oktatónak, aki az információt tanítási célból használja fel, valószínűleg nem kell mindig alkalmaznia, bár fontos ismernie a Creative Commons Licenceinek különböző típusait és ezek ikonjait, így kiválaszthatja a munkájához szükséges leginkább megfelelő tartalmat.

29 https://digiblog.hu/creative-commons-avagy-kreativ-kozjavak
30 https://creativecommons.org/

1. CC BY	***Nevezd meg!***
2. CC BY SA	***Nevezd meg! Így add tovább!***
3. CC BY ND	***Nevezd meg! Ne változtasd!***
4. CC BY NC	***Nevezd meg! Ne add el!***
5. CC BY NC SA	***Nevezd meg! Ne add el! Így add tovább!***
6. CC BY NC ND	***Nevezd meg! Ne add el! Ne változtasd!***

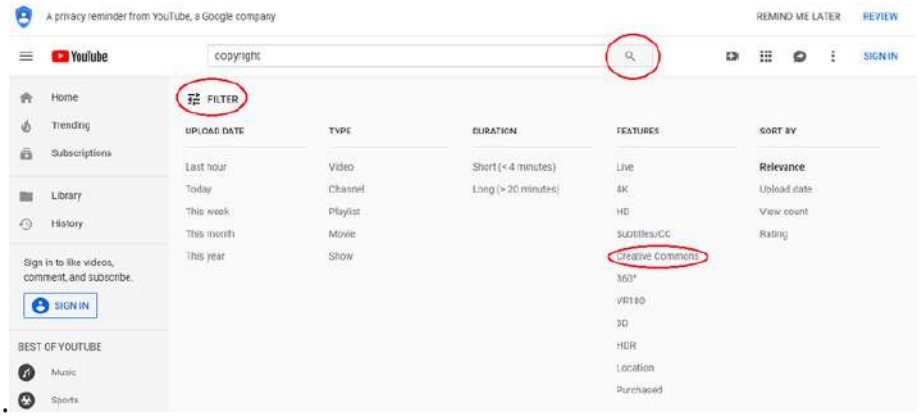
Creative Commons licenceinek típusai
A CC licence szimbólumainak forrása: http://creativecommons.org/about/licenses/

Mint a fent említett képen is láthatja, a Creative Commons licenc lehetővé teszi az ingyenes felhasználást annak megjelölésével, és bizonyos korlátozások mellett. Sok platform biztosítja azt a pedagógusok számára hasznos opciót, hogy nem kereskedelmi célokat szolgáló, ingyenes forrásokat tudjanak keresni. Az alábbi képernyőkép azt mutatja, hogyan lehet bekapcsolni ezt az opciót, a Google Képkeresőjében, hogy a CC licenc alá eső, nem kereskedelmi célokra szánt képeket találjon.



Képernyőkép egy Google keresésről (Forrás: www.google.com)

Egy másik példa a Youtube, ahol megtekinthet és le is tölthet a Creative Commons hatálya alá eső alkotásokat.



Képernyőkép egy YouTube keresésről (Forrás: www.youtube.com)

Ez csupán két példa, bár rengeteg weboldal kínálja fel ezeket a keresési opciókat. Jusson eszébe, hogy amikor tartalmat keresgél, nézze át a szűrőket és az Ön által használt platform speciális keresési beállításait, hogy meggyőződjön róla, van-e lehetősége ilyen tartalom keresésére.

A tartalomengedélyeztetés mellett más licenc típusok is vannak, célzottan a videóklipekre, képekre, vektorképekre és klipartokra, amiket stock (készlet) tartalomként ismerünk. Ezek általában előfizetési alapon működő szolgáltatások, amelyek lehetőséget adnak arra, hogy alacsony havi előfizetési díjjal vagy egyenként vásároljon tartalmat. Bizonyos weboldalak, mint például a vectorstock[31] vagy a canva[32] ingyenes tartalmakat kínálnak tulajdonságoktól függően és bizonyos korlátozások mellett. Egy számos ingyenes vagy olcsó tartalomforrást tartalmazó lista elérhető ingyenesen a hubspot.com blogon[33], és mi is szeretnénk Önt arra ösztönözni, **hogy böngésszen az ebben felsoroltak között, és ossza meg azokat a tanulókkal is.**

4.3 GDPR megfelelőség

Remélhetőleg mostanra sikerült meggyőznünk Önt, hogy a saját és a tanulók magánszférájának megóvása alapvető feladat. A személyes adatok védelme a mások magánéletének és a saját adataikhoz és személyiségükhöz való jogaik gyakorlásában való szabadságának tiszteletben tartását jelenti, mind online, mind offline.

Az Általános Adatvédelmi Szabályzat, a GDPR célja **a természetes személyek alapvető jogainak és szabadságának, különös tekintettel a személyes adatok megóvásához való jogának védelme.** A GDPR 2018. május 25-én lépett hatályba az Európai Unió valamennyi tagállamában, azzal az átfogó szándékkal, hogy harmonizálja az adatvédelmi törvényeket egész Európában (2016/679 / EU AZ EURÓPAI PARLAMENT ÉS A TANÁCS RENDELETE, 2016). A GDPR végrehajtása óta sok európai aggály merült fel a személyes adatok tárolásával és feldolgozásával kapcsolatban - és nem ok nélkül. Van azonban néhány tudnivaló, amit tanárként ismernünk kell, és ami jelentősen javítaná a GDPR-nak való megfelelés témájával kapcsolatos tudatosságát és tapasztalatait.

Először is nagyon fontos röviden megemlíteni az **adatvédelmi biztos vagy DPO** fogalmát. A jelenleg hatályban lévő GDPR-ral összhangban az Európai Unió legtöbb intézményén belül, beleértve az oktatási intézményeket is, kötelező kinevezni egy adatvédelmi biztost. Az iskola adatvédelmi tisztviselőjének alapvető feladatai között szerepel annak biztosítása, hogy a munkavállalók tisztában vannak az adatvédelmi problémákkal és követelményekkel, és munkájuk megfelel az adatvédelemre vonatkozó nemzeti és európai szabályozásnak. Az adatvédelmi biztosnak képesnek kell lennie arra, hogy tisztázza, mi számít **személyes és érzékeny (vagy különleges) adat**nak, és Ön milyen feltételek mellett és hogyan gyűjthet, tárolhat, dolgozhat fel és semmisíthet meg ilyen típusú adatokat. Általában közös megegyezés jön létre arra a két kifejezésre vonatkozóan, amelyhez minden szervezet a maga sajátos összetétele alapján hozzátesz valamit. **Személyes adat**nak számít minden olyan információ, amely segíthet azonosítani egy személyt, mint például a név, a kapcsolattartási adatok, valamint osztályzatok, vagy az iskolai értékelés egyéb formái. Az **érzékeny vagy különleges** kategóriába tartozik például az egyén vallási meggyőződése, szexuális irányultsága, étrend-korlátozásai (amelyek felfedhetik vallását), egészségi állapota, stb. Ezeket csak a szülők és a tanulók tudtával és beleegyezésével, és csak bizonyos feltételek mellett lehet feldolgozni. ***Itt*** olvashat bővebben a különleges kategóriába tartozó adatokról.

31 https://www.vectorstock.com
32 https://www.canva.com
33 https://blog.hubspot.com/marketing/free-content-marketing-tools-list

A fényképek, képek és videók személyes adatokat is tartalmazhatnak. Az arckép személyes adatnak számít. Ezen kívül más adatok, mint például a helymeghatározás, vagy a rögzítés dátuma és időpontja, és mások (ezek EXIF metaadatok néven ismertek) is eltárolódhatnak digitális képek esetén. Még inkább ijesztő módon a nagy felbontású felvételek lehetővé teszik az ábrázolt személyek biometrikus felismerését is. Ezeket az eseteket a GDPR érzékeny személyes adatoknak tekinti. Amikor egy prezentációhoz a tanulók képeit szeretné használni, vagy más módon kívánja azokat harmadik féllel megosztani, kérdezze meg az adatvédelmi biztost!

Az adatvédelmi biztoson kívül további két szerepkör fontosságára is rávilágít a GDPR, nevezetesen az **adatkezelőre és az adatfeldolgozóra**. Mindkét fél eltérő jogi felelősséggel rendelkezik, és ezeket a feladatokat természetes vagy jogi személy, hatóság, ügynökség vagy más testület láthatja el. A GDPR szerint az adatkezelő meghatározza a személyes adatok feldolgozásának céljait és eszközeit – a legvalószínűbb, hogy ez maga az iskola. Az adatfeldolgozó a személyes adatokat az adatkezelő nevében kezeli és szerződést kell kötnie az adatkezelővel. Az adatfeldolgozó lehet egy szoftvertermék, egy olyan online környezet, amelyet a tanításhoz vagy a szülőkkel való kapcsolattartáshoz használhat, de egy olyan személy is, mint például egy fotós, aki az iskolába jön, hogy fotókat készítsen az évkönyvbe, illetve bárki, aki olyan tevékenységet végez, mint az adatok gyűjtése, naplózása és rendezése. Ha, mint a legtöbb tanár, Ön is feldolgozza a diákok adatait, legyenek azok személyes vagy érzékeny adatok, az adatfeldolgozó szerepét látja el.

Adatfeldolgozóként Ön nagyon kényes szerepet tölt be a diákjai személyes adatainak védelmében. Néhány fontos tipp, ami segíthet a diákok adatainak védelmében:

- **Csakis legális szoftvert** használjon, és ismerje meg a **szoftver adatvédelmi szabályait.** Ha kétségei vannak arról, hogy egy adott szoftver megfelel-e a GDPR-nak, azonnal jelezze az adatvédelmi tisztviselőnek. Tudja meg, milyen **személyes vagy érzékeny adatokat** fednek fel a tanulók a szoftver használatával. Ösztönözze őket arra, hogy otthoni számítógépükön csak a törvényesen beszerzett szoftvereket használják, és tájékoztassák őket az illegitim szoftverek használatából eredő kockázatokról.
- **Ha olyan oktatási szoftvert használ,** amely megköveteli a tanulóktól, hogy felhasználói fiókot hozzanak létre, **hangsúlyozza, hogyan védhetik meg az adataikat** álnév alkalmazásával, és ösztönözze őket, hogy tudatosan gondolják végig, hogy az információ személyes jellegűnek minősül-e, vagy esetleg felfedheti-e a személyazonosságukat.
- **Ha új szoftvertermék** bevezetését fontolgatja az iskolában, akkor **értesítenie kell az iskola adatvédelmi megbízottját** annak biztosítása érdekében, hogy az a megfelelő módon történjen.
- **Beszélje meg** az adatvédelmi megbízottal, hogy mi az **adatfeltörés**. Az adatok feltörésének megértése kiemelkedően fontos jogi kötelezettség az Ön számára, és ha azt gyanítja, hogy ilyesmi történt, köteles jelentést tenni az adatvédelmi megbízottnak.
- **Titkosítsa** a személyes és/vagy érzékeny adatokat tartalmazó dokumentumokat és fájlokat. Titkosítsa a munkahelyi számítógépet vagy a személyes és/vagy érzékeny információkat tartalmazó mappákat, személyes adatokat csak az iskolai gépén tároljon, használjon erős jelszavakat, és állítsa be az eszközök automatikus lezárását öt percnyi üresjárat után.
- **Legyen óvatos a mobil tárolóeszközökkel** - titkosítsa azokat, vagy az adatokat, amelyeket USB-meghajtón keresztül szállít, és tudjon róla, hogy sok rosszindulatú program szállítható USB-meghajtók segítségével.
- **Rendszeresen** frissítse a **vírusirtó szoftvert**.

- **Legyen óvatos az online kommunikációval.** Ne írjon bele személyes adatokat az emailekbe, vagy ha mégis muszáj, küldje el titkosított tartalomként. A munkaeszközöket és profiljait mindig a munkával kapcsolatos kommunikációhoz használja. Legyen óvatos, amikor az emaileket megnyitja és válaszol rájuk.
- **Tájékozódjon** – tudjon meg többet az internetes higiéniáról és a védelemről, és próbáljon többet megtudni a GDPR betartásáról. A fejezet végén feltétlenül keresse fel a GDPR-ral kapcsolatos forrásokat.
- **Biztosítsa, hogy a tanulók és szüleik előzetes információ után adják beleegyezésüket** a nem rendszeres adatgyűjtéshez, például felmérésekhez, projektekhez, interjúkhoz stb. Tekintse át az adatvédelmi megbízottal közösen, hogy milyen adatgyűjtést kíván végrehajtani, amelyhez a szülők és a tanulók tájékozott beleegyezése szükséges.
- **Tanulja meg**, **hogyan lehet EXIF metaadatokat elrejteni a képekben** – javaslunk oktatóanyagokat, a ***Nortontól*** és a ***MakeUseOf*** – tól amelyek segítenek Önnek ebben.
- **Végül, de nem utolsósorban**, ösztönözze és mozdítsa elő a felelős adatkezelést és az adatvédelmet a tanulók körében. Magyarázza el nekik, és dolgozzon velük együtt az identitás tiszteletének és az adatok értékének megértésében. A ***Joint Research Centre*** által kifejlesztett Cyber Chronix mobiljáték vonzó módon vonja be a diákokat az adatvédelemről szóló vitába és értékelésbe. A játék azzal a céllal készült, hogy a fiatalokkal megismertesse a fogalmakat, ideértve a személyes adatok fogalmát, az elfelejtéshez való jogot, a személyes adatok megsértését, az adatok hordozhatóságát és a tájékozott beleegyezést. A játékosok egy futurisztikus bolygóra kerülnek, néhány fényévre a Földtől. A cél az, hogy segítsenek a karaktereiknek eljutni egy partyra, miközben számos adatvédelmi akadályba ütköznek az útjuk során.

Ha többet szeretne megtudni a GDPR-ról és a GDPR-nak való megfelelésről, vegye fel a kapcsolatot az iskola adatvédelmi biztosával és tájékozódjon[34].

4.4 Adatvédelmi irányelvek

A magánélet védelme és a saját adatokhoz való jog az Európai Unió alapokmányaiban megfogalmazott alapelvek között szerepel. Nekünk, mint az Európai Unió tanárainak, be kell tartanunk az Unió törvényeit, hogy megvédjük és tiszteletben tartsuk diákjaink saját adataikkal és személyazonosságukkal kapcsolatos jogait. Ez egyike az Emberi Jogok Európai Egyezménye alapvető nyilatkozatainak, és része az EU jogszabályainak, amelyeket a tagországoknak tiszteletben kell tartaniuk.

Ebben a részben elsősorban a webplatformokkal, a digitális eszközökkel, a programokkal, felszereléssel és alkalmazásokkal kapcsolatos adatvédelmi alapelveket tárgyaljuk, és megvitatjuk azok néhány, a tanári szakma gyakorlása szempontjából legfontosabb aspektusát.

Szeretnénk kiemelni azokat a problémákat, amelyek **az iskolában oktatási célokra alkalmazott új szoftver bevezetését érintik**. Ha új szoftvert szeretne alkalmazni a tanulási környezetéhez, akkor a legfontosabb lépés az, hogy megismerje a **szoftver adatvédelmi szabályzatát**, és kapcsolatba lépjen **az iskola adatvédelmi megbízottjával** a döntés meghozatala érdekében, arról, hogy ez a szoftver alkalmas-e iskolai használatra.

34 a II. fejezetben közzétesszük a tanár továbbképzésben résztvevők által készített tematikus gyűjteményt, melyben talál a témával kapcsolatos releváns szakirodalmat

Az adatvédelmi szabályzat olyan jogi nyilatkozat, amely ismerteti, hogyan és mit kezel a szoftver kibocsátója és potenciálisan (és a legvalószínűbben) a harmadik fél a felhasználói adatokra vonatkozóan. Más szavakkal, az adatvédelmi szabályzatnak elegendő információt kell szolgáltatnia arról, hogy mely adatokat gyűjtik, kezelik bizalmasan, osztják meg, vagy használják fel akár profitszerzés céljából.

Az adatvédelmi szabályzathoz **adathasználati nyilatkozat** is csatolható, amely határozatlan időre részletesebb információt nyújt arról, hogy mit, hogyan és milyen célokra gyűjtenek. **Ismerkedjen meg egy szoftver adatvédelmi politikájával és adathasználati nyilatkozatával (ha van ilyen), és vigye magával az iskola jogi részlegével, etikai bizottságával és adatvédelmi tisztviselőjével folytatott megbeszéléshez.**

Mit kell keresni egy adatvédelmi szabályzatban?

A Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) „*A Tanács ajánlásainak a személyes adatok magánéletének és határokon átnyúló áramlásának védelmére vonatkozó iránymutatásokról szóló tanácsi ajánlások*" értelmében a magánélet védelmére vonatkozó irányelvei szerint

- értesíteni kell arról, mikor, milyen adat kerül gyűjtésre, és milyen célból,
- mik az adatok gyűjtésének okai az adatvédelmi szabályzatokban,
- jóváhagyást kell kérni ezen adatok gyűjtésére és feldolgozására, valamint tájékoztatást kell adni a tárolt adatok védelme érdekében alkalmazott biztonsági intézkedésekről,
- minden adatvédelmi szabályzatnak továbbá tájékoztatnia kell az adatok nyilvánosságra hozataláról, és mindenkor hozzáférést kell biztosítania az adatok megtekintéséhez.

Végül, de nem utolsósorban, a szoftver kibocsátójának az adatvédelmi szabályzat kitételeként egyértelmű elszámoltathatósági rendszert kell leírnia, amelyben kijelenti, hogy miként fogják időben tájékoztatni az összes felhasználót a magánszférájukkal kapcsolatos biztonsági sérülésekről, és biztosítani számukra azt rendszert, amely révén a felhasználók az adatgyűjtőket felelősségre vonhatják a magánélettel való visszaélés miatt.

Miután meggyőződött arról, hogy ezek a pontok jelen vannak a választott szoftver adatvédelmi és adathasználati nyilatkozatában, ismerkedjen meg az iskola új oktatási szoftverek kiválasztására vonatkozó szabályzatával. Kövesse a szabályzatban meghatározott irányelveket, és vegye fel a kapcsolatot a döntés meghozataláért felelős emberekkel. Lehet, hogy a használni kívánt szoftvert az iskola már engedélyezte, és jelenleg egy kolléga használja. Ebben az esetben kérdezzen bármit, amit tudnia kell ennek a szoftvernek az oktatási környezetben történő használatáról, hogy biztosítsa a diákok magánszférájának etikus és legális kezelését.

Nem ritka, hogy tanárként szembekerülünk a tanulókkal vagy a szülőkkel az osztálytermi szoftver kiválasztása során. Legyen felkészülve az ilyen párbeszédekre, és indokolja meg, miért ezt a szoftvert választotta, beleértve **az osztályban már használt szoftveres eszközöket illető ismereteit és azok adatvédelmi irányelveit.** Vizsgálja meg kritikusan az osztálytermében már használt szoftvert. Bizonyos szoftvertermékeket már évek óta használhatnak az iskolában, de ez nem feltétlenül jelenti azt, hogy megfelelnek, vagy figyelmen kívül hagyhatja a magánszféra irányelveit és a hallgatói adatok kezelésére vonatkozó nyilatkozatokat.

Az adatvédelmi irányelvek közötti böngészés során legyen körültekintő, és **keressen olyan kifejezéseket, mint a FERPA (a családi oktatási jogokról és a magánélet védelméről szóló törvény), a COPPA (a gyermekek online magánélet-védelméről szóló törvény), a GDPR (általános adatvédelmi rendelet) vagy a PPRA (a tanulók jogainak védelmét módosító törvény)**. Beszéljen a jogi részleggel az esetlegesen nem megfelelő iskola adatvédelmi irányelvekről.

Az is megtörténhet, hogy a tanulói egy új szoftverterméket akarnak használni egy feladathoz vagy egy iskolai projekthez. Fontos, hogy ne tántorítsa el a diákokat attól, hogy túllépjenek az iskolai tanterv eszközein, és hogy az osztálytermi lehetőségeken kívül más oktatási lehetőségeket is felfedezzenek, ám ez bizonyos veszélyeket és felelősségeket hordoz Önre nézve. Oktatóként hivatalosan nem hagyhatja jóvá az iskolai szoftverek által nem támogatott eszköz felhasználását. Ha egy ilyen termék használata nem egyeztethető össze a feladat céljaival, akkor egyértelmű a helyzet. De ha igen, ez nagyszerű lehetőség arra, hogy megtanítsa a diákjainak mindazt, amit figyelembe kell venni egy új szoftver használatakor.

Először azt javasoljuk, hogy kérje meg a tanulókat, tájékoztassák a szüleiket, és velük együtt telepítsenek egy új szoftvert, vagy menjenek végig egy új szoftver beüzemelésén. Nagyszerű lehetőség a diákok bevonására az adatvédelem és az adatok biztonságának megvitatásába. Kérdezze meg a diákjait, hogy létre kell-e hozniuk egy profilt a szoftver vagy a platform használatához, amelyet telepíteni szeretnének a feladathoz, milyen információkat kell megadniuk a szoftver használatához, és jól adják-e meg ezeket az információkat. Az adatok bármilyen adatok lehetnek, nevektől és email címektől kezdve a pénzügyi információkig, életkorig vagy lakcímig - hozzájárulnának-e a tanulók szülei ezeknek az információknak a megadásához, és a használni kívánt szoftverhez kell-e szülői engedély?

Vegyen részt párbeszédben a tanulókkal arról, hogy az alkalmazás használatával megosztott információkat megosztják-e másokkal - ki láthatja például a nevüket? Mondja meg nekik, hogy ellenőrizzék az adatvédelmi irányelveket vagy az adathasználati nyilatkozatot. Gyűjt-e az alkalmazás további adatokat? A további adatokhoz a képekből is hozzá lehet jutni - megosztanak-e valahol személyes fényképet? A kép helymeghatározási információkat is tartalmazhat – megosztják-e a tartózkodási helyüket vagy az országot? Gyűjt-e az alkalmazás valamiféle okból GPS-adatokat?

Ezeket a kérdéseket kell mérlegelnie, ha új szoftvert tervez bevezetni a tanításban, tehát ugyanazokat az elővigyázatossági elveket kell alkalmaznia, mint amiket egyébként a tanulóknak tanácsolna. Ne feledje, hogy nem jelent problémát, ha a diákok nem tudnak azonnal válaszolni minden kérdésre. Ha lehetséges, kérje meg őket, írják le ezeket a kérdéseket, és tanulmányozzák egy-két napig, és kérje meg őket, hogy beszéljenek a szüleiknek az esetleges kétségeikről. Ez egy nagyszerű tanulási lehetőség a számukra a saját jogaikról és a szoftvertermékek használatához szükséges személyes adatok megadására vonatkozó álláspontjukról. Ügyeljen rá, hogy tudassa a tanulókkal, hogy ezek az ő adataik, és nekik vannak jogaik felettük.

4.5 Tisztelet és felelősség tanítása

Meglehetősen gyakori, hogy a tanárok félnek felhozni a digitális felelősségvállalás témáját, ha hiányoznak azok az eszközök és ismeretek, amelyek a diákok biztonságának a digitális világban történő megőrzéséhez szükségesek. A legfontosabb lépés, hogy bővíti saját tudását, és Ön is azt teszi, amiről beszél. Ha azt látják, hogy **Ön is betartja azokat a dolgokat, amikről beszél,** akkor értékrendet mutat a számukra, ami sokkal inkább kifejezőbb a puszta szavaknál.

Tudjuk, hogy nem olyan könnyű új anyagot beépíteni a már meglévő, szorosan kötött iskolai tantervbe. Noha felismertük, hogy szükség van az internetbiztonsági ismereteknek és kérdéseknek szentelt foglalkozásokra, javasoljuk, hogy kezdje el ezeket a témákat folyamatosan **beépíteni a mindennapi tanórákba**. A legjobb módszer annak biztosítására, hogy a tanulók megismerjék a digitális polgársággal járó jogokat és kötelességeket az, hogy a digitális állampolgárság témáját rendszeres óráik részévé tegyük. Mivel az órái valószínűleg magukban foglalják valamilyen szinten a technológiával való foglalkozást is, kialakulhatnak a jó digitális kultúra gyakorlásának szokásai. Ha például a tanulóknak prezentációt kell készíteniük egy adott témáról, követelje meg tőlük, hogy lábjegyzékként szerepeltessenek minden szerzői és szellemi tulajdonjogot a diákban, és kérje meg őket, hogy egy bizonyos színnel emeljék ki ezeket. Mindig, amikor a hallgatók írásbeli dolgozatot adnak be Önnek, kérje őket arra, hogy adják meg az általuk használt fényképek forrásait, és mutassa meg nekik azokat az online helyeket, ahonnét szerzői jog nélküli képeket szerezhetnek. A fiatalabb diákokat is megkérheti arra, hogy gondolkozzanak el azon, hogyan éreznék magukat, ha valaki az ő engedélyük nélkül hasznot húzna a nehezen elvégzett munkájukból.

Javasoljuk továbbá olyan interaktív webhelyek és alkalmazások használatát, mint például a Szerzői jog tiszteletben tartása[35], amelyek az életkornak megfelelő és vonzó tartalmat szolgáltatnak annak érdekében, hogy a tanárok a digitális világban meglévő szabadságukról, jogaikról és felelősségükről tanítsák a diákjaikat.

A tanároknak képesnek kell lenniük megértetni és megtanítani a tanulókkal a szerzői jogokat, a nyilvános domaint, a tisztességes felhasználást és a Creative Commons-t. Ebben a misszióban számos forrás, óraterv és alkalmazás áll a tanárok rendelkezésére, hogy hozzásegítsék a fiatal felnőtteket az okos döntések meghozatalához szükséges stabil alapismeretek megszerzéséhez online:

- Common Sense Education[36] – fantasztikus órák és animált videók a szerzői jogokról és a tisztességes felhasználásról.
- Teaching Copyright[37] – ismeretek a nyilvános domainről.
- Creative Commons[38] – itt kiváló minőségű, vonzó videókat talál a szerzői jogokról és a Creative Commons licencekről.

Fontos, hogy megosszon a diákokkal olyan listákat és forrásokat, amelyek tartalma szabadon használható oktatási célokra. Az egyik ilyen lista a fent említett hubspot.com blog[39]. A tanulók körében terjeszthető további hasznos listák a mediacommons webhelye[40], a techsavvyed.net[41], a buffer.com[42], a blogtyrant.com[43], a resignal.com[44], a sitepoint.com[45], hogy csak néhányat említsünk. Győződjön meg róla, hogy a tanulók rendelkeznek-e olyan erőforrásokkal, amelyek szükségesek ahhoz, hogy a tartalmat tisztességes módon használni tudják a feladataikhoz az iskolaéveik alatt.

35 http://respectforcopyright.org
36 https://www.commonsense.org/education/lesson/copyrights-and-wrongs-9-12
37 https://creativecommons.org/about
38 https://www.teachingcopyright.org
39 https://blog.hubspot.com/marketing/free-content-marketing-tools-list
40 https://mediacommons.psu.edu/free-media-library
41 http://www.techsavvyed.net/archives/1997
42 https://buffer.com/library/free-images
43 https://www.blogtyrant.com/376-super-useful-royalty-free-creative-commons-and-public-domain-websites
44 https://resignal.com/blog/30-free-image-websites-creative-commons-royalty-free
45 https://www.sitepoint.com/creative-commons-sources

Mint a leckében korábban már említettük, mindenki, aki eredeti és kézzelfogható tárgyat hoz létre, függetlenül a felhasznált média fajtájától, szerzői jogi művet készít. Ez azt jelenti, hogy **a tanulók eredeti munkája szerzői jogvédelem alatt áll**. Ügyeljen rá, hogy engedélyt kérjen tőlük, ha meg akarja osztani a munkáikat, például megmutatni a kollégáinak, vagy újra felhasználni. Ettől értékesnek érzik majd a munkájukat, és megmutatja nekik a szerzői jogok fontosságát is. Sok diák nem igazán törődik a saját szerzői jogaival, vagy nem is tud róluk, így fontos, hogy tudjanak róla, hogy a szerzői jogi törvények őket is védik, és arra irányulnak, hogy tovább fejlesszék az alkotóképességüket, és a különféle médiaeszközök segítségével felfedezzék a kreativitásukat.

Valószínűleg néhány tanulónak ez már nem újdonság, mivel manapság nem szokatlan, hogy a tinédzserek kreatív tartalmakat tesznek közzé különböző platformokon, és akár pénzt is keresnek ezzel. Ha van YouTuber diákja, vagy tud valakiről, aki már online tartalmat értékesít, érdemes lehet bevonni őket a társaik saját szerzői jogaikkal kapcsolatos tanulásának folyamatába. Folytasson le velük egy rövid szemináriumot, ahol a tizenévesek, akik gördülékenyen alkalmazzák ezeket a fogalmakat, megoszthatják tapasztalataikat a társaikkal és Önnel is. A tanulók valószínűleg nagyobb érdeklődést is mutatnak majd egy társuk szavai iránt, aki már jobban megérti a szerzői jogok fontosságát.

Tanítsa meg hallgatóit a GDPR-ra és a saját személyes adataikkal kapcsolatos jogaikra. Ismertesse meg őket az adatok visszavonásának jogával, és segítsen nekik megérteni az adatok fontosságát. Beszéljen velük az oktatási célokra használt különféle szoftverekről, és foglalja össze az ezekre vonatkozó adatvédelmi irányelveket, hogy belássák, ez olyasvalami, amit érdemes megemlíteni, és amiről érdemes beszélni.

Végül, de nem utolsósorban, ne felejtsük el, hogy a tanulók digitális tisztességre való tanítása nemcsak a tanár feladata. Közös felelősség, amelyet megosztunk társadalomként. A szülők rábeszélése, hogy gyermekeikkel beszélgetéseket folytassanak a digitális felelősségről szintén fontos lépés, amelyet megtehet annak érdekében, hogy segítsen a diákoknak továbbfejleszteni a témával kapcsolatos ismereteiket.

Startup Stock fotó a Pexels-ről (Forrás: www.pexels.com)

ÖSSZEFOGLALÁS

Ebben a leckében áttekintettük a pedagógus szakma szempontjából legfontosabb szerzői jogi, tulajdoni, és tartalom licenccel kapcsolatos témákat, és a GDPR-nak való megfeleléssel kapcsolatos általános eszközöket. Adtunk néhány általános tippet a digitális személyazonosság kezelésével és védelmével kapcsolatban az oktatási tevékenység keretében Ön által készített dokumentumokról és adatokról.

Arra számítunk, hogy Ön mostanra már ismerős a nyílt licencek, valamint az adatvédelmi irányelvek néhány területén, és rendelkezik olyan magabiztossággal, amely lehetővé teszi ezeknek az ismereteknek az alkalmazását az oktatási forrásanyagok fejlesztésében és versenyelőnyként történő felhasználásában, érdeklődési körének, igényeinek és oktatási céljainak megfelelően. Kifejezetten javasoljuk, hogy ásson mélyebbre, és jusson több ismerethez a témákról. Végül, de nem utolsósorban, reméljük, hogy meggyőztük Önt arról, hogy a tanulók felelősséggel történő felruházása a digitális tartalom használatával és a saját működő alkotásaik terjesztésével kapcsolatban kiemelkedően fontos a jövőbeni karrierjük, iskolai feladataik és alapvető digitális higiéniai szokásaik szempontjából. Egy olyan világban, amelynek előrehaladása a kemény munkától, a kreativitástól és az intellektuális teljesítménytől függ, a kölcsönös tisztelet kultúrájának ápolása lehetővé teszi a tanulók számára, hogy felelősségteljes felhasználóként és tartalom-előállítóként nőjenek fel, ami fontos tényező lesz a közösségünk fejlődésében.

További részletekért - az ebben a részben nyújtott források felhasználása mellett - arra bátorítjuk Önt, hogy végezzen saját kutatást, és beszéljen az iskola rendszergazdájával, adatvédelmi biztosával.

Felhívjuk a figyelmét, hogy a Be@CyberPro projekt NEM ad jogi tanácsot, és nem mutat be a területen bevált jogi gyakorlatokat. Ez a fejezetrész csak alapvető kiinduló oktatási anyagot kínál, amelyben megismerkedhet a fentiekkel, és amely segíti abban, hogy rájöjjön, mire kell rákérdeznie, és hogy fel tudja tenni a jó kérdést. Ezeket a forrásokat kritikus szemlélettel, és csak általános jellegű oktatási információként kell kezelnie a kérdések megválaszolásában vagy a döntésekben, a bevált gyakorlatok alapján, és a helyi jogszabályok és tanácsadás szintjén.

Linkek, hivatkozások és további információ
https://www.symbaloo.com/mix/maganszferavedelme

3. MODUL: AZ EGÉSZSÉG, A JÓLÉT ÉS A KÖRNYEZET VÉDELME

BEVEZETŐ

Ebben a fejezetben is igen sok szó esik majd a biztonságról és az egészségről. Most azonban – új, eddig még nem érintett - nézőpontból vizsgáljuk a témát. Olyan fontos kérdésekkel foglalkozunk, mint a technológiák folyamatos és hosszantartó használatának fizikai és pszichológiai egészségre gyakorolt hatásai, az egészségre káros veszélyforrások. Szó lesz továbbá a közösségi média pozitív és negatív hatásairól, írunk a digitális átalakulás környezetre gyakorolt hatásáról is, végezetül pedig az európai és hazai kiberstratégiáról és jogi szabályozásról.

Az első részben arra hívjuk fel a figyelmet, hogy a technológia hosszantartó, folyamatos használata milyen hatást gyakorol az egészségre. Foglalkozunk az ergonómiai követelményekkel, a fizikai egészségkárosító veszélyekkel, melyek a felnőttek mellett a fiatalokat, sőt a gyermekeket is érintik.

Foglalkozunk továbbá a pszichológiai jóléttel, amely magába foglalja az egyén érzelmi egészségét és általános működését. A magas pszichológiai jóléttel rendelkező emberek tetterősnek és támogatottnak érzik magukat, boldogok, és elégedettek az élettel. Ahogyan a digitális technológia egyre inkább elterjedtté válik, életünk részévé lett, időszerű annak felvetése, hogy ez a digitális környezet milyen hatással van az emberek pszichológiai jólétére.

A digitális technológiák veszélyeztethetik az emberek jólétét, kezdve az internetes zaklatástól az online biztonság és adatvédelem megsértéséig. Az embereknek a digitális világhoz igazított változatos készségekre van szükségük ezeknek a kockázatoknak az enyhítésére. A munkaerő-piaci készségeken túl az érzelmi és társadalmi készségek különösen fontosak a digitális technológiák teljes kihasználása és az online világban való biztonságos navigálás érdekében.

A technológia szélsőséges használatát számos mentálhigiénés kockázattal hozták összefüggésbe, mint például a depresszió, a szorongás, a függőségek, a figyelemhiány és a bipoláris zavarok, különösen a gyermekek körében. Mindezeken túl foglalkoznunk kell azzal is, hogy a digitális technológiák milyen hatással bírnak a társadalmi jólétre.

Mint minden technológiai újításnak, a közösségi médiának is vannak negatív és pozitív hatásai. A legújabb tanulmányok azonban egyértelműen be is bizonyítják, hogy a digitális technológiák (és köztük a közösségi média) képesek összekapcsolni az embereket egymással, javítani az életminőségüket a magány és a társadalmi elszigeteltség feloldása révén.

A számítógépek és valamennyi digitális eszköz fokozott használata megváltoztatja az életünket. Ezt az óriási hatást nevezzük digitális átalakulásnak, mely az előnyei mellett potenciálisan negatív hatással bír a környezetre nézve.

Mint minden más eszköz esetében, az etikus és felelősségteljes felhasználást és az ártalmak csökkentését szem előtt kell tartani, és ez az emberek viselkedésén múlik.

A rövid életciklus, a folyamatos frissítések és kedvenc technológiánk új verziói azt jelentik, hogy sok hulladék keletkezik. Az elektronikai hulladékok, valamint a gyártási folyamatok során keletkező hulladékok ártalmatlanításához nagyon speciális ártalmatlanítási módszereket kell alkalmazni. Ezt a hulladékot „elektronikai szemétnek" hívják, és mindenféle veszélyes anyagot tartalmaz, amelyek a környezet számára nagyon ártalmasak. Speciális módszerekkel kell őket ártalmatlanná tenni. Oktatásra és szabályozásra van tehát szükség annak biztosításához, hogy ezeket az eszközöket valóban okosan használják fel.

Végezetül ebben a fejezetben röviden bemutatjuk, hogy az Európai Unió hogyan szabályozza e rohamosan fejlődő, változó területet, és teremti meg ezáltal állampolgárai számára a biztonságos kiberteret. Az EU kibervédelmi stratégiája mellett fontosnak tartjuk azt is, hogy Magyarország hol tart a jelenlegi - az EU-val harmonizáló - nemzeti szabályozásban.

1. A FIZIKAI EGÉSZSÉG KÁROSODÁSA A TARTÓSAN SZÁMÍTÓGÉPPEL DOLGOZÓKNÁL

Ebben a fejezetrészben összefoglaljuk azokat az egészségügyi kockázatokat és veszélyeket, melyek a számítógéppel dolgozó felnőtteket éppúgy érintik mint a tartósan, a digitális eszközökkel (kommunikáció, játék, tanulás és egyéb közösségi együttlét) sok időt töltő fiatalokat, és egyre inkább a gyerekeket is. Foglalkozunk a legjellemzőbb betegségtípusokkal, az ergonómiával, az ergonómiai követelmények és szabványok szerinti eszközállomány és munkakörnyezet kialakításával.

Minden Európai országban nyilvánvaló célkitűzés volt az elmúlt évtizedben a digitális írástudás[46] széles körű elterjesztése. Ugyanakkor azt is látnunk kell, hogy a megváltozott környezet – amelyben egyre többen töltenek el mind több időt – milyen hatást gyakorol a számítógép előtt ülők fiziológiai jellemzőire.

Ebben a részben azt a kérdést járjuk körül, hogy milyen egészségügyi veszélyei, egészségkárosító hatásai lehetnek a túlzott számítógép-használatnak, továbbá, hogy miként lehet ezeket az ártalmakat megelőzni.

Az irodai környezetben végzett munkát alacsony kockázatú környezetnek tekintik, annak ellenére, hogy az Európai Unión belüli munkavállalók nagy (és egyre növekvő) aránya veszélyeztetett, és jelentős számú munkavállaló potenciálisan ki van téve az egészségre felmerülő kockázatoknak.

46 Az információs és kommunikációs technológiák (IKT) kezelésére napjainkban használatos gyűjtőfogalom a digitális írástudás (digital literacy) integrálni igyekszik a tudást és a képesség elemeket, alapismereteket és speciális használatot. Maga a fogalom, az írástudás, mint képesség értelmezésén alapszik. Az írástudás folyamatos tanulást igényel, s így teszi lehetővé, hogy elérjük életcéljainkat, bővítsük ismereteinket és képességeinket, és hatékonyan vehessünk részt szűkebb és tágabb közösségünk életében. (UNESCO Literacy portál, 2009

Forrás: https://kaposvarivedonok.blog.hu/2011/09/15/gerinc_vedelme

1.1 Ergonómiai követelmények

A képernyő előtti munkavégzéshez – a munkahely elemeinek (pl. szék, asztal, képernyő, billentyűzet, irattartó, lábtámasz) összhangját meg kell teremteni az ergonómiai követelmények figyelembevételével. A képernyő előtt végzett munka csak látszólag könnyű, valójában nagyfokú, állandó figyelemösszpontosítással, és a szem fokozott terhelésével jár.

Irodai ergonómia [47]

A nem megfelelő testhelyzet, a munkakörnyezet helytelen kialakítása, a képernyős munkahelyekre[48] vonatkozó ergonómiai követelmények be nem tartása még fárasztóbbá teszi ezt a munkát.

47 **Ergonómia** az ember-gép-munkakörnyezet kapcsolatát vizsgáló tudományág. Az ergonómia a görög ergon = 'munka' (***görögül***: ργον), valamint a nomos = 'tan, törvény' (***görögül***: νόμος) szavakból alkotott szóösszetétel. Célja a szűkebb és tágabb munkakörnyezet, a gépek, munkaeszközök emberhez igazítása, az emberi adottságoknak lehető legjobban megfelelő munkaeszközök és munkakörnyezet kialakítása.

48 Képernyős munkakörnek az a munkakör minősül, amelyben a munkavállaló a napi munkavégzése során összesítve legalább négy óra időtartamban képernyős eszközt használ.

Emiatt a számítógéppel dolgozók gyakran panaszkodnak a következőkre: fáradtság, ideges-ség, szembántalmak, fej-, hát- és kézfájás.

A számítógép tartós használatának hatása
Forrás: https://www.usanotebook.hu/blog/milyen-hatassal-van-a-szamitogepa-szemunkre-es-hogyan-tudjuk-megkimelni/495

Ezek a panaszok a stressz hatásaiból, a szem túlterheléséből, a nem megfelelő testhelyzet-ben végzett tevékenységből, az ergonómiai követelményeket nem kielégítő eszközhasználat-ból és egyéb, a munkakörülmények nem megfelelő kialakításából adódhatnak.

Milyen elvek szerint alakítsuk ki a számítógépes munkahelyünket?

Az ergonómiai szempontból megfelelő számítógépes munkahelyek kialakításának fontos szerepe van, mivel a számítógéppel dolgozók jelentős része munkahelyéhez kötött munkát végez.

Helyes testtartás
Forrás: https://tudasbazis.sulinet.hu/hu/termeszettudomanyok/az-egeszseges-eletmod/az-egeszseges-elet-mod/a-munkahelyek-kialakitasanak-ergonomiai-szempontjai/a-szamitogepes-munkahelyek-kialakitasa

Tíz pont a tervezéshez

Nagyon sok múlhat azon, hogy milyen tényezőket veszünk figyelembe akkor, amikor a számítógépes munkahelyeket tervezzük. A Cornell Egyetem tanulmánya a következő 10 kérdést tartalmazza, melyre a megfelelő válaszokat kell megadni annak, aki egy egészséges munkahely megvalósítását tűzi ki célul.

- Hogyan fogják használni a számítógépet (kizárólag egyvalaki ül majd a képernyő előtt, vagy megosztott munkahely lesz)?
- Milyen típusú a számítógép (asztali vagy hordozható)?
- Milyen az asztal?
- Milyen a szék?
- Milyen típusú munka folyik majd az adott gépen?
- Mi van a látómezőben (kiegészítő anyagok, segédletek)?
- Milyen a pozitúra, mely meghatározó a munkavégzés során?
- Mit kell a használó keze ügyében tartani?
- Hová kerül a billentyűzet, és hová az egér?
- Mi a jellemző a környezetre, ahol a munka folyik (fényviszonyok, szellőzés, hőmérséklet, zajok)?

