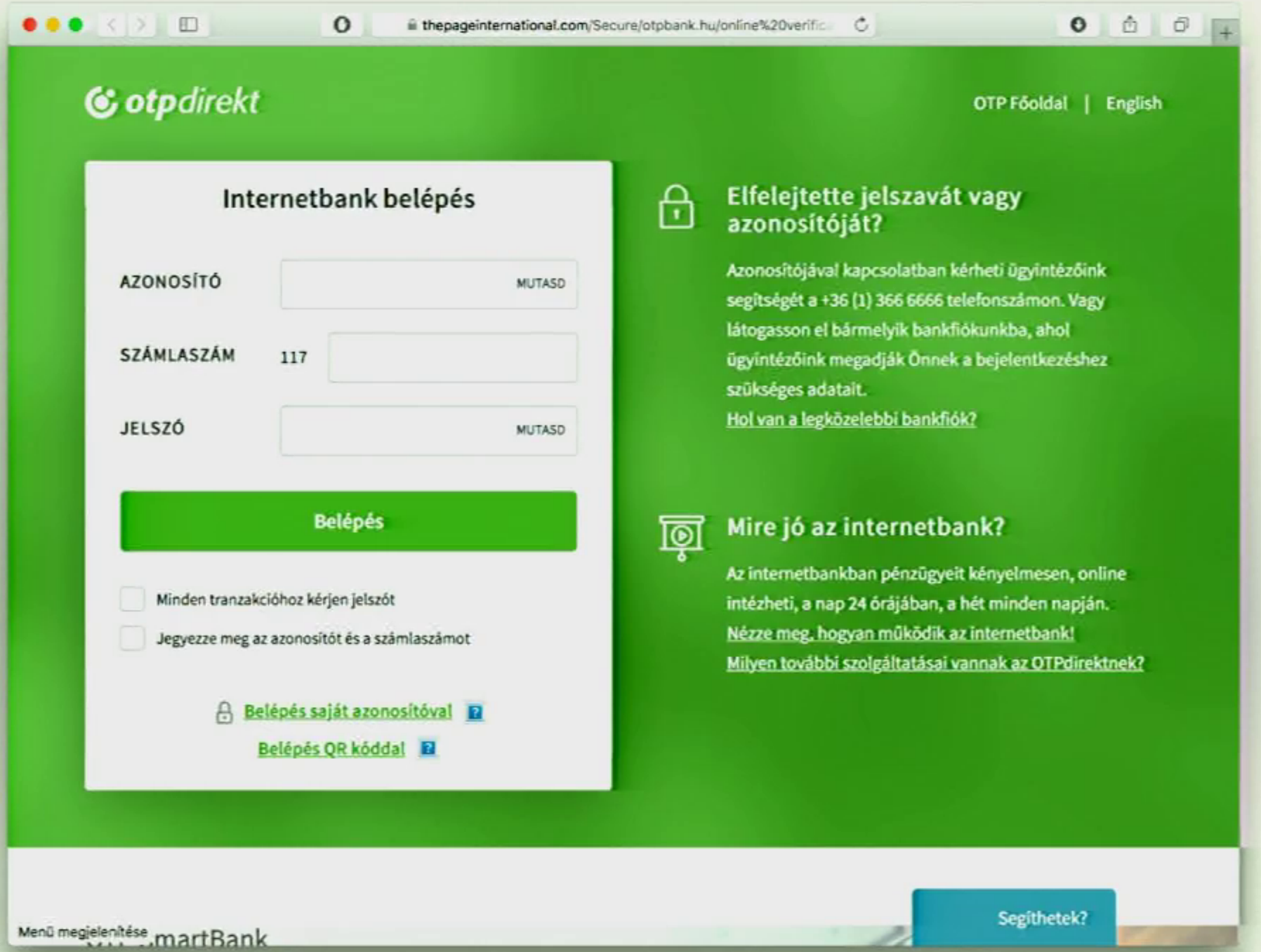
A támadás örökzöldje, a

Social Engineering

Koczka Ferenc - Eszterházy Károly Egyetem
Networkshop - 2018


thepageinternational.com/Secure/otpbank.hu/online%20verific
otpdirekt
OTP Főoldal | English
Internetbank belépés
AZONOSÍTÓ
MUTASD
SZÁMLASZÁM
117
JELSZÓ
MUTASD
Belépés
Minden tranzakcióhoz kérjen jelszót
Jegyezze meg az azonosítót és a számlaszámot
Belépés saját azonosítóval
Belépés QR kóddal
Elfelejtette jelszavát vagy azonosítóját?
Azonosítójával kapcsolatban kérheti ügyintézőink segítségét a +36 (1) 366 6666 telefonszámon. Vagy látogasson el bármelyik bankfiókunkba, ahol ügyintézőink megadják Önnek a bejelentkezéshez szükséges adatait.
Hol van a legközelebbi bankfiók?
Mire jó az internetbank?
Az internetbankban pénzügyeit kényelmesen, online intézheti, a nap 24 órájában, a hét minden napján.
Nézze meg, hogyan működik az internetbank!
Milyen további szolgáltatásai vannak az OTPdirektnek?
Menü megjelenítése
Segíthetek?

OTPBank értesítés

Biztonsági frissítés

Címzett: undisclosed-recipients:;

Bejövő -...-eszterhazy.hu tegnap 13:22

ÉO

Tisztelt Ügyfelünk,

A banki ügyfeleinket célzó, személyazonosság-lopási kísérletek nagyobb száma miatt

más, hogy őrzze meg ügyfeleinket, ütemezésünk frissítése a biztonságunkra

modul a hétvégén. Belépett a bejelentkezéshez és válaszd a leginkább kompatibilitást

modul az online tevékenységek biztonságának növelése érdekében.

Kérjük kattintson ide **https://www.otpbank.hu/netbank/security/upgrade**

Köszönjük a velünk folytatott banki munkáját, a fiókunk biztonságának megőrzése prioritásunk.

Üdvözlettel.

otpbank.

© Copyright 2018 OTP Bank

Az OTP BANK KÖNYV VERIFIK... 6:13

Részletek

Sürgős figyelem: az Otp Bank frissíté...

