|  |
| --- |
| **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!**  **Köszönetünket szeretnénk kifejezni az ELTE Gyertyánffy István Gyakorló Általános Iskola tanulóinak, pedagógusainak és a szülőknek, hogy támogatták a tananyagok mintaóráinak megvalósítását!**    A szervezők nevében üdvözlettel:    **Magyar Bankszövetség**  **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).  Az óra tananyaga a Nemzeti Kibervédelmi Intézet és a Nemzeti Nyomozóiroda közreműködésével készült el. Szakértőik segítségének köszönhetően életszerű példákat és praktikus tanácsokat tudunk most bemutatni. |
| **Technikai információ** |
| Ha részt vesz az órán banki önkéntes, mutatkozzon be röviden! (A tanár üdvözölje és kérje fel a bemutatkozásra.) |

|  |
| --- |
| **2. dia (Kihagyható)** |
|  |
| **Tanórán átadandó információk** |
| **ÉLŐ KIBERFENYEGETETTSÉGI TÉRKÉP (https://threatmap.bitdefender.com/ )** A diára (a dián lévő képre) kattintva, vagy a fenti hivatkozást megnyitva – működő internetkapcsolattal – megtekinthető a térkép online verziója.  *Az alapértelmezett böngészőben megnyíló térképet érdemes teljes képernyőn (Full Screen) bemutatni. A teljes képernyős módba való belépés (és az onnan kilépés) a legtöbb böngészőben az F11 gombbal történik. (Egyes klaviatúrákon az „Fn” billentyű együttes lenyomása is szükséges lehet. A teljes képernyős nézet természetesen a böngésző menüjéből is elérhető.)*  Amennyiben nincs internetelérés, vagy más okból nem használható az élő térkép, úgy a következő dián látható videót mutassuk be.  Ha esetleg a videó lejátszása sem megvalósítható (pl. a számítógép gyenge teljesítménye miatt), akkor az ezen a dián látható kép alapján beszéljünk.  **MIT LÁTUNK?**  A térkép megmutatja, hogy egyetlen nap alatt több millió kibertámadás zajlik (a fenti számláló mutatja, hogy a mai napon hány db volt már). A világ különböző részein zajló támadások folyamatosak, kormányokat, vállalatokat és magánszemélyeket is érintenek. Bal oldalon alul a „Legend” a felvillanó színekkel is jelölt támadás típusokat mutatja: Piros: támadás, Sárga: vírusfertőzés, Fehér: SPAM/Kéretlen levelek. A támadások részleteit a képernyő alsó sávjában lehet megtekinteni (Időpont, célpont, támadás típusa, támadó fél országa, célpont országa, érintett országok)  **Fő üzenet:** Az interneten folyamatos küzdelem zajlik, amelynek eszközei a kibertámadások. Magyarország sok szempontból biztonságosnak mondható, pl. Európában nálunk van az egyik legkevesebb bankkártyás csalás. Ennek ellenére bármikor veszélybe kerülhetünk és felkerülhetünk erre a térképre. Ezért fontos figyelmet fordítanunk a támadások elleni védekezésre! |
| **Háttérinformációk** |
| **A térkép további részletei:**   * Bal oldalon alul a „LEGEND” a felvillanó színekkel is jelölt támadás típusokat mutatja: Piros: támadás, Sárga: vírusfertőzés, Fehér: SPAM/Kéretlen levelek. * Középső alsó sáv „LIVE ATTACKS”: A támadások részleteit a képernyő alsó sávjában lehet megtekinteni (Időpont, célpont, támadás eszköze, támadó fél országa, célpont országa, érintett országok)   Az esetek nagy százalékában ezek a típusú támadások (főleg ilyen nagy volumenben) automatizált módon történnek közvetlen emberi interakció nélkül. Fontos, hogy ezek a térképek nem mutatják az embert közvetlen érintő támadásokat, például a telefonos csalásokat, befektetési csalásokat és online piactereken történő csalásokat. |
| **Technikai információ** |
| Amennyiben sikerült bemutatni az élő térképet, akkor a következő diát át kell ugrani. |

|  |
| --- |
| **3. dia (Kihagyható)** |
|  |
| **Tanórán átadandó információk** |
| **KIBERFENYEGETETTSÉGI TÉRKÉP** (előre rögzített videó)  Csak akkor kell lejátszani, ha az online térkép bemutatására nem volt lehetőség. |
| **Technikai információ** |
| A videó automatikusan indul, 30 másodperc hosszú, újraindul, ha véget ért, de bármikor tovább lehet lépni. |

|  |
| --- |
| **4. dia** |
|  |
| **Tanórán átadandó információk** |
| A mai óra célja a kibertérben jelenlévő veszélyek kiszagolása, a „szimat” javítása. Kezdjük bemelegítésként egy rövid, mindössze három kérdésből álló kvízzel… |
| **Technikai információ** |
| Ha önkéntes is részt vesz az órán, a kvíz levezetése lehet az ő feladata. |

|  |
| --- |
| **5. dia** |
|  |
| **Tanórán átadandó információk** |
| Helyes válasz: **B** |
| **Háttérinformációk** |
| Online piactereken (Vinted, Marketplace, Jófogás) vagy más interneten keresztüli értékesítésnél a fizetést a legbiztonságosabb átutalással a bankszámlánkra kérni a nevünk és bankszámlaszámunk (vagy másodlagos azonosítónk megadásával).  Ha mi vagyunk az eladók, semmilyen más információt nem szükséges és nem is szabad elküldenünk, nehogy csalás áldozatává váljunk. Semmiképp ne küldjünk eladóként pénzt. (Sok csalás erre irányul.)  Hogyan ismerhető fel?   * Név és bankszámlaszámon kívül **egyéb banki adatokat kérnek**, annak ellenére, hogy a vásárlónak kell a termék ellenértékét utalnia. * Netbankba történő belépést kezdeményeznek az összeg átutalásának jóváhagyása céljából. * Esetenként program telepítésére kérik, ami egy távoli elérést biztosító alkalmazás.   Hogyan védekezhetünk a fiktív vásárló jelentkezése ellen?   * Eladóként pénzt a pénzt fogadjuk és nem küldünk, így nekünk semmit sem kell megerősítenünk vagy tennünk az utalás teljesüléséhez. * Online piactéren vagy más, interneten keresztüli értékesítésnél az a legbiztonságosabb, ha **a fizetést a bankszámlára kérjük**, amihez nem kell más, mint a **név és bankszámlaszám megadása**! * Ahhoz, hogy bankszámlára pénzt utaljanak, **nincs szükség semmilyen programra, és a netbankba sem kell bejelentkezni**!   **Soha ne adjuk meg senkinek bankszámla- vagy kártyaadatokat, az internetbankhoz tartozó belépési adatokat és jelszavakat**! |
| **Technikai információ -** |
| - |

