

TDK Dolgozat

Készítette: Hamrik Livia

Intézmény: Pécsi Tudomány Egyetem

Kar: Természet Tudományi Kar

Tanszék: Informatika tanszék

Készítette: Hamrik Livia

Évfolyam: 3. évfolyam

Téma magyar címe: Online bankolásban lévő lehetőségek kiaknázása a XXI. században

Téma angol címe: The application of online banking system, in the XXI. century

Témavezető: Horváth Zoltán

Témavezető beosztása: tanársegéd

Kézirat lezárva: 2015. január 5.

Tartalomjegyzék

1.	BEVEZETÉS	1
2.	TÖRTÉNETE	3
3.	INTERNET BANKOLÁS TERJEDÉSE MAGYARORSZÁGON.....	6
4.	ELJÁRÁS, LEHETŐSÉGEK	7
4.1.	SZOLGÁLTATÁS IGÉNYLÉSE	7
4.2.	SZOLGÁLTATÁS LEHETŐSÉGEI.....	8
5.	BANKKÁRTYÁK	10
5.1.	VIRTUÁLIS BANKKÁRTYA.....	12
5.2.	NFC-S KÁRTYÁK.....	13
5.3.	VISA	15
6.	KÜLÖNBÖZŐ FIZETÉSI MÓDOK.....	16
6.1.	PAY PALL	16
6.2.	BITCOIN	17
6.3.	PAYSAFECARD	18
6.4.	ABAQOOS	18
6.5.	SKRILL	19
6.6.	NETELLER	20
6.7.	ENTROPAY	20
7.	INTERNET BANKOLÁS ELŐNYEI HÁTRÁNYAI.....	21
8.	INTERNETES CSALÁSOK, ÉS NÉHÁNY BIZTONSÁGI MEGOLDÁS	22
8.1.	SSL, CSALÁSOK, KÉMPROGRAMOK	22
8.2.	PHARMING	25
8.3.	TANÁCSOK E-BANKOLÁSHOZ	26
8.4.	AZONOSÍTÓ ÉS VÉDELMI RENDSZEREK	27
9.	ONLINE BANKOLÁS TECHNIKAI LEHETŐSÉGEI.....	30
10.	FOLYAMATOS FEJLŐDÉS.....	40
11.	JÖVŐKÉP.....	47
11.1.	NFC	47
11.2.	OKOSTELEFON ALKALMAZÁSOK	48
11.3.	PREPAID KÁRTYÁL	51
11.4.	APPLE PAY	52
11.4.1.	<i>Apple Pay, a világ legbiztonságosabb fizetési módszere.....</i>	<i>52</i>
11.4.2.	<i>Apple Pay által használt biztonsági token.....</i>	<i>52</i>
11.4.3.	<i>Apple Pay tranzakciók működése</i>	<i>53</i>
11.4.4.	<i>Touch ID és Kriptogramok.....</i>	<i>53</i>
11.4.5.	<i>Mit jelent mindez a felhasználóknak?</i>	<i>54</i>
11.4.6.	<i>Az Apple Pay jelenlegi hátrányai</i>	<i>54</i>
	SWOT ANALÍZIS	55
	ÖSSZEFOGLALÁS.....	57
	IRODALOMJEGYZÉK.....	58

1. BEVEZETÉS

Az elmúlt húsz év legnagyobb technikai innovációja az internet elterjedése, ami teljesen megváltoztatta a körülöttünk lévő világot és mindennapi szokásainkat. A XX. század második felében kialakult technikai forradalom, a telekommunikáció és az információ technológia gyökeresen új helyzetet teremtett a pénzügyi rendszer struktúráját illetően is. A különböző nagyteljesítményű kommunikációs csatornák megjelenése és az információtárolás, és feldolgozás új lehetőségeket teremtettek a pénzügyi rendszer működése számára. A kommunikációs csatornák fejlődésében a mobil telefonhálózatok megjelenése, a vonalas adatátvitel minőségének ugrásszerű fejlődése és a műholdas információ továbbítás tömegessé válása emelhető ki. Az előbbi vívmányokra épülő klíringhálózatok (nemzeti klíring rendszerek, a közös európai klíring rendszer (TARGET), nemzetközi bankkártya hálózatok (VISA, EUROCARD)) és az internet jelentős mértékben megváltoztatták a pénz illetve az ezzel kapcsolatos szolgáltatások elérhetőségét, sebességét.

Minden olyan bank által nyújtott szolgáltatást, mely elektronikus alapon működik e-banking-nak, elterjedtebb nevén elektronikus bankolásnak nevezzük. Tehát így ide tartozik minden olyan pénzforgalmi szolgáltatás, mely elektronikus alapokon fekszik. Továbbá elterjedt az olyan speciális hálózatok kialakulása, melyek felgyorsították a nemzetközi fizetési lehetőségek gyarapodását. Ha bankolásról beszélünk, mindenképpen az értékesítést is szóban forgó fogalomként kell tekintenünk. Ilyenkor emberi természetünknel fogva személyes kapcsolatokra gondolunk, ám az elmúlt jó néhány év lendületes technikai fejlődése és kommunikációs vívmányainak köszönhetően nem csak az internet használatát, hanem a különböző pénzügyi szolgáltatásokat is egy teljesen új modern alapra fektette. Természetesen ez a hihetetlen átalakulás nem maradhatott következmények nélkül. Ha egy adott szolgáltatás vagy termék értékesítéséről van szó, akkor napjainkban már egy egyre jobban elszemélytelenedő felfogásra gondolunk. Hogy pontosan miért is... Nos, a mai fiatalok, sőt egyre gyakrabban az idősebb korosztály sem járja a boltokat, hogy bármit is vásároljanak, inkább áthelyezik egy virtuális webes felületre, úgynevezett webáruházakra, ahol időt megtakarítva bonyolítják le ezt. Ez nemcsak, hogy felgyorsítja, de le is egyszerűsíti a vásárlást, hiszen nem kell órákig téblábolnunk az áruházak között, elég ha leülünk gépünk elé és egy jó hideg limonádé mellett keresgélünk az elénk tároló lehetőségek között. Természetesen ez egy személyes kapcsolatokat igen csak nélkülöző megoldás. Mindehhez szorosan köthető a mára már mindennapos szolgáltatás az online bankolás. Napjainkban a kommunikációra az egyik leggyorsabban forgó eszköz az internet lett, persze ez alatt nem

csak a közösségi oldalak elterjedésére gondolok, hanem minden olyan másra, melyek kiaknázására számos pénzügyi illetve banki szervezet jött létre. Nem meglepő módon ezzel a fejlődéssel párhuzamosan, elterjedtek az elektronikus bűnözések is.

Hogy valójában mit is nyújtanak nekünk ezek az elektronikus banki szolgáltatások?! Meg lehet-e határozni pontosan, hogy ez mit is jelent, vagy csak egy gyűjtőfogalom, nos nem, koránt sem.

Talán úgy lehetne a legjobban körülhatárolni, mint egy eszköz által biztosított banki és pénzügyi intézményt, amely lehetővé teszi egy adott felhasználó számára, hogy a lehető legtöbb bankkal kapcsolatos tranzakciót interneten keresztül elvégezhesse. Ez egyfajta pénzinformatika, mely az adott banki intézmények és a gyorsan fejlődő számítástechnikai megoldások valamilyen együttesét alkotja. Ennek köszönhetően mind a magánpénzügyek, mind a vállalati pénzügyek intézése tulajdonképpen áthelyeződik egy virtuális térbe. Hogy ez előny-e? Gyakorlatilag ez nem is kérdés, hiszen az efféle banki szolgáltatások során az emberek otthon ülve vagy munkahelyükön is képesek olyan tranzakciók lebonyolítására mely az üzleti életükhöz szükséges. Folyamatosan csökken azoknak a száma az online szolgáltatások előretörésével, akik különböző pénzügyeik elintézése érdekében még elmennek az adott bankfiókjukhoz és személyesen bankolnak.

Természetesen az elektronikus pénzügyeinkhez tartozó szolgáltatások nem csak az internet használatára korlátozódnak le, számos egyéb lehetőség is adódik eme szolgáltatások alkalmazására. Mint például bankkártyánk vagy mobiltelefonunk segítségével is végre tudunk hajtani pénzügyi műveleteket. Magyarországon a cégek több mint 60%-a alkalmazza már a bankok által nyújtott online szolgáltatások valamelyikét. Ám ez a technikai vívmány nem csak a vállaltok, hanem a mindennapi emberek életében is egyre rohamosabban terjed. Hogy mire is jó az online bankolás akár egy egyetemista vagy egy vállalati igazgató számára? Erre három egyszerű kis szó van: gyorsaság, kényelem, és természetesen költséghatékonyság. Melyiknek tudnánk ellenállni a mai rohanó világban?!

2. TÖRTÉNETE

A fiókon kívüli szolgáltatások első lépcsőfokai az '50-es években megjelenő bankkártyák és telefonos ügyfélszolgálatok voltak. A '80-as évek második felében, a személyi számítógépek egyre gyorsabb terjedése lehetővé tette az Office Banking, majd később a Home Banking (a banki és a pénzügyi szervezetek Európában és az Egyesült Államok történő szuggesztív kutatásainak és programozási kísérleteinek megkezdése) rendszerek kialakulását. Az elektronikus banki szolgáltatások körének kiteljesedését a World Wide Web tette lehetővé, ezzel teljesen új alapokra helyezve a bankok és ügyfelek közötti információáramlást. 1983-ban a Nottingham Building Society (NSB), elindította az első internetes banki szolgáltatást, az Egyesült Királyságban. Ez a szolgáltatás alapját képezte a legtöbb ezt követő internetes banki létesítménynek. Ez a lehetőség nem volt túl fejlett, és korlátozott volt a tranzakciók illetve funkciók száma is, melyet a számlatulajdonosok végrehajthattak. Az online banki szolgáltatások ezt követően egyre inkább elterjedtek, a rendszerek fejlődésével párhuzamosan. Bár vannak előnyei és hátrányai is, ennek ellenére az elektronikus pénz forradalommá vált, amely fokozza a bankszektorokat. Habár a fiókon kívüli elérhetőség kialakítása valódi piaci igényné vált, a személyes kiszolgálatok továbbra is megmaradtak. Az értékpapírok interneten való megkötése még több banknál is hiánycikk. A nagy kamattal kecsegtető akciósbankbetétek lekötését is csak személyesen lehet igényelni.

HISTORY OF ONLINE BANKING

BROUGHT TO YOU BY YODLEE

Since the early 1980s, innovations in online banking have made it easier for people to manage their money. Banks are offering more and more tools, information, and access to financial accounts to help customers achieve their financial goals. TowerGroup Research projects that global usage of personal finance management tools will reach 70 million in 2014.

Let's see how it all started and who's using the tools today.

START

1983

The Bank of Scotland offers Nottingham Building Society (NBS) customers the first Internet banking service in the UK and calls it "Homelink." Connecting via a television set and a telephone to send transfers and pay bills, this service formed the basis for online banking as we know it today.



1994



January 1994
Online banking is built into Microsoft Money personal finance software. 100,000 households begin accessing bank accounts online.
(Online Banking Report, Jan. 2012)



The Stanford Credit Union creates the first online banking website.

2001

December 2001
Eight US banks have at least 1 million online users each. 19 million US households are accessing bank accounts online.
(Online Banking Report, Jan. 2012)

Yodlee opens its doors, creating the first account aggregation software and giving consumers the ability to view all of their financial accounts in one place.



2005

As banking moves online, rules must shift with the times. FFIEC announces rules and regulations for financial institutions: FIs to carry out risk-based assessments, evaluate customer awareness programs, and implement security measures to authenticate remote account access.



Direct banks (banks that operate without a physical branch) begin to offer their services primarily online: ING Direct, PC Financial (Canada), First Direct (UK), HSBC Direct and eTrade Bank (US).



Consumer PFM portals like Mint.com start to gain popularity among users as easy-to-use and well-designed tools to manage their finances.



2009

54 million US households accessing bank accounts online.
(Online Banking Report, Jan. 2012)



2007

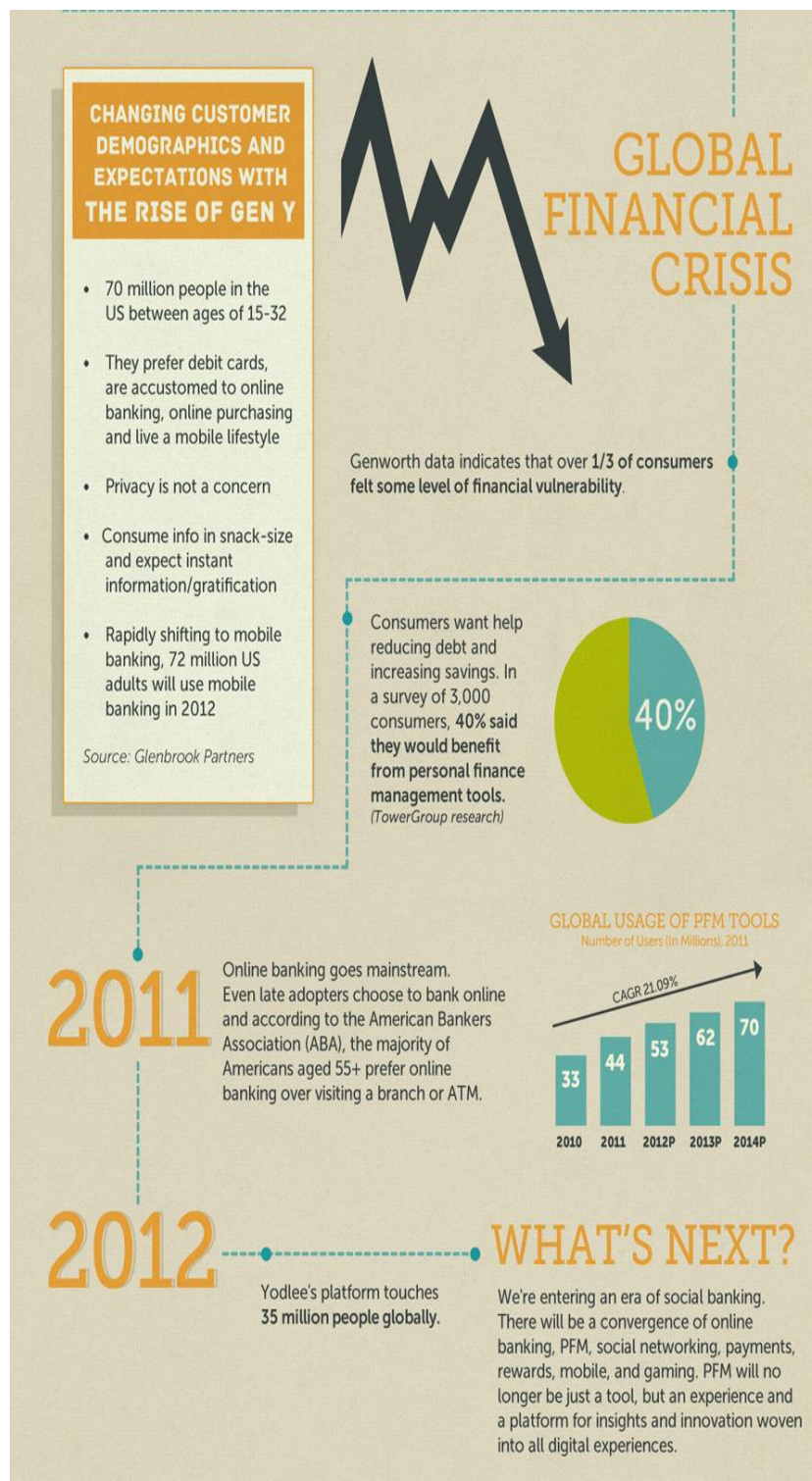
Pocket Power
Apple launches the iPhone and a shift from banking via personal computer to banking via smartphone begins.



RATIO OF POPULATION TO BANK BRANCHES

1970	9.340
2009	3.684

Bank branches are consolidating. Ratio of the US population to bank branches shifts from 9.340 in 1970 to 3.684 in 2009. Branches are increasingly less important to consumers and banking moves to kiosk and online solutions.



1. ábra: Online bankolás fejlődése kialakulásától napjainkig. 1983 NBS az első internet bankoló rendszer, 1994 már 100 ezer felhasználó, 2001 és 2009 között meg háromszorozódott az amerikai felhasználók száma, 2007-ben az Apple által elindult a mobil bankolás is, 2011-ben előtérbe került az online használat a személyes ügyintézés helyett, 2012-ben 35 millió felhasználója volt világszerte a Yodlee rendszerének.

3. INTERNET BANKOLÁS TERJEDÉSE MAGYARORSZÁGON

Magyarországon a 90-es évek második felétől kezdett egyre lendületesebben fejlődni az ügyfelek körében az interneten keresztül történő banki ügyintézés. Először 98-ban az Inter-Európa Bank, majd az ezt követő évben a toplista élét vezető OTP-nél, 2000-ben a Raiffeisennél és a Citibanknál, illetve a Kereskedelmi és Hitelbanknál is megjelentek az online szolgáltatások. Több banki felmérés elvégzése után kiderült, hogy mindazok száma, akik a pénzügyeik intézéséhez ezt a módszert alkalmazzák, mára meghaladta a 80 ezer főt, ami valljuk be napról-napra csak több lesz. Nemzetközi szinten a britek vezetnek a legnagyobb online banki ügyféllel. Magyarországon természetes ebben is élen az OTP áll, egyértelműen piacvezetők, a korábban említett alkalmazok számának több mint fele, rendszeres használója a bank által nyújtott internetes műveleteknek, így átlagosan havi majdnem 400 ezer lekérdezéses tranzakciót hajtanak végre. Jól látható a későbbiekben taglalt adatokból, hogy az országban, de világszerte is az emberek még félve használják az internet e téren nyújtott lehetőségeit, de ez a tendencia fokozatosan változni látszik a fejlődő technikának köszönhetően, melyek növelik a biztonságérzetet.

