



Korszerű pénzkezelés - DIGITÁLIS BIZTONSÁG

.....









Tanórára felkészítő anyag tanárok és önkéntesek számára

9-12. évfolyam

PÉNZ7 – Pénzügyi és vállalkozói témahét

2020. március 2-6.

Üdvözlés, bevezetés	 Korszerű pénzkezelés - DIGITÁLIS BIZTONSÁG    
1. dia	
Átadandó információk	
<p>Erre a tanórára a PÉNZ7 – Pénzügyi és vállalkozói témahét c. program keretében kerül sor.</p> <p>A PÉNZ7 egy európai kezdeményezés része, amelynek célja, hogy a fiatalok tudatosabban kezeljék pénzügyeiket, többet tudjanak a gazdaság és a pénzvilág működéséről.</p> <p>Miközben megbeszéljük majd a mai izgalmas témánkat, Magyarország és sok más ország iskoláiban is ugyanezt teszik a diákok (jelenleg is, illetve az egész héten).</p> <p>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.</p>	
Az önkéntes szerepe (ha részt vesz az órán)	
Rövid bemutatkozás. (A tanár üdvözlje és kérje fel a bemutatkozásra.)	
Üdvözlés, bevezetés	
2. dia	
Átadandó információk	
<p>A mai óra célja a „szimat” javítása.</p> <p>Hogy milyen veszélyeket kell ügyesen kiszagolnunk, az a továbbiakban kiderül.</p> <p>Előtte bemelegítésként egy rövid kvízzel kezdünk...</p>	
Az önkéntes szerepe (ha részt vesz az órán)	
-	

1. feladat: Bemelegítő (Kahoot) kvíz

3. dia (vagy 4-8. dia)

kahoot.it



Átadandó információk

Nyissátok meg a mobilotokon a Kahoot alkalmazást vagy a böngészőben a kahoot.it oldalt és írjátok be a kivetített kódot!

Az önkéntes szerepe (ha részt vesz az órán)

A kvíz levezetése lehet az önkéntes feladata, illetve szükség esetén segíthet a tanulóknak a kvízhez való csatlakozásban.

A kvíz erejéig váltás a Kahootra böngészőben (<http://bit.ly/P7-2020q2> – a fényképre kattintva is elérhető), aztán folytatás a prezentációval A JOBB ALSÓ SAROKBAN LÉVŐ KAHOOT LOGÓRA KATTINTVA!

Amennyiben esetleg technikai problémába ütközik a szoftver használata, a kvízkérdéseket a 4-8. diák segítségével is fel lehet tenni (megoldások a jegyzetben). Ez esetben a diavetítés során, simán billentyűlenyomással (space/enter/...) lépünk tovább!

1. Mi a leginkább óvatos viselkedés ha bankunk adatagyűjtés céljából keres fel bennünket egy ismeretlen telefonszámról?

A

A hívást óvatosan tekintjük.

Magyar Bankszövetség

B

Visszahívjuk kiérünk és felkeressük a bankot az ügyfélszolgálatán.

FINET
Magyar Nemzeti Bank
10527 Budapest, Széchenyi István tér 1.

C

Válaszolunk a kérdésekre.

FINTELLIGENCE
www.finteelligence.com

D

Meglepetészik honnant tudják a telefonszámunkat, és válaszolunk.

2. Melyik személyes adataid lemásolása esetén tudnak a legnagyobb valószínűséggel visszaéléseket elkövetni?

A

Telefonszám, naptár, e-mail-cím és lakcímeted.

Magyar Bankszövetség

B

Bankkártyaszám, lakcímeted és telefonszám.

FINET
Magyar Nemzeti Bank
10527 Budapest, Széchenyi István tér 1.

C

Bankkártya, bankkártya, telefonszám és bankkártya PIN kódja.

FINTELLIGENCE
www.finteelligence.com

D

Bankkártyaszám, név, a kártya érvényesség dátuma és CVV2 biztonsági szám.

3. Melyik online jelszó a legkevésbé ajánlott?

A

H3l0k4

Magyar Bankszövetség

B

987651

FINET
Magyar Nemzeti Bank
10527 Budapest, Széchenyi István tér 1.

C

Szövezt7#v1sz

FINTELLIGENCE
www.finteelligence.com

D

1oo#B1zDns4g

4. Melyik személyes jellemző másolatával történhet visszaélés a legkisebb valószínűséggel?

A

Lábnyom

Magyar Bankszövetség

B

Arccod

FINET
Magyar Nemzeti Bank
10527 Budapest, Széchenyi István tér 1.

