**1. dia**

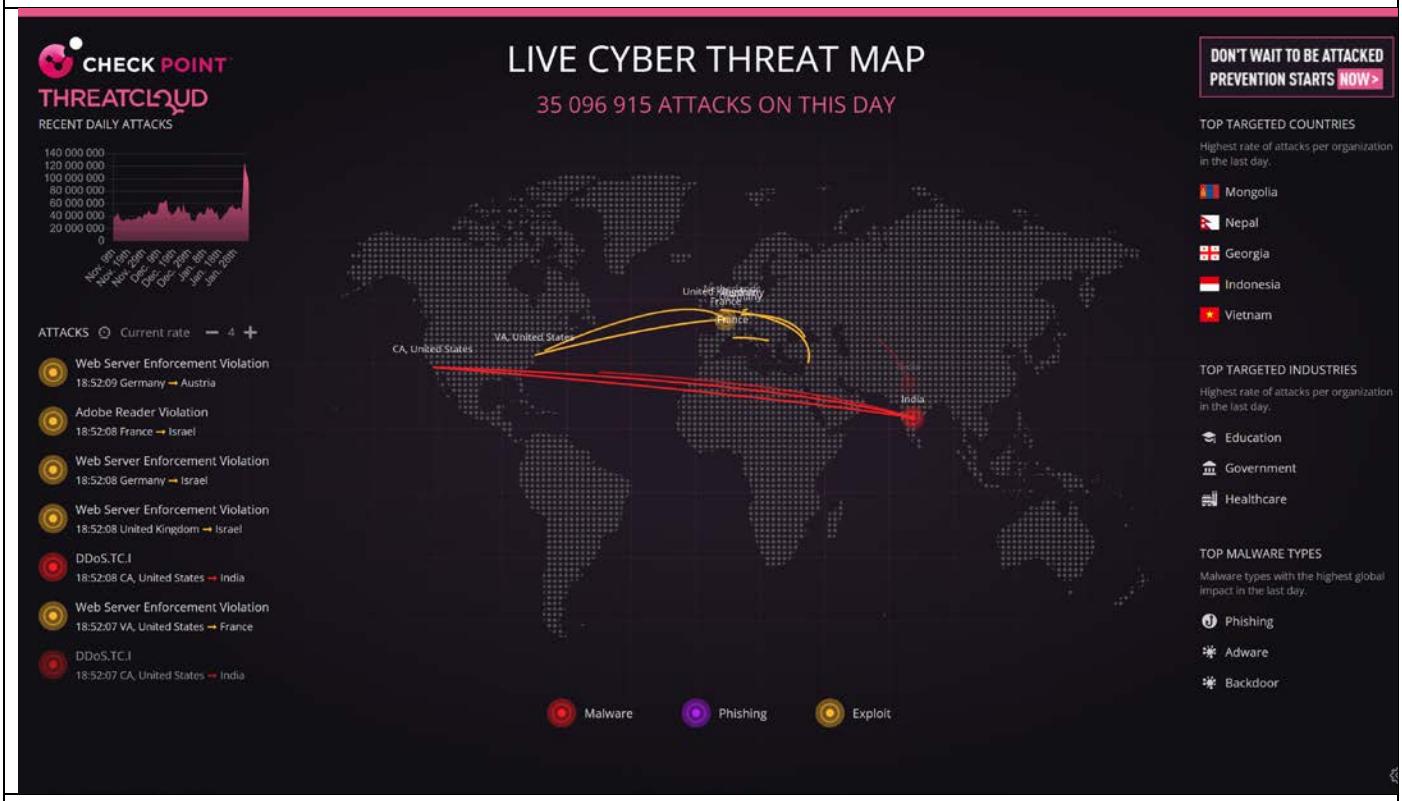

**Tanórán átadandó információk**

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.
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




### Tanórán átadandó információk

**ÉLŐ KIBERFENYEGETETTSÉGI TÉRKÉP (**https://threatmap.checkpoint.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. A támadásokban részt vevő fő (TOP) kártevő típusokat lásd jobboldalt alul.