A Cornell Egyetem tanulmányának készítői nem feledkeztek meg arról sem, hogy felhívják a figyelmet a munkavégzés során beiktatandó szünetekre. Ez lehet egyszerű szempihentetés (szemtorna), kézlazítás (az ajánlott idő két perc), pihentető szünet (fél- vagy egyóránként javasolt felállni, sétálni), átmozgató tornagyakorlatok.

1.2 Egészségügyi kockázatok és veszélyek a fiataloknál, gyermekeknél

A számítógép és a többi intelligens eszköz folyamatos, és napi több órán keresztül történő használata inkább káros a szervezetünkre, mint hasznos. Nem csak mentális, hanem fizikális problémákról, illetve betegségekről beszélhetünk (bár sokkal több a mentálisan károsító hatás). Tagadhatatlan, hogy a mai, gyorsan fejlődő világban ezek az eszközök fontos szerepet játszanak az emberek életében, de mindig tudnunk kell, hol a határ.

Az utóbbi évek ezirányú kutatásai a fiatalok egészségügyi problémáit is kimutatták, ezek közül csak azokkal foglalkozunk, melyek a **fizikai egészségre jelentenek veszélyt**, a többiről a következő részben olvashatnak**.**

Gerincferdülés, mozgásszegény életmód

Ha valaki sokat ül a számítógép előtt, előbb-utóbb megfájdul a háta, nyaka. Ha nem mozgunk eleget emellett, akkor rövidesen gerincproblémák jelentkezhetnek. Ugyanakkor a mozgáshiány következményei közül a legfontosabb a testsúlynövekedés és az összes, elhízással járó szövődmény. A gyermekkorban kialakuló súlyfölösleg növeli a felnőttkori magas vérnyomás, cukorbetegség lehetőségét, illetve károsan befolyásolja az ízületek, csontok állapotát, számos mozgásszervi betegséget okozva később.

A technológiai függőség fizikai tünetei között szerepelhet még:

- Súlygyarapodás vagy fogyás
- Carpalis alagút szindróma
- Fejfájás
- Nyaki- vagy hátfájdalom
- Száraz, kivörösödött szemek

„Gerald Hüther német agykutató és neuropszichológus a GEOkompakt egyik interjújában azt mondta, hogy Dél-kelet Ázsiában történtek olyan esetek, amikor számítógépes játékok mellett haltak éhen és száradtak ki gyerekek. A srácok nem érezték a saját testüket, teljesen a játékkal azonosultak, nem ittak és nem ettek, ez lett a vesztük.

A lányoknál más a helyzet. Ők inkább virtuálisan ismerkednek, chatelnek. Ez egy pótcselekvés náluk, ugyanis, ha nem sikerül ismerkedniük a való világban, a virtuális térbe menekülnek, ha itt sem érnek el sikereket, idővel előfordulhat náluk a depresszió. Létező jelenség a Facebook depresszió. Ezek természetesen a legsúlyosabb következmények.

A mértéktelen számítógépezés, azaz a monitor bámulása, a retina beszűküléséhez vezethet, és ez bárkit veszélyeztethet, korra való tekintet nélkül, sőt, előrevetíti a keringési zavarokat - közölték a Sydney-i Egyetem Látáskutatási Központjának munkatársai."[49]

2. A PSZICHOLÓGIAI JÓLÉT VÉDELME A DIGITÁLIS KÖRNYEZETBEN

Technológiafüggőség (internet, okostelefon), mint a felhasználás korlátozására való képtelenség

A technológiafüggőség, az internetfüggőség, az internethasználati rendellenesség és az internetfüggőségi rendellenesség egyaránt a különféle technológiák, különösen az internet, okostelefonok és közösségi oldalak használata körüli sokféle rögeszmés, kényszeres viselkedés leírására alkalmazott kifejezések.

Tanulmányok kimutatták, hogy a technológia használata ugyanolyan kémiai reakciót válthat ki az agyban, mint a drogok, az alkohol, a dohányzás és a szex. A vélemények megoszlanak abban, hogy ez egy új pszichológiai rendellenesség, vagy egy másik, már létező rendellenesség napfényre kerülése. Következésképpen nincs egyetértés abban, hogyan lehet ezt megmérni és megelőzni. Ennek ellenére növekvő érdeklődés mutatkozik a technológia túlzott használatának leküzdése irányában.

Forrás: https://addictus.blog.hu/2016/11/30/van_egy_rossz_hirem_valoszinuleg_fuggo_vagy

49 https://www.webbeteg.hu/cikkek/neurologia/15719/professzor_katona_ferenc_digitalis_bennszulottek

2.1 A technológiai függőségek érzelmi, pszichológiai, társadalmi, környezeti és biológiai tényezői

A technológiafüggők gyakran szenvednek legalább egy másik függőségben is. A technológiafüggőség biológiai, genetikai és környezeti tényezők kombinációjából származhat:

- **Mentális egészség**: az olyan rendellenesség, mint a szorongás, a depresszió, a figyelemhiányos hiperaktivitási rendellenesség (ADHD), a rögeszmés-kényszeres rendellenesség (OCD) vagy a bipoláris zavar növelheti a technológiai függőség kialakulásának esélyét.
- **Személyiség**: az alacsony önértékelés, a magány, a nyugtalanság és az elvonultság előre jelezhetik az internet túlzott használatát, annak érdekében, hogy az illető mások segítségével növelje az önbizalmát.
- **Környezet**: a stresszről és a pozitív környezeti hatások hiányáról (pl. munka, családi kapcsolatok és felelősségvállalás) az a vélekedés van érvényben, hogy növelik az internetes függőség kialakulásának kockázatát.

A függőségre utaló viselkedés tüneteinek meghatározása

A függőség fogalma nem csak az anyagoktól, például alkoholtól vagy kábítószerektől való függőséget jelenti, amelyet anyagfüggőségnek neveznek. Ha valaki nem tudja kontrollálni, hogyan használ egy anyagot, vagy hogyan vesz részt egy tevékenységben, és a mindennapi életében ettől függővé válik, egyaránt függőséget él meg.

A technológiafüggőség figyelmeztető jelei között szerepel:

- eufória érzése, miközben elektronikus eszközöket használ;
- a család és a barátok elhanyagolása;
- az alvás kihagyása;
- hazudozás a használatról;
- aggodalom, szégyen, bűntudat vagy depresszió érzése a technológia használata miatt;
- visszavonulás más tevékenységektől, amelyek valaha kellemesek voltak.

Mobiltelefon-függőség, és annak egészségügyi kockázatai *VIDEÓ*, melynek megnézését és a diákokkal történő megvitatását is javasoljuk!

2.2 Az internet káros hatásai

Ha nem figyelünk oda kisebb gyermekeknél, hogy milyen weboldalakon böngészik, könnyen erőszakos képek áldozatává válhat. Sok fiatal nem tudja felmérni a veszélyét, és könnyen bajba kerülhetnek. Az interneten keresztül sok embert átvernek vagy becsapnak.

A számítógépnek soha nem szabad helyettesítenie a képeskönyveket, a meséket és a szülőket
Forrás: https://www.gyerek-portal.hu/szamitogep-es-hatasai-a-gyerekekre.html

Az internetes zaklatás jelensége, tünetei, tények és kapcsolódó fogalmak

A Global Advisory Study Ipsos Public Affairs az internetes zaklatást úgy definiálja, mint:

„Amikor egy gyermek vagy (18 év alatti) gyermekek csoportja szándékosan megfélemlít, sért, fenyeget vagy zavarba hoz egy másik gyermeket, vagy gyermekek csoportját, különösen az információs technológia, például egy weboldal vagy internetes csevegőterem használata, mobiltelefon vagy más mobil eszköz révén".

Az internetes zaklatás egy más típusú zaklatás, amelyre a szülőknek és az iskoláknak különös figyelmet kell fordítaniuk a jelenleg is létező általános erőszakellenes törekvések mellett.

Kapcsolódó fogalmak

- **Kirekesztés**: valaki szándékos kizárása egy online csoportból, például egy "BFF" státuszból (Mindörökké legjobb barát) vagy egy játéklistáról.
- **Fenyegetés**: sértő, durva és bántó üzenetek ismételt küldése.
- **Kiposztolás és csalás**: valaki titkainak vagy zavarba ejtő információinak megosztása online. Valakinek a becsapása annak érdekében, hogy kiszedjék belőle a titkait vagy valamilyen zavarba ejtő információt, amit azután megosztanak az interneten.
- **Internetes követés**: ismételt üzenetküldés, amely sértő fenyegetéseket tartalmaz, vagy erősen megfélemlítő; olyan online tevékenységek folytatása, amelyek miatt az adott személy aggódik a biztonsága miatt.
- **Megszemélyesítés**: „átverés", valaki fiókjának a feltörése, és üzenetek küldése az illető nevében, annak érdekében, hogy rossz színben tüntessék fel, bajba sodorják, veszélybe hozzák, megsértsék a jó hírnevét vagy tönkretegyék a baráti kapcsolatait, vagy esetleg olyan üzenetek, amelyek később kísértő jelleggel visszatérnek.
- **Cikizés**: kegyetlen pletykák vagy szóbeszédek küldése vagy kiposztolása egy személyről, hogy tönkretegyék a jó hírét, vagy a baráti kapcsolatait.
- **Trollkodás**: szándékosan provokatív üzenetek küldése érzékeny témákról, konfliktusok kialakítása, az emberek felzaklatása és kiborulásra, összetűzésre való buzdítás.
- **Hamis profil**: online személyazonosság és személyes adatok ellopása hamis személyiségek létrehozásához és online kapcsolatok kialakításához.
- **Kiberpredátorok**: a szexuális és más ragadozók vadászhatnak az interneten, kihasználva a gyermekek ártatlanságát, visszaélve a bizalmukkal, és végül nagyon veszélyes személyes találkozókra csábítva őket.

Internetes zaklatás

Ez a videó bemutatja az internetes zaklatás általános formáit és a jeleket, amikre a fiataloknak figyelniük kell.

Az internetes zaklatás megelőzése hatékony megközelítésének fő elemei:

- Az internetes zaklatás megismerése és megbeszélése.
- Az internetes zaklatás megelőzésének beiktatása a vonatkozó szabályokba és gyakorlatokba.
- A jelentési utak elérhetőségének és láthatóságának biztosítása.
- Soha ne válaszoljunk a zavaró üzenetekre vagy képekre. Ehelyett tartsuk meg a bizonyítékokat, és jelentsük az eseményt.
- Ismerkedjen meg a használt szolgáltatások fiókkezelő eszközeivel, különös tekintettel az adatvédelemre és a blokkoló szolgáltatásokra.
- A technológia pozitív felhasználásának előmozdítása.
- Az online biztonság és a digitális írástudás előmozdítása.
- A megelőző tevékenységek hatásának értékelése.

A gyermekek védelmével kapcsolatos stratégiákban mind az EU-ban, mind pedig a tagállamokban, egyre konkrétabban jelenik meg a gyermekek digitális veszélyeztetésével kapcsolatos szabályozás, és nyomon követhető az a szemléletváltozás is, mely felvilágosítással és párbeszéddel is támogatja a fiatalok ezirányú védelmét, és hozzájárul tudásuk gazdagításához is.

3. DIGITÁLIS TECHNOLÓGIÁK A TÁRSADALMI JÓLÉT ÉS A BEILLESZKEDÉS TÁMOGATÁSÁRA

A közösségi médiahasználat előnyeinek felvázolásával szeretnénk felhívni a figyelmet a digitális eszközök társadalmi beilleszkedést, a fizikai és mentális jólét fenntartását segítő megfelelő alkalmazására, valamint a mindenki számára elérhető, kockázatok nélküli online kreativitás ösztönzésére.

A fiatalok még mindig hisznek az olyan alapvető erkölcsi-emberi értékekben, mint az igazság, becsületesség, és a jó szándék, és nem feltételezik, hogy valaki direkt megtéveszti őket. Ezért váltak a számítógépes bűnözők és támadások tökéletes célpontjaivá, mialatt éjjel-nappal a közösségi médián lógnak.

A Web 2.0 új korszakot hozott az internet történetében azáltal, hogy mély változásokat váltott ki a mindennapi kommunikációban, a társadalmi élet minden szegmensében.

MI A KÖZÖSSÉGI MÉDIA?

A web 2.0 lényege az, hogy az internetet közös létrehozási, együttműködési és kommunikációs platformmá változtatja. Általában az online tartalom szerzői eldönthetik, hogy nyilvánosan megosztják-e ezeket másokkal, vagy bizalmasan kezelik. A közösségi média szolgáltatásának fő területei:

- kommunikáció, beszélgetés (mint a skype, fórumok);
- közösségi hálózatépítés (mint a facebook, a whatsapp, a linkedin);
- digitális tartalmak készítése, módosítása, megosztása (mint a youtube, a flickr);
- közösségi játékok.

A társadalmi beilleszkedést segítő online közösségek

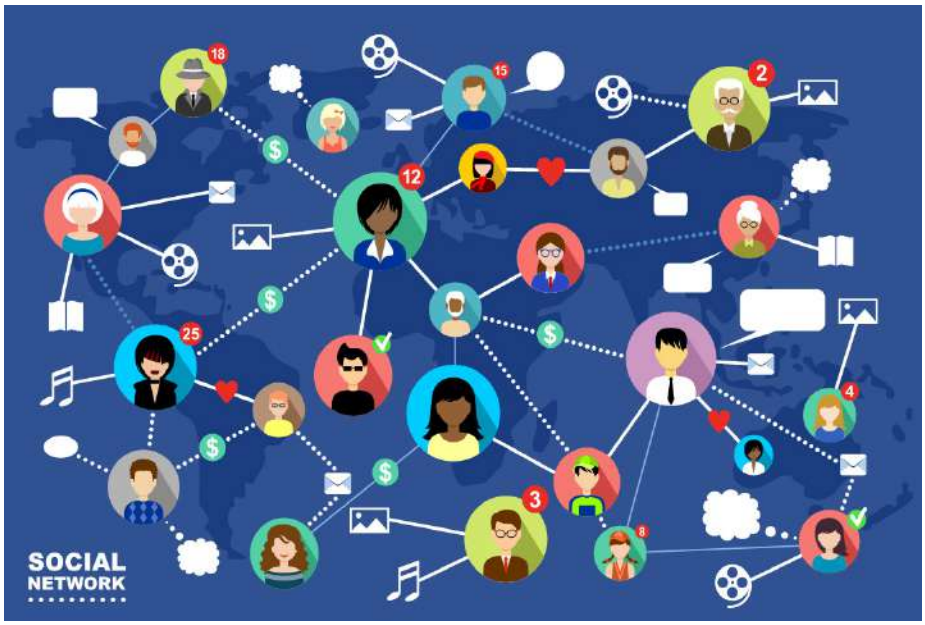
Két tényező motiválja az online közösségek tagjait az összekapcsolódásra és az összetartásra:

- A közösséghez való tartozás igénye.
- Annak lehetősége, hogy részesüljenek a közösséghez tartozásból származó előnyökből.

Az online közösségek nem csupán összegyűjtik és összetartják az egyébként relatíve idegen embereket, hanem ezek a csoportok átfedhetik egymást, és akár egymásba is épülhetnek.

3.1 Közösségi hálózatépítés

A közösségi hálózatok online eszközök az emberekkel való kapcsolatteremtéshez az interneten keresztül. A netes közösségek általában nyitottabbak, mint a valódi közösségek.



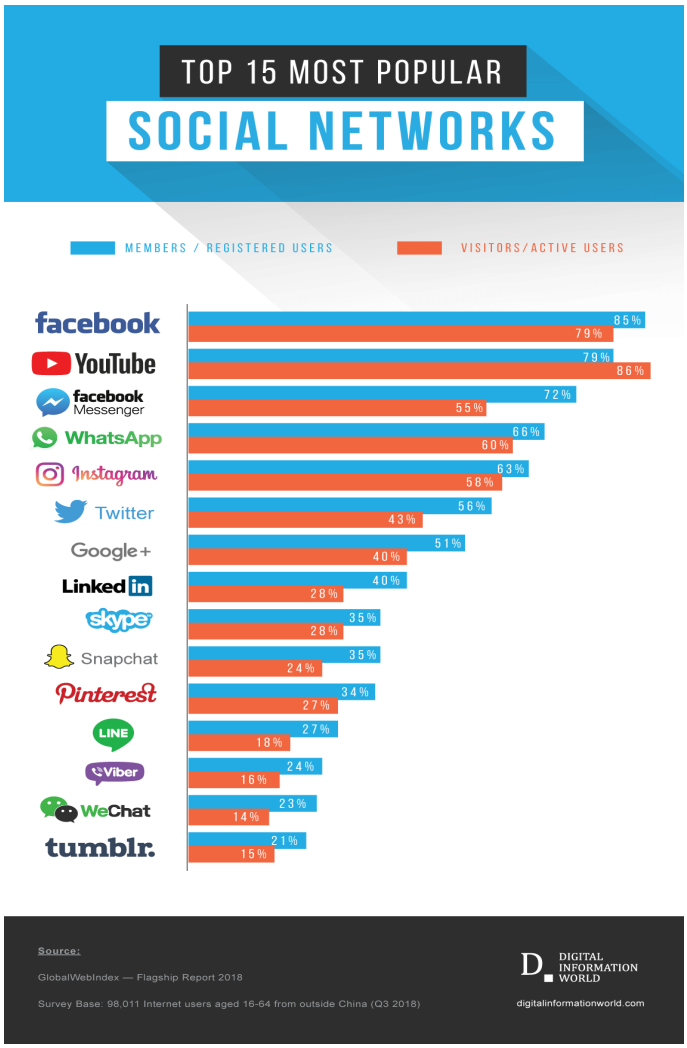
Forrás: Depositphotos

Ezek mind olyan online platformok, ahol a közös érdekű, vagy azonos céllal rendelkező emberek kölcsönhatásba lépnek.

Közösségi média trendek - 2020.

A mai napig a legsikeresebb és legnépszerűbb közösségi hálózati szolgáltatás a **Facebook**, több mint 500 millió regisztrált felhasználóval. A fiatalok között egyre nagyobb népszerűségnek örvend a TIKTOK, amely egy olyan applikáció, ami a kifejezetten rövid felvételek készítését és megosztását teszi lehetővé, ahol a felhasználó ingyenesen hozzáadhatja a kedvenc zenéjét, ezen kívül különböző emoji matricákat, speciális effektszűrőket, arcfiltereket, stb. is használhat a videóban. A TIKTOK kifejezetten a fiatalok körében tett szert rövid idő alatt óriási népszerűségre.

Ugyanakkor jelentős a YouTube rajongók és használók köre is, amint látszik az alábbi, 2020 első negyedévében készült felmérésből, mi szerint a YouTube már megszerezte magának a második helyet a közösség médiákban.



Forrás: https://hu.pinterest.com/pin/824651381752868161/

3.2 Tanulók a közösségi médiában

A közösségi média először a tanulókhoz jutott el, akik gyorsan megtanulták, hogyan lehet hálózatokat kiépíteni a tanárok által irányított osztálytermektől távol.

Ez az új generáció

- rabja az új technológiának, intuitív módon használja az informatikai eszközöket és navigál az interneten, mivel minden nap sok órát tölt ott;
- nem érdeklődik túlságosan a technológiai eszközök működése iránt, leginkább nem is érdekli egyáltalán;
- nem hajlandó nagy mennyiségű szöveget elolvasni;
- vizuálisan műveltebb, mint a korábbi generációk;
- általában egynél több médiumot használ: tévét néz, mobiltelefonon beszélget, zenét vagy rádiót hallgat egyszerre - jártas a «multitasking»-ban;
- gyors az információfogyasztásban: hozzászokott ahhoz, hogy nagyon gyorsan megkapja az információt, és azonnali válaszokat vár el;
- intenzíven használja a technológiát szocializálódásra: szívesen csatlakoznak a fizikai, a virtuális és a hibrid közösségekhez is.

Az új technológiák és hálózati eszközök vonzóak a diákok számára, és motiválhatják a tanulási folyamatban való részvételüket. Ezek az online eszközök és tananyagok nem helyettesítik a hagyományos tanítási módszereket, de kiegészíthetik a tanítási tevékenységeket.

A kreatív munka fontosságát az Állampolgárok Digitális Kompetencia-keretrendszere is hangsúlyozza, amely meghatározza a kompetenciakészletet az „Alkotás" területén, összeállítva az alapvető IKT-készségeket a digitális tartalmak készítéséhez és azok másokkal történő megosztásához online.

3.3 Az eszközökhöz való illetéktelen hozzáférés elleni védelem

Még ha a tanulók rendelkeznek is a technológiával és a készségekkel az eszközök használatához, és sürgetőnek érzik, hogy csatlakozzanak az online közösségekhez, előfordulhat, hogy nem ismerik a közösségi média sötét oldalát. A tanárok és a szülők felelőssége, hogy elejét vegyék a közösségi platformokon őket érő visszaéléseknek, amik állítólag arra valók, hogy a segítségükre legyenek.

Ha nem elég óvatosak, akkor a fiatalok nem tudják elkerülni az internetes zaklatást, például az érzelmeikkel való visszaéléseket, amikor támadások érik őket. A számítógépes zaklatással való szembenézés egyébként nagyon nehéz lehet a fegyvertelen tinédzserek számára, így a tanárok és a szülők feladata felhívni a figyelmüket a lehetséges kockázatokra.

TÉNYEK, AMIKET TUDATOSÍTANI KELL

Védd meg a személyes adataidat!

- A közösségi média alkalmazásai alapértelmezés szerint nagyjából úgy vannak konfigurálva, hogy minél több információt szerezzenek rólunk, és hogy a lehető legtöbb ember férjen hozzá ezekhez.
- Abban a pillanatban, amikor közzétettük az információkat, elveszítjük az irányítást ezen adatok áramlása felett.

Konfigurálj megfelelően!

- Ha nem állítjuk be megfelelően ezen alkalmazások adatvédelmi beállításait, amikor magunkról adatot írunk be és teszünk közzé, akkor mindegyik rossz kezekbe kerülhet.

Légy kritikus!

- A híreket és egyéb információkat, amelyeket az emberek megosztanak a közösségi médiában, ritkán ellenőrzik.
- A hamis híreket és a megtévesztéseket a közösségi média terjeszti, ami a természetes élőhelyük.

KOCKÁZATOK, AMIKRE ODA KELL FIGYELNI

- A megosztott személyes információkat felhasználhatják ellenünk vagy egy családtagunk ellen.
- A széles körben közzétett nyaralási tervek tájékoztathatják a betörőket arról, hogy otthon vagyunk-e vagy sem.
- Mindaddig, amíg a név, a telefonszám, az email és az igazolvány felhasználható a megszemélyesítésünkre, használhatják ezeket hamis ajánlatokat küldésére is, amelyek megtévesztés céljából készülnek.
- A nem védett banki adatok lehúzott számlákkal járhatnak.
- A téves információ hibás döntések meghozatalához, vagy a lakosság összezavarásához vezethet.

ALKALMAZHATÓ STRATÉGIÁK

Ha információt osztunk meg a közösségi médiában:

- Ellenőrizzük a preferált közösségi média webhelyén az adatvédelmi beállításokat, majd állítsuk be őket megfelelően. Lehet, hogy nem kell idegeneknek is lépést tartaniuk az életünk részleteivel.
- Gondoljuk meg kétszer is, mielőtt személyes adatokat teszünk közzé. Legyünk óvatosak!

Ha információt fogadunk a közösségi médiából:

- Használjuk az intuícióinkat, és gondolkodjunk kritikusan.
- Ellenőrizzük az információforrást.

3.4 Az oktatási módszerek újragondolása

Minden tanuló tagja egy vagy több közösségi hálózatnak. Folyamatos online jelenlét jellemzi őket. Virtuális közösségekben élnek, és szabadidejük nagy részét a világhálón töltik. Akár kapcsolatokat is fel lehet építeni a közösségi weboldalakon, és sokan nem tudják elképzelni a világot mobilinternet vagy közösségi média nélkül.

Hogyan lehet ezeket mindenekelőtt a saját javunkra, azaz mentális jólétünkre és önfejlesztésre fordítani?

A 21. századi készségeket nem feltétlenül lehet a legjobban fejleszteni a frontális, tanárközpontú tanítási módszerekkel, ezért a tanároknak a tanulóközpontú, aktív tanulási módszerek felé kell elmozdulniuk, és együttműködés-alapú tevékenységeket szervezniük, úgy, hogy a kreatív online tevékenységeket az osztálytermekbe integrálják[50].

A könyv második fejezetében bemutatunk olyan megoldásokat, melyeket a tanártovábbképzésben résztvevő pedagógusok terveztek és valósítottak meg. A kipróbált terveket bemutatjuk, megosztjuk, hogy minden pedagógus számára könnyebbé tegyük e fontos téma tanítását diákjaik számára.

4. DIGITÁLIS TECHNOLÓGIÁK KÖRNYEZETI HATÁSAI

A számítógépek és valamennyi digitális eszköz fokozott használata megváltoztatja az életünket. Ezt az óriási hatást nevezzük digitális átalakulásnak, melynek előnyei között szerepel a kommunikáció, az üzleti hatékonyság, a szórakozás, stb., ugyanakkor potenciálisan negatív hatással bír a környezetre nézve. Mint minden más eszköz esetében, az etikus és felelősségteljes felhasználást és az ártalmak csökkentését szem előtt kell tartani, és ez az emberek viselkedésén múlik. Oktatásra és szabályozásra van tehát szükség annak biztosításához, hogy ezeket az eszközöket valóban okosan használják fel.

A rövid életciklus, a folyamatos frissítések és kedvenc technológiánk új verziói azt jelentik, hogy sok hulladék keletkezik. Az elektronikai hulladékok, valamint a gyártási folyamatok során keletkező hulladékok ártalmatlanításához nagyon speciális módszert kell alkalmazni. Ez a hulladék („elektronikai szemét") mindenféle veszélyes anyagot tartalmaz, amely a környezet számára nagyon káros.

A digitális átalakulás ugyanakkor pozitív hatást is gyakorolhat a környezetre. A technológia támogatja a környezettel való foglalkozást, és a felelősségteljes fellépések előmozdítását célzó szabályok kidolgozását.

4.1 A fenntartható ember-számítógép kapcsolat

A technológia fokozott használata növekvő környezeti veszélyekkel jár, kezdve az üvegházhatást okozó gázok kibocsátásával járó gyártástól az e-hulladék gondatlan ártalmatlanításáig, vagy az „elektronikai szemét"-ig.

A fenntartható fejlődés a 20. század utolsó két évtizedében érdeklődésre, vitákra és új ötletek felvetésére okot adó kérdéssé vált. Mára kiderült, hogy az informatikai rendszerek tervezőinek környezettudatosabbnak kell lenniük, például az elhasznált termék forrásainak újbóli felhasználásával, és tudatában kell lenniük azzal a problémával, amit a rövid élettartamú termékek nagy volumene és a túlzott mértékű papírfelhasználás eredményez.

50 Javasoljuk a következő módszert és könyvet a megoldás kereséséhez: https://mek.oszk.hu/19700/19775/19775.pdf;

Felelősséggel tartozunk az IKT fenntartható használatának és fogyasztásának biztosításáért a technológia oktatási, munka és szabadidős felhasználása során. Ez azt jelenti, hogy meg kell találnunk a digitális tevékenységeink környezetre és társadalomra gyakorolt káros hatásainak csökkentésére szolgáló módszereket. Számos tanulmány készült a technológia környezetre gyakorolt káros hatásairól és a szakértők különféle módszereket javasoltak ezek csökkentésére.

Ez a megközelítés szerepel a zöld IT koncepcióban, amely az IKT fogyasztásnak a társadalomra gyakorolt és a technológiai fejlődésnek kitett környezet pozitív és negatív hatásainak kiegyensúlyozására irányul, annak érdekében, hogy a társadalomra és a környezetre gyakorolt hatás minimális legyen.

4.2 IKT eszközök gyártása, beszerzése és kidobása

A **kiskereskedelmi feldolgozóipar a legszennyezőbb iparág a földön**, az olajipar csak a második. Tekintettel arra, hogy az IKT berendezések gyártása mennyire fontos a modern társadalomban, minden erőfeszítést meg kell tennünk azért, hogy körültekintően kezeljük a vásárolt termékeket és ügyeljünk arra, hogy a gyártók, akiktől vásárolunk, tudatában legyenek üzleti tevékenységük környezetre gyakorolt hatásainak és lépéseket tegyenek, hogy minimalizálják azokat.

„Az elektronikai kütyük (okostelefonok, tabletek, számítógépek) első ránézésre tiszta termékeknek számítanak: nem füstölnek, mint a dízel járművek vagy a szén alapú hőerőművek (ha eltekintünk néhány problémás, kigyulladó mobiltelefontól). Ha viszont kicsit jobban utánajárunk, akkor kiderül, hogy előállításukhoz leukémiás megbetegedések, tüdőrák, agydaganat, vetélések és más problémák köthetőek."[51]

Az elektronikai és informatikai eszközeink (okostelefonok, tabletek, notebookok) élete nem akkor kezdődik, amikor megvásároljuk vagy ajándékba kapjuk, s nem ér véget akkor, amikor megunjuk vagy újra cseréljük őket. Egy-egy ilyen termék teljes életútja a legyártáshoz és a csomagoláshoz felhasznált nyersanyagok kitermelésével kezdődik. Figyelembe kell venni továbbá a készülékek gyártása során felhasznált energiát, illetve a gyártási folyamat során bekövetkező környezetkárosítást, valamint a társadalmi hatások között az üzemekben alkalmazott munkakörülményeket is.

Az IKT ágazatban tevékenykedő cégek számára azért tud ennyire jövedelmező lenni ez az üzletág, mert ezeknek a termékeknek a valódi ára nem szerepel az árcédulán: a környezeti- és társadalmi költségeket ráterhelik a társadalomra.

***Indítsák el Annie Leonard klasszikus filmjét*, Az elektronikai termékek történetéről:**

4.3 Az IKT eszközök újrahasznosítási lehetőségei (elemek, printerek, patronok, papír)

Az elhasználódott elektronikus eszközök, más néven az e-hulladék vagy elektronikai hulladék közé tartoznak a régi számítógépek, nyomtatók, szkennerek, mobiltelefonok, valamint tévék és zenei rendszerek, és sajnos a legtöbben még mindig a hulladéklerakókba helyezik, gyakran a szegényebb országokba szállítva, ahol hátrányos helyzetű emberek szerelik szét őket.

51 https://greenfo.hu/hir/az-elektronikai-kutyuk-arnyai/

Az elektronikai hulladékok ártalmatlanítása mellett az újrahasznosítás is számos előnnyel járó megoldás. Új készülékek gyártásához biztosít nyersanyagokat és nagyon sok nemesfém nyerhető vissza az újrahasznosított számítógépekből. A gondos újrahasznosítás megakadályozza a mérgező vegyi anyagok környezetbe jutását.

Mint az elektronikus hulladékká váló eszközök fogyasztói, a vevők felelősséggel tartoznak az újra hasznosításban. Szem előtt kell tartani azt is, hogy a nyomtató toner kazettáit megfelelő módon ártalmatlanítani kell, mivel veszélyes anyagokat tartalmaznak.

Az elektronikai hulladék biztonságos és professzionális ártalmatlanításáért a **gyártók felelnek**, és bármennyire is szeretnénk azt hinni, hogy ezt maguktól és önként is megteszik, nem mindig van így. **Ezért létezik alapvető jogi szabályozás, és adták ki 1988-ban az Európai Bizottsági Irányelveket,** amelyben előírták az elektromos és elektronikus berendezések újrahasznosítását és környezetbarát ártalmatlanítását, meghatározva ebben a gyártók kötelezettségeit.

4.4 Az elektromos és elektronikus hulladékokra vonatkozó direktívák, nemzeti jogszabály

Az elektromos és elektronikus berendezések (WEEE), például az elhasználódott számítógépek, tévék, hűtőszekrények és mobiltelefonok az egyik leggyorsabban növekvő hulladéközönt jelentik az EU-ban, évente csaknem 2 millió tonna hulladékot kitéve.

Az elektromos és elektronikus berendezések hulladékában sok veszélyes anyag és összetevő keveredik, amik jelentős környezeti és egészségügyi problémákat okozhatnak, ha nem kezelik megfelelően.

Ezeknek a problémáknak a megoldása érdekében két jogszabályt fogadtak el: az elektromos és elektronikus berendezések hulladékairól szóló irányelvet (WEEE irányelv) és az egyes veszélyes anyagok elektromos és elektronikus berendezésekben való felhasználásának korlátozásáról szóló irányelvet (RoHS irányelv). Ezeket az irányelveket át kellett ültetni az egyes EU-tagállamok nemzeti jogszabályaiba.

A nemzeti szabályrendszerhez való csatlakozás szerint az egyes államoknak finanszírozniuk kell az elektromos és elektronikus berendezések hulladékainak környezetbarát kezelését is. **Magyarországon a 2011/65/EU irányelve alapján lépett hatályba a kormányrendelet (374/2012 (XII.18.).**

5. AZ EURÓPAI ÉS HAZAI KIBERSTRATÉGIÁRÓL ÉS JOGI SZABÁLYOZÁSRÓL

Az előző fejezetekben megismerkedtünk az internet árnyoldalaival, a széles körű használatból fakadó problémákkal, veszélyekkel.

Ebben a fejezetben röviden szeretnénk bemutatni, hogy az Európai Unió milyen módon próbálta és próbálja szabályozni ezt a rohamosan fejlődő, változó területet, és ezáltal megteremteni állampolgárai számára a biztonságos kiberteret.

Az EU kibervédelmi stratégiája mellett fontosnak tartjuk azt is, hogy Magyarország hol tart a jelenlegi - az EU-val harmonizáló - nemzeti szabályozásban. Az e területre vonatkozó - a tanárok, diákok és szülők szempontjából legfontosabb - tudnivalókat foglaltuk össze.

5.1 Az európai szabályozás kialakulása és jelenlegi helyzete

2017-es adatok szerint „az uniós polgárok átlag 63%-a napi szinten használja az internetet és mindössze 24% annak a kisebbségnek aránya, amely egyáltalán nem használja (ki) a világháló adta lehetőségeket. Egész Európa internethasználata még ennél is magasabb, 73%-os. Ez a világátlag (50%) felett van, de ne felejtsük el, hogy igen elmaradott térségek adatai is részét képezik a felméréseknek.

A „mindössze" kifejezés tehát természetesen igen relatív, mert az uniós polgárok 24%-a is összesen 121 millió lakost jelent, tehát korántsem beszélhetünk egy kis létszámú csoportról.[52]

Eleinte az egyes nemzetállamok önállóan próbálták kialakítani kiberbiztonsági rendszereiket, de idővel bizonyossá vált, hogy a hatékony védelmet és szabályozást csak Európai Uniós szinten lehet megteremteni. Az elmúlt évtizedben az EU szakemberei rengeteget dolgoztak azért, hogy ez az egységes stratégia megvalósuljon. 2016-ra mondhatta el magáról az Európai Unió, hogy egységes kibervédelmi alapelveket tud adni tagállamai kezébe, melyek valós segítséget képesek nyújtani a fenyegetések kezelésére. Ezt azonban hosszú folyamat előzte meg:

- 2001-ben jelent meg az első Európai Uniós dokumentum **„Javaslat egy európai hálózat- és informatikai biztonsági politikára"** címmel. E javaslat áttekintette a lehetséges biztonsági fenyegetéseket, károkozásukat és a szóba jöhető megoldásokat. Emellett megállapította azt is, hogy az akkori szabályozások nem megfelelőek a problémák kiküszöbölésére és megelőzésére.

52 Molnár Dóra: Egységes Európai kibertér? Az Európai Unió kiberbiztonsági politikájának fejlődése Hadmérnök, XII. Évfolyam 1. szám – 2017. március

- 2003-ban fogadták el az EU első biztonsági stratégiáját[53] **„Egy biztonságos Európa egy jobb világban. Az Európai Biztonsági Stratégia”** címmel. A stratégia az EU biztonsági érdekeinek előmozdítására vonatkozó alapelveket és egyértelmű célokat határozott meg, s részletesen tárgyalja a globális és így Európát is fenyegető kihívásokat. **A stratégia felülvizsgálataként kiadott 2008-as jelentés már a fő kihívások között említette a kiberbiztonságot**.
- Az **i2010 európai információs társadalom stratégia** 2005-ben jelent meg. E dokumentum „az egységes európai információs tér negyedik fő kihívásaként tartalmazta a biztonságot, mint az internet biztonságának növelését a csalókkal, a káros tartalommal és a technológiai meghibásodásokkal szemben a befektetők és a fogyasztók bizalmának erősítése érdekében. A megbízható, kiszámítható és biztonságos informatika a digitális szolgáltatások kritikus feltételeként szerepelt.”[54]
- A 2009-ben kiadott „**Európa védelme a nagyszabású számítógépes támadások és hálózati zavarok ellen: felkészültség, a védelem és az ellenállóképesség fokozása”** című dokumentum volt az első, mely már kifejezetten az információs rendszerek védelmével foglalkozott. Ebben már határozottan hangsúlyozták a nemzetközi szervezetekkel való együttműködés fontosságát, valamint a nemzeti kibervédelmi csoportok, szervezetek létrehozásának fontosságát, melyek kiemelkedő jelentőségű feladatai között jelölték meg a korai előrejelzést és az incidenskezelést.
- Az EU 2000 óta folyamatosan indít programokat a „digitális vívmányok biztonságos használatának elősegítésére”. Ezek célja az olcsóbb, biztonságosabb internet biztosítása mindenkinek, az egységes európai információs tér megteremtése, és a szektor támogatása volt. A jelenleg futó tíz éves program, **„az európai digitális menetrend"** az „Európa 2020” stratégia hét kiemelt kezdeményezésének egyike, melyet azért alkottak meg, hogy az információs és kommunikációs technológiák (IKT-k) alkalmazásának kulcsfontosságú szerepet jelöljön ki Európa 2020-ra kitűzött céljainak sikeres megvalósításában. A menetrend feladata felvázolni azt az utat, amelyen járva az IKT-k társadalmi és gazdasági potenciálja a legteljesebb mértékben kihasználható; vonatkozik ez mindenekelőtt az internetre, amely az üzlet, a munka, a játék, a szabad kommunikáció és véleménynyilvánítás terén a gazdasági és társadalmi élet pótolhatatlan eszközévé vált. [55]
- 2013-ban adták ki **az Európai Unió átfogó biztonsági stratégiáját:** A „**Nyílt, biztonságos és megbízható kibertér**” nevű stratégia foglalja össze, hogy az EU hogyan tervezi hatékonyan megelőzni és elhárítani az internetes támadásokat és hálózati zavarokat.
- 2015-ben adták ki az **Európai Egységes Digitális Piaci Stratégiát**, melyben már célként jelent meg az európai egységes digitális piac megteremtése is.
- 2016-ban fogadták el a következő két, kiemelt jelentőségű jogi normát:
    - Az **adatvédelmi (GDPR) rendeletet**[56] (General Data Protection Regulation), mely kiemelten kezeli az egyének azon jogát, hogy ellenőrizhessék személyes adataik gyűjtését, feldolgozását, tárolását, s ennek megfelelően a kezelő szervezetek számára is új feladatok ellátását rendelte el egységesen az Unión belül.

53 Az Európai Unióban a stratégia jelenti a szabályozás legmagasabb szintjét.
54 Munk Sándor: Kiberbiztonsági célok, jövőképek, szabályozók az EU-ban és kapcsolatrendszerük az interoperabilitással. Hadmérnök, XIII. Évfolyam „KÖFOP” szám- 2018. január
55 Az európai digitális menetrend http://infoter.eu/attachment/0003/2807_com2010_0245hu01.pdf
56 Az Európai Parlament és a Tanács (EU) 2016/697 rendelete

Az EU általános adatvédelmi rendelete (GDPR)
Forrás: https://newsroom.consilium.europa.eu/events/general-data-protection-regulation/119072-altalanos-adatvedelmi-rendelet-20180514

- A **NIS irányelv** (Directive on Security of Network and Information Systems) a hálózati és információs rendszerek biztonságáról szóló irányelv, mely jelenleg az Európai Unió legmagasabb szintű kiberbiztonsági szabályozása, és fő célja megakadályozni az európai infrastruktúra elleni kibertámadásokat.

- **2018 októberében** az Európai Tanács olyan intézkedésekre szólította fel tagállamait, melyek fokozzák a kiberbiztonságot az EU-ban. A kiberfenyegetésekkel szembeni fellépésre vonatkozó megújított uniós kötelezettségvállalás alapja az Európai Bizottság 2017 szeptemberében előterjesztett kiberbiztonsági reformcsomagja. **E reform a kiberbiztonsági stratégia**, valamint annak fő pillére, a hálózati és információs rendszerek biztonságáról szóló irányelv (kiberbiztonsági irányelv) révén bevezetett intézkedésekre épül.
- 2020. február 19. Európai Adatstratégia: napjainkban egyre inkább adatvezéreltté válik a társadalom. Az európai adatstratégia azért született, hogy az EU e folyamatok élére tudjon állni. Egy egységes piacon szabadon áramolhatnak az adatok az Európai Unión belül és az ágazatok között, aminek a vállalkozások, a kutatók és a közigazgatási szervek egyaránt hasznát látják. Az egyének, a vállalkozások és a szervezetek annál jobb döntéseket tudnak hozni, minél több, számukra releváns, nyilvánosan hozzáférhető, nem személyes adatnak vannak a birtokában.

5.2 Kiberbiztonsági szervezetek az EU-ban

Az uniós szabályozásokban többször fogalmaztak meg olyan igényt, hogy a hatékony észlelés, megelőzés és védelem érdekében szükséges nemzetközi kiberbiztonsági szervezetek, hálózatok felállítása és üzemeltetése is.

Ilyen szervezet például a 2014-ben létrehozott **Európai Hálózat- és Információbiztonsági Ügynökség (European Network Information and Security Agency, ENISA**[57]), melynek célja, hogy segítse az Unió és a tagországok felkészülését az információbiztonsági kihívások felderítésére, kezelésére és megelőzésére.