C

Hálgod

FINTELLIGENCE
www.finteelligence.com

D

Fuflid

5. Milyen csatornákon próbálhatják lehalászni az adataidat?

A

Szinte mindenhol érhetek támadások.

Magyar Bankszövetség

B

Telefonon

FINET
Magyar Nemzeti Bank
10527 Budapest, Széchenyi István tér 1.

C

Társkereső oldalak cetszobáiban

FINTELLIGENCE
www.finteelligence.com

D

Emailen

Kérdés:
Mivel fizetsz, ha nem készpénzzel?

9. dia

MIVEL FIZETSZ
HA NEM
KÉSZPÉNZZEL ?



Átadandó információk

Soroljatok fel nem készpénzes fizetési lehetőségeket!

- Ajándékkártya / ajándékutalvány
- Bankkártya
- Mobiltelefon / okosóra
- Átutalás
- ...

Az önkéntes szerepe (ha részt vesz az órán)

Célzott kérdéssel segítheti a diákokat a válaszadásban. Pl. „Legtöbbször hogyan kapják a felnőttek a fizetésüket?” (átutalással)

2. feladat: Álláspont

10. dia

FELADAT ÁLLÁSPONT



FINTELLIGENCE
PÉNZÜGYI KULTÚRA KÖZPONT

Magyar
BANKÖVETÉS

PÉNZ7

PÉNZIRÁNYTŰ

Átadandó információk

Az osztály véleményét nyilvánít a következő állításról:

„Egy 16 éves diáknak jó ha van bankszámlája és bankkártyája” (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 egy 16 éves diáknak legyen bankszámlája és használjon bankkártyát. Az ülő diákok szerint pedig ebben az életkorban nincs szükség bankszámlára és bankkártyára.

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!

Érdeemes úgy vezetni a beszélgetést, hogy szóba kerüljenek:

1. készpénzhasználat előnyei
2. készpénzhasználat kockázata, veszélyei, hátrányai
3. bankkártya-használat előnyei
4. bankkártya-használat kockázata, veszélyei, hátrányai.

(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 önkéntes szerepe (ha részt vesz az órán)

A beszélgetés irányítása lehet az önkéntes feladata.

Bankkártya diákoknak?

11. dia

Bankkártya diákoknak?
Lehet egy diáknak bankkártyája?

KISEBBERNEK
A 18 év alattiak csak a szülők vagy a törvényes képviselők hozzájárulásával nyithatnak bankszámlát, és igényelhetnek hozzá bankkártyát.

LEHETSÉGES
A 18 év alattiak csak a szülők vagy a törvényes képviselők hozzájárulásával nyithatnak bankszámlát, és igényelhetnek hozzá bankkártyát.

NAGYOKNAK
A 18. életévet betöltve bárki önállóan létesíthet bankszámlát, és igényelhet hozzá különféle banki szolgáltatásokat, így bankkártyát is.

FINTELLIGENCE
PÉNZÜGYI KULTÚRA KÖZPONT

Magyar
BANKSZÖVETÉS

PENZ7

PÉNZIRÁNYTŰ

Átadandó információk

Az előző feladatban megbeszélt előnyök és hátrányok összevetése alapján könnyen lehet, hogy valaki arra a következtetésre jut, hogy szívesen használna bankkártyát.

Nézzük meg hogyan lehet egy diáknak bankkártyája – ezzel már el is árultam, hogy lehet... A bankok kínálnak készpénzkímélő megoldásokat diákoknak.

A 18 év alattiak csak a szülők vagy a törvényes képviselők hozzájárulásával nyithatnak bankszámlát, és igényelhetnek hozzá bankkártyát.

A 18. életévet betöltve bárki önállóan létesíthet bankszámlát, és igényelhet hozzá különféle banki szolgáltatásokat, így bankkártyát is.

Az önkéntes szerepe (ha részt vesz az órán)

-

BANK, BANKSZÁMLA, BANKKÁRTYA

12. dia



BANK, BANKSZÁMLA, BANKKÁRTYA

MIRE AKARJUK HASZNÁLNI A KÁRTYÁT?

Vásárlás? Készpénzfelvétel? Itthon vagy külföldön?
Saját pénzből vagy hitelből is?

MIT KÍNÁLNAK A BANKOK?

Bankszámlához kapcsolódik? Hitelkeret? Kamatkondíciók?
Egyszerű? Biztonságos? Mobilfizetés? Külföldön is? Pénzmem?

MI MENNYIBE KERÜL?

Éves kártyadíj? Készpénzfelvétel díja? Hitelkamat?
Egyéb hiteldíjak? Betéti kamat?

