KÁVÉESKA
zážitky malé i velké

městská část
BRNO-STŘED

BOTANKA
centrum volného času

HOAX - podvodný e-mail

Odvrácená tvář elektronické komunikace

Brno 27.3.2018

Josef Džubák
www.hoax.cz

HO@X

H O A X [:houx:] - co to je?

Robert Nares

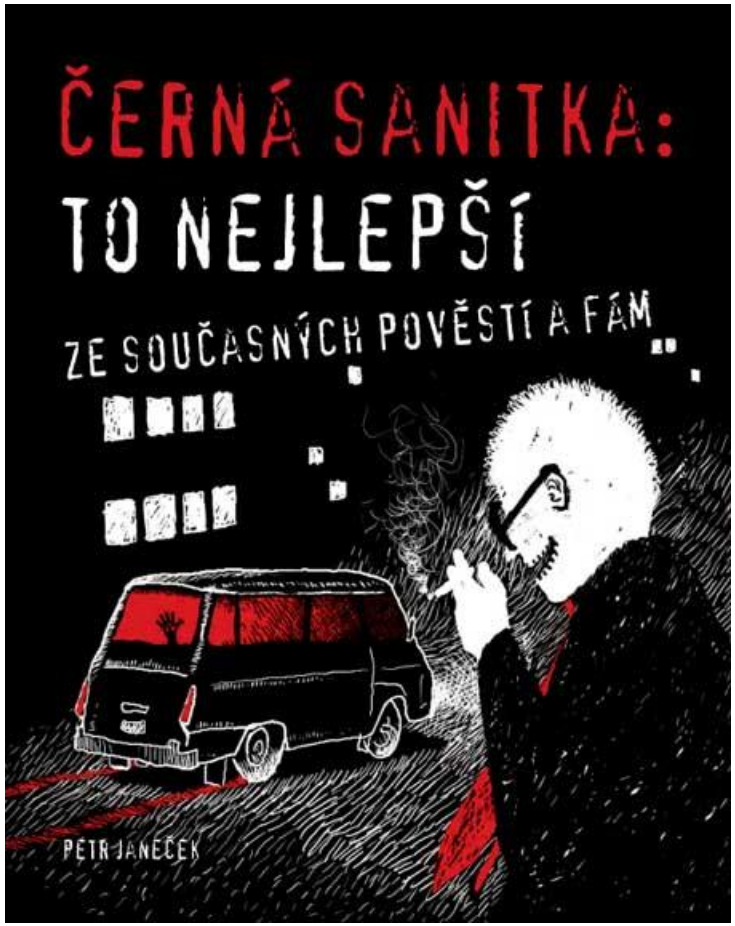
1753-1829

anglický jazykovědec

Slovo <u>HOAX</u> vzniklo na konci 18. století

zkrácením slova <u>hocus</u> = trik / podvádění / klamání

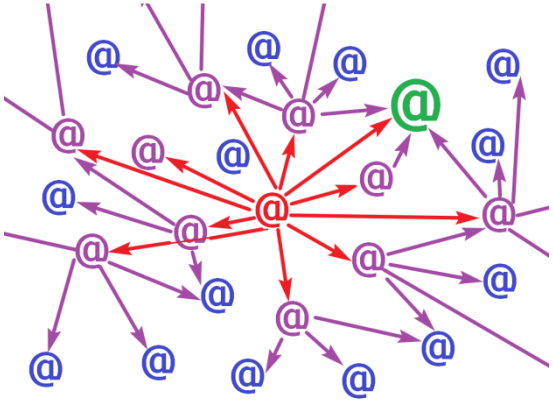
H O A X [:houx:]

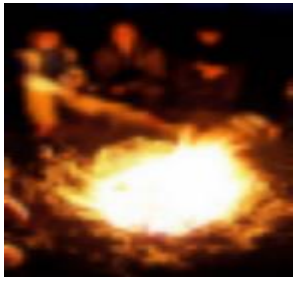


- Novinářská kachna
- Mystifikace
- Fáma
- Městská legenda
- Žert
- Podvod

HOAX a rychlost šíření

S novějšími technologiemi se zvyšuje rychlost přenosu a sdílení informací





HO@X

HO@X.CZ JE TU PRO VÁS UŽ 17 LET

HOAX | PHISHING | LOTERIE | SCAM419 | MALWARE | ŘETĚZOVÉ E-MAILY

RYCHLÉ VYHLEDÁVÁNÍ

Sem zadej hledanou frázi.

- AKTUALITY
- DATABÁZE
- CO JE TO HOAX
- ČÍM HOAX ŠKODÍ
- NETIKETA
- INTERNETOVÉ PODVODY
- NEJČASTĚJŠÍ DOTAZY
- DISKUSE K TÉMATU
- FÓRUM
- ZAJÍMAVÉ ODKAZY
- NAPSALI O NÁS
- FOTOGALERIE
- KONTAKT

HOAX

Jedním z velmi častých nešvarů, který se na Internetu vyskytuje, je šíření poplašných, nebezpečných a zbytečných řetězových zpráv, tzv. hoaxů.
Cílem serveru HOAX.cz je informovat uživatele o těchto nástrahách, se kterými se denně setkává a které znepříjemňují nebo ohrožují jeho běžné používání Internetu a jsou i v rozporu s Netiketou.
Najdete zde pravidelně aktualizovanou databázi nejrozšířenějších podvodných e-mailů. Dříve než rozešlete jakýkoliv řetězový e-mail, navštivte naši databázi a ujistěte se, že právě Vy nerozesíláte zbytečnou poplašnou zprávu svým přátelům, známým či obchodním partnerům.

NEJROZŠÍŘENĚJŠÍ HOAXY

- FACEBOOK - nepřijímejte žádost o přátelství...
- MARGARÍNY a zdravotní riziko (Rama s nama)
- Recyklované mléko
- Nebezpečný moderní jogurt
- Windows live aktualizace
- Pomeranče s krví a HIV
- Nové radary ve svodidlech
- Výroky Jiřího Suchého - co nikdy neřekl
- Šok v lékárně - kdo nemusí platit za léky

Naši partneři

NA PRAVDĚ ZÁLEŽÍ.
IGIHO STRÁNKA O VIRECH WWW.VIRY.CZ
SECURITY
bezpečí
hustej INTERNET.cz
Manipulátoři.cz
PARANOIA
NEŠLAPE.CZ vzdálená pomoc

HOAX - cesty šíření v síti

- E-mail
- Diskuzní skupiny
- ICQ, Skype...
- Sociální sítě - *Facebook, Twitter...*
- Blogy
- Specializované (propagandistické) weby

HOAX - témata šířených zpráv

- Fámy z virtuálního a reálného světa
- Falešné sliby odměn za přeposlání e-mailu
- Prosby o pomoc *smyšlené / neaktuální*
- Řetězové dopisy štěstí a žertovné zprávy

- Podvody, podvodné e-maily

- Polopravdy a účelově upravené zprávy

Nesmyslná varování před virem

DŮLEŽITÉ VAROVÁNÍ!

OPRAVDU SI TO PŘEČTI NEBO MÁŠ PO PC A TVÍ ZNÁMÍ TAKY!

Nepřijímejte nic od kontaktu pete_ivan@hotmail.com a ani video o Bushovi, je to hacker, zformátuje počítač a zničí i heslo k Vaší elektronické poště.

Pozor, pokud ho Vaše kontakty přijmou, tak ho dostanete i Vy, takže jim pošlete rychle zprávu – je důležité poslat toto oznámení všem!!! Vašim přátelům, rodině, spolupracovníkům,..... V nejbližších dnech si musíte dát pozor neotvírat žádnou zprávu, která bude mít přílohu s názvem: Pozvánka (invito, invitation) nezávisle na tom, od koho ta zpráva bude. Je to virus, který zničí celý harddisk. Tento virus přijde od známé osoby, kterou máte mezi kontakty. Proto musíte upozornit všechny o tomto nebezpečí. Je lepší dostat tuto zprávu 25 krát, než dostat virus a otevřít ho. Pokud byste přece dostali poštu od přítele s přílohou: pozvánka, neotvírejte ji a vypněte ihned počítač. Jde o nejhorší virus ohlášený CNN. Tento nový virus byl objeven teprve nyní a Microsoftem byl klasifikován jako nejdestruktivnější virus všech dob. Tento virus byl objeven včera společností McAfee a neexistuje proti němu zatím žádná antivirová ochrana. Tento virus jednoduše zničí Nulový sektor harddisku, ve kterém jsou zachovány vitální informace jeho funkcí.

Fáma o recyklovaném mléce

SKANDÁL:mlékárenské společnosti mohou ze zákona prošlé mléko až pětkrát přepasterizovat a uvést znovu do prodeje,
Je nutno velmi dobře prohlédnout tetrapack, jestliže najdete 12 45 - tj. chybí 3 - pak se jedná o mléko, jež třikrát prošlo a bylo třikrát přepasterizované. A ovšem v krabici je každé balení jiné. De facto pijeme špinavou vodu!

Fáma o infikovaném ovoci

POMENANČE Z LIBIE JSOU POSTŘÍKANÉ HIV KRVÍ, celní služba v chorvatsku to zjistila !!!!!posílejte dál hlavně kdo má malé děti!!!!!!!!!!!!!!!!

STANOVISKO ODBORNÍKŮ

- **Přenos nákazy HIV jídlem je velmi nepravděpodobný**
- **Virus HIV hyne po zaschnutí či naředění krve**
- **Pokud jde o krev je 50x nakažlivější možnost nákazy žloutenkou než HIV**

Fáma – v nouzi zadej PIN opačně

Jakmile se ocitnete v situacii a musíte pod nátlakem vybrat peníze z bankovního automatu na požádáni/přinuceni nasilnikem, zadejte svůj PIN opačně:
to je od konce - např. máte-li 1234, tak zadáte 4321, automat vám peníze přesto vydá, ale též současně přivolá policií, která vám přijde na pomoc. Tato zpráva byla před nedávnem vysílaná v TV, protože málo lidí využívalo tuto skutečnost, protože o tom nevěděli.

Přepošlete toto co nejvíce lidem.

STANOVISKO BANK

Zpráva je zcela nesmyslná.
Ke každé kartě patří jedinečný PIN. Pouze správně zadaný PIN umožní provádět v bankomatu transakce s kartou.
PIN kód zadaný odzadu, je chybný a nelze po jeho zadání provést jakoukoli transakci.