Címzett: undisclosed-recipients:;

--

otpbank

Sürgős figyelem!

Tisztelt Ügyfelünk,

Ez azt jelenti, hogy bizonyos gyanús próbálkozásokat próbálunk megfizetni egy másik IP-helyszínről Afrikában, az alábbi részletek alapján.

Összeg: 1050,00 USD
Dátum: 2013.03.07
Biller Név: SDRO ENFORCEMENTS.
Biller Becenév: OSR
Biller: 0000198788 SDRO ENFORCEMENTS.
Ügyfél-hivatkozási szám: 910260905157

Ezért ideiglenesen felfüggesztettük fiókját és az online banki hozzáférést, amíg frissítjük és ellenőrizzük fiókját. jelenleg frissítjük és frissítjük kiszolgálónk és rendszeradatbázisunkat az olyan betolakodókkal szemben, akik veszélyeztetik a fiókjukat. Kérjük, kövesse az alábbi utasításokat a fiók biztonságossá tétele érdekében. és kérjük, küldje el az OTP kódot, amelyet elküldünk a mobiltelefonunknak a frissítés befejezéséhez és a fiókod online veszélyeinek védelméhez, amelyek megpróbálnak kárt okozni a fiókjában. kérjük, kövesse figyelmesen az utasításokat, különben fiókja blokkolja az ügyletek végrehajtását. Sajnáljuk, ha bármilyen kényelmetlenséget okozna neked.

Kérjük, kattintson ide Biztonságos fiókja:
https://www.otpbank.hu/online/debit/verification

Köszönjük a Banking-ot velünk, ígérjük, hogy biztonságos fiókját biztosítja.

A Mail szerint ez az üzenet kéretlen posta. Nem kéretlen Áthelyezés a Kéretlenbe

E-TEK CO.,LTD.

Bejövő...szerver.hu tegnapelőtt 7:39

Részletek

EL

Quote Best Price for attached List

Címzett: me, **Másolat:** ocean-team@jdlk.co.kr,

Válaszcím: dhruvkabra@hotmail.com

Good afternoon sir

Please find the attached items and quote your best price

Grade for HEB 200 UPN 200 , L 100 X 100 X 8 , L 160 X 160 X 14 and S235 JR , S275JR or Equivalent

API 5 L GRADE –B , NUTA AXE BOLT with WASHER – ASTM-232, Gratings – normal

All items need MTC . please provide ABS Approved certificate (Plates must be need ABS Certificate)

E-TEK CO.,LTD.

