|  |
| --- |
| **1. dia** |
|  |
| **Tanórán átadandó információk** |
| **Köszöntő, szerzői információk**  Ön a PÉNZ7 programsorozat kiberbiztonsági tanóráihoz készült tanári útmutatót tartja kezében.    Magyarországon tizenegyedik alkalommal vehetnek részt az iskolák a **PÉNZ7** programban, amely kilencedik éve a tanév rendjébe illeszkedő pénzügyi és vállalkozói és 2025-től önálló kiberbiztonsági témahét. A programsorozat célja, hogy a fiatalok tudatosabban kezeljék pénzügyeiket, megbízható forrásból származó, a hétköznapi életben is hasznosítható ismeretekhez jussanak a gazdaság, a pénzvilág és a digitális biztonság működéséről.    A jelen tanév témái közül a **Digitális lábnyom - Digitális pénztárca című** tananyag célja, hogy segítse és vezesse a pedagógusokat, illetve az órákhoz csatlakozó önkénteseket a **kiberbiztonsági tanórák** megtartásában. Az óravázlatok, prezentációk, mintaóra videók gyakorlati segédanyagként a PÉNZ7 programsorozattól függetlenül, tetszőleges időben és tantárgyi keretek között is rendelkezésre állnak.    A tanári útmutatóban az önkéntesek közreműködésére is találnak javaslatot, ha az órát a pedagógus és a választott szakember közösen vezetik le. Az órák megtarthatók az önkéntesek közreműködése nélkül is, illetve az iskolával kapcsolatot tartó önkéntes szakemberek a későbbiekben is segíthetik a témák feldolgozását, egy, vagy akár több tanóra keretében.    Mivel a PÉNZ7 programsorozathoz csatlakozó iskolák diákjainak felkészültsége, családi és anyagi háttere nagymértékben eltérhetnek egymástól, a pedagógusoknak arra is lehetőségük van, hogy az óravázlatot a helyi viszonyokhoz, a diákok körülményeihez és ismereteihez igazítsák.    FIGYELEM! A tananyag digitális oktatási platformok használatára vonatkozó ajánlásokat is tartalmaz, ezen feladatelemek megvalósítása esetén a diákoknak mobiltelefonjuk vagy egyéb okoseszköz használatára is szüksége lehet.    **A tanári útmutató mellett prezentáció, webinárium és próbaóráról készült filmfelvétel is segíti a felkészülést.**    **Reméljük minden diák nem csak hasznos tudást, de élményeket is szerez az órák végére a személyes adat- és pénzügyi kibervédelem izgalmas világának felfedezése közben. Rendelkezzen mindenki digitális szimattal, hogy okosabb legyen, mint egy kiber-csaló!**    A szervezők nevében üdvözlettel:    **Magyar Bankszövetség**  **BEMUTATKOZÁS, BEVEZETŐ**  Erre a tanórára a PÉNZ7 – Pénzügyi és vállalkozói témahét című program keretében kerül sor.  A PÉNZ7 egy európai kezdeményezés része, amelynek célja, hogy a fiatalok tudatosabban kezeljék pénzügyeiket, többet tudjanak a gazdaság és a pénzvilág működéséről és arról, hogy léteznek internetes csalók, akik mások megkárosítására törekednek  Miközben megbeszéljük majd a mai izgalmas témánkat, Magyarország és sok más ország iskoláiban is ugyanezt teszik a diákok (jelenleg is, illetve az egész héten). |
| **Technikai információ** |
| Ha részt vesz az órán banki önkéntes, mutatkozzon be röviden! (A tanár üdvözölje és kérje fel a bemutatkozásra.) |

|  |
| --- |
| **2. dia** |
|  |
| **Tanórán átadandó információk** |
| **TÉMAFELVETÉS, RÁHANGOLÓDÁS**  Napjainkban Ti, gyerekek is egyre kisebb korban kaptok digitális eszközöket a kezetekbe, már egészen pici kortól találkoztok az internettel és digitális tartalmakkal. Ti most már abba a korba léptek, hogy hamarosan akár önállóan is használtok majd alkalmazásokat, játékprogramokat, üzenetküldő alkalmazásokat és sok más egyéb hasznos és új alkalmazást.  Ráadásul hamarosan tapasztalni fogjátok, hogy az interneten is, ahogy a való életben fizetni kell dolgokért. Ez történhet egy játékban játékpénzzel és történhet valamilyen alkalmazásban igazi pénzzel – de digitálisan.  Ezért a mai órán a digitális lábnyomokkal és a digitális pénztárcával és ezek veszélyeivel fogunk megismerkedni.  **Kérdések:**  **- Kinek van már saját okostelefonja vagy tabletje?**  **- Kinek van már saját közösségi média (Facebook, TikTok, Instagram, Snapchat) fiókja?**  **- Akinek van, az hogyan regisztrált be? (Ezen alkalmazások regisztrációs korhatára 13 év!)**  **- Ki keresett már rá saját magára az interneten?**  **- Mit találtatok?** |
| **Háttérinformációk** |
| **Korai regisztráció:**  Jellemző, hogy a gyermekek a 13 éves korhatárt messze megelőzve, már akár 9-10 évesen is regisztrálnak közösségi média felületekre. Sajnos ebben a szüleik vagy idősebb testvér segítenek jellemzően, a regisztráció során hamis születési adatok megadásával. Ez nagyon rossz példa!  **Korhatár:**  A közösségi média felületek 13 éves korhatárának több oka is van. Az egyik, hogy a gyerekek 13-14 éves korukig **nem tudják megkülönböztetni a fikciót a valóságtól**, az agyuk körülbelül erre a korra érik meg rá. Mivel a közösségi média felületeken rengeteg hamis, szerkesztett, és AI generált tartalom van, a gyerekek nem tudják mi a valóság és mi nem. Ezen kívül rengeteg nem gyerekeknek való tartalom van alapból is: szexualitás, háború, erőszak, trágár szövegek. Ezek összességében károsan befolyásolhatják a fejlődésüket.  **ÓRAI CÉLKITŰZÉSEK:**   1. **Digitális lábnyom:** A gyerekek Frici és Csuka bácsi történetén keresztül megismerkedjenek a digitális lábnyom fogalmával és az internetre feltöltött tartalmak, mint digitális lábnyomok láthatóságával és ennek legkézenfekvőbb veszélyével. Megkülönböztetjük az aktív és passzív digitális lábnyomokat. Megtanuljuk, hogy hogyan lehet csökkenteni a digitális lábnyomunkat. 2. **Digitális pénztárca:** A gyerekek a Pénz7 videóján és a legismertebb internetes játékok (Roblox/ROBUX, Minecraft/MINECOIN, Call of Duty/CP - Call of DUTY POINT, League of Legend/RP – RIOT POINT) virtuális fizetési eszközein, valamint a DiákSzéf alkalmazáson és a bankkártyákon keresztül megismerkednek a digitális pénztárca fogalmával. |