Co mají hoaxy společné?

Co mají hoaxy společné

Snaží se přesvědčit svojí důležitostí

Nové nebezpečí, naléhavá pomoc, šokující informace

Údajný důvěryhodný zdroj

Microsoft varuje, laboratoř NASA zjistila

Výzva k dalšímu rozeslání !!!

Pošlete všem..., raději 20x dostat než..., varuj všechny...

HOAX – odměna za šíření e-mailu

Prosim Vas neberte to na lehkou vahu. Bill Gates se rozhodl podelit se o sve bohatstvi. Pokud tohle budete ignorovat, pozdeji Vas to muze mrzet.

Microsoft a AOL jsou ted nejvetsi Internetove spolecnosti a aby se ujistili, ze Internet Explorer zustava nejrozsirenejsim programem, rozebehli e-mailovy beta test. Jestli preposlete tento mail svym pratelum, Microsoft to zjisti (pokud jste uzivatele Microsoft Windows) do dvou tydnu.

Za kazdeho cloveka, kteremu tento mail preposlete, Vam Microsoft zaplati $ 245, za kazdeho cloveka, kteremu to poslete a on take, Vam Microsoft zaplati dalsich $ 243, a za kazdeho tretiho cloveka, ktery tuto zpravu obdrzi, Vam zaplati $ 241.

Do dvou tydnu se Vas Microsoft bude kontaktovat, aby obdrzel Vasi adresu a pak Vam posle sek.

HOAX – peníze za šíření e-mailu

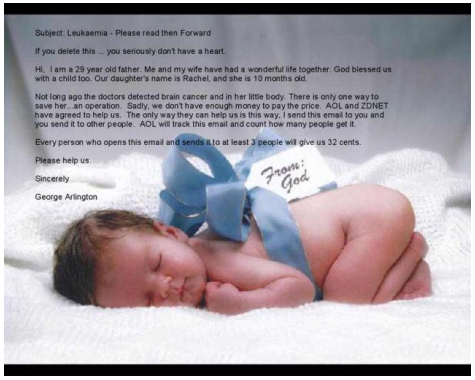
Úroveň	Částka $	Počet lidí
1.	1 225	5
2.	7 350	25
3.	37 975	125
4.	191 100	625
5.	956 725	3 125
6.	4 784 850	15 625
7.	23 925 475	78 125
8.	119 628 600	390 625
9.	598 144 225	1 953 125
10.	2 990 722 350	9 765 625
11.	14 953 612 975	48 828 125
12.	**74 768 066 100**	**244 140 625**
13.	373 840 331 725	1 220 703 125

Srpen 2016: majetek Billa Gatese dosáhl 90 miliard dolarů

HOAX – vymyšlené prosby o pomoc

Když to vymažete... tak opravdu nemáte srdce.

Ahoj, jsem 29letý otec. Já a moje žena máme spolu překrásný život. Bůh nás také obdaroval dítětem. Jméno naší dcery je Rachel a je jí 10 měsíců.
Před nedávnem lékaři zjistili rakovinu mozku v jejím malém tělíčku. Existuje jen jeden způsob, jak jí zachránit... OPERACE.
Bohužel nemáme dostatek peněz na její zaplacení. AOL a ZDNET souhlasili, že nám pomohou.Jediný způsob, jakým nám mohou pomoct je tento: Já posílám tento e-mail vám a vy jej pošlete dalším lidem. AOL bude sledovat tento e-mail a počítat, kolik lidí jej obdrželo. Každá osoba, která otevře tento e-mail a pošle ho nejméně 3 lidem nám přinese 32 centů.



HOAX – neaktuální prosby o pomoc

- Původně skutečné prosby o pomoc
- Aktuální byly pouze několik dní
- Stále se šíří, lidé je bez ověření posílají a sdílejí
- Časem může být zpráva nesmyslně změněna

HOAX – neaktuální prosby o pomoc

TÉMATA

- *Prosba o krev pro nemocného člověka*
- *Hledání pohřešované osoby*
- *Nabídka štěňátek*

HOAX – neaktuální prosby o pomoc

Leden 2001

Poslite to dalej prosim to nie je hra, to je zivot !!!
Jeden clovek zomiera na onkologii - potrebuje krv skupiny "A1B RH neg", ktora je vraj zriedkava (1:50).
Ak ju niekto ma a moze darovat, nech zavola na telefonne cislo 00421/ 07/ 593 78 681 (Onkologicky ustav, Alexander Gal).
Ak nie, skuste poprosit priatelov.
Mozno spolu niekoho najdeme.
Dakujem za pomoc.

Prosinec 2004

● **ONKOLOGICKÝ ÚSTAV** Alexandra Gala v Bratislavě se obrací na nositele krevní skupiny A1B RH negativní, která by mohla zachránit život jednoho z pacientů, který zde pomalu umírá a k záchraně by potřeboval tuto neobvyklou krevní skupinu. Pokud by se našel vhodný dárce, ať zavolá na slovenské tel. číslo 00421-7-59378681. **(sch)**

Je možné kolující hoaxy zastavit?

Jak zastavit kolující hoaxy

Bez ověření skutečnosti a aktuálnosti neposílám!

Má opravdu význam posílat zprávu všem?

V případě, že nechci ověřovat, nerozesílám!!!

Boj s hoaxy = boj s větrnými mlýny

"Já to stejně pošlu všem,

co kdyby to náhodou byla pravda!"

HOAX – Řetězové e-maily

Toto je test přátel. Pošli ho tolika přátelům, kolika budeš moci a když jej dostaneš nazpět, budeš vědet, kdo jsou tvoji skuteční přátelé.

Když přerušíš řetěz, budeš mít smůlu.

Teď si něco přej....

Máš 30 sekund.... ....start!

Když toto pošleš:
2 lidem - přání se Ti splní do roka
5 lidem - do 3 měsíců
7 lidem - do 1 měsíce
10 lidem - do týdne
15 lidem - do zítra

Může řetězový e-mail škodit?

Jak cizí lidé získali moji adresu?!?

Jak může řetězový e-mail škodit

Stovky adres v kolujícím e-mailu nejsou výjimkou!

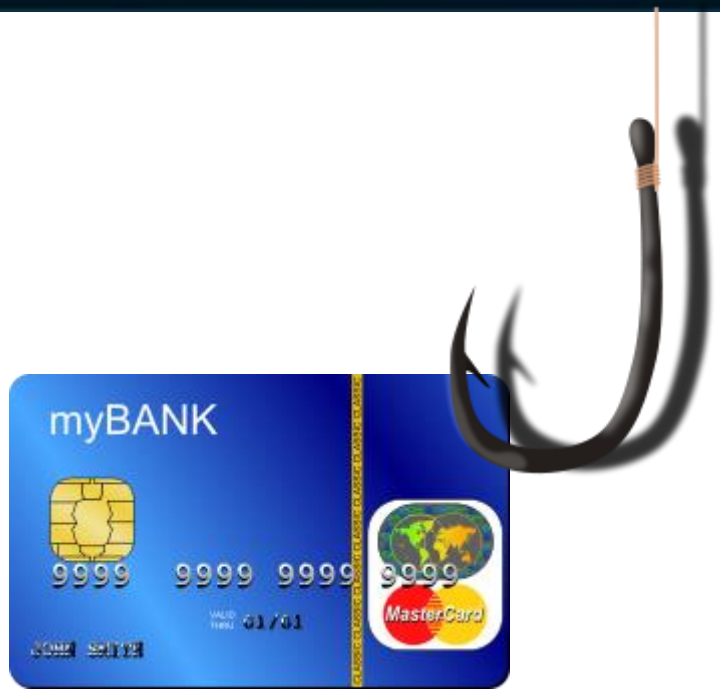
250 adres

Máme adresy, jdeme na PHISHING

P*assword*

H*arvesting*

***f*ISHING**



Sběr hesel r(h)ybařením

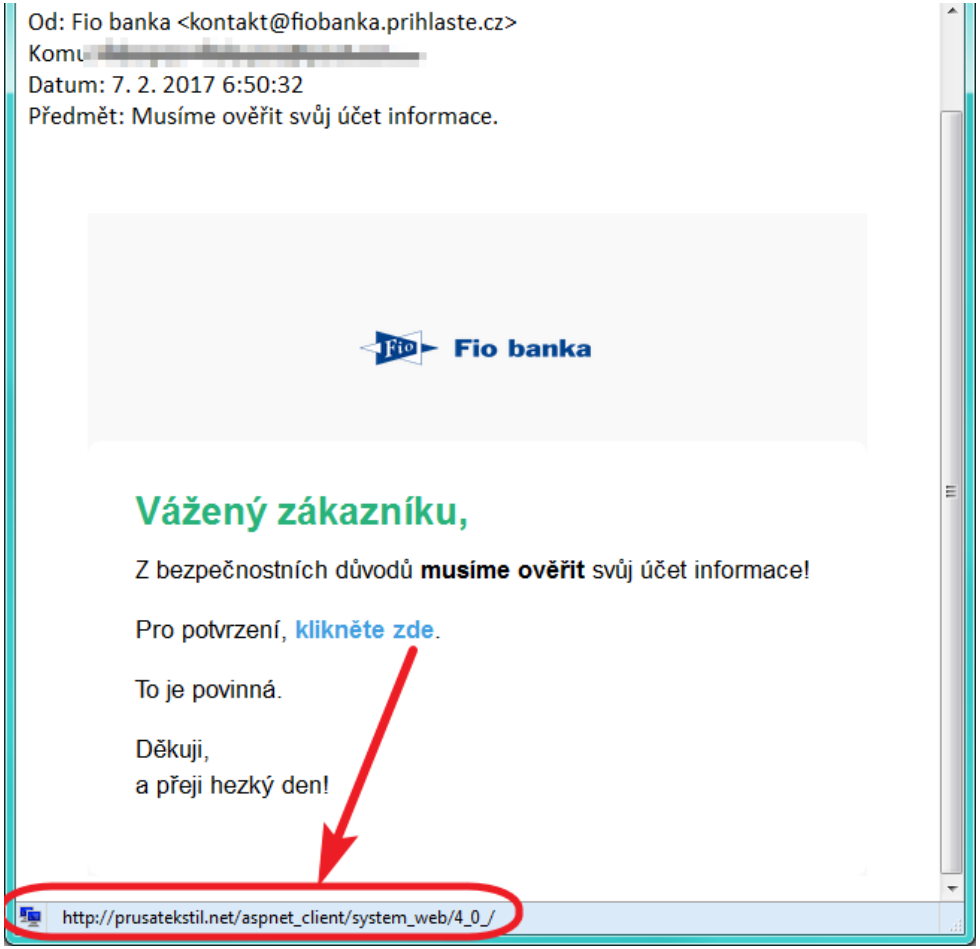
Odvrácená tvář elektronické komunikace 27.3.2018