224-8, SuJeong-Ro, Jangan-Myeon, Hwasung-Si, Kyengki-Do, KOREA

TEL : 82-31-351-2961~2, FAX : 82-31-351-2963

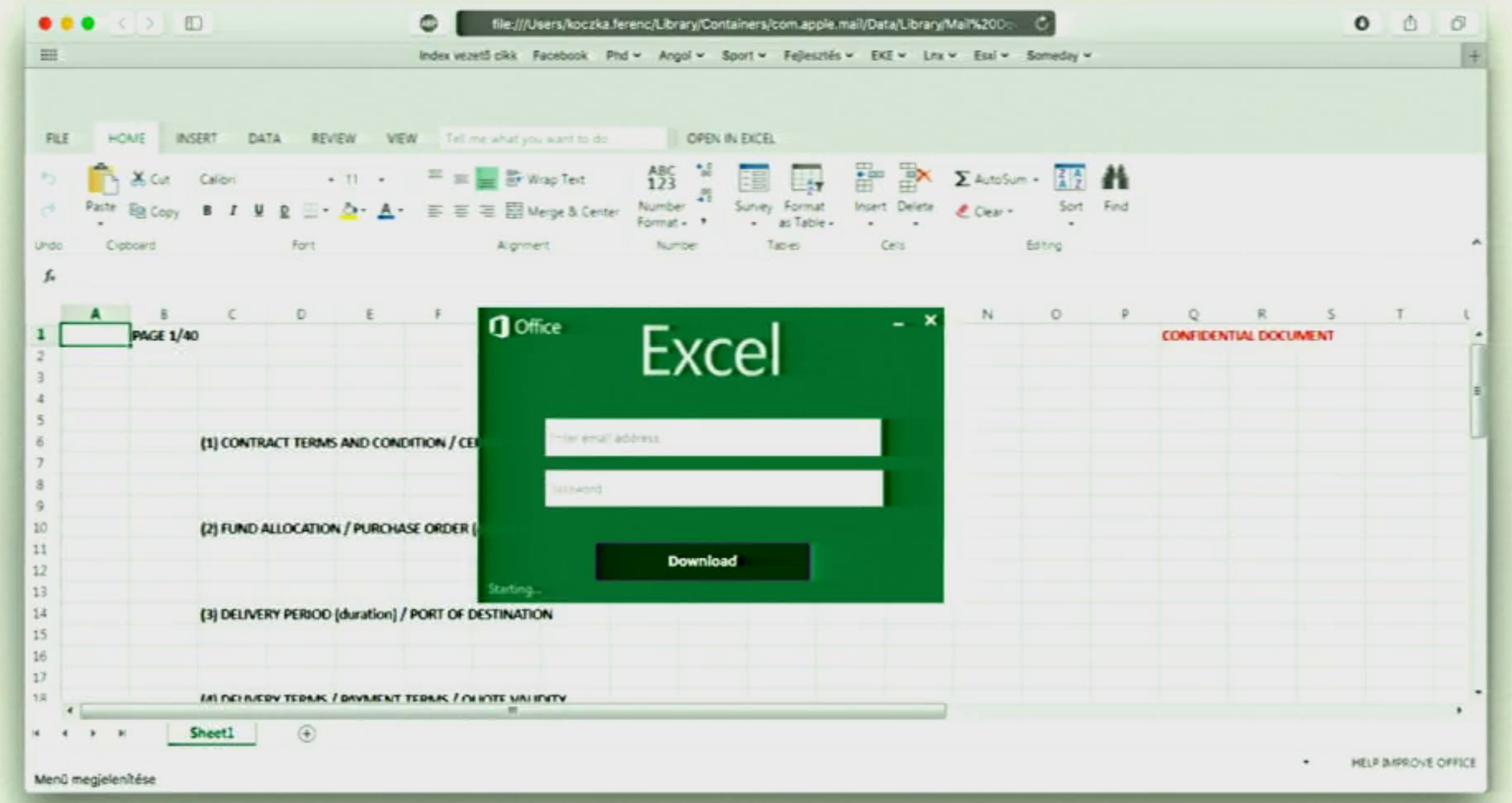
Homepage : www.e-tek.co.kr

Mirror-site : www.e-tek.or.kr

E-mail : etek@e-tek.co.kr

JDLHPH1803043_pdf.gz

SDSVN-180312_xlsx.gz


Office
Excel
Enter email address
Password
Download
Starting...
PAGE 1/40
CONFIDENTIAL DOCUMENT
(1) CONTRACT TERMS AND CONDITION / CE
(2) FUND ALLOCATION / PURCHASE ORDER
(3) DELIVERY PERIOD [duration] / PORT OF DESTINATION
Sheet1
Menü megjelenítése
HELP IMPROVE OFFICE

Felhasználói biztonságtudatosság

Mérés

Forrás:

Felhasználói biztonságtudatosság kezelése, fejlesztése és mérése a Volánbusz Zrt.-nél

Pesti Tamás szakdolgozata, NKE, Budapest, 2017.

17. **Töltött le és telepített Ön már szoftvereket, akár a munkájához kapcsolódóan (pl. PDF-konvertálás, vagy képek átméretezése), akár személyes használatra (pl. zenehallgatás) a munkahelyi számítógépén?** *Lehetséges válaszok:* **Igen** – 7 fő / **Nem** – 28 fő

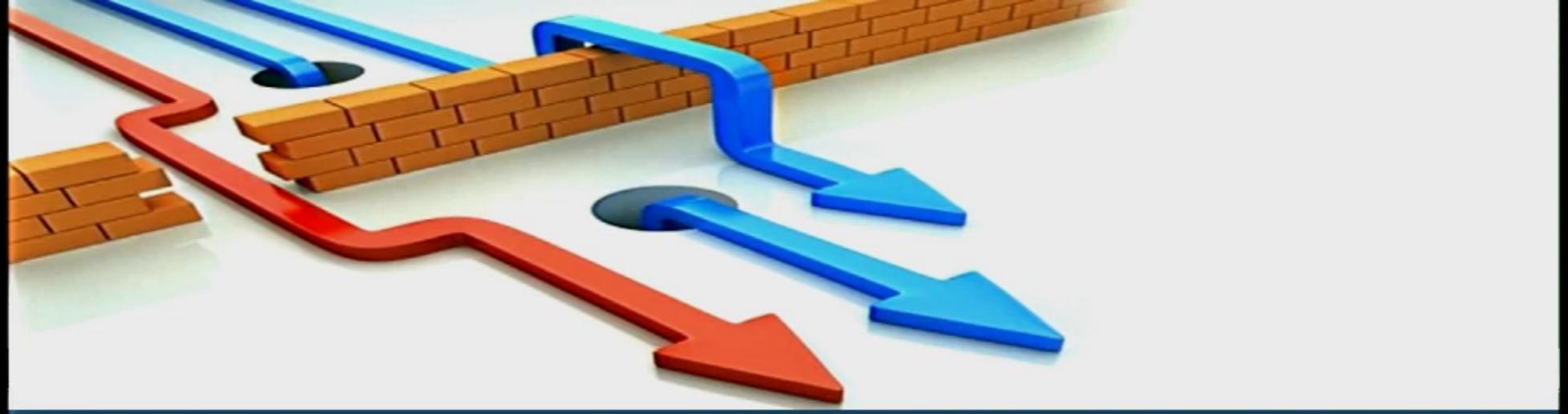
Szöveges kiértékelés: A válaszadók közül csak az informatikai érintettségű kollégák válaszolták „igen"-el, mivel ők rendelkeznek olyan szintű jogosultsággal, akik képesek munkavégzésükhöz szükséges szoftverek letöltésére. A többi munkatárs minimális jogosultsági szinttel rendelkezik, amellyel idegen szoftverek letöltésére nincs lehetőségük és ezzel teljes mértékig tisztában is vannak.

18. **Kérte-e már el az Ön jelszavát a főnöke, vagy valamelyik munkatársa?** *Lehetséges válaszok:* **Igen** – 2 fő / **Nem** – 33 fő

Szöveges kiértékelés: Ahogyan a válaszadók reakcióiból is látható, szinte mindenki tisztában van a biztonságos jelszóhasználattal, valamint az ebből eredendő veszélyforrásokkal. A jelszavakat nem szokták megosztani másokkal, kivéve azt az esetet, amelyet már korábban is említettem, hogy mivel korlátozott felhasználói azonosítóval rendelkezünk bizonyos rendszerek esetében, ezért előfordul, hogy egyes munkavállaló ideiglenesen (helyettesítés, vagy betegség alkalmával) egy másik kolléga azonosítójával, illetve jelszavával dolgozik, de ez egyáltalán nem egy bevált módszer nálunk.

19. **A céges informatikai rendszerbe történő bejelentkezéskor ugyanazt a jelszót használja-e, mint a személyes célokra fenntartott fiókjai (pl. twitter, privát e-mail, facebook, iTunes, stb.) esetében?** *Lehetséges válaszok:* **Igen** – 8 fő / **Nem** – 27 fő

Szöveges kiértékelés: A megkérdezettek jelentős része eltérő jelszót használ informatikai rendszereik esetén, mint az egyes közösségi médiákon. Szóbeli kiértékeléskor a kollégák azt is kihangsúlyozták, hogy a vállalati rendszerek megkövetelik tőlük a biztonságosabb és komplexebb jelszavak megadását, míg a közösségi médiákon ilyen jellegű biztonsági előírások nincsenek.