BANKSZÁMLA választó program
bit.ly/szvp

MÉRLEGELÉS, KÁRTYAVÁLASZTÁS

Az elvárásaink és a kínálat összevetése alapján megalapozottan tudunk bankkártyát
választani.

Átadandó információk

A választás egyik legfontosabb szempontja, hogy MIRE AKARJUK HASZNÁLNI A KÁRTYÁT?
Vásárlás? Készpénzfelvétel? Itthon vagy külföldön?
Saját pénzből vagy hitelből is?

Természetesen meg fogja határozni a lehetőségeinket, hogy MIT KÍNÁLNAK A BANKOK.
Bankszámlához kapcsolódik? Hitelkeret? Kamatkondíciók? Egyszerű? Biztonságos?
Mobilfizetés? Külföldön is? Pénzmem?

Mint minden szolgáltatásnál, a bankkártya esetében is fontos tisztában lennünk a
felmerülő költségekkel, azaz azzal, hogy MI MENNYIBE KERÜL?
Éves kártyadíj? Készpénzfelvétel díja? Hitelkamat? Egyéb hiteldíjak? Betéti kamat?

Mivel az egyes bankok számlacsomag konstrukciói jelentősen eltérhetnek egymástól, ezért
érdemes tételesen áttekinteni, összehasonlítani, hogy mi mennyibe kerül.
Ma már az interneten is összehasonlíthatók a bankszámlák díjai, szolgáltatásai, például a
Magyar Nemzeti Bank Bankszámla választó oldalán az itt látható linken (bit.ly/szvp).

MÉRLEGELÉS, KÁRTYAVÁLASZTÁS

Az elvárásaink és a kínálat összevetése alapján megalapozottan tudunk bankkártyát
választani.

Az önkéntes szerepe (ha részt vesz az órán)

-

Bankkártyás fizetés – biztonsági tippek

13. dia

Bankkártyás fizetés – biztonsági tippek

- Soha ne tartsuk a PIN kódunkat felírva a bankkártya közelében!
- Mindig takarjuk a PIN kódunkat!
- Ha bármilyen gyanús jelenséget észlelünk kártyás fizetés során, azonnal hívjuk a bankunkat és jelentsük!



MAGYAR
BANKSZÖVETSÉG

FENYI
www.fenyi.hu
FINTELLIGENCE
FINTELLIGENCE

FINTELLIGENCE
FINTELLIGENCE

Átadandó információk

Ha már van bankkártyánk, nagyon fontos, hogy körültekintően bánjunk vele, mert ha nem így teszünk, könnyen pénzt veszíthetünk.

Nézzük a legfontosabb tanácsokat!

Soha ne tartsuk a PIN kódunkat felírva a bankkártya közelében.

Lehetőleg egyáltalán ne írjuk fel.

Mindig takarjuk a PIN kódunkat!

...ha pénzt veszünk fel, vagy ha kártyával vásárolunk.

Ha bármilyen gyanús jelenséget észlelünk kártyás fizetés során, azonnal hívjuk a bankunkat és jelentsük!

Pl. valamikor kis összegű levonásokat látunk, pedig nem vásároltunk.

Az önkéntes szerepe (ha részt vesz az órán)

-

Bankkártyás fizetés – biztonsági tippek

14. dia



Bankkártyás fizetés – biztonsági tippek

- Soha ne tévesszük szem elől a bankkártyánkat és ne tartsuk olyan helyen, ahol jól látható!
- Online bankoláshoz használjunk biztonsági sms-t, az internetes vásárlásokhoz pedig webkártyát!
- Gondoskodjunk a szoftverek naprakészességéről és a megfelelő vírusvédelemről!

Magyar
BANKSZÖVETSÉG

FINIZ
www.finiz.hu
FINIZ – intelligens bankvilág

FINTELLIGENCE
FINTELLIGENCE

Átadandó információk

Soha ne tévesszük szem elől a bankkártyánkat és ne tartsuk olyan helyen, ahol jól látható! Ne adjuk ki a kezünkbe és semmiképpen se engedjük, hogy olyan helyre vigyék, ahol nem látjuk mi történik vele.

A képen látható szituáció esetleg akkor elfogadható, ha nem érintőkártyáról van szó és ott helyben történik az asztalnál a fizetés (a kártya terminálba való bedugásával).

A bankkártyánkat soha ne tartsuk látható helyre letéve, vagy a kezünkben – ma már egy átlagos okostelefon kamerája is alkalmas lehet arra, hogy fotók formájában rögzítse a kártyánk adatait.