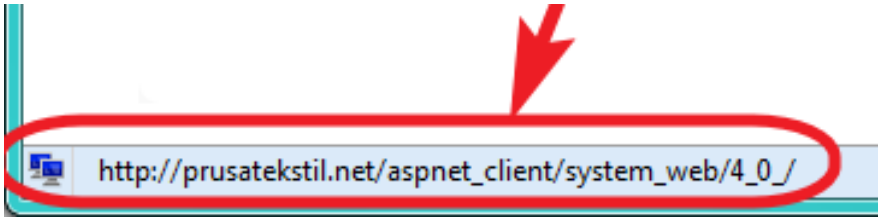
HO@X

PHISHING

- Uživatelům je doručen e-mail s důležitou výzvou
- V textu je odkaz pro nápravu problému
- Uživatel přejde na podvodné stránky s falešným formulářem
- Vyplněná data z falešných formulářů získají podvodníci

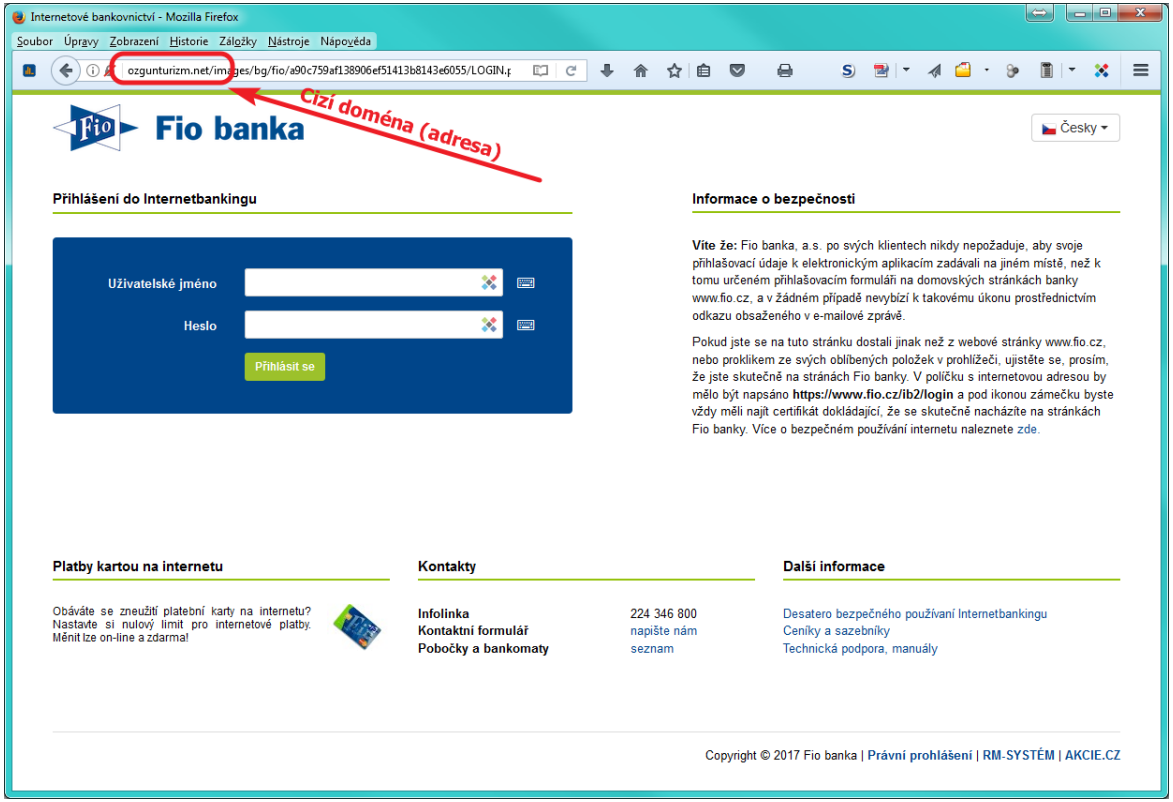
Podvodný e-mail s falešným odkazem





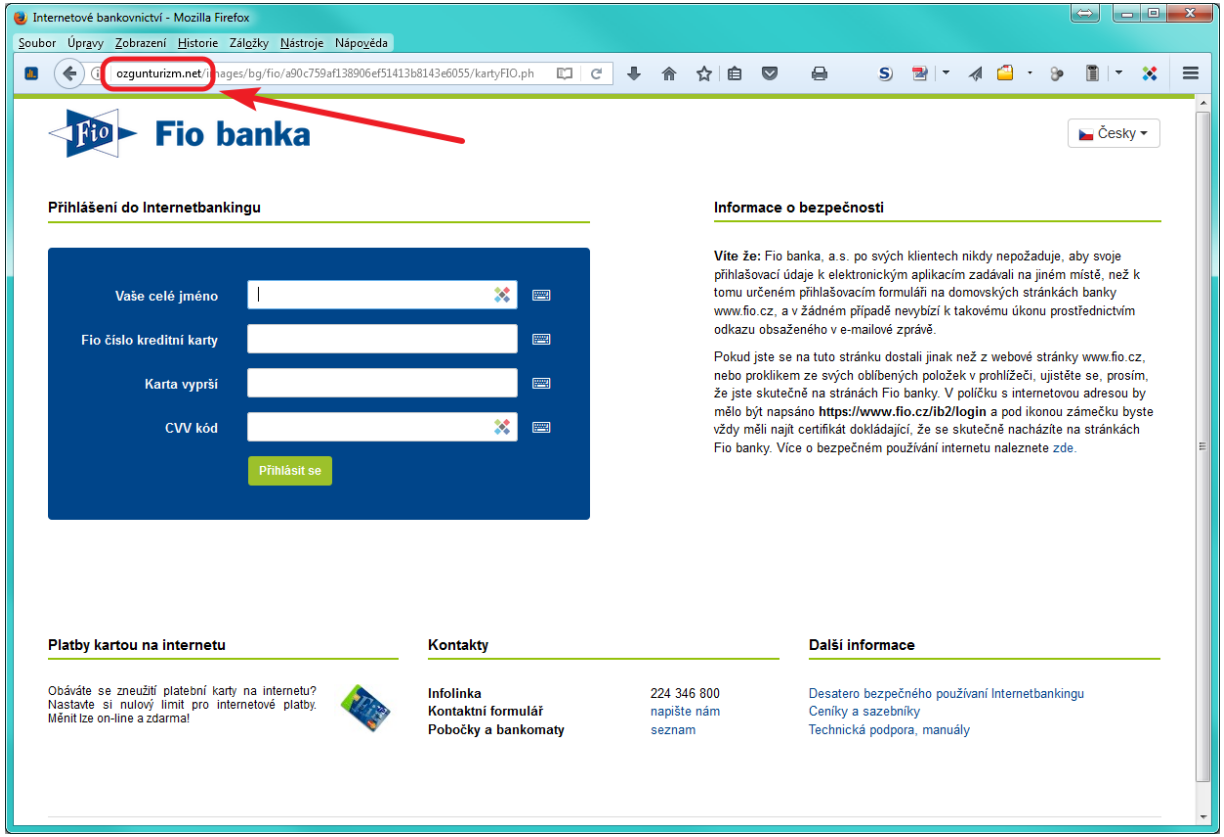
Falešná stránka – vzhled stejný, ale jiná adresa

ozgunturizm.net/image/blabla



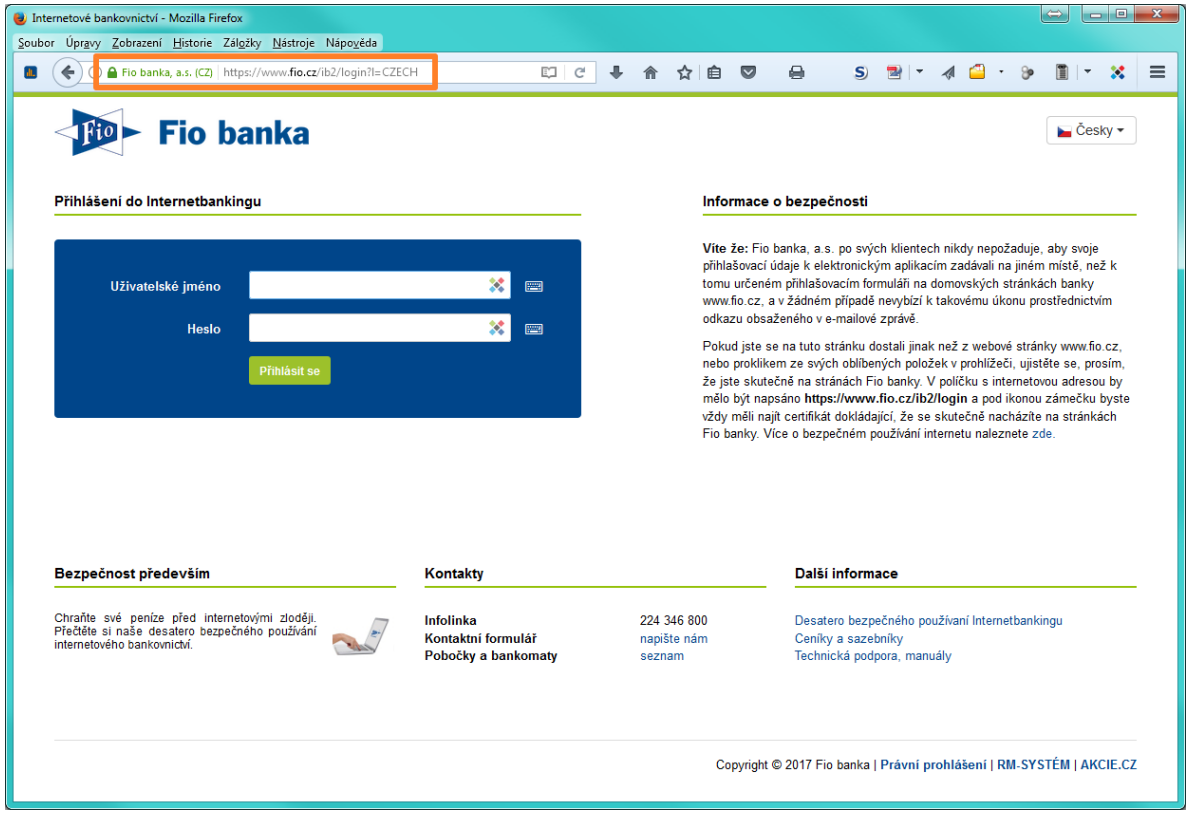
Falešná stránka – vzhled stejný, ale jiná adresa