**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 fent: támadások napi számának alakulása 3 hónapos időtávon
- Bal oldalon lent: a térképen megjelenő támadások részletei
- Jobb oldalon fent: TOP célpont országok
- Jobb oldalon középen: TOP célpont iparágak

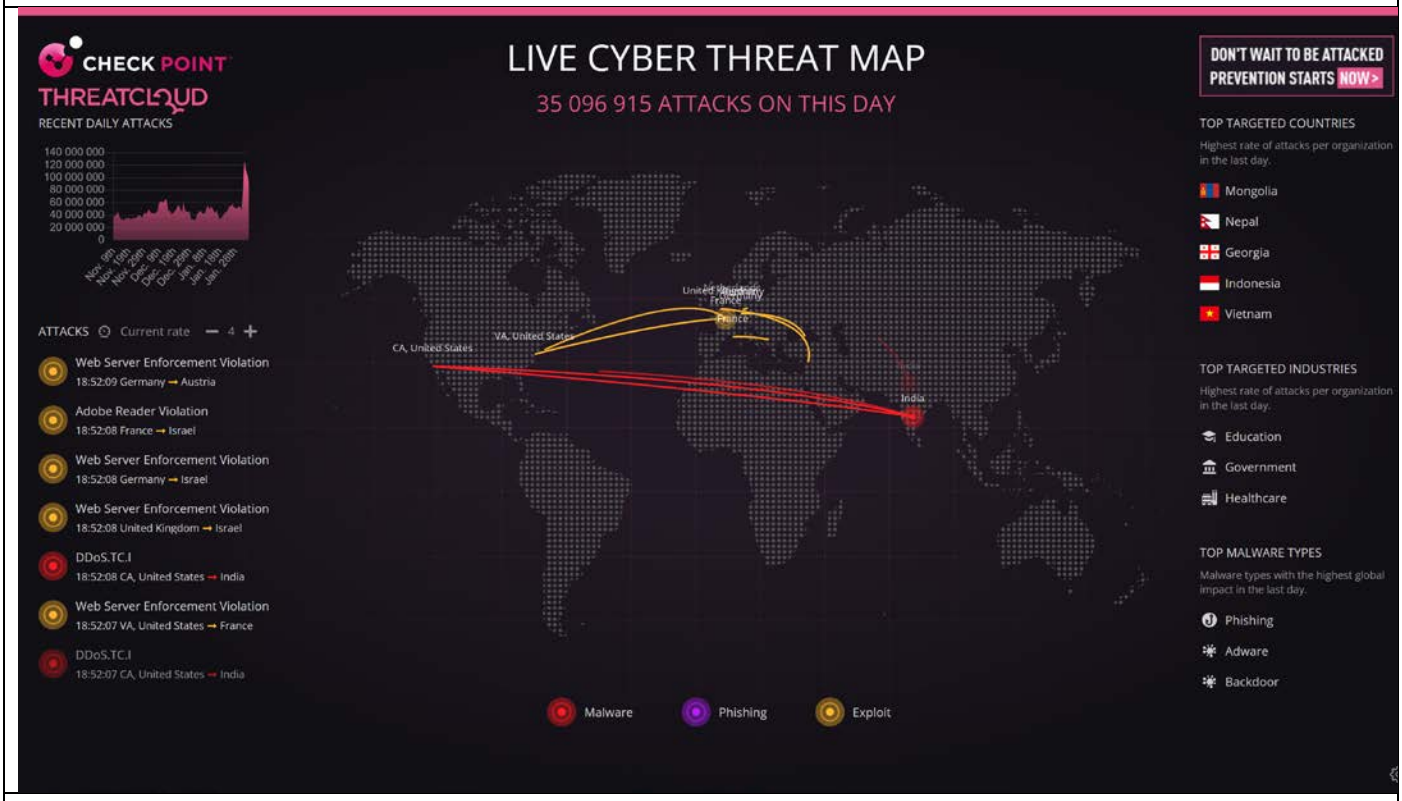
- Jobb oldalon lent: TOP kártevő típusok
- Alul: Jelmagyarázat
  - *Malware*: kártevő szoftverek összefoglaló neve (ide tartoznak pl. a vírusok, agresszív reklámprogramok, kémprogramok)
  - *Phising*: adathalászat
  - *Exploit*: biztonsági rés, sérülékenység kihasználása különböző célokra (pl. rendszergazdai jogok megszerzése egy számítógépen)