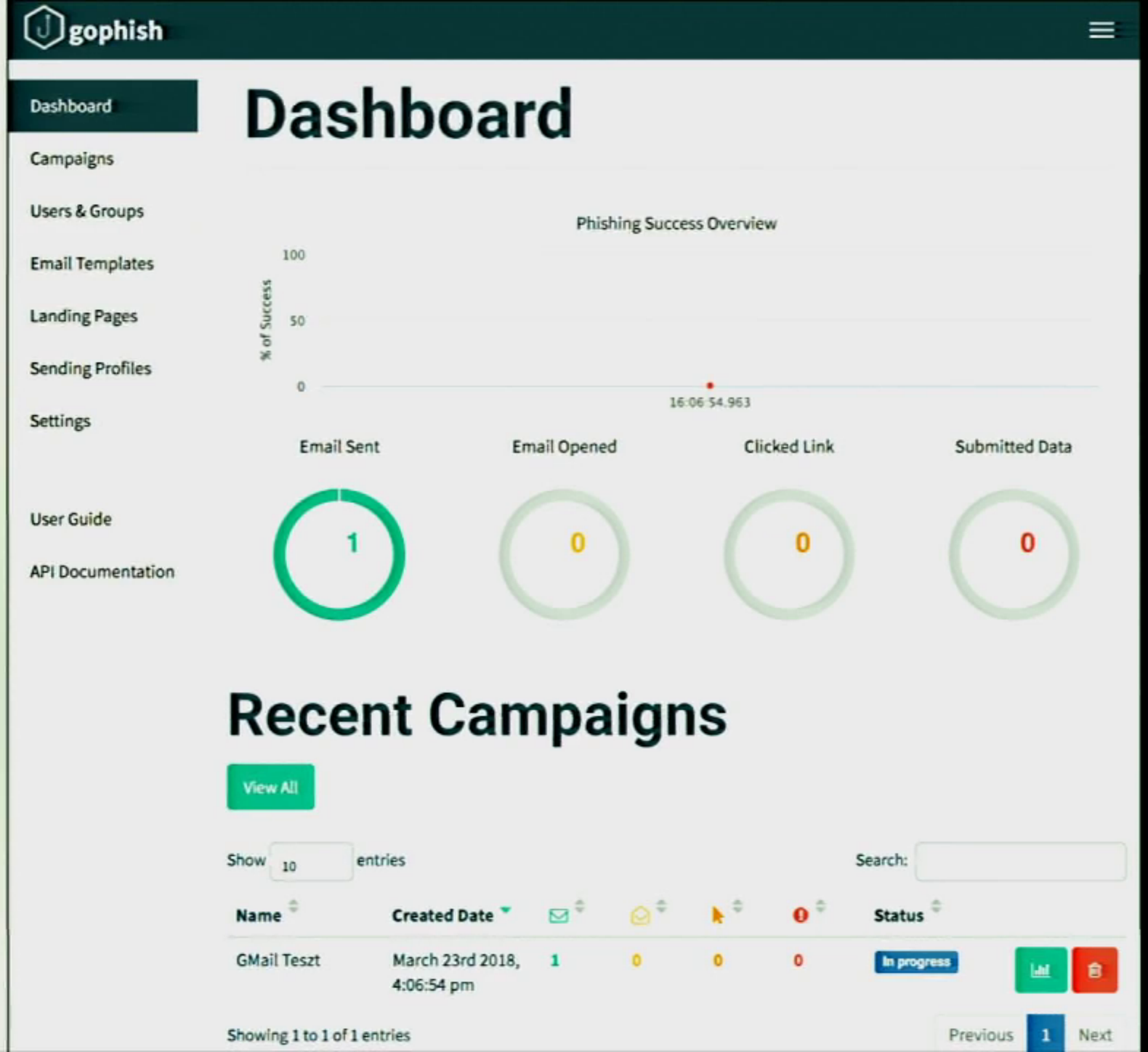
Penetration test

Mi történne, ha tényleg célpont lennénk?

Kész eszközök

GoPhish

- Metasploit
- Social Engineering Toolkit



Domain regisztráció

Az uni-esztehazy.hu domain whois rekordja

Domain:	uni-esztehazy.hu
Domain-használó neve:	Eszterházy Károly Egyetem
Utca, házszám:	Eszterhazy tér 1
Irányítószám, település:	3300 Eger
Ország:	HU
Telefon:	+36520400
Telefax:	
Névszerver:	server.eszterhazy.hu
Névszerver:	sec.246.hu
Regisztrálva:	2017-12-23 14:01:28
Módosítva:	2018-01-01 00:12:17
Adminisztratív kapcsolattartó:	Koczka Ferenc
Utca, házszám:	Eszterhazy tér 1
Irányítószám, település:	3300 Eger
Ország:	HU
Telefon:	+36520400
Telefax:	
Technikai kapcsolattartó:	Koczka Ferenc
Utca, házszám:	Eszterhazy tér 1
Irányítószám, település:	3300 Eger
Ország:	HU
Telefon:	+36520400
Telefax:	
E-mail:	nf@uni-eszterhazy.hu

Domain regisztráció

uni-eszterhazy

Continue to Cart

Yes! Your domain is available. Buy it before someone else does.

uni-eszterhazy.com

~~Ft4,339.00~~ Ft749.00 Add to Cart

when you register for 2 years or more. 1st year price Ft749.00 Additional years Ft4,339.00

uni-eszterhazy.co.uk Add this: Ft2,778.00

Feltételek

- Jól konfigurált elsődleges és másodlagos DNS szerver, spf rekord.
- Teljesen jól konfigurált SMTP szerver.
- DKIM.
- Tanúsítvány: letsEncrypt

- A domain szinte azonnal használatba vehető.
- A fizetés problémás; OTP pénztári befizetés - de akár ki sem kell fizetni.