5.3 Nemzeti szabályozás – magyarországi sajátosságok

Magyarország az ezredfordulótól kezdve kiemelten fontosnak tartotta az információs társadalom fejlesztését, 2000 és 2014 között négy stratégia is készült, melyek középpontjában e téma szerepelt:

- **2001: Nemzeti Információs Társadalom Stratégia**, mely fő célkitűzései a következők voltak:
  - a gazdaság információtechnológiára alapozott fejlesztése;
  - az oktatás és a kultúra, a társadalompolitika fejlesztése;
  - az elektronikus kormányzati és önkormányzati rendszerek fejlesztése;
  - a célokhoz szükséges infrastrukturális rendszerek kialakítása és fejlesztése.
- **2003: Magyar Információs Társadalom Stratégia**, amelynek legfőbb célja egy tudásalapú gazdaság megteremtése volt, mely az emberek életminőségének és életkörülményeinek növelését célozza.
- **2010: Digitális Megújulás Cselekvési Terv 2010-2014:** melyben már olvashatunk a kiberbiztonságról és az információbiztonsági jogszabályokról is.
- **2013**-ban jelent meg a **Nemzeti Kiberbiztonsági Stratégia** (1139/2013 (III.21) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. „A stratégia célja a szabad és biztonságos kibertér kialakítása és a nemzeti szuverenitás védelme a XXI. század meghatározóvá vált új közege, a kibertér létrejöttének következtében megváltozott nemzeti és nemzetközi környezetben.”
- E stratégia alapján készült el a **2013. évi L Törvény az Állami és Önkormányzati Szervek Elektronikus Információbiztonságáról** jogszabály, mely középpontjában – a Kormány és kormánybizottságok kivételével – a magyar állami szervek biztonságának megőrzése és biztonsága áll. [58]
- **2014: Nemzeti Infokommunikációs Stratégia 2014-2020:** melyben először szerepelt kiemelt helyen a biztonság és az infokommunikációs rendszerek zavartalan működésének biztosítása.

57 https://www.enisa.europa.eu/
58 Kovács László: Kiberbiztonság és -stratégia

- DIGITÁLIS JÓLÉTI PROGRAM – 2017. június: **A digitális fejlődés egyik legnagyobb kihívása az internetbiztonság megteremtése és fenntartása.** A szerzői jogok megsértése, az ipari kémkedés, és az államilag támogatott kibertámadások napi szinten érintik a nemzetállamok információs vagyonát és kritikus infrastruktúra-elemeit, a kiberkémkedés pedig soha nem látott kihívások elé állítja a nemzetbiztonsági szervezeteket. Éppen ezért a **Digitális Jólét Program 2.0 egyik kiemelt célja a biztonságos kibertér megteremtése is.** ***1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról***

5.4 Kiberbiztonsági szervezetek

Ahogyan Európában, úgy hazánkban is megalakultak azok a kibervédelmi szervezetek, melyek elsődleges célja a hatékony észlelés, megelőzés és védelem:

Ilyen a 2015-ben létrejött **Nemzeti Kibervédelmi Intézet (*https://nki.gov.hu/*)**, melynek feladata:

- a kibertérből érkező támadásokkal és fenyegetettségekkel való közvetlen foglalkozás, incidenskezelés (GovCERT = **Kormányzati Eseménykezelő Központ**);
- a jogszabályi előírások ellenőrzése és érvényesítése (a **Nemzeti Elektronikus Információbiztonsági Hatóság**, ***http://neih.gov.hu/***);
- a védelmi képességek fejlesztése és üzemeltetése[59].

59 A Nemzetbiztonsági szakszolgálat honlapja: http://nbsz.hu/?lang=hu&mid=42

ÖSSZEFOGLALÁS

Ebben fejezetben öt nagy témával foglalkoztunk az alábbiak szerint:

- A digitális technológia folyamatos és hosszantartó alkalmazása, használata, illetve annak hatása a fizikai egészségre (fizikai egészségkárosító hatás).
- A digitális technológia használatának pszichológiai hatása (az emberek, fiatalok jólétét veszélyeztető cselekedetek, jelenségek).
- A digitális technológiák társadalmi jólétre és a beilleszkedésre gyakorolt hatása.
- Digitális technológiák környezeti hatásai.
- Az európai és hazai kiberstratégiák és jogi szabályozás.

A fejezetben összefoglaltuk azokat az egészségügyi kockázatokat és veszélyeket, melyek a számítógéppel dolgozó felnőtteket éppúgy, mint a tartósan sok időt a digitális eszközökkel (kommunikáció, játék, tanulás és egyéb közösségi együttlét) töltő fiatalokat, egyre inkább a gyerekeket is érintik.

Foglalkoztunk a legjellemzőbb betegségtípusokkal és az ergonómiával is. A fejezetnek ebben a részében megismerhette, hogyan lehet elkerülni a számítógéppel végzett munka által okozott egészségügyi kockázatokat, hogyan maradhat mind fizikai, mind mentális értelemben fitt, hogyan tudja megvédeni magát a számítógépes bűnözőktől és az online zaklatással szemben, és hogyan taníthatja meg mindezt a diákjainak is.

Fontosnak tartottunk arról is szólni, hogy a közösségi média miként befolyásolja mindennapi életünket, milyen negatív és pozitív társadalmi és személyes hatása van. Nem maradhatott ki az a fontos tény sem, hogy a digitális technológiának, az eszközök gyártásának, használatának és „kidobásának” milyen környezeti hatásai vannak.

Végül pedig rövid összefoglalót készítettünk arról, hogy milyen módon és tartalommal fejlődött a jogalkotás a kibertér védelmével kapcsolatban az Európai Unióban és nemzeti szinten.

SZAKIRODALOM

1. Képernyős munkahelyek biztonsága. Spiegel Gyula, Budapest, 2018. Készült a GINOP-5.3.4-16-2016-00022 projekt keretében: ***https://nagykerbiztonsag.hu/wp-content/uploads/2018/03/kepernyos_munkahelyek.pdf***
2. Tizenévesek digitáliseszköz-használati szokásai - egy felmérés eredményei Teenager's use of digital technology - Results of a survey), Lánszi Anita, Budapest, 2018 ***https://www.researchgate.net/publication/324603622***
3. Minden második gyermek veszélynek van kitéve az Interneten ***https://news.microsoft.com/hu-hu/2017/07/10/minden-masodik-gyerek-veszelynek-van-kiteve-neten/***
4. Digitális bennszülöttek - a kisgyerek ismerje a számítógépet, de ne idő előtt! ***https://www.webbeteg.hu/cikkek/neurologia/15719/professzor_katona_ferenc_digitalisbennszulottek***
5. Módszertani megújulás a szakképzésben. Fordított osztályterem a gyakorlatban. Budapest, 2018 ***https://mek.oszk.hu/19700/19775/19775.pdf***
6. Erdősi Péter Máté, CISA- Solymos Ákos, CISM, CRISC: IT biztonság közérthetően, Neumann János Számítógép-tudományi Társaság 2018. ***http://njszt.hu/sites/default/files/document/2019/NJSZT_IT_Biztonsag_kozertheto-en_v3.pdf***
7. Munk Sándor: Kiberbiztonsági célok, jövőképek, szabályozók az EU-ban, és kapcsolatrendszerük az interoperabilitással. Hadmérnök, XIII. Évfolyam „KÖFOP" szám- 2018. január ***http://www.hadmernok.hu/180kofop_12_munk.pdf***
8. Kiberbiztonsági reform Európában ***https://www.consilium.europa.eu/hu/policies/cyber-security/A Bizottság (EU)***
9. 2017/1584 ajánlása (2017. szeptember 13.) a nagyszabású kiberbiztonsági eseményekre és válsághelyzetekre való összehangolt reagálásról ***https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:-32017H1584&from=EN***
10. Molnár Dóra: Egységes európai kibertér? Az Európai Unió kiberbiztonsági politikájának fejlődése, XII. Évfolyam 1. szám – 2017. március ***http://hadmernok.hu/171_20_molnar2.pdf***
11. Egy biztonságos Európa egy jobb világban. Az Európai Biztonsági Stratégia ***https://www.consilium.europa.eu/media/30811/qc7809568huc.pdf***
12. Erős kiberbiztonság kialakítása Európában, Az Unió helyzete 2018. Európai Bizottság ***https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-cybersecurity_hu.pdf***
13. Európai Digitális Menetrend (Europe's Digital Agenda 2010-2020) ***http://infoter.eu/alapdokumentumok/europai_digitalis_menetrend***

14. 2020. február 19. Európai adatstratégia
https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_hu

15. 2013. évi L Törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.286841

VIDEÓK

1. A mobiltelefon veszélyei
https://youtu.be/KWdaoVnnkCI
https://www.youtube.com/watch?v=ygIXMK4H7RQ

2. Annie Leonard filmje „az elektronikai termékek történetéről”
https://www.youtube.com/watch?v=dcBNRCldLvE

3. Az EU általános adatvédelmi rendelete (GDPR)
https://newsroom.consilium.europa.eu/events/general-data-protection-regulation/119072-altalanos-adatvedelmi-rendelet-20180514

4. MODUL: KARRIERLEHETŐSÉGEK AZ INTERNETBIZTONSÁGBAN

BEVEZETŐ

Az előző fejezetekben az általános sérülékenységekkel szemben saját magunk megvédésére szolgáló mechanizmusokat mutattunk be és megvitattuk a biztonsági rések kiaknázásában rejlő különféle módszereket.

Az internetbiztonság területe a számítástechnika, technológia, mérnöki munka és a matematika tudásterületeit egyesíti, de a társadalomtudományokat, a pszichológiát, a szociológiát és a jogot is magában foglalja, vagyis a karrierlehetőségek hatalmas tárházát és jól fizetett állások sokaságát kínálja. Manapság, mikor a terület a képzett szakemberek hiányával szembesül, azt feltételezik, hogy ennek egyik oka az ágazaton belüli karrierlehetőségek ismeretének és a megfelelő információnak a hiánya lehet. Ez a tendencia egyáltalán nem szerencsés, hiszen ennek folyományaként érdektelenség mutatkozik a továbbtanulás vagy a pályaválasztás terén ezen a területen, félrevezető információ áramlik a munkalehetőségekről, sztereotípiák alakulnak ki az ezen a területen tevékenykedő szakemberekről. Ez a fejezet összefoglalja az internetbiztonsági szakma szempontjából releváns készségekkel, kompetenciákkal és karrierprofilokkal kapcsolatos információkat, hogy megkísérelje kitölteni a szakterületen belüli karrierről alkotott általános ismeretek hiányosságait.

Elsőként azt vizsgáljuk meg, hogy az internetbiztonsági szakember hol helyezkedik el a mai társadalmi ökoszisztémában, különös tekintettel az internetbiztonság társadalmi értékére. Ezen felül bemutatjuk a gazdaság néhány olyan területét, amelyet az internetbiztonság közelről érint. Ugyanilyen fontos, hogy belemerüljünk a biztonsági feladatokba, készségekbe és kompetenciákba.

Itt külön figyelmet fordítunk az ESCO-ban (Európai Készségek, Kompetenciák, Képesítések és Foglalkozások) meghatározott készségekre és foglalkozásokra, valamint az e-CF (Európai E-kompetencia Keretrendszer) internetbiztonsághoz kapcsolódó munkaköri profiljaira. Végezetül példákkal és esettanulmányokkal igyekszünk felkelteni a kíváncsiságát, és ami ugyanolyan fontos, növelni a magabiztosságát, hogy beszéljen a tanulókkal az internetbiztonságban rejlő lehetőségekről.

Ebben a fejezetben elsősorban a polgári internetbiztonsági karrierprofilokra fókuszálunk, és nem tárgyaljuk a katonai internetbiztonsági szakmai pályafutásokat.

Forrás: www.pixabay.com

1. INTERNETBIZTONSÁG ÉS TÁRSADALOM

A technológia manapság elkerülhetetlen jelenléte a mindennapjainkban azt eredményezte, hogy az internetbiztonság kiemelkedő jelentőségűvé vált a társadalomban. Gondoljunk csak azokra az adatokra, amelyeket mi és a gyermekeink is napi szinten továbbítunk különféle mobilalkalmazásokon keresztül, emailben, szoftvertermékek használatával, közösségi médián keresztül vagy a kiválasztott böngészőnk használatával. Egyetlen gombnyomással képesek vagyunk információt továbbítani a világ minden sarkába, csakhogy ezt az információátadást meg lehet szakítani, el lehet téríteni, ki lehet szivárogtatni, ki lehet használni és vissza lehet vele élni. Még a legújabb technológiák, mint például az e-bankolás vagy az e-kereskedelem, valamint a felhőtárolás és a felhőkben való munka is veszélyeztetettek, és az információink, valamint az államunk információinak védelme is a jól képzett és magasan kvalifikált internetbiztonsági szakértőktől függ.

Mivel az összes technológiát a személyes, vagy a különféle érzékenységi szintű információk átadására használják, ezek védelme rendkívül fontos szerepet játszik a normál életünk és a társadalomban való működési képességünk szempontjából. A számítógépes bűnözés és az internetes zaklatás óriási terhet ró a társadalomra, főként mivel az internet a terrorizmus (Wenke és Rotoloni, 2016) és a gazdasági kizsákmányolás (Europol, 2018) elsődleges eszközévé vált, amivel szemben az internetbiztonság és a személyes tudatosság a számítógépes biztonsági kérdésekben állnak a megelőzés taktikájaként.

Az Europol 2018. évi jelentése után ismét nyilvánvaló, hogy az Iszlám Állam (IS) területének 2016. és 2017. közötti elvesztése nem jelenti tekintélyének elvesztését a követői körében, vagy a támadásokra való buzdítás nyilvánvaló csökkenését. Ehelyett a csoport továbbra is az internetet használja doktrínájának hirdetésére és terrorcselekmények ösztönzésére. A katonai vereség sok szempontból még fontosabbá tette az internetet az IS számára; a különbség annyi, hogy az államépítő törekvéseikről áttértek a nyugati terrortámadások inspirálására és megkísérlésére az internet segítségével.

A számítógépes bűnözésről szóló, 2018-tól kezdődő jelentésében az Europol figyelmeztet bennünket a pénzügyi indíttatású kártevő támadásokra, mint olyan fenyegetésre, amely várhatóan folytatódni fog és a következő két évben akár kétszeresére emelkedhet.

Az illegális adatszerzés mellett a hanyag felhasználói magatartás miatt vagy az adatok feltörése után a társadalom különféle szervezeti rétegeiben a személyazonosság-lopásokról szóló jelentések egyre több és személyes következményekkel járnak.

Vegyük példaként a 2017-ben bejelentett, az Equifax társasággal kapcsolatos legnagyobb adatfeltörést, amely világszerte több mint 100 millió hitelfelhasználót érintett. Az EU GDPR-jának 2018 májusában történt hatályba lépésével az adatok feltörésének jelentése ma már törvényi előírás az egész EU-ban, és jelentős bírságokat, új fenyegetéseket és kihívásokat hoz magával. A számítógépes bűnözés növekedése miatt az Európai Unió az internetbiztonságot, mint egyik alapvető értékét ismerte el, ami több, az EK által támogatott, az internetbiztonsággal kapcsolatos kezdeményezést eredményezett.

Az internetbiztonság olyan foglalkozás, amely óriási értéket képvisel a társadalom számára. Az internetbiztonsági szakemberek - különféle munkakörökben és szakértelemmel -, akárcsak az orvosok, a rendőrök vagy az ügyvédek, segítik az embereket abban, hogy a társadalom fizikai és mentális egészségét és biztonságát megőrizzék a mindennapokban.

Az internetbiztonsági szakemberek segítik az olykor borzalmas és obszcén bűncselekmények elleni küzdelmet, például részt vesznek a gyermekek szexuális kizsákmányolása (CSE) elleni küzdelemben. Szintén az Europol 2018. évi jelentéséből nyilvánvaló, hogy a gyermekek szexuális kizsákmányolásával kapcsolatosan észlelt online anyag (CSEM), beleértve a saját előállítású kifejező tartalmakat (SGEM), továbbra is növekszik. Mivel egyre több fiatalkorú fér hozzá az internethez és a közösségi média platformokhoz, az online szexuális kényszerítés és zsarolás kockázata továbbra is emelkedőben van. A beágyazott hírfolyam lehetőségekkel is rendelkező közösségi médiaalkalmazások népszerűsége az ezeken a platformokon élőben kiposztolt SGEM számának erőteljes növekedését eredményezte.

Sok a veszélyeztető tényező, és az internetbiztonsági szakemberek a társadalom tudatosságának és internetbiztonsági szokásainak általános minőségi javításával tudnak fellépni ellenük. Segítenek a zaklatók felderítésében, a tartalom eltüntetésében, az áldozatok megtalálásában és támogatásában, valamint az ilyen bűncselekmények hatásainak enyhítésében és a megelőzésben.

A technológiai fejlődés érettségével, internethasználatunk rendkívüli megnövekedésével, és óriási mennyiségű érzékeny adat előállításával párhuzamosan az internetbiztonság társadalmi értéke várhatóan még jobban emelkedik majd a belátható jövőben.

2. INTERNETBIZTONSÁGI FOGLALKOZÁSI TERÜLETEK

A vállalatok manapság kijelölnek egy alkalmas személyt vagy embercsoportot az általános internetbiztonsági helyzetük biztosítása érdekében. Ez lehet például egy általános adatvédelmi szabályzat vagy katasztrófa utáni helyreállítási terv, amely magában foglalja a kockázatértékelést, a helyreállítási stratégiákat, és a prioritások kiosztását is.

Azt hinni, hogy az internetbiztonság csak a nagyobb vállalatok luxusa és kiváltsága, és hogy csupán technikai hátteret igényel, ma már nem elfogadható. Minden üzleti, tudományos intézménynek vagy kormányzati szervezetnek konkrét cselekvési tervvel kell rendelkeznie az adatok védelme, tárolása, feldolgozása, elemzése, törlése, kezelése kapcsán, illetve a biztonsági rés vagy katasztrófa utáni helyreállítás esetére. Az internetbiztonság manapság üzleti és személyes prioritás is, nem csupán informatikai kérdés. Bármilyen típusú szervezet - legyen az ipari, tudományos vagy kormányzati szervezet - számára az egyik legnagyobb fenyegetés az úgynevezett „kritikus infrastruktúrák" lehetséges hibája. A kritikus infrastruktúrák olyan rendszereket vagy eszközöket jelentenek, melyek meghibásodása vagy működésképtelensége ellehetetleníti a szervezetek funkcióit, ami gazdasági következményekkel jár, vagy akár a nemzetbiztonságot is veszélyeztetheti.

A számítógépes támadások egy másik nagyon csábító területe, ahol rendkívül fontos az internetbiztonság, természetesen a pénzügyi szektor. Az internetbiztonsági szakemberekre nagy szükség van a pénzügyi szektorban, ahol a támadások exponenciálisan növekednek, valamint a potenciális sebezhetőségek kihasználásának is vannak kockázatai. A pénzünket online kezeljük - online banki platformokat és alkalmazásokat használunk azért, hogy ne kelljen fizikailag bemennünk a bankba elintézni ezeket. Ha felhasználóként figyelmetlenné válunk, akkor egy kártékony szoftverrel megfertőzött eszköz veszélybe sodorja a pénzügyi biztonságunkat, sőt, a legrosszabb esetben megfelelő internetbiztonsági infrastruktúra hiányában behatolhat a pénzügyi szolgáltató hálózatába is. Ugyanez vonatkozik a biztosítótársaságokra, állami ügynökségekre, oktatási és tudományos szervezetekre.

A mai társadalom minden területén felmerült a globális internetbiztonsági tudatosság és az általános ismeretek javításának szükségessége. Nem kétséges, hogy az internetes technológia fejlődése miatt az internetbiztonsággal és az alapvető számítógépes higiénével kapcsolatos személyes tudatosságunk fejlesztése után a helyi internetbiztonsági szakemberek ösztönzése és az internetbiztonsági szakma objektív képviselete a legfontosabb feladat. Az internetbiztonsági szakember objektív megjelenítése nem a „magányos hacker egy alagsorban", hanem egy nagyon fontos szakember, aki sokféle tudományágban dolgozik, ami kompetenciák, készségek és képesítések széles spektrumát igényli. Lássunk erre néhány példát.

2.1 Példák a lehetséges munkaterületekre: egészségügyi ellátó rendszerek

Ha az internetbiztonságra gondolunk, akkor vagy személyes védelmünket és biztonságunkat, illetve a személyes adataink védelmét, vagy a munkahelyünk érzékeny dokumentumainak védelmét értjük alatta. Az egészségügyi ellátás azonban a számítógépes támadások legsebezhetőbb célpontjai közé tartozik. Ennek több oka is lehetséges, de ezek közül a legvalószínűbbek a következők:

- A személyes adatok és érzékeny információ nagy mennyisége, amelyet a kórházakban és az egészségügyi adatbázisokban, adattárakban és rendszerekben kezelnek.
- Kis informatikai részleg, korlátozott szakértelemmel az internetbiztonság területén, ahol esetleg nincs is internetbiztonsági szakértő az informatikai csapatokban.
- Korlátozottan rugalmas költségvetés, különösen az állami egészségügyi rendszerek esetében, amely nem teszi lehetővé az internetbiztonsági ellenőrzések elvégzését, a meglévő infrastruktúrák megerősítését, az informatikai osztály vagy az adminisztráció képzését.

Ne feledje, hogy nemcsak a nagy egészségügyi rendszerekről beszélünk, hanem a kis magánkórházakról, a kisvárosok kórházairól, laboratóriumokról és másokról is. Az internetbiztonság óriási szerepet játszik az ilyen rendszerekben, és ezek hiánya esetén is.

A legfrissebb jelentések, mint például a Symantec 2018-tól kezdődő jelentései azt mutatják, hogy az egészségügyi ellátó egységek és rendszerek ellen elkövetett számítógépes támadások száma drasztikusan megnövekedett az elmúlt években. Ez nem csak a személyes adatainkra és a magánszférára nézve jelent kockázatot. Például egy kórházi infrastruktúra elleni számítógépes támadás irányulhat célzottan olyan eszközökre is, amelyek nyomon követik a beteg állapotát, vagy megszakíthat egy robot segítségével végzett műtétet. Az egészségügyben egyre több az internetes eszköz (IoT), mint például a HVAC rendszerek vagy az orvostechnikai eszközök. Ezeket az eszközöket gyakran könnyebb megtámadni, és még ennél is ijesztőbb, hogy ezek gyakran a kórház fő hálózatához kapcsolódnak, ami azt jelenti, hogy még átjáróként is szolgálhatnak egy kifinomultabb támadáshoz.

Önmagában az orvosi eszközök instabillá tétele is, anélkül, hogy rajtuk keresztül támadnák a kórház egész infrastruktúráját, pusztító következményekkel járhat. Egy orvosi eszköz megtámadása megölheti a beteget vagy ronthat az állapotán.

A kórházi infrastruktúra elleni erőteljes számítógépes támadás irányulhat az ellátási láncra is, és potenciálisan halálos következményekkel járhat. Ezért alapos oka van annak, hogy manapság egyes egészségügyi intézmények megkövetelik a beszállítóiktól, hogy megbízható internetbiztonsági tervvel rendelkezzenek.

Az egészségügyi ellátó rendszereket érő egyik leggyakoribb támadás továbbra is a zsarolóvírus-támadás, mivel az egészségügyi ellátó rendszerekben feldolgozott adatok vonzóak a bűnözők számára.

2.2 Példák a lehetséges munkaterületekre: ipari és kritikus infrastruktúrák

A SCADA (felügyeleti vezérlési és adatgyűjtési) rendszert leggyakrabban vezérlőrendszer-architektúraként definiálják, amely érzékelőket, mikrovezérlőket, hálózati adatkommunikációt és grafikus felhasználói felületeket használ a folyamatkezeléshez, de más perifériás eszközöket is használ. A SCADA rendszerek használatát is fontolóra vették az építésben a projektvezérelt folyamatok irányítása és üzemeltetése során. (***Antunes és Poshdar, 2018***)

Forrás: afcyber.af.mil

Nagyon ismert támadás volt a SCADA rendszer ellen a 2010. évi Stuxnet-támadás egy iráni atomerőművel szemben. A Stuxnet önmagában egy rosszindulatú számítógépes féreg, amely kifejezetten az iráni atomerőmű PLC-it célozta meg, amelyek a gépeket és ipari berendezéseket irányítják, ideértve a centrifugákat is, amelyek a nukleáris anyagok szétválasztására szolgálnak. Röviden szólva ez a féreg megtámadta az iráni atomerőmű centrifugáit, és a gyorsan forgó centrifugák széttörtek, így tönkretéve a nukleáris centrifugák majdnem egyötödét.

Mindannyian el tudjuk képzelni egy atomerőmű fizikai meghibásodásának veszélyét és annak pusztító következményeit. Ilyen jellegű károkat lehet elkövetni számítógépes támadás útján, amely jól megmutatja, hogy globális szinten mennyire fontos a képzett internetbiztonsági szakemberek hiányának csökkentése és az internetbiztonsági karrier ösztönzése.

Hasonló mértékben függ az internetbiztonságtól a szállítás területe is. Gondoljunk csak a repülőtéri és repülési, illetve az olajszállító tartályhajók és a fúrótornyok biztonságára! Az internetbiztonsággal kapcsolatos kutatás és innováció 2019-től kezdődő könyvében az AEGIS rámutat arra a tengeri területtel kapcsolatos általános aggályra, hogy az infrastruktúra és a szállítás az internetbiztonságot tekintve nem naprakész. A modern hajók élettartama körülbelül 25-30 év, de nagyon sok olyan 30 évnél idősebb hajó van kint a tengeren, amelyeket gyakran nem újítanak fel a legújabb technológiáknak megfelelően, és biztonsági szempontból sem megfelelőek.

Az IoT vonatkozásában a megfelelő internetbiztonsági védelem fontossága még nyilvánvalóbbá válik, mivel sok közlekedési rendszer, beleértve a repülőtéri rendszereket is, a modern technológiára támaszkodik az utasok azonosítása és a fedélzeten lévő IT-infrastruktúrák védelme érdekében. A közlekedési ágazat navigációs rendszerei gyakran támaszkodnak a modern technológiákra is, amelyek számítógépes támadások célpontjai lehetnek.

Az AEGIS fehér könyve[60] 2019-től kezdve azt írja: „Súlyos következményekkel járhat például, ha az internetes támadások a portok vagy navigációs rendszerek által használt konténerkövető szoftvert célozzák meg. Fennáll az élet és a vagyon veszélyeztetése is, ha az ilyen támadások a hajók összeütközését okozzák. A szisztematikus késedelmek ütközések nélkül is pénzügyi és szállítási problémákat okoznak, amelyek világszerte hatást gyakorolhatnak a kereskedelmi tevékenységekre. Szintén a tengeri hajózási társaságokat célozzák meg olyan támadásokkal fenyegető csoportok, amelyek az üzleti emailekre (BEC) és azok hamisítására (BES) irányuló csalásokkal foglalkoznak, melyek eredményeként évente sok millió dollárt lopnak el."

3. POZÍCIÓK KÜLÖNFÉLE TUDOMÁNYTERÜLETEKEN

A munkaerőpiacon sok hivatkozás található, amikor foglalkozásokról, munkahelyekről, profilokról és készségekről beszélünk. Mi inkább a legismertebbek, például az ESCO, az EU új munkaerő-osztályozása, az e-CF vagy az 16234-es Európai Szabvány, valamint az USA ONET portáljának használatát részesítettük előnyben. Bevezetésként tisztáznunk kell néhány alapfogalmat:

- A foglalkozás leírását az ESCO-ból vettük át: „Egy foglalkozás olyan szakmák csoportja, amelyek hasonló feladatokat foglalnak magukban, és amelyek hasonló készségeket igényelnek. A foglalkozásokat nem szabad összekeverni a munkakörökkel vagy a beosztásokkal. Míg a munka egy meghatározott munkakörnyezethez kötődik, és egy személy hajtja végre, addig a foglalkozásokat közös jellemzők alapján csoportosítják."[61]
- Minden foglalkozáshoz meg lehet határozni egy foglalkozási leírást (amivel meghatározható egy adott munka profilja). Az ESCO esetében a profilok a foglalkozás magyarázatát tartalmazzák leírás és alternatív elnevezések formájában, valamint felsorolják azokat az ismereteket, készségeket és kompetenciákat, amelyeket a szakértők az európai foglalkoztatás szempontjából relevánsnak tartottak.

60 europa.eu/commission/sites/beta-political/files/feher_konyv_europa_jovojerol_hu.pdf
61 https://ec.europa.eu/esco/portal/escopedia/Occupation

3.1 Az ESCO portálon[62] szereplő foglalkozások, leírásuk és a hozzájuk kapcsolódó feladatok

- **IKT biztonsági vezető**: megvédi a vállalati és munkavállalói információkat az illetéktelen hozzáféréstől. Meghatározza az információs rendszer biztonsági előírásait, irányítja az összes információs rendszer biztonsági telepítését és biztosítja az információk rendelkezésre állását. CISO néven is ismertek.
- **IKT biztonsági menedzser:** az IKT biztonsági menedzserek javasolják és végrehajtják a szükséges biztonsági frissítéseket. Tanácsot adnak, támogatnak, tájékoztatnak, képzést és biztonsági ismereteket biztosítanak, és közvetlenül beavatkoznak a hálózat vagy a rendszer egészébe vagy egy részébe.
- **IKT vezető auditor**: figyelemmel kíséri az információs rendszerek, platformok és működési eljárások ellenőrzéséért felelős IKT-auditorokat, a hatékonyság, a pontosság és a biztonság érdekében kialakított vállalati szabványoknak megfelelően. Felméri az IKT infrastruktúrát a szervezetet érintő kockázatok szempontjából, és ellenőrzéseket végez a veszteségek csökkentése érdekében. Meghatározza és kidolgozza a jelenlegi kockázatkezelési ellenőrzések, valamint a rendszerváltozások vagy frissítések végrehajtásának javítását.
- **IKT alkalmazásmenedzser**: az IKT alkalmazásmenedzserek modelleket, irányelveket, módszereket, technikákat és eszközöket kutatnak, terveznek és fejlesztenek, amelyek javítják a szervezet számítógépes biztonságát, ellenálló képességét és egy katasztrófa utáni helyreállítást.
- **IKT biztonsági technikus**: az IKT biztonsági technikusok szükség esetén javaslatot tesznek és végrehajtják a szükséges biztonsági frissítéseket és intézkedéseket. Tanácsot adnak, támogatnak, tájékoztatnak, képzést biztosítanak és biztonsági ismereteket nyújtanak.
- **IKT biztonsági tanácsadó:** az IKT biztonsági tanácsadói tanácsadást végeznek és megoldásokat vezetnek be az adatokhoz és a programokhoz való hozzáférés ellenőrzéséhez. Elősegítik a biztonságos információcserét.
- **IKT biztonsági rendszergazda**: az IKT biztonsági rendszergazdák biztonsági intézkedéseket terveznek és hajtanak végre az információk és az adatok védelme érdekében az illetéktelen hozzáférés, a szándékos támadás, a lopás és a korrupció ellen.
- **Etikus hekker**: az etikus hekkerek az iparág által elfogadott módszerekkel és protokollokkal összhangban elvégzik a biztonsági rések felmérését és behatolási teszteket. Elemzik a rendszereket olyan potenciális sérülékenységek szempontjából, amelyeket a nem megfelelő rendszerkonfiguráció, a hardver vagy a szoftver hibái, vagy az üzemeltetési hiányosságok okozhatnak.
- **IT auditor:** az informatikai auditorok az információs rendszerek, platformok és működési eljárások ellenőrzését végzik a hatékonyságra, pontosságra és biztonságra vonatkozó vállalati szabványoknak megfelelően. Felmérik az IKT infrastruktúrát a szervezetet érintő kockázatok szempontjából, és ellenőrzéseket vezetnek be a veszteségek csökkentése érdekében. Meghatározzák és javaslatot tesznek a jelenlegi kockázatkezelési ellenőrzések, valamint a rendszerváltozások vagy frissítések elvégzésének javítására.
- **Információbiztonsági elemző**[63]: megtervezi, végrehajtja, frissíti vagy figyelemmel kíséri a biztonsági intézkedéseket a számítógépes hálózatok és az információk védelme érdekében. Biztosíthatja, hogy rendelkezésre álljanak a megfelelő biztonsági ellenőrzések, amelyek megóvják a digitális fájlokat és a létfontosságú elektronikus infrastruktúrát. Reagálhat a számítógépes biztonsági támadásokra és vírusokra.

62 https://ec.europa.eu/esco/portal/occupation

63 Ezt a foglalkozásleírást az USA foglalkozási információinak nyilvános adatbázisából tettük hozzá az ESCO portálon lévő foglalkozásokhoz

3.2 Szükséges készségek

Az ezekhez a foglalkozásokhoz leggyakrabban szükséges készségek a következők:

- **IKT kockázatkezelés elvégzése**: eljárásokat dolgoz ki és hajt végre az IKT kockázatok, például a hackek vagy adatszivárgások azonosítására, értékelésére, kezelésére és enyhítésére, a vállalat kockázatstratégiájának, eljárásainak és előírásainak megfelelően. Elemzi és kezeli a biztonsági kockázatokat és eseményeket. Intézkedéseket javasol a digitális biztonsági stratégia javítására.
- **Informatikai biztonsági előírások kezelése**: irányítja a vonatkozó ipari szabványok, a bevált gyakorlatok és az információbiztonság jogi követelményeinek megfelelő alkalmazást és ezek betartását.
- **Végrehajtja a katasztrófa utáni helyreállítási tervet**: elkészíti, teszteli, és ha szükséges, végrehajtja a cselekvési tervet az elveszített információs rendszer adatainak visszanyerésére vagy helyettesítésére.
- **IKT auditokat végez:** auditokat szervez és hajt végre az IKT-rendszerek, a rendszerek összetevőinek való megfelelés, az információfeldolgozó rendszerek és az információbiztonság értékelése érdekében. Azonosítja és összegyűjti a lehetséges kritikus kérdéseket, és megoldásokat javasol a szükséges szabványok és megoldások alapján.
- **Azonosítja az IKT rendszer gyenge pontjait**: elemzi a rendszer- és hálózati architektúrát, a hardvert és a szoftvert, valamint az adatokat, annak érdekében, hogy azonosítsa a rendszer gyenge pontjait, vagy a behatolásokkal és a támadásokkal szembeni sérülékenységét.

Noha a fenti lista létező foglalkozásokat mutat be, az internetbiztonsági területen való elhelyezkedés nem korlátozódik csupán ezekre a foglalkozásokra. Az egyes vállalatoknál kialakított konkrét munkakörök nem mindig felelnek meg tökéletesen a hivatalos foglalkozásoknak, hanem olyan feladatköröket ölelhetnek fel, amelyeket gyakran rugalmasan, a munkakörön belül kell kialakítani.

A szerepkör azt jelenti, amit egy adott munkafolyamaton belül végeznek egy szervezetben. Az IKT rendszergazdák például, akik a rendszerek és az IKT-infrastruktúra konfigurációját és erőforrásait kezelik az IKT munkájuk részeként játszhatják az internetbiztonsági szakemberek szerepét, mivel a kockázatok felmérése vagy a biztonsági technikáknak a hálózat egészén vagy egy részén történő alkalmazása a feladatkörükbe tartozik.

Sok olyan munkakör, de akár foglalkozás is, ahol nem teljes munkaidőben foglalkoznak internetbiztonsággal, gyakran megköveteli, hogy a megfelelő szakemberek szerepet vállaljanak az informatikai biztonságban. Az ESCO-val kapcsolatos kutatásaink során olyan foglalkozásokat is felfedeztünk, amelyek internetbiztonsággal kapcsolatos feladatokat és készségeket is magukban foglalnak, mivel az adott területen gyakran szükség van speciális szerepek betöltésére.

Tipikus példák az ilyen beosztásokra: az IKT-rendszergazda, webmester, IKT-hálózati mérnök, digitális kriminalisztikai szakértő, IKT-kapacitástervező IKT-alkalmazásfejlesztő, adatbázis-adminisztrátor, IKT-katasztrófaelhárító elemző stb.

A szerepleírások tekintetében megvizsgálhatjuk az európai E-kompetencia keretrendszert (e-CF), amely az információs és kommunikációs technológia (IKT) munkahelyen alkalmazandó 40 kompetencia forrásanyaga, és amelyet a CEN hivatalosan közzétett EN 16234-1 Európai normaként. Az ehhez kapcsolódó CWA 16458-1: 2018. dokumentum határozza meg azt a 30 IKT-szakmai szerepleírást, amiket az IKT-szakemberek bármely szervezetben végezhetnek, a kompetencia meghatározásához az e-CF-t[64] véve alapul. Az internetbiztonsághoz közvetlenül kapcsolódó kettő ezek közül a következő:

- **Internetbiztonsági menedzser:** meghatározza és végrehajtja a digitális biztonsági stratégiát a szervezet egészében. Proaktív internetbiztonsági védelmet valósít meg vizsgálatok, tájékoztatás, figyelmeztetés és oktatás révén a szervezet egészében.
- **Internetbiztonsági szakértő:** meghatározza, javasolja és végrehajtja a szükséges internetbiztonsági technikákat és gyakorlatokat, összhangban a biztonsági előírásokkal és szabályzattal. Hozzájárul a biztonsági eljárásokhoz az ezekkel kapcsolatos tudatosság és megfelelés kialakításával tanácsadás, támogatás, információ és képzés révén.

4. INTERNETBIZTONSÁGI KARRIEREK

Az internetbiztonsági karrierek közül a legismertebb az etikus hekker, akiknek a közhiedelemmel ellentétben szabványok és normatívák határozzák meg és szabályozzák a tevékenységüket, és munkájukban a nevükben szereplő etika alapvető szerepet játszik.

Habár az internetbiztonság meglehetősen új szakmai terület, a technológia megjelenése miatt minden ágazatban dolgoznak internetbiztonsági szakemberek is:

- ipar és környezetvédelem: támadásoknak ellenálló rendszerek a kritikus infrastruktúrákhoz, az ICS / SCADA biztonság, az intelligens ipari hálózatok és az intelligens ipari hálózatok védelme;
- közlekedés és kommunikáció: intelligens autók védelme, drónok és műholdas kommunikációs rendszerek biztonsága és védelme;
- pénzügy és biztosítás: csalások felderítése a banki és biztosítási ágazatban, SIEM (biztonsági információs eseménykezelés);
- egészségügy és gyógyszeripar: az e-eszközök (IoT) védelme, az egészségügyi kutatási információk titkosítása, az egészségügyi adatok biztonságos tárolása;
- oktatás: számítógépes oktatás, internetbiztonsági labor;
- honvédelem és e-kormányzat: internetes hírszerzés, elhárítás és események szimulálása.

64 ftp://ftp.cencenelec.eu/CEN/WhatWeDo/Fields/ICT/eEducation/WS/eSkills/ICTSkills/CWA%2016458-1_2018.pdf

Így válik az internetbiztonság olyan szakmává, amelyben a foglalkozástól függően nagyon különböző feladatok végezhetők. A hálózati sebezhetőségeket tesztelő és felderítő etikai hekkerektől kezdve a technológiai kockázatokkal foglalkozó tanácsadókig, akik a különböző ügyfelek cégeinél vizsgálódnak, hogy tanácsot adjanak nekik ezek csökkentésének különböző módjairól és az egyes sérülések következményeiről az internetes hírszerzés elemzőinek munkája alapján, akiknek üzleti adatokkal és a meglévő kockázatokkal elemzést kell készíteniük, felderítést végezve az ügyfelek védelmének érdekében. A védelmi feladatuk révén – mint valamiféle kibertéri rendőrök - mindegyik hozzátesz valamit a hálózatok biztonságossá tételéhez valamennyiünk számára. Az alábbiakban annak érdekében, hogy a tanárok példákat is bemutathassanak, készítettünk egy összeállítást ezekből a foglalkozásokból, összehasonlítva őket más, hagyományosabb szakmákkal.

5. HOGYAN LEHET VALAKI INTERNETBIZTONSÁGI SZAKEMBER?

Az ehhez szükséges tanulmányok az utóbbi években sokat változtak és az adott országtól[65], akár az országon belüli régiótól is függnek, mivel a terület meglehetősen új. *A Cybersecurityeducation.org[66] szerint „a munkáltatók gyakran részesítik előnyben azokat a potenciális alkalmazottakat, akik legalább alapszintű diplomával rendelkeznek olyan tudományágakban, mint például információs rendszerek (IS), információtechnológia (IT), alkalmazott matematika, számítógépes programozás, mérnöki vagy más számítógépes terület. Szükség lehet a pálya során szakmai továbbképzésre, olyan szervezetek és vállalkozások akkreditálásával, mint például a Microsoft, a Cisco, vagy más olyan nagy szoftvergyártó, amely biztonsági dolgozókat alkalmaz.”* Az utóbbi években az internetbiztonsági csapatok különböző háttérrel rendelkező szakembereket toboroznak. Bár a technikai képzés továbbra is a legfontosabb, igény van kriminológusokra, szociológusokra, pszichológusokra, ügyvédekre, marketing és reklám szakemberekre, grafikusokra stb. Mindegyikre természetesen a megfelelő internetbiztonsági képzettséggel.

Lássunk egy részletesebb példát az egyik ilyen pályára, például az incidenskezelés[67] területén. Ők az elsők, akik mentésre indulnak, amikor számítógépes vészhelyzet történik: ők az internet tűzoltói.

A napi feladatok során felmérik a rendszerek sebezhetőségét, eljárásokat dolgoznak ki az egyes vészhelyzetekre való reagáláshoz, behatolási tesztet, kockázatelemzést és biztonsági ellenőrzéseket végeznek a támadások megelőzése érdekében, és ha számítógépes támadás történik, gyorsan akcióba lépnek, és jelentik az eseményt a menedzsment csapatoknak. Átfogó rálátásuk van az internetbiztonságra. Az alacsonyabb pozíciót jelentő számítógépes biztonsági eseményekre reagáló csoportba kerüléshez internetbiztonságra szakosodott tanulmányok kellenek, például internetbiztonsági szakképesítés, vagy internetbiztonsági mérnöki diploma, a pozíciótól és a fizetéstől függően. Egy másik lehetőség a számítástechnikai mérnöki, távközlési, vagy alkalmazott matematika vagy fizika szakok elvégzése, majd az internetbiztonság mesterfokozatának megszerzése, vagy más, hasonló végzettség.