|  |
| --- |
| **3. dia** |
|  |
| **Tanórán átadandó információk** |
| **LÁBNYOMOK A MINDENNAPOKBAN FELADAT:**  Ha a természetben vagy az utcán jártok, akkor ti is láthattátok már, hogy az állatok különböző nyomokat hagynak maguk után. A következő feladatban keressük meg, hogy milyen állatok hagyhatták maguk után ezeket a nyomokat?  **Kérdések, miután megvannak az állatok:**   * Mit tudhatunk meg a lábnyomokból?   + Állat fajtája,  + Mikor járt arra? (Friss a nyom vagy már megszáradt, elmosódott)  + Közlekedés iránya,  + Sérült, vagy sántít-e az állat? (Ilyenkor nem terheli a sérült lábat, nem olyan erős a nyom).  + Mennyire sietett az állat? (Ha szalad, akkor nagyobb a távolság a nyomok között)  + Egyedül volt-e vagy többen voltak? (Kivéve a farkasok a hóban, mert ők egymás nyomában haladnak)  **A lábnyomok a természetben is sok-sok információt hordoznak. Pedig nem is láttuk magát az állatot, de mégis mennyi mindent megtudtunk róla. Hasonló a helyzet az internettel és velünk, internet használókkal.** |
| **Háttérinformáció** |
| (**KUTYA - EMBER)** Az emberi talp leginkább a medve lábnyomára hasonlít. A kutya lábnyoma nagyon hasonlít a hasonló állatok (farkas, sakál) lábnyomához.  **(MEDVE)** Ma már Magyarországon egyre gyakrabban előfordulhatnak medvék. Ha medvelábnyomot találunk a sárban, és friss a nyom (nem száradt meg, nem mosta el az eső, nem szállt bele levél) akkor a medve nemrég járt arra, legyünk óvatosak és tájékozódjunk, hogy érdemes-e továbbmennünk vagy mielőbb érjünk el egy biztonságos menedékházba.  **(DINOSZAURUSZ)** A dinoszauruszok nagyon régen, sokmillió éve kihaltak, de lábnyomaikat helyenként megőrizték az akkor még vizes mocsarak, amelyek ma már megkövesedve látszódnak sziklák oldalain. |
| **Technikai információ** |
| A lábnyomok kattintásra indulnak és kattintásra jelenik meg az állat neve és képe. |
| **4. dia** |
|  |
| **Tanórán átadandó információk** |
| Amikor használunk egy interneten keresztül elérhető alkalmazást például Instagram, TikTok, Időkép stb., vagy meglátogatjuk egy kedvenc zenészünk oldalát, vagy rákeresünk egy játékra akkor AKTÍV és PASSZÍV digitális nyomokat hagyunk magunk után.  Az **AKTÍV** nyomokat saját elhatározásunkból hagyjuk, például egy lájk egy jelzés mindenkinek és az utókornak, hogy az adott tartalom, kép, videó, poszt tetszik nekünk és egyetértünk vagy örülünk neki. Ha feltöltünk magunkról egy nyaralós képet a Balatontól, akkor már maga a kép tartalma és a kép adatai is digitális lábnyomként funkcionálhatnak.  **PASSZÍV** nyomokat már akkor hagyunk, ha felcsatlakozunk az internetre, mivel az internet-szolgáltatónk ilyenkor kioszt egy egyedi címet (Pl. 185.161.73.5 ), amivel az eszközünk (telefon, számítógép, wifi router) azonosítható az interneten. Ez az IP cím (IP – Internet Protocol cím), amely minden weboldalt és alkalmazást üzemeltető számítógép a világ számos részén eltárol, lenaplóz és a későbbiekben ez visszakereshető. Ennek az elkerülésére persze vannak technikák (VPN, TOR hálózat, Proxy szolgáltatások), de ezeket nem most kell megbeszélni is ismertetni.  A másik kritikus PASSZÍV digitális lábnyom (a sok közül) az úgynevezett süti/cookie fájlok. |
| **Háttérinformációk:**  Az alábbiakban egy példa, hogy hogyan magyarázzuk el ezt a két PASSZÍV digitális lábnyomot a gyerekeknek!  **IP cím**: „Képzeld el az internetet egy hatalmas városnak. **Minden háznak van egy egyedi címe**, hogy a pizzafutár pontosan tudja, hova vigye a pizzát. Az interneten a házak helyett számítógépek vannak, és a címük **az IP cím**. Az IP cím egy hosszú számsor, ami megmutatja, hogy hol található a számítógéped a nagy internetes városban.  A **süti/cookie** pedig olyan, mint **egy kis jegyzet**, amit a weboldalakat tároló számítógépek a webes böngészés közben hagynak a számítógépeden. Például, ha bejelentkezel egy játékos oldalra, a süti megjegyzi, hogy ki vagy, így legközelebb nem kell újra beírnod az azonosítódat esetleg a jelszavadat. Vagy ha egy webshopban nézelődtél, a süti megjegyzi, hogy milyen játékokat néztél, és legközelebb hasonló játékokat ajánlhatnak neked.  Tehát:   * **IP cím: A számítógéped vagy telefonod címe az interneten.** * **Süti: Egy kis jegyzet, amit a weboldalak hagynak a számítógépeden, hogy emlékezzenek rád.**   Miért fontosak ezek?   * IP cím: Segít abban, hogy a számítógéped el tudja küldeni és tudja fogadni az üzeneteket az interneten. * Süti: Megkönnyíti a böngészést, személyre szabott ajánlatokat adhat.   **Hogyan tudom csökkenteni a fenti két fajta digitális lábnyomot?**   * AKTÍV: Mértékletesség, ésszel posztolás * PASSZÍV: Privát böngészés, ami egy beállítás a böngésző programokban   Miért érdemes csökkenteni a digitális lábnyomot?  Az internet egy jó dolog, mert rengeteg érdekes dolgot tudhatsz meg pár kattintással, és összeköthet másokkal, de nem csak jó, hanem rosszindulatú emberekkel is találkozhatsz, ezért megfontoltnak kell lenni, ha valamit az interneten csinálsz, nem szabad “ész nélkül” kattintgatni. Ez az első lépés, hogy megtanulj biztonságosan internetezni, amihez még sok mindent meg fogsz tudni idővel. |
| **Technikai információ** |
| A böngésző programokban lehetőség van olyan „**Privát” üzemmódban böngészni**, amely a vagy már eleve meg sem jegyez adatokat, vagy a böngésző bezárása után automatikusan töröl minden adatot maga után a számítógépről (Például böngészési előzmények, mentett adatok és weboldalak, süti fájlok, mentett jelszavak). Ez az üzemmód segíthet a digitális lábnyom csökkentésében.   * **Google Chrome:** Inkognitó mód * **Mozilla Firefox:** Privát ablak * **Microsoft Edge:** InPrivate ablak * **Safari:** Privát böngészés * **Opera:** Privát ablak |
| FELADAT: Keresd meg a telefonod/számítógéped böngészőjében a PRIVÁT módot! |