4. ELJÁRÁS, LEHETŐSÉGEK

Az Online bankolásnak két fajtáját különböztetjük meg. Az egyik a Home-banking, a másik pedig az Office-banking. A két típus között semmi technikai különbség nincs, csupán a felhasználók köre más. A Home-banking rendszereket, ahogy a neve is mutatja, elsősorban lakossági illetve kisvállalati felhasználók használják, melyből következik, hogy a szolgáltatásokat a nagytömegűség valamint a standardizált termékek, szolgáltatások jellemzik. Az Office-banking közép-, és nagyvállalatoknak kínálja, ebből következik, hogy itt lehetőség van az egyéni igények kielégítésére.

Az online bankolási eljárások során számos pénzügyi tranzakció elvégezhető egyszerűen egy számítógép, laptop vagy akár egy okos telefon és a hozzá kapcsolódó internet felhasználásának segítségével.

4.1 SZOLGÁLTATÁS IGÉNYLÉSE

Az internetes bankolás szolgáltatásának igénybevételéhez, a szolgáltatást a bankunknál kell igényelni, erre vonatkozó szerződés aláírásával. Ebben rögzítésre kerül, hogy milyen szolgáltatásokat vehet igénybe az ügyfél interneten keresztül. Ezt követően kapjuk meg a banktól a felhasználónevet, a jelszavakat, ami rendszerint egy azonosítási és egy aláírási jelszóból áll.

A biztonság növelése érdekében, egyes bankoktól a felhasználó azonosítására szolgáló chipkártyát vagy tokent is kaphatunk.

Elterjedt és bevett módszer az egyszeri jelszó használata. Ez egy SMS-ben kapott véletlenszerűen generált szám/betű sor, melyet az online felületre való belépéskor illetve tranzakciók rögzítésekor küld a rendszer, az azonosítási jelszó bekérése után.

4.2 SZOLGÁLTATÁS LEHETŐSÉGEI

- Számlaegyenleg lekérdezés
- Számlakivonat lekérdezés
- Elvégezhetünk különböző tranzakciókat
- Módosíthatjuk a bankkártya limitünket
- Igényelhetünk bank és/vagy hitelkártyát
- Feltölthetjük mobilunkat
- Különféle megtakarításokat kezelhetünk
- Értékpapír számla kezelés
- Megbízások kezelése/módosítása
- Ügyfélszolgálat, üzenetek olvasása, küldése, egyéb lehetőségek

Az átutalás költségei nagyban függenek az elvégzett tranzakcióktól. Nem mindegy, hogy bankon belül, más de hazai bankok között, esetleg külföldi számlára utalunk. Az euró övezeten belül, nincs különbség a hazai és külföldi átutalások között az azonos valuta miatt, viszont ha az Unión belül, de nem euro zónás országba utalunk akkor változhat/változni fog a díj összege.

Általában az online felületen elvégzett megbízások díjai alacsonyabbak, mint a bankfiókban elvégzett megbízásoké. A hagyományos banki szolgáltatásokon kívül, több extra szolgáltatást is el tudunk végezni online felületen.

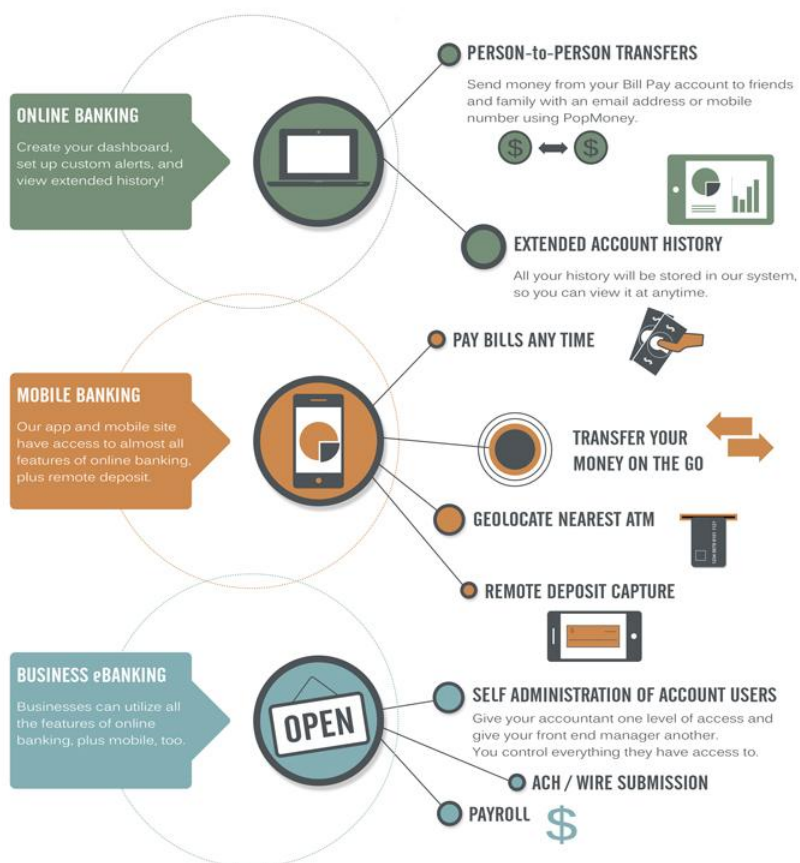
Mindenképpen megemlíteném a már felsorolt lehetőségek mellett, a Telebank használatát is. Hogy ez miért is jó, nos... A gazdasági vezetők számára az információhoz való hozzájutás, ezzel együtt az időmegtakarítás szinte alapkövetelményként fogalmazódik meg. Telebank szolgáltatással információhoz juthatunk az érkezett illetve indított utalásainkról, számlatörténetről, hitel információkhoz juthatunk, vagy éppen megtudhatjuk az aktuális valuta és deviza árfolyamokat.

Különféle beállításokat is tudunk a későbbiek folyamán változtatni.

- bankkártya letiltás
- limitmódosítás
- SMS értesítések megváltoztatása
- speciális műveletek elvégzése



2. ábra: E-bankolásban rejlő lehetőségek



3. ábra: Online bankoláshoz tartozó eljárások, regisztrációtól a vásárlásig.

5. BANKKÁRTYÁK

A bankkártya egy olyan eszköz, ami helyettesíti a készpénzt, valamint az azzal történő fizetést. A bankkártyát a különböző bankok bocsájtják ki, a számlákat vezető magán-, és vállalkozó ügyfelei számára. Ez azonban a bank tulajdonát képezi. A GfK Piackutató Intézet felméréséből kiderül, hogy a közép és kelet-európai térségben a bankkártyák és az internetes banki szolgáltatások használata dinamikus növekedést mutat. A bankkártyáknak többféle változata létezik, melyet az alábbiak szerint csoportosíthatunk:

- felhasználó szerint
 - Lehet lakossági (azaz különböző magánszemélyek számára kibocsájtott kártya)
 - Business kártya azaz üzleti célra kibocsájtott kártya
- felhasználhatóság szerint
 - Betéti kártya (debit kártya): Olyan kártya, melyet csak akkor kaphat az ügyfél, ha a kibocsájtó banknál számlát vezet.
 - Hitelkártya: Szerződésben foglalt hitelkerethez kapcsolódó kártya. Ehhez hitelszámla tartozik.
 - Többfunkciós kártya: Olyan kártya, mely egyszerre több funkciót is ellát, a felsoroltak közül

A bankkártyák széles körben elterjedt fizetési eszközök, mellyel több funkciót is elláthatunk, gyorsan és egyszerűen.

- Lehet vele vásárolni akár online, akár a legegyszerűbb boltokban, taxiban stb.
- ATM-ből készpénzt felvenni
- Mobiltelefon feltöltési lehetőség ATM-nél, vagy például hipermarketekben egyszerű fizetési lehetőségként
- bankszámlaegyenleg lekérdezés
- ATM-en keresztül bankszámla befizetés

A bankkártyának, és használatának azonban minden esetben használati díjai vannak. Először is a legtöbb kártyának van előállítási, valamint éves használati díja. Ez többek között a készpénzkezelés, szállítás és őrzés díjaiból adódik. Ezek a díjak előre meghatározott fix díjak, melyek kártyánként és bankonként eltérőek. Emellett természetesen bizonyos költségekkel jár a fizetés, készpénzfelvétel vagy éppen az utalás is. A legtöbb bankkártyát egyaránt használhatjuk belföldön és külföldön is. A vásárlás a legtöbb kártya esetén ingyenes, de a

készpénzfelvétel külföldön általában 3 USD, viszont devizaárfolyammal számolva terhelik meg a bankszámlánkat

A bankkártyákat megkülönböztetjük az adatok tárolásának módja szerint is. Lehet egy kártya mágnes csíkkal , vagy chippel ellátva.

A mágnes csíkos kártyák a kártyára, valamint a kártyabirtokosra vonatkozó adatokat, kódolt formában a kártya hátlapján elhelyezett, általában szürke színű mágnes csíkon tárolja. Ám a biztonság növelése céljából egyre kiszorulóban vannak a hagyományos mágnes csíkos kártyák, a mikro chippel ellátott kártyákkal szemben.

A chipet tartalmazó kártyák vagy más néven smart kártyák, micro processzorral ellátott integrált áramkörös kártyák. Az adatokat nem mágnes csík, hanem a kártya elején található chip tárolja. Ez a megoldás jóval biztonságosabb, mint a mágnes csíkos. A PIN megadásával ráadásul az is ellenőrizhető, hogy a valódi tulajdonos használja-e a kártyát.

A bankkártyák egy személyhez kötődnek, át nem ruházható, és más személy által nem használható. A kártya sérülése, vagy elvesztése során haladéktalanul le kell tiltani, a lejáratí idő után pedig meg kell semmisíteni.

Nagy előnye még a készpénzzel szemben, hogy egyetlen kártya helyettesíti a különböző címleteket, így nem kell bajlódni a készpénzfelváltással, valamint a különböző hamisításokkal szemben is védett eszköz. Hátránya azonban, hogy egyes kisboltokban, vagy autóbuszon még nem lehet kártyás fizetést választani, így mindenképpen készpénzt is kell magunknál tartani, valamint technikai probléma esetén pl. a leolvasók meghibásodása esetén készpénzzel kell fizetnünk.

Bankkártya igénylés esetén lehetőségünk van, a biztonsági PIN-kód megváltoztatására, vagy éppen a kártyára személyes képet is választhatunk. Különböző SMS-es értesítésekkel, tovább növelhetjük a biztonságot, és egyből tudomásunkra juthat a kártyánk illetéktelen használata is. Természetesen azonban ezek is plusz költséggel járnak, melyek szolgáltatótól függnék. Ilyen értesítéseket kérhetünk például arról, ha megterhelik a kártyánkat, vagy ha nekünk érkezik pénz akkor is.

A bankkártya használat egyik legjobb lehetősége, az internetes, vagy telefonos vásárlás. Ekkor fizikailag nem kell használnunk a kártyát, csupán a kártya adatait kell megadni. Itt azonban megfelelő körültekintéssel kell lennünk, és kizárólag megbízható partnernél szabad ezeket az adatokat megadni.

Ezt ellenőrizhetjük, hogy az internetes partnerünk/kereskedők oldalán, akárcsak a hagyományos üzletek kirakatain megtalálhatóak-e az elfogadott kártyák logói. (MasterCard,

Visa, American Express stb.) Ezt a biztonság kedvéért célszerű összehasonlítani a kártyákon található jelzéssel. A fizetés előtt, ellenőrizzük, hogy a weblapon a kommunikáció titkosítva van, melyre az URL címben a „https” utal, valamint a jobb alsó sarokban található lakat, vagy a bal alsó sarokban található kulcs. Ezekre kattintva megjeleníthető a biztonsági tanúsítvány.

Internetes kártyahasználat során az alábbi adatokra lehet szükségünk:

- Bankkártya birtokos neve
- Bankkártya száma: a kártya előlapján található 16 jegyű szám
- Bankkártya lejárat dátuma: a kártya előlapján található dátum hónap/év formátumban
- CVC2 vagy CVV2 kód: a kártya hátoldalán az aláírási panelen (virtuális kártya esetén a hátoldalon, a színes sávon) található, a kártyaszám utolsó négy számjegye után szereplő 3 jegyű szám
- Bankkártya típusa: VISA / MasterCard

5.1 VIRTUÁLIS BANKKÁRTYA

A virtuális bankkártya kizárólag online felületen történő vásárlásra használható, mágnes csikkal és/chippel nem rendelkező, aláírás nélküli egyedi designnal ellátott kártya. Ez egy online debit kártya, azaz elektronikus engedélyhez kötött.

Különböző online boltok, úgynevezett webshopok megjelenésével, és terjedésével, megnőtt az internetes vásárlások száma is. Sokan azonban óriási kockázatot látnak még ma is az online fizetésben. Nekik kínál megoldást az internetkártya.

A kártya lényege, hogy csak és kizárólag online lehet használni. Nem helyettesít más felületen pl. boltokban készpénz, és nem használható olyan dolgokra sem, mint egy hagyományos bankkártya. PL. nem lehet ATM-ből készpénzt felvenni. A kártya egy egyszerű plastik lap, mely nevet, kártyaszámot, kártya lejárat dátumát, és egy háromjegyű biztonsági kódot, az úgy nevezett CVC2-t. Ezek csak az internetes vásárláshoz szükséges adatok.

A biztonságot, a kártya mögötti kártyafedezeti számlák garantálják. A kártya csak és kizárólag ehhez kapcsolódik, így a vásárlások előtt, a hagyományos folyószámláról át kell vezetni a szükséges összeget, erre a kártyafedezeti számlára. Az előzőleg említett biztonsági intézkedéseket azonban itt is be kell tartani. Vagyis ellenőrizzük, hogy megfelelő partnernél, megfelelő oldalon vásárolunk-e.

Ha internetkártyánk adatai ennek ellenére mégis rossz kézbe kerülnének, akkor itt is azonnali tiltást kell véghezvinni, valamint pótolni kell a kártyát. Azonban a kártya letiltásnak is vannak díjai, melyek, akár többre is kerülhetnek, mint az internetkártyán található összeg. Mivel

azonban az illetéktelen személy is csak a kártyafedezeti számlán található összeghez fér hozzá, így érdemes minél kevesebb összeget tartani az internetkártyán.

A kártyák árazása bankonként itt is eltérő, és bár használatuk jóval korlátozottabbak, mint hagyományos társai, a költségek közel sem olcsóbbak. A bankok azonban különböző alternatív lehetőségeket is kínálnak. Pl. az FHB Bank által kínált kártya, a kártya aktiválásáig kizárólag meghatározott webshopban való vásárlásra alkalmas. A Citibank egy alternatív folyószámlát kínál, amit a meglévő kártyához lehet kapcsolni, így funkcionálhat fedezeti kártyaként. Természetesen ilyen megoldások egyike sem pótolja az internetkártyát, de a neten történő vásárlások kockázatát csökkenti.

5.2 NFC-S KÁRTYÁK

A MasterCard és Maestro kártyák új generációját egy, az NFC technológián alapuló chippel is ellátták, mely korszerű, egy érintéssel működő gyors bankkártya alapú fizetési technológiát jelent. Ez a PayPass. Ezt az NFC rendszer teszi lehetővé (Near Field Communication), ez napjaink legmodernebb technikai rendszere, mely a rádiófrekvenciás azonosítás egyik továbbfejlesztett újdonsága.

Ez a technológia biztonságos vezeték nélküli adatátvitelt tesz lehetővé, néhány centiméteren belül. A megoldás is nemzetközi szabványon alapul. Ezek a kártyák a másodperc töredéke alatt kapcsolódnak az elfogadóeszközhöz, mely azonosítás után dolgozza fel a tranzakciót.

Ezeket a MasterCard és Maestro PayPass kártyákat, nem szükséges vásárláskor átadni az eladónak, elég a PayPass terminálhoz érintenünk. A kártyahasználatról természetesen így is kapunk nyugtát vagy számlát.

Villámgyorsan fizethetünk a PayPass elfogadóhely-matricával jelzett helyeken. Pl. gyorséttermekben, kávézókban, drogériákban, élelmiszerüzletekben, újságosoknál, mozikban, sőt ma már akár taxiban, vagy különböző futárszolgálatnál is.

A MasterCard PayPass és Maestro PayPass egy plusz funkcióval ellátott bankkártya a jelenlegi bankkártyákhoz képest: egy érintéssel is használható, így minden eddiginél gyorsabban lebonyolíthatja a fizetést.

5000 Ft alatti vásárlás esetén nem szükséges a PIN kód megadása, ám ez személyre szabható, 5000 Ft feletti vásárlás esetén azonban már itt is kötelezően meg kell adnunk a PIN kódot.



4.ábra: Pay Pass leolvasó, és a hozzá használható eszközök

5.3 VISA

Visa Classic kártya: A világ egyik leggyakoribb kártyája napjainkban. Egyszerű, megbízható a legszélesebb körben elfogadott kártyatípus. Alkalmas online vagy offline használatra is, fizetés során csak a PIN megadása szükséges.

Visa Gold kártya: Használata megegyezik a Classic kártyáéval, ám azon magánszemélyeknek ajánlott akik, sokat utaznak akár üzleti akár magán okokból. A kártya különféle beépített biztonsági szolgáltatásokkal van ellátva.

Visa Platinum kártya: Kombinálja a Classic és Gold kártyák előnyeit, melyet ezen túlmenően, különböző extrákkal, és kiegészítő egyéb szolgáltatásokkal kaphatunk. pl. emelet szintű védelmi rendszer.

Visa Electron: Egy rendkívül modern, elektronikus fizetésre alkalmas eszköz. Belföldön és külföldön is használható azokon a helyeken ahol az Electron jelzés fel van tüntetve. A kártyával világszerte közel 2 millió ATM-ből juthatunk pénzhez.