65 A Magyarországon lévő képzési lehetőségeket e könyv II. fejezet 1.4.2 pontjában mutatjuk be. Ugyanakkor itt is megtalálják a továbbképzési lehetőségeket a „szakirodalom, hivatkozások” pontban.
66 Source: https://www.cybersecurityeducation.org/careers/security-engineer
67 Source: https://www.cybersecurityeducation.org/careers/incident-responder

ÖSSZEFOGLALÁS

Ebben a fejezetben áttekintettük az internetbiztonság területével kapcsolatos karrierprofilokat és összegyűjtöttük a szükséges készségeket és kompetenciákat a különféle kompetenciakeretek alapján. Ugyancsak feltártuk az internetbiztonsági szakma helyét a kortárs társadalmi-gazdasági ökoszisztémában. Megvitattuk, miért multidiszciplináris terület az internetbiztonság, és hogy a sikeres működéshez területspecifikus ismeretek, társadalomismeret és természetesen a technikai készségek munkahelyspecifikus keveréke szükséges. Tekintet nélkül arra, hogy a technikai készségek az internetbiztonsági karrier kulcsfontosságú részét képezik, és mennyiségileg könnyebben értékelhetők és mérhetők a jelöltek körében, rájövünk, hogy szükség van annak az elméletnek a terjesztésére, hogy ez csupán az egyik összetevő, ami az internetbiztonsági karrierhez kell.

Ezért ösztönözzük azokat a tanárokat, akiknek a diákjai érdeklődnek az internetbiztonsági karrier vagy oktatás iránt – de úgy gondolják, hogy hiányzik a sikerhez szükséges technikai hátterük – hogy átfogóbb megközelítést alkalmazva beszéljenek velük az internetbiztonságról. [68]

A sebezhetőségek minimalizálása, a fenyegetések észlelése és az ellenálló képesség menedzselése nem csak technikai ismereteket igényel, hanem annak megértését is, hogy a felhasználói szokások hogyan informálhatnak minket a hálózatok, a szoftverek, a webplatformok és az eszközök állapotáról, és sebezhetőségének kockázatáról. (Arachchilage, 2013)

Az internetbiztonság, mint ágazat, nem csak technikai, hanem társadalmi és szervezési alkalmasságot is igényel szakembereitől. (Dawson, 2018). Az internetbiztonság, mint ipari terület, különféle készségekkel, kompetenciákkal és ismeretekkel rendelkező diákok számára is karrierlehetőséget és személyes fejlődési lehetőséget nyújt. Az egyik ilyen foglalkozás kapcsolatos lehet a számítógépes bűnözés elleni nyomozással, ahol a munkakörtől függően bizonyos technikai ismeretekre lehet szükség, bár a társadalmi készségek és a kriminálpszichológiai szaktudás fontosabb (Ono M., 2011).

Az internetbiztonsági szakma nem egyetlen munka, feladat vagy tudásbázis[69]. Magában foglalja a különféle típusú területeket, tudományokat és kompetenciákat, önmagában is az egész életen át tartó tanulás, az önfejlesztés és a növekedés lehetőségeinek platformjává válik, és felelősek vagyunk az ágazat megfelelő képviseletéért a fiatal lányok és fiúk előtt, akik még a pályaválasztásnál vagy a továbbtanulásnál tartanak.

68 E könyv II. fejezetében közzétettünk olyan - az online tanártovábbképzés keretében készült - prezentációkat is, melyek a hazai továbbképzési lehetőségeket tartalmazzák.

69 A nemzetközi projekt keretében interjúkat készítettünk Magyarországon különböző IT biztonsági területen sikeres karriert elért hölgyekkel, akik példaképként bemutathatók szolgálhatnak a pályaválasztás előtt álló fiataloknak.
https://www.szamalk-szalezi.hu/noi-peldakepek-az-informatika-vilagaban

SZAKIRODALOM, HIVATKOZÁSOK

1. Antunes, R., & Poshdar, M. (2018). Envision of Integrated Information System for Project-Driven Production in Construction. *Proc. 26th Annual Conference of the International. Group for Lean Construction (IGLC)*, (págs. 134–143). doi:10.24928/2018/0511
2. Arachchilage, N. A. (2013). A Game Design Framework for Avoiding Phishing Attacks. *Computers in Human Behavior 29* , 706–714. doi:10.1016/j.chb.2012.12.018
3. Choo K., R. (2011). The Cyber Threat Landscape: Challenges and Future Research Directions. *Computer Security 30*, 719–731. doi:10.1016/j.cose.2011.08.00
4. Dawson, J. &. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers in Psychology, 9*, 744. doi:10.3389/fpsyg.2018.00744
5. Department of Homeland Security. (2014). *Best Practices for Planning a Cybersecurity Workforce White Paper.* U.S. Department of Homeland Security.
6. Európai képességek, kompetenciák, és foglalkozások egységes osztályozási rendszere (ESCO)
   https://www.oktatas.hu/kepesiteseknyito/kepesitesek/esco
7. Kiberbiztonság, karrierlehetőségek
   https://nki.gov.hu/intezet/karrier/
   https://eduline.hu/felsooktatas/komoly_hiany_van_informaciobiztonsagi_szake_JX5XSH
   https://fujitsuhungary.blog.hu/2020/04/14/2020_a_tehetseges_kiberbiztonsagi_szakemberek_hianyanak_kezelesehez_radikalisan_uj_gondolkodasmod_sz
8. Női példaképek az informatikai biztonság, kiberbiztonság szakmában
   https://www.szamalk-szalezi.hu/noi-peldakepek-az-informatika-vilagaban/
9. Newhouse W., K. S. (August de 2017). Cybersecurity Workforce Framework, NIST Special Publication. *National Initiative for Cybersecurity Education (NICE), U.S. Department of Commerce.* , 800-881. doi:10.6028/NIST.SP.800-181
10. Ono M., S. D. (2011). Cognitive ability, emotional intelligence, and the big five personality dimensions as predictors of criminal investigator performance . *Criminal Justice and Behavior, 38*, 471–491. doi:10.1177/009385481
11. IT-biztonsági, kiberbiztonsági kurzusok és intézmények
    - **Óbudai Egyetem Neumann János Informatikai Kar**
      http://nik.uni-obuda.hu/hu/oktatas
    - **Nemzeti Közszolgálati Egyetem, Államtudományi és Nemzetközi Tanulmányok Kar**
      https://antk.uni-nke.hu/oktatas/mesterkepzes/kiberbiztonsagi-mesterkepzesi-szak
    - **Cyber Institute Kft (KÜRT Akadémia jogutódja)**
      https://cyberinstitute.hu/kepzesek/etikus_hacker_kepzes_2020

II. DIGITÁLIS BIZTONSÁG A GYAKORLATBAN

BEVEZETŐ

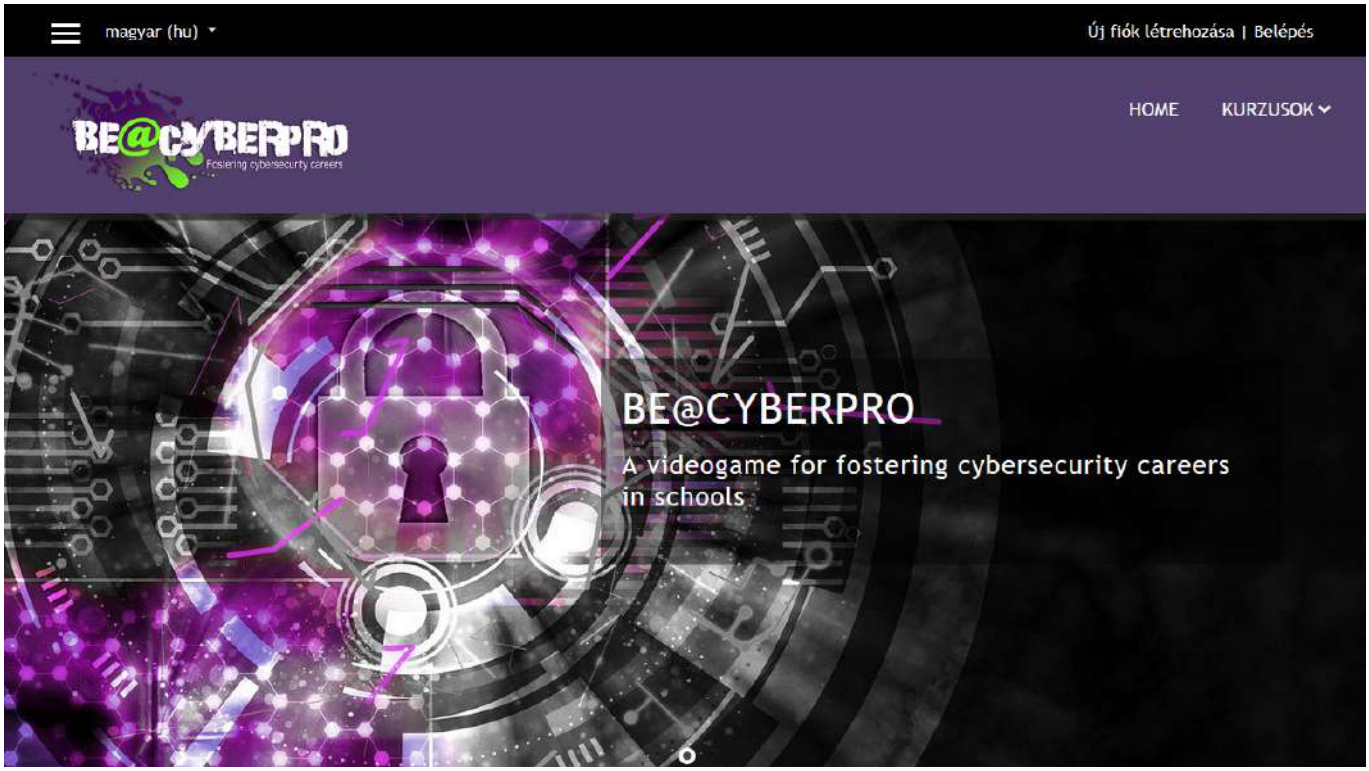
A könyv második fejezetében konkrét *segítséget szeretnénk adni a tanároknak ahhoz, hogy felkészítsék diákjaikat a digitális országúton való biztonságos és felelősségteljes „közlekedésre”, magatartásra.*

Ahogy erről már a bevezetőben is írtunk, a Be@CyberPro nemzetközi projekt keretében négy ország szakembereivel közösen készítettük el „Digitális biztonság” témában azt a tananyagot, melynek valamennyi modulját az első fejezet tartalmazza.

A partnerországok kilenc intézménye által közösen kidolgozott online kurzust elsősorban a tanárok és oktatók számára ajánlottuk. A tananyaggal és a gyakorlati feladatokkal azoknak szeretnénk segíteni, akiknek a munkája összefügg a pályaválasztással, a gyermekek digitális védelmével, a tudatos viselkedés kialakításával az online térben, és akiknek tanárként is, szülőként is feladata a folyamatos önképzés.

Kiemelt témákat választottunk a tanár és oktató kollégák továbbképzéséhez, mert úgy gondoltuk, hogy a digitális biztonság állampolgárként és tanárként önmagunk számára is nagyon fontos, de ennél is jelentősebb a felelősségünk a diákok felkészítésében.

A másik célunk a projektben az volt, hogy minél több fiatalt – közöttük is elsősorban a lányokat – „irányítsunk” az informatikai pályára, mert mindannyiunk érdeke, hogy a digitális térben is minél több fiatal szakember dolgozzon.



A közösen kidolgozott tananyagot minden partnerországban egy-egy pilot kurzus keretében ki is próbáltuk. Magyarországon az online kurzuson 54 fő vett részt. A pedagógusok 68%-a vidéki oktatási intézményben, míg 32%-a fővárosi iskolában dolgozó tanár volt. A képzésen résztvevők több mint fele informatika, míg 45% más szakon oktat.

Valamennyi résztvevő megfogalmazta, hogy elsősorban azért jelentkezett a kurzusra, mert nagyon aktuálisnak és fontosnak tartja a témákat, nem csupán a maguk, hanem a diákjaik szempontjából is. A célok meghatározásából azt is megtudhattuk, hogy a pedagógusok ismereteik gazdagításán túl fontosnak tartották az erről való beszélgetést, vitát, és azt is, hogy tudásukat széles körben megoszthassák.

A képzés nagyon sikeres és eredményes volt, köszönhetően a jó tananyagnak, a feladatoknak és a nagyon aktív tanároknak. Már a képzés idején elhatároztuk, hogy mindenképp közzétesszük azokat az értékeket, melyeket egyenként és közösen a pedagógusok létrehoznak, segítve ezzel valamennyi iskola tanárait és diákjait.

Ezt az elhatározásunkat megerősítette a világjárvány következményeként létrejött helyzet is, ami a gyerekek és fiatalok digitális térben való tartózkodásának idejét a duplájára emelte, megnövelve ezáltal a veszélyeket és kockázatokat is. (Erre még visszatérünk a záró fejezetben!)

A gyermekek és a fiatalok digitális térben történő felelősségteljes magatartásra tanítása, a tanárok és szülők példamutatása, a védelemmel, tanácsadással kapcsolatos feladatok ma a legfontosabb tennivalók.

Ebben a fejezetben ehhez a munkához szeretnék hozzájárulni azzal, hogy közzétesszük a legjobb és mindenki számára talán leghasznosabb feladatmegoldásokat, amelyek játékok, óratervek, tanácsok és ajánlások tanároknak és szülőknek.

1. FELKÉSZÜLÉS A „DIGTÁLIS BIZTONSÁG" TANÍTÁSÁRA AZ ONLINE KURZUS KERETÉBEN

A kurzus minden moduljához a témához kapcsolódó, egyéni feladatot terveztünk, melyek lehetőséget adtak arra, hogy a résztvevő tanárok megtervezzék, hogy milyen módszerekkel fogják átadni a megszerzett ismereteiket a diákoknak.

1.1 Szabadulószoba játék az aktív tanuláshoz

Az első modul feladataként a pedagógusok egy JÁTÉKOT terveztek, és ki is próbálták azt saját iskolájukban, valamelyik tanított csoporttal. Azért választottunk a fiatalok körében kedvelt aktív tanulási módszert, mert a tudást így a diákok játékos formában sajátíthatták el. A szabadulószobák – kreatív tervezéssel, a diákok bevonásával, aktivizálásával – nagy sikert arattak, melyről a pedagógusok beszámoltak munkáikban.

1.1.1 Feladatleírás

Az alábbiakban készítettünk egy szabadulószoba-vázat, amely használható egésszé akkor válik, amikor Önök a rendelkezésre álló helyszín és eszközök figyelembevételével és a csoport sajátosságainak megfelelően elkészítik a hiányzó feladatokat.

A feladatok valamilyen, a képzésben is tárgyalt internetbiztonsági témához kötődjenek, sikeres megoldásuk esetén pedig az általunk megadott kulcsszavakat kapják a tanulók.

A feladatokat például a LearningApps programban tudják megcsinálni, de készülhetnek bármilyen Ön által ismert és használt eszközön. (Ha valaki ezeket nem ismerné, a modul mellékleteként megtalálja a használati útmutatókat.)

Célszerű többségükben online, mobil eszközzel megoldható feladatokat adni, a feladathoz vezető QR- kódokat pedig elrejteni a teremben. Adhatunk néhány papíralapú feladatot is (például keresztrejtvényt), a „sajnos ez hamis nyom" esetére pedig érdemes a feliratot szétvágva szétszórni a teremben.

Előkészületek:

- a feladatok elkészítése, az offline feladatok kinyomtatása a megfelelő példányszámban;
- QR-kódok generálása az online feladatokhoz és a QR-kódok kinyomtatása;
- „hamis nyomok" összeállítása, kinyomtatása;
- megadott QR-kód kinyomtatása;
- a nyomok elrejtése a játék helyszínén a látható és a kereséssel megtalálható helyekre (pl. fiókba, asztal/szék aljára ragasztva, könyvek közé / könyvbe, szemetesbe, faliújságra stb.);
- kerettörténet kinyomtatása;
- wifi kapcsolat, okoseszköz biztosítása (csoportonként 1 eszköz).

A játék helyszíne az osztályterem. A játékot 3-4 fős csoportokban javasoljuk játszani, a játék időkerete 45-60 perc (ez függ a feladatok nehézségétől, a nyomok megtalálhatóságától, és a csoportoktól), elvárásként érdemes előre meghatározni, mennyi idő alatt tekintjük teljesítettnek.

Kerettörténet:

Kiberbiztonsági nyomozósegédi állásra szeretnétek jelentkezni, és éppen megérkeztek az állásinterjú helyszínére. A teremben nincs senki, csupán az alábbi üzenet:

Tisztelt Jelentkezők!

A meghirdetett álláshoz szükséges tudásukat és rátermettségüket úgy bizonyíthatják, ha a megadott időn belül megtalálják azt a titkos, 10 jegyű számsort, amelyet elrejtettem a feladatokban. Figyeljenek minden nyomra, dolgozzanak megfontoltan, végül a helyszínen lévő asszisztensemnek (tanár) mondják meg a számot, és ő közli majd, hogy sikeres-e a megoldás. A játék során nagyon figyeljenek: ne árulják el a többi csoportnak, ha találtak valamit, vagy rájöttek valamire!

KIHÍVÁSOK (megnevezés és leírás)	MEGLEPETÉSEK, HAMIS NYOMOK ÉS SEGÉDESZKÖZÖK	SZÜKSÉGES ANYAGOK / FORRÁSOK	IDŐ
A tanár által készített feladatok megtalálási sorrendje nem releváns, viszont a megfejtéshez mindet meg kell oldani.	A tanár által készített feladatok megfejtései az alábbiak legyenek: ▪ Saferinternet ▪ Hungary ▪ Facebook ▪ Telefonszám ▪ Sajnos ez egy hamis nyom ▪ Sajnos ez egy hamis nyom	Elkészített feladatok kinyomtatva / QR-kódok, elrejtve a teremben. Hamis nyomok elrejtve, okoseszköz internetkapcsolattal, papír, ceruza	5'-40'
A feladatok megfejtéseiből kirakható, hogy „Saferinternet Hungary, Facebook, telefonszám" amiből a diákoknak rá kell jönniük, hogy a megnevezett szervezetre kell a közösségi oldalon rákeresniük, és a 9 jegyű telefonszámot (707080574) lejegyezniük.	Ez viszont egyelőre kevés, keresni kell még egy nyomot a teremben a tizedik számjegyhez.		
A hiányzó utolsó számjegy a lejjebb található QR-kód alapján található ki. A kód egy álhír-teszthez navigál, a felette lévő felirat (Végül hamis) pedig arra utal, hogy a teszt hamis állításainak száma (9) kell "végül" a kódhoz, tehát ez adja meg az utolsó számot. A keresett számsor: 7070805749		Általunk biztosított QR-kód (lásd lejjebb) kinyomtatva, elrejtve okoseszköz internetkapcsolattal, papír, ceruza	5-10'

A játék helyes megfejtése tehát 7070805749, a nyertest akkor hirdessük ki, ha minden csapat végzett. Az állást azok nyerik el, akik a legrövidebb idő alatt szolgáltattak helyes megfejtést.

Végül hamis

A fenti játékot Ön a feladatok nehézségével és elhelyezésével tudja könnyíteni/nehezíteni, vagyis csoportra szabni. A feladatokhoz alább javaslunk néhány programot, de olyat is használhat, ami nincs benne a felsorolásban.

A fenti játékváz néhány egyszerűbb program segítségével gyorsan a csoport igényeire alakítható. Az alábbiakban bemutatjuk pár szóban ezeket a programokat.

LearningApps

A LearningApps, vagy magyarul Tankocka (***www.learningapps.org***) oldal olyan személyre szabható játékokat tartalmaz, amelyek segíthetik a megértést, memorizálást, vagy ellenőrizhetik a tananyag elsajátítását. Lehet benne párosító játékot, keresztrejtvényt, vagy szókeresőt készíteni, hogy csak néhány példát említsünk a sok közül. Az oldalon a tanulók is készíthetnek tankockákat, ami szintén segíti a tananyag elmélyülését. Remek példa erre a tanulók által készített tankocka-mátrix: ***https://learningapps.org/3459799***

(Angol videó a témahétről, és benne a tankockáról: ***https://youtu.be/yvRioMc8mvM***)

Óriási előnye a felületnek, hogy a címkék és témák megjelölésével rákeresve, a „nyilvános" tankockákat elmenthetjük a sajátjaink közé, így akár pillanatok alatt összeállíthatunk a mások által megosztott tankockákból egy gyakorló felületet a saját diákjainknak, segítve őket a tananyag elsajátításában. Mindezek mellett az oldal bejelentkezés után remekül működtethető virtuális osztályteremként is.

1.ábra: példák a LearningApps-ban található feladattípusokra

A LearningApps-ról összefoglaló videót Novák Károly előadásában itt láthatunk: ***https://youtu.be/wk8By0GACEk***. A TankocKapocs – LearningApps/tankockák felhasználói Facebook csoportban pedig naprakész segítséget kaphatunk, ha elakadnánk.

QR-kód generátor

Ezt a két kulcsszót beírva rengeteg regisztráció nélkül használható generátort találunk, ahová egyszerűen beilleszthetjük a kód mögé rejteni kívánt tartalmat. A LearningApps program automatikusan generál QR-kódot minden feladathoz.

Jigsaw Planet – puzzle bármiről

A játék sokszor segít megérteni a tananyagot – erre kínál gyors és egyszerű megoldást a Jigsaw Planet (***https://www.jigsawplanet.com/?lang=hu***). A felületen pár kattintással bármilyen általunk feltöltött képről készíthetünk igény szerinti elemszámú és formájú kirakósjátékot, és elküldhetjük a linket a diákjainknak. Megtehetjük például, hogy az oldalon megosztunk a diákokkal egy saját készítésű infografikát szétvágott puzzle formájában. Játék közben minden erőfeszítés nélkül, észrevétlenül ismerkedhetnek meg a tananyagbeli szintekkel, kapcsolatokkal, összefüggésekkel – és mire elkészül a kirakó, már – a szó szoros értelmében – van egy kép a fejükben a témáról.

Infografika – Piktochart

Egyre vizuálisabbá váló világunkban sokszor kapjuk magunkat azon, hogy szívesebben nézünk végig egy informatív, részletgazdag, de kevés szöveget tartalmazó plakátot, mint hogy elolvasnánk egy hosszú leírást ugyanabban a témában. A fiatalokra ez még sokkal inkább jellemző, és ahhoz, hogy a szövegolvasást megszerettessük velük, érdemes az információt számukra jól feldolgozható formában eljuttatni. Ehhez kiváló eszköz az infografika, ami az információkat képpé rendezve tárja elénk. A program használata egyszerű, a benne rejlő lehetőségek végtelenek, hiszen már régóta ismerjük a törvényszerűséget: egy kép többet mond ezer szónál.

A www.piktochart.com oldalon regisztrálva választhatunk meglévő sablonok közül, de akár teljesen üres „vásznon" is elindíthatjuk a munkát. A bal oldali vezérlőpulton húzással vagy kattintással választhatjuk ki a kívánt hátteret, betűtípust, színhatást, valamint adhatunk képet, szöveget, linket, ikont a munkánkhoz. Az oldal óriási előre feltöltött kép- és ikonadatbázissal dolgozik, így pillanatok alatt elkészülhet az infografika, de ha mégsem találunk olyat a vizuális elemek között, ami kifejezné a gondolatainkat, meglehetősen nagy tárhely áll a rendelkezésünkre, ahová feltölthetjük saját képeinket.

Végül a kész alkotást letölthetjük egyben, vagy blokkokban, ez utóbbinál, például egy projekttevékenység összefoglalásához nagyméretű posztereket is létrehozhatunk, nyomtathatunk.

Az infografika nagy segítség lehet az óratervezésben: ha a téma szerkezetét egy infografikán foglaljuk össze, amihez folyamatosan visszatérünk a magyarázat során, a diákokban jobban megmarad a vizuális rendszer segítségével az anyag. Fordítva pedig remek ellenőrzése lehet például a tudásnak és a megértésnek, ha azt kérjük, mutassák meg infografikán, mit tanultak. Sokat segíthet esztétikus rendszerezésekben is: vizuálisan jeleníthetünk meg vele bármilyen tananyagrészt, a szófajoktól, a mértékegységeken át az időjárás elemekig, vagy a történelmi eseményekig. (A leírás Babócsy Ildikó szabadulószoba ötlete nyomán készült).

1.1.2 Változatok szabadulószobára – tanári megoldások

A feladat megoldásaként elkészült szabadulószobák közül kiválasztottuk a legjobbakat. A megoldások mellett a tanárok és a diákok reflexióit is megismerhetik a következő anyagokból.

A munkák a Be@CyberPro projekt pilot tanárképzése keretében készültek az első modulfeladat megoldásaként. A játékok „oktatási, tanulási célra" forrásmegjelöléssel felhasználhatók és módosíthatók.

Fenyvesiné Jászai Lídia munkája

ALAPADATOK

Iskola: SZÁMALK-Szalézi Szakgimnázium

Csoportvezető: Fenyvesiné Jászai Lídia

Tanított szakma: Pedagógia és családsegítő munkatárs

Tanított tantárgy: Oktatástechnológiai alapok

Tanított szakma: Irodai titkár

Tanított tantárgy: Titkári ügyintézés, Adatkezelés gyakorlata, Levelezési gyakorlat

TERVEZÉS

Célcsoport: Pedagógia és családsegítő munkatárs 14. évfolyam

Tantárgy, amihez az óra kapcsolódik: Oktatástechnológiai alapok

VÁZLATOS ÓRATERV

Előkészületek:

- a feladatok elkészítése LearningApps-ben, Excel táblázatban keresztrejtvény, az offline feladatok kinyomtatása a megfelelő példányszámban – 4 csoport volt, mindent 4 példányban nyomtattam ki;
- QR-kódok generálása az online feladatokhoz, és a QR-kódok kinyomtatása;
- „hamis nyomok” összeállítása, kinyomtatása;
- megadott QR-kód kinyomtatása;
- a nyomok elrejtése a játék helyszínén a látható és a kereséssel megtalálható helyekre:
- asztal/székek alá, szekrény mellé, sötétítő függöny mögé, vetítő mögé,
- kerettörténet kinyomtatása, 4 példányban;
- wifi kapcsolat, okoseszköz biztosítása (csoportonként 1 eszköz) – biztosítva volt.

AZ ÓRA MENETE	MEGJEGYZÉSEK	SZÜKSÉGES ANYAGOK/ FORRÁSOK	IDŐ
Bejönnek a tanulók, elmondom, hogy mi lesz a feladat. Megtörténik a csapatokra osztás.		Elkészített anyagok, QR kódok kinyomtatva és elrejtve a teremben. Hamis eszközök elrejtve, okoseszközök, toll, papír, cellux, olló	5 perc
Elkezdik a feladatot.	Olvasnak, van, aki egyből értette és elkezd keresni. Van, aki olvas, van olyan csapat, aki felosztotta egymás között: valaki olvas, van, aki elindult megkeresni feladatot.	A padokon a kerettörténet ki van nyomtatva és egy segédanyag az internetbiztonsággal kapcsolatban, ami segít nekik.	5 perc
Feladatok keresése, megoldások leírása.	Közben folyamatosan bátorítani kell őket, hogy haladjanak a feladatokkal		35 perc
Megoldás: Az egyik csapat kitalálta a megoldást.	Segítség! Hogy olvassák el a megoldásokat többször, lássák mi a lényege. Mit, hol kell keresni?		Összesen: 45 perc
Vége	Adtam még 15 percet, hogy a többiek is kitalálják.		Vége: 60 perc

KINYOMTATOTT FELADAT

Tisztelt Jelentkezők!

A meghirdetett álláshoz szükséges tudásukat és rátermettségüket úgy bizonyíthatják, ha a megadott időn belül megtalálják azt a titkos, 10 jegyű számsort, amelyet elrejtettem a feladatokban. Figyeljenek minden nyomra, dolgozzanak megfontoltan, végül a helyszínen lévő asszisztensemnek (tanár) mondják meg a számot, és ő közli majd, hogy sikeres-e a megoldás. A játék során nagyon figyeljenek: ne árulják el a többi csoportnak, ha találtak valamit, vagy rájöttek valamire!

A DIGITÁLIS TARTALOM VÉDELME

1. A digitális tartalom biztonságos tárolása

Felsoroljuk, milyen lehetőségeink vannak az adataink tárolásához:

- Notebook számítógép
- Optikai lemezek (CD, DVD, BluRay, HD-DVD stb.)
- Flash memóriák (Pendrive-ok, SD-kártyák stb.)
- Mágneses merevlemezek
- Kemény burkolatú merevlemezek
- Távoli szerverek
- Felhőtárhelyek

Sokszor azonban nincs meg az a szokásunk, hogy az információkat több helyen is tartsuk, és nem ismerjük a visszaszerzés módját abban az esetben, ha elveszne. Mi tehát a legjobb adattárolási stratégia?

2. Az eszközökre vonatkozó adatok titkosítása, jelszavas védelem

A biztonság első szintjén számos lemez és flash tartalmaz egy kis szoftvert, amely lehetővé teszi a felhasználó számára, hogy titkosítsa a hardver tartalmát, és egy belső fájlkezelőn keresztül tegye hozzáférhetővé. Ezt a fájlkezelőt is megvédhetjük jelszóval. Könnyen megérthető, hogy milyen hasznos a titkosítás: ha a készülékünket ellopják, az információ nem érhető el mások számára. Ennek oka, hogy a fizikai információk elrendezkedése nem értelmezhető az operációs rendszernek, kivéve, ha az eszköz belső fájlkezelője azt korábban már dekódolta. Ennek ellenére az információink biztonsága nem függhet kizárólag ettől.

Látjuk, hogy vannak távoli szerverek és szabad hely a felhőben az információk tárolására. Ezeken a helyeken az adataink várakozhatnak, sőt titkosíthatjuk is őket, de felhasználásuk számos lépést igényel ahhoz, hogy információink biztonságban maradjanak. Először is elmagyarázzuk a különbséget a helyi tárolás és a felhőtárolás között.

3. A helyi tárolás és a felhőtárolás közötti különbség

Helyi tárolásról akkor beszélünk, amikor a hardvert, ahol az információinkat tároljuk, közvetlenül elérhetjük. Felhőtárolás akkor történik, amikor az adatainkat egy fizikai adathordozóra küldjük el úgy, hogy mi közvetlenül nem érhetjük el, de programok, alkalmazások vagy webes ügyfelek igen.

Tehát a felhő valójában jól szervezett (távoli merevlemezek, szerverek stb.) tárhelyek gyűjteménye, amelyet rajtunk kívülállók kezelnek. A felhasználó számára ez egy interneten keresztül elérhető virtuális tér, amelyben a dokumentumok és a számítógépes programok tárolódnak úgy, hogy az ugyanazon hálózathoz csatlakozó többi felhasználó is hozzájuk férhessen és használhassa azokat.

4. Mit jelent az összehangolás?

Az összehangolás azt jelenti, hogy a fájlok, amiket a helyi eszközeinkben formálunk, ugyanazokat az állapotokat és változatokat tartják fenn, mint amit a felhőtárolóban találunk. Az összehangolás előnyös, mert az adatok ugyan helyi szintűek (gyors hozzáférés, nincs késleltetés stb.), de felhőben történt biztonsági mentéssel. A felhőszolgáltatók rendszerint tele vannak olyan alkalmazásokkal, amik segítik adataink összehangolását.

Az összehangolásban részt vevő minden helyi környezetnek van egy applikációja – vagy asztali alkalmazása -, amely fenntartja ezt az állapotot a helyi és a felhőszintű fájlok között. Ezeket az alkalmazásokat telepíteni kell az operációs rendszerünkben az összehangolás érdekében. Mindazonáltal magunknak kell megvizsgálnunk, hogy a fájlok megfelelően összehangoltak-e, figyelve az ikonokat (nyilak, ellenőrzések stb.) a tálcán és azt, hogy az alkalmazás stabil állapotban van-e. Az olyan asztali alkalmazások, mint például a One Drive, a Google Drive vagy a Dropbox meg tudják mutatni nekünk ezeket a státuszokat. Csak ellenőriznünk kell az igénybe vett szolgáltatás ikonjait, és a rendszerünk legértékesebb fájljait a tálcán. Általánosságban elmondható, hogy a szolgáltatók nem biztosítják az adatok másolatát a felhőtárolókban, mert ezek általában fizetős szolgáltatások. Akkor lehetünk ebben biztosak, ha a központunk szerződést köt egy felhőtároló-szolgáltatóval.

5. A biztonsági mentés alapszabályai

A központoknak nemcsak biztonsági rendszerre van szükségük az adatok megőrzéséhez, hanem bizonyos módszerekre is arra az esetre, ha netán komoly adatvesztés történne.

Általánosságban véve 4 különböző típusú biztonsági mentés létezik:

- **Teljes biztonsági mentés:** ahogy azt a név is sugallja, az ilyen típusú biztonsági mentés teljes biztonsági másolatot készít az egység / meghajtó összes fájljáról. A biztonsági információ 100% -át lefedi, ami általában több időt igényel az elvégzéshez, és több helyet is foglal el. Ha biztosak akarunk lenni abban, hogy minden el van mentve, akkor ez a legjobb megoldás.
- **Differenciálmentés:** csak azokról a fájlokról készít másolatot, amik az utolsó mentés után készültek. Ezért csak új és/vagy módosított fájlokat tartalmaz.
- **Inkrementális mentés:** az utolsó teljes, differenciált vagy növekményes biztonsági mentés óta módosított összes fájl másolatát menti. A leggyorsabb módszer a biztonsági másolatok készítéséhez.
- **Tükörmentés:** hasonló a teljes biztonsági mentéshez. A különbség csak az, hogy a fájlokat nem tömörítik, és nem lehet jelszóval védeni. Ezért több helyet foglal el, és kevésbé biztonságos.

Csapattagok nevei:_____

FELADATLAP, ahová a megfejtéseket írhatjátok!

1.	
2.	
3.	
4.	
5.	
6.	

A játék helyes megfejtése (10 jegyű számsor): _____

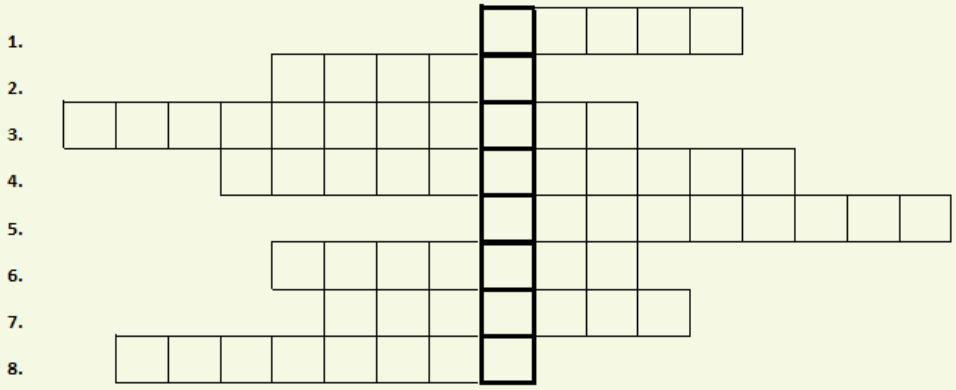
A 10. számjegyet ebből tudod kitalálni!

Végül hamis

Excelben elkészített keresztrejtvény:

Csapattagok nevei:

Ez a keresztrejtvény a harmadik megfejtést segíti!



1. Mi annak az internetes szolgáltatásnak az összefoglaló neve, amelyen képeinket, dokumentumainkat tárolhatjuk? Nem drive.
2. Ha több dokumentumod van a gépen, ezekben rendezed el.
3. Mi az előadás más szóval?
4. Milyen biztonságos felületre tudod feltölteni a képeidet?
5. Mi az adatkezelés fő célja?
6. Melyik a legismertebb operációs rendszer?
7. A pendrive mire alkalmas?
8. Hogyan nevezzük más néven a hordozható számítógépet?

MEGFEJTÉST ÍRD IDE:

DIGITÁLIS FORRÁSOK ÉS EGYÉB KELLÉKEK ELKÉSZÍTÉSE

Hogyan kapcsolódnak eszközök, az 1. modul tartalma az adott tantárgyhoz?

Az Oktatástechnológiai alapok tantárgyhoz, minden szempont szerint kapcsolódik az első modul tartalma, bármilyen anyagot készítünk az órán, fontos, hogy biztonságosan tudjunk hozzáférni és kezelni. Fontos, hogy csak azok láthassák, akikkel szeretnénk megosztani.

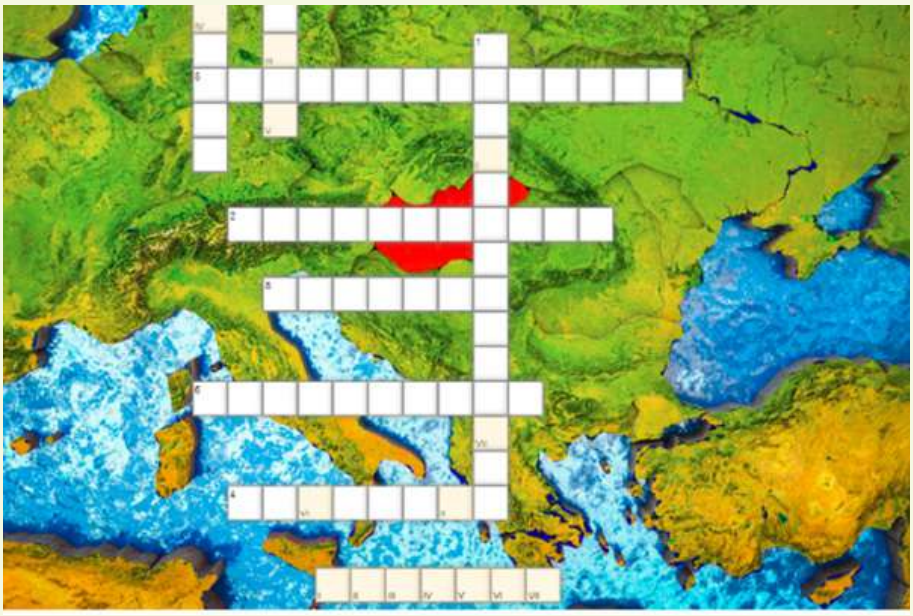
A kellékek bemutatása:

Az irodai titkár 14. évfolyammal gondolkodtunk közösen a feladatokon és velük pedig átbeszéltem a kerettörténetet és azt kértem, hogy feladatokat készítsenek. Így a LearningApps-el is megismerkedtek. Egy-két feladatot így betettem az órába, de azt még átszerkesztettem, sokat segítettek nekem is a gondolkodásban. Plusz voltak olyan kérdések, amit én nem úgy tettem volna fel, de benne hagytam, hiszen ugyanolyan fiatalokkal szeretném a feladatokat megoldani, mint akikkel készítettem. Kíváncsi voltam, hogy hasonló-e a gondolkodásuk. És a válasz: igen. Azokra a kérdésekre tudták a válaszokat. Például egy olyan kérdés volt, hogy „Mi az, amit a tenyerünkön hordozunk?” Telefon – tudták a választ. Nekem nem jutott volna eszembe, de ehhez a generációhoz úgy látszik, ez hozzátartozik.

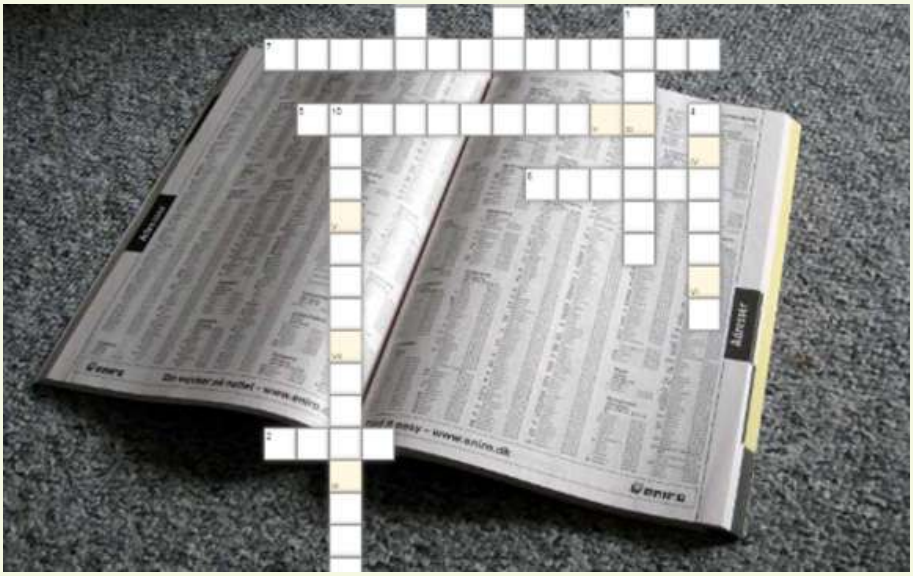
- **digitális eszközök esetén link**

Legyen ön is milliomos játék: Megoldás: Saferinternet
https://learningapps.org/9046945

Keresztrejtvény:
Megoldás: Hungary – külön egy Magyarországot kiemelő háttérképet is beletettem
https://learningapps.org/9045178



Keresztrejtvény:
Megoldás: Telefonszám – külön egy telefonkönyv háttérképet is beletettem
https://learningapps.org/9047016



Párosító játék: Sajnos ez egy hamis nyom
https://learningapps.org/9044975

- **egyéb eszközök esetén rövid leírás**

Táblázatkezelőben készült keresztrejtvény, amit már bemásoltam az óratervhez. Játék végén egy feladatlap, ahova írhatják a megoldásokat. Ezt is bemásoltam az óratervhez.

A JÁTÉK LEBONYOLÍTÁSA, TAPASZTALATOK ÖSSZEGZÉSE

Írjatok magáról a folyamatról. Hatékony volt a csoporton belüli együttműködés? Hogyan fogadták a tanulók?

Sikerült kiberbiztonsági tudatosságukat növelni?

Az egész folyamatot végig figyeltem, folyamatosan jelen kellett lenni, nem csak testben, hanem lélekben is, hiszen segíteni is kellett őket. Azt vettem észre, hogy először azt sem tudták, hogy hirtelen hová csöppentek. Nagyon sok mindent kellett előkészítenem. Örültem, hogy előtte a teremben nem voltak, így el tudtam helyezni mindent, anélkül, hogy bármilyen tudomást szereztek volna, hogy én ott voltam előtte a teremben.

Volt olyan csapat, aki nagyon ügyesen egyből felfogta a játékot és neki is látott, ahol értetlenség volt, odamentem és mondtam, hogy induljanak és keressenek, hisz ez egy kiszabaduló szoba.

A papírokat ügyesen megtalálták, viszont volt egy csapat, aki visszarejtette a feladatokat. Bár belegondolva, lehet, hogy úgy is jó lett volna a feladat, hogy mindegyikből csak egyet nyomtatok ki, és ha valaki végez a megfejtéssel, akkor visszateszi a feladatokat, de nekem ez a megoldás túl hosszúnak tűnt.