|  |
| --- |
| **5. dia** |
|  |
| **Tanórán átadandó információk** |
| **BEVEZETÉS:**  Most egy rövid történettel fogtok megismerkedni, amin keresztül megérthetitek, hogy miért fontos a saját digitális lábnyomunkkal foglalkoznunk. A történet Friciről és Fülöpről, a két jóbarátról szól, akik bajba kerülnek az interneten majd ezután Csuka bácsitól, a tapasztalt internetbiztonsági szakértőtől kérnek segítséget.  **FELOLVASÁS vagy VIDEÓ: (kb. 6 perc)**  A csatolt **(Frici\_könyv\_2\_fejezet\_2\_frissített\_verzió)** felolvasása vagy a videó levetítése (Következő dia) |
| **Háttérinformációk** |
| A könyv 2019-ben jelent meg és eredetileg a Facebook szerepelt ebben a fejezetben és fotók, mint digitális lábnyomok. De 2025-ben frissítésre került és a nyomtatott könyv is a PÉNZ7 program keretében újra elérhető lesz.  **Technikai információ** |
| Amennyiben rendelkezésre áll, be lehet mutatni a könyvet fizikai valójában is.  A következő oldalon a videó a képre, majd alul a videó vezérlő indító gombjára kattintva indul: |

|  |
| --- |
| **6. dia** |
|  |
| **Tanórán átadandó információk** |
| Az alábbi videóban Zsomac, az influenszer olvassa fel a „Frici és a virtuális fogkrém” című fejezetet. A videó annyiban több egy egyszerű felolvasásnál, hogy a történetben haladva úgynevezett deepfake videó technológiával változik a mesélő arca, a szerepeknek megfelelően. |
| **Háttérinformációk** |
| **Technikai információ** |
| Bármi miatt a beágyazott videó nem indulna el online a Youtube-on is elérhető a teljes videó, ehhez internetkapcsolatra lesz szükség. |

|  |
| --- |
| **7. dia** |
|  |
| **Tanórán átadandó információk** |
| **TÖRTÉNET FELDOLGOZÁS:**  **Általános kérdések:**   * Hogy tetszett a történet? * Mi fogott meg belőle benneteket?   **Tematizált kérdések (válaszok a dián):**   1. Milyen digitális lábnyomokat hagytak a fiúk az interneten? 2. Miért aggódott Frici a videóval kapcsolatban, amiket a TikTokra feltöltött? 3. Mit mondott Csuka bácsi, miért veszélyes meggondolatlanul képeket feltölteni az internetre? 4. Miért mondta Csuka bácsi, hogy "a fogkrémet nehéz visszanyomni a tubusba"? Mire utal ez? 5. Milyen lehetőségei vannak a közösségi oldalakon, akár TikTok, Instagram, Facebook a képek és videók láthatóságának beállítására? Soroljátok fel őket! 6. + Konklúzió levonása pirossal |
| **Technikai információ** |
| A válaszok kattintásra jelennek meg egymás után. |
| **Háttérinformáció a QR kódok veszélyeiről:**  Nemzeti Kibervédelmi Intézet **QR kódos csalásokat bemutató részletes ismertetője** (26 oldal):  <https://nki.gov.hu/it-biztonsag/elemzesek/qr-kodos-csalasok/> |

|  |
| --- |
| **8. dia (Kihagyható)** |
|  |
| **Tanórán átadandó információk** |
| **CSOPORTOS JÁTÉK: 6 perc**  **//Idő hiányában kihagyható//**  A Szókirakós wordwall játékot közösen is végig tudja vinni az osztály, ilyenkor nem kerülnek a betűk a helyükre, de a megoldást közösen ki tudjuk mondatni a gyerekekkel, megerősítve a fogalmat.  A gyerekek, ha rendelkezésre áll számítógép vagy elég okostelefon, akkor alakítsanak 2-3 fős csoportokat és fejtsék meg a szókirakó feladatait időre.   * 2 fős csoportoknál 3-3 szó rakható ki * 3 fős csoportoknál 2-2 szó rakható ki   Jelre szabad a játékot indítani, a leggyorsabb csapat győz.  Opciók:   * Ha kevés az idő, akkor lehet az első kettő megfejtésig játszani. Mind a 6 rejtvény megoldása akár 5-6 percet is igénybe vehet. * **Ha nincs számítógép vagy telefon a gyerekeknél, akkor az előadó a játékot behívva, a böngészőprogramban közösen is ki lehet találni a feladványokat.** |
| **Háttér információ:** |
| **A szókirakó megoldásai:** 1. képek megosztása 2. videók feltöltése 3. tartalmak lájkolása 4. kommentek 5. blogolás 3. keresési előzmények  A játékhoz nem kell személyes adatokat megadni. |
| **Technikai információ** |
| * A segítő segíthet a gyerekeknek a játék weboldalra navigálásban. * Elakadás esetén a segítő segíthet egy-egy betű helyes helyre húzásában. A sorrendiség nem fontos, a pozíciók a lényegesek. * A játék működik mobilon/tableten és számítógépen is. |

|  |
| --- |
| **9. dia** |
|  |
| **Tanórán átadandó információk** |
| **DIGITÁLIS LÁBNYOMOK – ÖSSZEFOGLALÁS: (2 perc)**   1. Téma: A dián látható képek segítségül szolgálhatnak az **AKTÍV** digitális lábnyom megértésében  * Magyar Labdarúgó Szövetség adatbank – nyilvános adatok a gyermek focistákról. * Maci Laci – Fiktív Facebook profil, nyilvános adatokkal * TikTok videó képe egy póniról és a hozzászólások   Az MLSZ kép kapcsán lehet beszélgetni a hobbiról és az erről internetre felkerülő adatokról, lábnyomokról, hogy ez akár jelszavak kitalálásában is segítheti a támadót. A közösségi média profilokban megadott információk szintén indokolatlanul sokat mutatnak meg belőlünk és hivatkozási indokok lehetnek kapcsolat felvételre.   * Te is ebbe az iskolába jártál? * Te is szereted ezt a filmet? * Te is jártál már Siófokon? * Stb.   **PASSZÍV** digitális lábnyom kapcsán a két legfontosabb az IP cím fogalma, ami alapján a internetre csatlakoztatott eszközök azonosíthatók, valamint a süti (cookie) fájlok, amelyekben számos, a felhasználó böngészéséhez kapcsolódó adat megőrződik.  **Fontos átadni azt az ismeretet, hogy a digitális lábnyomok MINDENKI számára szabadon hozzáférhetőek és azokból könnyen megismerhetőek leszünk. Ez pedig segíthet a bizalmunkba férkőzni! A cél ennek elkerülése.**  A TikTok videó kapcsán **a kommentekről** lehet beszélgetni, amelyek minket minősítenek és lehetnek **kedvesek, jó vagy rosszindulatúak is**. Minket is betámadhatnak ezeken keresztül.  <https://www.youtube.com/watch?v=7NQy2AUqgyU> közösségi média adatok összegyűjtése és személyiség profil alkotás, adatlopás, kártyás csalás (ez magyar nyelvű osztályokban is bemutatható, mert nem a képi világ elég beszédes.)   1. Téma: Közösségi oldalakkal kapcsolatosan el kell mondani, hogy figyelmesen vizsgálják át a gyerekek, akár a szüleikkel, akár pedagógussal közösen a biztonsági és adatvédelmi beállításokat. Ezekről minden közösségi média platformon magyar nyelvű tájékoztatók és útmutatók is elérhetőek, ha valamilyen kérdésre nem egyértelmű a válasz. 2. Téma: A digitális lábnyomunk csökkentése ott kezdődik, hogy nem kerülnek fel rólunk adatok az internetre. Mértékletes posztolás és a talált, de nem szükséges információk törlése, vagy töröltetése is segít csökkenteni a digitális lábnyomunkat. Ezzel minden internetet használó gyermeknek tisztában kell lennie.   Angolos osztályokban az alábbi videók is levetíthetők: |
| **Technikai információ** |
| **Videók angolul:**   * <https://www.youtube.com/watch?v=yrjT8m0hcKU> (Kávézó, add meg a neved, adatok összegyűjtése és pohárra írása. Erős csodálkozás.) * <https://www.youtube.com/watch?v=pj4azlRkJYs> Közösségi média alapvető biztonsági tanácsok |