Az esetek nagy százalékában ezek a típusú támadások (főleg ilyen nagy volumenben) automatizált módon történnek közvetlen emberi interakció nélkül.

**Technikai információ**

Amennyiben sikerült bemutatni az élő térképet, akkor a következő diát át kell ugrani.

## 3. dia




### 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 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.)

**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**

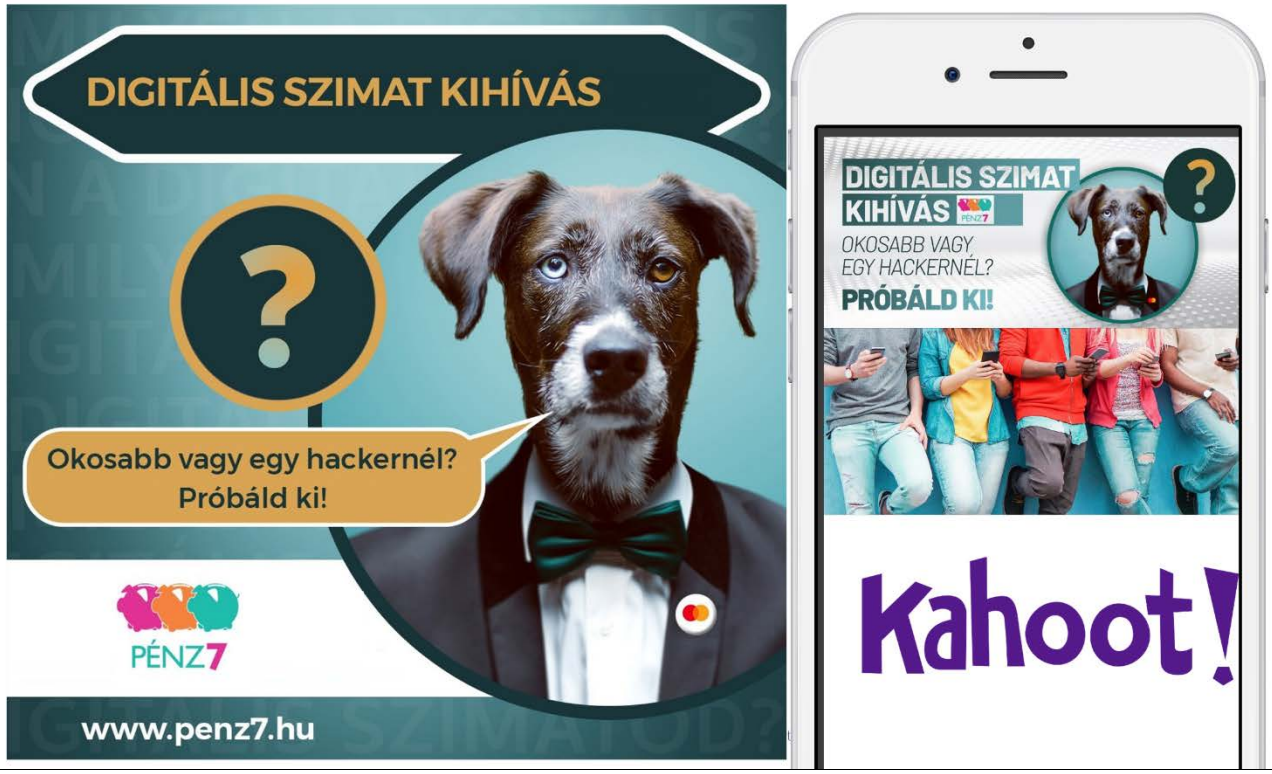
**A legrosszabb egyértelműen a D válasz.**

**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**




**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 tudástesztje mellett egy nyereményjátékot is elérnek a honlapon.**

**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**

# FELADAT

# ÁLLÁSPONT

FINTELLIGENCE PÉNZÜGYI KULTÚRA KÖZPONT
MAGYAR BANKSZÖVETSÉG
PÉNZ7
PÉNZIRÁNYTŰ

## 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 álláspontón 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, 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.