Én mindegyik feladatból kinyomtattam annyit, ahány csapatot gondoltam a feladatra. Viszont, ahogy kinyomtattam különböző jelöléseket tettem rá, hogy legalább azzal segítsem őket, hogy ne ugyanazt a feladatot kezdjék el újra elkészíteni. Például a lapok tetejére háromszög, kör, négyzet alakokat rajzoltam, így tudták, hogy hány feladatot kell elkészíteni, és mennyivel vannak már meg.

Élvezték a játékot. A végén, úgy találta ki a csapat a feladatot, hogy nem 9 hamis hír volt, hanem a 2019-ből a kilences számot vették ki, és így lett meg.

Sokan az utolsó feladatot nem tudták hova tenni és jól értelmezni, így az nehezítette meg a megoldást.

Volt olyan csapat is, akinek nem jutott eszébe, hogy a Facebookon keressen rá az adatokra. Mondtam 45 perc letelte után, hogy olvassátok el a megfejtéseket, többször is, és a kerettörténetet is még egyszer.

A végén mindenkinek tetszett, csak azt sajnálták, hogy az utolsó számjegyre nem jöttek rá, mert az nehéz volt, de mondogattam nekik, hogy hamis-hamis. Az utolsó hamis hír lehetne egy kicsit könnyebb ezt mondták, vagy több rávezetés benne.

A kiberbiztonsági tudatosságot is sikerült növelnem bennük az óra eleji segédanyaggal, és a kérdések is ezzel kapcsolatosak voltak, de következő órán ismételten felelevenítem bennük.

Feltételezzük, hogy nem mindenki informatika tantárgyhoz kapcsolta a módszert. Milyen speciális hozadéka volt az adott tantárgy szempontjából? Voltak nehézségek? Mit tanultatok közben? Megérte-e a befektetés? Fogjátok-e alkalmazni a későbbiekben ezt a módszert? Osszatok meg minden olyan tapasztalatot, amit fontosnak éreztek!

Szerintem a mai világban az internetbiztonság nagyon fontos és hasznos tudás a fiataloknak, sőt nekünk is, hisz bővíthetjük tudásunkat mi is.

A diákoknak nagyon tetszett ez a szabadulószoba. Más osztálynál is fogom alkalmazni. Megérte a fáradozást és a tanulók is értékelték. Mondták, hogy biztos sok munka lehetett vele. De az óra után én is jól éreztem magam, én is izgultam értük, hogy ki szabadulnak-e. És sikerült.

Holnap lesz az internetbiztonság nemzetközi napja, több órámra is be szeretném vinni a témát, ezeken a feladatokon keresztül, amit készítettem.

Pappné Szabó Alexandra munkája

ALAPADATOK

Iskola: Soproni Szakképzési Centrum Hunyadi János Középiskolája, Csorna

Csoportvezető: Pappné Szabó Alexandra

Tantárgy: magyar nyelv és irodalom, pszichológia, ügyfélszolgálati kommunikáció

Csoporttagok:

- A 10. évfolyam 19 fővel
- Egy 12. évfolyamos tanuló ügyviteli szakgimnázium szakirányon

TERVEZÉS

Célcsoport: 10. B osztály

Tantárgy, amihez az óra kapcsolódik: osztályfőnöki óra keretében zajlott a digitális szabadulószoba játék, ami számos olyan kompetencia fejlesztésére is szolgál, amelyek elengedhetetlenek az ügyvitel tagozathoz, illetve a mindennapos iskolai munkához, pl. együttműködés, közös gondolkodás, empátia, odafigyelés másokra, IKT-eszközök használata.

A tervezéshez hozzátartozik az is, hogy a tanulókkal évente többször beszélgetünk a kiberbiztonságról, előadásokon is részt vettek már hasonló témában.

A szabadulószobával kapcsolatban az előző órán elmondtam, hogy egy csoportfeladat vár rájuk, és hozzák magukkal a terembe az okostelefonjukat is.

Az óra megkezdése előtti teendők: a keresztrejtvény, a puzzle, és az egyes feladatokhoz tartozó QR-kódok kinyomtatása és elhelyezése az aulában és az osztályteremben.

A nyomokat a következő helyekre tettem:

1. tanári asztal fiókja;
2. az aulában található nagy virág cserepe;
3. a tanári szék háttámlájára ragasztva;
4. az aula faliújságjára kitűzve;
5. a könyvesszekrény oldalára ragasztva;
6. a lift melletti falra ragasztva;
7. az interaktív tábla vetítőjére akasztva.

VÁZLATOS ÓRATERV:

Időkeret	Tevékenységek	Eszközök
1-5. perc	▪ a játék menetének ismertetése, ▪ 4 csoport alakítása ▪ az értékelőlapok, tabletek átadása ▪ a tanterem átrendezése a munkához	▪ tabletek, ▪ okostelefonok, ▪ QR-kód olvasó applikáció, ▪ kinyomtatott értékelőlapok, ▪ kinyomtatott kerettörténet minden csoport számára ▪ íróeszköz ▪ wifi kapcsolat
6-40. perc	a csoportok önállóan dolgoznak, a tanár is jelen van, és szükség esetén segít, válaszol a kérdésekre	▪ kinyomtatott QR-kódok és keresztrejtvény borítékban elhelyezve a teremben és az aulában, ▪ okostelefonok, tabletek
41-45. perc	A tanóra végén közös megbeszélés, a tapasztalatok, nehézségek megosztása egymással. A győztes csapat kihirdetése.	

A csoportvezető tanár tervezi meg a munkát. Egy végzős tanuló segít: elkészíti azt az értékelőlapot, amin az egyes csoportok jelölhetik, rögzíthetik a megoldásokat, és végül a teljes megfejtést. Az ehhez felhasznált internetes oldal: ***popplet.com***

DIGITÁLIS FORRÁSOK ÉS EGYÉB KELLÉKEK ELKÉSZÍTÉSE

A kellékek bemutatása

Digitális eszközök esetén link:

- ***http://popplet.com/***
- ***https://learningapps.org/watch?v=pivopp9p520***
- ***https://learningapps.org/watch?v=pt1tmng8c20***
- ***https://learningapps.org/watch?v=pzujjgn7t20***
- ***www.piktochart.com***

Egyéb eszközök esetén rövid leírás: *a tanár saját készítésű keresztrejtvénye*

A JÁTÉK LEBONYOLÍTÁSA, TAPASZTALATOK ÖSSZEGZÉSE

Az osztály 19 főből áll, köztük 4 SNI-s és 3 tartósan beteg tanulóval. Osztályfőnökként minden alkalmat megragadok a közösséghez tartozás és az empátia, mások elfogadásának erősítésére. A digitális tanulószoba – már a munka megkezdése előtt is – jó lehetőségnek tűnt ehhez.

4 csoportot alakítottunk a tanulók szabad társválasztása alapján. Röviden ismertettem a feladatot, és minden csoport megkapta a kerettörténetet és az értékelőlapot kinyomtatva. Minden csoport kapott egyet az iskola táblagépei közül, és saját mobiltelefonjukat is használhatták. Kértem, hogy adjanak nevet a csoportnak.

Ezt követően elmondtam, hogy az osztályteremben és az aulában nyomokat rejtettem el, amelyek megtalálása és felhasználása után eljuthatnak a végső megfejtéshez: egy telefonszámhoz.

A feladatok tetszőleges sorrendben oldhatók meg, és ügyeljenek arra, hogy ha megtaláltak egy nyomot, akkor csak egy borítékot vegyenek el a helyszínről.

Tájékoztattam a tanulókat arról is, hogy egy tanóra áll a rendelkezésükre, és az a csapat nyeri a versenyt, szabadul ki a szobából, amelyik a legrövidebb idő alatt szolgáltatja a helyes megfejtést.

A játék kezdetén kicsi tanácstalanságot figyeltem meg két csoportnál is, aztán a lelkesedés vitte őket előre. Hamar kialakult a munkamegosztás a csapatoknál: ki az, aki leolvassa a QR-kódot, ki lesz a feladatmegoldó (ez változott a játék során, mert volt, aki a puzzle-ban volt ügyes, mások inkább a tankockás feladatokban), és ki írja majd be a megoldásokat az értékelőlap megfelelő helyére. Előfordult egy-egy hangosabb vita, de alapjában véve sikeresnek tartom a munkát.

Számomra is érdekes élmény volt látni az osztályomat ebben az új helyzetben. A csapatok az ismertetés után azonnal szétszéledtek az aulában és a teremben, és csak egyszer volt „feltorlódás” a borítékok keresésében.

Az iskolavezetést a tanóra előtt tájékoztattam arról, hogy milyen munkát terveztem aznapra, és ha esetleg szokatlan zajszint vagy mozgolódás figyelhető meg, akkor ennek az lesz az oka. Igazgatónőnek tetszett az ötlet, és azóta már a tapasztalataimról is beszélgettünk. Ő történelmet tanít, és érdeklődve hallgatta a beszámolómat, amit pénteken a félévzáró értekezleten is megtettem a kollégák előtt.

KERETTÖRTÉNET

Kiberbiztonsági nyomozósegédi állásra szeretnétek jelentkezni, és éppen megérkeztek az állásinterjú helyszínére. A teremben nincs senki, csupán az alábbi üzenet:

Tisztelt Jelentkezők!

A meghirdetett álláshoz szükséges tudásukat és rátermettségüket úgy bizonyíthatják, ha a megadott időn belül megtalálják azt a titkos, 10 jegyű számsort, amelyet elrejtettem a feladatokban. Figyeljenek minden nyomra, dolgozzanak megfontoltan, végül a helyszínen lévő asszisztensemnek (tanár) mondják meg a számot, és ő közli majd, hogy sikeres-e a megoldás. A játék során nagyon figyeljenek: ne árulják el a többi csoportnak, ha találtak valamit, vagy rájöttek valamire!

Az osztály meglepődve fogadta, amikor elmondtam, hogy kiberbiztonsági szabadulószobát terveztem számukra, de a többségük lelkesen fogott hozzá a munkához.

Egyes feladattípusokkal már találkoztak az általam tartott tanórákon, pl. keresztrejtvény, tankocka – ezek ismerősek voltak számukra. QR-kódokat azonban eddig még én magam sem használtam a pedagógiai munkámban.

Az előkészület, a feladatok elgondolása nálam azzal kezdődött, hogy úgy éreztem, nem fogom tudni elkészíteni a feladatot. Aztán, ahogy többször átolvastam a kapott segédanyagot, megnéztem az internetes oldalakat, kipróbáltam azokat, valahogy már kicsit jobban bíztam magamban.

Tudom, hogy nem lett tökéletes, de ez az első szabadulószobám! És abban biztos vagyok, hogy nem az utolsó. Már gondolkodom azon, hogy pl. diáknapon az iskola egyes osztályai számára lehetne hasonlót, több feladattal, nagyobb időkerettel és több helyszínnel létrehozni.

Az akasztófa-játékot két csoport is többször elkezdte, mire sikerült kirakniuk.

A tanulók többségének az álhírek kiválasztása okozott nehézséget. Gyakran úgy gondolják, hogy amit az interneten olvasnak, látnak, az csak valódi és igaz lehet.

Magyar nyelv és irodalomórákon is sokszor igyekszem tudatosítani bennük a kritikus gondolkodás fontosságát és a hiteles források használatát. Ha csak annyiban járult hozzá a szabadulószoba a kiberbiztonsági tudatosságukhoz, hogy ne fogadjanak el bármely oldalon megjelenő információt, hanem nézzenek utána a forrásoknak, akkor egy lépést tettünk előre a tudatosabb internethasználat felé. A végső megfejtéshez szükséges Facebook-oldalról még a következő napon is beszélgettünk.

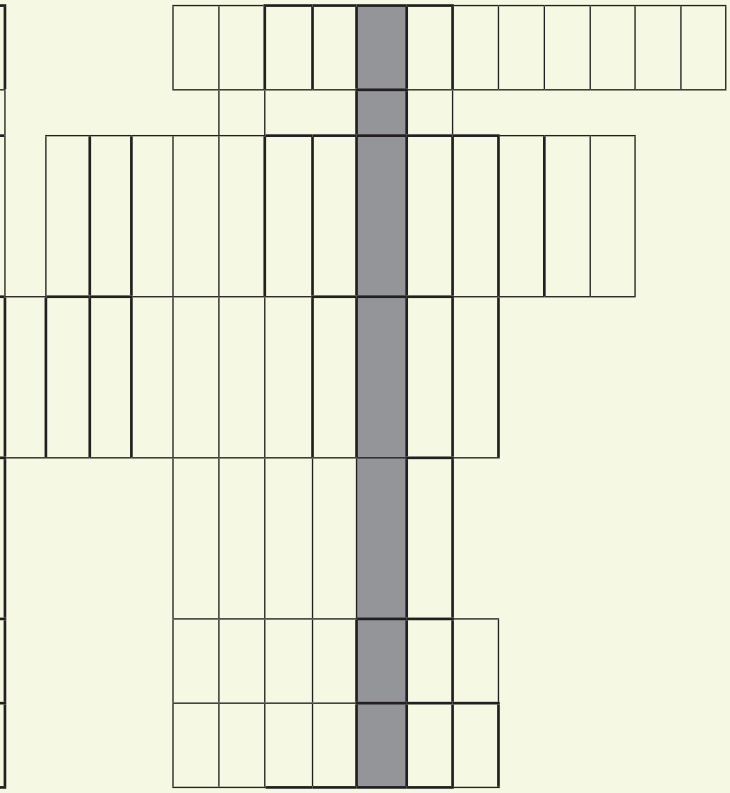
FELADATOK

1. A feladat megoldásával eljuthattok a megfejtés 1. szavához

Az első feladat egy tankocka volt, melynek során képeket kellett összepárosítaniuk, és ha ez sikerült, megkapták az első szót a megfejtésből: Safeinternet.

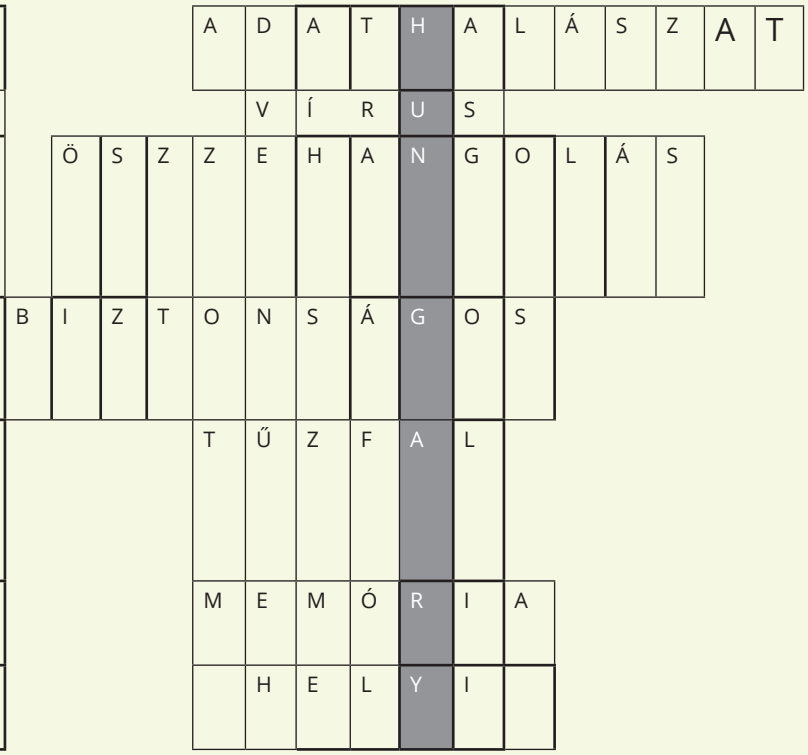
2. A keresztrejtvény fősorából megtudhatjátok a megfejtés 2. szavát

1	A szélhámosok gyakran hamis emailt használva próbálkoznak ezzel.
2	Van belőle trójai és féreg is!
3	A fájlok, melyeket a helyi eszközeinken formálunk, ugyanazokat az állapotokat és változatokat tartják fenn, mint amit a felhőben találunk.
4	Akkor ilyen a jelszavunk, ha tartalmaz számokat, nagy- és kisbetűket vegyesen és speciális karaktereket is.
5	Olyan rendszer, ami lehetővé teszi számunkra, hogy megvédjük a készülékünket az internetről származó veszélyekkel szemben.
6	Az ember fejében és a számítógép alaplapján is van!
7	Ilyen tárolásról van szó, ha a hardvert közvetlenül elérhetjük.



A keresztrejtvény fősorából megtudhatjátok a megfejtés 2. szavát *(megoldás)*

1	A szélhámosok gyakran hamis emailt használva próbálkoznak ezzel.
2	Van belőle trójai és féreg is!
3	A fájlok, melyeket a helyi eszközeinken formálunk, ugyanazokat az állapotokat és változatokat tartják fenn, mint amit a felhőben találunk.
4	Akkor ilyen a jelszavunk, ha tartalmaz számokat, nagy- és kisbetűket vegyesen és speciális karaktereket is.
5	Olyan rendszer, ami lehetővé teszi számunkra, hogy megvédjük a készülékünket az internetről származó veszélyekkel szemben.
6	Az ember fejében és a számítógép alaplapján is van!
7	Ilyen tárolásról van szó, ha a hardvert közvetlenül elérhetjük.



3. Ez a feladat segít a megfejtés 3. szavának megtalálásában

Ebben a feladatban a learningapps.org oldalon kellett egy sorbarendezést elvégezni. Egy mondat kifejezéseit összekevertem, és ha a helyes sorrendet kialakították, akkor megkapták a megfejtést: azt a fogalmat, amit meghatároz a definíció: Facebook.

A mondat: Ez az online közösségi felület segít a kapcsolattartásban és élményeink megosztásában.

4. A megfejtés 4. szava

A megfejtés negyedik szavához úgy juthattak a tanulók, ha egy akasztófa-játékban sikerült kirakniuk a telefonszám kifejezést.

5. Sajnos, ez egy hamis nyom!

A borítékban találtak egy puzzle-t, amelyből egy cica képét – azzal a felirattal, hogy Sajnos ez egy hamis nyom! – rakhatták ki. Ezt a feladatot mindegyik csoport nagyon gyorsan megoldotta.

6. Sajnos ez hamis nyom!

A második hamis nyomot a www.piktochart.com oldalon készítettem el.

7. Az álhírek száma adja a telefonszám utolsó számjegyét

Végül hamis

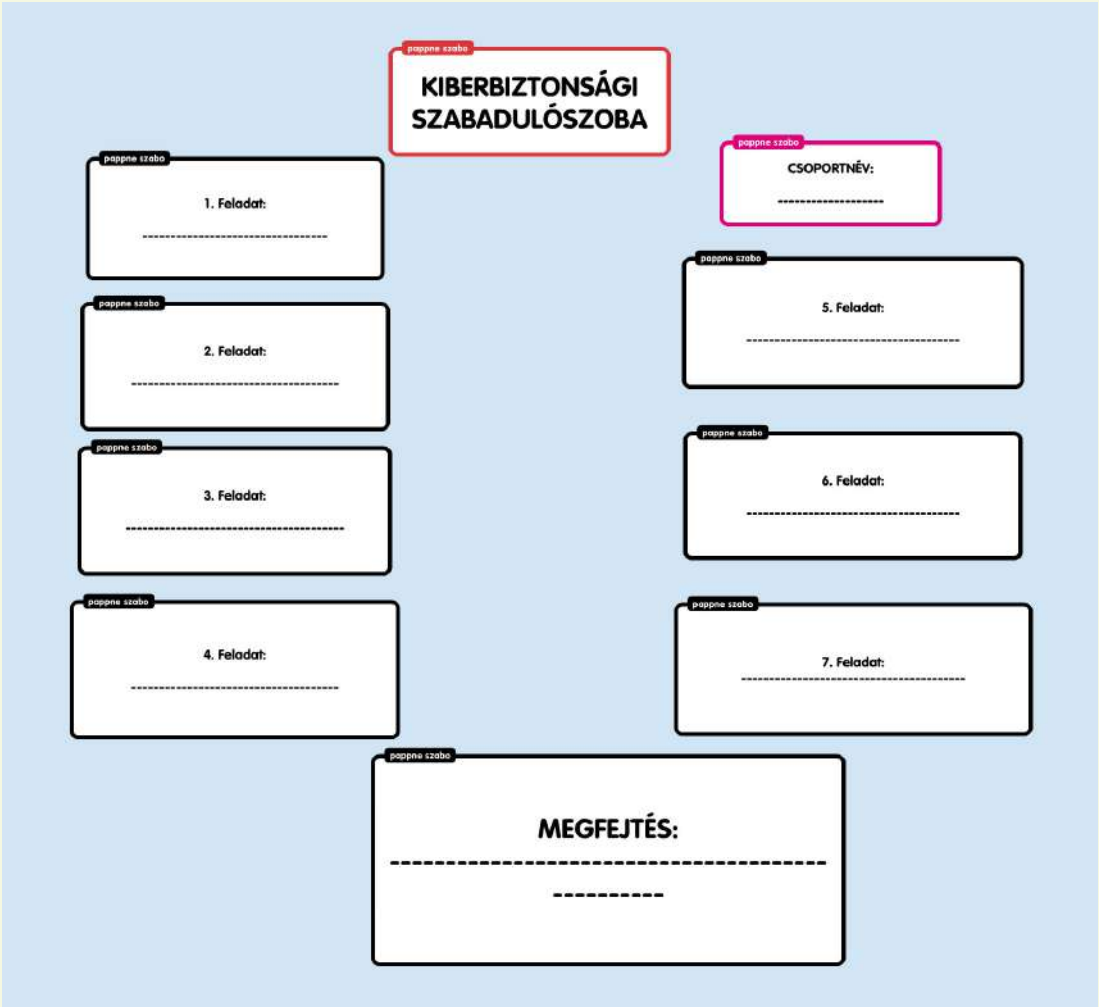
A végső megfejtéshez szükséges telefonszámot a Facebook-oldalon egy csoport kicsit nehezen találta meg, de végül mindegyik csapatnak sikerült.

A tanóra játékra szánt idejét kihasználtuk: a leghamarabb végző csapat már 27 perc alatt, a legkésőbb végző pedig 35 perc alatt fejezte be a munkát, és mutatták be az értékelőlapot.

A lezárásra elég volt a hátralévő idő, de a részletes megbeszélésre a következő irodalomórán került sor.

A későbbiekben gondolkodom azon, hogy ha valamelyik csapat lényegesen korábban végez, akkor számukra valamilyen egyéb feladatot, tevékenységet találjak ki, hogy ne legyen üresjárat, és a többiek ne érezzék a sürgetettséget.

ÉRTÉKELŐLAP



Teleki József munkája

A továbbképzésben résztvevő kollégáknak nem volt kötelező az általunk felkínált minta alapján elkészíteniük a szabadulószobát, előállhattak saját ötlettel is. Teleki József munkája erre a megoldásra egy kiemelkedően kreatív példa.

ALAPADATOK

Iskola: Szolnoki Szakképzési Centrum Ruhaipari Középiskolája és Általános Iskolája

Csoportvezető: Teleki József

Csoporttagok: 9. K osztály − 20 fő (5X4 fős csapatokban)

TERVEZÉS

Célcsoport: Szakgimnázium 9. évfolyamos diákjai

Tantárgy: INFORMATIKA

VÁZLATOS ÓRATERV

A játék helyszíne egy előre berendezett tanterem. A játékot 3-4 fős csapatok játszhatják. A játékidő: 40 perc. A tanulóknak egy virtuális széfet kell kinyitniuk. A páncélszekrényt nyitó számkombináció megszerzéséhez QR-kódot kell megkeresniük a tanteremben. Mindegyik QR-kód egy feladatot rejt, amit helyesen megoldva hozzájutnak a számkombináció egyik eleméhez. A feladatokat tetszőleges sorrendben oldhatják meg, de a széf csak a megfelelő sorrendben beírt számsor esetén nyílik. Ha a diákok bemutatják a mobiltelefonjukon a kinyitott széfet, akkor a csapat minden tagja kap egy Riszi Bankót, melyet a tanév során beválthatnak, és így egyszer mentesülhetnek a dolgozatírás, vagy felelés alól.

A kerettörténet

A messzi-messzi időben a középiskolánkat alapító lázadó diákok, az ős Jedi lovagok tudását felhasználva megalkották a varázserővel bíró Riszi Bankót. A jedihagyományok szerint, amelyik osztály birtokolja a Riszi Bankót, annak nem kell dolgozatot írni, nem kell felelnie egy álló hétig.

A bankót azonban a Sötét oldal tanárai, élükön a gonosz informatikatanárral ellopták, és egy széfbe zárták. A ti feladatotok megkeresni az öt elrejtett QR-kódot a tantermen belül! Ha jól dolgoztok, és megoldjátok a feladatokat, megtudjátok azt a hatjegyű számsort, amivel ki lehet nyitni a Riszi Bankót rejtő virtuális páncélszekrényt.

A kód legyen veletek!

Szükséges eszközök:

- mobiltelefon QR-kód olvasóval;
- internet hozzáférés;
- Riszi Bankó kinyomtatva annyi példányban ahány fős az osztály;
- papír, ceruza a kódolási feladatok megoldásához;
- kinyomtatott QR-kódok a tanteremben elrejtve, illetve a befejező QR-kód a tanterem ajtaján kiragasztva.

A feladatok és megfejtéseik:

Jelszó (kvíz):

Melyik a legbiztonságosabb jelszó?

a) Kiscica123

b) 2010januar2

c) 987654321

d) AxRz+z4L=61 (helyes válasz)

Kinek mondhatod el a jelszavad?

a) Legjobb barátodnak

b) Tanárodnak

c) Senkinek (helyes válasz)

d) Szomszéd öreg néninek

Mikor kell módosítani a jelszavad?

a) Az alapértelmezett jelszót az első bejelentkezéskor (helyes válasz)

b) Rendszeresen, de évente célszerű (helyes válasz)

c) Erős jelszót sohasem kell módosítani

d) Csak akkor, ha feltörték

Jelöld az IGAZ állításokat!

a) Ne mentsd a jelszavad a böngészőben! (helyes válasz)

b) Jó minden alkalmazásban ugyanazt a jelszót használod, mert így nem felejted el.

c) Ne használj jelszó-emlékeztetőt! (helyes válasz)

d) Legyen rád jellemző a jelszó!

Melyik a legbiztonságosabb megoldás mobiloknál a jelszó helyett?

a) Semmi. Csak a jelszó a jó megoldás.

b) Arcfelismerés (helyes válasz)

c) Ujjlenyomat (helyes válasz)

d) Mintázat

Rosszindulatú programok (párosító)

Vírus	Rosszindulatú kód, mai akkor fertőz, ha futtatják.
Féreg	Emberi beavatkozás nélkül sokszorozódik, kihasználva a biztonsági réseket. Lelassítja a gépet.
Trójai programok	Legális szoftvernek álcázott programmal települ a gépre és utat nyit a támadónak.
Zsarolóprogramok	Blokkolják a számítógéphez való hozzáférést addig, amíg váltságdíjat nem fizetnek. Általában féregként vagy trójai programként terjednek.
Kémprogram (rootkit)	Az operációs rendszert módosító szoftver, amely „hátsó ajtót” nyit a támadónak.
Spam	Az interneten küldött kéretlen üzenetek, amelyek reklámozás, adathalászat, rosszindulatú programok terjesztése stb. céljából készülnek.
Adathalászat (phishing)	Legálisnak álcázott csaló email
Kémprogramok (spyware)	Internetes böngészéskor települő program, mely a felhasználó adatait lopja el.

Kétszintű hitelesítés (titkosírás):

A többtényezős hitelesítés azt jelenti, hogy egy felhasználó csak akkor kaphat hozzáférést bizonyos személyes adatokhoz, dokumentumokhoz, tartalmakhoz, ha többféle bizonyítékkal igazolja személyazonosságát. Az első lépésben általában jelszót, a másodikban egy email-ben vagy SMS-ben küldött kulcsot kell megadni. Hogy mely általad is ismert szolgáltatásnál élhetsz vele, megtudod, ha a képen látható kódkerék segítségével megfejted a titkosírást: IDFHERRNCJRRJOH!

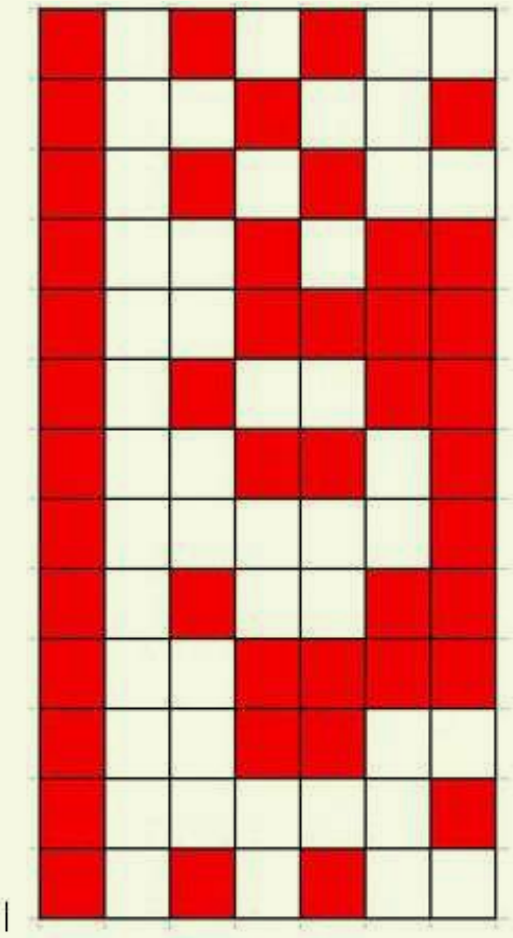
Megfejtés: Facebook Google (szóközzel a kettő között)

Védekezés a spam ellen (kódfejtő):

Az ábra egy szót rejt, melyet a betűk megtalálásával tudtok megfejteni. Minden sor egy betűt rejt. A megfejtés egy tipp ahhoz, hogy mit csinálj, ha több olyan embernek küldesz emailt, akik nem ismerik egymást!

ASCII BINARY ALPHABET

A	1000001	N	1001110
B	1000010	O	1001111
C	1000011	P	1010000
D	1000100	Q	1010001
E	1000101	R	1010010
F	1000110	S	1010011
G	1000111	T	1010100
H	1001000	U	1010101
I	1001001	V	1010110
J	1001010	W	1010111
K	1001011	X	1010111
L	1001100	Y	1011001
M	1001101	Z	1011010



Megfejtés: titkos másolat

Adathalászat (kódolvasó):

Az adathalászat tipikus módszere van elrejtve ebben a szótáblában. Hogy megtaláld a leírást kövesd a kódot!

A lépéseket kötőjelek választják el, minden lépés a következő betűhöz vezet. Indulj a @-tól!

F1J1-L1J1-L2B1-L2J1-L3B1-J3F1-F7-B1L6-J2-F4-B2-L1J1-L7-B2L1-J1F2-L4

(F=fel, L=le, B=balra, J=jobbra)

D	M	T	P	E	F
@	O	E	Z	T	K
F	R	W	Ő	N	T
G	G	X	C	E	J
H	Ő	W	E	K	H
J	A	T	R	L	G
K	J	Q	S	É	Z
T	K	Í	T	V	F
Z	É	Y	Z	Á	D
U	L	X	I	Ű	S
I	É	V	U	M	A
O	M	A	I	Ú	Y
P	N	T	P	Ő	X
Ő	B	B	L	V	C

Megfejtés: megtévesztő email

A virtuális széfet nyitó kombináció: 94718

A Riszi Bankó	Ezt kapják meg a feladatot sikeresen teljesítő, a virtuális széfet kinyitó diákok. (Természetesen nagyobb, bankó méretben)	
Jelszó	Öt kérdésből álló kvíz feladat a biztonságos jelszavakkal kapcsolatosan. A játékos addig nem mehet tovább a következő kérdésre, amíg meg nem találja a helyes választ. Helyes megoldás esetén a csapat hozzájut a páncélszekrényt nyitó számkombináció első számjegyéhez, amely a 9.	
Rosszindulatú programok	A rosszindulatú programok típusait és a jellemzőiket kell párosítania a diákoknak. Helyes megoldás esetén a csapat hozzájut a páncélszekrényt nyitó számkombináció második számjegyéhez, amely a 4.	
Kétszintű hitelesítés	A diákoknak kódkerék segítségével kell megfejteniük egy titkosírást, mely elárulja milyen általuk kedvelt szolgáltatásoknál élhetnek a kétszintű hitelesítéssel. Helyes megoldás esetén a csapat hozzájut a páncélszekrényt nyitó számkombináció harmadik számjegyéhez, amely a 7.	
Védekezés a spam ellen	A tanulók egy tippet kapnak, hogyan küldjenek emailt egyszerre több embernek, akik nem ismerik egymást. A megoldás ASCII kóddal megalkotott színkódot kel dekódolniuk. Helyes megoldás esetén a csapat hozzájut a páncélszekrényt nyitó számkombináció negyedik számjegyéhez, amely a 1.	

Adathalászat	A diákoknak egy betűtáblában kell lépkedniük egy kódot követve. Minden lépéssel egy betűhöz jutnak, melyet összeolvasva egy adathalász módszert ismernek meg. Helyes megoldás esetén a csapat hozzájut a páncélszekrényt nyitó számkombináció ötödik számjegyéhez, amely a 8.	
Széf	Itt kell beírni a megfejtett számkombinációt. Ez a QR-kód nincs elrejtve. A virtuális széfet nyitó kombináció: 94718.	
A kinyitott széf	***https://dbimg.eu/i/m8qyvnj9bv.jpg***	

A JÁTÉK LEBONYOLÍTÁSA, TAPASZTALATOK ÖSSZEGZÉSE

Iskolánkban minden szeptember egy „beszoktató” héttel kezdődik, amelyen a 9. osztályos diákok játékos feladatok segítségével ismerkednek az iskolával és egymással. Erre az alkalomra készült az a játék, melynek alapját felhasználtam ehhez a szabadulószobához is. Bár most csak egy osztállyal próbáltam ki a játékot, ám ezúttal is nagy sikert aratott.

A felelést vagy dolgozatot egy alkalommal kiváltó kupon (Riszi Bankó) ezúttal is jó motivációnak bizonyult, a játékosítás pedig a máskor kevésbé aktív tanulókra is kedvezően hatott.

A csapatok többféle technikával próbáltak kijutni a teremből. Voltak, akik együtt dolgoztak, közösen próbálták megoldani a feladatokat. Az újabb QR-kódot pedig azután keresték, ha megszerezték a széfet nyitó kombináció egyik elemét. Mások inkább specializálódtak, voltak kódkeresők és kódfejtők. De egy csapat minden tagja külön-külön próbált megbirkózni egy-egy feladvánnyal, és az így megszerzett számokat tették a „közösbe”.

A tapasztalatok szerint a legtöbb időt a kódolásos feladatok vették el a csapatoktól. A színekre fordított ASCII-kódtábla használata, pontosabban a feladat értelmezése több csapatnál igényelt egy kis segítséget.

Összességében azonban sikeres volt a szabadulószoba, mely hozzájárult a diákok digitális tartalmak védelmével kapcsolatos ismereteinek bővítéséhez.

1.2 Kutatás a diákok körében

A második modul végén egy kutatási feladatot kaptak a tanárok. ***„A közösségi hálón való aktivitás, tudatos médiahasználat és felelős viselkedés a digitális világban”*** témakörben kellett felmérést végezni saját iskolájukban és a kapott eredményeket elemezni.

1.2.1 Feladatleírás

Végezzetek egy **kutatást** a saját tanulóitok körében „A közösségi hálón való aktivitásuk, tudatos médiahasználatuk és felelős viselkedésük a digitális világban” témakörben.

A kutatás célja, hogy kiderüljön, mi az, ami jelenleg a diákok számára a legnagyobb veszélyt jelenti a digitális „úton”, és hogyan kellene segítenünk őket abban, hogy tudatossá váljon az online tevékenységük.

Az egységes megoldás érdekében készítettünk egy online kérdőívet, amit itt találtok meg: ***http://bit.ly/2OaIN71***

Részfeladatok:

Adjatok egy egyedi kódot diákjaitoknak, és kérjétek meg őket (legalább egy osztályt), **hogy töltsék ki a kérdőívet**. A kitöltés névtelen, a kódra azért van szükség, hogy le tudjuk szűrni mindenkinek a saját diákjai által kitöltött adatokat. (A felmérés lezárása után mindenki megkapja a saját diákjai által kitöltött adatokat).

Összesítsétek és elemezzétek az eredmény, készítsetek néhány grafikont!

Fogalmazzatok meg néhány következtetést a 2. modul tartalmával összhangban: Menynyire vannak tisztában a diákok az internet és a digitális jelenlét veszélyeivel? Melyek azok a témakörök, amit célszerű velük az órákon megbeszélni?

1.2.2 A kutatás összesített eredménye

A pedagógusok által készített felmérések eredményét az alábbiakban – összesített formában – osztjuk meg, idézve a pedagógus kollégák elemző munkáiból.

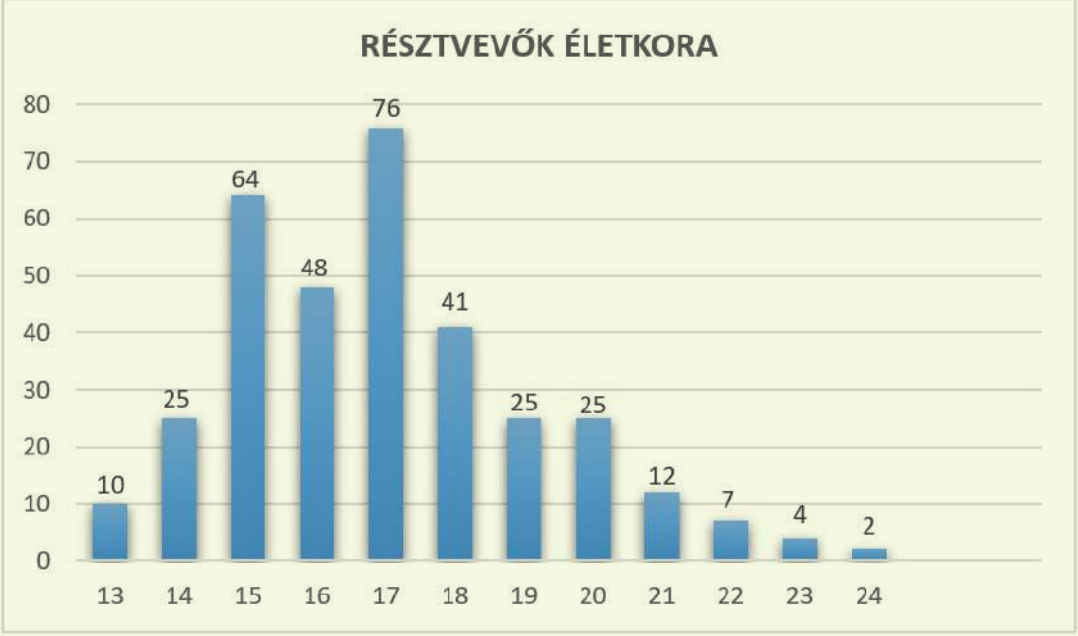
Diákok a „digitális biztonságról"

A kutatás célja az volt, hogy feltárjuk, mi az, ami jelenleg a diákok számára a legnagyobb veszélyt jelenti a digitális „úton", és hogyan kellene segítenünk őket abban, hogy tudatossá váljon az online tevékenységük.

A kurzusban résztvevő aktív tanárok a kapott eredményeket összesítették és elemezték, továbbá megfogalmaztak néhány következtetést is. Elsősorban az alábbi kérdésekre koncentráltak:

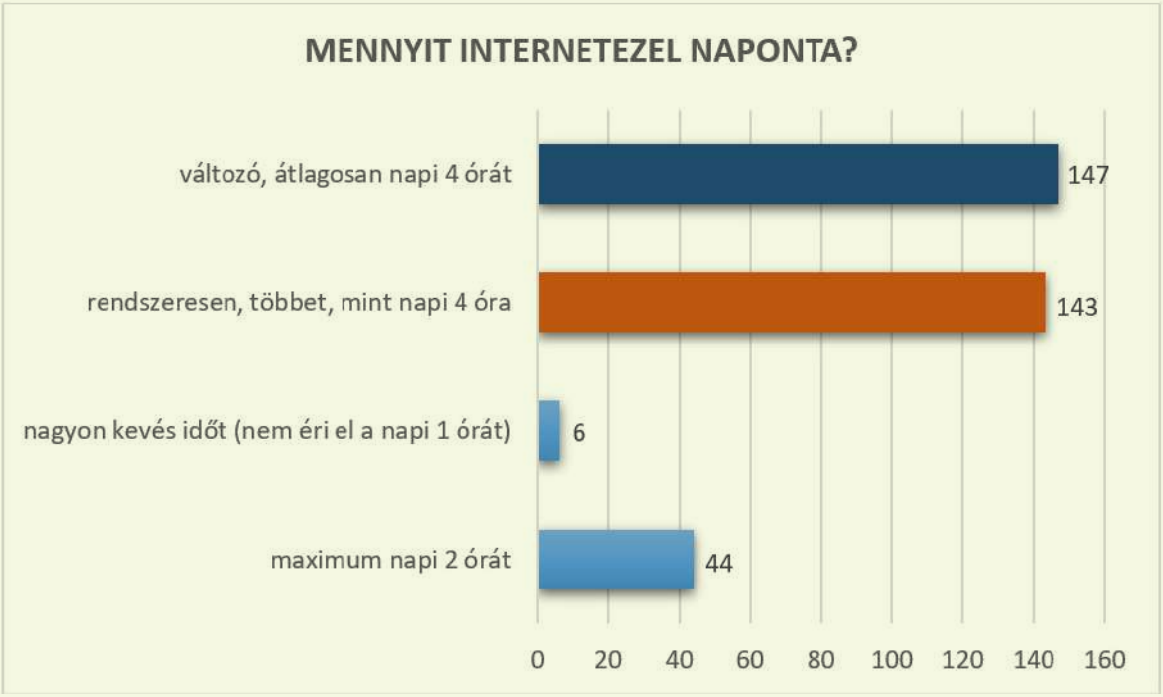
- Mennyire vannak tisztában a diákok az internet és a digitális jelenlét veszélyeivel?
- Melyek azok a témakörök, amiket célszerű a diákokkal megtanítani, megbeszélni?

Az elemzésben a tényadatok mellett a pedagógusok munkáiból idézünk (melyek egy-egy iskolában végzett felmérés tapasztalatait tükrözik) a fontosnak tartott információkból, melyek kiegészítik és megerősítik az összegzett eredményeket.