|  |
| --- |
| **6. dia** |
|  |
| **Tanórán átadandó információk** |
| Helyes válasz: **D** |
| **Háttérinformációk** |
| Fontos a bankoddal való kapcsolattartás. A bank ügyintézői különböző ügyekben kereshetnek telefonon, melynek során a beazonosításhoz néhány személyes vagy pénzügyi adatra is szükség lehet (pl. születési évünk és édesanyánk vezetékneve vagy mikor jártunk utoljára az X bankfiókban), azonban mindig kérjük ilyen esetben „keresztazonosítást”, melynek során az ügyintéző által feltett kérdésekre a válaszok egyik részét az ügyintéző adja meg, míg a válaszok másik részét az ügyfél. Így megbizonyosodhatunk arról, hogy nem egy csaló álcázza magát banki ügyintézőnek. Keresztazonosítást leszámítva semmilyen esetben ne adjuk meg személyes adatainkat se!  Jelszót, bankkártya adatokat a bank soha nem kér ügyfeleitől telefonon vagy elektronikus csatornákon történő ügyfélkapcsolat létesítése során. A legjobb megoldás bármilyen megkeresés, banki (vagy annak álcázott) kapcsolatfelvétel esetén, ha semmilyen adatot nem adunk meg, hanem elköszönünk és mi hívjuk fel a bankunkat az ismert kapcsolattartási telefonszámon és kérünk tájékoztatást a megkeresésről. Ezáltal nem válhatunk könnyen adathalászat vagy megtévesztés, pszichológiai manipulálás áldozatává. (A, D válaszlehetőség)  A bankszámlaszám nem titkos adat, azzal önmagában nem lehet visszaélni, ugyanakkor mivel hitelesítési folyamat része is lehet, ezért érdemes azt is csak a szükséges esetekben kiadni. (B válaszlehetőség)  A jelszavakkal a későbbiekben foglalkozik a tananyag. (C válaszlehetőség) |

|  |
| --- |
| **7. dia** |
|  |
| **Tanórán átadandó információk** |
| Helyes válasz: **A** |
| **Háttérinformációk** |
| **A legrosszabb egyértelműen a D válasz.**  **A B és a C „megoldások” kockázata változó, hiszen:** Valószínűleg a böngészőben vagy a kereskedői oldalon jelszóval védett privát fiókunk van, de ez nem garantálja a biztonságos tárolást (pl. egy nem megbízható, nem frissített eszköz, vagy elavult böngésző esetén).  A webáruházban elmentett kártya adatokat többnyire a kereskedő tárolja el – ezen rendszerek megbízhatósága széles skálán mozoghat.  Ugyanakkor **az A válasz egyértelműen a legjobb**. Az online fizetési megoldásokat szolgáltató bankoknál elmentett kártyaadataink (szintén egy jelszóval védett személyes fiókban) tokenizálva kerülnek tárolásra. Az adott szolgáltatóval szerződött kereskedők felületein ezáltal kényelmesen és biztonságosan tudunk fizetni.  Még nagyobb biztonságot érhetünk el, ha csak alapesetben nulla egyenlegű vagy kockázatokkal arányos összeget tartalmazó webkártya (jellemzően virtuális kártya) adatait mentjük el. |

|  |
| --- |
| **8. dia (Kihagyható)** |
|  |
| **Tanórán átadandó információk** |
| Akinek van kedve tovább tesztelnie magát, az bármikor megteheti A PÉNZ7 honlapján (www.penz7.hu), ahol további kvízeket talál a PÉNZ7 KVÍZEK és a DIGITÁLIS SZIMAT KIHÍVÁS menüpontokban.  Ha több idő (pl. dupla tanóra) áll rendelkezésre, akkor az óra végén is rá lehet térni a kvízekre. (Ha önkéntes is részt vesz az órán, egy választott kvíz levezetése lehet az ő feladata, illetve szükség esetén segíthet a tanulóknak a kvízhez való csatlakozásban.)  **A gyerekek figyelmét érdemes felhívni arra, hogy a DIGITÁLIS SZIMAT KIHÍVÁS egy tudásteszt, amelyet családjaikban, rokonaikkal, barátaikkal együtt is játszhatnak.** |

|  |
| --- |
| **9. dia** |
|  |
| **Tanórán átadandó információk** |
| **Mit tekintünk online vásárlásnak? Azt, amikor az eladó által üzemeltetett internetes áruház (webshop / webáruház / online bolt / …) felületén (vagy esetleg e-mailben) számítógépünk vagy okos eszközünk segítségével rendelünk meg valamilyen terméket vagy szolgáltatást.**  Itt szóba kerülhet:  - Ki kezdeményezi a tranzakciót ilyen esetben?  - Ki adja meg az adatokat?  - Hogyan tárolhatók a bankkártyaadatok?  **Milyen módok léteznek a fizetésre egy webshopban?**  **FELADAT: Soroljatok fel fizetési lehetőségeket!**   * Bankkártyával (vagy ajándékkártyával, ajándékutalvánnyal) a webshopban (előre)\* * Átutalással (előre)\* * Készpénzzel a futárnak vagy személyes átvételi ponton (utánvét) * Bankkártyával / mobiltelefonnal / okosórával a futárnak, személyes átvételi ponton vagy csomagautomatánál (utánvét) * Fizetési kérelem, QR-kód (előre/utánvét)   **\*Mérlegeljük minden esetben az előre történő fizetés kockázatait és az utánvétel költségét, és inkább válasszunk utánvételt, különösen nagyobb összegű vásárlás esetén!**  Egyes esetekben átutalással is van lehetőség utánvéttel fizetni (azonnali átutalás). |
| **Technikai információ** |
| Ha jelen van önkéntes, célzott kérdésfeltevéssel segítheti a diákokat a válaszadásban. |