4.. Az egyes bankkártyák használatát különböző tranzakciós limitek beállításával tudjuk korlátozni. Pl. vásárlás napi maximum 30 000,- 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 a mobilunkon.

**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:**
- kis és nagy betűket is tartalmaz
- számok is vannak benne
- speciális karaktert is találhatunk benne (pl. dollár jel)
- 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**

| Karakterek száma | Csak számok | Kisbetűk | Kis- és nagybetűk | Számok, kis- és nagybetűk | Számok, kis- és nagybetűk, speciális karakterek |
|---|---|---|---|---|---|
| 4 | azonnal | azonnal | azonnal | azonnal | azonnal |
| 5 | azonnal | azonnal | azonnal | azonnal | azonnal |
| 6 | azonnal | azonnal | azonnal | azonnal | azonnal |
| 7 | azonnal | azonnal | 2 mp | 7 mp | 31 mp |
| 8 | azonnal | azonnal | 2 perc | 7 perc | 39 perc |
| 9 | azonnal | 10 mp | 1 óra | 7 óra | 2 nap |
| 10 | azonnal | 4 perc | 3 nap | 3 hét | 5 hónap |
| 11 | azonnal | 2 óra | 5 hónap | 3 év | 34 év |
| 12 | 2 mp | 2 nap | 24 év | 200 év | 3000 év |
| 13 | 19 mp | 2 hónap | 1000 év | 12 ezer év | 202 ezer év |
| 14 | 3 perc | 4 év | 64 ezer év | 750 ezer év | 16 millió év |
| 15 | 32 perc | 100 év | 3 millió év | 46 millió év | 1 milliárd év |
| 16 | 5 óra | 3000 év | 173 millió év | 3 milliárd év | 92 milliárd év |
| 17 | 2 nap | 69 ezer év | 9 milliárd év | 179 milliárd év | 7 billió év |
| 18 | 3 hét | 2 millió év | 467 milliárd év | 11 billió év | 438 milliárd év |