|  |
| --- |
| **10. dia** |
|  |
| **Tanórán átadandó információk** |
| **TÉMAFELVETÉS, RÁHANGOLÓDÁS**  Az interneten is, ahogy a való életben is, fizetni kell dolgokért. Ez történhet egy játékban játékpénzzel és történhet valamilyen alkalmazásban igazi pénzzel – de digitálisan.  A digitális pénzeket digitális pénztárcában kell tárolni. De vajon mi is az a digitális pénztárca?  A mai órán a digitális pénzzel, a digitális pénztárcával és ezek veszélyeivel fogunk megismerkedni.  **Kérdések:**  **- Milyen módon lehet fizetni vásárláskor?**  **- Ha valaki kap zsebpénzt, akkor milyen formában kaphatja? (Összegre ne kérdezzünk rá!)**  **- Van-e valakinek saját bankkártyája? (Egyes bankoknál már 6 éves kortól lehet igényelni a gyermeknek bankkártyát)**  **- Láttátok-e már, hogy apu vagy anyu hogyan használja a bankkártyáját?**  **- Vett-e már valaki közületek – akár apuval vagy anyuval közösen, valamit az Interneten?**  **- Hogyan történt ez a vásárlás, elsősorban a fizetés része?** |
| **Háttérinformációk** |
| Több magyar bank is biztosít gyerekeknek, diákoknak önálló számlacsomagot, így a számlához a szülő igényelhet bankkártyát is. Egyre terjed a Revolut és a Wise is, ahol kifejezetten a gyerekeknek szóló számlacsomag és bankkártya ajánlatok is vannak. |
| **Technikai információ** |
| - |

|  |
| --- |
| **11. dia** |
|  |
| **Tanórán átadandó információk** |
| **VIDEÓ NÉZÉS** (Pénz7 2024-es jubileumi bevezető videójából kivágott részlet) **(1:19 perc)**  **TÉMAFELDOLGOZÁS:**  **Kérdések a videó és a játékpénzek témakörében:**  **TÉMAFELDOLGOZÁS:**  **Kérdések a videó és a játékpénzek témakörében:**   1. **Kérdés:** Milyen játékokban használt pénzeket ismertek? 2. **Hogyan működik a játékbeli pénz?** A játékokban gyakran van saját pénz, mint például arany, érmék, vagy gemmák, coin-ok. Ezt a pénzt különböző módokon gyűjtheted össze: teljesíthetsz feladatokat, nyerhetsz harcokat, vagy lootolhatsz, ami azt jelenti, hogy különleges tárgyakat találsz vagy nyersz a játék során. A való életben is össze kell gyűjteni a pénzt, ahhoz, hogy el tudd később költeni.   **Mi az a digitális pénz?** Képzeld el, hogy a játékokban használt pénz, a „coinok”, „zsetonok" vagy „érmék”, olyanok, mint a pénz a való életben. A játékban lévő pénzeket is össze kell gyűjteni, majd hasonló dolgokra költheted, mint a való életben, például ruhákat a karakterednek, vagy élelmet, vagy speciális eszközöket, amik segítenek a játékban. A való életben is ugyanígy működik a pénz. |
| **Háttérinformációk** |
| **Fizetőeszközök a játékokban:**   * **Roblox: Robux** A Robux a Roblox játékbeli valutája, amellyel ruhákat, kiegészítőket és játékbeli tárgyakat vásárolhatsz. * **Minecraft: Minecoins** A Minecoins a Minecraft boltjában használható pénznem, amellyel skin-eket, textúra csomagokat és más játékbeli tartalmakat vásárolhatsz. * **League of Legends: Riot Points (RP)** Riot Points a League of Legends pénzneme, amit skinek, hősöket és egyéb játékbeli tartalmak vásárlására használhatsz. * **Fortnite: V-Bucks** A Fortnite-ban használt digitális pénznem, amit az új karakterek, ruhák és egyéb tartalmak vásárlására lehet használni**.** |