|  |
| --- |
| **10. dia** |
|  |
| **Tanórán átadandó információk** |
| **Az imént felmerült a bankkártya (mint online fizetési mód), a következő feladat ehhez kapcsolódik…**  Az osztály véleményt nyilvánít a következő állításról:  ***„*Nyugodtan lehet online fizetni bankkártyával, mert biztonságos.*”*** (FONTOS, hogy a mondat pontosan így hangozzon el!)  Megkérjük az osztályt, hogy mindenki álljon fel, majd üljön le az, aki NEM ÉRT EGYET az állítással. Az állítást célszerű többször megismételni.  Ezt követően tehát azok állnak, akik egyetértenek az állítással: azt gondolják, hogy az online bankkártyás fizetés biztonságos. Az ülő diákok szerint pedig vélhetően a fizetési kártyás vásárlásnak az interneten vannak veszélyei.  A feladat bármilyen közösségben értelmezhető, de az különböző osztályokban értelemszerűen más megoldások születnek. (A korosztályos sajátosságok, a családi háttér terén megjelenő különbségek, a lakhely, településtípus sajátosságai meghatározók lehetnek.)  A két csoport (álló és ülő diákok) kialakulása után, kb. három-három vélemény/érv meghallgatása következhet. Szólítsuk meg a csoportokat és biztassuk őket a döntésük megmagyarázására! |
| **Háttérinformációk** |
| Érdemes úgy vezetni a beszélgetést, hogy szóba kerüljenek:  1. Az online bankkártyahasználat veszélyei, hátrányai  2. A bankkártya-használat előnyei, kiemelve az eseti jelleggel feltöltött webkártyahasználat lehetőségét  3. Kapcsolódó esetek, körülmények (pl. bankkártyás fizetés a csomag átvételekor, bankkártya adatok tárolása)  (Előfordulhat, hogy az egész osztály egy állásponton van, de ez nem probléma, hanem egy érdekes helyzet, ami szintén jó lehetőséget ad a téma megbeszélésére. Az is jó következtetés lehet, hogy mindkét csoportnak igaza van, hiszen az online bankkártyás fizetés biztonsága valójában a helyes kivitelezés függvénye.) |
| **Technikai információ** |
| Önkéntes jelenlétében a beszélgetés irányítása lehet az ő feladata. Ha valamilyen körülmény miatt könnyebbséget jelent, a felállás kézfelrakással helyettesíthető. |

|  |
| --- |
| **11. dia** |
|  |
| **Tanórán átadandó információk** |
| Ahogyan az imént megbeszéltük, nem csak fizikai vásárlás során (pl. boltban), hanem online környezetben is használhatjuk a kártyánkat.  1. Ha lehetséges, 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 (van egyszerhasználatos is), 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 kóddal, arcfelismeréssel, 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.  5. Gondoskodjunk a szoftverek frissítéséről és a megfelelő vírusvédelemről, továbbá az eszközeinken az automatikus zárolás beállításáról, különösen az online bankolásra használt számítógépünkön vagy a mobilunkon.  6. Az SMS-ben vagy banki alkalmazásban érkező biztonsági kódot/push üzenetet soha ne adjuk meg senkinek, banki ügyintézőnek sem! |
| **12. dia** |
|  |
| **Tanórán átadandó információk** |
| **A legtöbben már tudják, hogy az „123456” és a „kiscica12” nem a legjobb jelszavak. Azt szokták mondani, hogy ezeknél ERŐSEBB jelszavakra van szükségünk – ez a legtöbb banki művelethez (pl. átutalás Netbankból) is elengedhetetlen. Nagyot léphetünk előre az online önvédelemben, ha biztonságos jelszavakat használunk.**  **De milyen a jó, biztonságos, avagy ERŐS jelszó? ...valami ahhoz hasonló, amit alul, zölddel látunk a képen:**  - legalább 12 karakter hosszú  - kis és nagy betűket is tartalmaz  - számok is vannak benne  - speciális karaktert is találhatunk benne (pl. dollár jel, pont, # stb.)  - nincsenek benne személyes információk (név, becenév, cím, e-mail cím, telefonszám, rokon vagy háziállat neve, születési dátum stb.)!  - nincs benne semmi, ami könnyen hozzánk köthető (pl. kedvenc film, vagy játék, esetleg háziállat neve)  **Ezt a jelszót egy könnyen megjegyezhető dalszöveg-részletből alkottuk meg, néhány egyszerű művelettel.**  **(Érdemes megkérdezni a diákokat, hogy felismerik-e ezeket a műveleteket.)**   1. **A szavak kezdőbetűit használtuk.** Nagy betűk, írásjelek maradtak. Kettős mássalhangzóknál mindkét karaktert felhasználtuk. 2. A hosszú Ú betűt rövid U-ra változtattuk. 3. **Néhány betűt számokra vagy speciális karakterekre cseréltünk az általunk kitalált szabályok szerint:** „h” helyett „7” (hét); „S” és „s” helyett „$”; „v” helyett „@” (Alt Gr + V magyar billentyűzeten) |
| **Háttérinformációk** |
| A leggyakrabban használt jelszavak sajnos pont az „123456”, illetve a „jelszó”. (Angol nyelvterületen „123456” és „password”.) Ezt ellopott, kiszivárgott jelszavak adatbázisainak elemzéséből lehet tudni. |

|  |
| --- |
| **13. dia (Kihagyható)** |
|  |
| **Tanórán átadandó információk** |
| Az előbb elmondottakon túl igaz az is, hogy minél bonyolultabb és hosszabb a jelszavunk, annál jobb. Az ábrán az látható, hogy jelenleg a támadóknak mennyi időbe telik feltörni a különböző hosszúságú és összetettségű jelszavakat.  Az imént megalkotott jelszavunk (Szm7$z$z,Um@n,Je7,) 18 karakter hosszú és a lehető legösszetettebb (minden lehetséges karakter típust tartalmaz), így meglehetősen biztonságosnak tekinthető. |
| **Háttérinformációk** |
| A táblázatban meghatározott idők brute force-támadásra (szó szerint angol nyelven: „nyers erő”), más néven a teljes kipróbálás módszerére vonatkoznak. Ezen támadás lényege, hogy a támadó az összes lehetséges jelszót (vagy kódot, kulcsot stb.) egyenként kipróbálva találja meg az alkalmazott jelszót.  A 18 karakteres jelszavunk – a jelenlegi technológia mellett – 438 milliárd évet „bír”, ami jóval több mint az univerzum életkora (az ősrobbanás-elmélet szerint 13,7 milliárd év).  Egy jelszó erősségét könnyen ellenőrizheted az NBSZ NKI weboldalán található webes programmal:  <https://nki.gov.hu/it-biztonsag/tartalom/eszkoztar/jelszo-ellenorzo/> |

|  |
| --- |
| **14. dia (Kihagyható)** |
|  |
| **Tanórán átadandó információk** |
| Az előzőekben bemutatott módszerrel néhány erős jelszót könnyen megalkothatunk, de ez biztosan kevés, hiszen jóval több jelszóval (és felhasználónévvel) történő azonosítást igénylő szolgáltatást használunk.  (Nagyon fontos, hogy mindenhol más jelszót használjunk, hiszen így ha valamelyik szolgáltatásunkból kikerül a jelszavunk, a többi akkor is biztonságban van.)  Erre lehet megoldás a jelszószéf (password manager).  A jelszószéf egy olyan szoftver, ami titkosított formában tárolja jelszavainkat. Előnye, hogy csak egyetlen, ún. mesterjelszót kell fejben tartanunk, azt, amellyel hozzáférhetünk magához a jelszószéfhez és bármikor elérhetjük jelszavainkat. |
| **Háttérinformációk** |
| Nem mindegy, hogy milyen jelszószéfet használunk – a jelszószéfek használatának vannak kockázatai is.  Ilyen például, hogy a mesterjelszó vagy az alkalmazás kompromittálódásával az összes jelszavunk egyszerre kerülhet csalók kezébe.  Nem megbízható jelszószéf programból könnyen kikerülhetnek a jelszavaink.  Az online jelszószéf megoldások használata kényelmesebb lehet, ugyanakkor könnyebb támadási felületet jelenthetnek. |

