



Korszerű pénzkezelés - DIGITÁLIS BIZTONSÁG

.....



PÉNZÜGYI BIZTONSÁGI TUDÁSTÁR

kiegészítő információk
tanárok és önkéntesek számára

PÉNZ7 – Pénzügyi és vállalkozói témahét

2020. március 2-6.

Szerkesztette: Pál Zsolt

TARTALOM

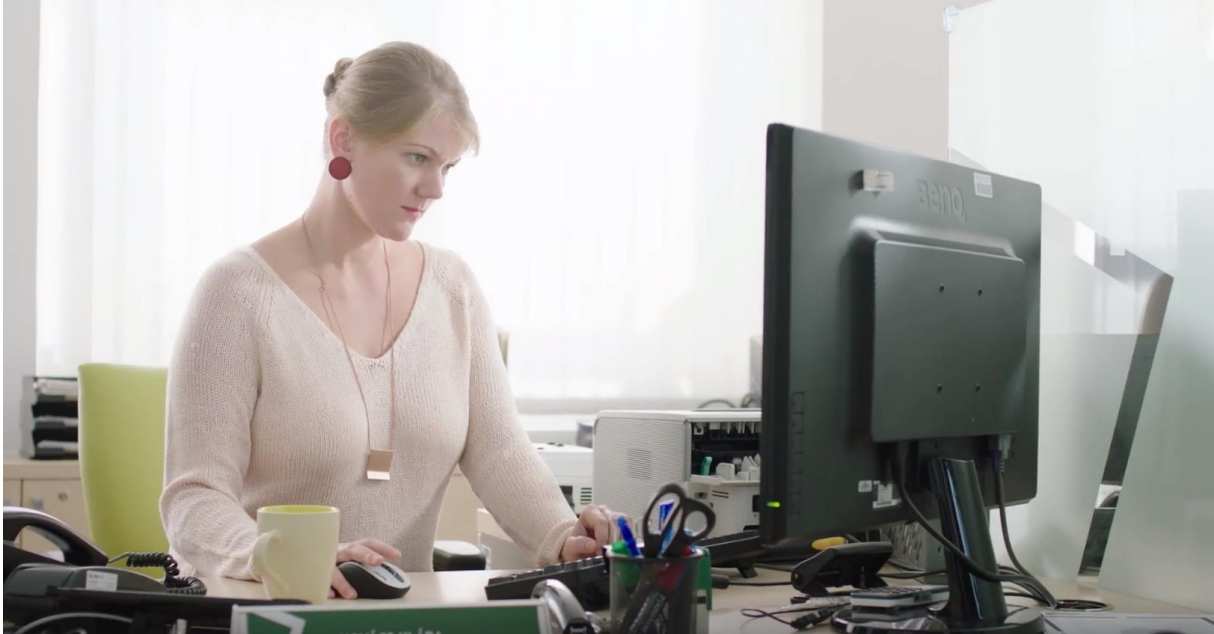
Digitális biztonság – szemléltető videók.....	3
Bankkártyás fizetések biztonsága.....	5
Azonnali fizetés	6
Iránytű a pénzügyekhez és Küldetések a pénz világában tankönyvek	7
További hasznos programok, kezdeményezések, szolgáltatások.....	8
Még több digitális biztonság – ajánlott források.....	11

Az itt leírt információk a **PÉNZ7 – Pénzügyi és vállalkozói témahét** tanárai és önkéntesei számára kerültek összegyűjtésre, annak érdekében, hogy a 2020-as PÉNZ7 tanórái során a **Korszerű Pénzkezelés – Digitális biztonság** c. témát az érdeklődő kollégák még szélesebb háttérismeretek birtokában tudják bemutatni.

Ez a tudástár partnereink által készített szakmai tartalmak, illetve az interneten publikusan elérhető anyagok felhasználásával készült, amelyek forrása minden esetben megjelölésre került, mi több, a legtöbb esetben az olvasó – internetes hivatkozások formájában – a publikálás eredeti helyéhez van irányítva.

Digitális biztonság – szemléltető videók

A Nemzeti Kibervédelmi Intézet szervezésében készült kisfilm az adathalász (phishing) támadásokról (A képre kattintva elérhető.)