Adatgyűjtés

- Állatorvostudományi Egyetem: http://www.univet.hu/hu/egyetem/munkatarsak
- ***Andrássy Gyula Budapesti Német Nyelvű Egyetem: zárt telefonkönyv***
- Budapesti Corvinus Egyetem: http://www.uni-corvinus.hu/index.php?id=telefon
- Budapesti Gazdasági Egyetem: https://uni-bge.hu/Footer/phonebook
- Budapesti Metropolitan Egyetem: https://www.metropolitan.hu/telefonkonyv/
- Budapesti Műszaki és Gazdaságtudományi Egyetem: http://telefon.eik.bme.hu
- Debreceni Egyetem: https://unideb.hu/hu/telefonkonyv
- Debreceni Református Hittudományi Egyetem: http://www.drk.hu/wp-content/uploads/2017/09/DRK-Telefonkönyv-2016-09-28.pdf
- Dunaújvárosi Egyetem: http://telefonkonyv.uniduna.hu/Telefonkonyv/SearchUser
- Eötvös Loránd Tudományegyetem: https://telefonkonyv.elte.hu
- ***Evangélikus Hittudományi Egyetem: nem találtam általános tudakozót.***
- Kaposvári Egyetem: http://www.ke.hu/telefonkonyv
- Károli Gáspár Református Egyetem: http://www.kre.hu/portal/index.php/component/spidercontacts/showcontact/272.html?contact_id=55&page_num=1&back=1&order_by=first_name&Itemid=272
- Közép-európai Egyetem: http://eguide.ceu.edu/?criteria=dep&submit=Search&params=department
- ***Liszt Ferenc Zeneművészeti Egyetem: nincs telefonkönyve.***
- ***Magyar Képzőművészeti Egyetem: nincs telefonkönyve.***
- ***Magyar Táncművészeti Egyetem: nincs telefonkönyve.***
- Miskolci Egyetem: http://www.uni-miskolc.hu/telefon/index.php
- Nemzeti Közszolgálati Egyetem: nincs telefonkönyve
- Neumann János Egyetem: https://gk.uni-neumann.hu/kvk-oktatok-elerhetosegei
- Nyíregyházi Egyetem: http://www.nye.hu/telefonkonyv/telefonkonyv.pdf
- Óbudai Egyetem: http://www.uni-obuda.hu/search/oc_searcher
- ***Országos Rabbiképző – Zsidó Egyetem: nincs telefonkönyve.***
- Pannon Egyetem: http://mk.uni-pannon.hu/index.php/egyetemi-telefonkonyv
- Pázmány Péter Katolikus Egyetem: https://ppke.hu/telefonkonyv
- ***Pécsi Tudományegyetem: csak bejelentkezés után.***
- Semmelweis Egyetem: http://semmelweis.hu/telefonkonyv/
- Nyugat-magyarországi Egyetem: http://nyme.hu/index.php?id=19780&L=1&id=19780
- Szent István Egyetem: http://telefonkonyv.szie.hu/eidkeres.php
- Színház- és Filmművészeti Egyetem: nincs telefonkönyve.
- Szegedi Tudományegyetem: https://www.u-szeged.hu/telefonkonyv
- Zsigmond Király Egyetem: http://www.uni-zsigmond.hu/kapcsolat/oktatok

Phising 1750

- Látszólag levelezési listára küldött téves levél.
- Az informatikai munkatársak nem voltak a címzettek közt.
- Jogi záradékkal.
- Nyilvánvalóan nem a munkatársnak szól.
- Az egyik potenciális veszélyforrás: Excel tábla.
- Kis odafigyeléssel nyilvánvalóan hamis tartalom.
- A webszerveren tracking mechanizmus mentén azonosítható a letöltő személye.

[Eke-Dolgozok] Bérjegy... 31 / 48 üzenet

Feladó **Kalán Erika**
Dátum **2018-03-19 07:29**

Tisztelt Szalay Úr!!

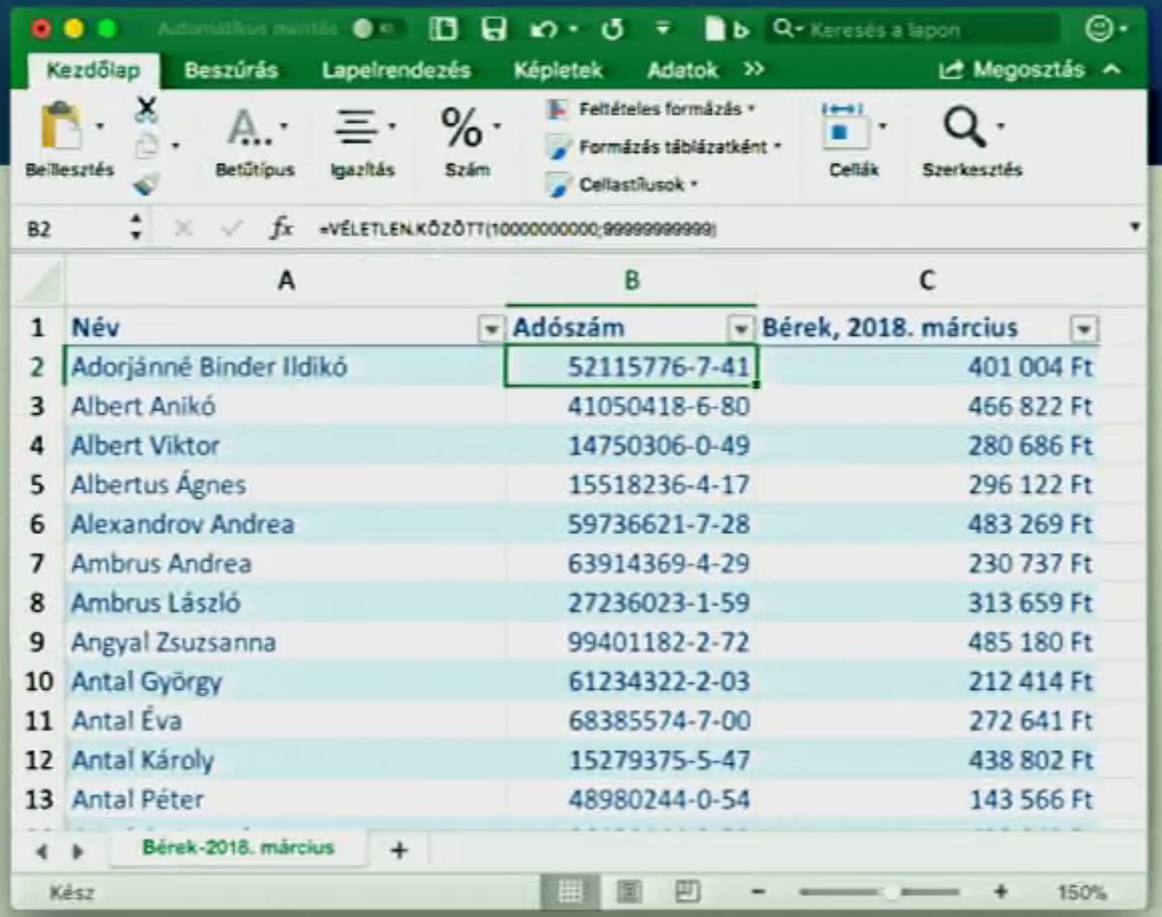
Kérésére küldöm az Eszterházy Károly Egyetem dolgozóinak 2018. március havi kifizetések listáját. Sajnos az Excel táblázat túl nagy, ezért ezen a linken tölthető le: berjegyzek-201803.xlsx