|  |
| --- |
| **15. dia (Kihagyható)** |
|  |
| **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 jelszókezelés biztonságára és a jelszószéf használatára hívja fel a figyelmet.  A felhasználók számára javasolt minden online szolgáltatásnál egyedi [erős jelszót](https://nki.gov.hu/it-biztonsag/tartalom/eszkoztar/jelszohasznalat/) alkalmazni. Az erős jelszó kapcsán pedig az a konszenzus, hogy minél hosszabb (több karakterből áll) egy jelszó, annál biztonságosabb, ugyanis annál nagyobb számítási kapacitás szükséges a feltöréséhez. Ezen felül a legtöbb szakember szerint az a legjobb megoldás, ha egyenesen egy több szóból álló jelmondatot választunk jelszóként.  Az egyedi erős jelszavak fejben tartása – egy adott mennyiség után – ugyanakkor már komoly gondot okozhat, amire megoldást jelenthet egy jelszókezelő szoftver alkalmazása. |

|  |
| --- |
| **16. dia (Kihagyható)** |
|  |
| Mi az a jelszókezelő (password manager)?  * Egy szoftver, amely titkosított formában tárolja jelszavainkat, így azokhoz illetéktelenek (ideális esetben) nem ─ vagy csak irreálisan nagy erőforrás ráfordításával ─ férhetnek hozzá. A megoldás előnye, hogy ehhez csupán egyetlen, ún. mesterjelszót kell fejben tartanunk, azt, amellyel hozzáférhetünk magához a jelszószéfhez. A mesterjelszóból kerül leképezésre az a titkosító kulcs, amivel a hitelesítő adatokat (felhasználónév, jelszó) tároló adatbázis ─ esetlegesen további kriptográfiai komponensek bevonásával ─ titkosításra kerül. * Az ilyen programok használata általában egyszerű: mindössze “kinyitjuk” a mesterjelszóval a jelszószéfet, és már hozzá is férünk az abban tárolt jelszavainkhoz, amelyeket onnan kimásolhatunk. A legtöbb terméknél arra is van lehetőség, hogy a szoftver egy kattintásra, automatikusan töltse ki a hitelesítő adatokat. * Rengeteg jelszókezelő termék létezik, azonban ezek között sok eltérés tapasztalható. Az egyik legfontosabb különbség abban mutatkozik meg, hogy az adott szoftver hol tárolja a hitelesítő adatokat: lokálisan (számítógépen, telefonon), vagy felhőben (a szolgáltató szerverén). * A felhőalapú megoldások előnye, hogy több eszközön is relatíve egyszerűen lehet szinkronizálni a titkosított jelszóadatbázishoz való hozzáférést, illetve általában több extra kényelmi szolgáltatás kapcsolódik hozzájuk (például automatikus bejelentkezés). * Egy másik fontos különbség lehet, hogy önálló (standalone) programról, vagy csupán egy böngésző bővítményről (plugin) van-e szó. Az önálló programok használatát javasoljuk, a bővítményeket ugyanis esetleges sérülékenységeik mellett a böngészők sebezhetőségei is közvetlenül érinthetik. * A nagyobb okostelefon gyártók (Apple, Google) biztosítanak beépített jelszókezelő megoldást.  Mit kell mindenképp eldöntenünk a jelszókezelő megoldás kiválasztása előtt?  * Elsősorban azt, hogy pontosan mire is szeretnénk használni. Csupán arra, hogy ne kelljen egy otthoni noteszba ─ vagy irodai monitorra ragasztott cetlire ─ felírva tárolnunk jelszavainkat? Ebben az esetben egy otthoni, megbízható számítógépen, egy standalone, lokális megoldás elegendő lehet. Vagy szeretnénk azt, hogy jelszavainkat bárhol, bármikor elérjük? Ehhez valószínűleg egy felhő-alapú szolgáltatásra lesz szükségünk. * Tisztában vagyunk-e azzal, hogy mit tegyünk, ha elveszítjük a hozzáférést a jelszókezelőhöz (például ellopják az eszközt, amin tároltuk), vagy ha elfelejtjük a mesterjelszót? |

|  |
| --- |
| **17. dia (Kihagyható)** |
|  |
| **Tanórán átadandó információk:**   * Jegyezzétek meg a kis robot intelmét!   **Kérdés:** - Mire hívta fel a figyelmet?   * Az erős (biztonságos) jelszavakat nehéz fejbentartani, ezért érdemes azokat egy titkosított jelszószéfben tartani, így kicsi az esélye, hogy illetéktelen hozzájuk fér. * Mielőtt kiválasztunk egy jelszószéf megoldást, gondoljuk át, mikor és hogyan, hány eszközön szeretnénk használni, és ennek megfelelően válasszunk egy biztonságos gyártó termékét! * Az online fiókok esetében ne felejtsünk el a kétfaktoros azonosítást is bekapcsolni! |