6. KÜLÖNBÖZŐ FIZETÉSI MÓDOK

Ahhoz hogy az ember egy online bankkártyás fizetési tranzakciót elindítson nincs szüksége semmiféle bonyolult banki szerződésekre. Ám egy fizetési rendszer elindításhoz már szükségünk van egy szolgáltatási szerződés aláírására, valamint műszaki integrációra. A fizetésekről automatikusan online számlát készít a rendszer, mindössze csak egyetlen egyet kell az ügyfélnek magának elkészítenie az elszámolási időszak végén. Vagyis a szerződés aláírását követően teljesen automatizált a számla adat bekérés, a már említett számlázás, és ennek valós idejű követése. Majd a magunk által készített számla alapján a részesedés kifizetésre kerül a legvégén.

Azonban egy gördülékeny fizetési folyamat esetén még a gyakorlott internetes vásárlóknak is sok információra van szükségük. A magyarok a webes vásárlók körében még mindig nincsenek túl nagy számban, vagyis az online fizetési módok terén még félve lépnek fel az emberek. Ennek oka leginkább, hogy alacsony a bizalom például az online bankkártyás fizetéssel szemben, pedig ha valójában végiggondoljuk nem is biztos hogy ez a legrosszabb és legveszélyesebb fizetési mód.

Ha az ügyfelek valahol elakadnak a folyamat során, akkor az ügyfélszolgálat a rendelkezésére áll, ha szükséges.

Természetesen az online fizetési módszerek számos lehetősége tárul az ügyfelek elé, mint például a következők.

6.1 PAY PAL

A PayPal kifejezéssel szerintem már elég sokan találkoztak főleg a 20-40 közötti korosztály. Hiszen ez az egyik legismertebb, legelterjedtebb online fizetési mód, bárki, aki csak egy e-mail címmel rendelkezik, már használhatja is. Ugyanis itt a hagyományos számlaszámtól eltérően, ahogy azt a klasszikus banki szolgáltatásoknál megszoktuk az e-mail cím alatt vannak a számlák vezetve. Továbbá ez egy olyan online rendszer, ami lehetővé teszi még azt is, hogy ingyenes fizetési átutalásokat végezzen az ügyfél hitelkártyáján keresztül, akárcsak a megszokott számlás pénzáttalalások között. Nem csak hogy elterjedt, de talán az egyik legbiztonságosabb fizetési módszer is az internetes szolgáltatások körében. Ezt a módszert szerte a világban alkalmazzák több mint 100 országban, és több mint 100 millió ember.

De még is hogyan történik a vásárlás PayPallal? Nagyon egyszerűen. Nincs szükség semmiféle számlanyitáshoz ahhoz, hogy ha egy web áruházban fizetni szeretne az ügyfél.

Elég csupán, ha a fizetési módoknál kiválasztja a vásárlás végén a PayPalt. Miután sor került a megrendelésre meg kell adnia az ügyfélnek a hitelkártyája számát, majd azt, hogy meddig érvényes még illetve a biztonsági CVC kódot is, továbbá egy e-mail címre. Ezt követően már csak annyi dolga van a vásárlónak, hogy az erre a célra létrehozott PayPal segítségével belépjen a rendszerbe és fizessen. A PayPal fizetési módot bárki egyszerűen meg tudja oldani!

6.2 BITCOIN

A Bitcoin egy új fizetési eszköz, virtuális pénz, elszámolási egység, vagy technológia, melyet 2009 elején közvetlenül a 2008-ban kirobban nagy gazdasági világválság után hozott létre több ismeretlen személy által alkotott csoport. A Bitcoin megvalósít minden olyan tulajdonságot, melyet közgazdasági értelemben megvalósít a pénz is. Azaz, értékmérő, forgalmi fizetési eszköz. Az Amerikai Felügyelet döntése értelmében pénznek minősül. Előnye az azonnali és költségmentes tranzakció, a decentralizáltság és az anonimitása. A rendszer sajátossága a peer-to-peer (személyek közötti) csomópont mentes hálózati megosztás. Mitől ilyen biztonságos egy virtuális pénz? Mert a hitelesítés a számlánkon lévő Bitcoinokról nem csak a saját számítógépünkön, hanem a hálózat összes gépén megtörténik. Azaz, az összes egységet fel kellene törni ahhoz, hogy veszteség érje a felhasználót. Ez biztosítja azt is, hogy nehezebben hamisítható mint a hagyományos pénz.

A Bitcoint BTC-vel rövidítjük, akár a hagyományos devizák rövidítését. (Pl. EUR-Euro, HUF-Forint) Egyre több elemző befektetésként gondol a Bitcoinra, hiszen a valós devizáktól eltérően itt nem infláció, hanem defláció van. Bitcoinhoz a legegyszerűbben a tőzsdén juthatunk, cserélhetünk vagy vehetünk valós pénzért, vagy bányászhatunk, azaz új blokkot hozhatunk létre.

Az eBay, online fizetési feldolgozó szolgáltatójának, a PayPal-nak amerikai dollárban végrehajtott tranzakcióinak mennyiségét a hírek szerint hamarosan felülmúlja a bitcoin. Egy kutatás eredményeképpen az is elmondható, hogy napi szinten megközelíti a 300 millió dolláros használatot mind az online fizetés, mind az online vásárlás együttesében.

6.3 PAYSAFECARD

A Paysafecard akár csak a PayPal, Európa egyik legnépszerűbb és leginkább bevált fizető eszköze. Ez egyfajta előre kifizetett online fizetőeszköze. Ehhez nincsen szükség sem a személyes adatokra, sem a bank- vagy hitelkártya számára. Az ügyfél így teljesen megőrizheti a Paysafecarddal magánszféráját. Ez egy egyszerűen, biztonságosan és gyorsan működő online fizetési eszköz, olyan mintha csak készpénzzel történne a fizetés. Elég elterjedt főként az interneten ismert játék, zene, film és szórakozás-szolgáltatónál, valamint számos más egyéb szegmensben is. A használata teljesen egyszerű: első lépésben vásárolni kell egy Paysafecard kártyát. Majd a be kell állítani a lehetőségeket fizetési módjaként. Végül meg kell adni egy PIN-kódot, és már nincs is további teendők ezzel.

Itt az ügyfél saját fizetési számlája az úgynevezett My Paysafecard, továbbra is egyszerű ezzel a fizetés, nem kell hozzá semmi más csupán csak az ügyfél felhasználóneve, és jelszava. Ezek megadásával már túl is van a vásárló a regisztráción és beléphet. Ezt követően fel kell tölteni a megvásárolt Paysafecard PIN-eket, természetesen az ügyfél saját My Paysafecard számlájára. Majd a feltöltött Paysafecard PIN-ek összege egyenlegként áll rendelkezésre a My Paysafecard számláján.

6.4 ABAQOOS

Az Abaqoos egy újabb online fizetési mód, amely akárcsak a korábbiak lehetővé teszi, hogy minél gyorsabban és biztonságosabban fizessen be pénzt az ügyfél. Ennél a módszernél, két féle lehetőségünk van a fizetésre. Az egyik az Abaqoos online banki átutalással, amelyet már a toplistás OTP-és ügyfelek online pénzügyi alkalmazások során igénybe is vehetik. Illetve a másik lehetőség a az Abaqoos utalvánnyal történő fizetés, amit bárki igénybe vehet. Ahhoz hogy egyáltalán valaki online banki átutalással tudjon befizetni a módszer használatával létre kell hozni egy Abaqoos pénztárcát az OTP direkt online banki rendszerében. ennek a létrehozása sem igényel, komoly megerőltetést, gyors, egyszerű és elég csak egyszer végigcsinálni. A regisztrációt követően az ügyfél kap egy 14-jegyű azonosítót, amivel aktiválhatja a már létrehozott pénztárcát, és ugyan ezzel az azonosítóval újra is lehet tölteni, természetesen mindez az ügyfélszolgálaton keresztül történik, e-bank vagy éppenséggel mobil bank szolgáltatás használatával.

6.5 SKRILL

A Skrill vagy régi néven Moneybookers egy igen népszerű nemzetközi elektronikus pénztárca, amit minden ügyfél kizárólag csak a saját országának pénznemében tudja feltölteni a saját bankszámlájáról, vagy akár bankkártyájáról, de lehetséges a feltöltése még csekkkel vagy egyéb, az adott országban elérhető fizetési módokon. Ez a módszer lehetővé teszi a biztonságos vásárlást az interneten keresztül a nélkül, hogy rettegni kellene attól, hogy a bankkártya adatai ellopásra kerüljenek.

Azonban néhány országokban még az is lehetséges, hogy közvetlenül a bankszámláról vagy bankkártyáról utaljunk pénzt anélkül, hogy előbb a Skrill számlát kellene, feltöltenénk.

A Skrill használatának leggyakoribb területei a szerencsejáték, online játékokon való fizetés, Skype egyenleg feltöltés, online áruházakban való fizetés, pl. az Ebayen, vagy akár egyes tőzsdéken is fizethetünk vele.

A Skrill előnyei a felhasználók számára:

- országhatárok nélküli azonnali pénzküldés online
- töredéke a hagyományos banki tranzakciók költségeinek
- a pénzküldéshez a kedvezményezett email címén kívül semmi más azonosításra nincs szükség
- használat/fizetés során semmi azonosításra nincs szükség
- könnyen feltölthető
- a jóváírások ingyenesek

6.6 NETELLER

A NETELLER oldala lehetővé teszi egy biztonságos ingyenes számla nyitását. Ezt az ingyenes számlát, az ügyfél feltöltheti bankszámlájáról kezdeményezett átutalással, vagy hitelkártya átutalással. A számla megnyitását követően több lehetőségünk adódik online pénzügyi műveleteink elvégzésére, mint például a be- és kifizetést kezdeményezése, valamint átutalásokat indíthatóak az online fizetést elfogadó számos vásárlási hely bármelyikén. A NETELLER számlanyitás kezelése igen csak egyszerű és roppant biztonságos internetes átutalási lehetőséget kínál, emellett folyamatos támogatást és információt is nyújt e-mail-ben, illetve élő chat, valamint telefon segítségével.

Tulajdonképpen miért érdemes ezt a rendszert használni? A fent említettek tudnám csak megerősíteni, miszerint gyorsabb és könnyebb lehetőséget nyújt a különböző internetes oldallal kapcsolatos be- és kifizetések kezelésére. NETELLER számla megnyitását és hitelesítését követően néhány másodperc elteltével már lehet is utalni akár saját számlára; illetve a számlának nem csak megnyitása díjmentes, hanem a használta is, ami eltér a klasszikus bankszámlák alkalmazásától, amik nem kevés költséget vonzanak maguk után.

Felmerül persze a kérdés hogy, biztonságos-e a NETELLER? Igen, biztonságos és elterjedt eszköze az online fizetésnek. Az eddig legjobban kifejlesztett titkosítási eszközöket, az SSL (Secure Sockets Layer, biztonságos socket réteg) protokollt /melyről a továbbiakban bővebben is ejtenék szót/, valamint a 128 bites titkosító kulcsot használja böngészőprogramokhoz. Tűzfal mögött történik az adatok biztonságos tárolása.

6.7 ENTROPAY

Az EntroPay akár csak az eddigiek online számla, ami egy előre fizetett EntroPay virtuális VISA kártyát ad. Ezt a kártyát bárhol fel lehet használni online fizetésre, ahol a VISA elfogadott. Ez az online fizetés szint úgy egy biztonságos módszere, mellyel ugyan elkerülhető, hogy felfedjük a hitelkártyánk adatait. Egy EntroPay számla és egy EntroPay VISA kártya igényelése nem tart semeddig, elég egyszerű. Az itt kapott kártyát megint csak hitelkártyával vagy akár bankkártyával és banki átutalással tölthetjük fel. A feltöltést követően akár egy jól ismert domino telefonos feltöltő kártya már használatba is kerülhet. Amikor egy EntroPay számlát nyitunk, szükséges regisztrálni egy feltöltési forrást azaz egy bankkártyát vagy hitelkártyát. Amikor készen állunk arra, hogy az új kártya feltöltésre kerüljön, az EntroPay közvetlenül a bank- vagy hitelkártyáról emeli le az összeget és írja jóvá azt az EntroPay VISA kártyán.

7. INTERNETBANKOLÁS ELŐNYEI, HÁTRÁNYAI

Az internet bankolás legfontosabb előnye, hogy különféle szolgáltatásokért nem kell a bankba mennünk, vagy nem kell hosszasan sorban állni az üzletekben, hanem otthonról pár kattintással elvégezhetővé válnak a banki szolgáltatások, vagy internetes vásárlások. Ez nem csak nekünk ügyfeleknek jó, hanem például sokkal több időt spórolhatnak a bankok, kereskedők, kevesebb papírmunkával jár, mely gyorsabb és kényelmesebb szolgáltatást jelent. Nagy előnye, hogy nem kell semmihez igazodni, gondolok itt például a nyitvatartási időkre, hiszen online minden a nap 24 órájában elérhető a világ minden pontján.

Az online bankolással azonnali információhoz juthatunk pl. aktuális egyenleg, tranzakció elvégzésekor azonnal jelzi az esetlegesen előforduló kitöltési hibákat. Az is nagy előnye, hogy ez a szolgáltatás a legolcsóbb a bankszolgáltatások között. Ennél drágább a telefonos ügyfélszolgálat, majd a bankfióki ügyintézés, ahol mindkét esetben az élömunka költségét hárítják ránk a bankok.

Mivel az elektronikus bankolás során gépek szolgálnak ki minket, melyek teljesen kiváltják az élő munkát, így a bankok jelentős költségek spórolnak meg rajtunk. Ezáltal a felénk biztosított kedvezmények mértéke is jelentősen növekedhet.

Az internetes bankolás előnyei egy szóval mondvá vitathatatlan. Egyszerű, gyors, rugalmas, olcsó. Azonban ezzel együtt továbbra is léteznek kockázatos szolgáltatások, mivel a rendszer működéséhez azonosítókat, jelszókat és személyes adatokat kell megadni.

Az e-bankolás leggyakoribb problémája, hogy ez merőben új szolgáltatás még. Probléma lehet az is, hogy a már meglévő, de továbbfejlesztés alatt álló szoftver nem indul el, vagy nem érhető el teljesen. A másik nagy probléma, hogy a rendszerrel kapcsolatos kérdésekkel, problémákkal szemben, az ügyintézők kevésbé felkészültek. Emellett előfordul a rendszer túlterheltsége is, de nem mehetünk el a legfontosabb feltétel az internetkapcsolat megléte mellett sem. A rendszer másik nagy problémája az ezekkel szemben elvárt biztonsági feltételei lehetnek.

Habár az internet a nap 24 órájában működik, jogszabályban rögzített rendelet szerint a magyar bankok többségénél a zárást követő online tranzakciók is csak késleltetve történnek, ez a legtöbb ügyfél számára kellemetlen lehet.

Egy másik rendelet szerint azonban napközben, 4 órán belül teljesíteni kell mindenféle tranzakciót, a zárás után beérkezetteket pedig a záróra utáni 24 órán belül.

8. INTERNETES CSALÁSOK, ÉS NÉHÁNY BIZTONSÁGI MEGOLDÁS

Az online banki felületek elterjedésével egy időben, velejárójaként elterjedtek az internetes csalások is. Leggyakoribb csalási kísérletek közé a csalók által, a bank nevében küldött ál e-mailek tartoznak, melyek a számlatulajdonos adatait kérik. Más kémprogramok viszont, a billentyűzet leütését figyelik, és ezeket szűrve próbálják kideríteni a banki jelszavainkat.

8.1 SSL BIZTONSÁGI PROTOKOLL, CSALÁSOK, KÉMPROGRAMOK

Az SSL protokoll, egy olyan biztonsági protokoll, mely segítségével titkosított csatornánk keresztül kommunikálhatunk a bank szerverével, vagy különböző online vásárlási felületen a kereskedővel. Biztosítja, hogy az adatátvitel során ne lehessen visszafejteni és manipulálni az adatokat. Ezáltal ellenőrizhetjük egy oldal identitását. SSL protokoll során a http után egy „s” betű kerül mely utal a biztonságra (secure). Minden „https” oldal lekérése során a böngésző megvizsgálja, hogy az adott oldalnak van-e érvényes SSL tanúsítványa. Ha nincs, akkor megjelenik egy biztonsági figyelmeztetés.

Technikai működése az SSL protokollnak

A „https” alapján felismeri a böngésző, hogy szükséges-e tanúsítvány kérése a szerverről. Ehhez a szervernek a tanúsítványt meg kell kapnia a tanúsító helytől. csak ez után jelzi a böngésző felé a szerver a tanúsítványt. A tanúsítvány érvényességéhez szükséges információkat a böngésző a tanúsító hely jegyzékéből kapja.

Ez egy többszintű azonosítási rendszer. Felhasználó név, jelszó, biztonsági kódok megadása külön-külön egy-egy szintet jelent. Ez egyben egy többcsatornás rendszer is, hiszen egy másik eszközön is azonosítanunk kell magunkat. Pl. egyszer használatos biztonsági jelszó küldése SMS-ben, vagy tokenel történő kódgenerálás, chip-, webkártyák.

Nyilvános helyen történő ügyintézés során ügyeljünk arra, hogy jelszavunkat ne lássa senki, az elvégzett ügyintézés során megfelelően, szabályosan lépünk ki, töröljük a böngésző előzmény listáját, ne használjunk segédprogramokat, és ügyeljünk arra, hogy a rendszer semmilyen jelszó vagy felhasználónevet ne tároljon. Ajánlott bizonyos időközönként a jelszó megváltoztatása is.

A leggyakoribb csalási kísérlet, **adathalászat módszere**. Azaz, a csaló kéretlen levelet küld a bank nevében (spam). Leggyakrabban adategyeztetés, vagy karbantartás miatt kérik az ügyfeleket, arra, hogy adják meg a belépéshez szükséges felhasználónevet, jelszókat.