Kalán Erika
Ügyintéző
Humánerőforrás Osztály

A jelen üzenetben található információk bizalmasak, üzleti titoknak minősülnek, azokat kizárólag a címzett használhatja fel Amennyiben nem Ön ennek az üzenetnek a címzettje, Kérjük, azonnal értesítse a feladót és az üzenetet törölje a rendszeréből. Felhívjuk figyelmét,, hogy a nem önnek címzett elektronikus levél jogosulatlan felhasználása, másolása, terjesztése vagy a tartalmával való visszaélés törvénytelennek minősülhet és szigorúan tilos.

Phising 1750

- Látszólag levelezési listára küldött téves levél.
- Az informatikai munkatársak nem voltak a címzettek közt.
- Jogi záradékkal.
- Nyilvánvalóan nem a munkatársnak szól.
- Az egyik potenciális veszélyforrás: Excel tábla.
- Kis odafigyeléssel nyilvánvalóan hamis tartalom.
- A webszerveren tracking mechanizmus mentén azonosítható a letöltő személye.



	A	B	C
1	Név	Adószám	Bérek, 2018. március
2	Adorjánné Binder Ildikó	52115776-7-41	401 004 Ft
3	Albert Anikó	41050418-6-80	466 822 Ft
4	Albert Viktor	14750306-0-49	280 686 Ft
5	Albertus Ágnes	15518236-4-17	296 122 Ft
6	Alexandrov Andrea	59736621-7-28	483 269 Ft
7	Ambrus Andrea	63914369-4-29	230 737 Ft
8	Ambrus László	27236023-1-59	313 659 Ft
9	Angyal Zsuzsanna	99401182-2-72	485 180 Ft
10	Antal György	61234322-2-03	212 414 Ft
11	Antal Éva	68385574-7-00	272 641 Ft
12	Antal Károly	15279375-5-47	438 802 Ft
13	Antal Péter	48980244-0-54	143 566 Ft

Phising

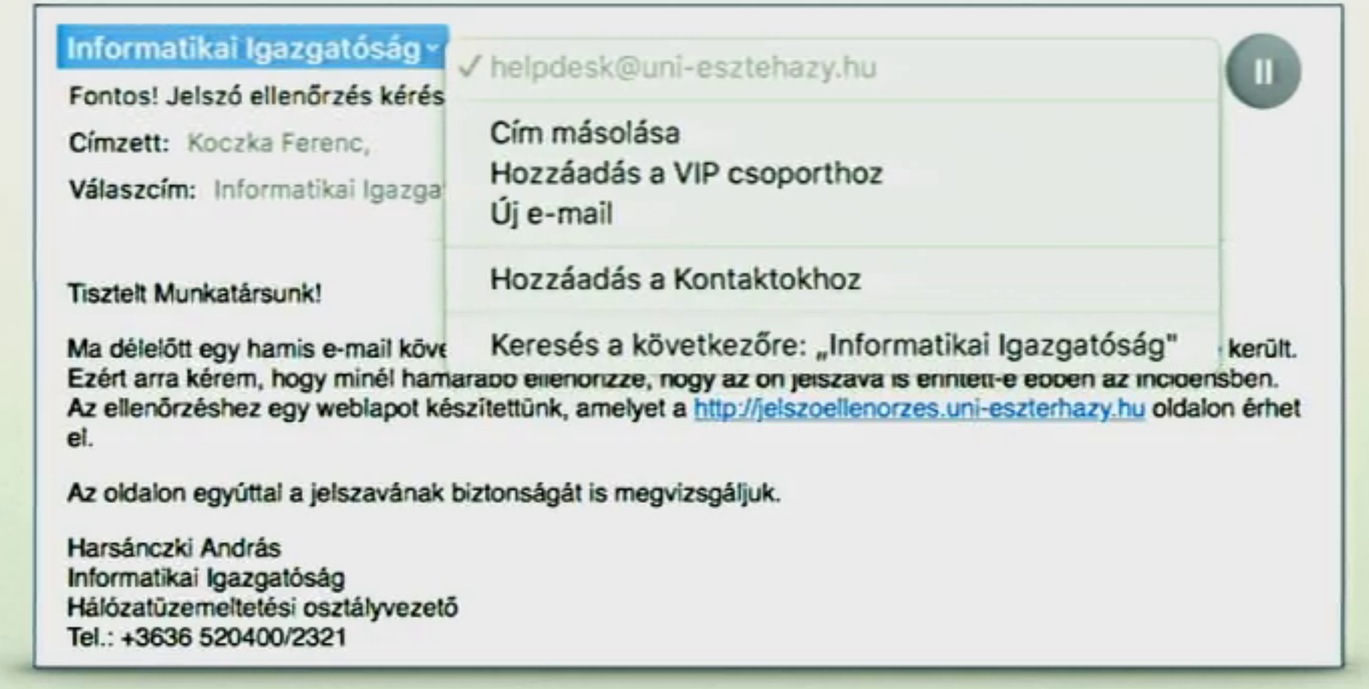
- 1750 levélből 969 letöltés, 532 különböző munkatárstól.
- 2 óra alatt a nagy része lefut.
- 150 körüli letöltés, miután megírtam, hogy csak pentesztet végeztünk.