|  |
| --- |
| **18. dia** |
|  |
| **Tanórán átadandó információk** |
| A jelszavak hátránya, hogy rengeteg félét kell használnunk és bármennyire is erősek, ezeket valahol tárolni kell mind a felhasználóknak (pl. jelszószéf), mind a rendszereknek, ahova be akarunk lépni. Ez a gyenge pontjuk is egyben. Az interneten jelenleg is több milliárd darabos jelszóadatbázisok érhetőek el, amelyek akár a mi valahonnan ellopott jelszavainkat is tartalmazhatják  Ezen a problémán segít a két vagy többfaktoros hitelesítés, ahol a sikeres azonosító és jelszó megadás után egy második faktort is meg kell adni. Ez a második faktor jellemzően egy nagyon rövid ideig (pár perc) élő, egyszer használatos kód, amit a rövid élettartama miatt nagyon körülményes ellopni, ezért használata egy újabb „védelmi vonalat” jelent a felhasználói fiók védelmében. Ilyen egyszer használatos kódok érkezhetnek SMS-ben, azonnali üzenetküldő alkalmazásba (Pl. WhatsApp), e-mailben, és hitelesítő alkalmazás is generálhatja őket. A dián ez a verzió van bemutatva. (A felhasználó mobiltelefonjára telepített Google Authenticator program. De lehet használni a Microsoft Authenticatort is. Mindkettő ingyenes).  **Feladat, ha van internetkapcsolat:** „Have I been Pwned” oldalt (https://haveibeenpwned.com/) megmutatni, ahol az e-mail címünk alapján megnézi az oldal, hogy volt-e érintett az e-mail cím és jelszó valamilyen adatlopásban vagy adatszivárgásban. Példaként lehet használni az [akos.solymos@upcmail.hu](mailto:akos.solymos@upcmail.hu) Jelenleg már nem létező e-mail címet. Ez több adatszivárgásban is érintett volt az elmúlt évtizedben. |
| **Háttérinformációk** |
| A két vagy többfakoros hitelesítés bár bonyolultabb, de nagyobb védelmet biztosít a fióknak, hiszen ha felhasználónevünket és jelszavunkat el is lopták és sikeresen meg is adja a támadó, akkor sem fog tudni belépni, mivel a második faktort nem tudja. Hiszen az a belépéskor generálódik és az igazi tulajdonos fér csak hozzá.  Példaként meg lehet mutatni a dián, hogy ha a támadók megszerezik a Facebook azonosítót és jelszót, akkor már az első lépés után bent lehetnének a Facebook fiókban. De megállítja őket a második faktor. |
| **Technikai információ**  A Have I been pwned oldalt az önkéntes vagy az előadást támogató már előzetesen megnyithatja egy böngésző programban. Felsőbb évfolyamokon vagy szülői, pedagógusoknak szóló előadás során lehet kérni a közönségből is e-mail címet ellenőrzésre. |

|  |
| --- |
| **19. dia (Kihagyható)** |
|  |
| **Tanórán átadandó információk:**  Most pedig nézzük meg a Nemzeti Kibervédelmi Intézet mini képregényét! Figyelmesen olvassátok el, hogy mit mondanak a szereplők! |
| **Háttérinformáció (ha a korábbi képregény nem került bemutatásra):**  A Nemzeti Kibervédelmi Intézet képregénysorozatot készített, amelyet a 2024-es Kibervédelmi hónap keretén belül mutatott be a honlapján. Ez a képregény a kétfaktoros hitelesítés használatára hívja fel a figyelmet. |

|  |
| --- |
| **20. dia (Kihagyható)** |
|  |
|  |

|  |
| --- |
| **21. dia (Kihagyható)** |
|  |
| **Tanórán átadandó információk:**   * Jegyezzétek meg a kis robot intelmét!   **Kérdés:** - Mire hívta fel a figyelmet? |

|  |
| --- |
| **22. dia** |
|  |
| **Tanórán átadandó információk** |
| **TÉMAFELDOLGOZÁS:**  **Kérdés**: - Találkoztatok-e már QR kóddal?  **Kérdés:** - Mit csinál egy QR kód?  A **QR kódos vásárlás** egy egyszerű és gyors módja az online vagy fizikai térben történő tranzakcióknak, amely a QR kód (Quick Response kód) technológiát használja. A folyamat lehetővé teszi a felhasználók számára, hogy egy okostelefon vagy más eszköz segítségével, a kód beolvasásával vásároljanak vagy fizessenek.  **A folyamat lépései:**   1. **QR kód megjelenítése**: A kereskedő, webáruház, vagy szolgáltatás a vásárlás végén egy QR kódot jelenít meg, amely tartalmazza a fizetési információkat (pl. összeg, kereskedő adatai, tranzakciós azonosító). 2. **Kód beolvasása**: A vásárló okostelefonjával beolvassa a QR kódot egy mobil banki alkalmazáson, digitális pénztárcán vagy egy másik erre alkalmas alkalmazáson keresztül. 3. **Adatok ellenőrzése**: A kód beolvasása után az alkalmazás megjeleníti a tranzakció részleteit (pl. az összeg és a kereskedő neve). A felhasználónak lehetősége van ellenőrizni az adatokat. 4. **Fizetés megerősítése**: Ha minden adat helyes, a vásárló jóváhagyja a fizetést a mobilalkalmazáson keresztül, ami történhet jelszóval, biometrikus azonosítással (pl. ujjlenyomat, arcfelismerés) vagy más módszerrel. 5. **Tranzakció visszaigazolása**: A sikeres fizetés után mind a vásárló, mind a kereskedő kap egy visszaigazolást a tranzakcióról. Ez lehet elektronikus nyugta vagy egy egyszerű értesítés a mobilalkalmazásban.   **Előnyök:**   1. **Gyors és kényelmes**: Nincs szükség készpénzre, kártyára, vagy manuális adatbevitelre. A QR kódot egy pillanat alatt be lehet olvasni. 2. **Biztonságos**: A QR kód titkosított adatokat tartalmaz, és a tranzakciók hitelesítése (pl. biometrikus azonosítással) magas szintű biztonságot nyújt. 3. **Széles körben használható**: Kereskedők, automaták, webáruházak és szolgáltatók is könnyedén alkalmazhatják ezt a fizetési módot. |
| **Háttérinformációk** |
| A **QVIK** egy magyar fejlesztésű mobilalkalmazás, amely a gyors és egyszerű QR kódos fizetést teszi lehetővé. Az alkalmazás segítségével a felhasználók néhány másodperc alatt biztonságosan tudnak tranzakciókat végrehajtani okostelefonjuk használatával. Fő előnye, hogy nincs szükség bankkártya vagy készpénz használatára, így a fizetési folyamat digitalizált és érintésmentes. A QVIK támogatja a magyar banki rendszereket, és különösen alkalmas kisebb üzletek, szolgáltatók és vásárlók közötti fizetések lebonyolítására. A felhasználók egyszerűen beolvassák a kereskedő által megadott QR kódot, majd megerősítik a fizetést a mobilalkalmazásban. A QVIK könnyen kezelhető felülettel rendelkezik, így széles körben elérhető és felhasználóbarát megoldást kínál.  Nemzeti Kibervédelmi Intézet **QR kódos csalásokat bemutató részletes ismertetője** (26 oldal):  <https://nki.gov.hu/it-biztonsag/elemzesek/qr-kodos-csalasok/> |