Azonban mindig figyeljünk arra, hogy a bankok, soha semmilyen esetben sem kérhetnek ilyet e-mailben, vagy telefonon. Ezek az e-mail-ek, általában egy a bankéra nagyon hasonlító email címről érkeznek, mely akár tartalmazhatja a bankunk logóját is.

Pl. xyzbank@xyzbank.hu cím helyett xyzbank@xyzbank.hu.com cím használata.

A kezdeti csalási kísérletek egyszerűségük miatt azonban már a manuális ellenőrzésnél megbuktak. Az újabb módszerek azonban jóval pontosabbak.

A csalók a kiszemelt ügyfelek bankjában számlát nyitnak hamis igazolvánnyal vagy álnéven. Ha sikeresen megszerezték a jelszavakat és azonosítókat, akkor azonnal utalnak. Bankon belül már sokkal gyorsabban átkerül egyik számláról a másikra a pénz, ahonnan egyből fel is veszik a csalók, vagy továbbutalják. Ez a módszer sajnos még az elmúlt pár évben is rendkívül jól működött.

Az egyszintű azonosítás mellett, azonban még akkor sem vagyunk teljes biztonságban, ha nem dőlünk be ezeknek a módszereknek. Az időben nagyon gyakori volt a saját gépünkbe telepített kém módszer, melyek válaszadás nélkül is megszerezhették adatainkat. Minden olyan programot melynek fő célja, hogy a felhasználó tudomása nélkül megszerezzék a megtámadott gép felhasználójának személyes adatait, vagy banki jelszavait azonosítóit, számlaszámát **kémprogramoknak** nevezzük. Feltelepülésük lényegében észrevehetetlen történik, kihasználva a felkészületlen, és figyelmetlen felhasználók hibáit, valamint a számítógépek biztonsági hiányosságait. Léteznek azonban trójainak álcázott álprogramok is, melyek a felhasználó „segítségével” települnek fel a számítógépre. A támadások után a megfertőzött rendszer nem úgy működik, mint a normális. Gyakoriak a fagyások, a CPU lefoglalásából eredő belassulások, valamint a rendszerösszeomlások. Egyes programok képesek beépülni a vírusirtóba is, vagy képesek kikapcsolni a tűzfalat. Ezek a kémprogramok, egy egyszerű internetes letöltés, vagy weboldalak látogatása során is észrevehetetlenül telepítődnek gépünkre. Ezek rögzítik a gépünkön a billentyű leütéseket, továbbítják az illetéktelen megfigyelőknek, és különféle szűrések után jutnak hozzá a belépési adatokhoz.

Ehhez nem kell mást csinálniuk, mint a www.xyzbank.hu/jakabpass adatsort értelmezniük, melyből kiderül melyik bank internetes felületén léptem be, mi volt az azonosítóm (jakab), a jelszavam (pass). Így szabályosan használhatják a számlánkat anélkül, hogy bármiféle hibát is elkövettünk volna.

Ezt a módszert azonban könnyen kiküszöbölhetjük, ha egy internet banking szolgáltatáshoz nem egy statikus jelszó tartozik. Erre a legegyszerűbb lehetőség, ha az azonosító megadása

után a rendszer generál egy új, addig nem használt jelszót, melyet e-mailben, vagy SMS-ben kapunk meg. Ezáltal máris többszörös lesz a biztonsági rendszer. Persze sokakban egy újabb kérdést vet fel ez az opció, hisz az eddigi bank-ügyfél kommunikációba belép a mobilszolgáltató is, ami akár tovább növelheti a kockázatokat. Ám az elmúlt 1-2 év tapasztalatai azt mutatják, ez a biztonsági funkció a támadások nagy részét visszaszorította. Ezzel a megoldással gyakorlatilag a többszörös azonosítóval rendelkező internet banking szolgáltatásoknál megszűntek a sikeres visszaélések. Ám még ennél is léteznek fejlettebb megoldások, pl. token, chipkártya (különösen online vásárláshoz), biológiai azonosító. (ujjlenyomat, vagy íriszazonosító)

Az elmúlt évek egyik legnagyobb csalási programja a **Zeusz**, 30 ezer európai net bankolónak, több mint 10 milliárd Forintnak megfelelő kárt okozott. A szoftvert Magyarországon is alkalmazták. A Bankszövetség, az OTP Bank és az Erste bank közleményei szerint a kártevő program nem csak, a számítógépekre, de akár az okos eszközökre is képes települni. Az okos eszközök, a bank által küldött SMS-ben található jelszó megszerzéséhez kellhet. A szoftver működésének lényege, hogy beépül az online banki felület és a felhasználó közé, elérve minden adatot. Belépéskor, az online felületen egy várakozásra figyelmeztető üzenet jelenik meg, ám ekkora valójában már nem a bank honlapján vagyunk. A várakozás alatt, a program jogosulatlan pénzmozgásokat végez.

Eurograbber:

Egy olyan vírustámadás, amely a felhasználó gépe ellen fordul. Megfertőzi az operációs rendszert, és weboldalakat meghamisítja.

A gép botnetbe szervezésére is sor kerül. A botnet más néven zombi számítógépek hálózata. A zombi számítógép olyan számítógép, melyet vírusokkal és trójaiakkal fertőzött meg egy cracker. ezzel a számítógép erőforrásait saját célra, DoS támadások erősítésére használja. Spamek küldésére is az ilyen botokkal irányított gépeket használják. A cél nagy teljesítményű gyors és anoním hálózat kiépítése spammereknek. Egy áll címszó „biztonság fejlesztése” alatt kapunk kéretlen üzenetet mely során személyes adatokat kérnek el. Például egy telefontípust, mellé egy telefonszámot, amire a támadó egyből küld el SMS-t, és az ügyfél ennek megnyitását követően az SMS-ben szereplő linkre kattintva nyomban telepíti a vírust a telefonjára is.

Működésének lépései

1. Felhasználó bejelentkezik a NetBankjába
2. A vírus aktiválódik ezáltal
3. A vírus elküldi a támadónak a megadott azonosító adatokat
4. A támadó elindít egy tranzakciót
5. A tranzakciós SMS-t megszerzi a mobilra telepített vírus
6. A vírus által beszúrt oldal még egy token kódot, vagy az SMS-ben kiküldött kódot kéri be
7. A támadó megszerzi a megtámadott személy pénzét

8.2 PHARMING

A legújabb módszer pedig a Pharming. Ez a módszer IP-cím azonosításon alapul. Az IP cím, az internetes honlapok azonosítására szolgál. A böngésző címsorába mikor beírjuk a megjeleníteni kívánt honlap címét, egy központi számítógép megkeresi az ennek megfelelő IP címet, és így jelenül meg a számítógépünkön a keresett honlap. A Pharming lényege, hogy a csalás során a támadó a központi számítógépet törli fel, és a megjeleníteni kívánt weblappal teljesen megegyező, de más IP címmel ellátott ál weblapot jelenít meg. A belépéskor használt adatok ekkor kerülnek a csalóhoz. Az ügyfél azonban semmit sem vesz észre a dolgokból, mivel rögtön a kódok megadása után, visszajutunk az eredeti honlapra, ahol meg is kapjuk az azonosítás sikerességét igazoló visszajelzést.

Ez ellen könnyen védekezhetünk. Az egyik módszer, hogy nem a kívánt honlap címét írjuk be a címsorba, hanem az IP címet. Ezt minden banknál el lehet kérni. A másik módszer, hogy nem közvetlenül a címsorba írjuk be a címet, hanem a Googlebe.

A mobil bankolás azonban még veszélyesebb lehet. Kétszintű biztonsági rendszerről ugyanis addig beszélünk, amíg legalább 2 egymástól független eszközön megy az azonosítás és jelszóküldés. A okos telefonon való utaláskor pont ez a biztonsági rendszer szűnik meg. Ekkor a vírus akár az érkező SMS-ekhez is hozzáférhet. Ám ez ritka, hisz ilyenkor mind az adott bank rendszerét, mind az SMS-t ismernie kell a vírusnak, hogy a megfelelő kódokhoz jusson. Hogy ne álljon fenn a megnövekedett veszély, ezért itt is csak legális, folyamatosan frissített programokat szabad használni, valamint naprakész, kártékony szoftverek ellen megfelelő védelmet biztosító szoftvereket szabad csak használni.

Az online banking, vagy online kereskedelem fejlődését két fő tényező határozza meg. A felhasználói bizalom, és az adatbiztonság. Mindkét területen folyamatos a fejlődés. Azonban a bizalom kérdése nem csak a felhasználók részéről, hanem a bankok részéről is felmerül. Egyes pénzügyi intézetek ügyfeleik számítógépeit ellenőrzés alá vonják, átvizsgálva az Antivirus programok frissességét. Ha a bankok biztonsági intézkedéseik ellenére is adódik bármiféle visszaélés a bankok többnyire átvállalják a felelősséget. Azonban akad egy kivétel. A PIN kóddal való visszaélés, ekkor a bankkártyákhoz hasonlóan a felelősség a felhasználót terheli.

8.3 TANÁCSOK E-BANKOLÁSHOZ

Az online bankoláshoz tartozó általános műveletek és védelmi tanácsok, melyek növelik a felhasználók bizalmát, a szolgáltatás alkalmazásával kapcsolatban. Ha egy adott bank online oldalára regisztrálunk további tanácsokat kaphatunk a biztonságos tranzakciók végzéséhez.

- Okos telefonon, vagy akár sima számítógépen is ügyelni kell a nyilvános hálózatokon történő adatátvitelkor a megfelelő kódolásra. A programok használata során meg kell győződni arról, hogy a nyilvános WiFi hálózat megfelelően van-e kódolva. Erről a különböző bankok honlapján megfelelő tájékoztatót találhatunk.
- A jelszavak kiválasztásánál ügyeljünk a nehezen kitalálható jelszó megalkotására. Fontos a kis és nagy betűk, számok, és különleges karakterek használata. Legtöbb esetben, már a szoftver is csak az ilyen „kevert” karakterekből álló jelszavakat fogadja el. A PIN, és bármi egyéb jelszavakat a megfelelő körültekintéssel tároljuk, senki illetéktelen személynek ne adjuk meg!
- Csak saját gépről/eszközről intézzük ügyeinket. Minden online banki ügymenet során ki kell jelentkezni, a banki tranzakciók után pedig mindig törölni kell a köztes tárolót (cache) a számítógépen. Ezt a különböző böngészők beállítások menüjében érhetjük el.
- Fontos a megfelelő, naprakész programok alkalmazása. Semmilyen ajánlott, vagy bizonytalan programot nem szabad letölteni.
- Naprakész vírusvédő szoftver, és tűzfal használata különösen ajánlott! Figyeljünk arra, hogy a frissítéseket mindig az adott szoftver kiszolgálójának oldaláról töltsük le!
- Folyamatosan ellenőrizzük a programok megfelelő működését. Szokatlan, vagy rendellenes működés esetén feltétlenül kapcsolatba kell lépni a bankkal.
- A számlamozgást is folyamatosan ellenőrizzük. Szokatlan pénzmozgások esetén azonnal kapcsolatba kell lépni a bankkal. Ezek mielőbbi felismerése érdekében,

különösen ajánlott a különböző SMS-es értesítők használata, mely egyből jelez, ha valaki használta a számlát.

- Napi limit beállítása a bankkal együtt.
- Semmilyen e-mailre nem szabad reagálni, amiben bármi adatot próbálnak megtudni tőlünk. Az e-mail elolvasása után, értesítsük a bankot ne kövessük az e-mail utasításait.
- Bankkártya, banki hozzáférés haladéktalan letiltása telefonon, vagy online is azonnal elvégezhető.

8.4 AZONOSÍTÓ ÉS VÉDELMI RENDSZEREK

Napjaink legbiztonságosabb megoldásának a chipkártyás megoldást tartják. Ez esetben a számítógéphez egy chipleolvasó csatlakozik, és az azonosítás ezen keresztül történik. Vagyis sem a PIN kódok, sem más azonosításra szolgáló adat nem kerül ki a hálózatra. A kísérleti szakaszban résztvevő ügyfelek ingyenesen jutottak ehhez a rendszerhez, később azonban fizetős lesz.

Az F-Secure biztonsági cég szolgáltatása egy extra védelmi réteget biztosít online banki tranzakciókhoz. Az Internet Security 2013-as programjuk blokkol minden olyan hálózati kapcsolatot melyek veszélyeztethetik a banki műveletek biztonságát. ez a funkció a háttérben fut, és így nem akadályoz semmilyen banki műveletet, ezzel együtt folyamatosan ellenőrzi a weboldalakat. Az ellenőrzött weblapokhoz folyamatos hozzáférést biztosít. Ehhez a megoldáshoz nem kell semmilyen speciális extra szoftvert telepíteni.

A G Data InternetSecurity 2014 két keresőmotorral ellátott felhő alapú védelmi rendszer. A program tűzfala blokkolja a betörési kísérleteket, a beépített levél szűrő, pedig folyamatosan mentesíti a felhasználót a kóros levelektől. A biztonságos online bankoláshoz a G Data BankGuard szolgáltatás megóvja a böngészőket a trójai vírussal szemben, és egyedülálló közvetlen védelmet biztosít az internetes hitelkártyák használata során.

Az internet bankolás terjedésének robbanás szerű terjedését az elektronikus aláírás jogszabályba való megjelenésétől várják. Fontos azonban megjegyezni, hogy a számítástechnikával kapcsolatos bűnözések 75%-áért az emberi mulasztás, és a megfelelő biztonsági lépések nem megfelelő betartása okozza.

BOSS

Ausztráliában a Bonds Software Assurance Centerben kifejlesztettek egy, a biztonságos online bankolásra alkalmas szoftvert, amely a BOSS (Bank On Secure System) nevet kapta. A végfelhasználóknak szánt alkalmazás, mely lehetőséget teremt az otthon banki műveletek kényelmes elvégzésére. A lényege, hogy az egész egy bootolható CD-ről fut, így kikerüli annak a lehetőségét, hogy a merevlemezen bujkáló vírusok, vagy egyéb trójai programok kárt okozzanak, hisz ez által nem válnak aktívvá. Ennek az alkalmazása nem vesz túl sok gondolkodást igénybe, mindössze behelyezzük a CD-t, és újraindítjuk a gépünket. Ettől kezdve a rendszer betöltése már nem a merevlemezünkről fog történni, hanem a behelyezett CD-ről, ami csak olvasásra alkalmas, tehát nem okozhat benne vírus kárt. A szoftver sajátossága, hogy emellett még a billentyűzetfigyelők ellen is védekezik egy virtuális billentyűzettel, vagyis a felhasználói nevek és jelszavak beviteléhez is elég az egér. Előnye még hogy a meglévő rendszereken is képes működni, nincs szükség sem a felhasználóknak számítógépükön új eszköz beszerzésére, sem a bankokban nem kell új rendszert telepíteni, csak a korábban említett CD kell hozzá. Ami ellen azonban még ez sem véd az, az utóbbi időben teret nyert internetes csalásforma, az adathalászat. A korábbiakban már említett kísérletek sorra sikerrel járnak, noha az elmúlt időszakban számos bank népszerűsítette azt a tényt, hogy online soha, semmilyen körülmények között nem kéri el ezeket az adatokat a felhasználóktól. Egyre előtérbe kerül, hogy a mindennap használt operációs rendszerünktől, egyúttal az abba beépülő és futni képes vírusoktól, trójaiaktól független megoldásra milyen nagy az igény.

Kaspersky Internet Security 2014

Funkciói (okos eszközökre, és asztali számítógépekre egyaránt alkalmas)

- Biztonságos pénzügyek funkció
- Biztonságos adatbevitel funkció
- Új Zeta shield és Anti-blocker technológia a célzott támadások ellen, valamint webes védelem valós idejű vírusvédelemmel

Biztonságos pénzügyek funkció

A program egyik legfőbb funkciója a Biztonságos pénzügyek funkció, mely megfelelő védelmet kínál a felhasználók számára, legyen szó internetes vásárlásról, vagy online banki ügyintézésről. Ez a funkció azonnal bekapcsol mikor a felhasználó bármely olyan felületre lép melyeken az említett 2 opció valamelyike megtalálható.

A program működése

- A megnyitott weboldal URL címét összehasonlítja a már biztonságosnak ítélt weblapok URL címével a szoftver adatbázisából
- Ha nincs bekapcsolva az automatikus funkció, akkor a program egyből javasolja, hogy az adott weblapok a Biztonságos Pénzügyek üzemmódban kerüljenek megnyitásra
- Ellenőrzi a biztonsági tanúsítványokat, azaz elkerülhető, hogy hamis oldalra kerüljünk.

Biztonságos adatbevitel funkció (fizikai vagy akár virtuális billentyűzettel)

- Különbféle billentyűzetfigyelő-programokkal illetéktelenek megszerezhetik a bankkártya számunkat, PIN és egyéb azonosító kódokat. A program Biztonságos Adatbevitel technológiája erre a problémára kínál megoldást. Fizetésre alkalmas weboldal megnyitása után (vagy akár szimplán egy olyan oldalon ahol jelszavunkat adjuk meg) a funkció automatikusan aktiválódik, ezzel távol tartva a billentyűzet-megfigyelőket.

Új Zeta shield és Anti-blocker technológia a célzott támadások ellen, valamint webes védelem valós idejű vírusvédelemmel

- Dupla védelmi réteg az új típusú fenyegetések, és a képernyőt zároló fenyegetések ellen, valamint, a webes védelem funkció biztosítja a védelmet az adathalászokkal és az egyéb rossz indulatú weboldalakkal szemben.
- Ezzel együtt valós idejű felhő alapú vírusvédelmet nyújt vírusok, trójaiak, kémprogramok és egyéb számítógépes támadásokkal szemben.