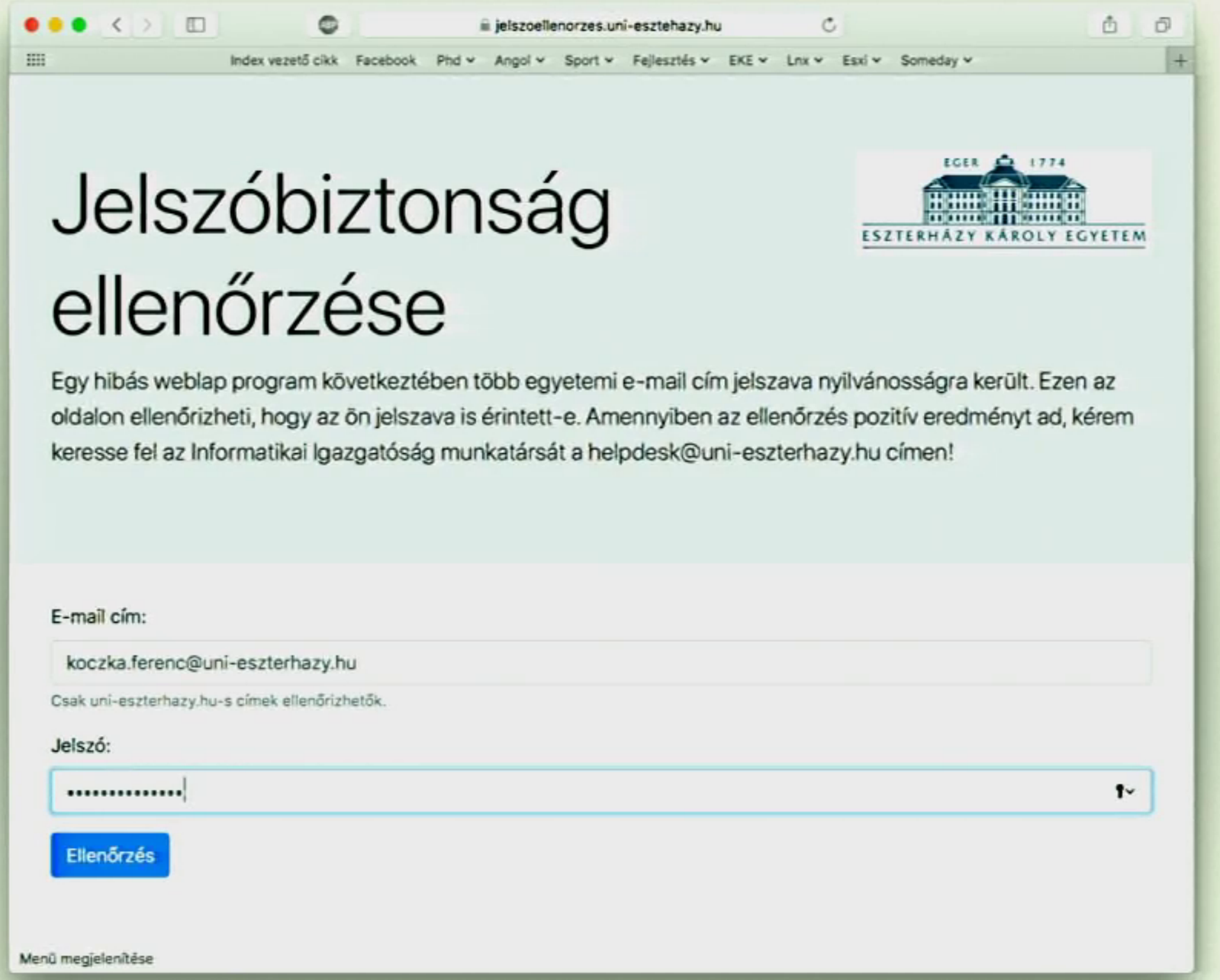
- A béradatok megismerhetősége csábító volt.
- A domain megtévesztő, és sok esetben nem is látható.
- A jogszerű magatartásról.

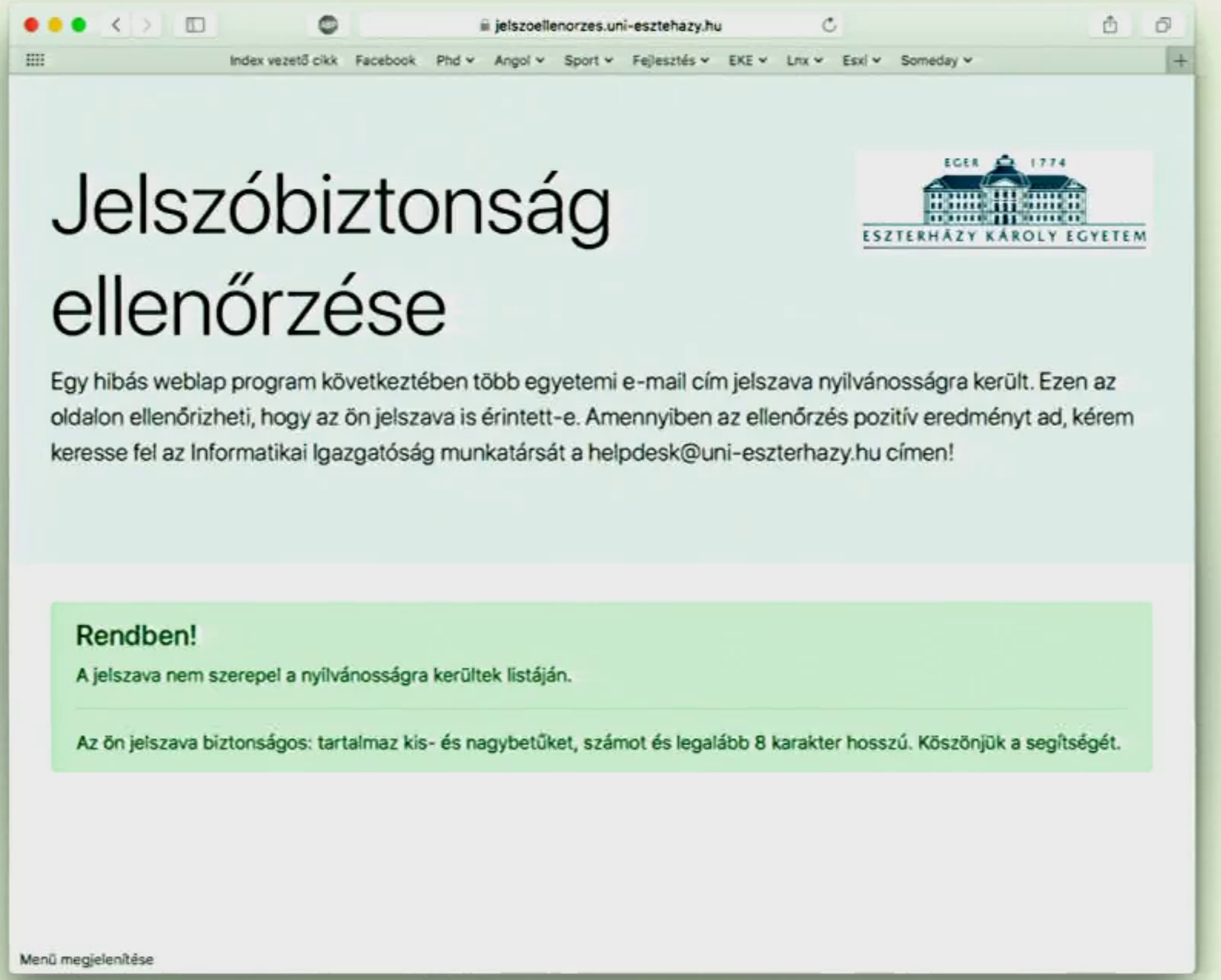
- Hasonló nevű domain jelzése a tárgyban.
- Tömeges levéltörlés tool.
- Kliensek beállítása a feladó címének megjelenítésére.

