Személyes adataink védelme

Már Magyarországon is szinte mindenhol elérhető a szélessávú internet, legyen az ADSL, kábeltv vagy vezeték nélküli – legyen az mobiltelefonos vagy WIFI. Ez sok terhet levesz a felhasználó válláról, hiszen nem kell például egy átutalásért a bankba rohangálni. Viszont sokkal sebezhetőbbé váltunk.

Az ideális bank

Egy bank esetében nagyon fontos, hogy a tranzakciókról – legyen az akár ezer forint vagy akár több millió – csupán a küldő és a fogadó félnek legyen tudomása.

1. ábra Így néz ki egy Netlock tanúsítvány

Ennek megfelelően a bankok titkosított oldalakon (***https***) vagy saját titkosító programmal biztosítják a megbízható internetes banki ügyintézéseket. Persze ez ahhoz, hogy egy bank megbízható legyen, szüksége van ***hiteles tanúsítvány***ra. Ilyet ***Magyarország***on például a ***Netlock***, külföldön a ***Verisign*** adhat, de számos egyéb tanúsítvány kezelő cég van. A tanúsítvány egyfajta virtuális személyigazolványként is felfogható.

Phising

Phisingnek, vagy más néven ***adathalászat***nak hívják azt, amikor ***személyes*** – sokszor ***bizalmas*** – adatokat próbálnak ***megszerezni*** tőlünk.

Nyilvános és titkos kulcsok

A dolog lényege, hogy két ***kulcs*** van a rendszerben: egy ***privát*** és egy ***publikus***. A mechanizmus röviden úgy működik, hogy minden banki tranzakció esetén a bank publikus kulcsával titkosítja a böngésző a küldött csomagokat. Ezt a titkosított adatcsomagokat ezek után azonban már csak a bank tudja megnézni a privát kulccsal, éppen ezért az ilyen típusú titkosításnál a privát kulcsot titokban kell tartani, míg a publikus kulcs bárkinek kiadható. Vagyis nem igaz a következő egyenlet: adat + publikus kulcs - publikus kulcs = adat. A megoldás briliáns, noha nem feltörhetetlen. Megfelelő számítási kapacitással – ne tízezer gépes klaszterben gondolkodjon az Olvasó – fel lehet törni, de anyagilag egyelőre nem biztos, hogy megéri.

Kis kitérő: néha fel-felbukkannak hírek az úgynevezett ***kvantum számítógép***ekről, azonban ezek még a gyakorlatban nem használhatóak, viszont ha valaha is elkészülnek, nagyságrendekkel gyorsabbak lesznek a mostaniaknál. Tehát amihez most kell egy tízezer gépes klaszter, ahhoz a kvantumszámítógépek korában egy is bőven elég lesz. Ennek megfelelően a jelenleg használt kódolási megoldások is értéktelenné válhatnak. Persze ehhez elég sok víznek kell lefolynia a ***Dunán***.

Whois – Állj, ki vagy?!

www.budapestbank.net

```
domain:       budapestbank.net
owner:        Hugh Funderburg
email:        vrwerfverw41@yahoo.com
address:      12913 Melrose Rd
city:         Caledonia
state:        -
postal-code:  61011
country:      US
phone:        +815.8851429
admin-c:      CNET-626553 vrwerfverw41@yahoo.com
tech-c:       CNET-626553 vrwerfverw41@yahoo.com
billing-c:    CNET-626553 vrwerfverw41@yahoo.com
nserver:      ns1.willbe-one.com
```

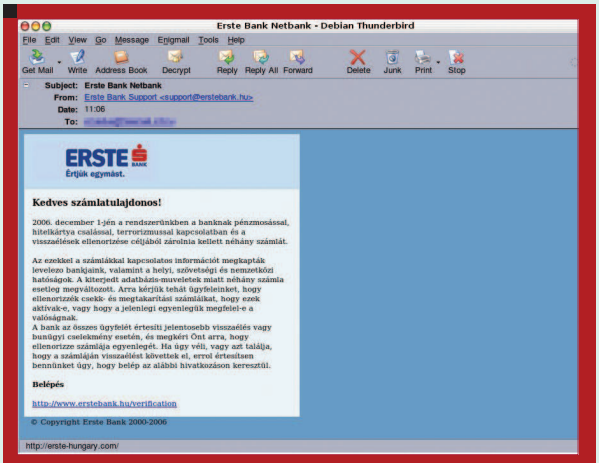
folytatás

```
nserver:        ns2.willbe-one.com
status:         hold,infringe-3rd-parties
created:        2006-11-30 22:07:00 UTC
modified:       2006-12-05 11:06:38 UTC
expires:        2007-11-30 22:07:00 UTC

contact-hdl:    CNET-626553
person:         Hugh Funderburg
email:          vrwerfverw41@yahoo.com
address:        12913 Melrose Rd
city:           Caledonia
state:          –
postal-code:    61011
country:        US
phone:          +815.8851429
```