|  |
| --- |
| **12. dia** |
|  |
| **Tanórán átadandó információk** |
| **TÉMAFELDOLGOZÁS:**  **Mi az a digitális pénztárca?**   1. **A pénz megjelenési formája:** A való életben az elkölthető pénz lehet készpénz (bankjegyek vagy érmék) és digitális pénz, amit valamilyen digitális eszközön (Digitális pénztárcában) kell tárolni. (bankkártya vagy valamilyen fizetési alkalmazás a legtöbb okostelefonban ezek előre telepítve vannak (Androidon GooglePay, iPhone-on ApplePay,) 2. **3. Miért előnyösebb a digitális pénz és a digitális pénztárca?** - Nem kell a bankjegyekre és apróra figyelni (sérülés, elhagyás). Ha a digitális pénztárcádat elhagyod vagy ellopják könnyen le tudod tiltani. A benne lévő digitális pénzhez nem fér hozzá a tolvaj. 3. **Mire kell ügyelni a digitális pénztárcánál és a digitális pénz használata közben?** Tudatos költés: Mivel a digitális pénz csak a játékban létezik, fontos, hogy jól gondold át, mire költöd. Ne költs el mindent egyszerre, hanem próbálj meg spórolni a fontos dolgokra. 4. **Valódi pénz és játékbeli pénz kapcsolata:**  Fizettetek-e már egy ingyenesen letölthető játékban valami kis extráért (loot, egyedi matricák, könnyebb előrehaladás a játékban, stb.)? Ezeket mikrotranzakcióknak hívják. Ezekkel nagyon kell vigyázni, mert a játékfejlesztők ezt ravaszul azért találták ki, hogy egyenként kis összegért vásároljatok egyedi “apróságokat”, de ha nem figyeltek oda, a sok kis összeg végül sokezer forintot is kitehet a végén. Ha okos vagy, ezekre kevesebbet fordítasz, az interneten sokféleképp kifejezheted az egyéniségedet, a könnyebb előrejutás pedig elveszi a játék igazi izgalmát. A zsebpénzedet ennél sokkal okosabban is el tudod költeni. Ha az osztálytársaid, ismerőseid között ez nagy divat, ne foglalkozz vele, mert Te ezt már tudod, okosabb vagy náluk. Fontold meg mire érdemes költeni és ezt mindig a szüleiddel megbeszélve tedd! |
| **Háttérinformációk** |
| A digitális pénztárcák olyan rendszerek, amelyek biztonságos, alternatív fizetési módot biztosítanak a mobiltelefonokon vagy más eszközökön található alkalmazások segítségével, így szükségtelenné válik a fizetéshez a bankkártyánk elővétele. De biztonságos ennek a fizetési módszernek a használata?  Sok fogyasztó még mindig bizonytalan a válaszban, és pont emiatt – ahogy számos [piaci felmérés is rávilágított](https://fintechzone.hu/kihasznaljuk-a-hazai-digitalis-fizetesi-infrastrukturak-lehetosegeit-reszletek-digitalis-fizetesi-indexben/) – nem merik használni ezt az egyébként már több éve elérhető technológiát. A továbbiakban segítünk jobban megismerni a digitális pénztárcákban rejlő lehetőségeket és annak biztonságos használatával kapcsolatos tippeket osztunk meg.  **Hogyan működik a digitális fizetés?**  Számos mobiltelefon gyártó kínál már pénztárca-alkalmazást. Miután kiválasztottuk a számunkra legszimpatikusabbat, és azt valamilyen biztonságos alkalmazásboltból letöltöttük, általában szükséges egy regisztráció, majd hozzá kell adnunk egy fizetési módot a digitális pénztárcához, ami általában egy bankkártyát jelent, ami lehet virtuális bankkártya is. Ezt követően az alkalmazás hitelesíti a kártyát a kibocsátó banknál, és ezután már használható is az alkalmazás. Amikor fizetést kezdeményezünk, akkor a készülékünk – mobiltelefonunk, okosóránk, stb. – kétféle módon léphet kapcsolatba a kereskedő fizetési termináljával: az úgynevezett MST (Magnetic Secure Transmission – Mágneses Biztonságos Átvitel) vagy az NFC (Near Field Comunication – rövid hatótávú kommunikációs szabvány) nevű technológiák segítségével. A két technológia működési elve eltérő, azonban az közös bennük, hogy közvetlenül továbbítják a szükséges adatokat a fizetési terminálhoz, anélkül, hogy a kártyát le kellene húzni a mágnescsík olvasón, vagy be kellene helyezni azt a kártyaolvasóba.  Biztonságos?   * Igen. Mindkét technológia biztonságos módszert alkalmaz a hatékony adatvédelem érdekében, mivel digitális tokeneket – vagyis virtuális kódokat – használnak. Ezek általában 15-16 jegyű számsorok. Emiatt a saját bakkártya-adataink nem kerülnek tárolásra a telefonon és nem is kerülnek továbbításra a kereskedő részére. Magukat a token-információkat egy úgynevezett token-szolgáltató tárolja – általában egy bank vagy hitelkártya-társaság -, amely az információvédelem érdekében hatékony biztonsági rendszerekkel rendelkezik. Tehát a fizetések során a terminálnak nem adja meg az alkalmazás a bankkártyánk számát, hanem helyette egy egyszer használatos számsort, vagyis tokent generál és csak azt adja át. Ha ehhez még valaki hozzá is fér, akkor – ellentétben a bankkártyán lévő számmal – ez nem használható már fel további vásárláshoz. Ezen felül további biztonsági funkció a titkosítás alkalmazása: a tranzakciók és az adatok is titkosítva vannak. Ráadásul az alkalmazások a tranzakciók jóváhagyása érdekében gyakran követelnek meg biometrikus azonosítást is: ujjlenyomat-azonosítást vagy arcfelismerést, vagy ezek hiányában jelkódot, esetleg kétfaktoros hitelesítést. |

|  |
| --- |
| **13. dia** |
|  |
| **Tanórán átadandó információk** |
| **TÉMAFELDOLGOZÁS:**   * **Elvesztett vagy ellopott eszközök**   Ha a telefonodat vagy számítógépedet elhagyod vagy ellopják, azzal a digitális pénztárcád is veszélybe kerülhet. Ha valaki hozzáfér az eszközödhöz, amelyen a digitális pénztárca van, akkor megláthatja és elérheti a pénzedet is.  **Mit tegyél, hogy elkerüld az ilyen helyzeteket?** Mindig figyelj oda az eszközeidre, és ha elveszíted vagy ellopják, azonnal értesítsd a szüleidet, akik segíthetnek a problémák megoldásában. Érdemes olyan alkalmazásokat használni, amelyek lehetővé teszik az eszköz távoli lezárását vagy adatainak törlését. Az okostelefonok tartalmát - beleértve a digitális pénztárcát is- távolról törölni lehet. Ezen kívül lehetőség van akár egyes alkalmazások elindítását is külön jelszóhoz vagy PIN kódhoz, arcfelismeréshez kötni. Érdemes ezt beállítani a digitális pénztárca funkciót betöltő alkalmazásokra.    **2. Jelszóvédelem hiánya**  Ha a jelszavad nem elég erős, vagy ha azt mások könnyen kitalálhatják, akkor könnyen hozzáférhetnek a digitális pénztárcádhoz. Ha például a jelszavad "123456" vagy a kedvenc állatod neve, amit könnyen kitalálhatnak, akkor mások könnyen beléphetnek a fiókodba.   * **Mit tegyél, hogy ez ne történhessen meg?** Használj erős jelszót, ami nem könnyen kitalálható, például nagybetűkkel, kisbetűkkel, számokkal és szimbólumokkal kombinálva. Minél hosszabb, annál erősebb! Még jobb, ha egy jelmondatot választasz, amire könnyen tudsz emlékezni, például:**”Alig.váromhogyp1zzázzunk”** Soha ne oszd meg a jelszavad senkivel, és tárold biztonságosan! Még az osztálytársakkal vagy a legjobb barátoddal sem! * **Kiberbűnözés és csalások**   Kiberbűnözés és csalások akkor történnek, amikor valaki megpróbálja ellopni a pénzedet az interneten keresztül. Sajnos a világ tele van rosszindulatú emberekkel, akik nem nézik, hogy gyermek vagy felnőtt pénzét lopja el. Az adathalászat során a kiberbűnözők lemásolják a bankok, játékoldalak és más szervezetek weboldalainak a belépési felületeit (Lásd a dián a Fortnite és MBH Bank hamis weboldalát) abból a célból, hogy a felhasználó itt próbáljon belépni és a megszerzett belépési adatokkal a támadó megszerezze az áldozat személyes adataidat és a pénzét.   * **Mit tegyél, hogy te ne ess áldozatul?**   + Ne kattints olyan linkekre vagy üzenetekre, amik gyanúsak, ismerősöktől, vagy ismeretlenektől jönnek.  + Mindig ellenőrizd, hogy tényleg az küldte az üzenetet, aki a levélben vagy üzenetben mondja magát.  + Soha ne add meg automatikusan se e-mailben, se weboldalon, de telefonbeszélgetésben sem a személyes-, vagy bankkártya adataidat.  + Ha ilyet kér egy oldal, akkor előtte győződj, meg hogy biztonságos! Szólj valamelyik szülődnek és együtt döntsétek el, hogy megadhatóak-e a kártyaadatok.  + Ha internetbankba, vagy a digitális pénztárcádhoz kapcsolódó weboldalra kell belépni, mindig ellenőrizd le a weboldal címét! Már egy betű eltérés is csaló oldalra vihet!  + Ha furcsaságokat tapasztalsz egy olyan üzenetben vagy weboldalon, ami a digitális pénztárcádba vagy mobilbankodba történő belépésre szólít fel, akkor előbb ellenőrizzétek le közösen a szüleiddel az oldal megbízhatóságát! |
| **Háttérinformáció** |
| Érdemes a www.kiberpajzs.hu oldalon megmutatni, hogy milyen egyéb internetes pénzügyi csalások vannak.  Ezenkívül a telefonok távoli nyomon követésére és az adattörlésére érdemes felhívni a szülők figyelmét:  Google:  <https://support.google.com/accounts/answer/6160491?sjid=13179928872757886525-EU&hl=hu#app&zippy=%2Cuse-the-find-my-device-app%2Cerase-reset-or-remove-your-device%2Ca-k%C3%A9sz%C3%BCl%C3%A9kkeres%C5%91-alkalmaz%C3%A1s-haszn%C3%A1lata>    Apple:  <https://support.apple.com/hu-hu/guide/icloud/mmfc0ef36f/icloud> |