Útočníci požadují důležité údaje k platební kartě



PHISHING – hotovo, přechod na pravé stránky

Pravé stránky banky

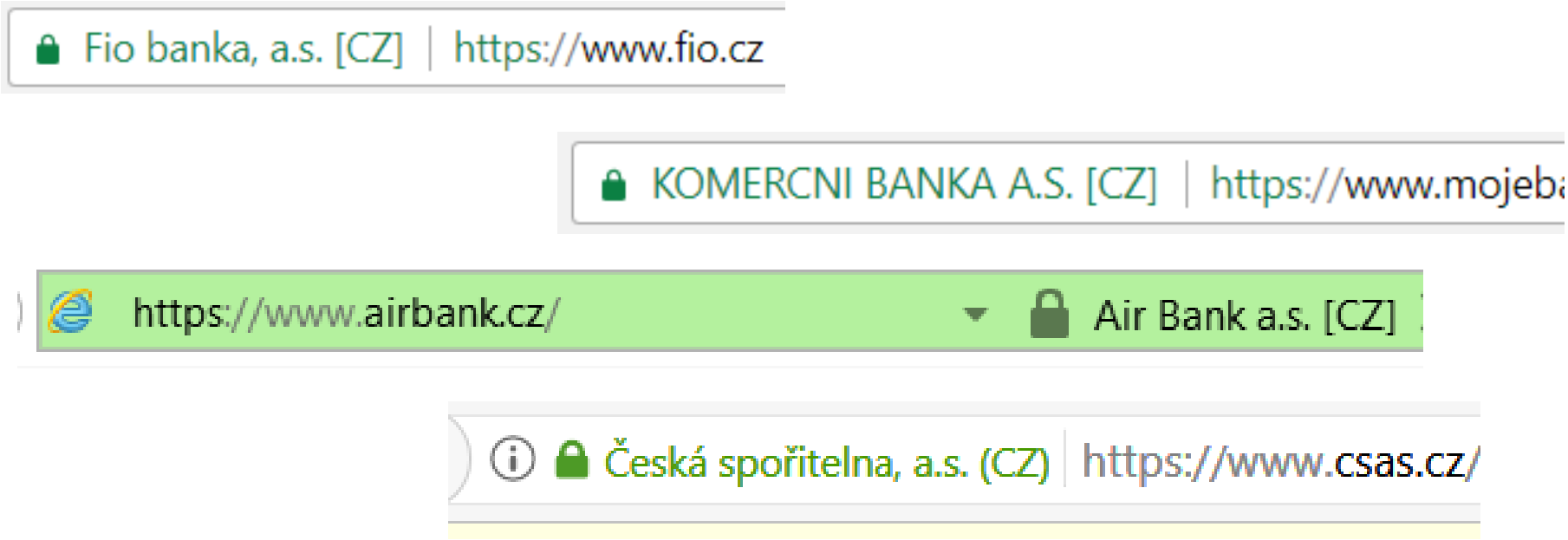


PHISHING - jak se bránit

- Neklikejte na odkazy v e-mailu!
- Adresu stránek raději napište ručně
- Dejte pozor na překlepy
- Pokud se vaše elektronické bankovnictví chová nestandardně zpozorněte, kontaktujte podporu
- Používejte aktualizovaný OS a SW
- Používejte důvěryhodný počítač

PHISHING - jak se bránit

Komunikace mezi počítačem a bankou probíhá zabezpečeným připojením: https://



PODVODNÉ LOTERIE

- Na e-mailové adresy jsou rozesílána oznámení o výhře, přestože se uživatel žádné loterie nezúčastnil
- Zaslání výhry je podmíněno zaplacením drobného poplatku
- A pak dalšího poplatku
- A dalšího...

Podvodné loterie – ukázka 1

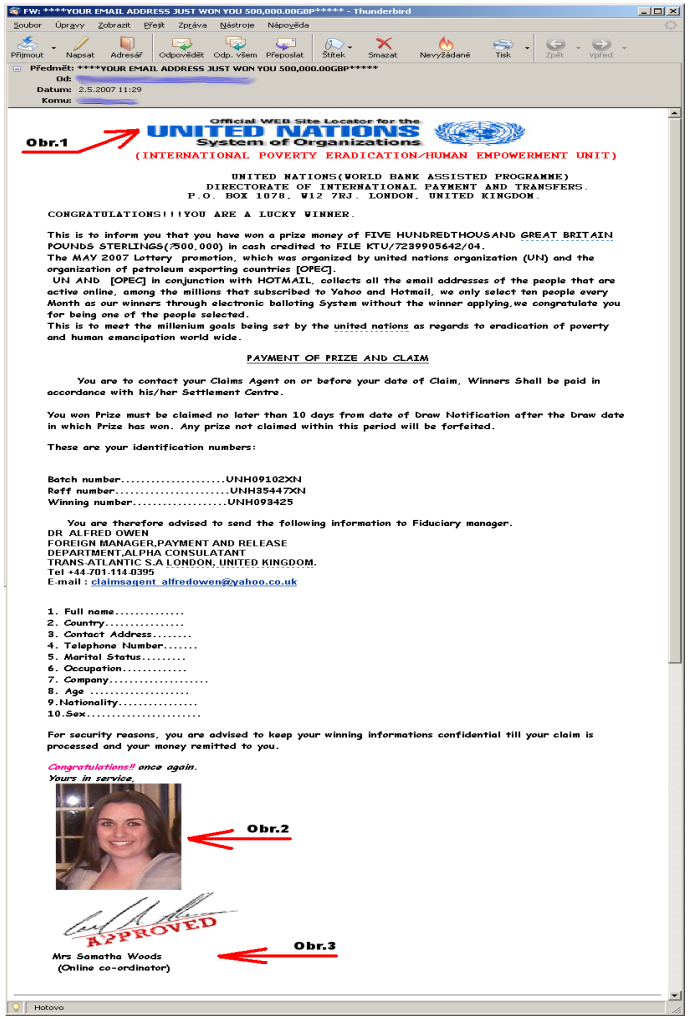
Od: UK Národní loterie DESKA

Předmět: Vaše e-mailová adresa Vyhrál

Tímto se oficiálne oznámit, že výsledek našeho pocítace cerpat 844 tohoto dne zvolený Vaše jméno a e-mailová adresa spojená s Ticket Number 034-22478556 s poradovým císlem 129, které následne vyhrála Velká Británie loterie hlavní cenu ocenení ve 2. category.You byly potvrzeny jako vítez kategorie B ve Spojeném království vylosuje pocítac loterie remíz. Vaše tvrzení soubor byl rádne predána do této funkce s pokyny, které jsme se pri manipulaci s prenosem svých cenu 1,000000.00 ? GBP. (One Million Velká Británie libra) nominován na váš úcet. Laskave poslat níže informace o pohledávky.

S pozdravem
Pan Dave Walker
Tell: +44***********
Mrdavewalker****@live.com**

Podvodné loterie – ukázka 2



FW: ****YOUR EMAIL ADDRESS JUST WON YOU 500,000.00GBP***** - Thunderbird

Soubor Úpravy Zobrazit Přejít Zpráva Nástroje Nápověda

Přijmout Napsat Adresář Odpovědět Odp. všem Přeposlat Štítek Smazat Nevyžádané Tisk Zpět Vpřed

Předmět: ****YOUR EMAIL ADDRESS JUST WON YOU 500,000.00GBP*****
Od:
Datum: 2.5.2007 11:29
Komu:

Obr.1

Official WEB Site Locator for the
UNITED NATIONS
System of Organizations

(INTERNATIONAL POVERTY ERADICATION/HUMAN EMPOWERMENT UNIT)

UNITED NATIONS(WORLD BANK ASSISTED PROGRAMME)
DIRECTORATE OF INTERNATIONAL PAYMENT AND TRANSFERS.
P.O. BOX 1078. W12 7RJ. LONDON. UNITED KINGDOM.

CONGRATULATIONS!!!YOU ARE A LUCKY WINNER.

This is to inform you that you have won a prize money of FIVE HUNDREDTHOUSAND GREAT BRITAIN POUNDS STERLINGS(/500,000) in cash credited to FILE KTU/7239905642/04.
The MAY 2007 Lottery promotion, which was organized by united nations organization (UN) and the organization of petroleum exporting countries [OPEC].
UN AND [OPEC] in conjunction with HOTMAIL, collects all the email addresses of the people that are active online, among the millions that subscribed to Yahoo and Hotmail, we only select ten people every Month as our winners through electronic balloting System without the winner applying,we congratulate you for being one of the people selected.
This is to meet the millenium goals being set by the united nations as regards to eradication of poverty and human emancipation world wide.

PAYMENT OF PRIZE AND CLAIM

You are to contact your Claims Agent on or before your date of Claim, Winners Shall be paid in accordance with his/her Settlement Centre.

You won Prize must be claimed no later than 10 days from date of Draw Notification after the Draw date in which Prize has won. Any prize not claimed within this period will be forfeited.

These are your identification numbers:

Batch number.....UNH09102XN
Reff number.....UNH35447XN
Winning number.....UNH093425

You are therefore advised to send the following information to Fiduciary manager.
DR ALFRED OWEN
FOREIGN MANAGER,PAYMENT AND RELEASE
DEPARTMENT,ALPHA CONSULATANT
TRANS-ATLANTIC S.A LONDON, UNITED KINGDOM.
Tel +44-701-114-0395
E-mail : claimsagent_alfredowen@yahoo.co.uk

1. Full name.....
2. Country.....
3. Contact Address.....
4. Telephone Number.....
5. Marital Status.....
6. Occupation.....
7. Company.....
8. Age .....
9.Nationality.....
10.Sex.....