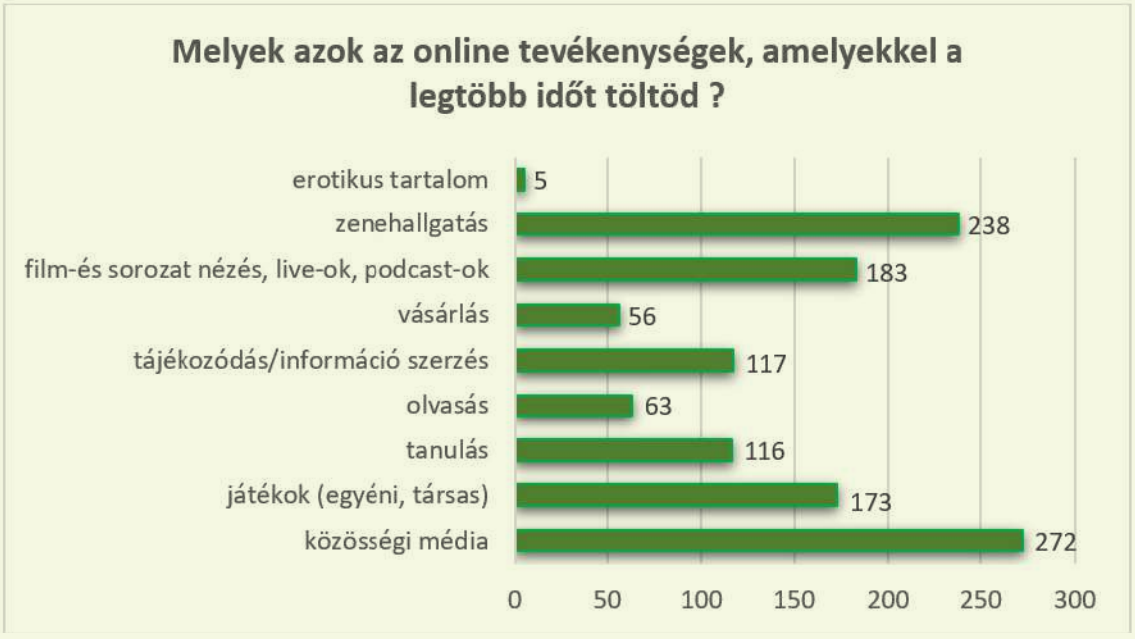


A felmérésben 340 13 és 24 év közötti diák vett részt. Ahogy ez a grafikonból is látható, a legtöbben középiskolások. A válaszadók között a lányok kicsit nagyobb arányban szerepeltek (53 %). A felmérésből az is egyértelműen kiderült, hogy a résztvevő korosztály naponta legalább 4 órát internetezik. Az alábbi grafikon is mutatja, hogy 290 fő nyilatkozott ennek megfelelően.

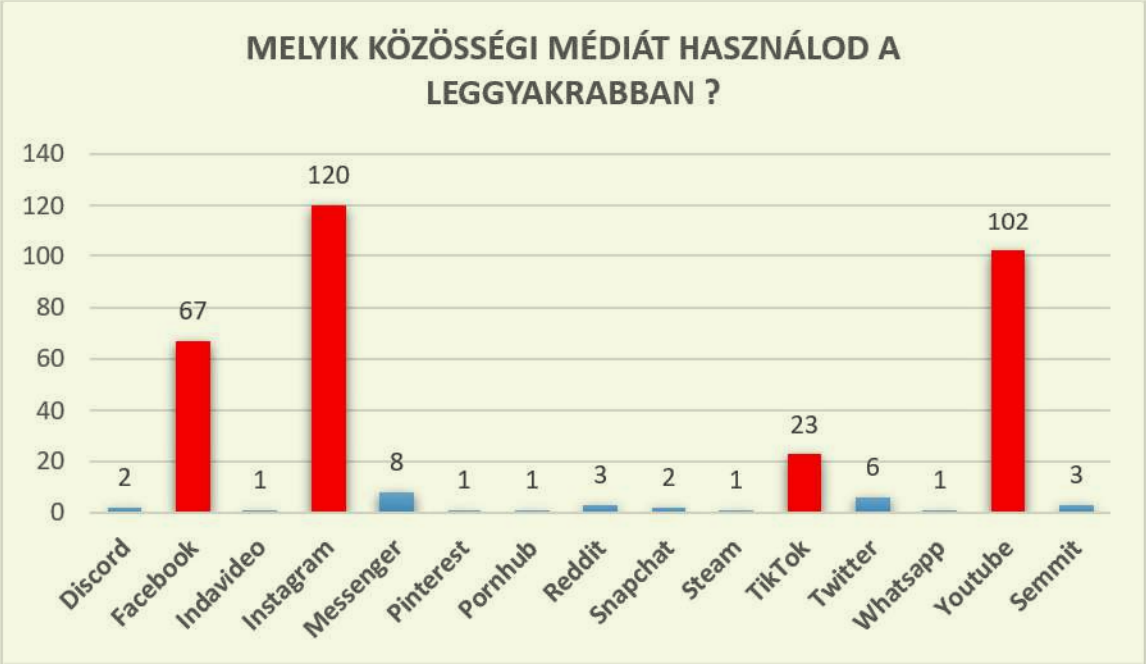
„Sokat beszélgetek a tanítványaimmal, és azt tapasztalom, hogy inkább minden iskolai tennivalót félretesznek, de az internethez ragaszkodnak. A tanár kollégákkal gyakran látjuk azt is, hogy a tanítási órák közötti szünetekben a mobiltelefonokat, tableteket „bújják", alig beszélgetnek egymással." (Pappné Szabó Alexandra)



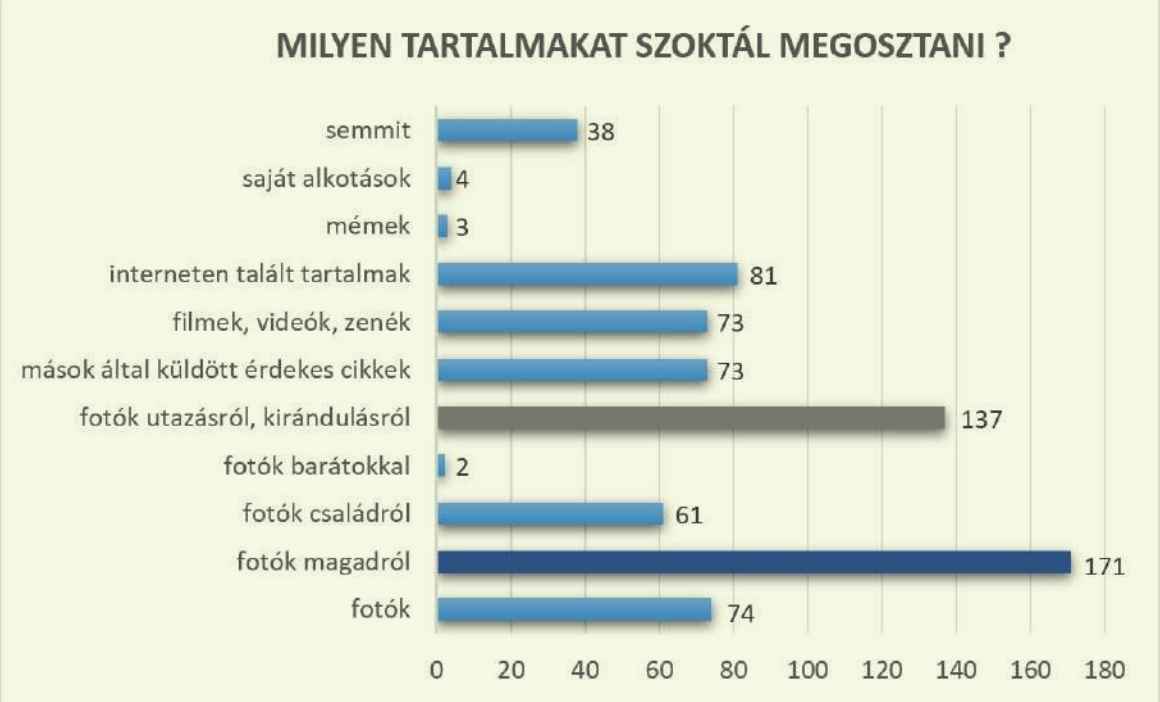
Arra a kérdésre, hogy melyek azok az online tevékenységek, amelyekkel a legtöbb időt töltik a diákok, az alábbi diagramm ad választ. Egyértelműen a közösségi média, a zenehallgatás, filmnézés és a játékok az, ami az első három helyet foglalja el a fiatalok mindennapjaiban. Az olvasás, a tanulás és az információszerzés csak ezek után következnek.



A közösségi médiák között vezet az INSTAGRAM, a második helyet foglalja el a YOUTUBE, míg a FACEBOOK a harmadik helyre szorult vissza. (a negyedik helyen áll a TIKTOK).

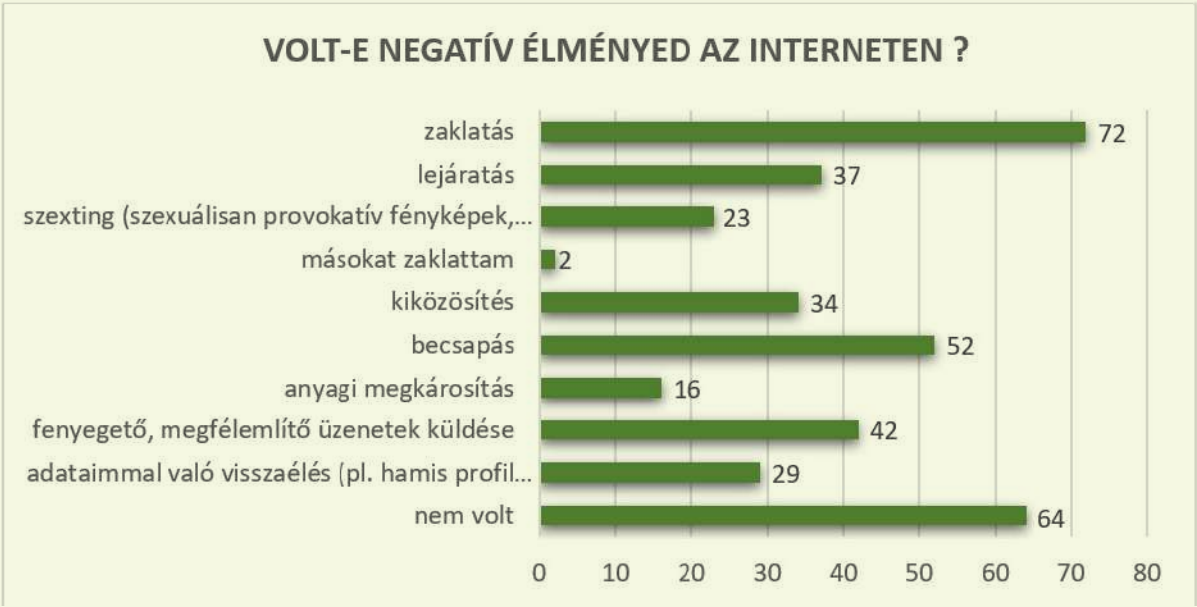


Nem meglepő, de nagyon veszélyes, és a fiatalok válaszai alapján egyértelműen vezet a tartalommegosztások között a FOTÓK nyilvánossága, megosztása saját magukról. Sőt, a második, negyedik helyen is a fotók megosztását láthatjuk, közéjük, a harmadik helyre beékelődve az „interneten talált tartalmak" megosztása került.



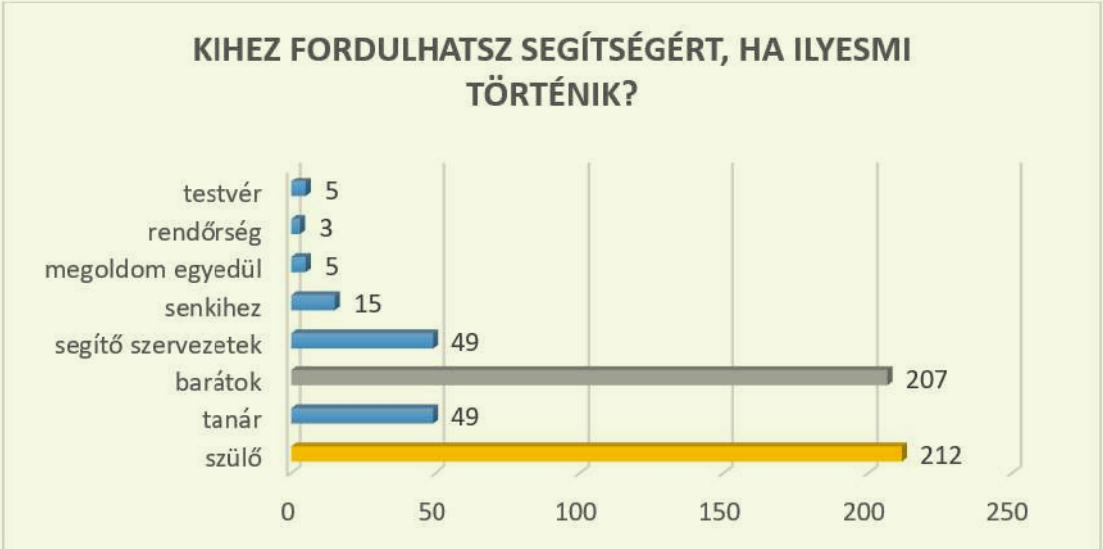
Amire szeretnénk felhívni a figyelmet a fentieken kívül, hogy kevés az olyan fiatal, akit ne ért volna még negatív élmény az interneten. A negatív élmények között vezet a „ZAKLATÁS": a válaszadók egynegyede találkozott már vele az interneten. A második helyet az „ÁTVERÉS" foglalja el (18 százalékuk volt érintett). Rendkívül fontos és elgondolkodtató eredmény, hogy a „FENYEGETŐ, MEGFÉLEMLÍTŐ ÜZENETEK KÜLDÉSE" a harmadik a dobogón, amely alig marad el az előző kettőtől (14%). Szeretnénk felhívni a figyelmet egy adatra: nagyon alacsony (19%) azoknak az aránya, akiknek még semmilyen negatív élménye nem volt.

„Összegezve a tapasztalatokat: leggyakrabban a lejáratő, hitelrontó posztok, rosszindulatú megjegyzések (trollok) okoznak kellemetlenséget a diákoknak a digitális térben. Ezeket a napi szinten előforduló írásos bántalmazásokat nem tudják kezelni a gyerekek. Az agresszív viselkedés, bántalmazás és kirekesztés másik melegágya az online játéktér. Mindezek mellett nem elhanyagolható tényező a szexuális tartalmú képek és üzenetek továbbításának veszélye sem. A személyes adatok védelme és a biztonságos internetezés mellett, az internetes zaklatás (cyberbullying) és a szexting témáinak feldolgozására is óriási szükség van az osztálytermekben." (Karsai Zita)



„Az átveréssel, kiközösítéssel és az adatokkal való visszaéléssel is sokan találkoztak már az interneten. Fontos lenne kideríteni pl. hogy hogyan viselkedtek, mit tettek, fordultak-e segítségért valakihez, kiben bíztak meg, kinek mondták el ezeket. Volt már példa arra is, hogy néhány diákunk saját osztálytársaival szemben alkalmazta a megfélemlítést, vagy éppen a személyes adataikkal, arcképmásukkal való visszaélést. Sajnos, nem mindig érzik ezeknek a megnyilvánulásoknak a hatását és súlyosságát. A fentiekben már írtam arról, hogy milyen fontos szerepe van a pedagógusoknak abban, hogy tanítványaik megértsék és tiszteletben tartsák a másik jogait. A szülőkkel való együttműködés is elengedhetetlen lenne, ugyanakkor nap mint nap szembesülünk azzal, hogy a szülők többsége nem tud/nem akar időt szakítani a gyermekét érintő fontos megbeszélésekre." (Pappné Szabó Alexandra)

Ha bekövetkezik bármilyen probléma a digitális térben, és azt a diák nem képes egyedül megoldani, akkor elsőként vagy a SZÜLŐHÖZ, vagy a BARÁTOKHOZ fordulnak a fiatalok. A tanár és a segítő szervezetek csak a harmadik és negyedik helyen szerepelnek.

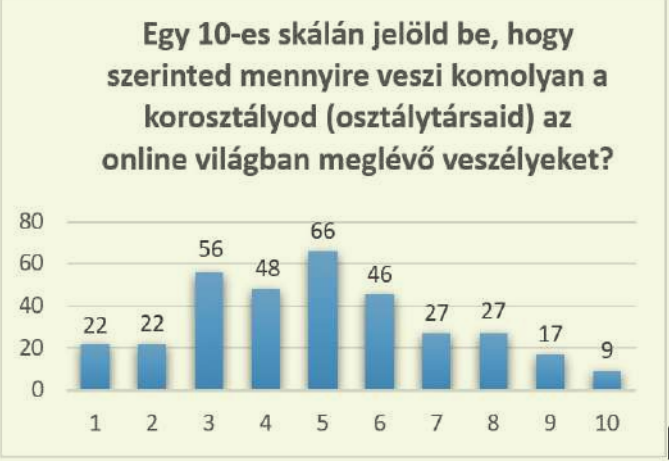


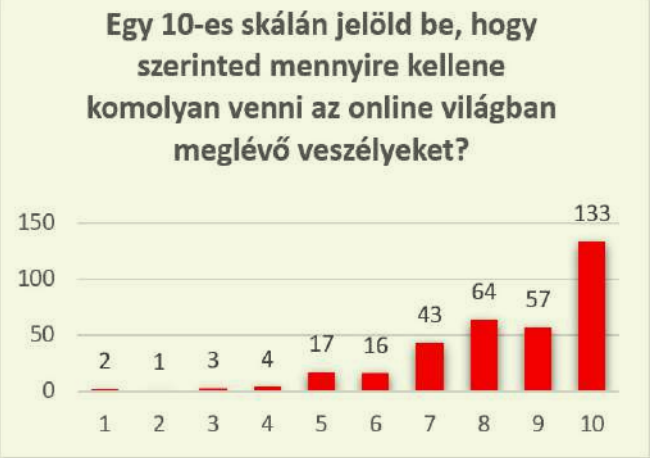
„Szintén bebizonyosodott a kutatás nyomán, hogy a tanulók internetes zaklatás, fenyegetés esetén inkább kérnek segítséget a barátaiktól, mint a tanáraiktól. A megkérdezettek fele hamarabb szól a barátjának, mint a pedagógusnak. A tanárokhoz a diákok harmada fordul bizalommal ilyen esetekben. Ennek a jelenségnek az oka egy további kutatás témája lehet". (Teleki József)

„Ezek az adatok is erősítik bennem azt a meggyőződést, hogy a szülőkkel és kortársakkal együttműködve lehetnénk igazán hatékonyak. Ezt a kérdőíves felmérést meg lehetne ismételni ugyanezen tanulók körében, miután már megvalósult valamilyen program, segítség, tájékoztatás stb. a témához kapcsolódva." (Pappné Szabó Alexandra)

Az utolsó két kérdésben arra kerestük a választ, hogy mennyire veszik komolyan a fiatalok az online világ veszélyeit, és szerintük mennyire kellene ezeket a veszélyeket komolyan venniük.

Érdekes elgondolkozni azon, hogy a diákok önmagukról (saját döntéseikről) igen magas (7-10 közötti) értéket jelöltek meg, míg a korosztályuk viselkedéséről sokkal alacsonyabb értéket feltételeznek (3-6 közötti értékek a legszámosabbak).





„Azt hiszem, ezek a választások azt is jelentik, hogy a kamaszok nagy része nem gondol arra, hogy ami az interneten szerepel, az nem csak hasznos és jószándékú lehet. Ha a pedagógusok is jobban megismerik e veszélyeket, és megtanulják azt, miként lehetne diákjaik számára is úgy világossá tenni, hogy ők abban ne valamiféle korlátozást lássanak, akkor előbbre léphetnénk." (Pappné Szabó Alexandra)

„A felmérésbe bevont fiatalok igencsak eltérően látják az online világ veszélyeit annak függvényében, hogy azt a saját- vagy a korosztályuk szemüvegén át nézik. Korosztályként szignifikánsan kisebbnek vélik a kitettségüket, mint személyes véleményüket tudakolva. A megkérdezett fiatalok saját magukra vonatkoztatva igen nagynak érzik annak a veszélyét, hogy áldozattá válnak az online világban, míg a korosztályukra vonatkoztatva ugyanennek a veszélyét közepesnek értékelik." (Teleki József)

Összefoglalva a tapasztalatokat, válaszolnunk kell az alábbi kérdésre: **Melyek azok a témakörök, amit célszerű velük az órákon megbeszélni? Erre a kérdésre a tanárok által leírt, kiemelt gondolatokból idézünk.**

„Az osztályfőnöki órák keretében is megismertethetjük diákjainkkal:

- *GDPR megfelelőség: személyes adatvédelem fontosságát;*
- *a mobil eszközök használatának veszélyeit;*
- *tanulóink legyenek tisztában az Európai Unió adatvédelmi irányelveivel, a magánélet védelme és a saját adatokhoz való joggal.*

Fontos:

- *a digitális tisztességre neveléshez a tanár mellett a szülők támogatására is szükség van;*
- *a kollégák tudásának növelése, szélesítése az internethasználat veszélyeire vonatkozóan ugyancsak elengedhetetlen". (Pappné Szabó Alexandra)*

„Mivel a személyes adatok egyre nagyobb mértékben tárolódnak interneten, egyre jobban ki vagyunk téve mindenféle támadásnak. Az internetes támadások és feltörések gyakoribbá váltak, és az emiatti veszteségek növekedőben vannak. Szerintem egyre nagyobb igény van arra, hogy tudjanak a diákok ilyen témákról, foglalkozzanak vele és ne csak felületesen kezeljék ezeket a dolgokat. Tudatosítanunk kell bennük, hogy felelősséget kell vállalniuk az adataikért, bárhová is töltik fel azokat és hogy a közösségi média „nem játék". Az adatvédelem és az internetbiztonság problémáiról nagyon fontos beszélni annak érdekében, hogy a jövő mindannyiunk számára biztonságosabb legyen." (Fenyvesiné Jászai Lídia)

"A mobiltelefonokra töltött applikációk engedélykéréseinek ellenőrzését senki nem tette meg a korábbiakban. A tanulók nem voltak tisztában ezzel az ellenőrzési és szabályozási lehetőséggel. Beszélni kellett a wifi és a webfelületek biztonságos használatáról, az adatok titkosításáról, valamint a személyes és érzékeny adatok kategóriájáról. Az érzékeny adatokat általában a közösségi média portáljain teszik közzé a tanulók, videók és fotók formájában. E tekintetben nem érzékelik, hogy hol van a nyilvános és a személyes élettér határa." (Karsai Zita)

„A tanulók többsége tisztában van a digitális világ veszélyeivel, de nem törődnek ezzel és nem veszik komolyan a digitális világból származható fenyegetéseket. Úgy érzem, hogy érdemes volt ezt a kutatást elvégezni a saját osztályomban. Ez volt az első ilyen jellegű felmérés, és rengeteg adat, információ birtokába jutottam a kutatás által. Az eredmények megmutatták, hogy mindig kell foglalkozni az internetbiztonság és a személyes védelem kérdéseivel. Minél több olyan programot, rendezvényt, órát kellene szerveznünk nekünk, tanároknak a diákjaink számára, melyekkel diákjainkat megtaníthatnánk a biztonságos, felelős viselkedési módokra a digitális világban, a veszélyek felismerésére és elkerülésére. Ha már egy digitális világban élünk, akkor az ebben a világban való létezés szabályait is meg kell tanítanunk diákjainknak, gyermekeinknek. Ez is kötelességünk." (Olasz-Barabás Brigitta)

1.3 Óratervek, projekttervek a digitális biztonságra való felkészítéshez

A következő (harmadik) modul feladata egy ÓRATERV ELKÉSZÍTÉSE volt. A kurzus résztvevőinek meg kellett tervezniük azt, hogy a digitális biztonság köréből a felmérés által kijelölt legfontosabb témákat hogyan tanítanák meg, hogyan dolgoznák fel diákjaikkal saját tantárgyuk keretében, illetve osztályfőnökként. Az óraterveket ki is kellett próbálni és reflexiót is írtak a kurzuson résztvevő pedagógusok.

1.3.1 Feladatleírás

1. Válassza ki a III. modulból azt a témát, amelyet szeretne feldolgozni a diákokkal!

2. Gyűjtsön ingyenes online tartalmakat, vagy készítsen sajátot a web 2.0 eszközök használatával, amit megoszthat a tanulókkal az osztályban!

3. Készítsen el egy óratervet/projekttervet a téma feldolgozására! Alkalmazzon aktív tanítási módszert (fordított osztálytermi módszer vagy projektmódszer)! Az óraterv/projektterv foglalja magába a következőket:

- tanulási célok (kompetenciák fejlesztése, tudás megszerzése, átadása),
- tanulói feladatok (otthon és a tanórán, egyedül, közösen),
- a tanórai munka időkerete és feladatai,
- a tanulói teljesítmény értékelése (ki, mit, mikor értékel, milyen módszerrel).

A következő oldalakon a tanárok által elkészített óratervekből, projekttervekből mutatunk be néhányat, melyek hasznosíthatók, módosíthatók, szabadon felhasználhatók. Célunk az, hogy – figyelembe véve a tantárgyat, tanítási módszereket – minél változatosabb terveket és tapasztalatokat tegyünk közzé.

1.3.2 A pedagógusok egyéni megoldásai

Olasz-Barabás Brigitta munkája

TERVEZÉS, ELŐKÉSZÜLETEK

Tanulócsoport: A DBPH [70] 5 órás (5*45 perces) programját az osztályomban (8.c) tanuló gyermekek számára készítettem, akik már jártasok a digitális világban, és naponta használnak digitális eszközöket, „kütyüket" és „digitális bennszülöttek".

ELŐKÉSZÜLETEK

A tantermet csoportmunkára rendeztük be a gyerekekkel. Mindenkinek hoznia kellett laptopot, tabletet vagy mobiltelefont. Előzetesen minden tanulónak ellenőriznie kellett, hogy a balintsulis.hu email címe aktív, működő elektronikus cím. Erre azért volt szükség, mivel a digitális tartalmakat Google Drive-on keresztül, a számukra létrehozott mappából tudták elérni a diákok.

Az 1. óra célja a csoportok megalakulása, a témák és feladatok ismertetése és a digitális dokumentumokkal és módszerekkel való ismerkedés volt.

A 2.- 4. órákon a kihúzott témák feldolgozása történt (keddtől csütörtökig).

Az utolsó, 5. óra a saját projektek bemutatása és értékelése volt.

A DBPH óráit óracserékkel, etika, informatika és magyar órákon valósítottam meg.

AZ ÓRATERV/ÓRAVÁZLAT ÉS ANNAK MEGVALÓSÍTÁSA

Nevelési-oktatási cél

Magyar, történelem, etika szakos tanárként és édesanyaként is rendkívül fontosnak tartottam, hogy diákjaim tájékozottak legyenek a digitális világ veszélyeivel, az egészségügyi kockázatokkal, a közösségi médiahasználat előnyeivel és hátrányaival kapcsolatban. Célom volt az is, hogy tanulóim digitális kompetenciáját megerősítsem és elősegítsem azt, hogy jártasságot szerezzenek a biztonságos internethasználat területén.

Értékelés: az egyes digitális feladatok értékelése a megadott szempontok szerint történt *(Mellékletben).*

Tanítás helye:	Törökbálint, Bálint Márton Általános Iskola és Középiskola
Tanítás ideje:	2020. február 17. 3. óra
Osztály:	8.c
Időkeret:	45 perc
Tanár neve:	Olasz-Barabás Brigitta
Tantárgy neve:	Etika
Tematikai egység:	A technika világa
Tananyag/téma:	Behálózva, az internet veszélyei, netikett
Az óra típusa:	Vegyes: részben új ismeretet feldolgozó és részben korábbi ismereteket összefoglaló

70 **Digitális Biztonság Projejekt Hét (DBPH)**

Tanulási-nevelési-fejlesztési cél:	Netikett szabályainak erősítése, a kiberbiztonsági tudat megerősítése, az egészségügyi veszélyforrások felismerésének kialakítása a tanulókban, a mentálhigiénés veszélyek ismeretének elsajátítása, és a közösségi média előnyeinek és hátrányainak megismerése

Idő (perc)	Az óra menete (Tananyag/Téma/Tevékenység)	Kulcsfogalom	Módszer/eszköz/in-doklás	Kapcsolódási pont	Ellenőrzés/ Értékelés
6 perc	A DBPH céljának és a projekthét programjának az ismertetése	digitális biztonság	tanári közlés, magyarázat	etika, informatika	_
6 perc	A digitális csoportok létrehozása, a témák kisorsolása	digitális biztonság	csoportalakítás szókártyákkal: a témák kihúzása	informatika	közös megbeszélés, csoportfelelősök megválasztása
8 perc	Feladatok és az értékelés szem-pontjainak ismertetése	dokumentumok, források	tanári közlés, magyarázat	etika, informatika	közös megbeszélés
20 perc	A megadott témák internetes tartalmainak feldolgozása digitálisan, csoportokban, differenciáltan	▪ internet, biztonság, veszély, pszichológia, ▪ mentálhigiénés problémák ▪ fenntartható fejlődés, ▪ egészségügyi kockázatok	A 3. feladat elkészítése csoportokban digitális források, eszközök segítségével (ppt, prezi, film, kahoot stb.), digitális kompetenciák fejlesztése (információk keresése, gyűjtése, feldolgozása, kritikai gondolkodás fejlesztése)	etika, informatika, pszichológia, egészségügy	kooperatív, differenciált csoportmunka támogatása
5 perc	A csoportok eddigi munkáinak ismertetése, szóbeli értékelése	kooperáció, interakciók tanári értékelése, tanulói önértékelések	A tapasztalatok frontális megbeszélése, összegzése (önértékelés fejlesztése)	pszichológia, peda-gógia	közös megbeszé-lés, formatív, fejlesztő értékelés

Reflexió

Magyar nyelv és irodalom, történelem, valamint etika szakos tanárként fontosnak tartom, hogy diákjaink, a jövő nemzedéke tisztában legyen történelmi múltjával, jelenével és szembe tudjon nézni a digitális világ kihívásaival. Az etika tantárgy „A technikai fejlődés" című fejezetének meghatározott témái lehetőséget biztosítanak arra, hogy a diákok digitális kompetenciáit fejlesszük és felkészítsük őket a virtuális világ veszélyeire és az azokkal való szembenézésre.

A **DBPH** elnevezésű rövid programmal az volt az elsődleges célom, hogy a gyermekek figyelmét felhívjam a digitális eszközök fizikai és pszichológiai hatásaira, figyelmeztessem őket a közösségi médiahasználat előnyeire és veszélyeire, illetve fontos cél volt annak a tudatnak a megerősítése, hogy a virtuális világban is figyelni és vigyázni kell magunkra. A digitális kompetenciák megerősítése, megszilárdítása a **DBPH** központi feladata volt, akár csak a kritikus gondolkodás fejlesztése. Célom volt még az is, hogy az 5. óra után megerősítést kapjanak diákjaim korábbi ismeretei, kompetenciái.

Az óratervem első két feladata a **DBPH** feladatainak az ismertetését és a gyermekek csoportmunkába való rendeződését szolgálta. A csoportmunkában végzett feladatok a kooperációs készségeik fejlesztését szolgálják. A Telenor digitális mintaiskolájaként rendelkezésünkre állnak intézményünkben a megfelelő IKT-eszközök, de a tanulóim szeretnek a saját eszközeiken dolgozni, és ez megengedett a mindennapi gyakorlatban is.

A **DBPH** súlypontja, legfontosabb szakasza a 2.-tól a 4. óráig tartó, a gyermekek által elkészítendő 3 feladat kivitelezését megvalósító órák voltak. A tevékenységorientált, kooperációra épülő és a digitális kompetenciák fejlesztését is szolgáló feladatokra az 1. órán szánt 20 perc csak a digitális források megismerésével telt. Természetesen a diákok is kereshettek a kidolgozandó témájukhoz kapcsolódó digitális anyagokat. Az előkészítő idő rövidsége miatt és a **DBPH** egyedüli megvalósítójaként én sem tudtam minden forrást felkutatni, így a Google Drive-ra én is folyamatosan töltöttem fel a diákok számára használható dokumentumokat.

A tanári értékelés és tanulói önértékelések közös megbeszélésével, összegzésével ért véget az 1. tanóra. Az egyes csoporttagok tudták, milyen feladatokat kell elvégezniük ahhoz, hogy az 5. bemutató órára elkészüljenek a **DBPH** produktumaival Az 5. óra végén minden tanulóban megerősítést kellett, hogy kapjon az az érzés, hogy az internet világában is lehetnek veszélyes helyzetek, akárcsak a valós életben. Erre fel lehet készülni és okos döntésekkel el lehet kerülni azokat.

A DBPH zárónapján történt az egyes csapatok feladatainak a korábban ismertetett szempontok szerinti értékelése. A csapatok összesen 60 pontot szerezhettek. A csapatok elismerő oklevelet kaptak a teljesítményükről. A tanári szummatív értékelés mellett a diákok és én titkos szavazással még az utolsó órán megválasztottuk a közönségdíjas projektet készítő csapatot.

Az órák jó hangulatban teltek. A gyerekek szerint máskor is kellene hasonló órákat, miniprojekteket szerveznem nekik. Úgy érzem, hogy ennél nagyobb dicséretet nem is kaphattam volna tőlük!

Mellékletek

1. Csoportalakítás szókártyákkal: Keressétek meg az összetartozó szókártyákat, és akik megtalálták társaikat és megalkották a csoportokat, azok üljenek egy asztalhoz! Találjatok magatoknak csoportnevet, majd válasszátok meg a csoportfelelősöket!

2. Témakártyák

- A „kütyük" használatának egészségügyi hatásai, kockázatai
- A digitális technológia pszichológiai, mentálhigiénés hatásai
- A közösségi médiahasználat előnyei és hátrányai
- A digitális technológiák környezeti hatásai
- Internetbiztonság, segítő szervek

3. Feladatok: minden csoportnak létre kell hoznia a következő órákon!

I. feladat: 1 db szövegre épülő dokumentumot (a szöveget/szavakat el lehet helyezni ppt-ben, preziben, szófelhőben, gondolattérképen)

Értékelés módja: a projekthét utolsó, 5. napján

- a szöveg tartalma-témának megfelelő (max. 5 perc)
- a kivitelezés/módszer megfelelő használata (max. 10 perc)
- forráshasználat, forrásmegjelöléssel (max. 5 perc)

II. feladat: 1 db kisfilm létrehozása a témával kapcsolatban (max. 5 perc)

Értékelés módja: a projekthét utolsó, 5. napján

- a film időkeretének betartása (max. 5 perc)
- a film tartalma, üzenete, szakmaisága (max. 10 perc)
- a létrehozott film szerkezet (max. 5 perc)

III. feladat: 1 Kahoot/Learninapps/Quizziz/Redmenta feladatsor létrehozása a témával kapcsolatban. Értékelés módja: a projekthét utolsó, 5. napján

- a témához kapcsolódó kérdések/tesztek szerkesztése (max. 5 perc)
- a tesztek/kérdések hasznos információtartalma (max. 1 perc)
- a tesztek/kérdések helyesírása (max. 5 perc)

4. Az eddig tanult és használt alkalmazások

- ***http://www.tagul.com***
- ***http://www.wordart.com***
- ***http://www.mindmup.com***
- ***http://www.postershop.hu/picasa-foto-kollazs-keszites.htm***
- ***https://prezi.com***
- ***https://www.picbow.com/photo-grid-online.html***

- *https://piktochart.com*
- *https://sway.com*
- *http://recite.com*
- *https://learningapps.org*
- *http://kockalapok.hu*
- *https://kahoot.com*
- *https://www.redmenta.com*

5. A google drive-ban található források

- *https://www.digitaliscsalad.hu/biztonsag/ezt-videot-mutasd-meg-kamasz-gyerekednek*
- *https://nagykerbiztonsag.hu/wp-content/uploads/2018/03/kepernyos_munkahelyek.pdf*
- *https://www.gyerek-portal.hu/szamitogep-es-hatasai-a-gyerekekre.html*
- *https://news.microsoft.com/hu-hu/2017/07/10/minden-masodik-gyerek-veszely-nek-van-kiteve-neten*
- *https://www.youtube.com/watch?time_continue=5&v=KWdaoVnnkCI&feature=emb_logo*
- *https://greenfo.hu/hir/az-elektronikai-kutyuk-arnyai*
- *https://www.youtube.com/watch?v=dcBNRCldLvE*
- *http://njszt.hu/sites/default/files/document/2019/NJSZT_IT_Biztonsag_kozerthetoen_v3.pdf*
- *http://nmhh.hu*
- *https://www.kek-vonal.hu/index.php/hu/szolgaltatasok/internetbiztonsag*
- *http://www.kamaszpanasz.hu/hirek/pedagogus-segedanyag/4421/internet*
- *http://www.police.hu/hu/hirek-es-informaciok/bunmegelozes/aktualis/biztonsa-gos-internethasznalat-0*
- *https://www.youtube.com/watch?v=tvagadvwoMw*
- *http://ithaka.hu/wp-content/uploads/2012/07/ITHAKA_NMHH_EU_KIDS_PPT_v1.0.pdf*
- *https://www.telenet.hu/hasznos-tan%C3%A1csok/internet-biztons%C3%A1g.html*
- *https://www.youtube.com/watch?v=aGP6EnX6_BE*
- *https://mese.tv/internet-biztonsag/sosem-vagy-egyedul.html*
- *https://24.hu/tech/2018/11/13/facebook-instagram-snapchat-kozossegi-media-men-talis-egeszseg*
- *https://www.digitalhungary.hu/kozossegi-media/?ap=47*
- *https://www.nyest.hu/hirek/hogyan-hat-az-agyunkra-a-kozossegi-media*
- *https://24.hu/tech/2019/10/11/tinedzser-lanyok-kozossegi-media-zaklatas-alvas-baratok/*
- *https://www.youtube.com/watch?v=98cNA1abGxM*
- *https://www.csupaszivmagazin.hu/a-kozossegi-media-veszelyei-a-gyerekekre*

Tóthova Edita munkája

Tanítás helye: Tatabányai Szakképzési Centrum Bláthy Ottó Szakgimnáziuma,

Szakközépiskolája és Kollégium

Tanítás ideje: 2020. január 29.

Osztály: 9.D

Az osztály létszáma: 37 fő, ebből a második csoport 17 fő (16 fiú, 1 lány)

Tantárgy: Informatika

Témakör: Internetbiztonság / Kiberbiztonság

Tananyag: Személyazonosság védelme

Időkeret: 45 perc

Tanár szakos : Tóthova Edita

Óra címe: Rejtőzködés az interneten, avagy mit mondjunk, vagy mit NE mondjunk el mindenkinek

Kompetenciák: Szociális és állampolgári kompetenciák / az anyanyelven folytatott kommunikáció / digitális kompetencia

Új ismeretek:

- Nemzeti Adatvédelmi és Információszabadság Hatóság,
- Az emberek digitális lábnyoma,
- Az internetes zaklatás, Felelősségteljes webhasználat.

Új fogalmak: Magánélet, személyes adatok, bizalmas információk

Oktatási célok:

- Felhívni a diákok figyelmét a személyes és egyéb adatok védelmének fontosságára.
- Segíteni a diákoknak módszereket találni személyes adataik védelmére és egy pozitív digitális lábnyom fenntartására.
- Arra ösztönözni a diákokat, hogy közös munkát végezzenek az együttműködési feladatok tevékenységek keretében.
- Arra ösztönözni a diákokat, hogy kreatív módon vizsgálják meg a forrásokat, elemezzék a különböző anyagokat és mutassák be eredményeiket.

Módszer: Rögzítő módszerek, az új ismeretek elmélyítése kérdésekkel, beszélgetéssel, számítógéppel való munka

Munkaformák: Megbeszélés, kooperatív munka

Eszközök:

- internetkapcsolattal ellátott digitális készülékek (pl. számítógépek, laptopok, tabletek stb.)
- internet böngésző;
- internetes kereső;
- opcionális: webkettes eszközök (wordle, scratch ***http://scratch.mit.edu***;
- tricider ***http://www.tricider.com***;
- voki ***http://www.voki.com***;
- google forms ***http://www.google.com/forms/about***;
- surveymonkey ***https://www.surveymonkey.com***;
- prezentációs szoftverek, prezi ***http://prezi.com***;
- használatához regisztráció szükséges: google forms, google slides & prezi;
- filctoll, tábla, számítógépek, vetítőgép.

Felhasznált irodalom:

- ***https://saferinternet.hu/Tippek-segedanyagok-videok/Oktatoknak/Oktatasi-anyagok/Oktatasi-anyagok***

RÉSZLETES ÓRATERV

Idő (perc)	Az óra menete	Módszerek	Tanár tervezett tevékenysége	Tanulók tervezett tevékenysége
2 perc	Adminisztráció	Megbeszélés, kérdések, tanári bevezetés	A tanár köszön, majd elvégzi a szükséges szervezési és adminisztrációs feladatokat. Meghallgatja a diákok jelentését, beírja az órát és a hiányzókat az osztálykönyvbe.	A tanulók elhelyezkednek a teremben, állva köszöntik a tanárt, majd jelentenek a hiányzókat illetően.
2 perc	Motiváció	Frontális	A tanár ismerteti az óra témáját és menetét	Figyelmesen hallgatnak
10 perc	Járj utána – beszéld meg!	Kooperatív munkavégzés	A tanár a tanórát megelőzően járjon utána, hogy találhatóak-e információk ezekről a központi fogalmakról a magyar Nemzeti Adatvédelmi és Információszabadság Hatóság weboldalán: https://www.naih.hu Amennyiben igen, javasolja a diákoknak, hogy ezeken a weboldalakon keressenek információkat a feladat elvégzéséhez. Egy szabad ötletelés keretében írjanak egy listát a fenti központi fogalmakhoz kapcsolódó szavakból. Például: a személyes adatok olyan információk, amelyek segítségével az egyének azonosíthatók – név, lakcím, email cím, telefonszám (vezetékes vagy mobil), bankkártyaszám, születési dátum, az egyénről készített kép- vagy hangfelvétel stb. A bizalmas információk közé tartoznak például a politikai nézetek, a vallási hovatartozás, a testi vagy szellemi egészségügyi állapot, stb. A magánélethez való jog a jog arra, hogy titokban tartsuk személyes ügyeinket, kapcsolatainkat, stb.	A diákok gondolkodjanak el a központi fogalmakon: magánélet, személyes adatok, bizalmas információk. Írják fel ezeket a táblára. Kérje meg a diákokat, hogy próbálják megfogalmazni e fogalmak definícióit vagy adjanak meg példákat.