|  |
| --- |
| **14. dia** |
|  |
| **Tanórán átadandó információk** |
| **TÉMAFELDOLGOZÁS (Opcionális)**  Ahogyan az imént megbeszéltük, nem csak fizikai vásárlás során (pl. boltban), hanem online környezetben is használhatjuk a kártyánkat.  1. Engedélyezzük vagy kérjük azt a lehetőséget, hogy szöveges üzenetben (SMS-ben), alkalmazásban (push üzenetben) vagy e-mailben értesítést kapjunk a számlánkat vagy kártyánkat érintő műveletekről (műveletmegfigyelés)!  2. Használhatunk webkártyát, ami egy olyan (jellemzően virtuális) kártya, amit speciálisan csak online vásárlásokra szokás (vagy csak arra lehetséges) alkalmazni. Eseti jelleggel tölthetjük fel a vásárláshoz éppen szükséges összeggel, így legrosszabb esetben is csak az ezen a másodlagos kártyánkon lévő összeget veszíthetjük el.  3. Az erős ügyfélhitelesítésnek kettő vagy több olyan elemen kell alapulnia, amelyek az ismeret, a birtoklás és a biológiai tulajdonság kategóriába sorolhatók. Ez azt jelenti a gyakorlatban, hogy például minden kártyás online vásárlásnál a hitelesítéshez a kártyához tartozó kód (CVV/CVC kód – Card Verification Value/Code) megadásán túl meg kell erősíteni a tranzakciót pl. egy SMS-ben vagy mobilbanki applikációban érkező kódda, vagy arcfelismeréssel, vagy ujjlenyomat megadással.  4. Az egyes bankkártyák használatát különböző tranzakciós limitek beállításával tudjuk korlátozni. Pl. internetes vásárlás napi maximum 30 000,- Ft értékben, készpénzfelvétel napi 5.000-Ft értékben.  5. Gondoskodjunk a szoftverek frissítéséről és a megfelelő vírusvédelemről, továbbá az eszközeinken az automatikus zárolás beállításáról, különösen az online bankolásra használt számítógépünkön vagy okostelefonunkon. |

|  |
| --- |
| **15. dia** |
|  |
| **Tanórán átadandó információk** |
| **A Mesterséges Intelligencia (MI**) olyan, mint egy **nagyon okos számítógép**, amely **megpróbál úgy gondolkodni, mint az emberek**. Képzeld el, hogy van egy robot, ami tud tanulni, és minél többet gyakorol, annál ügyesebb lesz! Például, ha megmutatsz neki sok képet cicákról és kutyákról, idővel felismeri, melyik a cica és melyik a kutya. Vagy egy másik példa, amikor beszélsz a telefonodhoz, és az megérti, amit mondasz, mert a mesterséges intelligencia tanulta meg, hogyan értse meg az emberi beszédet.  Az MI segít a játékokban, az internetes keresésekben, és sok más dologban is, ami megkönnyíti az életünket.  A Mesterséges Intelligencia (MI), a digitális pénz és a digitális bankolás úgy kapcsolódnak egymáshoz, hogy az  MI segít abban, hogy az emberek gyorsabban és biztonságosabban tudják használni a pénzüket a telefonjukon vagy számítógépükön keresztül.  Az **MI-alapú ügyfélszolgálati chatbotok és virtuális asszisztensek** gyorsan és hatékonyan tudnak válaszolni az ügyfelek kérdéseire a nap 24 órájában.  Az **MI képes gyorsan felismerni a szokatlan tranzakciós mintákat** és potenciális csalásokat az adatok elemzésével, amely segít a banknak megelőzni a pénzügyi visszaéléseket."  **Digitális pénz:** Ez olyan pénz, ami nem papír formában van a kezedben, hanem a telefonodon vagy számítógépeden. Például, ha vásárolsz egy játékot az interneten, digitális pénzzel tudsz fizetni.  **Digitális bankolás:** Ahelyett, hogy elmennél a bankba, otthonról is tudod használni a pénzedet, például telefonon keresztül. Az MI segít a bankoknak abban, hogy gyorsabban tudjanak dolgozni, és megvédje a pénzedet, ha valaki rossz szándékkal akar hozzáférni. |
|  |

|  |
| --- |
| **16. dia** |
|  |
| **Tanórán átadandó információk** |
| A **kriptovaluta egy olyan digitális pénz**, ami nem papírból vagy fémből van, hanem az interneten létezik. Képzeld el, hogy van egy játékpénz, amit csak online tudsz használni, és nem egy bank kezeli, hanem számítógépek sokasága. Az emberek úgy használják, mint a hagyományos pénzt: vásárolhatnak vele dolgokat, de nem kell hozzá bank. Vagy azért veszik, hogy ha később többet fog érni, akkor eladják.  A **blokklánc** **(blockchain), ami olyan, mint sok hatalmas füzet.** Ebben a füzetben minden egyes pénzmozgás (amikor valaki fizet valakinek kriptovalutával) le van írva, de nem lehet kitörölni vagy megváltoztatni, hiszen **azt minden** **egyes füzetben végre kellene hajtani**.  Mindenki, aki kriptovalutát használ, hozzáfér ehhez a füzethez, így mindenki láthatja, hogy milyen fizetések történtek, de az emberek személyes adatai titokban maradnak.  **A blokklánc azért fontos, mert segít abban, hogy senki se csalhasson, és mindenki biztos lehessen benne, hogy a pénz valóban ott van, ahol lennie kell.** |
|  |