|  |
| --- |
| **23. dia** |
|  |
| **Tanórán átadandó információk** |
| **TÉMAFELDOLGOZÁS:**  **A QR kódos fizetés kényelmes és gyors, de mint minden digitális technológia, ez is rejthet biztonsági kockázatokat. Az alábbiakban összefoglalom a leggyakoribb veszélyeket és azok elkerülési módjait:**  **1. Hamis QR kódok:**   * **Kockázat**: Csalók hamis QR kódokat helyezhetnek el a valódiként feltüntetett helyeken (pl. fizikai boltokban, weboldalakon), amelyek nem a kereskedőhöz, hanem a csalóhoz vezetnek. A vásárló így tévedésből a csaló számlájára utalhat pénzt. * **Elkerülés módja:** Mindig ellenőrizd a kód forrását! Kerüld az ismeretlen, gyanús forrásból származó QR kódok beolvasását. Csak megbízható kereskedőktől és alkalmazásokból származó QR kódokat használj**.**   **2. Adathalászat (Phishing):**   * **Kockázat**: A QR kódokat adathalász támadásokra is használhatják. Ha a kód egy hamis weboldalra irányít, ahol a felhasználó érzékeny adatokat (pl. banki információkat, jelszavakat) ad meg, ezek az adatok a támadókhoz kerülhetnek. * **Elkerülés módja:** Ne adj meg érzékeny adatokat olyan weboldalakon, amelyekhez QR kódon keresztül jutottál el, ha nem győződtél meg azok hitelességéről. Mindig ellenőrizd a weboldal URL-jét!   **3. Számítógépes kártevő (vírus) terjesztés:**   * **Kockázat:** Egyes QR kódok beolvasásakor rosszindulatú szoftver (malware) letöltését indíthatják el a felhasználó eszközére, ami adatlopáshoz vagy további káros tevékenységekhez vezethet. * **Elkerülés módja:** Csak olyan alkalmazásokkal olvass be QR kódokat, amelyek biztonságosak és védettek a malware támadások ellen. Használj megbízható antivírus szoftvert a telefonodon is. |
| **Háttérinformációk** |
| A QR kód veszélyszempontjából hasonló, mint a rövidített linkek. Pl. bit.ly stb. |

|  |
| --- |
| **24. dia (Kihagyható)** |
|  |
| **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.  **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. |
|  |

|  |
| --- |
| **25. dia (Kihagyható)** |
|  |
| **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. Mostanában még azonban nem erre használják elsősorban, hanem megveszik és remélik, hogy később töbet fog érni, akkor pedig majd eladják.  **A blokklánc (blockchain), ami olyan, mint sok hatalmas füzet, amiben mind ugyanaz található a kriptovalutával kapcsolatos pénzmozgások**. Ezekben a füzetekben minden egyes pénzmozgás (amikor valaki fizet valakinek) 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 ki fizetett kinek, 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.** |
|  |

|  |
| --- |
| **26. dia** |
|  |
| **Tanórán átadandó információk** |
| Ma már sajnos nem lehetünk biztosak benne, hogy azzal kommunikálunk, akivel gondoljuk. A leghétköznapibb szituációkban is végig kell gondolnunk, hogy valójában:   * Kivel beszélünk (telefon, videóhívás, SMS, e-mail, chat, …)? * Mi az a weboldal, amit meglátogattunk? * Mi az az alkalmazás / szoftver, amit éppen letölteni és/vagy használni készülünk?   …  Azaz, fel kell tennünk a kérdést magunkban: **KI VAGY TE?** |

|  |
| --- |
| **27. dia** |
|  |
| **Tanórán átadandó információk** |
| Mindenki ismeri a képszerkesztő szoftvereket (pl. a legismertebb a Photoshop). Készült rólunk egy kép otthon a kanapén, de egy ügyes grafikus pillanatok alatt el tudja érni, hogy úgy tűnjön mintha a Balaton partján ücsörögnénk. Ez az állítás a képekre vonatkozik… de mi a helyzet a mozgóképpel és a hanggal?  A technológia fejlődése lehetővé tette, hogy ma már bárki „utánozható” legyen videó és audió formában is – ráadásul valós időben. Az itt látható videó is ilyen „arc-csere” alkalmazást mutat be.  Ráadásul ahhoz, hogy valaki olyan személynek adja ki magát akit nem ismerünk, nincs is szükség ilyesmire. Erre hallhattok most egy hazai példát. |
| **Háttérinformációk** |
| GIF (bal felső animáció) forrása: <https://youtu.be/SWNcQgbIKmU?t=56> (5 másodperc) |
| **Technikai információ** |
| HANGFÁJL LEJÁTSZÁSA   * Jobb lenti hangszóró ikonra kattintva * Javasolt lejátszási időtartam: 22 mp * A hangfelvétel lejátszása közben az animációt (bal fent) érdemes kattintással leállítani, hogy ne vonja el a figyelmet. |

|  |
| --- |
| **28. dia** |
|  |
| **Tanórán átadandó információk** |
| Sajnos nagyon sokféle csalás létezik. A leggyakoribb típusokról a kiberpajzs.hu oldalon lehet bővebben tájékozódni.  A továbbiakban néhány kiemelt példát mutatunk be… |
| **Háttérinformációk** |
| <https://kiberpajzs.hu> |

|  |
| --- |
| **29. dia** |
|  |
| **Tanórán átadandó információk** |
| **Mit szólnál ha egyszer csak eltűnnének a számítógépedről az elmúlt 10 év családi fotói?**  Itt az egyik legsikeresebb zsarolóvírus, a WannaCry üzenete (ransom note) látható, amelyben pénzt követel a fájlokért cserébe, amelyeket titkosított a megfertőzött számítógépen.  Mint sok más online csalás vagy támadás esetében, a fizetőeszköz itt is bitcoin (BTC).  Több, mint 10.000 kriptoeszköz létezik – a legrégebbi és legismertebb a bitcoin (BTC). Ezek piaca jelenleg még szabályozatlan, ellenőrizetlen, így lehetőséget ad a bűnözői csoportoknak, hogy illegális tevékenységekhez használják őket.  Legfontosabb védekezési lehetőség a zsarolóvírusok ellen, ha rendelkezünk rendszeres mentéssel adatainkról (amennyiben az adatainkat titkosítja a vírus, de a támadók nem tudják az adatokat elvinni). |
| **Háttérinformációk** |
| A zsarolóvírus támadások száma az elmúlt években világszerte növekedett, hétről hétre egyre újabb és hihetőbb, “sikeresebb” zsarolóvírusokkal összefüggő technikákkal állnak elő a támadók.  A WannaCry támadás több, mint 230 000 számítógépet fertőzött meg világszerte, összesen 99 országban és 28 nyelven hozott létre zsarolóoldalakat, amelyeken pénz (BTC) fizetését követeli a fertőzött gépek felhasználóitól.  Például: Spanyolországban a Telefónica nevű telekommunikációs vállalatot, valamint több nagyobb méretű spanyol vállalatot bénított meg a vírus. Nagy-Britanniában a National Health Service számítógépes rendszerét, Németországban pedig a Deutsche Bahn vasúttársaság, ezen kívül a FedEx rendszerét érte támadás, többek között. A vírus gyors ütemű terjedését támasztja alá, hogy néhány óra leforgása alatt közel 100 országból jelentettek fertőzéseket. |