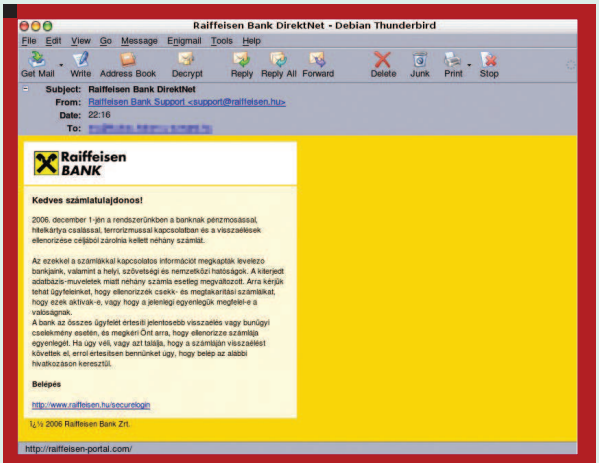
www.budapestbank.hu

```
domain:         budapestbank.hu
org:            org_name_eng: Budapest
                ➥Bank Co.
org:            org_name_hun: Budapest
                ➥Bank Rt.
address:        Váci út 188
address:        H-1138 Budapest
address:        HU
phone:          +36 1 4506000
fax-no:         +36 1 4506032
hun-id:         0990603035
admin-c:        2000243871
tech-c:         2000275450
zone-c:         2000275451
domain_pri_ns:  serval.bbrt.hu[195.56.141.43]
registered:     1999.06.03 20:22:53
changed:        2004.02.05 15:17:50
registrar:      1990930008

. . .
. . .
. . .

org:            org_name_eng: T-Online
                ➥Hungary Co.
org:            org_name_hun: T-Online Magyar
                ➥ország Zrt. (Registrar)
address:        Postafiók 204.
address:        H-1364 Budapest
address:        HU
phone:          +36 1 3713400
fax-no:         +36 1 3713405
hun-id:         1990930008
```

Mindkét lekérdezés 2006. december 7-én történt. Melyik hihetőbb?



2. ábra Hamis Erste Bankos e-mail



3. ábra Hamis Raiffeisen Bankos e-mail

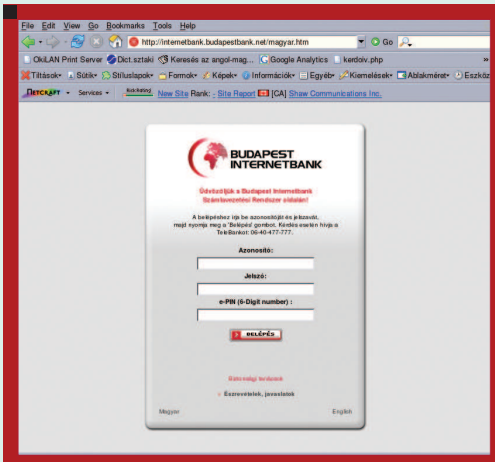
A ***phising*** célpontja leggyakrabban banki adat szokott lenni, de gyakran van példa más számra (például *IMEI*).

A sikeres ***phising*** azon áll vagy bukik, hogy a felhasználót sikerül-e meggyőzni, hogy ő most ténylegesen az adott oldalt nézi, és nem csak egy csali oldalt. Ezt legtöbbször a hasonló dizájnnal és tartománynévvel rendelkező oldal tudja elhitetni, de nem kell túl paranoiásnak lennünk, hogy ezt egyszerű eszközökkel kivédjük.

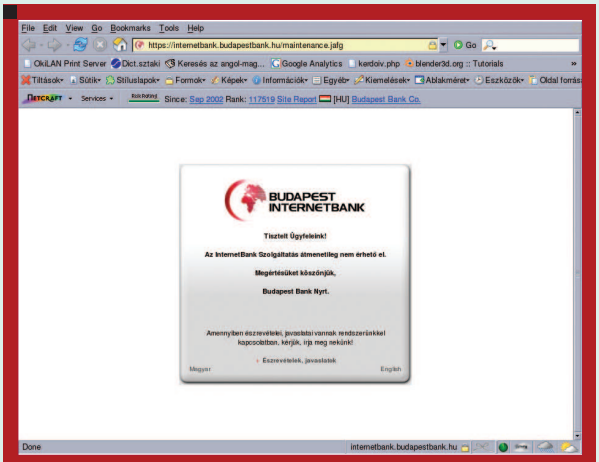
Hogyan védekezhetünk?

A ***phising*** ellen többféle védelem is létezik, de az alábbiakból minél többet alkalmazunk, annál nagyobb biztonságban érezhetjük magunkat. Persze teljes biztonság nincs.