Nem csak fizikai vásárlásra hanem online környezetben is használhatjuk a kártyánkat...

Online bankoláshoz használjunk biztonsági sms-t, az internetes vásárlásokhoz pedig webkártyát!





Az erős ügyfélhitelesítés még inkább ebbe az irányba mutat: a közeljövőben minden kártyás online vásárlásnál meg fogjuk erősíteni a tranzakciót egy biztonsági SMS-sel vagy biometrikus azonosítással (erről később még lesz szó).





WEBKÁRTYA: Egy olyan (jellemzően virtuális) kártya, amit speciálisan csak online vásárlásokra szokás használni. Eseti jelleggel tölthetjük fel a vásárláshoz éppen szükséges összeggel, így legrosszabb esetben is csak az ezen a másodlagos kártyánkon lévő összeget veszíthetjük el.

Gondoskodjunk a szoftverek naprakészességéről és a megfelelő vírusvédelemről!
Különösen az online bankolásra használt számítógépünkön vagy a mobilunkon.

Az önkéntes szerepe (ha részt vesz az órán)

-

Hogyan fizess a mobiloddal?	15
15. dia	<p style="text-align: center;">Hogyan fizess a mobiloddal? <small>(gy. mindig nézd le a "penztárcád")</small></p>  <p style="text-align: center;">    </p>
Átadandó információk	
<p>A legtöbb mobilfizetési megoldás napjainkban arra épül, hogy a mobilkészlet (okostelefon, okosóra stb.) a bankkártyánk egy virtuális változatát tárolja. A biometrikus azonosítási lehetőségek használatával a mobilfizetés még biztonságosabb lehet, mint a bankkártya alkalmazása.</p> <p>A közeljövőben várható az azonnali átutalás alapú mobilfizetési megoldások elterjedése is, így hát tegyünk egy rövid kitérőt és nézzük, meg mi is az azonnali átutalás.</p>	
Az önkéntes szerepe (ha részt vesz az órán)	
-	

Azonnali fizetési rendszer	16
16. dia	<p style="text-align: center;">Azonnali fizetési rendszer <small>2020. március 2-től</small></p>  <p style="text-align: center;">    </p>
Átadandó információk	
<p>Átutalással két bankszámla között tudunk pénzt mozgatni. 2020. március 2-től ezt az év bármely napján, hétfőig és ünnepnapon is, napi 24 órában megtehetjük és a pénz pár másodpercen belül oda is ér a címzetthez.</p>	
<p>Az átutalások indíthatók mobiltelefonszámra, e-mail címre vagy adószámra is (nem kell feltétlenül ismerni a címzett bankszámlaszámát). Az új fizetési kérelemmel a kedvezményezett kezdeményezheti a fizetést.</p>	
<p>Az átutalások akkor teljesülnek pár másodpercen belül, ha azok elektronikusan indított, belföldi, forint tranzakciók 10 millió forintos értékhatárig.</p>	
<p>Pár másodperc nagyon rövid idő, ezért érdekes az Azonnali Fizetési Rendszer a mobilfizetések szempontjából is.</p>	
Az önkéntes szerepe (ha részt vesz az órán)	
-	

TOP 3 biztonsági tanács Így használd az okostelefonod!

17. dia



Átadandó információk

Visszatérve az okostelefonjainkhoz, nézzünk 3 kiemelt tanácsot a biztonságos használatához.

MINDIG HIVATALOS appokat használj!

Mindig a hivatalos applikáció áruházakban, a gyártótól szerezd be a szoftvereket! A nem megbízható forrásból származó applikációk káros kódot tartalmazhatnak és adataink, illetve pénzünk elvesztéséhez vezethetnek.

Figyelj oda, hol töltöd a készülékedet!

Soha ne töltsd a telefonodat ismeretlen kábellel. A legtöbb töltőkábel adatátvitelre is alkalmas, emiatt veszélyes kávézóban, repülőtéren és egyéb nyilvános helyeken kihelyezett töltőállomásokra vagy pl. más számítógépére csatlakozni. A legjobb, ha csak a telefon saját töltőjét használod, leginkább otthon. Ha mindenképpen szükséges máshol is töltened a telefonodat külső akkumulátort vagy hordozható akkumulátoros töltőt (power bankot) használj!

Védd úgy a mobilodat mint a pénztárcádat!

Ne hagyd őrizetlenül az eszközödet! A készülék feloldásához használj jelkódot, vagy biometrikus azonosítást!

Na de mi is az a biometrikus azonosítás? (következő dia)

Az önkéntes szerepe (ha részt vesz az órán)

-

Kérdés: Mi az a biometrikus azonosítás?