Biztonságos bankolás Pendrive segítségével

Vállalati felhasználóknak kínál biztonságos online bankolási megoldást az Ironkey. IronKey Trusted Access for Banking megoldása egy USB-s eszközre és egy védelmi szolgáltatásra épül. A megoldás úgy működik, hogy csatlakoztatjuk a pendrivera hasonlító eszközt a számítógéphez, és a hitelesítéshez megadjuk az adatainkat. Ez a megoldás nagy mértékben a virtualizációra épül. Csatlakoztatás után egy Linux alapú virtuális környezetben kerülünk. Ekkor rögtön lehetőség nyílik egy gyors víruskeresésre, mellyel meggyőződhetünk arról, hogy a számítógépünkön nincs trójai, mely alkalmas lenne az adataink ellopására. Ha nincs fenyegetettség, akkor lehetőség nyílik egy webes banki rendszerhez való csatlakozásra. A program hátránya, hogy ezt a bankoknak is támogatni kell, valamint, hogy az Ironkey elvesztése esetén, az új beszerzéséig nincs lehetőség online banki ügyintézésre.

9. ONLINE BANKOLÁS TECHNIKAI LEHETŐSÉGEI

Az internet bankolással kapcsolatban számos új technikai vívmány áll pénzügyi műveletek elvégzéséhez az ügyfelek rendelkezésére. Az egyik ilyen népszerű újítás a Mobil Banking szolgáltatások, melyek mára már többféle technikai malőrt valósítottak meg. Az SMS-alapú mobil bankolás az egyik legelterjedtebb, legolcsóbb és legkönnyebben megvalósítható változata. Ennek a megoldásnak a használata során nem kerül az ügyfél banki kapcsolatban egyetlen banki ügyintézővel sem. A tranzakciót egy szimpla SMS-es segítségével hajtjuk végre, és a visszajelzés a tranzakció sikerességéről is SMS-ben érkezik.

Természetesen nem csak SMS alapú tranzakció hajtható végre mobiltelefonunkkal. A mai okos telefonok segítségével, már bárhol és bármikor elintézhethetjük pénzügyeinket, és mindössze csak internet-elérésre van hozzá szükségünk. Az online bankok a legnépszerűbb és legfrissebb funkciókat biztosítják telefonjainkra, vagy az olyan gyakran használt táblagépekre optimalizálva. Minden ez természetesen nem csak magyar nyelven érhetőek el, gyakori az online banki oldalak angol nyelvű leírása is. Mobil eszközön elsősorban a belépéshez szükséges a használt felhasználói azonosító, illetve a bejelentkezési kód, melyet regisztráció után kapunk. A belépést követően a pénzügyi műveletek végrehajtása már egyszerű az utalást, például jóváhagyhatja egy Token segítségével, melyről a továbbiakban beszélnek majd bővebben, de a lényege, hogy ez által ugyan nem teljes, de a lehető legjobb biztonsággal kezelhetjük saját bankszámlánkat. Itt néhány mozdulattal további hasznos információhoz juthatunk, nem csak saját számladatainkkal kapcsolatosan, hanem úgy általánosságban is, mint például megtekinthetjük a regisztrált Bank deviza és valuta árfolyamait, a legfrissebb hírekről, és legújabb funkciókról is pillanatok alatt értesülhet. Továbbá ha éppen készpénzre lenne szüksége az ügyfélnek, de nem tudja, hogy hol talál a közelben ATM-et mert nem ismerős a környéken, akkor az alkalmazás segítségével megkeresheti a hozzá legközelebb eső ATM-et, ami utazás során például igen előnyös lehetőség. És nem utolsósorban felveheti a kapcsolatot a banki ügyintézőkkel probléma esetén.

A mobil alkalmazások során is felmerül az online bankolók általános kérdése, hogy mennyire biztonságos ez. A Bankok úgy vélekednek, a saját mobil alkalmazásaikról, hogy növelik a biztonságérzetet. Hiszen az általuk készített alkalmazásokhoz, a csalóknak külön trójiákat kellene írniuk, ahhoz hogy hozzá tudjanak férni az ügyfelek pénzeihez. És ez még a profiknak sem biztos, hogy olyan egyszerű. Éppen ezért ez nem hogy csak az országban, ahol a kisebb

ügyfélszám miatt meg se éri, de még nemzetközi szinten is nagyon ritkán fordul, nem kimondottan jellemzőek az efféle támadási kísérletek.

De mindettől függetlenül azért még vannak gátjai e fizetési mód elterjedésének. Több felmérés is mutatja, hogy az emberek nehéznek, bonyolultnak tartják a mobil fizetést, természetesen ez nem a fiatalabb korosztályt érintik. Leginkább negatívumként a biztonságtalanságot hozzák fel, az ügyfelek tartanak attól, hogy együttműködési hibák jelentkeznek a mobil fizetési szolgáltatók között, félnek attól, hogy a tranzakciói elvégzése során valami hálózati hiba lép fel. Illetve felmerülhet még problémaként a lassúság, gyenge kezelhetőség is. Ám azok száma, akik még is aktív használói ennek a technikai vívmánynak arra sarkalják a nagyobb bankokat, hogy ez ügyben komoly lépéseket tegyenek. Az újítások során elsősorban azon ügyfelekre épít, akik azért hajlandóak fizetni, hogy ezen alkalmazások valamelyikét használhassák bárhol, és bármikor. Ezek a mobil hozzáférések már lehetővé teszik, hogy a bankok üzleti részét ugyan még csekély, de egyre szélesedő körben átláthassák. Ennek részét képezi, hogy az ügyfelek a korábbinál nagyobb szabadságot kapnak, könnyebbé válnak számukra a tranzakciók, több információhoz jutnak és megnövekszik az interaktivitás. Ilyen új funkció például a Mobil bankolás biztonságos dokumentumkezelése. Hogy ez mi is pontosan? Az iPhone-okra, iPadekre és Android készülékekre kifejlesztett alkalmazásokról van itt szó. Ezek az appok tulajdonképpen fotót készítenek a kitöltött hivatalos iratokról, majd a szkennelt dokumentumokat egy biztonságos csatornán keresztül továbbítja címzetthez. Sikeres kézbesítés után az applikáció törli a telefon memóriájából az átküldött file-t.

Az újítások sorát hosszabbítja az úgynevezett Safe Courier, mely a hasonló mobil megoldásokhoz képest lényegesen kibővítette azoknak a dokumentumoknak a körét, amelyeket mobilon keresztül továbbítani lehet. A korábbi applikációk csak adott intézmények saját formanyomtatványait tudták kezelni. Ez ezzel szemben a változatosabb formájú, típusú dokumentumok feldolgozására is alkalmassá vált, olyanokra, mint például a különböző kölcsönszerződések, vagy az adópapírok, de bármilyen átutalási kérelemmel is képes foglalkozni, továbbá még a hitelig a hitelkártya igénylő lap feldolgozására is alkalmas.

Aztán megemlíthetjük még, Xeroxot, mely azzal a szándékkal fejlesztette ki ezt a megoldást, hogy egyszerűen integrálni lehessen a különböző céges dokumentumkezelő rendszerekkel. Természetesen ez is alkalmas arra, hogy más egyéb ügyintézéseket felgyorsítson az eddigiekhez képest, így sikeresen alkalmazható akár az oktatási, egészségügyi, jogi, biztosítási vagy akár az önkormányzati adminisztrációban is, a fejlesztők véleménye szerint.

Néhány sorral feljebb már megemlítettem az úgynevezett Token-t, most említenék is róla néhány szót. Az úgynevezett token egy a Bank által biztosított eszköz mely jelszavakat generál, ezek a jelszavak csak egyszer használhatók az Internet alapú elektronikus szolgáltatásokba. Ez kiemelt védelmet nyújt pénzügyi műveleteink online elintézésére, és még könnyebb használhatóságot is biztosít. A token adatai alapján ellenőrzi a banki rendszer a felhasználói jogosultságot.

Ízelítő a technikai újdonságokról a pénzügyekben			
Terminálok	Bankolás	ATM-ek	Egyéb
Tenyérolvasó terminál	Okosszemüveges bankolás	Sétáló bankautomaták lehetünk	Felhőben futó biztonsági rendszerek
Ujjlenyomat olvasó terminál	Személyes pénzügyi menedzsment	Érintésmentes készpénzfelvétel	Katasztrófavédelmi rendszer a felhőben
Okostelefonból POS-terminál	Modern konakt centerek	Készpénzmentes bankautomaták	Mobilba költöztetett bankkártyák

Forrás: Portfolio.hu

5. ábra: Technikai újdonságok

Nos az Electra Internet Banking a hitelesítési lehetőségek széles választékát tárja elénk. Az online banki rendszerek egyik legfontosabb eleme a kétszintű hitelesítés. A bejelentkezés után a felhasználók csupán csak lekérdezéseket kezdeményezhetnek, aktív műveletek elvégzéshez külön hitelesítésre van már szükség, vagy is ez azt takarja, hogy az egyes tranzakciókat csak aláírás után lehet a bankba küldeni. Lehetőségünk van többes aláírások kezelésére is. Ez főleg a vállalatoknak hasznos funkció, hiszen ezzel megadhatók például első- és másodhelyi aláírók is egyaránt.

A rendszer az alábbi hitelesítési módokat támogatja:

- SMS jelszó
- token
- TAN kód
- aláírási jelszó
- QR kód
- chipkártya
- a legújabb a VICA
- biometrikus azonosítás

A felsorolt hitelesítési lehetőségek közül a pénzüintézetek szabadon választhatnak. Sőt lehetőségük van arra is, hogy ezen felsorolt módokat kombinálják is valamilyen formában a biztonság növelése érdekében, illetve hogy azokat limitekhez kössék. A hitelesítés módja továbbá lehet felhasználónként külön-külön állítható, így az egyedi ügyféligények is kielégíthetők.

SMS

Előnye:

- biztonságos
- könnyen használható, népszerű
- felhasználóhoz és tranzakcióhoz van kötve

Hátránya:

- költséges
- valamilyen külső szolgáltatótól függ

Már a korábbiakban is hangsúlyoztam, hogy az SMS jelszó az egyik legbiztonságosabb. A magyarországi bankok és takarékszövetkezetek által egyre gyakrabban alkalmazott hitelesítési mód. Európai összevetésben is a mi országunkban a legnépszerűbb ez a mód. Az SMS jelszavas hitelesítést Magyarországon elsőként a Cardinal Kft. vezette be 2002-ben. Azóta a legtöbb Electra Internet Bankinget használó pénzintézet az SMS jelszavas hitelesítést is támogatja. Ez előtt leírtam ennek a módszernek a működési elvét, így erre nem térnék ki még egyszer. Itt a biztonságot az adja, hogy az aláíráshoz szükséges kód, az internettől független csatornán érkezik a felhasználóhoz, az autentikáció alapja pedig az eszköz jelen esetben a mobiltelefon, ami a felhasználó birtokában van. Amit nem említettem még, hogy ez egy időkorlátos módszer, tehát a kiküldéstől számítva egy előre meghatározott ideig lehet csak felhasználni. Az SMS szövegében bizonyos helyzetekben az egyszer használatos kód mellett megerősítésképpen a tranzakció típusa és jellemző adatai is megjelenhetnek.

Token

Előnye:

- egyedi tranzakciós kódok
- független eszköz

Hátránya:

- drága
- plusz eszközt kell magunknál tartanunk

A token olyan hitelesítési hardver eszköz, mely nagyban hasonlít az SMS jelszavas megoldásra, azzal a különbséggel, hogy az egyszer használatos, egyedi aláírási kódokat nem a bank generálja, hanem az ügyfél birtokában lévő, önálló elektronikus eszköz. Az autentikáció lényege itt is egy bizonyos fizikai eszköz birtoklása, csak jelen esetben ez az eszköz nem a mobiltelefon, hanem egy token. A banki regisztráció során egyedi tokent rendelnek a felhasználóhoz, és a tokenekhez tartozó szerveralkalmazás feladata lesz eldönteni a továbbiakban, hogy a felhasználótól beérkezett token-kód valóban attól az eszköztől származik-e. Amit szintén nem említettem korábban, hogy kétféle token eszközt különböztetünk meg: az egyik beépített billentyűzettel rendelkezik, és egy PIN kód segítségével önmaga biztosítja azt, hogy a token elvesztése esetén a kódot még csak véletlenül se lehessen felhasználni, a másik amikor nem rendelkezik billentyűzettel, itt viszont egy aláírási jelszót is bekér, és ezzel biztosítja a védelmet még inkább.

TAN kód

Előnye:

- olcsó
- egyszerű használni
- egyszer használatos kódok

Hátránya:

- papíralapú, így nem védhető PIN kóddal
- „fapados”

Az ügyfél szintén egy egyszer használatos, egyedi előre generált aláírási kódokat kap, de ezeket most már nem egyesével, hanem kötegelve azt egy táblázatban összegyűjtve, egyszerre akár több tíz darabot is. Ezek egy, vagy a bank vagy az ügyfél által kinyomtatott papíron vannak, ha egy kód felhasználásra került, akkor azt a táblázatból kihúzza, és a következőt használja. Ahogy elérkezik, a legutolsó kódhoz egy új TAN kód listát tud magának generálni. Ez a megoldás a többihez képest elavultnak tűnik, ennek ellenére még széles körben elterjedt, hiszen nincs járulékos költsége, gondolok itt például a kiküldött SMS-ek díjára.

Aláírási jelszó

Előnye:

- olcsó
- egyszerű használni

Hátránya:

- könnyű ellopni
- statikus adat

Az aláírási jelszavas hitelesítést tartják az egyik leggyengébbnek a mai lehetőségek tárháza közül, és az adathalászat támadások által a legsérülékenyebb hitelesítési mód is lényegében. Az ügyfél rendszerint ugyanazt a hitelesítési kódot adja meg, így ha ez egyszer illetéktelen kezébe jut, bármikor visszaélhet azzal. Csak korlátozott funkcionalitás engedélyezhető.

Chipkártya

Előnye:

- PKI technológia
- legmagasabb szintű biztonság

Hátránya:

- csatlakoztatni és telepíteni kell
- inkompatibilis kártyák és meghajtók
- nincs mobilitás, nem használható okos eszközökön

2000-es évek környékén olyan ígérek terjedtek el, hogy minden eszköz tartalmazni fog egy chipkártya olvasót, ennek ellenére nem történt meg, hanem csökkent a csatlakoztatható perifériák köre, és ugyan ez a feltevés 2005-ben is jelen volt.

Chipkártyák alkalmazásához fizikai eszközt kell csatlakoztatni, de a felhasználó számítástechnikai platformja széttágulódott, a Windows mellett megjelent iOS, Android stb.

A megoldás nehézségei abból fakadnak, hogy a kártyák és kártyaolvasókhoz egyaránt szükséges meghajtókat telepíteni. A böngészők szintén nem tudják ezeket az eszközöket használni. Így elvesztjük a mobilitás előnyeit, a felhasználó gépéhez kötődik.

ViCA

A ViCA alkalmazás egy újfajta, korszerű hitelesítő eszköz. Segítségével a lehető legnagyobb biztonságban használhatjuk az adott bankok internet banking szolgáltatásait. Ennek használatával nincs szükség jelszavakra és nem jönnek többé SMS-ek sem. Egyszerűen bejelentkezhetünk az internet banking szolgáltatásba és jóváhagyhatjuk tranzakcióinkat. Phishing, pharming és Eurograbber-szerű támadások ellen védett. Személyes hitelesítő eszköz, melyet elsősorban be kell regisztrálnunk a bank elektronikus rendszerére.

A ViCA alkalmazáshoz történő hozzáférést az jelszava védi. Ez biztosítja, hogy az alkalmazást csak az regisztráló ügyfél használhassa, és illetéktelen személy ne férhessen hozzá. Az alkalmazás első használata előtt be kell állítani ezt a jelszót. Ez a jelszó egyénileg megválasztható. Az alkalmazás használata előtt továbbá még be kell azt regisztrálni az adott bankfiókhoz melynek ügyfelei vagyunk. Ezzel tulajdonképpen megadjuk, hogy az adott bank online rendszerében ezzel az alkalmazással szeretnénk azonosítani magunkat.

A virtuális chipkártya alkalmazással (ViCA) a mobiltelefonon, táblagép egy személyes hitelesítési eszközzé válik. Az alkalmazás segítségével az Electra Internet Bankig rendszerben generált csomagokat tudja az aláírásra jogosult személy távolról hitelesíteni. Ez egy zárt kommunikációs protokoll, mert a kulcs nem kerül ki az alkalmazásból.

QR kód

A QR kódot 1994-ben a Toyota egyik leányvállalata a Denso Wave fejlesztette ki. A QR kódot a többi kétdimenziós kód közül a számos támogatott adatformátum és a nagyon jó hibatűrés emelte ki. 1999-ben Japánban szabványosították és nemzetközi ISO szabványt is kapott 2000-ben. Ez által gyors terjedésnek indult ám valódi áttörést nem értek el vele. (Azonban Japánban, Németországban már évek óta használják a tömegközlekedésben, világszerte koncert vagy repülő jegyeken, és leggyakrabban különféle nyeremény, és marketing kampányok részeként.) 2010-ben megbukottnak látszódott a QR kód története, ám 2011-ben egy új ötlet „megmentette” merült fel, ami nem más, mint a mobilfizetés.

QR kódot le kell fényképezni, és a képet processzorral kell értelmezni. A processzor az összes QR kódban lévő három nagy és egy kicsi pontot keresi és értelmezi, ezek alapján küszöböli kép a méret, elforgatás, torzításból adódó eltéréseket.

A gyakorlatban használt QR kódok általában Version 3 vagy Version 4 típusúak, tehát 29-33 kis kocka méretűek széltében és hosszában.