Szm7$z$z,Um@n,Je7,

13

Forrás: Hive Systems

**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.

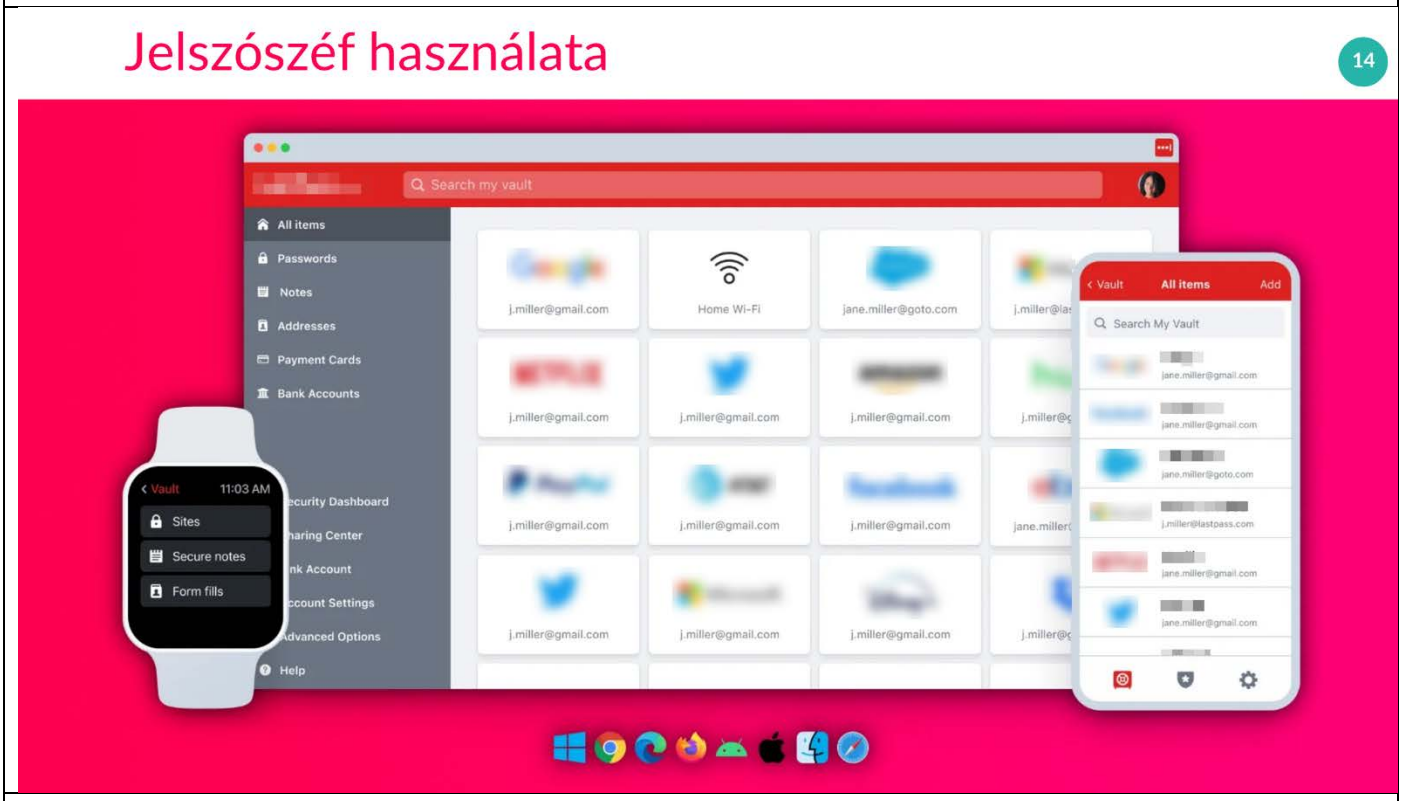
Az imént megalkotott jelszavunk (Szm7$z$z,Um@n,Je7,) 18 karakter hosszú és a lehető legösszetettebb (minden lehetséges karakter típust tartalmaz), így meglehetősen biztonságosnak tekinthető.