Idő (perc)	Az óra menete	Módszerek	Tanár tervezett tevékenysége	Tanulók tervezett tevékenysége
10 perc	Nézd – hallgasd – beszéld meg!	Kooperatív munkavégzés	Kérje meg a diákokat, hogy gondolkodjanak el azon, hogy mi történne, ha valaki túlságosan sok személyes adatot osztana meg a világgal az interneten. A diákoknak a téma iránti érdeklődésének felkeltéséhez és a gondolkodás ösztönzéséhez lejátszhat egy videót, például a következő linken található: http://goo.gl/rAUAw0 (A videó lejátszása előtt ellenőrizzék, hogy az Önök országából elérhető-e ez a videó a YouTube-on). Emellett ismertetheti a diákokkal az alábbi két tényt: ▪ Az emberek digitális lábnyoma (fényképek, az interneten publikált tartalmak stb.) jelentős szerepet játszanak a vállalatok munkaerő toborzási eljárásaiban. ▪ Az internetes zaklatás gyakrabban fordul elő olyan weboldalakon, amelyeket nagy számban látogatnak a tinédzserek. A személyes adatok védelme elősegíti az internetes zaklatás megelőzését. Erről bővebb információkat olvashatnak a következő weboldalon: http://www.e-abc.eu/en/about-bullying (a weboldalon nem szükséges regisztrálni).	Gyűjtsenek össze olyan érveket, amelyek amellett szólnak, hogy a diákok tudatosan korlátozzák a személyes adataikhoz való hozzáférést, és írják össze ezeket egy listában
20 perc	Együttműködés – kutatás	Kooperatív munkavégzés	A diákok már minden bizonnyal megértették, hogy a magánélet védelme rendkívül fontos, így a tanóra már személyes jelentőséget is nyert számukra. Megtanulták, hogy: ▪ Felelősségteljesen kell használniuk a közösségi médiát, ▪ meg kell védeniük internetes jó hírnevüket.	A diákok azzal foglalkozzanak, hogy kiderítsék, milyen konkrét módszerek segítségével érhetik el a következő két célt (a) Felelősségteljesen kell használniuk a közösségi médiát,

Idő (perc)	Az óra menete	Módszerek	Tanár tervezett tevékenysége	Tanulók tervezett tevékenysége
			Az EU NET ADB projekt http://goo.gl/TyAJh2 (a weboldalon nem szükséges regisztrálni) kutatási adatai szerint a felmérésükben részt vevő 14-17 éves diákok (7 európai országból) 92%-a legalább egy közösségi oldalnak a regisztrált felhasználója. Ossza a diákokat 2-3 fős kiscsoportokba. Kérje meg őket, hogy a csoporttal közösen dolgozva az interneten keressenek adatvédelmi nyilatkozatokat, és elemezzék ezeket, továbbá vizsgálják meg a biztonsági beállításokat néhány közösségi oldalon, például a Facebookon, a Google+-on, a YouTube-on vagy az Instagramon. Bízza meg a csoportokat az alábbi forrás-párok egyikének a vizsgálatával. Ezt a feladatot úgy is elvégezhetik, hogy a csoportok maguk választják ki azokat a forrásokat, amelyek témája a leginkább felkelti az érdeklődésüket, és a legközelebb áll a közösségi hálózatokon folytatott tevékenységeikhez. Facebook adatvédelmi alapismeretek https://www.facebook.com/about/basics Facebook Súgóközpont – Adatvédelem https://www.facebook.com/help Útmutató a Google+ szolgáltatáshoz tizeneéveseknek – Általános tippek http://goo.gl/6Ml93L Google+ Biztonsági központ – Adatvédelmi források http://goo.gl/7WzbQG	(b) meg kell védeniük internetes jó hírnevüket. A diákok következő kérdésekre keressenek válaszokat (a javasoltak kérdéseket a tanárok kiegészíthetik további kérdésekkel): ▪ Az oldal üzemeltetője milyen intézkedésekkel és tanácsokkal segít a felhasználóknak megvédeni személyes adataikat? ▪ Hogyan frissíthetem az adott weboldalon a profilomat, és hogyan módosíthatom a biztonsági vagy adatvédelmi beállításokat? ▪ Hogyan távolíthatok el az adott weboldalról olyan tartalmakat, amelyeket a beleegyezésem nélkül töltöttek fel mások? ▪ Hogyan tudom kiválasztani, hogy ki láthatja a fényképeket és az egyéb dolgokat, amelyeket közzéteszek a Facebookon? ▪ Hogyan tudok törölni valamit, amit közzétettem a Facebookon? ▪ Mi a Facebook Privacy Checkup, és hol található? (A „privacy checkup” jelentése: adatvédelmi ellenőrzés)

			▪ Google+ Biztonsági központ – Digitális jó hírnév kezelése tizenéveseknek https://support.google.com/plus/topic/2404767 ▪ YouTube Irányelvközpont – A személyes adatok védelme http://goo.gl/6ajG4U ▪ YouTube Biztonsági központ – Tinédzserek biztonsága http://goo.gl/H2oxRG ▪ Instagram központi Súgó https://help.instagram.com/ (magyar nyelven nem elérhető) ▪ Internetes jó hírnév ellenőrző lista http://goo.gl/hvnfZM (magyar nyelven nem elérhető) Miután áttanulmányozták a javasolt források tartalmát, mindegyik csoport összegezze a tanultakat azzal, hogy összeírja a személyes adatok védelmét, vagy az internetes jó hírnév fenntartását elősegítő 5 legjobb tanácsot.	
1 perc	Elköszönés		A tanár köszöni a figyelmet	A diákok megköszönik a foglalkozást

Fenyvesiné Jászai Lídia munkája

A pedagógus neve: Fenyvesiné Jászai Lídia

Műveltségi terület: Ügyvitel

Tantárgy: Titkári ügyintézés

Osztály: Irodai titkár 14. évfolyam

Az óra témája: A fizikai egészség védelme a technológia használata közben

Az óra cél- és feladatrendszere: a fejlesztendő attitűd, készségek, képességek, a tanítandó ismeretek (fogalmak, szabályok stb.) és az elérendő fejlesztési szint, tudásszint megnevezése

Az óra didaktikai feladatai: Bevezetés a témába, ráhangolás, motiválás, ismeretbővítés, gyakorlás, összefoglalás, rendszerezés, ismétlés, a házi feladat előkészítése, a házi feladat kijelölése, ellenőrzés, értékelés

Tantárgyi kapcsolatok: informatika

Felhasznált források: A fizikai egészség védelme a technológia használata közben tananyag

Idő-keret	Az óra célja	Nevelési-oktatási stratégia Módszerek Tanulói munkaformák Eszközök	Megjegyzések
5 perc	Óraszervezés	Házi feladat megtekintése tanári videó, megbeszélése Frontális Számítógép, projektor	https://biteable.com/watch/a-fizikai-egszsg-vdelme-2457017
35 perc	Motiváció Megbeszélés Feladatok	Szófelhők készítése Beszélgetés a témáról, téma kifejtés, aktív, interaktív módon LearningApps feladatok megoldása	Tanulók készítették órán – minták az óraterv után https://learningapps.org/9236843 https://learningapps.org/9253448
5 perc	Lezárás	Tanulói, tanári reflexió Házi feladat adása Videó megnézése: az elektronikai termékek történetéről	https://www.youtube.com/watch?v=dcBNRCldLvE

SZÓFELHŐK:

ÖSSZEFOGLALÁS (Reflexió)

A témaválasztásom a „Fizikai egészség védelme a technológiai használata közben”. Azért ezt a témát választottam, mert az irodai titkároknak hozzá tartozik a tematikájához az irodai ergonómia, és ezt átismételve és kiegészítve nagyon jó anyagot tudtam számukra biztosítani.

A VÁLASZTOTT AKTÍV TANÍTÁSI MÓDSZER: Fordított osztályterem

Elküldtem a diákoknak a készített videót. A tanulók 20-22 éves diákok. A hozzáállásuk a témában aktív, hiszen a vizsgájukhoz is kapcsolódik ez a téma. Érdeklődéssel fogadták ezt a módszert, hiszen már máskor is alkalmaztam velük, és nagyon szeretik. Így, ha ilyet viszek be órára mindig örülnek, és hamar eltelik az óra.

LearningApps-en készítettem a feladatokat nekik, amin gyakorolhatják az adott témát és az órán ők is készítettek szófelhőt. Nagyon tetszett nekik.

Az anyagokat az iskola tartalommegosztó rendszerén is megosztottam, így a diákok láthatják az anyagokat és a többiek munkáját is.

Pappné Szabó Alexandra munkája

TÉMA: A pszichológiai jólét védelme a digitális környezetben

A TÉMAVÁLASZTÁS OKA: Nap mint nap tapasztalom a tanári munkámban és a civil életben is, hogy a középiskolás korosztály egy része nincs tisztában az internet veszélyeivel, nem tudják, milyen jogokkal rendelkeznek, milyen fórumokon kérhetnének segítséget például ha zaklatás éri őket.

A kiberbiztonsági tanfolyam 2. modulja kérdőíveinek feldolgozásakor is megerősítést nyert ez a tapasztalatom és egyértelművé vált számomra, hogy ebben a témában készítem el a 3. modul zárófeladatát.

MÓDSZER: Fordított osztályterem

A fordított osztályterem aktív módszer, melynek lényege: a diákok digitális formában, pl. emailben, messengeren, pendrive-on megkapják a tanártól a segédanyagokat, amiket bárhol, bármikor megtekinthetnek, tanulmányozhatnak, majd azon dolgoznak egyénileg vagy csoportos formában.

A módszer a tananyag közlése helyett arra fókuszál, hogy a tanulók magasabb szintű készségei fejlődjenek, alkalmazkodjunk diákjaink egyéni igényeihez. Mindehhez rugalmas tanulási környezetre, tanulóközpontú megközelítésre, motiváló módszerekre van szükség. Így valósulhat meg az alkotva tanulás, mely hosszabb távon segíti az élethosszig tartó tanulás fontosságának felismerését is. Elengedhetetlen a tanár – munkát előkészítő – alapos tervező tevékenysége.

TANULÓK ÉLETKORA: 15-16 év (9-10. évfolyam)

A saját osztályommal, akik 10. évfolyamosok, mindenképpen szeretném megvalósítani a feladatot. A rendelkezésemre álló idő rövidsége és egyéb munkahelyi tennivalóim miatt még nem volt alkalmam kipróbálni.

A Z-generáció folyamatosan online életet él, ezért számukra érdekesebb, motiválóbb lehet, ha használhatják okoseszközeiket a feladatmegoldásokban.

Diákjaink, illetve ismerőseik egy részét érték már az online világban negatív tapasztalatok, pl. zaklatás, lejáratás, fenyegetés, szexting stb., és úgy vélem, kis csoportban – a tanár jelenléte nélkül – jobban meg tudják vitatni ezeket, mintha frontális osztálymunkában kerülne rá sor. Ezután következne az osztálytermi megbeszélés.

TANULÁSI CÉLOK – FEJLESZTÉSI TERÜLETEK:

- kompetenciák fejlesztése:
  - digitális;
  - szociális: együttműködés, véleményalkotás, mások véleményének meghallgatása és elfogadása, kulturált vita, közös felelősségvállalás;
- a tanulók legyenek tájékozottabbak a digitális világ veszélyeivel kapcsolatban;
- tudjanak különbséget tenni igazi és virtuális barát/barátság között;
- ismerjék meg a saját és mások jogait az online világban;
- tanulják meg megóvni bizalmas adataikat másoktól;
- ismerjék meg a segítségkérés lehetőségeit és formáit, ha bármilyen sérelem éri őket a digitális világban, pl. zaklatás, személyes adatokkal való visszaélés, lejáratás stb.;
- tudjanak mások számára segítséget ajánlani, ha őket érik ilyen jellegű sérelmek;
- a proaktív viselkedéssel való megismerkedés: az általuk létrehozott digitális tartalmak kezelése.

A MUNKA IDŐKERETE: 3 hét az alábbiak szerint

- Előkészítés: 1 tanóra frontális munkaformában. Megbeszélés, csoportok alakítása.
- 4 csoportot alakítunk, melyek nem azonos feladatokat kapnak. Az egyes csoportok tevékenységei végül összekapcsolódnak, és a közös megbeszélésen, prezentáción mindenki láthatja a többiek munkáját, és azt is, hogy egy teljes egészet képez a 4 csoport által elvégzett feladat.
- Csoportmunka: a tanulók projekt jelleggel otthon dolgozzák fel a tanyagot: ehhez 2 hét áll a rendelkezésükre. Az otthoni munka idején a tanárukkal folyamatos internetes és személyes kapcsolatban állnak: tanácsot, segítséget kérhetnek.
- Befejezés: tanórán a csoportok prezentálják társaik és pedagógusuk számára az elvégzett munkát, eredményeket, tanulságokat – ehhez minimum 2 tanórára van szükség.

SZÜKSÉGES ESZKÖZÖK

- laptop a tanár számára;
- minimum 1 tablet csoportonként;
- digitális tábla a bemutatókhoz;
- internetkapcsolat;
- Google-űrlap: kérdőív;
- A The Web We Want című munkafüzet: ***https://saferinternet.hu/Tippek-segedanyagok-videok/Oktatoknak/Oktatasi-anyagok/Oktatasi-anyagok***;
- a ***https://sway.office.com*** használatának megismertetése és alkalmazása.

ÉRTÉKELÉS

A formatív – fejlesztő célú – értékelés folyamatosan jelen van a tevékenységek során. A tanár győződjön meg arról, hogy diákjai valóban tanulnak valamit.

Előbb az egyes csoportok ismertetik a feladataikat, majd a megoldási módokat és az eredményeket, tapasztalataikat is megosztják társaikkal. Egymástól tanulhatnak a legtöbbet.

Mindenképpen szükséges időt szánni arra, hogy a többiek is elmondhassák véleményüket minden csoport témájáról, kérdéseket tegyenek fel egymásnak, illetve a tanárnak. Az önértékelés és a társak általi értékelés fontos eleme a folyamatnak.

Az értékelés része lehet a **The web we want** című munkafüzet 47-49. oldalán található teszt kitöltése: Mi mindent tanultál? Nettudós vagy netkezdő vagy?

Utána közös megbeszélés, megvitatás:

- Milyen fontos ismeretekkel lettek gazdagabbak?
- Mi okozott meglepetést, mi volt a legérdekesebb számukra?
- Megváltozik-e a későbbiekben az internethasználatuk?
- Jobban figyelnek-e arra, hogy mit osztanak meg?
- Szerintük mit lehetne tenni a zaklatások megelőzésére, az ellenük való hatékonyabb fellépéshez?
- Van-e olyan feladatrész, amit már másképp oldanának meg – és miért?

Az értékelés, közös megbeszélés jó alkalmat nyújthat arra is, hogy diákjaink szembesüljenek az eltérő generációk véleményének különbségeivel és azonosságaival.

Úgy gondolom, hogy az iskola Facebook-oldalára a csoportok Sway-összefoglalóját (beleegyezésük esetén) fel lehetne tölteni, hogy az iskola közössége is megismerje munkájukat, és a témával való foglalkozás fontosságát is erősítené. A bemutatókról, megbeszélésekről készített fotókkal is kiegészíthetnénk ezt a beszámolót.

A CSOPORTOK FELADATAI

1. csoport:

a) A **The web we want** című munkafüzet: ***https://saferinternet.hu/Tippek-segedanyagok-videok/Oktatoknak/Oktatasi-anyagok/Oktatasi-anyagok*.** A munkafüzet 17-18. oldalának feldolgozása (Gondolkodj, mielőtt posztolsz!)

b) Készítsetek rövid videót az iskola diákjai körében az internet veszélyeiről!

c) Állítsatok össze egy Google-kérdőívet a munkafüzet feladataihoz kapcsolódva, kortársaitok számára!

d) Értelmezzétek az alábbi tablót:

Gondolkodj, mielőtt megosztasz! A Facebook és a Media Smarts brossúrája ***https://saferinternet.hu/Tippek-segedanyagok-videok/Oktatoknak/Oktatasi-anyagok/Oktatasi-anyagok*** (letöltés ideje: 2020. 02. 24.)

e) Fogalmazzatok meg kortársaitok számára 5 tanácsot a posztolásokkal kapcsolatban! Hogyan tudnák megóvni magukat az online világ veszélyeitől?

f) Készítsetek Sway-bemutatót az elvégzett munkáról! (***https://sway.office.com***)

2. csoport:

a) A **The web we want** című munkafüzet: ***http://saferinternet.hu/upload/content/Web%20WeWant%20tini.pdf.*** A munkafüzet 19-22. oldalának feldolgozása (Akció, reakció, interakció...)

b) Készítsetek rövid videót tanáraitok körében az internet veszélyeiről!

c) Állítsatok össze egy Google-kérdőívet a munkafüzet feladataihoz kapcsolódva, tanáraitok számára!

d) Értelmezzétek az alábbi tablót: A Kék Vonal infografikája ***https://saferinternet.hu/Tippek-segedanyagok-videok/Oktatoknak/Oktatasi-anyagok/Oktatasi-anyagok*** (letöltés ideje: 2020. 02. 24.)

e) Fogalmazzatok meg tanáraitok számára 5 tanácsot arra vonatkozóan, hogy mire figyeljenek oda leginkább a kamaszok internetezése során! Hogyan tudnák megóvni őket az online világ veszélyeitől?

f) Készítsetek Sway-bemutatót az elvégzett munkáról! (***https://sway.office.com***)

3. csoport:

a) A **The web we want** című munkafüzet: ***https://saferinternet.hu/Tippek-segedanyagok-videok/Oktatoknak/Oktatasi-anyagok/Oktatasi-anyagok.*** A munkafüzet 23-25. oldalának feldolgozása (Hogyan lehetsz önmagad a neten?)

b) Készítsetek rövid videót a szüleitek körében az internet veszélyeiről!

c) Állítsatok össze egy Google-kérdőívet a munkafüzet feladataihoz kapcsolódva a szüleitek számára!

d) Értelmezzétek az alábbi videót: A posztolások veszélyei: 3 perc 32 mp-es videó ***https://www.youtube.com/watch?v=5ha0E-oJrOw*** (letöltés ideje: 2020. 02. 24.)

e) Fogalmazzatok meg szüleitek számára 5 tanácsot arra vonatkozóan, hogy mire figyeljenek oda leginkább gyermekeik internetezése során! Hogyan tudnák megóvni őket az online világ veszélyeitől?

f) Készítsetek Sway-bemutatót az elvégzett munkáról! (***https://sway.office.com***)

4. csoport:

a) A **The web we want** című munkafüzet: ***http://saferinternet.hu/upload/content/Web%20WeWant%20tini.pdf.*** A munkafüzet 26-28. oldalának feldolgozása (Részvétel proaktívan... és felelősségteljesen!) A munkafüzet 40-41. oldalának feldolgozása (Mutasd magad – de ne vidd túlzásba!)

b) Készítsetek rövid videót nagyszüleitek körében az internet veszélyeiről!

c) Állítsatok össze egy Google-kérdőívet a munkafüzet feladataihoz kapcsolódva, nagyszüleitek korosztálya számára!

d) Értelmezzétek az alábbi tablót: Az összes online barátodat ismered személyesen? A Safer Internet infografikája ***https://i.pinimg.com/originals/ac/4c/bf/ac4cbfb16a65c27c-19b725cc5302deed.png*** (letöltés ideje: 2020. 02. 24.)

e) Fogalmazzatok meg nagyszüleitek számára 5 tanácsot arra vonatkozóan, hogy mire figyeljenek oda leginkább, mikor unokáik interneteznek! Hogyan tudnák megóvni őket az online világ veszélyeitől?

f) Készítsetek Sway-bemutatót az elvégzett munkáról! (***https://sway.office.com***)

Teleki József munkája

NETEZZ OKOSAN! — PROJEKTTERV

Összefoglalás

A tanulók csoportokban (3-4 fős) dolgoznak.

Informatika órán a diákok megismerkednek a internetes zaklatás (cyberbullying) fogalmával, formáival, jellemzőivel, az áldozattá válás elkerülésének lehetőségeivel, illetve azzal, hogy mit tehetnek baj esetén. A diákok egy zárt Facebook csoportot működtetnek, melyen megosztják egymással a témakörben szerzett ismereteiket, tapasztalataikat, véleményüket.

Munkánk során számítógépet, projektort, interaktív táblát, Windows Office programokat, online adatbázisokat és szótárakat, Facebook, LearningApps (tankocka), Kahoot, Canva, Google alkalmazásokat, Google Drive tárhelyet használunk.

Zárás: Legyen ön is milliomos játék bemutatása, kipróbálása az osztályban, valamint plakátot készítenek az internet veszélyeiről, és ezek elhelyezése az iskolában.

Tantárgyak köre: Informatika

Osztály: Gimnázium 9-10. osztály

Időtartam: 3 X 45 perc

A PROJEKT PEDAGÓGIAI ALAPJAI

Tartalmi követelmények: Kerettantervek 51/2012. (XII. 21.) számú EMMI rendelet 3. melléklete, Kerettanterv a gimnáziumok 9-12. évfolyama számára alapján

Informatika:

- Informatikai eszközök etikus használata.
- Internetes portálok, szöveges és képi információforrások használata. Weboldalak megtekintése, mentése. Szöveg, kép mentése weboldalról.
- Hang-, képanyagok, videómegosztó rendszerek keresése. Elektronikus könyvek keresése, olvasása. Médiatárak keresése, médiumok elérése, használata. Oktatási célú adatbázisok használata. Oktatóprogramok használata.
- Információforrások gyűjtése. A felhasznált források feltüntetése a saját dokumentumban. Az információ hitelességének kritériumai és ellenőrzési lehetőségei. A megbízható források ismerete.
- Keresőkérdések megfogalmazása. Böngészőprogram kezelése, webcímek beírása, linkhasználat, portálkeresés. Kulcsszavas és tematikus keresés. Kereső operátorok ismerete. Keresőkérdések megfogalmazása, értelmezése, pontosítása.
- Az iskolához és a köznapi élethez kapcsolódó problémák megoldásának tervezése és megvalósítása csoportmunkában.

Tanulási célok/tanulási eredmények

Informatika:

- Az informatikai eszközök használatának következményei a személyiségre és az egészségre vonatkozóan.
- Adatvédelmi fogalmak ismerete.
- Az információforrások hitelességének értékelése.
- Szerzői joggal kapcsolatos alapfogalmak megismerése.
- Az infokommunikációs publikálási szabályok megismerése.
- Keresőkérdések alkotása, a keresés eredményének értelmezése, a keresés pontosítása. Információforrások kiválasztása, használata.
- Hatékony információ-keresés, a legfontosabb információk megtalálása, a hiteles és nem hiteles információk megkülönböztetése, kritikus információkezelés, a tartalom-előkészítés publikálásra.
- A feladatok elvégzéséhez szükséges információk azonosítása, meghatározása, megkeresése, felhasználása. A dokumentumok önálló publikálása.
- Online kommunikáció folytatása, csoportmunka végzése egy vagy több résztvevővel. A legújabb két- vagy többrésztvevős kommunikációs lehetőségek, valamint az elektronikus médiumok megfelelő kezelése.
- A legújabb médiainformatikai technológiák használata, önálló és kritikus attitűd kialakítása.

Differenciált oktatás alkalmazása

Sajátos nevelési igényű tanulók

- A gamification módszerének köszönhetően a sajátos nevelési igényű tanulók is megtalálhatják azt a területet, ahol eredményesen működhetnek közre a csoportmunkában és segíthetik a csapat munkáját a projektben.
- Dyslexiások támogatása képekkel kapcsolatos műveletekkel.
- Egyszerűbb, rövidebb, a lényegre koncentráló szöveges források adása.
- Lényeges információk kiemelése képekből, szövegből.
- Figyelemmegosztás képességének gyakorlása több egyidejű információ megadásával.

Tehetséges / Különleges képességű tanulók

- Kritikus gondolkodás fejlesztése.
- Egyéni feladatmegoldási módok választása.
- Lehetőséget adhatunk arra, hogy társaikat tanítsák.

ÉRTÉKELÉSI TERV

Az értékelés időrendje

A projektmunka megkezdése előtt

- Előzetes tudás felmérése
- Kahoot
- Answergarden

Mialatt a tanulók a projekten dolgoznak

- pontok aktivitásért, csoporton belüli munkáért
- rendszerező táblázat

A projektmunka befejeztével

- önértékelés
- csoporttársi értékelés
- „Legyen ön is milliomos” értékelése

Értékelési összefoglaló

A diákok pontokat szerezhetnek a teljesített feladatokért, az elkészített produktumokért.

Projekt megkezdése előtt

A Kahoot segítségével egy előzetes tudásfelmérést végzünk a diákok között. A teszt során a tanulók egymással is versenghetnek, szabadon választott „nick” neveket használva. A Kahoot lehetővé teszi, hogy minden kérdés után azonnali visszacsatolást kapjanak a témában meglévő ismereteikről, illetve tanuljanak az elrontott válaszaikból.

Az Answergarden alkalmazás segítségével egy ötletbörzét tartunk azzal kapcsolatban, hogy mi jut a diákok eszébe az internetes zaklatás kifejezés hallatán. Az alkalmazásban nagyobb méretű betűkkel jelenik meg az a szó, amit többen is írtak.

A projekt során

A diákok a projektben videokat, kisfilmeket tekintenek meg, melyek tanulságát levonva ismerhetik meg az internetes zaklatás (cyberbullying) formáit, megelőzésének lehetőségeit. Internetes kutatást végezve dolgozzák fel az internetes zaklatáshoz kapcsolódó fogalmakat. Zárt Facebook csoportot hoznak létre, ahol kutatásaik eredményét poszt formájában közzéteszik. A csoportok **Tankocka** segítségével Legyen ön is milliomos játékot készítenek egy másik csapat posztja alapján. A kész **Tankockát** szintén a Facebookon teszik közzé. A Canva alkalmazással plakátot készítenek az internetes világ veszélyeiről, a helyes magatartásról a közösségi oldalakon. A plakátokat a Facebookon és nyomtatva az iskola folyosóin is közzéteszik. A produktumok, a projektben végzett munka értékeléséhez ellenőrző listát (áttekintő és értékelő) táblázatot használnak. Az értékelés szempontjait tartalmazó táblázatot a projekt elején megkapják a diákok. Ennek segítségével kísérik figyelemmel, hogy minden feladatot elvégeztek-e.

A projektmunka befejezése

Az önértékelésben szerepet kap a metakogníció, nemcsak azt nevezik meg, mit sajátítottak el a projekt során, hanem azt is, hogyan tanulták meg.

A diákok az önértékelésen túl csoporttársaikat is értékelik. Ez sokszor ösztönzőbb, mint a tanári dicséret. A tanulóknak értékelőkártya segítségével kell kiemelniük a pozitívumokat csapattársuk tevékenységéből.

Az elkészített „Legyen ön is milliomos” játékot a tanulók próbálják ki és értékeljék.

A projekt végén a szerzett pontokat jeggyé alakítjuk.

A PROJEKT MENETE

Módszertani eljárások

1. óra

Idő	Óra menete	Módszer	Tanulói munkaforma	Eszköz
1 perc	A projekt kezdetén a pedagógus röviden ismerteti a projekt témáját és az ezzel kapcsolatos tervezett feladatokat.	Téma megjelölés	Frontális munka	
10 perc	**Kvíz megoldása** az internet veszélyeivel kapcsolatosan. A tanulók a jó válaszokra pontokat kapnak, a pontszám a válasz gyorsaságától is függ. Minden kérdés után meglátják a helyes választ is a tanulók.	Motiváció, meglévő ismeretek előhívása	Frontális-, egyéni munka, feladatmegoldás és ellenőrzés	Kahoot alkalmazás, okostelefon, Internet elérés
3 perc	**Közös szófelhő készítése** A projekt témájáról tartunk egy ötletbörzét azzal kapcsolatban, hogy mi jut eszébe a diákoknak az internetes zaklatás kifejezés hallatán. Az alkalmazásban nagyobb méretű betűkkel jelenik meg az a szó, amit többen is írtak.	Motiváció, meglévő ismeretek előhívása	Frontális-, egyéni munka feladatmegoldás	Answergarden alkalmazás, számítógép, internet elérés
3 perc	Közösen elkésztjük és megbeszéljük az **ütemtervet**, illetve a **projekt értékelési szempontjait**. Fontos, hogy ebbe legyen beleszólása a diákoknak, mert akkor könnyebben elfogadják a határidőket, illetve az értékelési szempontokat.	Motiváció	Frontálismunka Megbeszélés	Számítógép, projektor

5 perc	**Csoportalakítás** Lehet véletlen vagy irányított csoportalakítás. Én a látszólag véletlen csoportalakítást szoktam használni. Egyik megoldás, hogy az interaktív táblán színes lufik rejtik a neveket. Minden csoportnak más-más a színe. A tanulók az interaktív táblán „kidurrantják" a lufit és az adott színű csoportba kerül a benne lévő nevű tanuló. Így a diákok azt hiszik, a gép sorsolta őket össze. Valójában én határoztam meg a csoportok összetételét, ügyelve arra, hogy jobban és gyengébben teljesítő tanulók is kerüljenek egy-egy csoportba.	Motiváció	Frontális- és egyéni munka	Interaktív tábla Számítógép
2 perc	Facebook zárt csoporthoz csatlakozás		Egyéni munka	Okostelefon vagy számítógép Internethozzáférés
10 perc	**Videó megtekintése** Saferinternet – Védtelenül	Új ismeret feldolgozása	Frontális és egyéni munka	https://www.youtube.com/watch?v=zZnBDcYSsa0 számítógép, projektor, internet elérés
10 perc	A zárt Facebook csoportban is elérhetővé tett videóhoz kommenteket kell írniuk a csoportoknak előre kiosztott szerepeknek megfelelően: ▪ lány szerepében: „nem tehetek a történtekről" ▪ fiú szerepében: „én jót akartam" ▪ lány lelkiismeret: „amit megosztottál, az kikerült az ellenőrzésed alól"	Ismeretek rögzítése, rendszerezése, visszaadása. Vita	Csoportmunka	Facebook, internet elérés, okostelefon, számítógép
1 perc	**Video megtekintése** Saferinternet – Really? Biztonságos netezés, másként	Motiváció	Frontális és egyéni munka	https://www.youtube.com/watch?v=7e_vCNWQEfc számítógép, projektor, internet elérés

2. óra

Idő	Óra menete	Módszer	Tanulói munkaforma	Eszköz
1 perc	A projekt folytatásával kapcsolatos tervezett feladatok ismertetése.	Téma megjelölés	Frontális munka	
4 perc	**Videó megtekintése:** DeleteCyberbullying HU Internetes zaklatás: Van kiút!	Motiváció, meglévő ismeretek előhívása	Frontális munka	https://www.youtube.com/watch?v=Yobspa2b81M számítógép, projektor, internet elérés
25 perc	**WIKI-készítés az internetes zaklatásról:** A csoportok 3-4 az internetes zaklatáshoz kapcsolódó, az előző videóban is szereplő fogalmat kapnak. Feladatuk utánanézni a fogalmaknak az interneten. Az elkészített fogalommagyarázatot, képpel illusztrálva, a zárt Facebook csoportban bejegyzésként teszik közzé. Javasolt fogalmak: cyberbullying, kirekesztés, fenyegetés, lángháború, befeketítés, kibeszélés, kiposztolás és csalás, internetes követés, megszemélyesítés, kiberpredátorok, sexting, Catfishing.	Új ismeret feldolgozása	Csoportmunka	Internet elérés, számítógép, okostelefon, Facebook, szókártyák
12 perc	**„Legyen Ön is milliomos”!** A zárt Facebook csoportba közzétett bejegyzések alapján a csapatok „Legyen ön is milliomos”! játékot készítenek a LearningApps (tankocka) segítségével. Minden csapat egy másik csapat által feldolgozott fogalmakhoz készíti a játékot, amit aztán megosztanak a zárt Facebook csoportban.	Ismeretek rögzítése, rendszerezése, visszaadása	Csoportmunka	LearningApps, számítógép, internetes hozzáférés, Facebook

Idő	Óra menete	Módszer	Tanulói munkaforma	Eszköz
4 perc	**Videó megtekintése** Add Friend – Teljes film	Motiváció	Frontális és egyéni munka	https://www.youtube.com/watch?v=wRhFLHwsYF0 számítógép, projektor, internet elérés

3. óra

Idő	Óra menete	Módszer	Tanulói munkaforma	Eszköz
1 perc	A projekt folytatásával kapcsolatos tervezett feladatok ismertetése.	Témamegjelölés	Frontális munka	
4 perc	**Videó megtekintése:** DeleteCyberbullying HU : Internetes zaklatás: Van kiút!	Motiváció, meglévő ismeretek előhívása	Frontális munka	https://www.youtube.com/watch?v=Yobspa2b81M számítógép, projektor, internet elérés
25 perc	**Plakátkészítés**: A csapatok plakátot készítenek a Canva alkalmazás segítségével, amelyet meg is osztanak a zárt Facebook csoportban. A plakáthoz két téma közül választhatnak: ▪ Az internet veszélyei (figyelemfelhívás) ▪ „Hogyan csináld jól”	Új ismeret feldolgozása. Ismeretek alkalmazói elmélyítése, visszaadása	Csoportmunka	Canva alkalmazás, számítógép, Facebook, internet elérés
5 perc	**Játék** Az előző órán elkészített, és megosztott Legyen ön is milliomos játékkal mindenki játszik, majd értékeli a többi csapat munkáját az előre kialakított szempontok szerint.	Ismeretek alkalmazói elmélyítése, visszaadása	Csoport- és egyéni munka	LearningApps, számítógép, internetes hozzáférés, Facebook
5 perc	**Ön- és társértékelés**	Önértékelés	Egyéni munka	

Idő	Óra menete	Módszer	Tanulói munkaforma	Eszköz
3 perc	**Projekt zárása** A tanulók a három órát is értékelik 1-5-ig osztályozva különböző szempontok szerint. A feladatmegoldások során szerzett pontokat összesítjük, és jeggyé alakítjuk az előre megbeszéltek szerint.	Értékelés	Frontális munka	Számítógép, projektor
2 perc	**Video megtekintése:** Virág	Motiváció	Frontális és egyéni munka	https://www.youtube.com/watch?v=KeU3WP08m0U Számítógép, projektor

A PROJEKT RÉSZLETEI

Szükséges készségek

- A témához, problémához való célzott anyaggyűjtés.
- Önálló szövegalkotás.
- Alapvető helyesírási szabályok ismerete, alkalmazásuk a szövegalkotás folyamatában.
- Az interneten megjelenő információk hitelességének kritikus értékelése.
- Böngészőprogramok, keresők használata. Információkeresés az interneten.
- Okostelefon használat, alkalmazások telepítése, törlése.

A projekthez szükséges anyagok és eszközök:

- technológia – hardver
- interaktív tábla, számítógép, okostelefon, internet hozzáférés
- technológia – szoftver

Windows Office programokat, online adatbázisokat és szótárakat, Kahoot, Answergarden, LearningApps (tankocka), Canva, Google, Facebook alkalmazásokat, Google Drive tárhelyet használunk.

Nyomtatott anyagok:

- Értékelő és áttekintő tábla a Facebook bejegyzésekhez, kommentekhez (lásd melléklet)
- Önértékelőlap (lásd melléklet)
- Társértékelőlap (lásd melléklet)
- Legyen ön is milliomos tankocka értékelőlap (lásd melléklet)
- Szókártyák

Segédanyagok, internetes források:

- Videók
- Saferinternet – Védtelenül
  https://www.youtube.com/watch?v=zZnBDcYSsa0
- Saferinternet – Really?
  https://www.youtube.com/watch?v=7e_vCNWQEfc
- Add Friend – Teljes film
  https://www.youtube.com/watch?v=wRhFLHwsYF0
- DeleteCyberbullying HU : Internetes zaklatás: Van kiút!
  https://www.youtube.com/watch?v=Yobspa2b81M
- Virág ***https://www.youtube.com/watch?v=KeU3WP08m0U***
- Saferinternet.hu ***https://saferinternet.hu/Tippek-segedanyagok-videok/Oktatoknak/Oktatasi-anyagok/Oktatasi-anyagok***
- Wikipédia

MELLÉKLET

Legyen ön is milliomos tankocka értékelőlap

Minden kérdés érthető volt?	5	4	3	2	1
Fokozatosan nehezedtek a kérdések?	5	4	3	2	1
Volt olyan feladat, ami gondolkodásra késztette?	5	4	3	2	1
Tetszett a feladat?	5	4	3	2	1

Önértékelés

Mi az, amit megtanult a héten, és már biztosan tud?

8. .....
9. .....
10. .....

Hogyan tanulta meg mindazokat, amiket előbb felsorolt? Minden állításhoz írja oda azokat a számokat, amelyek jellemzőek voltak arra, ahogy azt megtanulta!

11. Jegyzetet készítettem.
12. Megbeszéltem a társammal a csapatból.
13. Megfigyeltem tanáromat, vagy mást, hogy hogyan csinálja.
14. Megkérdeztem a tanáromat.
15. Követtem a leírt utasításokat.
16. Internetet, számítógépet használtam.
17. Megpróbáltam magam megoldani.

A csoporttárs munkájának értékelése

Nekem tetszett a munkádban:

.....

.....

.....

.....

.....

Azért vagyok büszke erre a dicséretre:

.....

.....

.....

.....

ÉRTÉKELÉSI SZEMPONTOK FACEBOOK BEJEGYZÉS ÉS KOMMENTEK

	3 pont	2 pont	1 pont	0 pont
Terjedelem	Eléri vagy meghaladja a megadott terjedelmet.	Nem éri el a megadott terjedelem 2/3 részét.	Nem éri el a megadott terjedelem harmadát.	Nem készült bejegyzés.
Saját megfogalmazás	Teljesen önálló megfogalmazás. A gondolatmenet jól követhető, érthetően fejezte ki magát.	A bejegyzés nem tartalmaz szószerinti másolatot. Ha idéz, annak van célja. Gondolatmenet nehezen követhető.	A bejegyzést részben szó szerint másolta.	Teljes egészében másolat a szöveg.
Tartalom	Tartalmilag hibátlan, tárgyi tévedéseket nem tartalmaz.	Apróbb tárgyi tévedést, hibát tartalmaz	Sok vagy súlyos tárgyi tévedést tartalmaz.	Tartalmilag teljesen hibás.
Források használata	Megnevezte és linkkel is megjelenítette a felhasznált forrást.	A forrásokat úgy nevezte meg, hogy azokból egyértelműen kiderül, honnan, kitől származik az információ.	Hivatkozik forrásra, de az nem egyértelmű (pl.: az interneten találtam).	Nem jelölte, milyen források felhasználásával készítette a bejegyzést.
Helyesírás	Hibátlan.	1-2 olyan hibát tartalmaz, amit a helyesírás ellenőrző program nem javít. Legfeljebb maximum 3 központozási hiba.	4-6 központozási hibát tartalmaz, 1-2 súlyos hiba.	3 vagy több súlyos hibát tartalmaz. Súlyos hibának számít az igekötős igék, a névutós névszók és a tagadószó helytelen írása.
E-nyelv használat	Tudatosan, helyesen használja az e-nyelvet. Képekkel, emotikonokkal színesíti a közlést.	Megjelennek benne az e-nyelvi elemek (emotikonok, rövidítések), de nem tudatos.	Keveredik a szleng és az e-nyelvi elemek (emotikonok, rövidítések) használata.	Nem használja az e-nyelvi elemeket.

1.4 Hogyan lehet egy fiatal IT biztonsági, kiberbiztonsági szakember?

Az informatika szakterületről jelenleg Magyarországon legalább 22 000 szakember hiányzik, erről igen sok kutatás, cikk szól, és számos olyan intézkedés is történt az elmúlt években, ami a hiány megszüntetését, vagy enyhítését célozza[71].

Több olyan szakmai szervezet van, amely vállalta és folyamatosan segíti az iskolákban a pályaválasztást, a fiatal informatikusok mentorálását. Teszik ezt azért is, mert az informatikushiány elsődleges oka az lehet, hogy túl kevés az információ, hogy sokan azért nem mozdulnak el az IT-karrier felé, mert túl keveset tudnak róla.

Sajnos továbbra is makacsul tartja magát az a tévhit, hogy ez a pálya "lányoknak nem való", ami már eleve egy elég széles réteget zár ki, másrészt nem ismerik azokat a feladatokat, amelyeket az informatikusok végeznek, azokat a munkaköröket, melyekhez informatikus végzettség szükséges.

A projekt keretében ennek a megváltoztatására is vállalkoztunk. Ez indokolta azt is, hogy a tanártovábbképzés negyedik moduljában erre a témára fókuszáltunk, kiemelve azokat az informatikai továbbtanulási lehetőségeket, amelyek az IT biztonságra, kiberbiztonságra készítenek fel. A feladat is – melyet a 4. modulban a pedagógusok számára megfogalmaztunk – azt szolgálta, hogy a tanárok készüljenek fel a jelen és jövő informatikai pályáinak megismerésére, és arra is, hogy releváns információkkal segítsék a pályaválasztás előtt álló diákokat.

A negyedik modul feladata tehát a pályaválasztáshoz, az informatikai szakmákhoz kapcsolódik. Azokról a karrierlehetőségekről készítettek bemutató- vagy reklámanyagot a pedagógusok, melyek az informatikai vagy más szakmán belül is elsősorban az IT-biztonsággal, kiberbiztonsággal kapcsolatosak.

1.4.1 Feladatleírás

1. Készítsen prezentációt VAGY szórólapot osztályfőnöki órára, vagy „Pályaorientációs napra"! TÉMA: Hol tanulhatnak tovább azok, akik IT biztonsági, kiberbiztonsági szakemberek szeretnének lenni?
2. A prezentációban mutasson be olyan továbbtanulási lehetőségeket, melyek Magyarországon a kiberbiztonság, IT-biztonság karriercélt szolgálják. Minimum egy képzést részletesen írjon le, annak jellemzőivel együtt.
3. Ha szórólapot készít, akkor arra kérjük, hogy abban foglalja össze röviden, figyelemfelkeltő módon azt, hogy hazánkban hol van lehetőség (és milyen feltételekkel) „etikus hekker" képzésre. Mutassa be, mik a képzés jellemzői (előképzettség, képző intézmény, képzési idő, stb.).