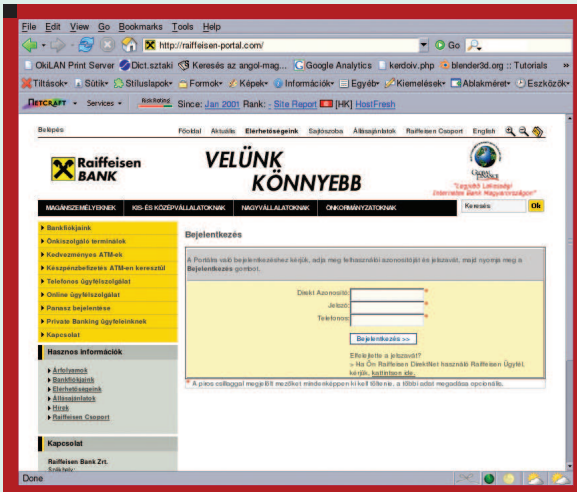
Az első és legfontosabb: ***jegyezzük*** meg fejből az online ***bankunk internet címét***, vagy legalábbis az elejét. Ezzel elkerülhető, hogy esetleg egy nem megfelelő oldalon adjuk ki adatainkat.



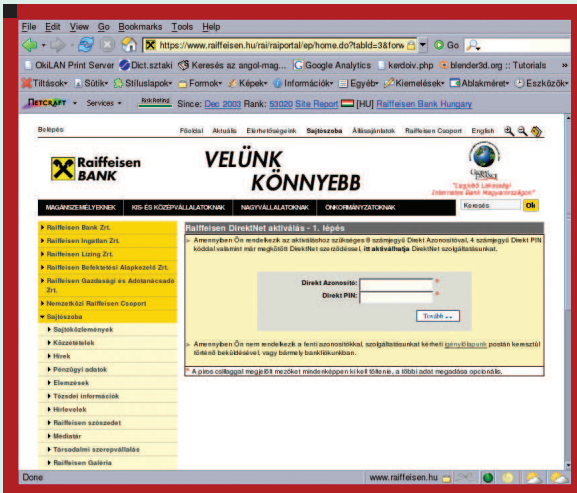
4. ábra A hamisított Budapest Bank nyitó oldal (2006.12.05.)



5. ábra Az igazi Budapest Bank nyitóoldala (2006.12.05.)



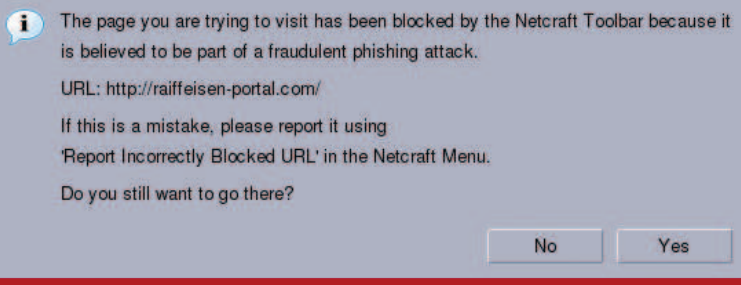
6. ábra Hamis Raiffeisen Bank nyitó oldal (2006.12.06.)



7. ábra Valós Raiffeisen Bank nyitó oldal (2006.12.06.)

A bank ***e-mailben*** és ***sms-ben nem kér adatokat***, illetve ***nem kéri***, hogy az e-mailben szereplő ***linkre kattintsunk***. Amennyiben ez történik, nézzük meg, hogy az e-mailben szereplő link milyen címre mutat. Fontos, hogy mire mutat és nem az, amit kiír. Ezt például ***Thunderbird***-ben úgy tudjuk megnézni, hogy a ***link fölé visszük az egeret*** és alul a ***státusz sorban*** megjelenik a hivatkozás. Ha a hivatkozás ***https*** helyett ***http***, akkor mindenképp gyanakodjunk.

E-mail esetén hasznos lehet az email forrásai is. Egész pontosan az utolsó ***Received from*** mező. Ritkán jön (értsd: ***soha***) magyar banki e-mail ***demon.nl***, ***ninja.com***, vagy ***wanadoo.fr*** tartományokból, mint ahogy az decemberben történt.
A banki weboldalakon ***nem kérik egyszerre*** az ***azonosítót***, a ***jelszót*** és a ***telebank kódját***. Ezzel is elég jól szűrhető az adathalászat, amennyiben nem rutinból töltjük ki a bejelentkezési ablakot.
Ha a bankunk támogatja, érdemes ***SMS értesítést kérni*** az online felületen végrehajtott ***műveletekről***, mint például a belépés, az átutalás kezdeményezése, illetve a jelszóváltás.
Ha nem is telepítünk minden frissítést, de legalább a ***titkosító könyvtárak frissítéseit***, illetve az online bankhoz használt ***böngésző frissítését*** tegyük meg.
Nyilvános helyen – például ***netkávézóban***, vagy más ***közös használatú gépen*** – ha lehet, ***mellőzzük*** az internetes ***banki ügyintézést***.