QR kódos fizetés

Korszerű

- okos telefonnal való fizetés
- marketing lehetőségek

Egyszerű

- nincs hibalehetőség
- egy lépésből álló fizetés

Gyors

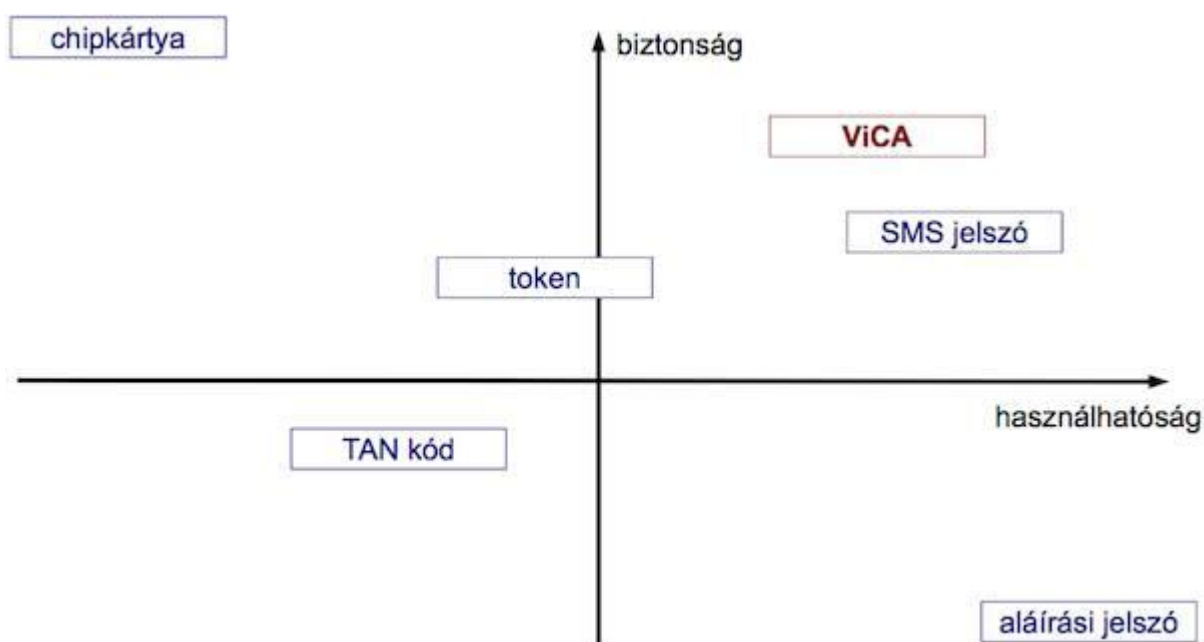
- a kód leolvasása pár pillanat
- PayPasshoz hasonlóan azonnali fizetés

Biometrikus azonosítás

Az ország nem elterjedt, így keveset tudunk róla. Németországban az online felületet használók közül is csak 15,6%-a támogatja. Előnye, hogy nem lehet eltulajdonítani, hátránya, hogy előítéletek vannak vele szemben, ezért kevésbé használatos. Egyes rendszerek könnyen átverhetők, illetve csatlakoztatást és telepítést is igényel.

	Chipkártya	ViCA
Fizikai eszköz	Plasztikkártya	Okostelefon
Hozzáférés	PIN-kód	ViCA jelszó
Funkciók	Bejelentkezés és aláírás	Bejelentkezés, aláírás és biztonságos üzenetküldés
Aláírás	RSA kulcspár	RSA kulcspár
Bejelentkezés	RSA kulcspár	RSA kulcspár
Üzenetek kezelése	-	ViCA jelszóval védve
Hozzáférés a privát kulcshoz	Hardveres védelem	Online, banki szerver védelem
Hordozhatóság	Csatlakoztatni kell a számítógéphez, meghajtókat kell telepíteni	Mobil, független eszköz
Költségek	Fizikai eszközöket (kártyaolvasó, kártya) kell vásárolni	A ViCA alkalmazás ingyenes

9.ábra: Chip kártya és ViCA virtuális kártyák összehasonlítása



10.ábra: Tranzakciós azonosítások

Az Electra Internet Banking az Electra online felhasználói felülete, mely lehetővé teszi az Electra szolgáltatásainak webes elérését a nap 24 órájában. A felhasználók egy szimpla böngészőprogram segítségével intézhetik ügyeiket, kapcsolatba léphetnek bankjukkal, információkat kérhetnek. A biztonsági rendszerek széles köre nem csak az ügyfeleket, és adataikat védik, hanem garantálják a tranzakciók hiba mentes, és egyszeri lebonyolítását. A megoldás széles körben alkalmazott a legtöbb magyarországi bankban, mely biztosítja, hogy a fejlesztőcsoport mindig naprakész az interneten felbukkanó újabb támadások és hibák elhárítása érdekében.

Az Electra Internet Banking a bankok összes ügyfélszegmensének ajánlott. Pl. a magánszemélyeknek akik többnyire csak információkérésre, és néhány megbízás beküldésére használják a rendszert, kis-, és középes vállalatoknak, vagy nagyvállalatoknak az Electra ügyfélprogram kiegészítő szolgáltatásaként.

Internet Banking felületen keresztül a bank bármilyen szolgáltatást vagy terméket elérhetővé tud tenni. A megkezdett műveleteket értesítők segítségével nyomon lehet követni, vagy akár PDF formában le lehet kérni a számlakivonatokat is.

Az Electra Internet Banking együttműködik az ügyfélprogrammal, és a Mobil Bankinggal egyaránt.

10. FOLYAMATOS FEJLŐDÉS

A GfK Hungária piackutató intézet felméréséből megtudhatjuk, hogy valaki online banki szolgáltatások igénybevétele után, gyakori felhasználóvá válik. Míg a lakosság nagy része havonta maximum egy alkalommal megy bankba ügyeket intézni, addig, egy online felhasználó átlagosan több, mint 5 alkalommal veszi igénybe a szolgáltatást.

A felmérésből megállapítható, hogy a szolgáltatások igénybevétele nagyban függ a felhasználó korától, valamint társadalmi státuszától.

- A felsőfokú végzettségűek körében minden 4 ügyfél online felhasználó
- Életkor alapján a 15-29 évesek a legaktívabbak
- A férfiak 20%, a nők 14% online felhasználó

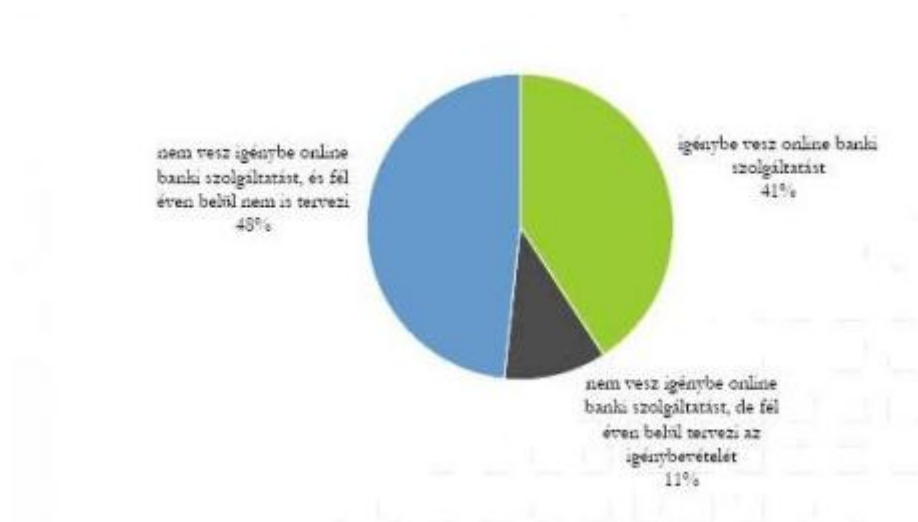
A növekedés a szélessávú internet hozzáféréseinek és terjedésének köszönhető. Az online banki csatornát a 28 tagállamból álló Európai Unión belüli ügyfelek több, mint 50%-a veszi igénybe, ez az arány azonban évről-évre dinamikusan növekszik.

A netbankokat azonban megfelelő tartalommal kell ellátni, ahhoz, hogy az ügyfeleket megnyerjék, és pozitív élmény legyen az online bankolás, a hagyományos banki szolgáltatásokkal szemben.

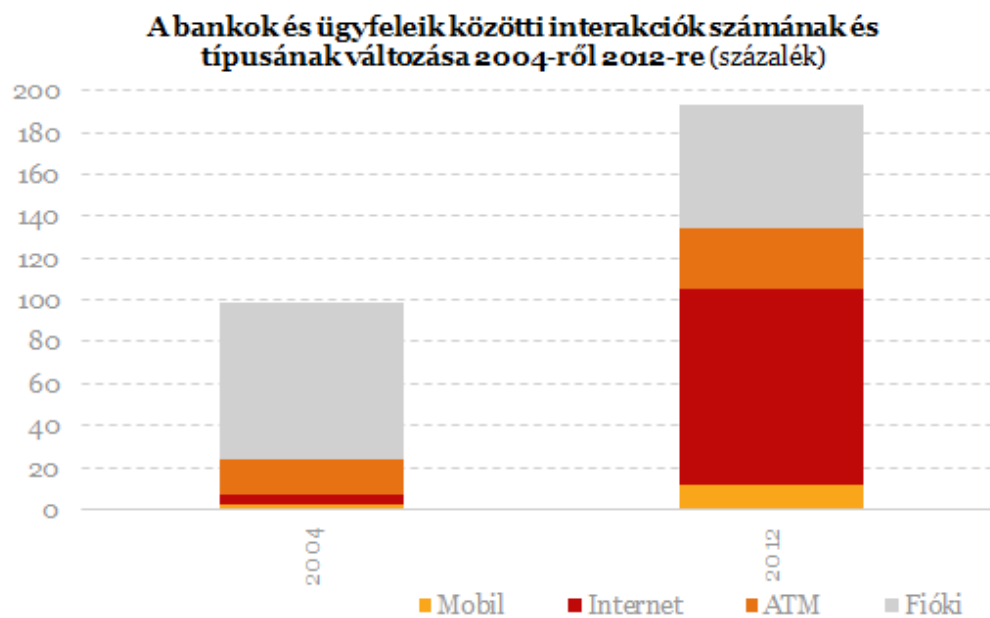
Egy amerikai kutatás szerint, a mostani 30 év alattiak, vagyis az Y-Generáció igényei fogják meghatározni a banki szolgáltatások jövőbeli alakulását. Ez a generáció, már a virtuális, közösség alapú pénzügyi tanácsadást részesíti előnyben a személyes bankolással szemben.

A Cisco felmérése szerint az 1980 és 1992 között született emberek négyszer többet tesznek pénzügyi észrevételeket blogokon, vagy online fórumokon. Emellett nekik jelent nagy előnyt, a mobil platformon nyújtható, személyre szabható tanácsadási rendszer, valamint a video ügyfélszolgálati rendszer, mely a jövő nagy lehetősége.

Kezdetekben az ügyfelek a bankfiókokból videón kommunikálnak majd a központban dolgozó pénzügyi szakértőkkel, később pedig a technológia az ügyfelek saját számítógépéről vagy mobil eszközről is elérhetővé tehető.

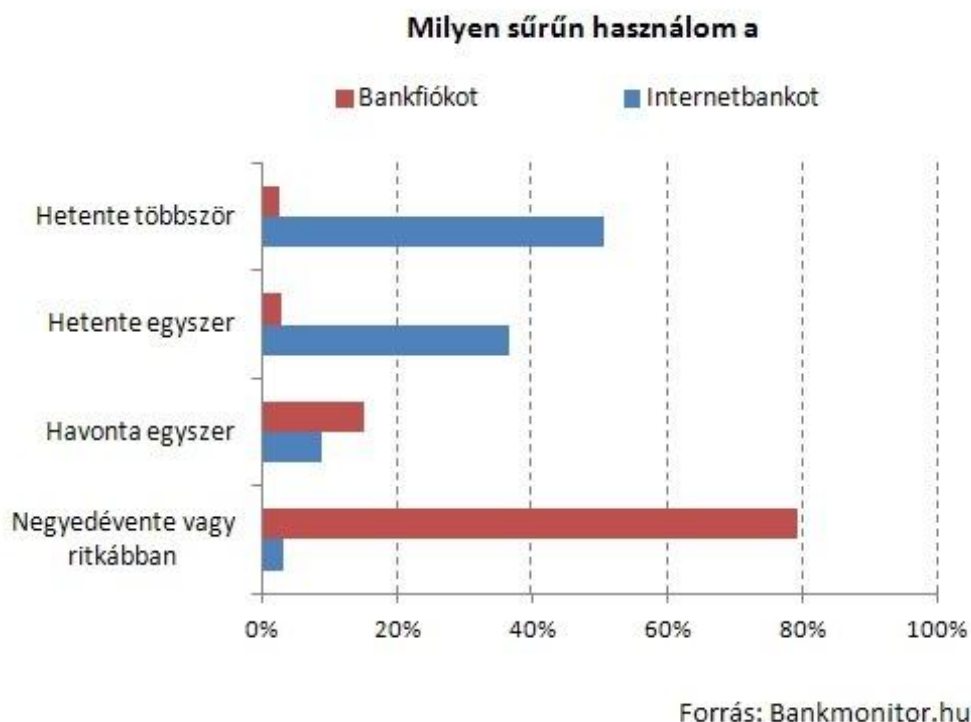


6. ábra: Online bankolást használókat bemutató diagramm



Forrás: BCG, Portfolio.hu

7. ábra: A szolgáltatások változása 2004 és 2012 között. A 2004-ben a banki szolgáltatást választók aránya mára már az internet használók táborát erősíti. Az internet hozzáférés növekedésével, nőtt az internet és mobilbankolók száma.



8.ábra: Személyes és internetes ügyintézés használata időszakosan lebontva

Egyes források szerint a legnépszerűbb közösségi oldalon a Facebook-on is elérhetővé szeretnék tenni, az online bankok legnépszerűbb szolgáltatását az átutalásokat. A 3.0 bankként is emlegetett rendszerben, online banki szolgáltatások egyesülnének a népszerű digitális platformokkal, mint pl. a Facebook.

Ezzel elsősorban a mai 20-30 év közötti embereket szeretnék elérni. Az újítás révén az ügyfelek nem call-centerből, vagy internetbankból utalnának, hanem a Facebookról, okos telefon alkalmazás segítségével. Az utalás egyetlen feltétele, hogy az utaló és a fogadó fél is használja az alkalmazást.

Ez a rendszer tesztkörnyezetben már bizonyított: a tavalyi évben, május 29-én az Alior Sync rendszerében megtörtént az első átutalás a Facebookon keresztül, ezután pedig az Alior Sync ügyfelei már élesben is használhatják.

Közösségi bankolás is a folyamatos fejlődés része (lesz). Hogy mit is jelent ez? Közösségi vagyis fenntartható bankként odafigyelünk a befektetéseinkkel, hiteleinkkel kapcsolatos társadalmi, és környezeti hatásokra. A cél az, hogy az ügyfelek közreműködésével, felelős és átlátható módon, választási lehetőségek révén forrást biztosítsanak olyan kezdeményezések számára, amely pozitívan hatnak pénzügyi helyzetünkre. A legfontosabb különbség a hagyományos bankolással szemben, hogy átláthatóbb, személyre szabhatóbb.

Egy kis személyes véleményt is fűznék a választott témámhoz. Kedvenc és legnépszerűbb hárombetűs bankunk, melynek rendszeres ügyfele vagyok én is nemrég új image-et vagy ahogy mostanában mondani szokás, imázst kapott, az OTP Direkt szlogennel. A fogalom a házibank, telebank és egy elektronikus számlacsomag együttesét tartalmazza. A dolog lényege, hogy az ügyfél közvetlenül, gyorsan, elektronikus módon tudja a bankügyeit intézni. Az ügyfelek számára azonban gyorsan kiderült, hogy a valóság némileg eltér a prospektus szövegétől. Ha már OTP... Az OTP Smartbank szolgáltatás okos telefonokra letölthető alkalmazás, melynek segítségével egyszerűen hozzá lehet juthatni a számlákkal kapcsolatos információkhoz és pénzmozgással járó tranzakciókat is lehet indítani. Ma már mintegy 2,7 millió okos telefon van Magyarországon, és egyre inkább az elektronikus csatornákra terelődik banki ügyintézés, így kézenfekvőnek tűnt az ilyen készülékekre telepíthető internetbanki alkalmazások bevezetése. Ez további előnyt és megtakarítást jelenthet a kisvállalkozások számára, hiszen az online ügyintézés még rugalmasabbá válik, mivel az már nem kötődik kizárólag a számítógéphez.

Az hogy miért is az OTP-ét hoztam fel példának... nos mint már említettem e bank ügyfele vagyok én is, illetve jelenleg a legtöbb újítással Magyarországon ez a bank kecsegtet, és az egyik leggyorsabban fejlődő is.