**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).

**14. dia**




**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**


**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?**

**16. 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.

## 17. dia

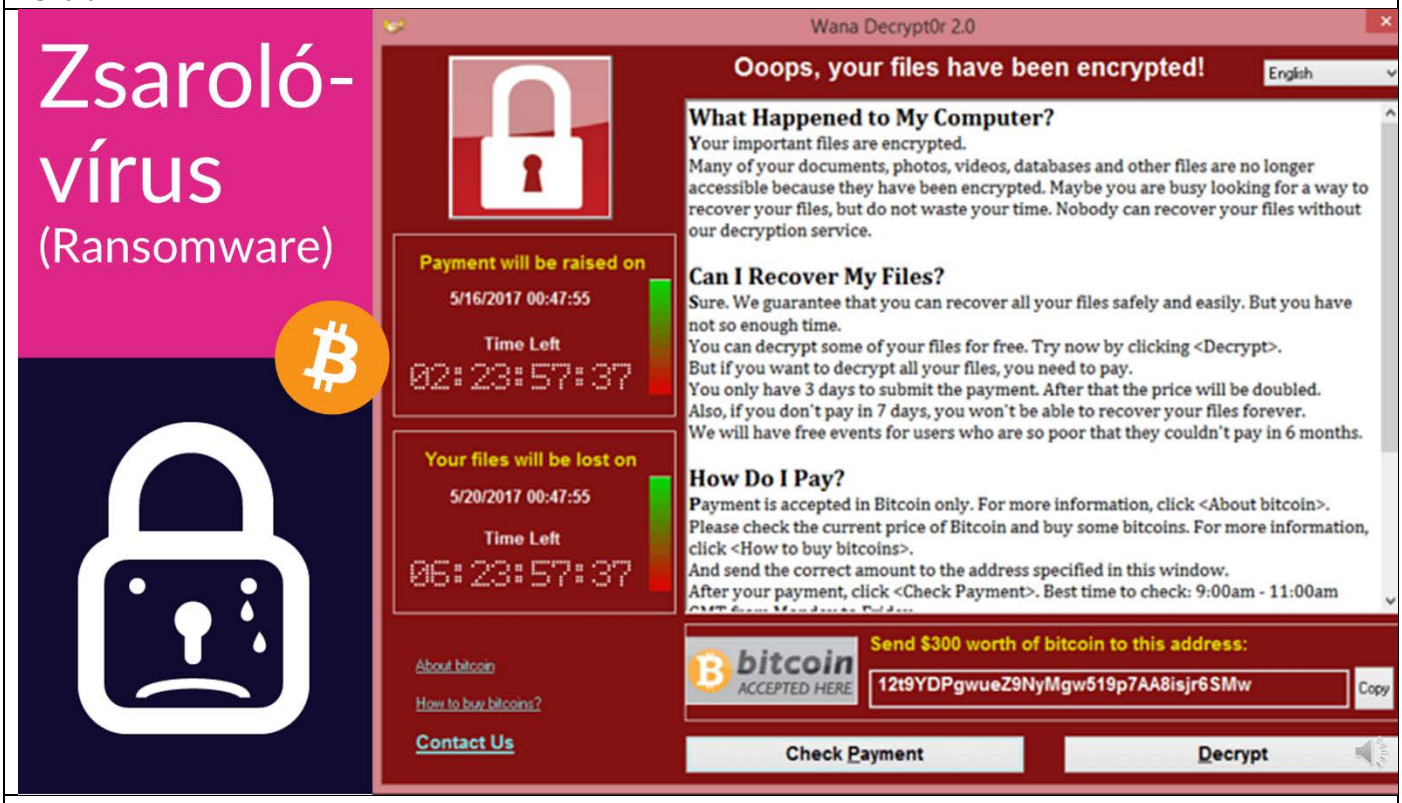

### Tanórán átadandó információk

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

**18. 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.

**19. dia**

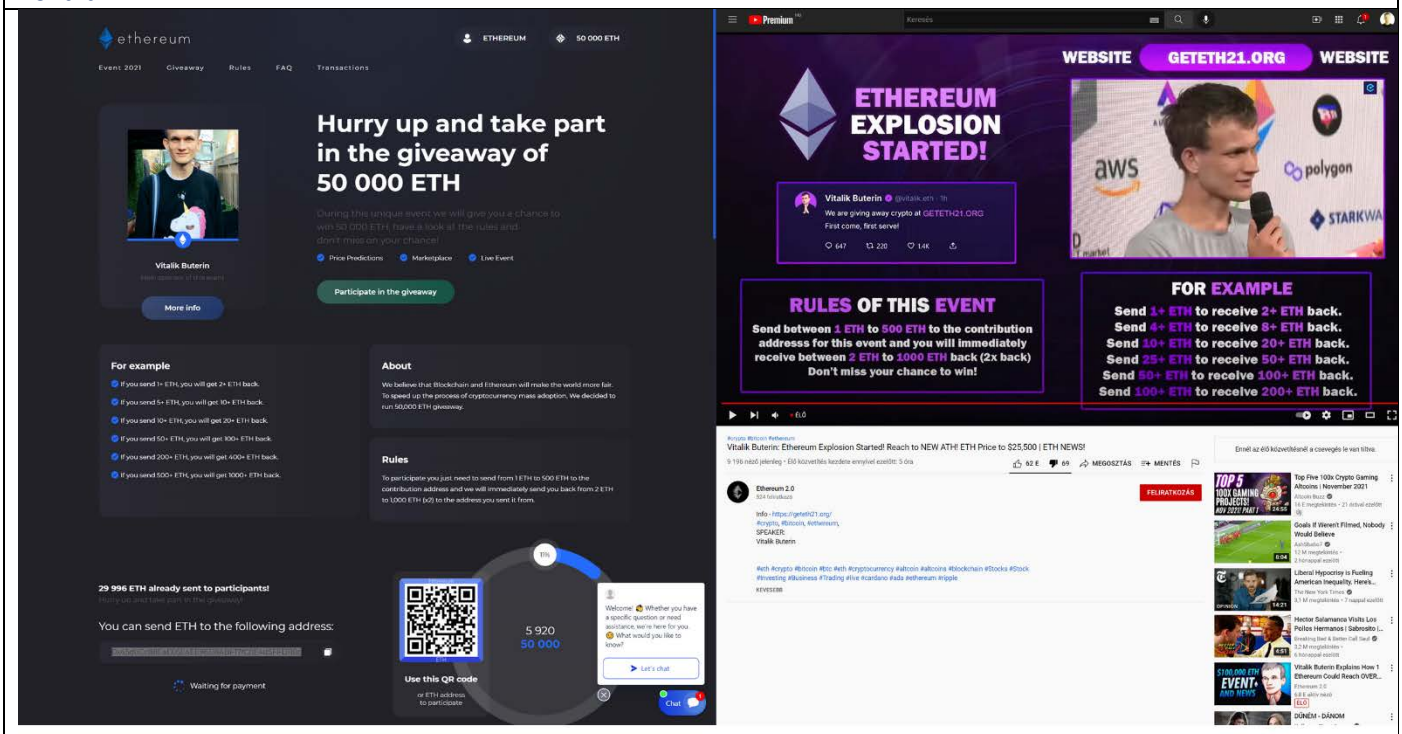