|  |
| --- |
| **30. dia** |
|  |
| **Tanórán átadandó információk** |
| Különböző felületeken rengeteg ezekhez hasonló reklámmal találkozhatunk. A fő tudnivaló: Ha túl szép, hogy igaz legyen, akkor NEM IGAZ!  A magasabb hozamú befektetések egyébként is kockázatosabbak – igaz mindez itt nem számít, mert ezek egyértelműen csalások.  A következő oldalon a középső, MOLGROUP „befektetéséhez” kapcsolód deepfake reklámvideót mutatjuk be.  A sürgetésről, egyszeri lehetőségről, lemaradásról még lesz szó a következő dián. |

|  |
| --- |
| **31. dia** |
|  |
| **Tanórán átadandó információk** |
| Különböző felületeken rengeteg ezekhez hasonló reklámmal találkozhatunk. A fő tudnivaló: Ha túl szép, hogy igaz legyen, akkor NEM IGAZ!  A magasabb hozamú befektetések egyébként is kockázatosabbak – igaz mindez itt nem számít, mert ezek egyértelműen csalások.  A csalók a legfrissebb, deepfake technológiát is bevetik. Jelen esetben Hernádi Zsolt MOL vezérigazgató egyik interjúját alakították át a csalók. A szájmozgás, a hang és még a gesztikuláció és hihető, talán egy pár helyen van elcsúszás vagy túlzott gesztikuláció. A fenti videó egy jól sikerült hamisítvány. A szövegben is megjelenik a sürgetés, az exkluzivitás, a hatalmas hozam ígérete!  Ezért minden esetben, ha befektetésről van szó, akkor hivatalos forrásból tájékozódjunk, ne adjunk meg telefonon vagy weboldalon személyes és pénzügyi adatokat és főleg ne utaljunk előre pénzt senkinek. A befektetésekhez is szigorú szabályokon alapuló szerződéskötés tartozik, nincsenek csodák, hogy elutalok x összeget valakinek és pár hét múlva visszautalnak 2x 3x nagyobb összeget.  Vannak komplex csalások, ahol a „beetetés” fázisában a csalók visszautalnak kisebb összegeket, majd amikor már egyre nagyobb összegek befeketése történik meg az áldozat részéről, akkor tűnnek el a befizetett pénzzel.  **Nincs ingyen pénz!!!**  Az egyik leggyakoribb formula: Küldj nekünk X összeget, visszaküldünk 2X-et 3X-t.  Ez biztosan mindig csalás!  Sok esetben, ahogy az itt látható példában is:   * egyébként legális, ismert felületen jelenik meg (pl. Youtube) * kriptoeszközt használ * sürget, a FOMO jelenséget igyekszik kihasználni   **Háttérinformációk:**  *Hogyan ismerhető fel?*   * Irreálisan magas hozamot ígérnek (ez „túl szép, hogy igaz legyen”). * A közösségi médiában újra és újra találkozni ezekkel a hirdetésekkel. * **Gyors megtérülést ígérnek** és biztosítanak arról, hogy a befektetés biztonságos. * Az ajánlat csak **korlátozott ideig él**, kimaradunk, lemaradhatunk róla. * Az **ajánlat személyre szóló**, és kérnek, hogy senkinek se szóljunk róla!   *Hogyan védekezhetünk a befektetési csalások ellen?*   * Ne vegyük fel a telefont, ha híváskor ismeretlen **külföldi hívószámot** jelez ki a telefon, és ne is hívjuk vissza rögtön – először ellenőrizzük azt! Különösen legyünk óvatos akkor, ha olyan külföldi számról érkezik a hívás, ahol nem él ismerős, vagy ahonnan nem várunk hívást, illetve, ha az országhívó **2-essel vagy 5-össel kezdődik** (ld. fentebb: afrikai és közép-amerikai azonosítók)! * Egy internetes kereséssel utána lehet járni annak, hogy az adott telefonszámmal kapcsolatban korábban felmerül-e a csalás gyanúja: ha igen, nagy valószínűséggel találni ezzel kapcsolatos információt a világhálón. * Utasítsuk el a befektetési lehetőségekkel kapcsolatos kéretlen telefonhívásokat, bármilyen egyszerű és könnyű pénzszerzésről, meggazdagodásról szólnak is! * Pénz átadása vagy befektetése előtt mindig **érdemes pénzügyi tanácsot kérni egy független féltől**, szakértőtől! |
| **FOMO** (Fear Of Missing Out) – “a kimaradok valamiből” érzés, vagyis a félelem, hogy lemaradunk egy jónak ígérkező lehetőségről. Sokan hajlamosak ilyenkor hirtelen, meggondolatlan módon cselekedni. |

|  |
| --- |
| **32. dia** |
|  |
| **Tanórán átadandó információk** |
| Napjainkban Magyarországon is elég gyakori a hamis banki vagy csomagküldő szolgáltató üzenetek alkalmazása…  Az ilyen csalásoknál gyakori, hogy:   * Valamilyen gyanús / jogosulatlan tranzakcióra, vagy a bankkártyánk letiltására hivatkozik az üzenet * Sürget – ha nem cselekszünk azonnal, akkor... pl. nem kapjuk meg a csomagunkat * Linkre való kattintásra bíztat (ahol adatok megadását kéri) * Nem létező bírság/pótdíj befizetését kéri egy üzenet. (A Rendőrség, sohasem így értesít bírságról vagy büntetésről, hanem hivatalos papír alapú levélben vagy Ügyfélkapun keresztül) Illetve érdemes az SMS feladójának telefonszámát is megnézni, nem magyar telefonszámról érkezett.   Soha ne kattintsunk ilyen módon kapott linkre! Ha az üzenet megfelelőnek tűnik, akkor is célszerű az eredeti forrás (pl. szolgáltató weboldala) használatával ellenőrizni vagy a szolgáltató ügyfélszolgálatán érdeklődni. |
| **Háttérinformációk**:  *Hogyan ismerhető fel?*   * Olyan csomag vámolásáról érkezik üzenet, amit egyáltalán nem várunk. * Az üzenetben gyakran **ékezetek nélküli szavak szerepelnek**, vagy **helyesírási hibák** fordulnak elő, esetleg **rossz magyarsággal**, **helytelenül** van megfogalmazva. * Az üzenetben szereplő link nem egy létező, ismert szolgáltató vagy webáruház webcíme, hanem általában egy **ismeretlen, betűkből és számokból kombinált hivatkozás**. * **Korábban a banktól (vagy szolgáltatótól) kapott SMS-ek egy másik telefonszámról érkeztek.** * Az üzenetben olyan szerkesztést vagy megszólítást használnak, amely **eltér** a korábban a **banktól** (vagy szolgáltatótól) kapott SMS-ekben használttól, **nem pontos a küldő megnevezése**. * Az üzenet úgy van megfogalmazva, hogy **sürgető** legyen. Akár nyereményjátékot hirdet, vagy arra utal, hogy csak a link megnyitásával teljesül az SMS-ben jelzett szolgáltatás.   *Hogyan védekezhetünk az SMS-es csalások ellen?*   * **Keltsen gyanút** minden olyan telefonhívás, SMS-üzenet, közösségi oldalon keresztül érkezett üzenet vagy e-mail, amelyben az internetbanki bejelentkezéshez és azonosításhoz szükséges **jelszót vagy PIN-kódot kér!** * **Soha ne válaszoljunk** olyan SMS-ekre, amelyekben bankkártyájához, bankszámlájához vagy internetbankjához kapcsolódó **adatokat kérnek**! **Az bankok sem e-mailben, sem telefonon, sem SMS-ben nem kér jelszavakat vagy PIN-kódokat**, sem más bizalmas adatokat. A bank munkatársai kizárólag akkor kérhetnek személyes adatokat, ha egy konkrét, folyamatban lévő ügyben keresi az ügyfelet, az által megjelölt módon. * Soha **ne telepítsünk olyan programot számítógépünkre vagy alkalmazást** telefonunkra, amit nem ismerünk**, különösen ne telepítsünk semmit mások kérésére!** * Ne utaljunk pénzt ismeretlen "biztonsági számlára"! |