Idő	Letöltések
07:00-08:00	27
08:00-09:00	264
09:00-10:00	121
10:00-11:00	40
11:00-12:00	24
12:00-13:00	17
13:00-14:00	16
14:00-15:00	9

Levél a helpdesktől




jelszoellenorzes.uni-eszterhazy.hu
Index vezető cikk
Facebook
Phd
Angol
Sport
Fejlesztés
EKE
Lnx
Esxi
Someday
Jelszóbiztonság ellenőrzése
EGER 1774
ESZTERHÁZY KÁROLY EGYETEM
Egy hibás weblap program következtében több egyetemi e-mail cím jelszava nyilvánosságra került. Ezen az oldalon ellenőrizheti, hogy az ön jelszava is érintett-e. Amennyiben az ellenőrzés pozitív eredményt ad, kérem keresse fel az Informatikai Igazgatóság munkatársát a helpdesk@uni-eszterhazy.hu címen!
E-mail cím:
koczka.ferenc@uni-eszterhazy.hu
Csak uni-eszterhazy.hu-s címek ellenőrizhetők.
Jelszó:
Ellenőrzés
Menü megjelenítése


jelszoellenorzes.uni-esztehazy.hu
Index vezető cikk
Facebook
Phd
Angol
Sport
Fejlesztés
EKE
Lnx
Esxl
Someday
Jelszóbiztonság ellenőrzése
EGER 1774
ESZTERHÁZY KÁROLY EGYETEM
Egy hibás weblap program következtében több egyetemi e-mail cím jelszava nyilvánosságra került. Ezen az oldalon ellenőrizheti, hogy az ön jelszava is érintett-e. Amennyiben az ellenőrzés pozitív eredményt ad, kérem keresse fel az Informatikai Igazgatóság munkatársát a helpdesk@uni-eszterhazy.hu címen!
Rendben!
A jelszava nem szerepel a nyilvánosságra kerültek listáján.
Az ön jelszava biztonságos: tartalmaz kis- és nagybetűket, számot és legalább 8 karakter hosszú. Köszönjük a segítségét.
Menü megjelenítése

Következtetések

- 304-en adták meg a jelszavukat.
- Ha az adminisztrátorok tehetik a dolgukat, természetesen ez a szám kisebb lett volna.
- Nem csengett a vészcsengő, nem ellenőrizték az url-t.
- Nem tűnt fel, hogy a weblap túl kidolgozott.
- Nem emlékeztek arra, hogy ilyet az informatika sohasem kér.
- A ribillió következtében jellemző volt a kapkodás, de sokan észbe kaptak és jelszót cseréltek.
- Azt gondolják, a vírusvédelmi szoftver megvédi őket.
- Nagyon könnyű tanúsítványhoz jutni.

Let's Encrypt

- Nincsenek központi tananyagok. (http://njszt.hu/de/it-biztonsag-kozerthetoen).
- Máshol ez az EIV feladata.
- Sokan megsértődtek.
- De egy darabig most figyelnek.
- Esetleg engem tesztelnek.

Továbbítás: Biztonsági frissítés
Címzett: Koczka Ferenc

Tisztelt Koczka Ferenc!

Gondolom ez esetleg érdekli. Hacsak nem ismét Öntől jött :D

Kellemes Ünnepet!

Üdvözlettel,

András

-------- Eredeti üzenet --------

Tárgy: Biztonsági frissítés
Dátum:2018-03-30 13:45
Feladó:otpbank értesítés <haneykhor@rdfloodind.com>
Címzett:

otpbank

Figyelem: Kedves vásárló,

Nagyon sajnáljuk, ha nehézségekbe ütközhet a fiókjában való bejelentkezéskor,

némi frissítést végzünk, és fenntartjuk szerverünket az új biztonsági funkciókhoz. Ez megengedi tudják, hogy az online OTPBanking tároló elérte kvótahatárát a rendszer adatbázisában.

A jövő

- Önállóan elvégezhető oktatási anyagok készítése.
- Oktatások elvégzése.
- “Humoros” tájékoztatók készítése.
- Új belépők automatikus tesztje.
- A munkatársak folyamatos tesztelése.
- Közös tananyag?

Köszönöm a figyelmet!