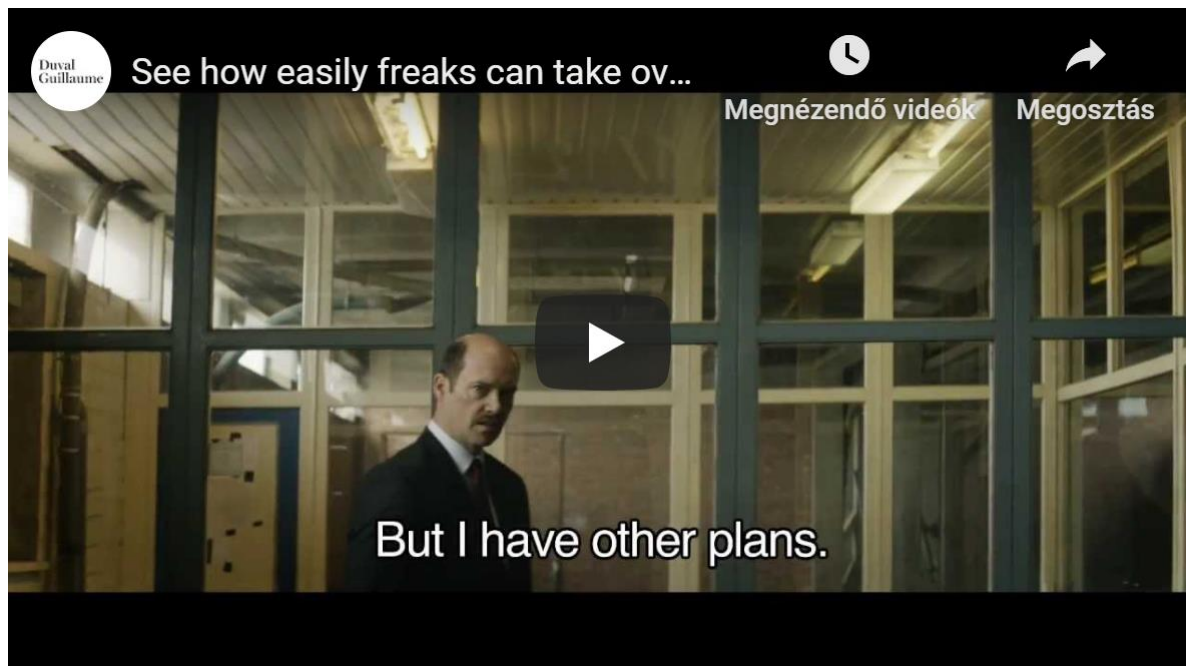


Amazing mind reader reveals his 'gift'
(A képre kattintva elérhető. Angol nyelvű videó.)



Személyiséglopás (See how easily freaks can take over your life)

(A képre kattintva elérhető. Angol nyelvű videó.)



Vigyázz a cápákkal (Watch out for the sharks)

(A képre kattintva elérhető. Angol nyelvű videó.)



Bankkártyás fizetések biztonsága

– Magyarország Európa legbiztonságosabb államai között

Az Európai Unió tagországai között csak Romániában, Görögországban, Lettországon és Lengyelországban volt alacsonyabb a bankkártyás visszaélések forgalomhoz viszonyított aránya a 2010-18-as időszakban - derült ki a Magyar Nemzeti Bank Fizetési rendszer jelentés című kiadványából. A visszaélések aránya hazánkban nem éri el a forgalom 0,01 százalékát a kilencéves összevetésben, miközben az euróövezet aránya 0,03 százalék felett áll, a SEPA európai fizetési övezetben pedig 0,04 százalék. Az elmúlt évben azonban a jegybanki statisztikák szerint jelentősen megugrottak a visszaélések hazánkban is: 2018-ban 66 037 esetben regisztráltak kártyacsalást a hazai pénzintézetek, ez kétharmadával több, mint a 2017. évi 39 355-ös esetszám. A jegybanki jelentés arra is rámutat, hogy a bejelentett károknak csupán 8 százalékát, 91 millió forintot kellett a kártyabirtokosoknak állniuk, a hatályos szabályozás szerint ugyanis csak akkor viseli a kárt az ügyfél, ha bizonyíthatóan neki felróható súlyos gondatlanság okozta azt a helyzetet, amelyben a visszaélés megtörténhetett. Mindez azt jelenti, hogy egymillió forintnyi kártyás fizetés után a magyar plasztiktulajdonosokat mindössze 9 forint tényleges kár érte. A jegybanki statisztikák igen pontosan mutatják a fő csalási tendenciákat. Miközben 2017-ben még a csalásban érintett tranzakciók 11,6 és a károk közel 16 százaléka kötődött hamisított kártyákhoz, addig tavaly az ilyen tranzakciók száma már nem érte el a visszaélések 5 százalékát, az ilyen ügyletekben megforduló pénzek pedig a károk 8,2 százalékát teszik ki. A legtöbb probléma egyértelműen az internetes vásárlásoknál történik: a 2017-es 30 567 eset után tavaly már 55 757 ilyen visszaélés történt. Magyarországon már több bank (Budapest Bank, Cetelem, CIB, Erste, K&H, OTP, UniCredit) alkalmazza az internetes vásárlásokat védő egyszer használatos kódküldéses, úgynevezett 3D Secure szolgáltatást, a mobilos fizetéseknél pedig több hitelintézet csak biológiai azonosítással engedi elindulni a fizetési folyamatot.