|  |
| --- |
| **34. dia** |
|  |
| **Tanórán átadandó információk** |
| Az online piactereken is egyre több csalással találkozhatunk. A csalók legtöbbször vevőnek adják ki magukat és az előző példákhoz (hamis banki / csomagküldő üzenetek) hasonlóan általában linkre kattintást kérnek.  Soha ne kattintsunk ilyen linkekre! Eladóként online piactereken a fizetést a legbiztonságosabb átutalással bankszámlánkra kérni a nevünk és bankszámlaszámunk (vagy másodlagos azonosítónk megadásával).  Semmilyen más információt nem lehet szükséges és nem is szabad elküldenünk, nehogy csalás áldozatává váljunk. Semmiképp ne küldjünk eladóként pénzt. |
| **Háttérinformációk** |
| **Mi az online piactér (marketplace)?**  Olyan online platform, ahol a vevő és az eladó virtuálisan találkozhatnak és adásvételt, illetve cserét tudnak lebonyolítani.  Ismert magyar online piacterek:**Jófogás, eMAG, Vatera, Pepita**  Keresett nemzetközi szolgáltatások: **Facebook Marketplace, Amazon, Ebay, Wish** |

|  |
| --- |
| **34. dia** |
|  |
| **Tanórán átadandó információk** |
| Az online piacteres csalások kapcsán, legyen szó, akár Marketplace, Vinted vagy Jófogás vagy Vatera (ezek a legnépszerűbbek) a csaló az adott futárcég (az előző dián és itt a folytatásaként is a Foxpost) logojával ellátott hamis levélben kéri az eladót, hogy kattintson a megadott linkre, hogy „hozzájusson a pénzéhez”. A valóságban egy normál banki átutalás során érkezik meg a pénz, nincs szükség a futárcég közvetítésére és nincs szükség a csalók által megadott felületen kattintani és belépni a netbankba. Hiszen a csalók úgynevezett „függönyoldalt” alkalmaznak, ahol az áldozat választhatja ki a saját bankját, majd jut el a hamis banki belépési oldalra. Idáig már semmiképp sem szabad eljutni, de ha mégis eljutottunk, akkor legyen gyanús, hogy nem a bankunk hivatalos internetcíme jelenik meg a címsorban, hanem még mindig a „futárcég” weboldalán vagyunk.  Soha ne lépjünk be mások által megadott internetbanki belépési oldalon! Ha az üzenet megfelelőnek tűnik, akkor is célszerű az eredeti forrás (pl. szolgáltató weboldala) használatával ellenőrizni vagy a szolgáltató ügyfélszolgálatán érdeklődni. Illetőleg érdemes a saját mobilbanki alkalmazásunkban ellenőrizni az egyenlegünket. |

|  |
| --- |
| **35. dia** |
|  |
| **Tanórán átadandó információk** |
| Végezetül 6 kiemelt biztonsági tippet ismertetünk.  01 – Ha ilyet kapunk, az adathalász támadás.  02 – Biztonságosabb online vásárlást tesz lehetővé.  03 – Helyette alkalmazzuk a szolgáltatónk által nyújtott mobil internetet. Amennyiben mégis egy nyilvános Wi-Fi hálózathoz csatlakozunk, akkor ne jelentkezzünk be egy online fiókba sem és próbáljunk meg egy VPN szolgáltatást használni, hogy ne tudják illetéktelenek a hálózaton "lehallgatni” a kommunikációnkat, érzékeny adatainkat.  04 – Ne klikkelj alapos vizsgálat nélkül linkekre! A fontosabb linkeket (például netbanki belépési oldal) a böngésző könyvjelzőjébe mentsd el és mindig csak onnan nyisd meg! Ne nyiss meg csatolmányokat alapos vizsgálat nélkül, és ha bizonytalan vagy, akkor inkább kérdezz rá a küldőnél.  05 – Vagyis eszközeink rendelkezzenek a legfrissebb biztonsági javításokkal.  06 – Időnként érdemes biztonsági mentést készíteni eszközeinkről, ügyeljünk arra, hogy a másolatok egy megbízható, jól védett helyen kerüljenek tárolásra. |

|  |
| --- |
| **37. dia (Kihagyható)** |
|  |
| **Tanórán átadandó információk** |
| **Remélem, hogy sokat javult a szimatotok és a jövőben nagyon ügyesen szagoljátok ki a veszélyeket!**  Az óra után / otthon:   1. Gondoljátok végig: Ti biztonságban érzitek-e magatokat? Ha nem teljesen, akkor mit kell jobban csinálnotok? 2. Válasszatok ki a környezetetekben (család, barátok) három embert és 48 órán belül mondjatok el nekik valamit az itt elhangzottakból, hogy ők is nagyobb biztonságban legyenek! 3. Tájékozódjatok tovább a nagyobb biztonság érdekében.   Ebben mi is tudunk segíteni. |

|  |
| --- |
| **38. 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!** |

|  |
| --- |
| **39. dia** |
|  |
| **Tanórán átadandó információk** |
| Köszönöm a figyelmet! |