18. dia

**MI AZ A
BIOMETRIKUS
AZONOSÍTÁS** 

Átadandó információk

Tudtok mondani biometrikus azonosítási megoldásokat?

VÁLASZLEHETŐSÉGEK

Elterjedt megoldások:

- Ujjlenyomat (mobileszközökben jellemző)
- Arcfelismerés / arc szkennelés / Face ID (mobileszközökben jellemző)
- Írisz / retina (szem) azonosítás
- Csukló vagy tenyér érhálózatának mintázata alapján történő azonosítás
- Tenyérlenyomat
- Hangfelismerés

Ritkább vagy más területeken használt megoldások:

- Az egyén mozgása (pl. járása vagy testtartása) alapján
- Fül alakja alapján
- Ujjak vagy kéz alakja, méretei
- DNS-azonosítás
- Gépelési stílus
- Dinamikus aláírás-azonosítás (ahogyan aláír az illető)

Az önkéntes szerepe (ha részt vesz az órán)

Célzott kérdésfeltevéssel segítheti a diákokat a válaszadásban.

Élő kiber-veszély térkép bemutatása

19. dia (vagy 20. dia)



Átadandó információk

MIT LÁTUNK?

A térkép megmutatja, hogy egyetlen nap alatt több millió hekker-támadás zajlik (a fenti számláló mutatja, hogy a mai napon hány db volt már). A világ különböző részein zajló támadások folyamatosak, kormányokat, vállalatokat és egyéneket is érintenek.

Fő üzenet: Gyakorlatilag zajlik a III. világháború – a hadszíntér ezúttal az internet.

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!

A térkép további részletei:

- Bal fent: támadások napi száma az elmúlt 3 hónapban
- Bal lent: a térképen megjelenő támadások részletei
- Jobb fent: TOP célpont országok
- Jobb középen: TOP célpont iparágak
- Jobb lent: TOP kártevő típusok
- Alul: Jelmagyarázat
 - *Malware*: kártevő szoftverek összefoglaló neve (ide tartoznak pl. a vírusok, agresszív reklámprogramok, kémprogramok)
 - *Phising*: adathalászat (később lesz róla szó)
 - *Exploit*: Biztonsági rés kihasználása különböző célokra (pl. rendszergazdai jogok megszerzése egy számítógépen)

Az önkéntes szerepe (ha részt vesz az órán)

-

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.)

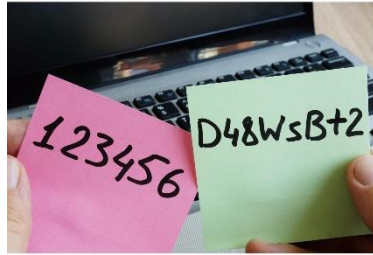
Amennyiben nincs lehetőség internet használatára, vagy más okból nem használható az élő térkép, úgy a 20. dián látható videót mutassuk be (automatikusan indul, 1 perc 20 másodperc hosszú, de bármikor tovább lehet lépni, illetve újraindul ha véget ért.)

Ha esetleg a videó lejátszása sem megvalósítható (pl. a számítógép gyenge teljesítménye miatt), az ezen a dián látható kép alapján beszéljünk.

(Amennyiben sikerült bemutatni az élő térképet, a 20. dia átugrandó.)

Beszélgetés a jelszavak biztonságáról, erős jelszó létrehozási módszer bemutatása.

21. dia



MILYEN
AZ ERŐS
JELSZÓ?

MAGYAR
BANKSZÖVETSÉG

FINIZ
www.finiz.hu
FINIZ - intelligens bankintézmény

FINTELLIGENCE
FINTELLIGENCE KFT.

Átadandó információk

A legtöbb banki művelethez (pl. Netbank belépés) felhasználónévre és jelszóra van szükség. Ennek megfelelően az imént bemutatott térképen látott támadások jelentős része is ezen információink megszerzésére irányul.

Nagyot léphetünk előre az online önvédelemben ha biztonságos jelszavakat használunk. Nézzük meg, milyen is a jó, biztonságos, avagy „erős” jelszó (ami már az óra eleji tesztben is szóba került)!

A képen láthatók közül melyik az erősebb? Egyáltalán miért van szükségünk erős jelszavakra?

Válasz: a jobb oldali

Válasz: nem szeretnénk hogy bárki rá tudjon jönni és hozzáférjen az adatainkhoz vagy a pénzünkhez

Mit gondoltok, melyek a leggyakrabban használt jelszavak? Válasz: „123456” (ki is van vetítve), illetve „jelszó”. (Angol nyelvterületen „123456” és „password”.) Ezt elloptott, kiszivárgott jelszavak adatbázisainak elemzéséből lehet tudni.