For security reasons, you are advised to keep your winning informations confidential till your claim is processed and your money remitted to you.

Congratulations!! once again.
Yours in service,

Obr.2

APPROVED

Mrs Samatha Woods
(Online co-ordinator)

Obr.3

Hotovo

FW: ****YOUR EMAIL ADDRESS JUST WON YOU 500,000.00GBP***** - Thunderbird

Soubor Úpravy Zobrazit Přejít Zpráva Nástroje Nápověda

Přijmout Napsat Adresář Odpovědět Odp. všem Přeposlat Štítek Smazat Nevyžádané Tisk Zpět Vpřed

Předmět: ****YOUR EMAIL ADDRESS JUST WON YOU 500,000.00GBP*****
Od: [redacted]
Datum: 2.5.2007 11:29
Komu: [redacted]

Obr.1

Official WEB Site Locator for the
UNITED NATIONS
System of Organizations

(INTERNATIONAL POVERTY ERADICATION/HUMAN EMPOWERMENT UNIT)

UNITED NATIONS(WORLD BANK ASSISTED PROGRAMME)
DIRECTORATE OF INTERNATIONAL PAYMENT AND TRANSFERS.
P.O. BOX 1078, W12 7RJ. LONDON, UNITED KINGDOM.

CONGRATULATIONS!!!YOU ARE A LUCKY WINNER.

This is to inform you that you have won a prize money of FIVE HUNDREDTHOUSAND GREAT BRITAIN POUNDS STERLINGS(£500,000) in cash credited to FILE KTU/7239905642/04.
The MAY 2007 Lottery promotion, which was organized by united nations organization (UN) and the organization of petroleum exporting countries [OPEC].
UN AND [OPEC] in conjunction with HOTMAIL, collects all the email addresses of the people that are active online, among the millions that subscribed to Yahoo and Hotmail, we only select ten people every Month as our winners through electronic balloting System without the winner applying,we congratulate you for being one of the people selected.
This is to meet the millenium goals being set by the united nations as regards to eradication of poverty and human emancipation world wide.

PAYMENT OF PRIZE AND CLAIM

You are to contact your Claims Agent on or before your date of Claim, Winners Shall be paid in accordance with his/her Settlement Centre.

You won Prize must be claimed no later than 10 days from date of Draw Notification after the Draw date in which Prize has won. Any prize not claimed within this period will be forfeited.

These are your identification numbers:

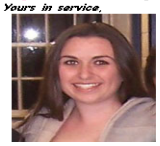
Batch number.....UNH09102XN
Reff number.....UNH35447XN
Winning number.....UNH093425

You are therefore advised to send the following information to Fiduciary manager.
DR ALFRED OWEN
FOREIGN MANAGER,PAYMENT AND RELEASE
DEPARTMENT,ALPHA CONSULATANT
TRANS-ATLANTIC S.A LONDON, UNITED KINGDOM.
Tel +44-701-114-0395
E-mail : claimsagent_alfredowen@yahoo.co.uk

1. Full name.....
2. Country.....
3. Contact Address.....
4. Telephone Number.....
5. Marital Status.....
6. Occupation.....
7. Company.....
8. Age .....
9.Nationality.....
10.Sex.....

For security reasons, you are advised to keep your winning informations confidential till your claim is processed and your money remitted to you.

Congratulations!! once again.
Yours in service,



Obr.2

APPROVED

Mrs Samatha Woods
(Online co-ordinator)

Obr.3

Hotovo

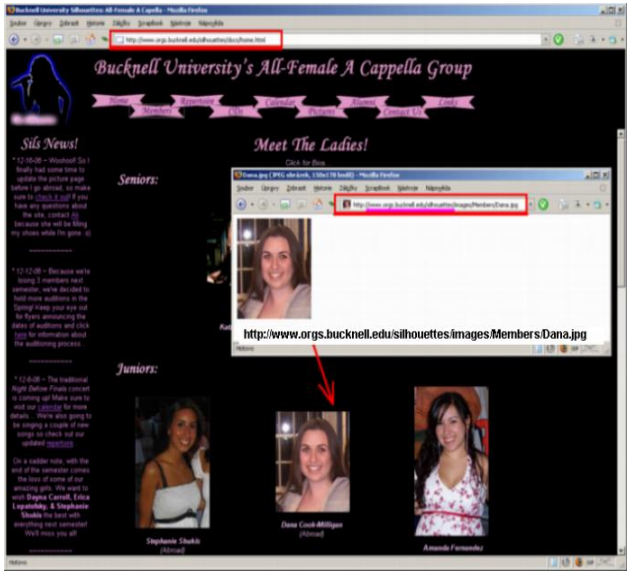
un.locator.en.small.300.gif (GIF obrázek, 300x79 bodů) - Mozilla Firefox

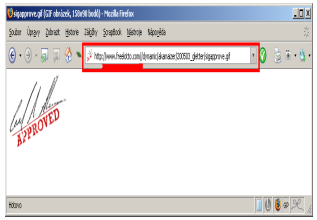
Soubor Úpravy Zobrazit Historie Záložky ScrapBook Nástroje Nápověda