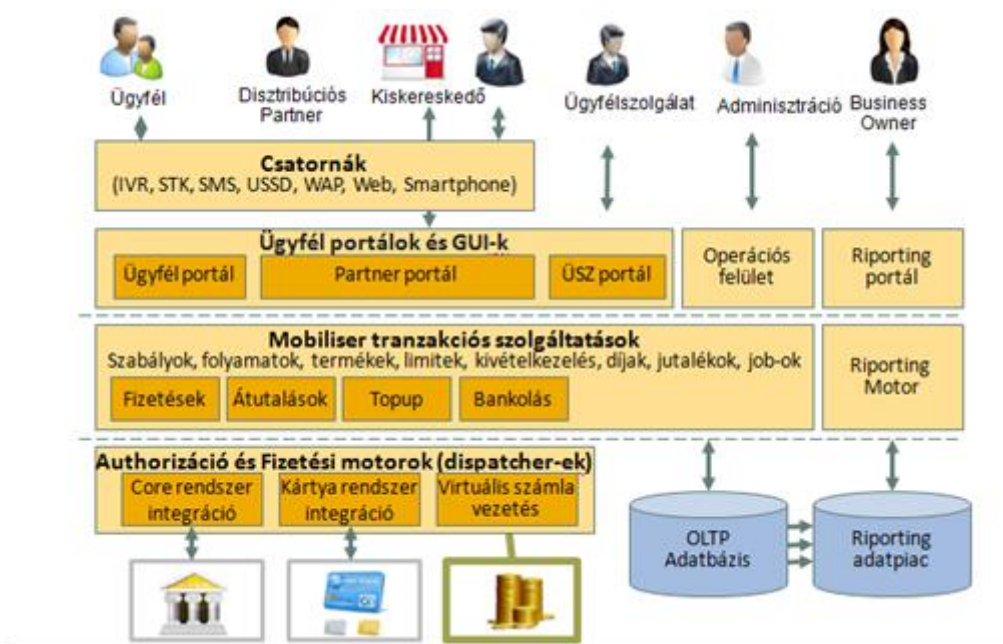
Manapság a bankkártyákat lassan a luxuscikkek közé sorolhatjuk, mert egy komolyabb kártya (pl. Visa Classic) havi költsége nagyban függ attól, hogy milyen gyakran vásárol, vesz fel pénzt és milyen egyéb szolgáltatásokat használ a kártya birtokosa.

Napjainkban a bankok folyamatos versengésbe állnak egymással. Céljuk hogy ügyfeleik számára a lehető legmegbízhatóbb, könnyen áttekinthető, kényelmes, vizuális eléréseket biztosítsanak. Ehhez különböző ügyfélcsatornákat használnak, ez akár legyen szociális médiáról, vagy bármely közös eszközről is, a bankok fontos célterülete. Ezen csatornán különböző folyamatokat hajtanak végre az eltérő kereskedelmi bankok. Első sorban mint azt ahogy már jó néhányszor hangoztattam a fióki ügyfélszolgálat szerepe a legmeghatározóbb, de az infrastruktúrát, és IT technikát tekintve ez csökkeni látszik. Ami azonban ezzel ellentétes irányba fejlődik az internet és mobil térhódítás pénzügyi tranzakciók során. Ny-Európában, már az okos telefonos mobil bankolás ugrásszerűen megnövekedett, hazánkba a bankok is még ismerkednek vele inkább, próbálgatják, felméri a lehetséges igényeket e területen, de mindenestre jól látható mennyire nő a fontossága és az ebbe fektetett tőke is gyarapodik. Teljesen más módon történik az ügyfelekkel való kommunikáció, elsősorban interaktív, sokkal kidolgozottabb igényesebb. Mindenféle újítással olykor játékosággal próbálják a piaci szerepben való növekedést inspirálni a bankok egy-egy ilyen újítással. Törekednek, hogy figyelemfelkeltő megközelítéssel nyerjenek teret az elképzeléseiknek. Természetes nem csak a felhasználó kör minél tágasabb kiépítés áll csak a háttérben, önös érdekeit mellett szól, hogy költségmegtakarítási célok is vezérlik, hisz a bankok a papírmunkáikat, adminisztratív feladataikat csökkentik. Kezdeti IT beruházással, a későbbi költségek csökkenthetőek. A GPS, a fényképezőgép segítségével különböző csalások ellen tudunk felkészülni, illetve megelőzni azokat. Vagy is az okos eszközöket kiegészítő lehetőségeket teremt a bankok számára, hiszen ezekre új szolgáltatásokat tudnak kialakítani, amivel ők is értéket adnak, ezzel is az ügyfelek kötődését növelni az adott bankkal szemben. Bár félelemmel fordul a nép az online felületekhez, még is átlagba véve biztonságos rendszerekről beszélünk akár online akár mobil bankolás során. Ami ide vágó technikai malőr, mely a biztonsági feltételeknek megfelelő azok SAP megoldásokban a rendelkezésünkre állnak. Különböző hűségprogramokon keresztül nyilvánul meg az SAP, mely a bankok számára szólítja meg az ügyfeleket. Az SAP megoldás az új generációs mobilbanki folyamatok támogatására. Ez a mobil újítás egyben online banki megoldást is jelent, ami az okos telefonról való elérést is biztosítja. Az alkalmazás a Sybase nevű amerikai technológiai cég felvásárlásával, teljes körű integrációjával jött létre az SAP-nál.

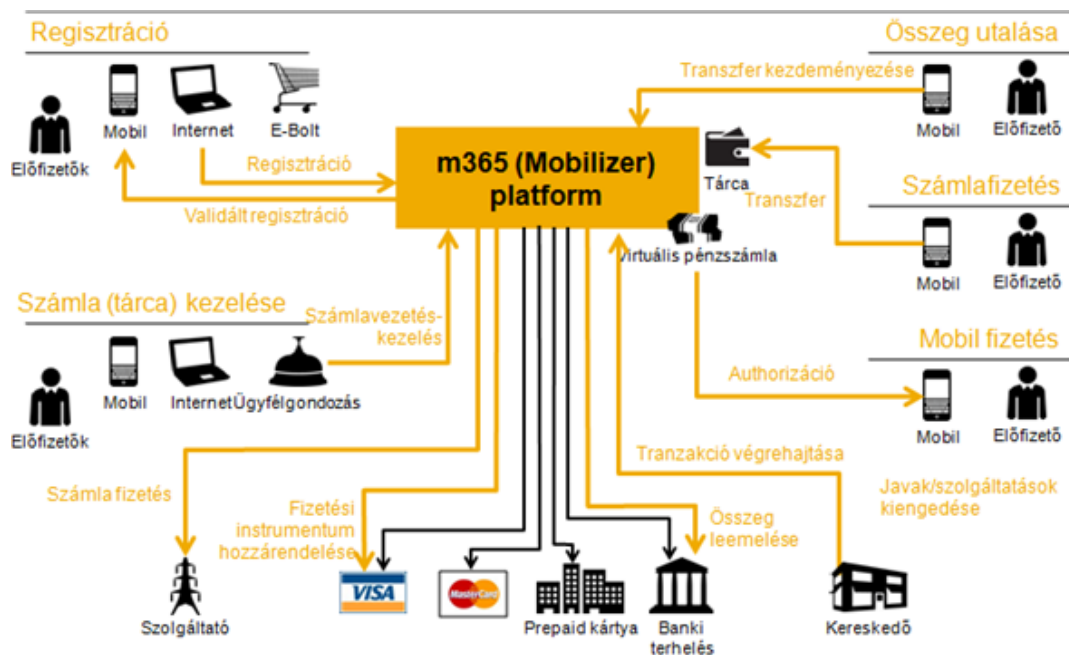
Az SAP M365 különféle dolgokat biztosít a fizetési tranzakciók végrehajtásához, mint például az ügyfél-figyelem felkeltésétől kezdve, robosztus, megbízható, autentikált, verifikált platformokat. Az ezen belül található fejlett reporting üzleti intelligencia modul az

lehetővé teszi az ügyfelekkel történő teljes körű átlátást, mely megelőlegezi a további ügyfélkapcsolat erősítő intézkedések kialakulását. A változás, ennek az alkalmazásának az eredménye a teljes költség (TCO) csökkenésében mutatkozik meg leginkább, s ez a költségváltozás egészen kiterjed a mobil bankolásra is, például az okos telefonok operációsrendszerére is hatékonyan kiterjeszthető. Egyszóval e megoldás során integráljuk az elektronikus banki rendszerünket integráljuk az SAP ügyviteli rendszerébe. Vagyis az ügyfél az ügyviteli szoftverből közvetlenül tudja a kivonatokat letölteni, a megbízásokat elvégezni. Az ügyfélprogram háttérbe kommunikál az SAP-val, azaz ennek segítségével ellenőrzi az utasításokat és jogosultságokat. A tranzakciók során elvégzett fizetési forgalom teljes folyamatai nyomon követhetők az SAP rendszerben. Mint már említettem igen magas működési költségeket lehet vele megtakarítani. Növeli az informatikai biztonságot.

Az SAP mobil megoldásainak motorja a Mobilizer elnevezésű tranzakció szolgáltatási platform, ami az M365 szerves része. Ez végzi el például a befizetési instrukciókat, továbbá végrehajtja az átutalásokat a meghatározott szabályok, előírások betartásával.



9.ábra: Mobilizer platform, és a tranzakcióban résztvevők, valamint a szereplők munkakörei



10.ábra: Tranzakció lebonyolítása M365-tel

Az SAP M35 megoldása globális szinten igen terjedőben van a piacon. Elérhető már a piacon a HANA legújabb támogatási csomagja, mely tovább támogatja az üzleti tranzakciókat és analitikai alkalmazásokat.

Egy kis példa szociális médián keresztüli integrációra az SAP, M365 segítségével. Ez már egy működő képes megoldás internetes banki szolgáltatásokra, illetve mobil alkalmazásokra ráépülve a bankok egy részénél. Ez például lehetővé teszi az ügyfelek számára a Facebook nevezetű közösségi oldalon lévő ismerős listáján keresztüli küldést, ez egy Facebook Connect Api használata a Facebook és az M365 applikáció között. Ez azért is előnyös, mert nincs szükség semmiféle adatmegadáshoz a tranzakció elvégzéséhez.

11. JÖVŐKÉP

Hogy mit is hoz a jövő? Várható trendek a jövő e-banking rendszereit tekintve: a funkcióinak bővülése; intuitív, könnyen használható felületek fejlődése; biztonsági megoldások továbbfejlesztése; költséghatékonyság.

A jövő online fizetési rendszerét egyértelműen a különböző okos telefon alkalmazások, az NFC chippel ellátott okos telefonokkal való fizetés, valamint a napjainkban debütáló újjlenyomat azonosítóval kombinált, token alapú tranzakció, az Apple Pay fogja meghatározni melyek egyre inkább kiszorítják a készpénz és a (hagyományos) bankkártyák mindennapi használatát. Emellett a Prepaid kártyák terjedése is jelentősen felgyorsul a közeljövőben.

11.1 NFC

NFC (Near Field Communication) melyről már említettem pár szót, egy rövid hatótávú kommunikációs szabványgyűjtemény okos eszközök között. Egymáshoz érintéssel, vagy maximum pár centiméteren belül elhelyezkedő eszközök között létrejövő rádiós kommunikáció. Alkalmazási területe a bonyolultabb, vagy magasabb szintű kapcsolatok gyorsítása, vagy az eszközök közötti azonosítási folyamat gyorsítása.

Szerencsére egyre több NFC képes terminállal találkozhatunk. Ezeknél érintkezés nélkül tudunk fizetni, bármilyen operációs rendszert támogató okos eszközökkel. NFC-vel való fizetés során, az azonosításhoz használt kódokat vagy újjlenyomatot egy úgy nevezett SE lapka hitelesít, ami ez után továbbítja az adatokat az NFC-s modemnek. Az SE lapka biztosítja a mobilfizetési tranzakciók védelmét, abban az esetben ha szoftveres vagy hardveres támadás érkezik a készülékek ellen. Az SE lapka biztonsági megoldása miatt, a SIM-ről vagy a telefonból akkor se lehet kinyerni az adatokat, ha valaki fizikailag hozzáfér.

A MasterCard célja 2020-ra alapvető szabvánnyá tenni, az egy érintéses fizetési rendszert a PayPass-t.

11.2 OKOS TELEFON ALKALMAZÁSOK

Az egész világon rohamosan terjedt az elmúlt 4 évben a különböző okos telefonos fizetési megoldások és különféle alkalmazások, melyek ezután még gyorsabban terjednek, mint valaha. Szerencsére nem csak a köznyelvben a mobil pénztárcával azonosított - egyébként a mobil fizetésnél jóval szélesebb felhasználási területtel bíró - NFC-technológia az egyetlen módja a mobil vásárlásnak, így azoknak is jut megoldás, akik nem rendelkeznek NFC chipes mobil készülékkel.

Pár évvel ezelőtt még ritka volt az olyan szolgáltatás, vagy alkalmazás amivel bárhol bármikor elintézhettük a bankügyeinket. Az okos eszközök megjelenése és roppant gyors terjedésével azonban különböző alkalmazások, szolgáltatások és megoldások jelentek meg. Ezek persze bankonként nagyon eltérőek lehetnek. Egyes pénzintézetek a mobil alkalmazásokat részesítik előnybe, mások a mobilböngészőben is futtatható programokat.

A bankoknál elérhető mobil alkalmazások főbb funkciói								
Újgenerációs funkciók	AXA	Erste	OTP ¹	Citi	K&H	MagNet	Raiff.	Sberb.
Pénzküldés telefonszámra	✓	✓	35% ²					
Internetes fizetés	✗	✗	✓					
QR kódos fizetés	✗	✗	✓					
Csekkbefizetés	✗	✓	✗					
Klasszikus netbanki funkciók	AXA	Erste	OTP ¹	Citi	K&H	MagNet	Raiff.	Sberb.
Számlainfo	✓	✗	✓	✓	✓	✓	✓	✓
Átutalás	✓	✗	✓	✓	✓	✗	✓	✓
Bankkártya műveletek	✓	✗	✓	✓	✓	✗	✗	✗
Megtakarítás	✓ ³	✗	✓	✓	✗	✗	✓	✗
Fiók és ATM kereső	✗	✗	✓	✓	✓	✗	✓	✓

1., A táblázatban a bank két eltérő szolgáltatását (az új generációs funkciókkal rendelkező OTPay, valamint a klasszikus netbanki funkciókat ellátó Smartbank) mutatjuk be.

2., Kizárólag az OTP Bank ügyfelei között lehetséges.

3., A funkció novembertől lesz elérhető az alkalmazásban.

Számlainfo - Számlaegyenleg, részletes számlainformációk megtekintése;

Átutalás - Saját számlák között, bankon belül, más belföldi bankba;

Bankkártya műveletek - Limitmódosítás, bankkártya aktiválás;

Megtakarítás - Betétlekötés, felmondás;

Forrás: Bankmonitor.hu
2014.10.15

11. ábra: A bankoknál elérhető mobil alkalmazások főbb funkciói

Bank	Főbb funkciók
AXA Bank	• Számlaegyenleg és részletes számlainformációk megtekintése • Átutalások (bankszámlára és telefonszámra) • Bankkártyához tartozó limitek módosítása • Üzenetváltás az ügyfélszolgálattal
Citibank	• Számlaegyenleg és részletes számlainformációk megtekintése • Átutalások (saját számlák között, bankon belül, más belföldi bankba) • Bankkártya aktiválás • Betét lekötések • Fiók és ATM kereső • Akciók, ajánlatok megtekintése
Erste Bank	• Pénzküldés telefonszámra • Csekkbefizetés (az adatok rögzítése a csekk beolvasásával) • Mobilfeltöltés • Az alkalmazásban végzett tranzakciók lekérdezése
K&H Bank	• Számlainformációk lekérdezése (számlaegyenleg, számlatörténet) • Forint- és devizautalások • Bankkártya műveletek (kártyák lekérdezése, limitmódosítás) • Megbízások lekérdezése, értéknapos átutalások törlése • Fiók, ATM és széfkereső • Banki kapcsolati adatok, elérhetőségek
MagNet Bank	• Számlaegyenleg, lekötött betétek megtekintése
OTP Bank	• Számlaegyenleg és részletes számlainformációk megtekintése • Átutalások (saját számlák között, bankon belül, más belföldi bankba) • Csekkbefizetés (az adatok rögzítése a csekk beolvasásával) • Távszámla, Díjnet számlafizetés • Bankkártya műveletek (kártya aktiválás, letiltás, limitmódosítás) • Betétlekötés, felmondás • Mobilfeltöltés • Hangvezérlés • Pénzküldés telefonszámra* • Internetes fizetés* • QR kódos fizetés*
Raiffeisen Bank	• Számlaegyenleg és részletes számlainformációk megtekintése • Átutalások (saját számlák között, bankon belül, más belföldi bankba) • Devizaváltás, devizaárfolyamok • Betétlekötés, felmondás • Fiók-, ATM- és OneCard kedvezményadó üzletkereső • Kapcsolat a bankkal (e-mail küldés, ügyfélszolgálat felhívása, stb.) • Hírek
Sberbank	• Számlatörténet lekérdezése • Forint- és devizautalások • Deviza és valuta árfolyamok • Bankfiók- és ATM-kereső • Kapcsolat a bankkal (e-mail küldés, ügyfélszolgálat felhívása, stb.) • Hírek

* Ezek a funkciók kizárólag az OTPay szolgáltatás keretében elérhetők.

12.ábra: Magyarország Top 8 bankjának elérhető mobil funkciói

Pár statisztikai adat az európai mobilfizetési alkalmazásokról, és használatukról

- Az európai okos telefonhasználók több, mint 50%-a már letöltött valamilyen vásárlási applikációt
- A megkérdezettek 56%-a rendszeresen is használja a letöltött applikációkat
- A megkérdezett európaiak 38%-a tervezi, hogy hamarosan fog applikáción keresztül vásárolni

De milyen alkalmazásokat használunk?

- A legnépszerűbb alkalmazások, a különböző vásárlási applikációk
- Őket követi, azok az applikációk, melyekkel képesek a felhasználók mobiltelefon-egyenleget feltölteni, vagy médiatartalmakat is képesek letölteni
- A következő évek slágere azok az alkalmazások lesznek, melyekkel akár színház, mozijegyet, vagy bármiféle divat és szépségápolási cikket tudunk venni/rendelni

A biztonság továbbra is a legfőbb szempont, ám a kutatásból kiderül, ha a fogyasztó az applikációk használatával képes pénzt megtakarítani, vagy leegyszerűsíthető a vásárlás folyamata, akkor még gyakrabban fogják használni az alkalmazásokat.