|  |
| --- |
| **17. dia** |
|  |
| **Tanórán átadandó információk** |
| **ÖSSZEFOGLALÁS** |
| **1. Mi az a digitális pénz?**   * Digitális pénz: Olyan pénz, amit nem tudtok kézzel megfogni, mint a papírpénzt vagy az érméket. Ez a pénz online létezik, és számítógépek, telefonok, bankkártyák segítségével tudjátok használni. * Példa: Ha a szüleitek interneten vásárolnak valamit, vagy egy játékban virtuális tárgyakat vesznek, akkor digitális pénzt használnak.   **2. Mi az a digitális pénztárca?**   * Digitális pénztárca: Ez egy applikáció vagy program a telefonon vagy a számítógépen, amelyben a digitális pénzt tarthatjátok. Olyan, mint egy valódi pénztárca, csak online formában. * Példa: A szüleiteknek lehet ilyen pénztárcája, amikor az interneten fizetnek vagy bankkártyával vásárolnak.   **3. Hogyan védhetjük meg a digitális pénztárcánkat?**   * Soha ne adjátok meg senkinek a jelszavaitokat vagy a bankkártyátok adatait. * Mindig kérdezzétek meg a szüleiteket, mielőtt valamit vásárolnátok egy weboldalon, hogy az biztonságos-e. * Használjatok hosszú jelszavakat, és ne írjátok le őket nyilvánosan elérhető helyre.   Mindig kérdezzétek meg a szüleiteket, mielőtt új applikációt töltenétek le, ami pénzt vagy bankkártya adatot kér . Ezt nem szabad könnyelműen kezelni!**\*\*\*\* Kiegészítő kérdések:**  **Miért hasznos a digitális pénz?**   * Gyors és kényelmes, nem kell mindig magatokkal hordani pénzt. * Könnyen nyomon követhetitek, hogy mennyit költöttetek. * Biztonságos is lehet, ha megfelelően használjátok.   **Hogyan működik a digitális pénz használata?**   * Ti is találkozhattok vele, amikor online boltokban, játékokban vagy applikációkban használtok pénzt. Egyre több helyen lehet így fizetni. * A bankok, kártyák vagy telefonos applikációk segítenek abban, hogy biztonságosan tudjatok vásárolni.   **Milyen veszélyei vannak?**   * Adathalászat: Hamis üzenetek vagy e-mailek, amikkel valaki másnak adja ki magát (például rendőrség, adóhivatal, vagy bank) megpróbálja megszerezni a jelszavaitokat vagy pénzeteket az interneten. A lényeg az, hogy hogy senkinek ne adjátok meg a jelszavaitokat, még a tanároknak sem, kizárólag a szüleiteknek! * Soha ne töltsetek le applikációt (Anydesk, Teamviewer), azért, hogy banki vagy egyéb ügyintéző „segítsen” ezen keresztül. Valójában ez csalás és a telefonotok vagy számítógépetek feletti irányítást akarják így megszerezni. * Túl sok költés: Könnyen elfelejthetjük, hogy mennyi pénzt költöttünk el, ha nincs előttünk kézzelfogható pénz. A digitális pénznél fontos, hogy mindig figyeljétek, mennyit költötök. * Hamis weboldalak és csalások: Olyan oldalak is léteznek , amelyek azt állítják, hogy biztonságosak, de valójában pénzt akarnak lopni tőletek . Meg kell tanulni felismerni az ilyen veszélyeket. |
|  |
| **Technikai információ** |
| Mit tehetünk a digitális pénztárcánk védelme érdekében?  Ahogy a kiberbiztonság más témáira is igaz, mi magunk tehetjük a legtöbbet a saját digitális pénztárcánk biztonságáért. Ehhez szeretnék az alábbi hat tippet adni:   * Védjük az okostelefonunkat vagy okosóránkat jelszóval, ujjlenyomattal vagy egyéb biometrikus hitelesítéssel! * Ne használjunk nyilvános Wi-Fi szolgáltatást az érzékeny, védendő adataink eléréséhez, mivel ez könnyű lehetőséget teremt a hackereknek ahhoz, hogy hozzáférjenek adatainkhoz! * Legyünk gyanakvók a rosszindulatú szoftverekkel szemben. Számos digitális fizetési alkalmazás létezik, azonban csak hivatalos alkalmazásboltból (Google Play, AppStore) forrásból töltsünk le alkalmazásokat! * Óvatosan a játék alkalmazásokkal! * Legyünk éberek! Amikor okostelefonunkat használjuk, kerüljük a szövegekben vagy e-mailekben található véletlenszerű linkekre való kattintást. Az üzenetek küldője sokszor szándékosan szeretné azt elérni, hogy az általa küldött linkre kattintsunk, és ezzel egy rosszindulatú kódot töltsünk le. * Használjuk telefonunk biztonsági funkcióit, és tartsuk azokat frissítésekkel naprakészen: ez az első védelmi vonal az adataink és a hackerek között. * Tartsuk szemmel digitális fiókjainkat. Csakúgy, mint a csekkek és bankkártyák használatakor, figyeljük a bank- és hitelkártya-kivonatokat, és azonnal jelentsünk minden gyanús tevékenységet. |

|  |
| --- |
| **18. dia (Kihagyható)** |
| A képen szöveg, Grafikus tervezés, képernyőkép, poszter látható  Automatikusan generált leírás |
| **Tanórán átadandó információk:**   * Most pedig nézzük meg a Nemzeti Kibervédelmi Intézet mini képregényét! Figyelmesen olvassátok el, hogy mit mondanak a szereplők! |
|  |
| **Háttérinformáció:**  A Nemzeti Kibervédelmi Intézet képregénysorozatot készített, amelyet a 2024-es Kibervédelmi hónap keretén belül mutatott be a honlapján. Ez a képregény a csaló linkekre hívja fel a figyelmet. |

|  |
| --- |
| **19. dia (Kihagyható)** |
| **A képen szöveg, Emberi arc, ruházat, személy látható  Automatikusan generált leírás**  **Tanórán átadandó információk:**  **n/a** |
| **Előfordul, hogy olyan SMS vagy e-mail üzenet érkezik a telefonra, amiben egy nyereményről érkezik értesítés vagy, ami még gyakoribb, az szerepel az üzenetben, hogy egy rendeléssel kapcsolatban kérnek teendőt vagy épp valami fenyegető dolog, például, hogy nincs befizetve egy számla. Ilyenkor a gyermekeknek a szüleikhez kell fordulniuk, akik el fogják tudni dönteni, hogy a megkeresés valós-e. Jó, ha tudják, hogy még ha valós problémáról is lenne szó, azt nem az üzenetben lévő linkre kattintva kell elintézni, hanem utána kell nézni (weboldalon vagy telefonálni kell).** |