Tudtok még mondani rossz jelszavakat?

Mitől rosszak ezek? Milyen jelszavakat ne használjunk semmiképp?

- Ne legyenek személyes információk a jelszavainkban (név, becenév, cím, e-mail cím, telefonszám, rokon vagy háziállat neve, születési dátum stb.)!
- Ne legyen semmi a jelszavunkban, ami könnyen hozzánk köthető (pl. kedvenc film, vagy játék neve)!

Még fontos tudnivaló:

- Soha ne oszd meg senkivel a jelszavadat (kivéve szülők, nevelők)!
- Ne írd fel a jelszavad! Ha mégis muszáj felírnod, olyan helyen tárold, ahol más nem találhatja meg.

Az önkéntes szerepe (ha részt vesz az órán)

-

Beszélgetés a jelszavak biztonságáról, erős jelszó létrehozási módszer bemutatása.

22. dia

Legyen saját „titkosírásod”!
Készíts csúper-szófontagok jelszót!

Micimackó minden kedden reggel sajtos-hagymás rántottát süt.

1. JELMONDAT
Az egész mondatot vegyél ki jelszóként!

Mmkrs-hrs.

2. BETŰK
Maradj a szavak kezdőbetűin!

3. TRÜKKÖK
Képzeld el a szavak kezdőbetűit összeírva!

Mm2r\$-hr\$.

FINTELLIGENCE
PÉNZÜGYI KULTÚRA KÖZPONT

Magyar BANKSZÖVETSÉG

PÉNZ7

NEMZETI KIBERVÉDELMI INTÉZET

Átadandó információk

A jó jelszó legfontosabb jellemzője, hogy mások által nagyon nehezen kitalálható, de számunkra könnyen megjegyezhető.

- 1. Nagyon jó lépés ebbe az irányba, ha egy JELMONDATot találunk ki jelszó helyet.**
Pl. „Micimackó minden kedden reggel sajtos-hagymás rántottát süt.”
- 2. Használhatjuk akár az egész mondatot is, de még jobb ha a szavak kezdőbetűit rakjuk össze.** Nagy betűk, írásjelek jó ha maradnak!

Ha rövid a mondatunk, használhatunk több betűt is a szavak elejéről (pl. minden szóból 2 betűt).

Figyeljünk oda hogy végül legalább 8 karakterünk legyen. (A legtöbb szolgáltatás ezt meg is követeli.)

- 3. Változtassunk meg néhány betűt számokra vagy speciális karakterekre az általunk kitalált szabályok szerint.**

A példánkban: „k” helyett „2” és „s” helyett „\$”

Kész az erős jelszavunk! Másnak nagyon nehéz lenne rájönnie, de mi emlékezni fogunk rá, hiszen csak a micimackós mondatunkat és néhány egyszerű szabályt kell megjegyeznünk.

Az önkéntes szerepe (ha részt vesz az órán)

-

Adathalászmódszerek és kivédési lehetőségek megismerése.

23. dia

A legerősebb jelszó sem ér semmit ha...

23



Átadandó információk

**A legerősebb jelszó sem ér semmit ha...
... ha ellopják.**

Hogyan lophatják el és hogyan tudjuk ezt elkerülni? A következő pár percben erről lesz szó.

Az önkéntes szerepe (ha részt vesz az órán)

-

Adathalászmódszerek és kivédési lehetőségeik megismerése.

24. dia

Adathalászat (Phishing) – Hogyan történik? 24



Átadandó információk

A "phishing" olyan adathalászmódszer, amellyel a csalók arra veszik rá a címzetteket, hogy adják meg személyes, pénzügyi és biztonsági adataikat. Az esetek többségében valamilyen – a valóságban nem létező – nyeremény vagy örökség ígéretével keresik meg a célpontokat, esetleg hivatalosnak tűnő (pl. adóhivatal) megkereséssel próbálkoznak, vagy valamilyen (nem valós) számla befizetésére akarnak rávenni.

A kiberbűnözők arra alapoznak, hogy az emberek elfoglaltak; első pillantásra ezek az e-mailek hivatalosnak tűnhetnek.

Vigyázzunk a mobil eszközök használata során! Az adathalászmódszer e-mailek nehezebben szűrhetők ki telefonon vagy tableten!

Az önkéntes szerepe (ha részt vesz az órán)

-

Adathalászmódszerek és kivédési lehetőségeik megismerése.