http://www.unsystem.org/~CRES/images/un.locator.en.small.300.gif

Official WEB Site Locator for the
UNITED NATIONS
System of Organizations

Hotovo



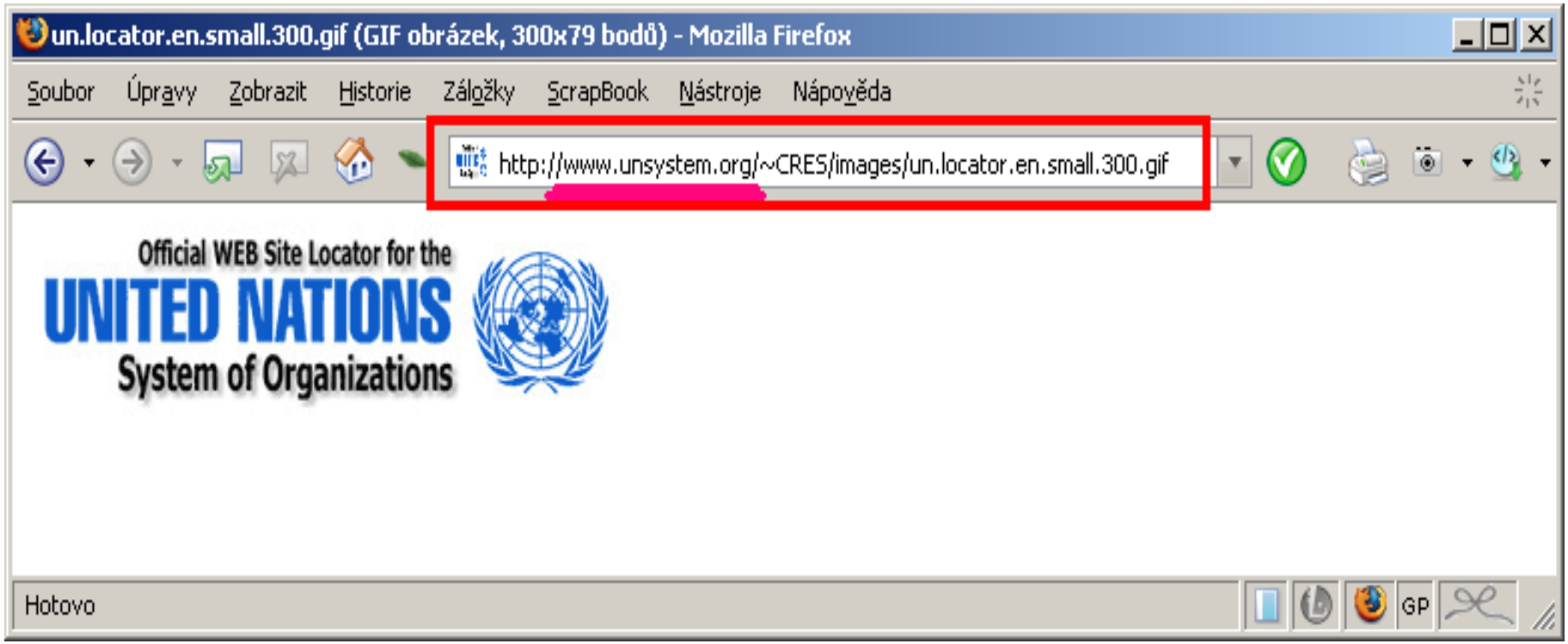


Odvrácená tvář elektronické komunikace 27.3.2018

HO@X

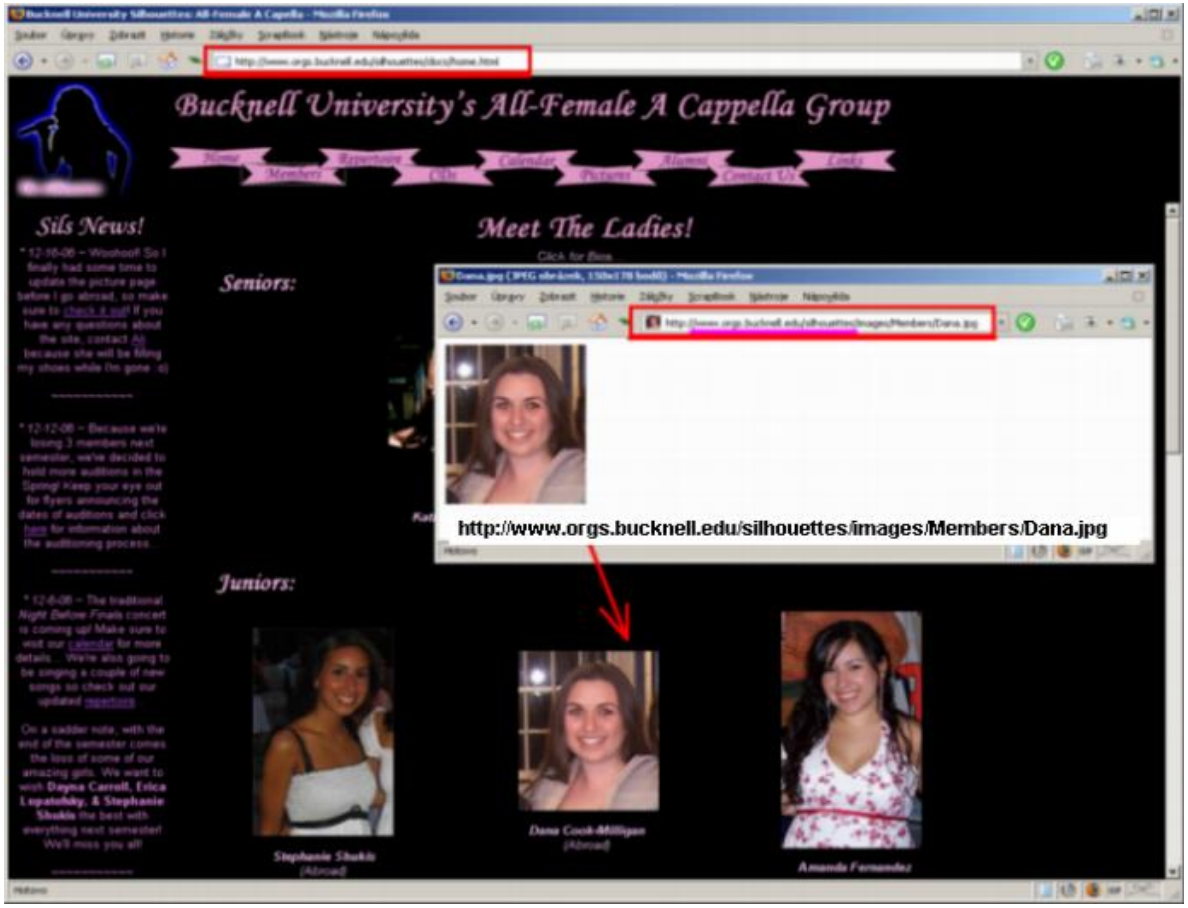
Podvodné loterie – ukázka 2

Zdroj obrázku v záhlaví - logo



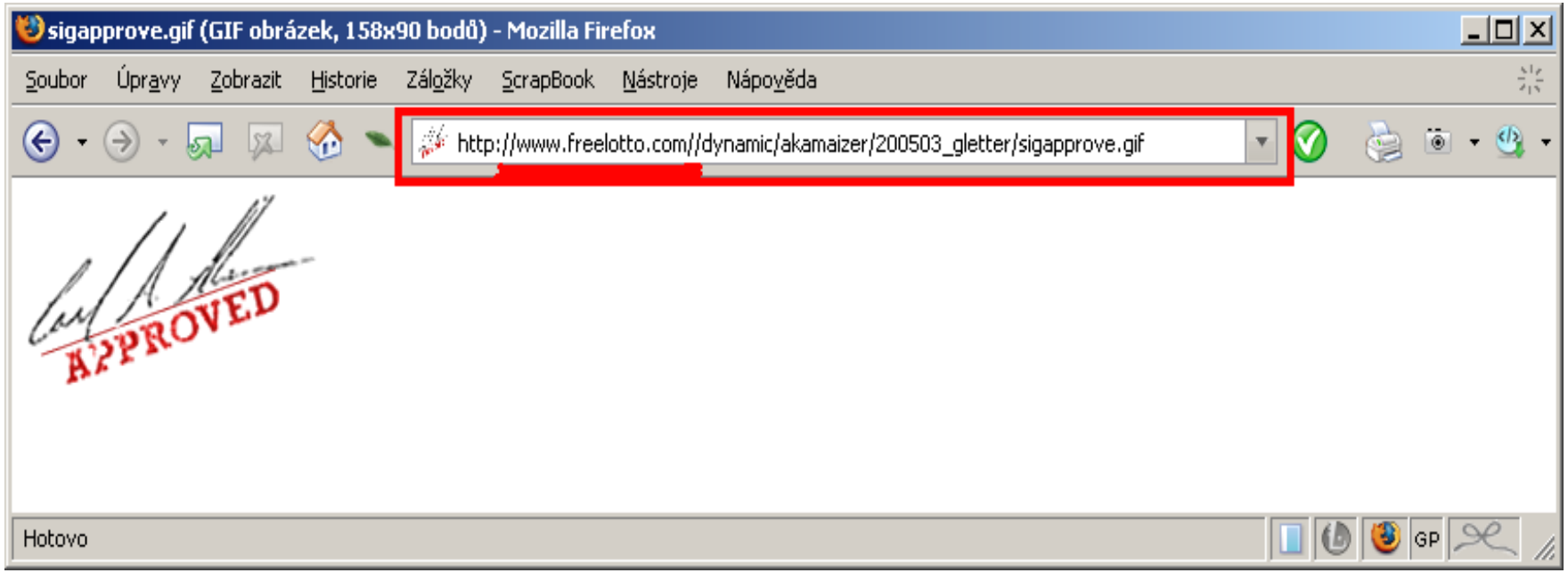
Podvodné loterie – ukázka 2

Zdroj obrázku údajné ředitelky loterie



Podvodné loterie – ukázka 2

Zdroj obrázku s podpisem



SCAM 419

Nigerijské podvodné e-maily

Scam = podvod

419 = §419 nigerijského zákoníku

SCAM 419

Princip podvodu je znám několik století

- Náhodné nebo vytipované oběti je slíbena velká odměna
- Aby bylo možné peníze získat, je potřeba malý poplatek
- Objevují se komplikace a je nutné platit nové výdaje

SCAM 419

Nejčastější scénáře

- *Dědictví po bohatém příbuzném z ciziny*
- *Vdova po milionářovi prosí o pomoc při převodu majetku z exotické země*
- *Bankovní úředník hledá falešného dědice*
- *Falešné inzeráty (automobily, pronájmy nemovitostí)*

SCAM 419

- Podvodníci poskytnou jakékoliv požadované dokumenty *falešné nebo získané od jiných důvěřivců*

- Připraveny jsou falešné stránky úřadů, bank a společností

- Oběti jsou nuceni platit další poplatky *buď pod vidinou zisku nebo je jim vyhrožováno*

SCAM419 – tisková zpráva POLICIE ČR

policie.cz

Chtěla být fiktivní dědičkou a přišla o 617.571 korun.

Jindřichův Hradec – Podvodné vylákání peněz přes internet.

Mladá žena z Jindřichova Hradce chtěla rychle zbohatnout bez jakékoliv vynaloženého úsilí a práce. Místo „zaručeného dědictví“ však přišla prostřednictvím internetu o celoživotní úspory. Fiktivní zpráva, kterou emailem obdržela zněla velmi lákavě.

http://www.policie.cz/clanek/chtela-byt-fiktivni-dedickou-a-prisla-o-617-571-korun.aspx

SCAM419 – popis případu

- Pachatel z účtu patchanprivacy004@yahoo.com poslal zprávu a představil jako Patrik Chan, zaměstnanec banky

- Údajně měl bohatého klienta Musa Omara Numana, který před šesti lety zemřel a zůstala po něm finanční částka 22.500.000,-USD

- Bance se nepodařilo zjistit žádnou příbuznou osobu, proto požádal Patrik Chan poškozenou, aby by se vydávala za jeho příbuznou a získala by 30% z částky

- Mladá žena kontaktovala doporučeného Pietera Rodolfa, který jí následně založil fiktivní účet u neexistující banky v Nizozemí

SCAM419 – popis případu

- Prostřednictvím účelově založených webových stránek vzbudili dojem, že účet skutečně existuje a přes internet ho i ovládá
- Pod různými záminkami vylákali 3.900 USD
- Podvodníci sdělili, že převodli částku 22.500.000 USD a na fiktivním webu tento převod byl zaznamenán
- Další požadovaný poplatek bylo údajné osvobození od daně ve výši 29.250 USD
- Poslední poplatek za údajný antiteroristický kód pro převod ve výši 49.550.60 USD již neuhradila.

Nejčastější dotazy k podvodným e-mailům

Proč podvodníci oslovili zrovna mě?

- **Nevytipovali si přímo vás, ale náhodně rozesílají e-maily**

Jak získali moji e-mailovou adresu?

- **Z dostupných zdrojů:**
  - ***Zveřejněná na internetu***
  - ***Je na napadeném počítači***

Jak se mohu bránit?

- **Antispamový filtr**
- **Neklikat na odkazy v e-mailech**
- **Nereagovat na e-maily podvodníků!!!**

MALWARE

- Všeobecné označení pro škodlivý kód

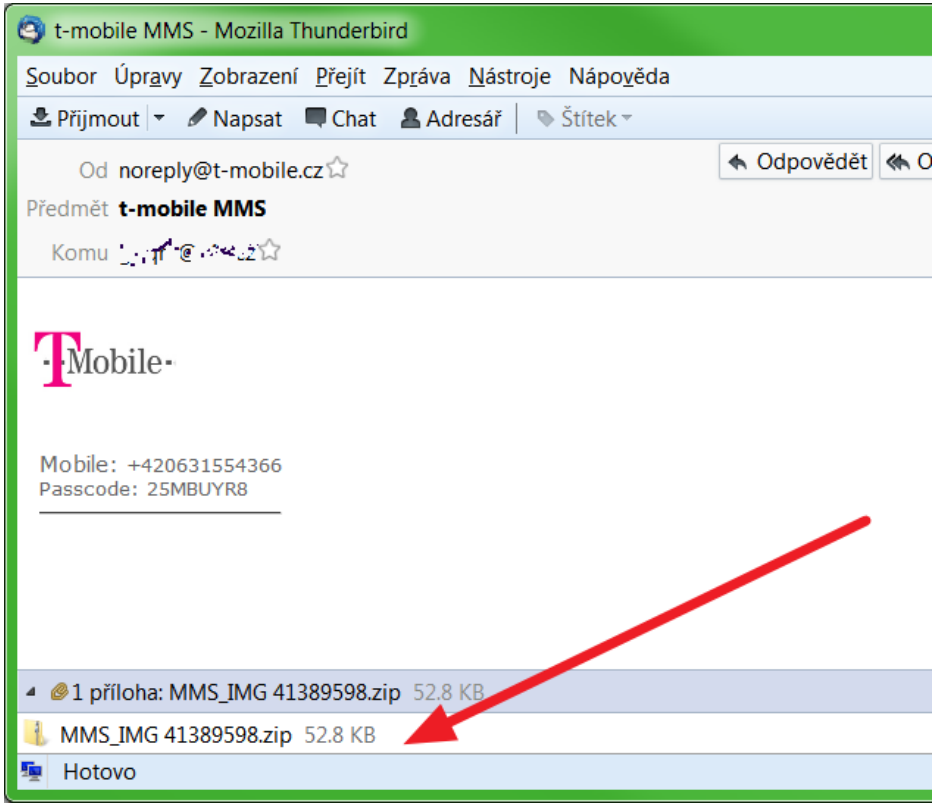
Trojský kůň, virus, spyware, ransomware, ... ***...havěť***