**Tanórán átadandó információk**

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 sürgetésről, egyszeri lehetőségről, lemaradásról még lesz szó a következő dián.

## 20. dia




www.penz7.hu
PÉNZ7 – Pénzügyi és vállalkozói témahét
20

### Tanórán átadandó információk

**Nincs ingyen pénz!!!**

Az egyik leggyakoribb formula: Küldj nekünk X összeget, visszaküldünk 2X-et.

Ez biztosan mindig csalás!

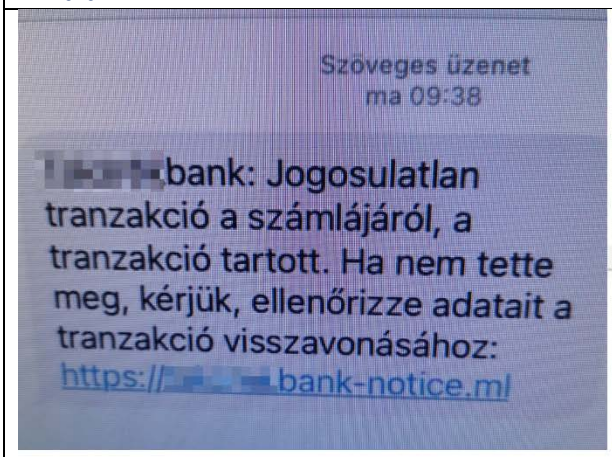
Sok esetben, ahogy az itt látható példában is:

- egyébként legális, ismert felületen jelenik meg (pl. Youtube)
- kriptoeszközt használ
- sürget, a FOMO jelenséget igyekszik kihasználni