(Világgazdaság 13.o. 2019. 07. 29.)

Azonnali fizetési szolgáltatás létrehozása Magyarországon

A hazai pénzforgalom hatékonyságának növelése, a fizetési piac és a magyar gazdaság versenyképességének javítása érdekében az MNB javaslatot tett az azonnali fizetési szolgáltatás létrehozására. Az új fizetési rendszer létrehozásának célja, hogy az év minden napján 24 órában működő szolgáltatással néhány másodperc alatt lebonyolíthatóak legyenek a fizetések a magyarországi fizetési számlák között, a szolgáltatás szabályrendszere pedig lehetővé tegye, hogy az alpinfrastruktúrára építve a piaci szereplők szerteágazó kiegészítő szolgáltatásokat hozzanak létre. Az azonnali fizetési rendszerrel a magyar pénzforgalomban is hasznosíthatóak lesznek az elmúlt években alacsony költségek mellett elérhetővé vált modern kommunikációs és informatikai technológiák. Ezeknek köszönhetően az azonnali fizetési szolgáltatás alkalmas lesz rá, hogy a bankok és egyéb pénzforgalmi szolgáltatók megfelelő fejlesztései esetén számos fizetési helyzetben lehetővé tegye az elektronikus fizetést, és a jelenleginél jóval szélesebb körben teremtsen választási lehetőséget a készpénzhasználat mellett. Az azonnali fizetési szolgáltatás kapcsán létrejövő új alpinfrastruktúra használatával az innovatív fizetési szolgáltatások a jelenleginél gyorsabban és egyszerűbben lesznek létrehozhatóak, így a pénzforgalmi piac jelenlegi szereplőinek javulhat a versenyképessége, az új piaci szereplők pedig egyszerűbben léphetnek be a pénzforgalmi piacra, ahol a jelenlegi szereplőkkel azonos infrastruktúrát használhatnak a szolgáltatásaikhoz. (MNB)

Bővebben: <https://www.mnb.hu/penzforgalom/azonnalifizetes>



További információ és adatok a hazai bankközi klíringrendszerről:

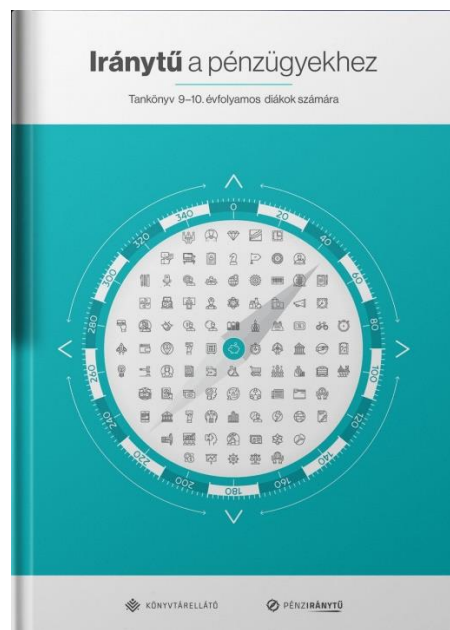


Iránytű a pénzügyekhez és Küldetések a pénz világában tankönyvek (Pénziránytű Alapítvány)

A könyvek a képekre kattintva érhetőek el.