Magyar Telekom: MobilTárca

A Magyar Telekom hozta létre Magyarország első mobilfizetési megoldását a MobilTárcát. A MobilTárca egy olyan szolgáltatás, amibe egy virtuális MasterCard PayPass bankkártyát integráltak egy NFC chippel ellátott okos telefonba, olyan extrákkal mint a hűségkártya, vagy különböző pontgyűjtők. Ez a megoldás kizárólag Telekom ügyfelek számára érhető el, és mivel virtuális PayPass kártyát jelenleg csak és kizárólag az OTP hoz forgalomba, ezért a potenciális felhasználók köre meglehetősen kevés. Továbbá jelenleg csak Android rendszeren működik a szolgáltatás.

Pár trükkel azonban elérhetővé válhat más felhasználók számára is. A mobiltárcás fizetési szolgáltatások ugyanis olyan szabványokkal működnek, melyeket az összes NFC-vel ellátott készülékek tudják (ez alól természetesen kivételt képeznek az Apple iPhone-ok, hiszen ott az NFC chip, kizárólag az Apple Pay funkcióra használható). A kezdeti beállításokhoz szükséges alkalmazást azonban a Telekom nem fejlesztette le ezekre a rendszerekre.

A Telekom megoldásának egyik legfontosabb nélkülözhetetlen eleme, egy átlagon felüli titkosítással ellátott SIM. Ez tárol minden kártyaadatot, a tranzakciók során csupán átadja a

kártyaazonosítót az NFC chipnek, melyet majd a terminál ki tud olvasni. Így akár kikapcsolt telefon sincs befolyással a működésére. És ez jelenti a kiskaput a többi felhasználó számára. Hiszen a szolgáltatást bárki igényelheti, így a titkosított SIM kézbesítése után elég egy MobilTárca applikációval kompatibilis Andoridot futtató készülékben felkonfigurálni. Ez után elég egy BlackBerry, vagy Windows Phone mobilba berakni, és máris használható.

11.3 PREPAID KÁRTYÁK

Prepaid kártya más szóval előrefizetett kártya A kártya lényege, hogy a kártyát előre töltjük fel egy bizonyos összeggel, így válik használhatóvá a kártya. A későbbiekben újra fel lehet tölteni. Az előre kifizetett összeg a kártyán vagy a kártyatulajdonos számláján tárolódik.

A MasterCard új európai felmérése szerint az előrefizetett, vagyis prepaid bankkártyák kiváló megoldást jelenthetnek azoknak, akik tudatosabban akarják beosztani a pénzüket. A MasterCard MasterPass márkajelzése, mely a PayPass (helyszíni) és a MasterCard Mobile alkalmazással bonyolított (távoli) fizetéseket egyesíti majd, Romániában és Lengyelországban már elindult, Magyarországon, Szlovákiában, Csehországban és Ausztriában előkészítés alatt áll vagy csak nagyon kezdetleges adatok vannak még az elterjedtségéről. A MasterCard ambíciói igen jelentősek a MasterPasst illetően, egyfajta "tárcák tárcája" lehetőségként tekint rá, hiszen helyi és globális megoldásokba is integrálható, sőt saját márkajelzéssel is felruházható.

A növekedés pilléreit a MasterCard továbbra is az innovációban látja, továbbá a diverzifikációban. Az innovációk eredményeképpen hordozható fizetőeszközök is megjelentek több célcsoportnak is.

Ilyen például a lengyelországi PEKA közlekedési kártya vagy a hazánkban is használatos Fesztiválkártya, mely tulajdonképpen teljesen megegyezik egy MasterCard PayPass bankkártya tulajdonságaival.

A prepaid bankkártya kitűnően alkalmas a készpénzforgalom kiváltására, az ott élő emberek bekapcsolására a pénzügyi rendszerbe, sőt a prepaid bankkártya egy jó lépés lehet a számlatörténet megszerzéséhez is, mely a hiteligénylések egyik fontos dokumentuma.

11.4 APPLE PAY

Az Apple szeptemberi bemutatója után 2014 őszén rajtol Amerikában (majd várhatóan 2015-ben Európában is) az új fizetési szolgáltatás az Apple Pay, mely lehetővé teszi a frissen bemutatott iPhone 6, iPhone 6 Plus és iWatch készülékekkel egyetlen érintéssel való fizetést a Visa, MasterCard és American Express elfogadóhelyeken.

11.4.1. APPLE PAY, A VILÁG LEGBIZTONSÁGOSABB FIZETÉSI MÓDSZERE

Az új lehetőség nagy kérdése, hogy jó ötlet-e az Apple-re bízni a bankkártya adatainkat. Ám a valóság az, hogy az Apple Pay egy rendkívül nagy biztonsággal ellátott mobilfizetési platform. Az Apple által is elérhetővé tett legújabb biztonsággal kapcsolatos dokumentum legalábbis erről árulkodik.

Az egyik legfontosabb, hogy sem az Apple szerverein, sem a készülékeken, sem pedig a kereskedő szerverein nem tárolódnak semmilyen bankkártya vagy hitelkártya adatok még titkosított formában sem.

Első lépésként regisztrálni kell a kártyát az Apple Pay rendszerben. (Ami lehet már az Apple iTunes alkalmazásában fizetésként használt kártya, vagy egy teljesen új is) A regisztráció után titkosított formában kerülnek tárolása az adatok kizárólag a kibocsájtó bank rendszerében.

A bank miután visszaigazolta a kártya érvényességét, egy token-t küld a készülék Secure Element rendszerébe, amely egy fizikailag jól elkülönített chip a készülékben. A későbbiekben ezt a biztonsági token-t használjuk a valós kártyaadatok helyett. Ez az úgy nevezett Device Account Number számsor.

11.4.2. APPLE PAY ÁLTAL HASZNÁLT BIZTONSÁGI TOKEN

Az Apple Pay által használt token önmagában egy véletlenszerűen generált, 16 számjegyből álló számsorozat, amely látszólag hasonlít egy valódi kártyaszámhoz, de önmagában ez a számsorozat teljes mértékig használhatatlan. A token tehát nem más, mint egy jegy vagy címke, amely a valódi kártyaadatokra mutat. Az egyetlen közös dolog, amiben megegyezik a token és a valódi bankkártya szám, az, az utolsó 4 számjegy. Ezt leszámítva teljesen eltérőek. Ezen túlmenően az Apple Pay által használt tokenek nem egy bizonyos matematikai szabály szerint generáltak, így nem lehetséges őket dekódolni sem, hiszen a titkosítás nem része az egyenletnek. Akár a legtehetségesebb hackereknek és kódfejtőknek is odaadhatnánk egy több millió darab tokenből álló listát, semmire sem tudnák használni azokat.

11.4.3. APPLE PAY TRANZAKCIÓK MŰKÖDÉSE

Amint elkezdődött a tranzakció, az iPhone elküldi a tokent a kereskedőnek, aki továbbítja azt az adott kártyának megfelelő bankhoz, ahol a token visszavezetődik az eredeti kártya adataihoz. Tehát a kártyát kibocsátó bank az a hely, ahol a token azonosítást kap és újra mellérendelődnek a valós kártyaadatok. Abban az esetben, ha a kártyával rendben van minden és a bank megerősíti, akkor egy üzenet formájában jelez a kereskedőnek, hogy a kártya rendben van és megkezdődhet a tranzakció.

Ez a folyamat valójában biztonságosabb, mint magának a hagyományos bankkártyának a használata, mivel ebben az esetben a kereskedő csak egy tokent kap és sosem rendelkezik a valós kártyaadatokkal.

Ezen módszerrel tehát az összes eddig bevett, a kártyaadatok ellopására kifejlesztett módszer idejétmúlttá válik, hiszen jelen esetben már nincs is mit ellopnia az illetőnek.

11.4.4. TOUCH ID ÉS KRIPTOGRAMOK

A szabályok értelmében azonban, hogy a token alapú tranzakciókat használhassunk elengedhetetlen egy személyi azonosítás is, melynek a tranzakció lezárulása előtt meg kell történni. Itt tovább egyszerűsödik a jelenleg is használt, PIN vagy egyéb jelszó használatával működő jelenlegi rendszerünk. Ahelyett ugyanis, hogy bármit megadnánk elég a Touch ID-ban regisztrált ujjlenyomatunkkal azonosítani magunkat. Ekkora azonban egy újabb biztonsági elem jelenik meg a rendszerben. Az Apple Pay funkcióval ellátott Apple termékek ugyanis minden tranzakció alkalmával küld egy dinamikus generált CVV számot piktogrammal együtt. A CVV normál esetben a napjainkban használt bankkártyák hátoldalán található utolsó 3 számjegyet jelöli, melyet minden internetes vásárlás esetén kötelező megadni. Itt azonban egy dinamikus számsor, mely közvetlenül a tokenhez kapcsolódik.

Ez a kriptogram tehát lényegében egy egyszer használatos digitális aláírás, mely azonosítja, hogy melyik készülékről érkezett az adott token. Ez a kriptogram tárolja, hogy melyik kereskedő milyen összeget vont le a kártyánkról.

A tokenek tehát nem használhatóak egy kísérő kriptogram nélkül, amely azt biztosítja, hogy az adott tokent csak az a készülék küldheti, amelyen eredetileg regisztrálva lett a kártya.

11.4.5. MIT JELENT MINDEZ A FELHASZNÁLÓKNAK?

Végül, de nem utolsó sorban elérkeztünk tehát a legfontosabb kérdéshez, azaz, hogy mit jelent mindez nekünk, a felhasználóknak? Bár az még kétséges, hogy a felhasználók milyen gyakran fogják használni az Apple Pay szolgáltatást, az viszont kétségtelen, hogy jelenleg az egyik legbiztonságosabb elektronikus fizetési formáról beszélhetünk. Egyrészt sem a kereskedő nem fér hozzá a tranzakció során a kártyaadatainkhoz, másrészt pedig kizárólag csak a mi készülékünk által küldött tokent kezeli a rendszer, így minden más készülékről indított fizetést kizár az Apple Pay a kriptogramnak köszönhetően. Egy esetleges készüléklopás esetén az iPhone felhasználók azonnal felfüggeszthetik vagy szüneteltethetik a készülékhez rendelt tokent, így az Apple Pay nem használható az eltulajdonított készülékekkel. Összességében tehát míg a felhasználói oldalról végtelenül egyszerű az Apple Pay használata, addig láthatjuk, hogy a felszín alatt jóval több minden történik, mint amire először gondolni mernénk.

11.4.6. APPLE PAY JELENLEGI HÁTRÁNYAI

1. A rendszer jelenlegi legnagyobb problémája, hogy csak a friss készülékek (iPhone6, iPhone 6 Plus és Apple Watch) támogatják a rendszert, mely kezdetben 10-15 millió embert érinthet. Ám erre megoldást jelenthetnek majd a korábbi Apple Watch kompatibilis modellek, hiszen hónapokon belül elérhetővé válik a frissítés.
2. A szakértők szerint az Apple Pay és az eddig megjelent online fizetési rendszerek olyan problémát próbálnak megoldani, ami nem is létezik. Vagyis mindenáron azt akarják elhitetni a felhasználókkal, hogy a készpénz és kártyák használata lassú, bonyolult és kényelmetlen.
3. Rendkívül kevés helyen használható a rendszer. A közel 6 millió szpotból csak 220 ezer elfogadóhellyel rajtolt a rendszer. Ráadásul sok neves partner nem teljes értékű támogatója a rendszernek, sokszor csak egyenleg feltöltésre alkalmasak fizetésre nem.
4. Az alábbi probléma miatt továbbra is kénytelenek vagyunk készpénzt és bankkártyát is hordani és használni, ami oda is vezethet, hogy inkább nem is bajlódik az ember az amúgy rendkívül egyszerű Apple Pay lehetőséggel.
5. Apple Pay sem sokkal gyorsabb mint a hagyományos kártyalehúzás
6. További hátrány, hogy a rendszer támogatóinak saját alkalmazását sokkal szélesebb körben tudjuk használni, akár régebbi iPhone készülékekről is.

SWOT ANALÍZIS

Az online bankolás belső tényezői és erőforrásai alapján, erősségek és gyengeségek felsorolása, valamint olyan külső tényezők melyek fenyegetést és veszélyt jelentenek a működésében és a jövőjét illetően. Az alábbi elemzéssel be szeretném mutatni az online bankolás legfőbb jellemzőit, a használatának erősségeit, mellyel szembe állítanám a gyengeségeit. Korábban említett technikai és a jövőben felmerülő lehetőségek megemlítése, illetve az ezekkel szemben fennálló veszélyek.

Erősségek • gyors • rugalmasság • költséghatékonyság • használatában nagyszámú létszám növekedés • magas szakértelem • személyre szabhatóság	Gyengeségek • személytelenné válik az ügyintézés • folyamatos internetkapcsolat szükségeltetik • rendszerhibák (pl. túlterheltség) • bizalom hiány
Lehetőségek • mobil bankolás • bankkártyák • NFC-s bankkártya/okos telefon • új fizetési lehetőségek (ujjlenyomat olvasós fizetés) • okos telefon alkalmazások	Veszélyek • külső támadások (pl. kémprogramok Zeus) • kéretlen e-mail • nem megfelelő programok használata • vírusok • a belépéshez szükséges azonosítók, és kódok elleni támadások

		Belső tényezők, erőforrások	
		Erősség	Gyengeség
Külső tényezők	Lehetőség	Az új lehetőségeknek köszönhetően egyre gyorsabbá válik az online tranzakciók elvégzése, ami sok pénzt spórol meg nekünk. Az új fizetési lehetőségek és az okos eszközök terjedésével pedig egyre népszerűbb a használata. A mobil bankolás megjelenésével egyre inkább személyre szabhatóbb az ügyintézés.	A fejlődő technika kihasználtságát nehezítik az esetlegesen előforduló rendszerhibák, illetve akadózó internet hozzáférés, valamint az okos eszközök alacsony akkumulátor üzemideje. Az ügyfelek még bizalmatlanok, hogy megpróbálkozzanak a számukra ismeretlen alkalmazások használatával.
	Veszély	Az erősségek eltompulnak a külső támadások végett, hiszen az ügyfelek bizalmatlanok. Az online bankok erőssége, hogy egyre felkészültebbek a programok a külső veszélyekkel szemben. Pl. Többcsatornás védelmi rendszerrel ellátott biztonsági csatornák használata.	A vírusok és kémprogramok növelik az ügyfelek bizalmatlanságát a rendszerrel szemben. Ezt a bizalmatlanságot használják ki a csalók. Az ügyfelek kezdeti félelme növeli a csalók támadási terét. Akik nem riadnak meg az újabb biztonsági rendszerektől, csupán egy újabb kihívás számukra.

ÖSSZEFOGLALÁS

Végül egy kis személyes véleménnyel zárnam.... Egyetemistaként az online bankolás a mindennapi élet részévé vált. Az órák rendszertelensége végett nem sok idő van elrohanni akár a legközelebbi bankba és kivárni a hosszú sorokat. Rengeteg minden elintézhető pár gombnyomással akár az ágyban ülve, két tétel tanulása között is. Az egyetem által kért különböző költségekért sem kell az intézmény pénztárához ellátogatni, elég csupán csak a bankkártyát kézbe venni, és az ETR oldal segítségével befizetni, ami tovább léptet a pénzügyek rendezése során az adott bank itt használt tranzakciójához, megkönnyítve nekünk, egyetemistáknak a dolgokat.

Továbbá rendszeres alkalmazója vagyok az OTP direkt online oldalának, ami rengeteg időt spórol nekem és természetesen pénzt is. Ennek köszönhetően gyorsabban tudok utalni, illetve ha éppen arra vagyok kíváncsi, hogy mennyi pénzből gazdálkodhatok a hó végéig, egy másodperc alatt meg tudom nézni, anélkül hogy ezért egy forintot is fizetnék, és a számlatörténetemet is nyomon követhetem, hogy mikor miért, és hol fizettem.

Egyszóval az online bankolás fokozatos terjedése nem csak a különböző vállalatoknak, vagy hétköznapi dolgozó személyeknek, hanem nekünk olyakor lusta egyetemistáknak is kedvez.

Az internet banking lendületes növekedésben van, és a tendenciák alapján ez az expanzió még évekig tartani fogja magát. A fejlődés megállíthatatlan a jövő mindenképpen az elektronikus bankolásé. Mi magunk csak arról dönthetünk szabadon, hogy mikor vesszük fel a kor ritmusát a bankszolgáltatások igénybe vételében is.

IRODALOMJEGYZÉK

1. A bankmonitor.hu által, a legnagyobb hazai bankok körében elérhető mobil alkalmazások 2014-es felmérése alapján. (11.2 fejezet)
2. Electronic Banking: The Ultimate Guide to Business and Technology of Online Banking 2001
3. Forbes magazin 2014. október (11.4 fejezet)
4. GfK Magyarország Piackutató Intézet felmérése alapján (9. fejezet)
5. HVG magazin „A Facebookon is utalhatunk majd pénzt” (9. fejezet)
6. Kevin Price Mueller Online Money Management 2001
7. Magyar Mobiltárca (11. fejezet)
8. Mahmod Shah & Steve Clarke E-banking Managment 2009
9. MasterCard 2014 áprilisa és júniusa között végzett, európai mobilfizetési alkalmazások használatáról szóló felmérése alapján (11. fejezet)
10. MasterCard 2014 áprilisa és júniusa között végzett, készpénzfizetést helyettesítő lehetőségek kutatásáról szóló felmérése alapján (11.fejezet)
11. Mohammad Ali Sarlak és Asghar Abolhasani Hastiani - Banking and Emerging Multidisciplinary Processes 2010
12. Professor Yamin Ahmad: Money and banking
13. Papp Emília: Virtuális bankolási trendek (HVG Hetilap) (10. fejezet)
14. RBI Bank: Report on Internet Banking
15. Ritwik Donde The Economic Times 2006 május. „Tipps to make online banking safe” (8. fejezet)
16. WSJ.D konferencia - Wall Street Journal főszerkesztője által készített interjú Tim Cookkal. (11. fejezet)