25. dia

Adathalászat (Phishing) – Mit tehetsz? 25



Átadandó információk

Mindig frissítsd a szoftvereid, beleértve a böngészőt, a víruskeresőt és az operációs rendszert is!

Légy óvatos, Ha egy „bank” üzenetben érzékeny információkat kér tőled (pl. az online banki jelszót)!

Olvasd el alaposan az e-mailt: hasonlítsd össze az üzenetet korábbi banki üzeneteiddel! Ellenőrizd, hogy van-e elírás vagy nyelvi hiba!

Ne válaszolj gyanús e-mailekre, inkább írd fel, ki küldte, majd továbbítsd a banknak!

Ne kattints a linkre, és ne töltsd le a mellékletet, inkább keress rá a címre a böngészőben! Ha kétségeid vannak, **ellenőrizd kétszer** a bank weboldalát vagy hívja a fel a bankot!

Az önkéntes szerepe (ha részt vesz az órán)

-

**3. feladat:
Ne akadj horogra!**

26-30. dia



Átadandó információk

A kivetített és kinyomtatva kiosztott e-mailekről a diákoknak el kell dönteniük, hogy valós hivatalos üzenet, vagy pedig adathalász levél.

Az egyes leveleknél (rövid áttekintés, elolvasás után) kézfeltartással szavazás, majd kérdés: ***Láttok-e valamilyen gyanús jelet, ami arra utal, hogy ez nem egy valódi üzenet?***
A tanár és a diákok közösen döntést hoznak.

A levelekben kitalált cégneveket használunk – erre célszerű felhívni a diákok figyelmét, hogy az ismeretlen név ne befolyásolja őket a döntésben.

Az önkéntes szerepe (ha részt vesz az órán)

A diákok feladaton való végig vezetése, a kinyomtatott e-mailek kiosztása.

A leveleket célszerű kinyomtatva is kiosztani a diákoknak!

27. dia



Számla-csalás

Gyanús jelek:

- Hiányzó ékezetek (pl. már a levél tárgyában is) és egyéb helyesírási hibák
- Nyelvtani, fogalmazási hibák, rossz „magyarság”
- Vélhetően nem valódi feladó cím: telenova.hu helyett telenovaszamla.hu
- Címzett: nem csak nekünk jött a levél (a mi e-mail címünkre), hanem valamiféle levelezési listára
- Linkre való kattintásra kér
- Sürget (fenyeget, hogy ha nem fizetek automatikusan „kikapcsol” az előfizetés)

28. dia



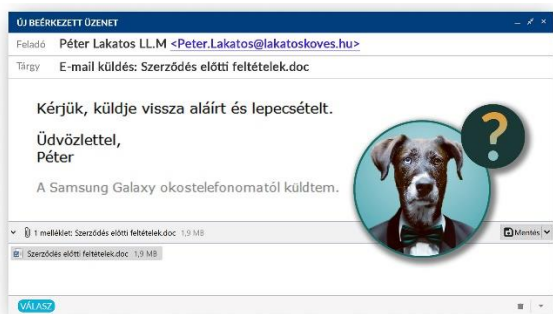
Pénzügyi adathalász levél

Gyanús jelek:

- A valós bankhoz nem köthető feladó cím: probank.hu helyett menteldok.com
- Címzett: Ismeretlen karaktersor, vélhetően nem csak nekünk jött a levél (a mi e-mail címünkre), hanem valamiféle levelezési listára
- Linkre való kattintásra kér (holott a bankunk soha nem kér ilyet, a banki szolgáltatásokat mindig a hivatalos honlapról elérhető internetbank, vagy banki mobilapplikáció segítségével használhatjuk)
- Arra hivatkozik, hogy a biztonságunk érdekében szükséges a lépés (sürget)

Profin megfogalmazott, helyesen írott levél is lehet adathalász támadás!

29. dia



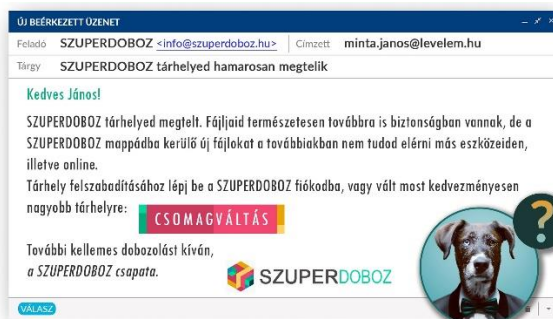
Veszélyes melléklet

Gyanús:

- Ismeretlen feladó
- Helyesírási, nyelvtani, fogalmazási hibák, rossz „magyarság”

Különösebb magyarázat nélkül melléklet megnyitására kér

30. dia



Valós szolgáltatástól kapott értesítés

- Ismert feladó (valóban használom ezt a szolgáltatást), tényleg a szuperdoboz.hu domainen érhető el
- Kimondottan nekem érkezett a levél
- A nevemen szólít
- Professionális fogalmazás

DE:

Ezek önmagukban nem elegendők. A legfontosabb, hogy csak olyan linkre kattintsunk, amiről biztosan tudjuk, hogy a valós szolgáltatáshoz vezet el.