|  |
| --- |
| **20. dia (Kihagyható)** |
| A képen szöveg, rajzfilm, Grafikus tervezés, Emberi arc látható  Automatikusan generált leírás |
| **Tanórán átadandó információk:**   * Jegyezzétek meg a kis robot intelmét!   **Kérdés:** - Mire hívta fel a figyelmet? |
| * **A kéretlen hivatkozásokra nem szabad rákattintani!** * **Ha fenyegető, rossz érzést keltő üzenetet kaptok, nem kell megijedni, csupán töröljétek vagy szóljatok a szüleiteknek, akik segítenek értelmezni, hogy miről van szó!** * **Nincs olyan dolog, aminek ne lehetne utánanézni a linkre való kattintás nélkül, akár számlabefizetés vagy banki téma, akár egy másik szervezettől érkezett az üzenet - látszólag. Például ha egy bank üzent, lépj be a bank hivatalos weboldalán, vagy az alkalmazásba, ott biztosan találsz plusz információt. Végső esetben fel is hívhatod a bankod ügyfélszolgálatát további információért.**   **Tudj meg minél többet a témáról!** |

|  |
| --- |
| **21. dia** |
|  |
| **Tanórán átadandó információk** |
| További pénzügyi tudatossági információkért lájkoljátok a PÉNZ7 Facebook oldalát és keressétek fel a penz7.hu honlapot! **Játszatok a DIGITÁLIS SZIMAT KIHÍVÁS kvízjátékkal!** |

|  |
| --- |
| **22. dia** |
|  |
| **Tanórán átadandó információk** |
| Köszönöm a figyelmet! |

**KIEGÉSZÍTŐ TUDÁSTÁR**

**Játékok a digitális lábnyom, személyes adatok témakör ismereteinek megerősítésére.**

* <https://wordwall.net/hu/resource/34481213> Internet veszélyei - fontos információk rólam
* <https://wordwall.net/hu/resource/54213613> - Fontos adatok rólam! (Személyes adatok ismerete)
* <https://wordwall.net/hu/resource/64622341> - Pozitív és negatív digitális lábnyomok
* <https://wordwall.net/hu/resource/27242926> - Digitális lábnyom szókirakó (az órán szerepel)

**TOVÁBBI OLVASNIVALÓK DIGITÁLIS LÁBNYOM TÉMÁBAN:**

* Hintalovon Gyermekjogi Alapítvány – Mit jelent a digitális lábnyom?

<https://www.youtube.com/watch?v=_XxKyeuwQjA>

* Námesztovszki Zsolt – Tudatos és biztonságos internethasználat – A digitális lábnyom

<https://www.youtube.com/watch?v=BpCKSQCHjG8>

* Erdély TV - A digitális lábnyom – Lexikon

<https://www.youtube.com/watch?v=htljk4COwgY>

* Mi az a digitális lábnyom és milyen veszélyeket rejt a közösségi médiában?

<https://www.quadron.hu/blog-9>

* Infokommunikáció – Digitális lábnyom

<https://nat2012.nkp.hu/tankonyv/informatika_6/lecke_02_007>

**További olvasnivalók, cikkek ONLINE PÉNZTÁRCA és PÉNZÜGYEK**

* Pénzügyi tudatosság gyerekeknek

<https://megtakaritasgyerekeknek.hu/penzugyi-tudatossagra-neveles/>

<https://elemzeskozpont.hu/penzugyi-tudatossag-gyerekeknek-8-fontos-szempont>

* Nemzeti Kibervédelmi Intézet:

<https://nki.gov.hu/it-biztonsag/tanacsok/a-biztonsagos-digitalis-penztarca-hasznalat/>

* A digitális pénztárcák előnyei a magyar felhasználók számára

<https://www.munchen.hu/a-digitalis-penztarcak-elonyei-a-magyar-felhasznalok-szamara>

* MNB - Elektronikus pénztárca

<https://www.mnb.hu/fogyasztovedelem/bankkartyak/bankkartya-tipusok/mi-az-elektronikus-penztarca>

* Bankaroo - Digitális bankolás applikáció gyerekeknek (angol)

<https://bankaroo.com/>

**Angol nyelvű videók:**

<https://www.youtube.com/@Bankaroo-lk5ec> Kávézó, lájkolás, adatok felírása a pohárra, személyes adatok védelme

<https://www.youtube.com/watch?v=F4WZ_k0vUDM> Sharenting és következményei

<https://www.youtube.com/watch?v=7NQy2AUqgyU> Személyes adatok védelmi, megosztás, közösségi média

**Google Online Safety Roadshow (1-2 perces videók)**

<https://www.youtube.com/watch?v=7NQy2AUqgyU> 1. Think before you share – Gondolkodj megosztás előtt

<https://www.youtube.com/watch?v=ue1r_63GkIw> 2. Protect your stuffs – Védd meg a dolgaid, jelszavak

<https://www.youtube.com/watch?v=ALJk5416mNM> 3. Know & Use Your Settings - (Láthatósági) beállítások helyes használata

<https://www.youtube.com/watch?v=BX3y_an89PQ> 4. Avoid the scam - Kerüld el a csalásokat!

<https://www.youtube.com/watch?v=5XXlDS7TtwY> 5. Be Positive – Legyél pozitív!

**Nemzeti Kibervédelmi Intézet weboldalán, a „Tudásközpont” link alatt rengeteg hasznos összefoglaló anyag van.**

Ezen gyűjtemények között az egyik az Elemzések nevet viseli. <https://nki.gov.hu/it-biztonsag/elemzesek/>

A digitális pénz7 témáihoz az alábbi elemzéseket ajánlja a Nemzeti Kibervédelmi Intézet:

* A keresőmotorok működése (44 oldal)
* Gamer platformok biztonsága és online tartalmak biztonságos vásárlása (22 oldal)
* Kulcs a digitális élethez – a biztonságos jelszókezelésről (34 oldal)
* Mekkora fenyegetést jelentenek valójában a deepfake-ek? (23 oldal)
* A Google térkép működése, hasznos tudnivalók (13 oldal)

**Digitális pénztárca használat:**

<https://nki.gov.hu/it-biztonsag/tanacsok/a-biztonsagos-digitalis-penztarca-hasznalat/>

**Háttérinformáció a QR kódok veszélyeiről:**

Nemzeti Kibervédelmi Intézet **QR kódos csalásokat bemutató részletes ismertetője** (26 oldal):

<https://nki.gov.hu/it-biztonsag/elemzesek/qr-kodos-csalasok/>

**Frici és a virtuális fogkrém című fejezet Zsomac által elmesélt verziója:**

<https://www.youtube.com/watch?v=ADXM9hVru_Q>