8. ábra Ha a Netcraft adatbázis már tud a csalásról, akkor az oldal megnyitása előtt jelez

9. ábra Egy 70 dolláros billentyűleütés figyelő (keylogger). Akár félmillió leütést is tárolhat.

A gépen bármi lehet, amely elárulja, mit csináltunk. Lehet akár egy ***trójai***, vagy egy ***keylogger*** (billentyűleütéseket megjegyző program), de akár ***külső keylogger*** is, amely a számítógép és a billentyűzet köze csatlakoztatható. Ugyanide tartozik: noha könnyedséget okoz, ***mégse mentsük le a jelszavakat*** a böngészőbe.

Gyakori hiba még, hogy ***nem titkosított VNC*** vagy ***rdesktop*** kapcsolaton keresztül jelentkezik be valaki. Ez a gyakorlatban talán nem akkora rizikó, de inkább legyünk elővigyázatosak. Ha egy e-mailben küldött banki weboldalra klikkelünk, mindenképp ***ellenőrizzük a tanúsítványt***. Ezzel például kideríthető, hogy valamelyik nagy tanúsítvány ***cég adta-e***, vagy csak egy ***saját készítésűvel*** van dolgunk...

Végül pedig, amennyiben módunkban áll, használjuk a ***Netcraft Toolbar***t. Igaz, hogy pár hasznos pixellel csökkenti a képernyőt, de oldalak böngészésénél olyan információkat ad, melyek segíthetnek leleplezni az adathalászokat. Minden oldallátogatás esetén ***kiad például egy zászlócskát*** annak megfelelően, hogy ***melyik országban*** van az adott szerver. Éppen ezért, ha egy ***magyar bankhoz kanadai***, vagy ***hongkongi zászlót ad be***, akkor mindenképp ***gyanakodnunk*** kell. Ha nem szeretnénk a ***Netcraft Toolbar***t használni, akkor ***gyanús domain esetén*** használjuk a ***whois*** parancsot.

A legegyszerűbb a végére: ha nem vagyunk biztosak a dolgunkban, ***hívjuk fel bátran a bank ügyfélszolgálatát***. Az ügyfélszolgálat telefonszáma leggyakrabban a bankkártyánk hátulján található.

2006 decemberében számos bank ügyfelét megpróbálták becsapni, azonban a saját bőrömön csupán három hamis banki email jutott el (időrendben: ***Budapest Bank***, ***Raiffeisen Bank***, illetve az ***Erste Bank***). Az ***Erste Bankról*** hamis változatáról azért nincs képernyő mentés, mert a hivatkozott oldal nem volt elérhető.

Jelenleg egyik fenti banknál sincs számlám. Ez azonban nem jelenti azt, hogy a jövőben nem fordulhat elő hasonló eset, hiszen akár a számlámat vezető bank is lehet a következő. Tehát vigyázzon a kedves Olvasó, az adathalászok már a spájzban vannak...

IMEI

Az ***IMEI*** szám a ***mobiltelefonok egyedi azonosítója*** – olyan mint a hálózati kártyáknál a ***MAC cím*** – amit azonban megfelelő programokkal módosíthat a felhasználó, azonban ez jelenleg ***Magyarországon*** és a világ nagy részén törvénytelennek számít.

Jó pár ***phising*** oldalt láttam már, amely az ***IMEI*** szám, az ország és a szolgáltató ismeretében vállalta, hogy megmondja a készülék hálózatfüggetlenítéséhez szükséges kódot. Ez azonban a legtöbb esetben csak ígéret, viszont a megadott ***IMEI*** szám más országban használható, hiszen az ***IMEI*** számok ***nyomonkövetése*** és ***tiltólistája*** csak egy-egy országon belüli szolgáltatók esetén közös legtöbbször. Előfordulhat például az, hogy ha mondjuk külföldön felbukkan a mi ***IMEI*** számunk és valami törvénytelen dolgot hajtanak végre vele – majd letiltják abban az országban –, úgy később esetleg, Mi, a jogos ***IMEI*** tulajdonosok se tudjuk használni a készülékünket.

Medve Zoltán
(e-medve@e-medve.hu)

2001-ben kezdett „Linuxolni”, de már korábban is ismerkedett a szabad szoftverek világával. Ha éppen nem a gép előtt ül, akkor fotózgat, olvasgat vagy bicajozik.

KAPCSOLÓDÓ CÍMEK

Netcraft Toolbar
➲ http://toolbar.netcraft.com/