Ezt a feladatot is kiválóan oldották meg a kurzuson résztvevő pedagógusok. A következő oldalakon bemutatjuk két tanár munkáját, melyek felhasználhatók iskolai pályaválasztási napon, osztályfőnöki órán.

71 Az utóbbi egy év kutatásaiból és cikkeiből ajánljuk a szülőknek és a pályaválasztás segítő tanároknak:
https://www.glamour.hu/geletstilus/5-no-akik-megalltak-a-helyuket-az-informatikaban-38334
https://digitrendi.hu/egyre-csak-novekszik-az-informatikushiany-europaban
https://ivsz.hu/oktatas/kutatas-az-informatikus-munkaerohianyrol
https://www.profession.hu/cikk/egeto-informatikushiany
https://digitrendi.hu/ennyit-kerestek-nalunk-2019-ben-az-informatikusok

1.4.2 Tanári megoldások pályaorientációhoz

Fenyvesiné Jászai Lídia munkája

SZÓRÓLAP

ETIKUS HACKER

ISKOLÁK
•
LEHETŐSÉGEK

Képzésről

- A hacker gondolkodásmód megismerése
- A hacker eszközök, és technikák elsajátítása

OE – Óbudai Egyetem - NIK

Tóthova Edita munkája

PREZENTÁCIÓ A PÁLYAVÁLASZTÁSI NAPRA

2. A PEDAGÓGUS TOVÁBBKÉPZÉSI KURZUS KERETÉBEN LÉTREJÖTT KÖZÖS TANÁRI PRODUKTUMOK

A tanártovábbképzési online kurzuson nemcsak egyéni feladatokat oldottak meg a tanár kollégák. Voltak viták, fórum-beszélgetések és közösen megoldott feladatok is, amelyek gazdagíthatják a szülői és tanári megoldási lehetőségeket. A tanárképzés során létrehozott produktumok közül megosztjuk Önökkel a következőket:

- Tematikus gyűjtemény
- A témával kapcsolatban megjelent tíz legjobb könyv

2.1 Tematikus gyűjtemény

A gyűjteményben megtalálhatók azok a tanulmányok, videók, cikkek, további óratervek és feladatok, melyek felhasználhatók a diákok felkészítéséhez, és a szülőknek is segíthetnek a téma megismerésében és az egyéni döntések meghozatalában is.

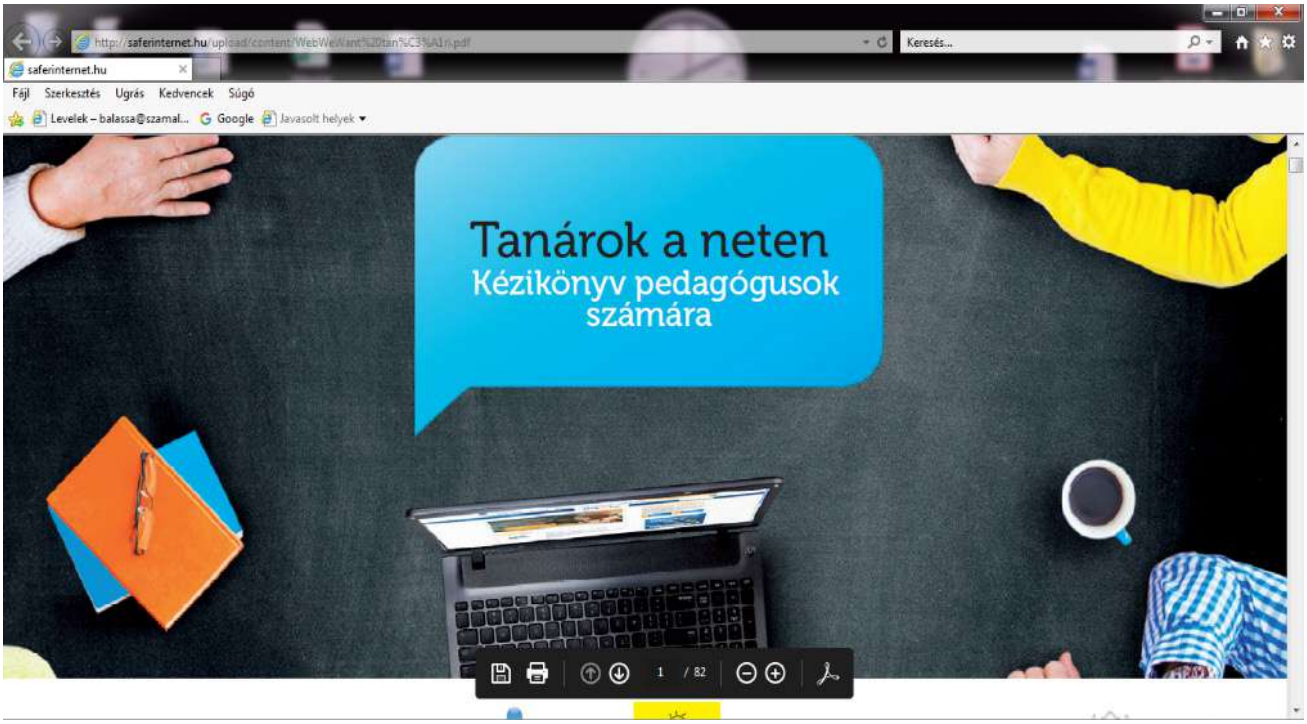
A gyűjtemény célja, hogy olyan szakmai anyagokra, webhelyekre, dokumentumokra hívja fel a pedagógusok és szülők figyelmét, melyek a „digitális biztonsággal", annak tanításával, jogi hátterével foglalkoznak. Ez a gyűjtemény szolgál arra is, hogy felhívja a figyelmet a veszélyekre, azok kezelésére (tanárként és szülőként), továbbá célja az is, hogy bemutassa a kormányzati és civil szervezetek szándékát is a digitális biztonságról való felkészítésre, felkészülésre. A gyűjtemény a tanárok számára kész óraterveket is tartalmaz. Ezek az óratervek különböző korosztályoknak készültek a digitális biztonsággal kapcsolatos témákban, az azokkal kapcsolatos tudás átadására, a digitális térben való felelős magatartás kialakítására.

Ebben a gyűjteményben elsősorban a pedagógusok számára fontos „*digitális biztonság*" témakörben teszünk közzé óraterveket, tananyagokhoz tartalmakat, továbbá a téma tanulói teljesítményértékeléséhez a LearningApps-ban készített feladatokat is átadjuk.

Gondolva a szülőkre is, összegyűjtöttünk olyan tartalmakat, amelyek segítenek a probléma áttekintésében, a veszélyek észlelésében, valamint azok megoldásában is (a megoldáshoz a szakszerű segítség megtalálását is segíteni szeretnénk).

PEDAGÓGUSOKNAK AJÁNLJUK

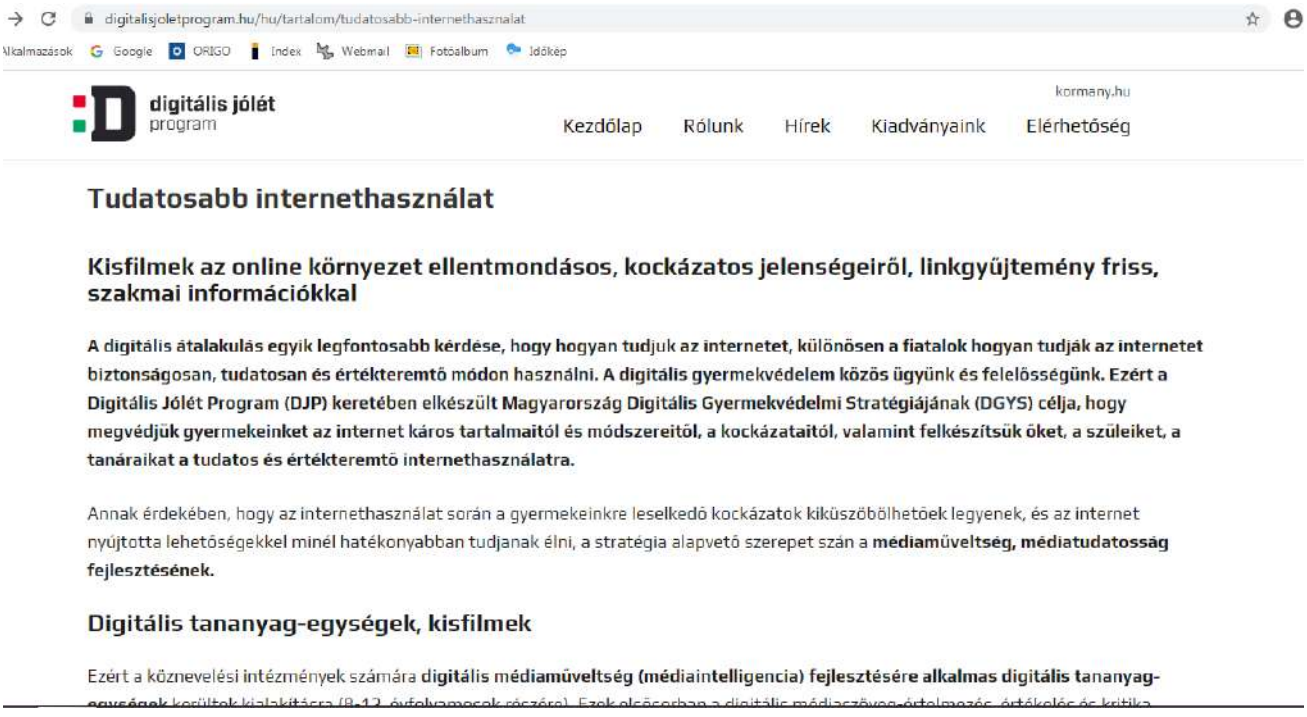
1. TANÁRI KÉZIKÖNYV – Minden tanárnak ajánljuk, ebben több mint 50 olyan óraterv található, melyek a digitális biztonsággal kapcsolatosak. Érdemes kipróbálni!
   https://saferinternet.hu/Tippek-segedanyagok-videok/Oktatoknak/Oktatasi-anyagok/Oktatasi-anyagok



2. IT BIZTONSÁG KÖZÉRTHETŐEN – Egy könyv, melyet érdemes letölteni!
   https://njszt.hu/hu/webform/it-biztonsag-kozerthetoen

3. A DIGITÁLIS VILÁG HATÁSA A GYERMEKEKRE
   A BRUNSZVIK TERÉZ SZAKMAI NAPOK keretében szervezett III. Nemzetközi Kisgyermek-nevelési Konferencia kötete (2019. VÁC)
   http://real.mtak.hu/92172/1/A%20digit%C3%A1lis%20vil%C3%A1g%20hat%C3%A1sa%20a%20gyermekekre.pdf

4. MAGYARORSZÁG DIGITÁLIS GYERMEKVÉDELMI STRATÉGIÁJA
https://www.kormany.hu/download/6/0e/c0000/Magyarorsz%C3%A1g%20Digit%C3%A1lis%20Gyermekv%C3%A9delmi%20Strat%C3%A9gi%C3%A1ja.pdf
5. Hasznos online elérhető tartalmak az internethasználat kockázatainak csökkentésére ANNOTÁLT LINKGYŰJTEMÉNY
https://digitalisjoletprogram.hu/hu/tartalom/tudatosabb-internethasznalat



6. DIGITÁLIS GYERMEKVÉDELEM
https://hintalovon.hu/hu/tanarkent-digitalis-osztalyteremben
7. EGY SZAKDOLGOZAT „AZ INTERNET VESZÉLYEI A FIATALKORÚAKRA” címmel
http://midra.uni-miskolc.hu/document/25672/20958.pdf

8. BIZTONSÁGOS INTERNETHASZNÁLAT (feladatok)
https://learningapps.org/view2104087

9. INTERNBETBIZTONSÁG
http://tanarblog.hu/cikk/internetbiztonsag-itthon-nehany-erdekes-oldal

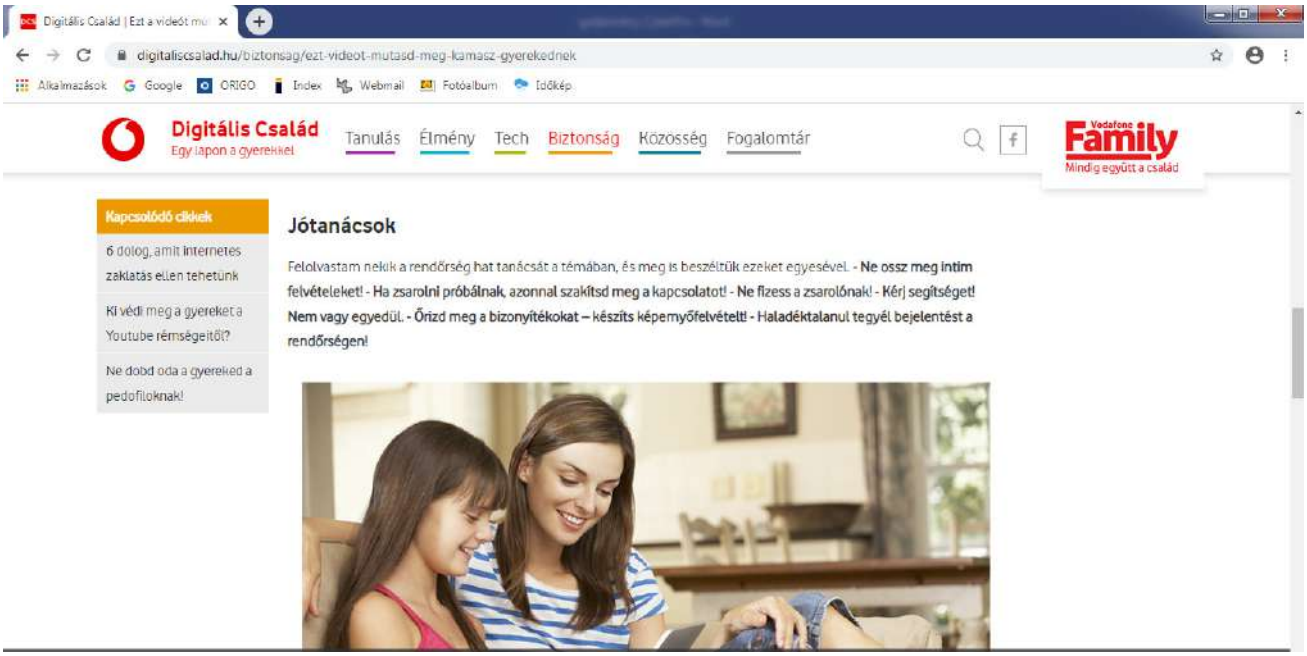
10. DIGITÁLIS BIZTONSÁG, A KORMÁNY KIBERVÉDELMI STRATÉGIAI PROGRAMJA
https://digitalisjoletprogram.hu/hu/tartalom/digitalis-biztonsag
11. RIASZTÁS ADATHALÁSZOK: ***https://www.youtube.com/watch?v=XfyNmro0RUU***
12. DIGITÁLIS ADATVÉDELMI SZABÁLYZAT
A Magyar Köztársaság Országgyűlése Magyarország európai uniós jogharmonizációs kötelezettségeinek teljesítése érdekében megalkotta az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvényt. Az iskolák ezért 2018-tól mára már elkészítették a „Digitális adatvédelmi szabályzatukat, mely az Európai Unió és a Tanács által elfogadott, a személyes adatok védelméről és az ilyen adatok szabad áramlásáról szóló rendeletében, más néven általános adatvédelmi rendeletben (General Data Protection Regulation, rövidítve: GDPR) foglaltak betartásával készült. “
https://www.accessnow.org/cms/assets/uploads/2018/09/GDPR-User-Guide-Digital-Hun.pdf

13. GDPR ÚTMUTATÓ TANÁROKNAK ÉS DIÁKOKNAK
https://www.schooleducationgateway.eu/hu/pub/resources/tutorials/brief-gdpr-guide-for-schools.htm

14. A DIGITÁLIS VILÁG ÚJ VESZÉLYEI
http://www.digitalisvilag.hu/digitalisvilag.php
http://www.mediatudor.hu/bunmegelozes/10_14.html
https://www.youtube.com/watch?v=SuDD6IWoJFw

SZÜLŐKNEK ÉS PEDAGÓGUSOKNAK AJÁNLOTT

1. EZT MUTASD MEG KAMASZ GYERMEKEDNEK!
https://www.digitaliscsalad.hu/biztonsag/ezt-videot-mutasd-meg-kamasz-gyerekednek



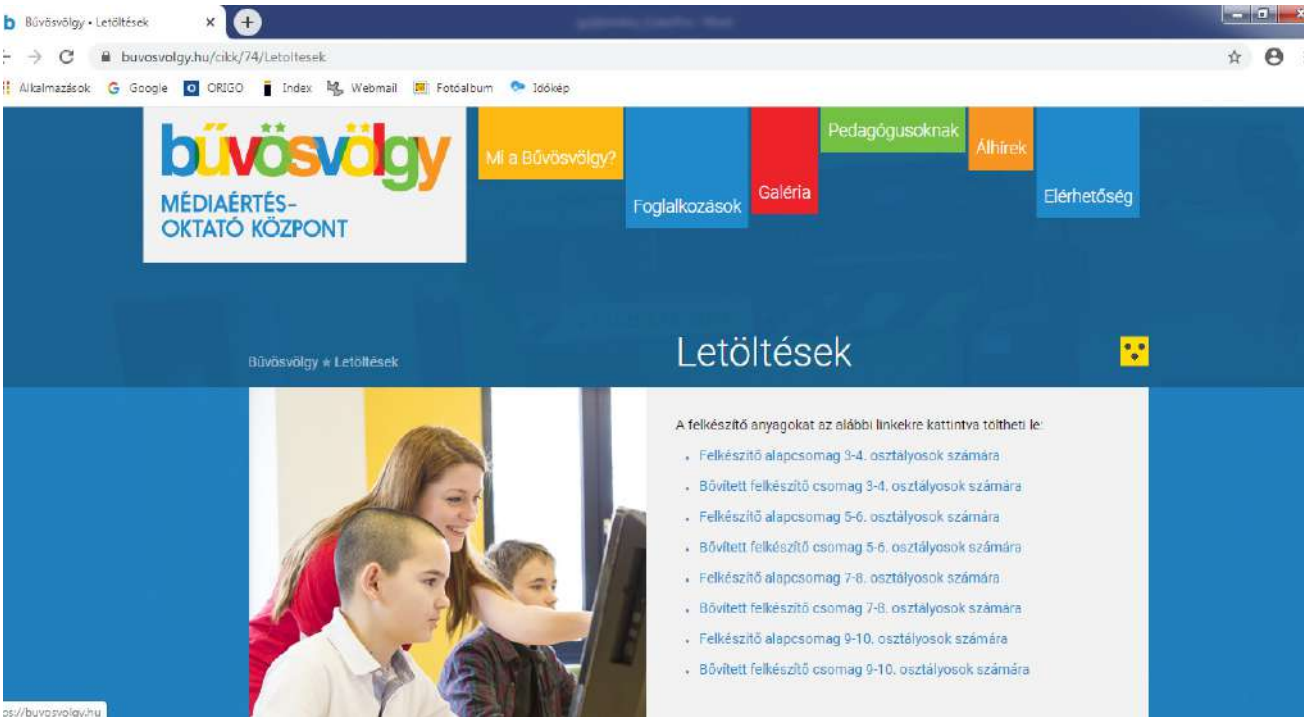
2. DIGITÁLIS SZÜLŐ
https://www.facebook.com/groups/digitalisszulo

3. SOK HASZNOS TANÁCS!
https://mek.oszk.hu/15900/15959/15959.pdf

4. MÉDIAPEDAGÓGIAI PREVENCIÓS PROGRAM
https://televele.hu

5. TARTALOMGYÁRTÓ FIATALOK
Manapság nagy népszerűségnek örvend a kisiskolások körében az internetes tartalomgyártás, és egyre több helyen találkozhatunk a “vlogger” szóval. Mit tehetünk szülőként, ha gyermekünk úgy dönt, hogy belevág a videókészítésbe és az azzal járó feladatokba?
https://www.youtube.com/watch?v=mvCPcXcdxzc

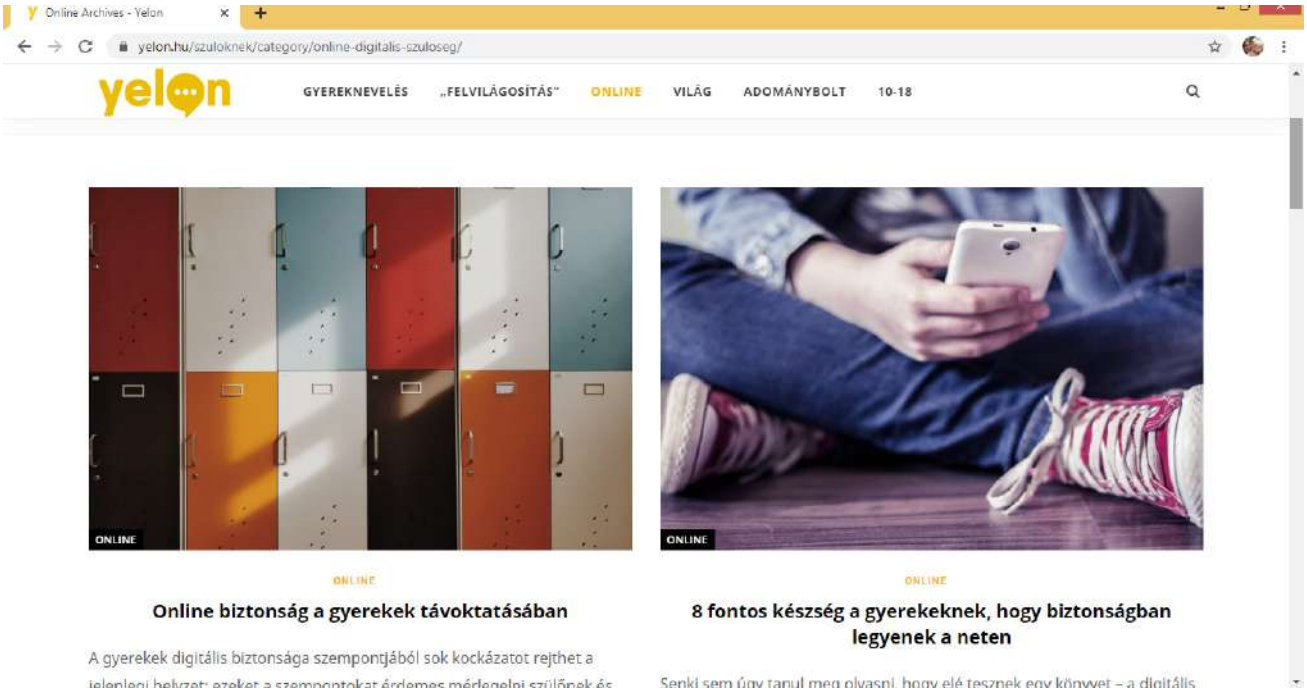
6. Ez nagyon fontos a SZÜLŐKNEK és a PEDAGÓGUSOKNAK
http://buvosvolgy.hu/cikk/74/Letoltesek



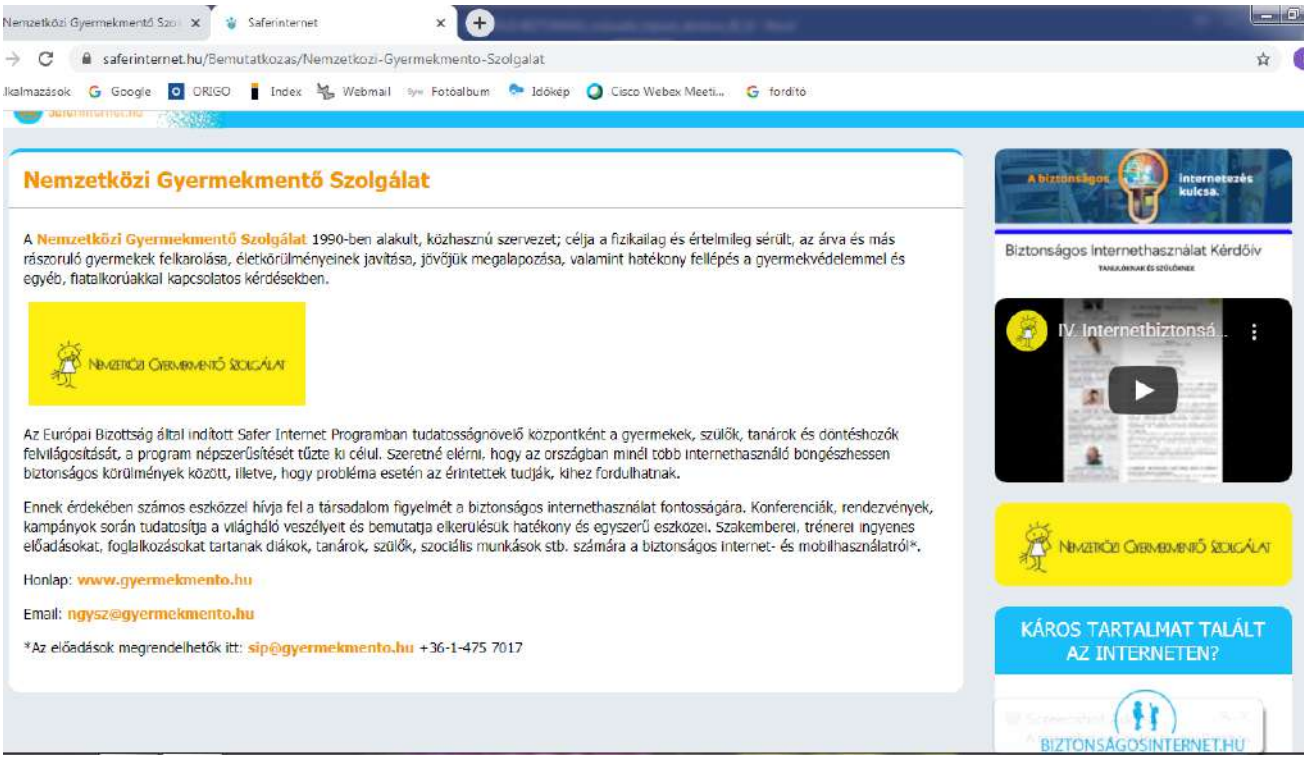
7. SZÓTÁR SZÜLŐKNEK
https://gyerekaneten.hu/

8. A LEGIZGALMASABB 15 FILM A MÉDIA VILÁGÁRÓL! (Ezt látni kell!)
https://panpeterstop.blog.hu/2020/07/27/top_15_film_a_kozossegi_media-rol?fbclid=IwAR074ceE1oaPTa2ZLq-dLjuxGbZjsusFcvBL0vovfnCRaeh3NBPoFLGPVUE

9. KAMASZOK ÉS SZÜLŐK SZÁMÁRA
https://yelon.hu/szuloknek/category/online-digitalis-szuloseg/



10. A SAFERINTERNET HUNGARY ÉS A GYERMEKMENTŐ ALAPÍTVÁNY ÉVES NEMZETKÖZI MÉDIAKONFERENCIÁIN TARTOTT ELŐADÁSOK ANYAGAI
https://www.gyermekmento.hu/tartalmak/hirek/mar-digitalis-formaban-is-elerheto-a-gyermekmento-szolgalat-altal-szervezett-mediakonferenciak-jubileumi-osszefoglalo-kotete--a-kobak-konyvsorozat--digitalis-galaxis-cimu-darabja
https://www.gyermekmento.hu/#conferences-section



2.2 A témában eddig megjelent legjobb 10 könyv a fiatalok számára

A téma megvitatásához, feldolgozásához összegyűjtöttük azokat a könyveket, melyeket érdemes elolvasni, a diákokkal is feldolgozni különböző órák keretében. Minden könyv a veszélyekre hívja fel a figyelmet különböző környezetben kiválasztva azokat a fiatalokat, akikkel megtörténnek a digitális világban olyan dolgok, amelyek tanulságul szolgálhatnak a többi fiatal számára. Érdemes érvelő vitát indítani egy-egy elolvasott könyvről, de más módon is feldolgoztathatják, a lényeg a megértés és a tanulságok levonása.

Könyvajánló

Ismert, hogy nagyon sok olyan helyzet adódik az online úton (*megfélemlítés, zaklatás, adatlopás, internetfüggőség, gyermekpornográfia, vagy épp harc az elmélyüléssel*), mely veszélyt jelent gyermekeink, fiataljaink számára, ezért keresni kell a megelőzés és megoldás módjait, lehetőségeit.

Felhívjuk a figyelmet a következő 10 legjobb kötetre (*regények, szakmai anyagok*, *ismeretterjesztő füzetek*), melyek feldolgozzák napjaink online kihívásait, problémáit!

A védekezés és a megoldás hatásos eszközeit az alábbi könyvekben találjátok:

1. Kevin Mitnick – WILLIAM L. SIMON: A legendás hacker – A megtévesztés művészete
   https://hu.wikipedia.org/wiki/kevin_mitnick
2. Klausz Melinda: Megosztok, tehát vagyok
   https://www.slideshare.net/emkamk/klausz-melinda-megosztseslajkmotivator
3. Nicholas Carr: Hogyan változtatja meg agyunkat az internet? – A sekélyesek kora
   https://hvgkonyvek.hu/konyv/hogyan-valtoztatja-meg-agyunkat-az-internet
4. Patricia Wallace: Az internet pszichológiája
   https://szucscsaba.hu/wp-content/uploads/2013/01/patricia-wallace-az-internet-pszichologiaja.pdf
5. Kalapos Éva: Massza
   https://www.libri.hu/konyv/kalapos_eva.massza-1.html
6. Innes Shona (Varró Dániel fordításában): Az internet olyan, mint a pocsolya
   https://moly.hu/konyvek/shona-innes-az-internet-olyan-mint-a-pocsolya
7. Parti Katalin: Gyermekpornográfia az interneten
   https://bookline.hu/product/home.action?_v=parti_katalin_gyermekpornografia_az_int&type=22&id=82658
8. Kozák Zsuzsanna: A médiáról.
   https://televele.hu/tevekenysegeink/projektjeink/mediaismeret-munkafuzetek-a-buvosvolgy-kiadasaban/
9. Szabó Borbála: Nincsenapám, seanyám.
   https://www.prae.hu/article/9590-mindenki-menekul/

10. Tari Annamária: Y generáció; Z generáció; Generációk online
https://www.lira.hu/hu/antikvar/egyeb_konyveink/yz-generaciok-online-antikvar

ÖSSZEGZÉS

A 21. század felgyorsult fejlődésének egyik hozadéka, hogy életünk szinte minden területére nagy befolyást gyakorolnak a technológiai újítások. Zsebünkben számítógépek tudását bíró telefonokkal járkálunk, és ezek kéznél vannak a nap minden pillanatában. Az információkhoz bárhol azonnal hozzáférhetünk, és meg is oszthatjuk azt másokkal. Társadalmunk egyre elképzelhetetlenebb internet és mobileszközök nélkül. Nem kérdés, hogy mindez alapvetően formálta át életünket, mindennapjainkat, magánszféránkat.

Biztosak vagyunk abban, hogy pedagógusként mindannyian nap, mint nap szembesülünk azzal, hogy fiataljaink idejük nagyobb részében az interneten élik életüket. Itt tartanak kapcsolatot ismerőseikkel (akár a mellettük ülőkkel is), életük fontos részét képezi a közösségi médiában való megjelenés és törekednek arra, hogy ott minél elismertebbek legyenek társaik által. A mindennapokban, de az iskolában felmerülő kérdésekre, problémákra is itt keresik a válaszokat, még akkor is, ha nem pontosan tudják, hogyan tegyék azt. Közösségekhez csatlakoznak, más fiatalokat követnek, s gyakran észre sem veszik, hogy az itt látottak és olvasottak milyen erősen befolyásolják véleményüket, tetteiket.

Éppen ezért fontos, hogy pedagógusként tisztában legyünk a felnövekvő generációkat érő hatásokkal, veszélyekkel, és komfortosan tudjunk mozogni az ő „természetes közegükben". Csak így leszünk képesek megérteni a problémáikat és segíteni diákjainknak, ha szükséges. Valójában ezt a célt tűztük magunk elé ebben a képzésben.

Nem mehetünk el szó nélkül amellett, hogy a minket körülvevő világ a járvány hatására megváltozott, a tanártovábbképzés befejezése előtt gyakorlatilag a teljes magyar oktatás átkerült az online térbe, csak digitális oktatás létezett a tanév végéig.

Azoknak a pedagógusoknak is használniuk kellett az internetet, akik korábban tiltakoztak ellene, és azoknak is meg kellett oldaniuk a digitális oktatást/tanulást, akiknek fizikai vagy hozzáértésbeli korlátaik voltak. Az otthoni munkavégzés, a digitális oktatás és a karantén okozta bezártság megnövelte az online térben töltött időt és a felhasználók számát is. A karantén váratlan „berobbanása", a „helyzet van, amit (péntekről hétfőre) meg kell oldani" érzés feszültsége és a résztvevők (tanárok, diákok és szülők) tapasztalatlansága nagyon sok átgondolatlan döntést eredményezett.

A „mélyvízbe dobott" tantestületek munkájában gyakran semmilyen tudatosság nem volt: olykor minden tantárgyhoz más platformra kellett regisztrálniuk a gyerekeknek, az online térben megtartott órákat nem az eredeti órarendi időpontokban tartották, emiatt ütközések, torlódások fordultak elő. Nagyon gyorsan derültek ki a személyiségi jogi és biztonsági problémák, visszaélések[72] az ingyenes videókonferencia-rendszerek használatával kapcsolatban, ami tovább nehezítette a helyzetet.

Az online térbe helyezett oktatás és feladatmegoldás gyakran extrém mennyiségű tananyagot jelentett a diákok számára, akiknek komoly túlterheléssel és jelentősen megnövekedett számítógép előtt töltött idővel kellett számolniuk – ami természetesen növelte a nem oktatási tartalmak (közösségi oldalak, videómegosztó portálok, online játékok stb.) csábító erejét is.

72 https://qubit.hu/2020/04/01/nagyon-sulyos-biztonsagi-problemak-vannak-a-zoommal-amit-most-a-fel-vilag-kenytelen-hasznalni

Önmagában az online oktatás, ha nincs az intézménynek egy biztonságos, diákok, szülők és pedagógusok számára jól átlátható és használható egységes és zárt felülete (mint pl. a Moodle vagy a Canvas), nagyon sok kérdést vet fel. Például: a hatályos jogszabályok szerint Magyarországon legálisan csak a 16. életévét betöltött személynek lehet saját email postafiókja – holott erre a legtöbb platform használatához szükség van.

Ez alól – ha a tanár, és/vagy a szülők ismerik a lehetőséget – „kibúvót", legális és biztonságos megoldást jelenthet például a Gmail vagy az iPhone családi rendszere, amelyben a szülő hivatalos fiókjához hozhat létre egy kapcsolt „gyermekfiókot", amit korlátokkal, de tud használni a 16 éven aluli tanuló is. A szülőnek rálátása, döntési jogköre van a fiókra (az IOs rendszerében például az alkalmazások letöltéséhez beállítható, hogy a szülőnek – ujjlenyomattal – engedélyeznie kell azt), és számos beállítás odafigyel a gyermekfiókra: például a Google csoporthoz tartozó Youtube-on a gyermek-fiókkal való böngészéskor automatikusan letiltódnak azok a tartalmak, amikre a feltöltő nem kapcsolta be a „gyermekbarát tartalom" jelzést. (Ez szintén eredményezett érdekes helyzeteket az online oktatás során, amikor a tanár a gyermekek számára olyan oktatóvideók megnézését adta feladatul, amelyek a gyermekfiókkal nem voltak elérhetőek.

Természetesen a szülők fiókjával megnézhetők ezek a tananyagok is, de ekkor már semmi sem garantálja, hogy nem kerül olyan tartalom (akár csak reklám formájában![73]) a gyermek elé, ami nem neki való – feltételezve, hogy a szülők saját munkájuk miatt nem tudnak minden pillanatban a gyermek mellett állni az online oktatásban történő tanulás során, megint a gyermekek online biztonsága forog kockán.

A gyermekek biztonsága az online térben mindig is vékony jégnek számított, a karantén és az online oktatás azonban tovább rontott a helyzeten – gondoljunk csak arra, hány gyereknek volt kötelező (!) iskolai platform híján[74] a legális 13 éves életkor betöltése előtt regisztrálnia valamilyen közösségi oldalon, hogy hozzáférjen a tananyagokhoz – ahol aztán, nagy valószínűség szerint nem csupán a tanuláshoz létrehozott csoportot látogatja majd.

A közösségi oldalak a pszichológiai negatív hatásokon túl (énkép, lájkvadászat, bullying, szexting stb.[75]) valós fizikai veszélyt is jelentenek a gyerekekre, elég csak a nemrég kirobbant gyermekpornográfia-botrányra gondolnunk, és csupán néhány cikket[76] elolvasnunk a témában[77].

---

73 Évekkel ezelőtt történt, hogy egy kicsi (3-5 éves) gyerekek számára készült videó közben volt egy reklám, melyben egyértelműen kiderült, hogy a Mikulás nem létezik, a szülők hozzák helyette az ajándékot. Ártalmatlannak tűnik, de ennek a korosztálynak komoly törést is okozhat – és mivel a mese biztonságos, talán nem is először látják, nem biztos, hogy a szülők mellettük vannak. Ugyan az eset messze nem a legrosszabb dolog, ami a gyerekekkel történhet az online térben, mégis jól példázza, mennyire nem lehetünk soha teljesen meggyőződve arról, hogy biztonságban vannak.

74 "A felmérés azt mutatja, hogy a tanárok nagyon sokféle informatikai rendszert használnak, beállítottságtól, életkortól, iskolai szintű előírásoktól függően, így például: Kréta, Google Classroom, Skype, Zoom, Microsoft Teams, email, Discord, Facebook, Google hangouts meet, DC, Bookrclass, Readmenta, Learningapps, Quizlet stb., így más-más csatornákon keresztül küldik a feladatokat, amelyeket követni és rendszerezni kell, hogy a gyermekek egyedül fel tudják dolgozni azokat. A legnépszerűbb a Kréta (63%) és Google classroom (71%), a videókonferenciára 42% használja a Zoomot, 36% a Skype-ot vagy a Teams-t." – részlet az alábbi cikkből: A digitális oktatás első tapasztalatai https://www.mixonline.hu/Cikk.aspx?id=174633

75 https://wmn.hu/ugy/53450-barbie-haz-helyett-brazil-tangas-hatsok (2020.08.29.)

76 https://divany.hu/eletem/2020/07/14/pedofilia-online-ter/ – és Gyurkó Szilvia egyéb írásait is ajánljuk!

77 Mint például ezt a 7 évvel ezelőtt íródottat, ami nem is lehetne aktuálisabb: https://nlc.hu/csalad/20130826/facebook-csalasok/ Néhány mondat a felvezetőjéből: „A Facebook egymilliárd felhasználójának 10 százaléka nem igazi személy. Ez a szürke statisztikai adat akkor válik riasztóvá, ha az ember felfedezi, hogy saját 9 éves lányának is van egy Facebook-profilja. Méghozzá olyan, amiről sem ő, sem a gyerek nem tud, pedig az ő nevével és fotóival az ő életéről szól.

A veszélyek és problémák mellett az is nagyon fontos, hogy pozitív visszacsatolással, kreatív javaslatokkal is találkozhatunk és konkrét fejlesztés-fejlődés is megvalósulhat a digitális oktatás keretében. Ez segítheti a további – a digitális biztonsággal kapcsolatos- feladatok megtervezését, megtanítást és elsajátítását is.

„*Szerintem a tanárok néha erejükön felül próbálnak teljesíteni, a legtöbbet kihozni az online oktatásból is. A középiskolás tanulókat én biztosan több felelősséggel ruháznám fel, többet dolgozhatnának párokban vagy csoportokban, és egymást is mentorálhatnák az alapján, hogy ki melyik tantárgyból jobb, vagy mely témakör áll hozzá közelebb.*"[78]

„Jelenleg egy újfajta tudás jön létre, amelynek meglesz a haszna, és a tapasztalatokat, a módszereket beépíthetjük a jövő oktatásába. Mindannyian jártasságot szerzünk az online tanításban, tanulásban, így könnyebben fogjuk elérni a tanulókat, mint korábban, és a hiányzó diákok is egyszerűbben tudják majd pótolni lemaradásukat. Mindenképpen pozitívum a tanuláshoz szükséges digitális kompetenciák fejlődése, a digitális technológiai eszközök és az infokommunikációs technológiák használatának elterjedése a diákok körében".[79]

A II. fejezetben a pedagógusok véleménye, ismeretei, továbbá az online kurzusban a diákokkal készített felmérés tanulságai alapján arra fókuszáltunk, ami a legnagyobb veszélynek, legfontosabb teendőnek látszik. A fiatalok digitális tudatosságra neveléséhez kívántunk segítséget nyújtani. Azt szeretnénk elérni, hogy a diákok felelősen tervezzék meg digitális lépéseiket, továbbá, hogy amennyiben mégis veszélybe kerülnek, ismerjék a megoldásokat, vagy legalább a segítségkérés lehetőségeit.

Ennek a fejezetnek – valójában az egész könyvnek – az a nem titkolt célja, hogy a digitális biztonság témában történő nevelés és oktatás beépüljön minden iskola pedagógia programjába és a tanrendbe.

A könyv írása közben kialakult élethelyzet fokozottan hangsúlyozta és igazolta ennek sürgető szükségességét. Ehhez kívántunk hozzájárulni a közzétett tartalommal és módszertani ajánlásokkal.

Budapest, 2020. augusztus 30.

78 https://divany.hu/szuloseg/2020/05/25/tavoktatas-digitalis-munkarend-szulok-tapasztalatok

79 A digitális oktatás tapasztalatai egy szakértő szemével. https://www.dszc.hu/informaciok/hirek/2164-a-digitalis-oktatas-tapasztalatai-egy-szakerto-szemevel

Könyvünknek nem titkolt célja,
hogy a digitális biztonság témában történő nevelés és oktatás
beépüljön minden iskola pedagógia programjába és a tanrendbe.

A könyv írása közben kialakult élethelyzet fokozottan hangsúlyozta és
igazolta ennek sürgető szükségességét.
Ehhez kívántunk hozzájárulni a közzétett tartalommal és
módszertani ajánlásokkal

SZÁMALK-Szalézi
Technikum és Szakgimnázium

PROMPT
IT AND SECURITY

BE@CYBERPRO
Fostering cybersecurity careers