Általános iskolai tankönyv és munkafüzet



Középiskolai tankönyv

További hasznos programok, kezdeményezések, szolgáltatások

Nemzeti Kibervédelmi Intézet (honlap)

<https://nki.gov.hu/>

A Nemzetbiztonsági Szakszolgálat részeként működő Nemzeti Kibervédelmi Intézet eseménykezelési és hatósági felügyeleti feladatokat lát el a létfontosságú információs rendszerek és rendszerelemek, valamint meghatározott bejelentés-köteles szolgáltatást – úgymint online piactér, internetes keresőszolgáltatás, valamint felhőszolgáltatás – nyújtó szolgáltatók esetében. Emellett, illetve ennek részeként számos tudatosságnövelő kezdeményezés, program és kiadvány kötődik az Intézethez, amelynek honlapja is rendkívül informatív forrás digitális biztonsági témákban.

IT BIZTONSÁGI TUDÁSTÁR

IT BIZTONSÁGI SZÓRÓLAPOK

A fenti szövegekre kattintva elérhető információk mellett jó példa a Nemzeti Kibervédelmi Intézet tudatosságfejlesztési szerepvállalására az alábbi tipp-gyűjtemény is.

10 IT BIZTONSÁGI TIPP NYARALÁSRA



A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézete a nyári időszak, szabadság, szünidő alatt is a biztonság tudatos magatartásra hívja fel a figyelmet.

Nyaralás során is érdemes kellő körültekintéssel eljárni számítógépes eszközeink és alkalmazásaink használata során, azokat a megfelelő védelmi elemekkel ellátva működtetni.

A zavartalan pihenés érdekében – utazás előtt – javasolt informatikai és „okos eszközeink” vonatkozásában az NBSZ NKI alábbi linken (vagy a fenti képre kattintva) elérhető kiadványa szerint eljárni.

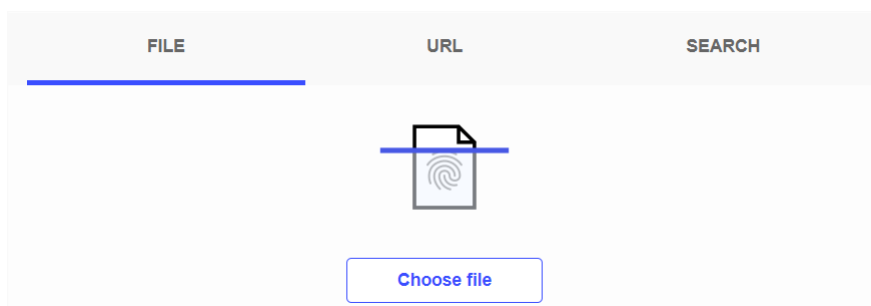
<http://bit.ly/2HIhs8J>

VirusTotal (ingyen szolgáltatás)

<https://www.virustotal.com/>



A VirusTotal egy online platform, amelynek segítségével bármikor, ingyenesen küldhetünk be gyanús fájlokat vagy weboldalakat és ellenőrizhetjük le, hogy kártékony kódot tartalmaznak-e. A szolgáltatás több mint 70 különböző vírusvédelmi rendszer feketelistáin keres és saját eszközökkel is eleméz.

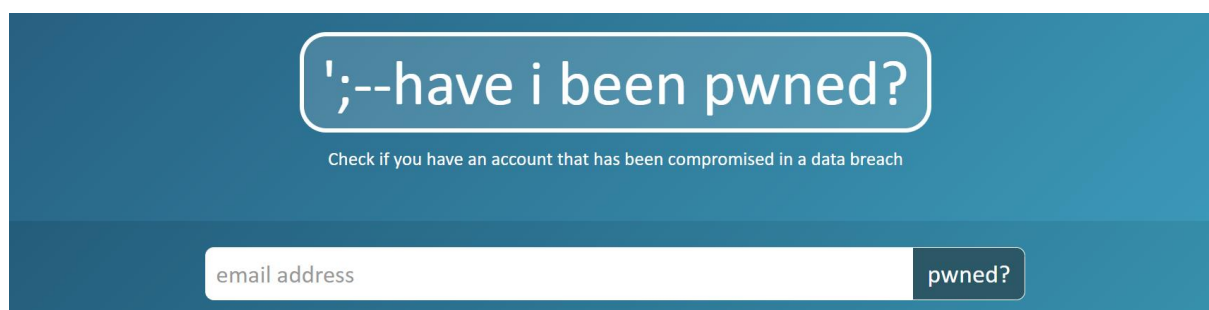


Have I Been Pwned? (HIBP – ingyen szolgáltatás)

<https://haveibeenpwned.com/>

A HIBP weboldalon e-mail címünket megadva leellenőrizhetjük, hogy az érintett volt-e valamilyen kiberbiztonsági incidensben. A szolgáltatás adatszivárgások százainak információit gyűjti, elemzi és összegzi – ezáltal akár milliárdos nagyságrendben tartalmaz kiszivárgott felhasználói adatokat, feltört fiókokat.