### Háttérinformációk

**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.

**21. dia**




# Hamis banki vagy csomagküldő üzenetek



**Tanórán átadandó információk**

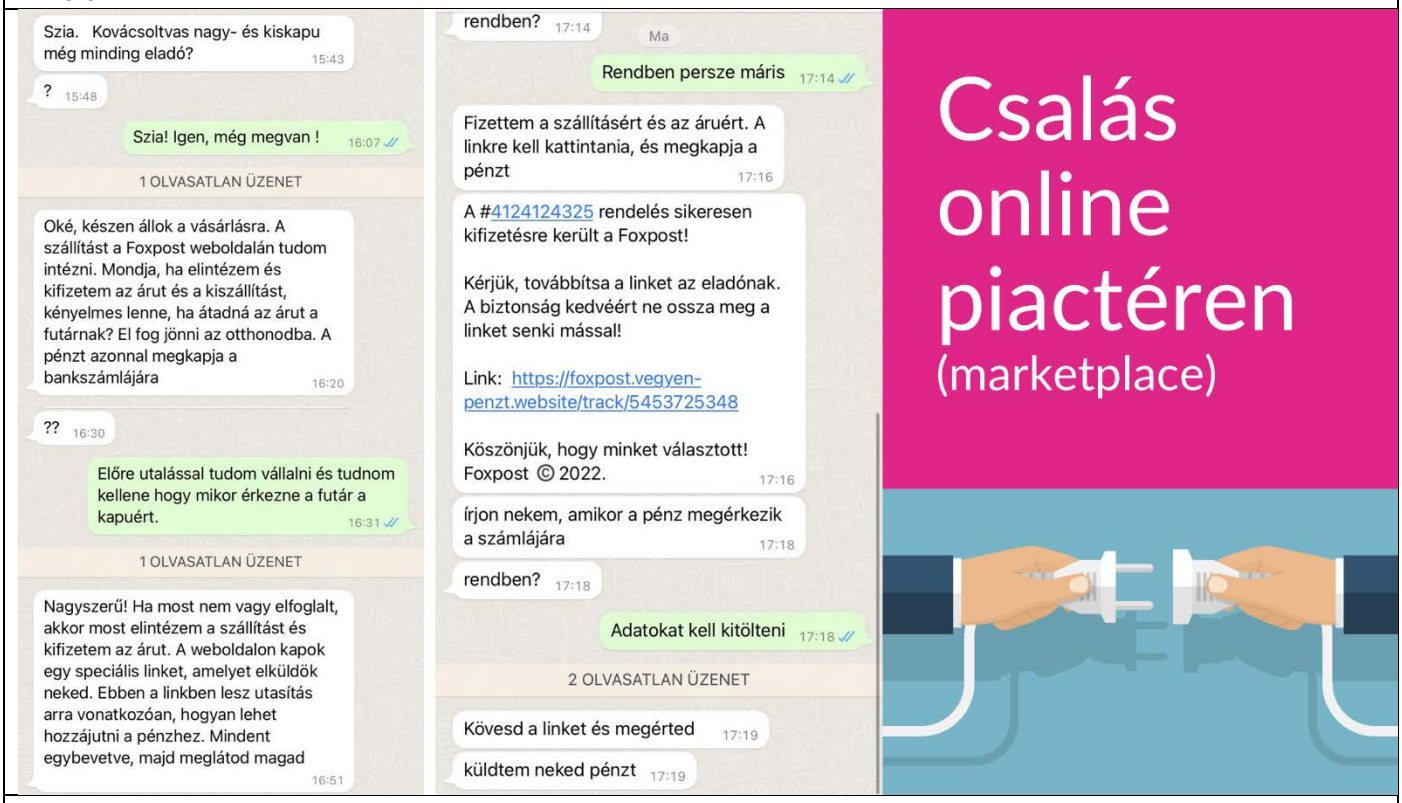
Napjainkban Magyarországon is elég gyakori a hamis banki vagy csomagküldő szolgáltató üzenetek alkalmazása…

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)

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.

## 22. 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**

**23. 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.

**24. dia**


**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.

**25. 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!**

**26. dia**

# Pénzügyi biztonság a kibertérben

KiberPajzs
Védelem a pénzügyekben

PÉNZ7

MAGYAR BANKSZÖVETSÉG

NEMZETI KIBERVÉDELMI INTÉZET

FINTELIGENCE PÉNZÜGYI KULTÚRA KÖZPONT

PÉNZIRÁNYTŰ

**Tanórán átadandó információk**

Köszönöm a figyelmet!