- Šíří se různými způsoby, také pomocí e-mailu

Melisa, I love you, ... ***...falešné exekuce***

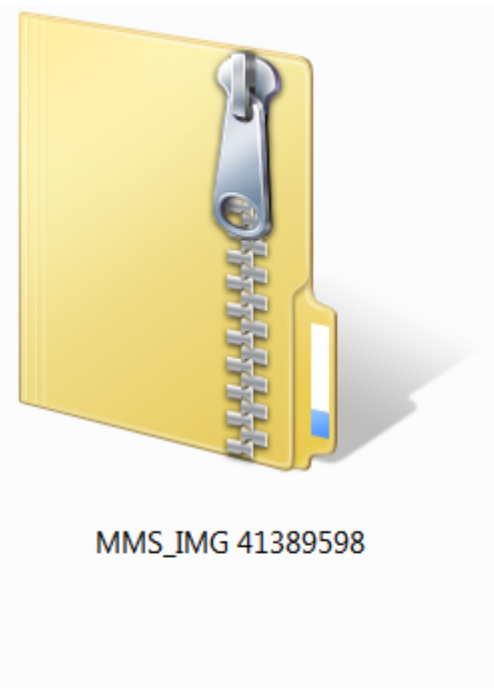
MALWARE (havěť) – ukázka 1

Podvodný e-mail s přílohou – jako zpráva s obrázkem

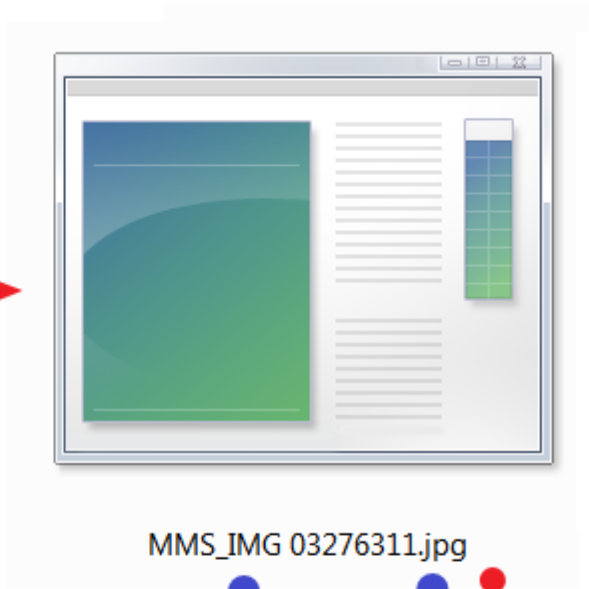


MALWARE (havěť) – ukázka 1

Místo obrázku je zabalena havěť



Po rozbalení jakoby obrázek



Skrytá přípona EXE
=
spustitelný soubor

MMS_IMG 03276311.jpg.exe

Není obrázek, ale program, který je možné spustit!

MALWARE (havěť) – ukázka 2

Exekuční příkaz 044970/2014-895 - Mozilla Thunderbird

Soubor Úpravy Zobrazení Přejít Zpráva Nástroje Nápověda

Od Antonín Nikl <[redacted]@[redacted].cz>

Odpovědět Přeposlat Archivovat Nevyžádaná pošta Smazat

Předmět **Exekuční příkaz 044970/2014-895** 12:56

Komu [redacted] Další akce

EXEKUČNÍ PŘÍKAZ

Soudní exekutor JUDr. Dohnal, Antonín, Exekutorský úřad Jeseník mesto, IČ 52333403, se sídlem Otakara Březiny 330, 284 01 Jeseník
pověřený provedením exekuce: č.j. 89 EXE 229/2014 -22, a ustanovení: Příkaz č.j. 044970/2014-895 /Čen/G V.vyř.,
vás ve smyslu §46 odst. 6 z. č. 120/2001 Sb. (exekuční řád) v platném znění vyzývá k splnění výše uvedených povinností, které ukládá exekuční titul, jakož i povinnosti uhradit náklady exekuce a odměnu soudního exekutora, stejně ták, jako zálohu na náklady exekuce a odměnu soudního exekutora:

Peněžitý nárok oprávněného včetně nákladu k dnešnímu dni: 9 961,00 Kč
Záloha na odměnu exekutora (peněžité plnění): 1 756,00 Kč včetně DPH 21%
Náklady exekuce paušálem: 4 519,00 Kč včetně DPH 21%

Pro splnění veškerých povinností je třeba uhradit na účet soudního exekutora (č.ú. 733852682/6500, variabilní symbol 87645500, ČSOB a.s.), ve lhůtě 15 dnů od doručení této výzvy 16 236,00 Kč

Nebude-li uvedená částka uhrazena ve lhůtě 15 dnů od doručení této výzvy, bude i provedena exekuce majetku a/nebo zablokován bankovní účet povinného ve smyslu § 44a odst. 1 EŘ a podle § 47 odst. 4 EŘ. Až do okamžiku vymožení povinnosti.

Příkaz k úhradě, vyrozumění o zahájení exekuce a vypučet povinnosti najdete v přiložených souborech.

Za správnost vyhotovení Antonín Nikl

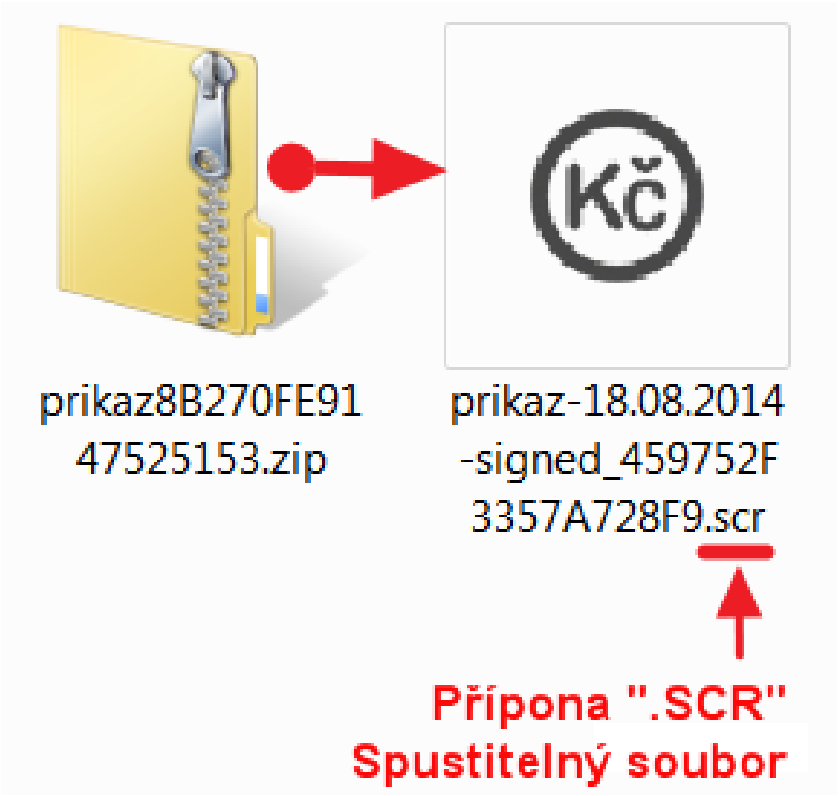
1 příloha: prikaz33169DD769B78346B.zip 64,8 KB Uložit

prikaz33169DD769B78346B.zip 64,8 KB

Žádné zprávy ke stažení

MALWARE (havěť) – ukázka 2

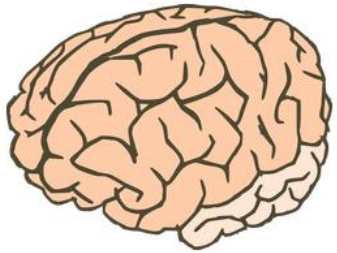
Příloha obsahuje místo dokumentu trojského koně