Ilyen esetben a legjobb, ha nem az e-mailben található linket/gombot használjuk, hanem – a szokásos módon (pl. a itt a <https://www.szuperdoboz.hu> weboldalt megnyitva) - érzük el az e-mailben hivatkozott szolgáltatást (ahol megtudhatjuk róla, hogy valóban van-e teendőnk).

Általános biztonsági tippek

31. dia



Átadandó információk

01 - ... Ha ilyet kapunk, az adathalász támadás.

02 – ... Biztonságosabb online vásárlást tesz lehetővé.

03- ... helyette alkalmazzuk a szolgáltatónk által nyújtott mobil internetet. Amennyiben mégis a nyilvános Wi-Fi hálózat mellett döntünk, ne jelentkezünk be egy online fiókba sem. Fontoljuk meg egy VPN szolgáltatás használatát.

04 - Amennyiben nem használjuk, kapcsoljuk le a Wi-Fi, valamint a Bluetooth kapcsolatokat és minden egyéb szolgáltatás tiltsunk le eszözeinken, amelyet az adott időszakban nem alkalmazunk.

05 - ... vagyis rendelkeznek a legfrissebb biztonsági javításokkal.

06 – Időnként érdemes biztonsági mentést készíteni eszközeinkről, ügyeljünk arra, hogy a másolatok egy megbízható, jól védett helyen kerüljenek tárolásra.

Az önkéntes szerepe (ha részt vesz az órán)

-

Légy a család biztonsági szakértője!

32. dia



Átadandó információk

Remélem, hogy sokat javult a szimatotok és a jövőben nagyon ügyesen szagoljátok ki a veszélyeket!

Az óra után / otthon gondoljátok végig, hogy:

Ti biztonságban érzitek-e magatokat? Ha nem teljesen, akkor mit kell jobban csinálnotok? Hogyan tudtok segíteni a családotoknak, barátaitoknak, hogy az ő adataik és pénzüik nagyobb biztonságban legyen?

Mire kell odafigyelnetek és hol tudtok tovább tájékozódni a nagyobb biztonság érdekében.

... utóbbiban segítünk...

Az önkéntes szerepe (ha részt vesz az órán)

-

További tájékozódás

33. dia



Átadandó információk

További pénzügyi tudatossági információkért látogljátok a PÉNZ7 Facebook oldalát és keressétek fel a penz7.hu honlapot!

Az önkéntes szerepe (ha részt vesz az órán)

-

Digitális Szimat Kvíz

34. dia



Átadandó információk

Más tanórán vagy otthon végezhető feladat.

A diákok számára lehetőség nyílik próbára tenni a mai **Digitális biztonság - Korszerű pénzkezelés tanórához kapcsolódó** felkészültségüket a hacker támadások keresztműzében álló világunkban. A Magyar Bankszövetség online kvízzjátékán, az 50 kérdéses **DIGITÁLIS SZIMAT KVÍZ**en a 7-14. évfolyamos versenyzők **2020. március 2-14. között** mutathatják meg a témakörben megszerzett tudásukat. A 10 legjobb játékos valós időben, verseny keretében méri össze ismeretei pontosságát és gyorsaságát, értékes nyereményekért. A játék a PÉNZ7 honlapján elérhető a [PÉNZ7 KVÍZ menüpontban](#) a verseny ideje alatt. A játékban való részvétel lehetősége nyitott és kötelezettségtől mentes bárki számára.

Az önkéntes szerepe (ha részt vesz az órán)

Ismertetheti a kvíz részleteit.

Prezentáció és tanóra vége

35. dia



**Korszerű pénzkezelés
- DIGITÁLIS BIZTONSÁG**



FINTELLIGENCE
PÉNZÜGYI KULTÚRA KÖZPONT



PÉNZIRÁNYTÓ

Átadandó információk

Elköszönés, a diákok munkájának megköszönése.

Az önkéntes szerepe (ha részt vesz az órán)

Búcsúzás, figyelem megköszönése.