Nem mindegy, hogy a miénk is köztünk van-e!

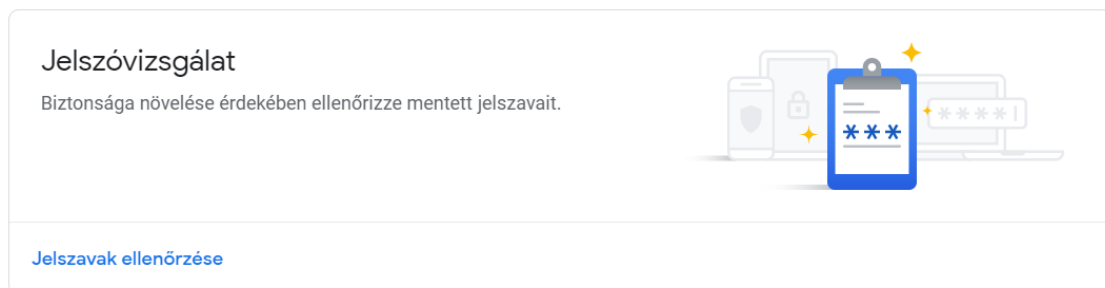


Google jelszóvizsgálat (ingyen szolgáltatás)

<https://passwords.google.com/>

A Google által működtetett webhely a Chrome-ban tárolt felhasználónév-jelszó párosokat ellenőrzi – segít ellenőrizni, hogy jelszavunkat vajon nem szerezték-e meg a hekkerek.

A szolgáltatás webes változatát a Chrome felhasználók a passwords.google.com helyen találják, ahol a Google fiók alapján történő bejelentkezés nyomán lefuttathatják az ellenőrzést, illetve szinkronizálhatják adataikat a különböző eszközökön futó Chrome-változatok között.



Az ellenőrzési igényt követően egy olyan listát kapunk a Chrome-ban, amelyen megtaláljuk a feltört felhasználónév-jelszó párokat, a fiókokat, amelyhez azonos a jelszó tartozik (ez a biztonsági szakértők réme), továbbá azokat a fiókokat, amelyekhez gyenge jelszó kapcsolódik.

Forrás: <http://bit.ly/2RH19id>

Még több digitális biztonság – ajánlott források

Hack és Lángos Podcast (ingyenesen elérhető audio tartalom)

<https://hackeslangos.show/>

„A Hack és Lángos egy podcast az IT biztonságról lehetőség szerint olyan nyelven is, amit nem csak szakemberek értenek. Szeretünk élő példákkal fűszerezve, sajátos hangulatban híreket értelmezni és elemezni.”



Csalóakadémia (Nemzeti Bűnmegelőzési Tanács)

<http://bit.ly/2SzfQ0Q>

A Nemzeti Bűnmegelőzési Tanács kisfilmjei az idősekre leselkedő veszélyekre figyelmeztetnek.

Netbiztonsági Kalauz (index)

<http://bit.ly/2u8BjdY>

„Már megint hekkerekkel vannak tele a hírek? Újabb adatlopásra vagy kibertámadásra derült fény? Lassan már ön is attól tart, hogy ellopják a jelszavát, beleolvasnak az üzeneteibe, áruba bocsátják a személyes adatait? Helyes, a félelme nem alaptalan. Adunk néhány tippet, hogy mire érdemes odafigyelnie, hogy csökkentse a veszélyt, és mutatunk pár további ötletet, ha egy kicsit paranoiás. Tegyen jót magának, és az interneten legyen mindig egy kicsit paranoiás.”



IT biztonság közérthetően (ingyenesen letölthető tankönyv)

<http://bit.ly/39LX7vb>

A Neumann János Számítógép-tudományi Társaság 2019-ben megújított (és várhatóan évente frissülő) tankönyve jól rendszerezve tartalmazza a bennünket körülvevő, rohamosan változó világ kihívásaihoz nélkülözhetetlen információkat. A tananyag az ECDL bizonyítvány megszerzéséhez szükséges vizsga IT biztonság moduljára való felkészüléshez is használható.

Erdősi Péter Máté, Solymos Ákos, 2019., Neumann János Számítógép-tudományi Társaság