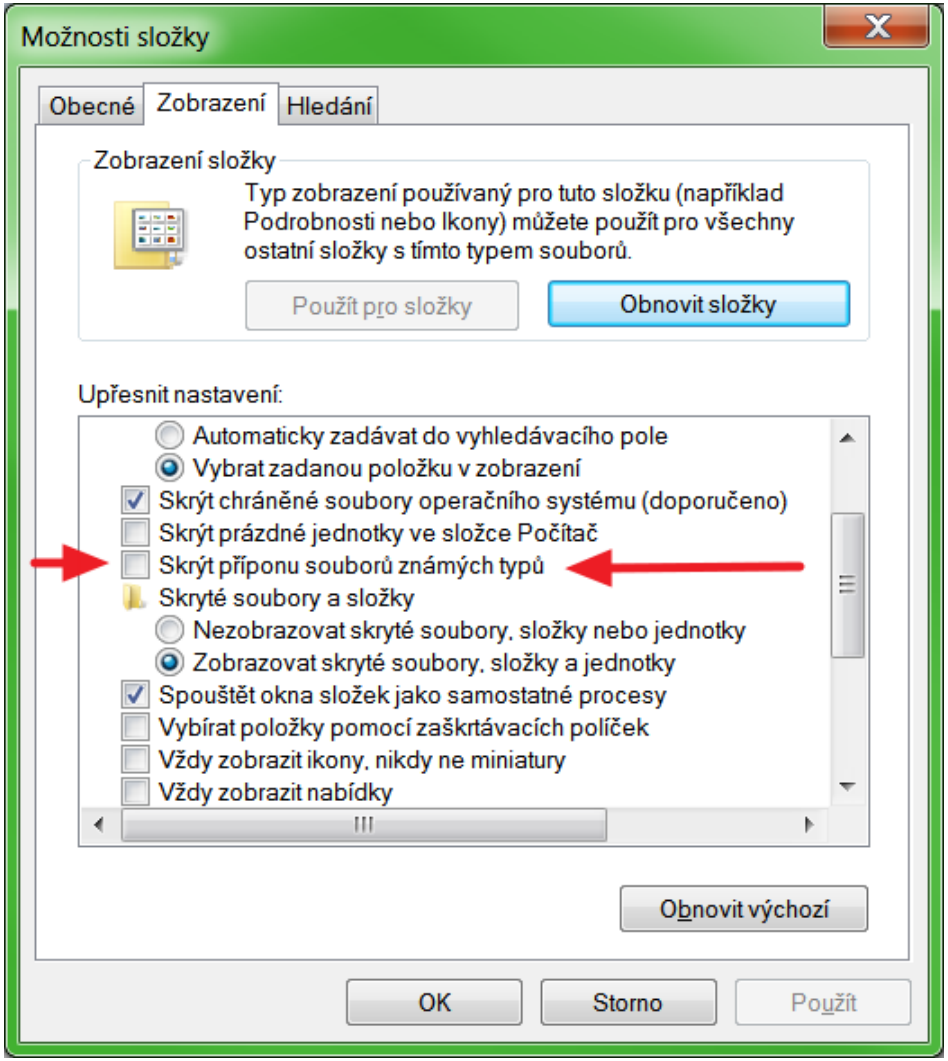
MALWARE - jak škodí

- Spyware
  - Získává hesla a přístupové údaje
- Zombie
  - Rozesílá spamy a šíří další havěť
- Ransomware
  - Šifruje data a požaduje výkupné

MALWARE - jak se bránit



- Buďte podezíraví
- Neotvírejte přílohy od neznámých lidí
- Přílohy od známých kontrolujte
- Dejte pozor na skryté přípony
- Používejte aktualizovaný OS a antivirový program
- Zálohujte!


Možnosti složky
Obecné
Zobrazení
Hledání
Zobrazení složky
Typ zobrazení používaný pro tuto složku (například Podrobnosti nebo Ikony) můžete použít pro všechny ostatní složky s tímto typem souborů.
Použít pro složky
Obnovit složky
Upřesnit nastavení:
Automaticky zadávat do vyhledávacího pole
Vybrat zadanou položku v zobrazení
Skrýt chráněné soubory operačního systému (doporučeno)
Skrýt prázdné jednotky ve složce Počítač
Skrýt příponu souborů známých typů
Skryté soubory a složky
Nezobrazovat skryté soubory, složky nebo jednotky
Zobrazovat skryté soubory, složky a jednotky
Spouštět okna složek jako samostatné procesy
Vybírat položky pomocí zaškrtávacích políček
Vždy zobrazit ikony, nikdy ne miniatury
Vždy zobrazit nabídky
Obnovit výchozí
OK
Storno
Použít

Podezřelé soubory lze kontrolovat www.virustotal.com

virustotal

VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

No file selected | Choose File

Maximum file size: 32MB

By clicking 'Scan it!', you consent to our Terms of Service and allow VirusTotal to share this file with the security community. See our Privacy Policy for details.

Scan it!

You may prefer to scan a URL or search through the VirusTotal dataset

English · Español · Français · Italiano · Português · Deutsch · Nederlands · Dansk
Русский · български език · Hrvatski · Српски · 日本語 · 한국어 · 中文 · فارسی

Výsledek testu podezřelého souboru

Firefox

Antivirus scan for 59d7939968214a1768...

Community Statistics Dokumentace FAQ About Česky Join our community Sign in

virustotal

SHA256: 1d79165e492c87a02a1cf43510206f2de572ed05ecb235e6d357cbdccb7ba9ac

File name: TT Bank Swift.zip

Detection ratio: 34 / 47

Analysis date: 2013-10-29 14:20:40 UTC (0 minut ago)

0 0

More details

Analysis | Additional information | Comments | Votes

Antivirus	Result	Update
Agnitum		20131028
AhnLab-V3	Trojan/Win32.Zbot	20131029
AntiVir	TR/Dropper.Gen	20131029
Antiy-AVL		20131029
Avast	AutoIt:Agent-ABD [Trj]	20131029
AVG	Autoit_c.PRY	20131029
Baidu-International	Trojan.Win32.Injector.Autoit.TX	20131029
BitDefender	Trojan.Autoit.BHS	20131029
Bkav	W32.MancamiLTAB.Trojan	20131029
ByteHero		20131028

Zálohujte!

Zálohujte!

Zálohujte!

CD / DVD

+ Data nelze neúmyslně přepsat

+ Lze skladovat v boxech

- Menší kapacita

- Mechanické poškození

Externí disk

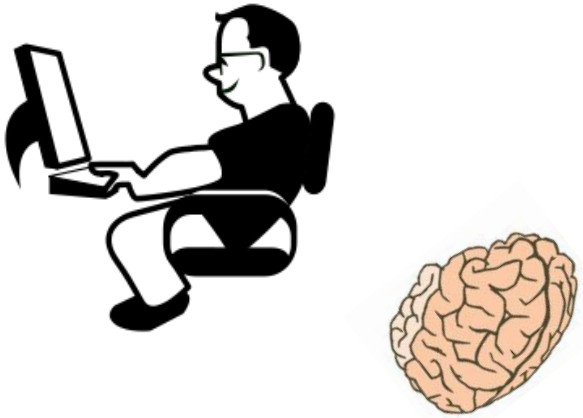
+ Data lze opakovaně přepisovat

+ Velká kapacita

- Data lze kdykoliv smazat

- Mechanické poškození

Nejslabší článek je vždy mezi klávesnicí a židlí!

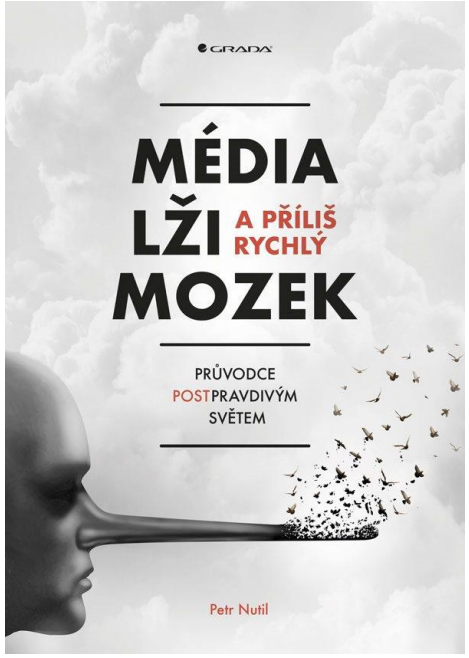


- Ne vše na internetu je pravdivé nebo nezkreslené
- Porovnávejte informace z různých zdrojů
- Prověřte zaměření a historii zdrojů informací

Kde najdu informace

HO@X
www.hoax.cz

Snopes.com
Rumor Has It



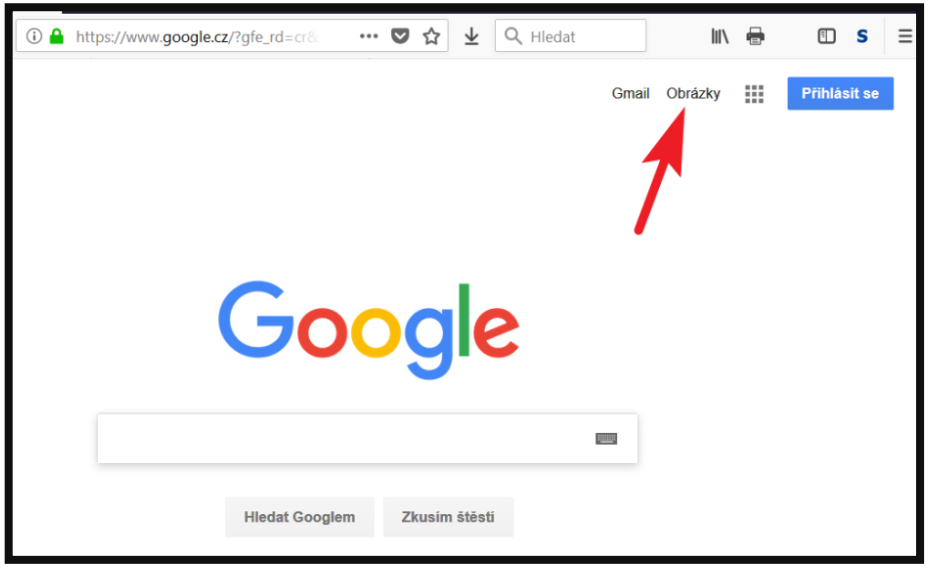
Google

bezpečí

Manipulátoři.cz

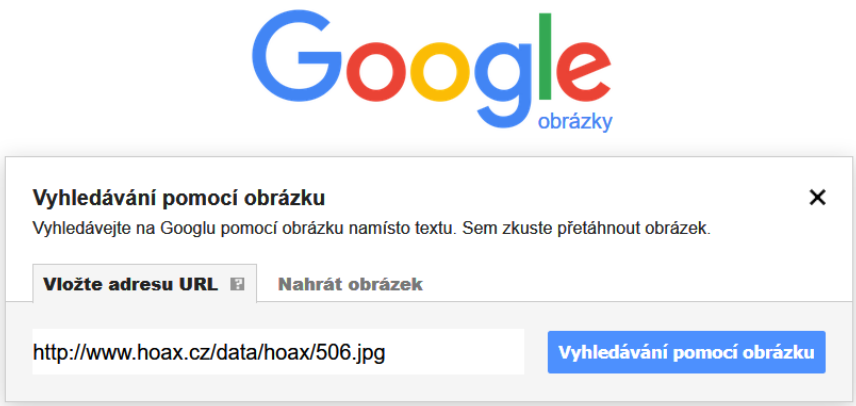
demagog.cz

A co obrázky?


https://www.google.cz/?gfe_rd=cr&
Hledat
Gmail
Obrázky
Přihlásit se
Google
Hledat Googlem
Zkusím štěstí

Google
obrázky

Vyhledávání obrázků Google



KÁVÉESKA
zážitky malé i velké

městská část
BRNO-STŘED

BOTANKA
centrum volného času

Děkuji za pozornost

Josef Džubák
dzubak@hoax.cz

HOAX
www.hoax.cz