

Josef Džubák

www.hoax.cz

H O A X - co to je?

[:houx:]

Slovo HOAX pochází z angličtiny

Vzniklo na konci 18. století

Zkrácení slova hocus = trik / podvádění / klamání

H O A X [:houx:]

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

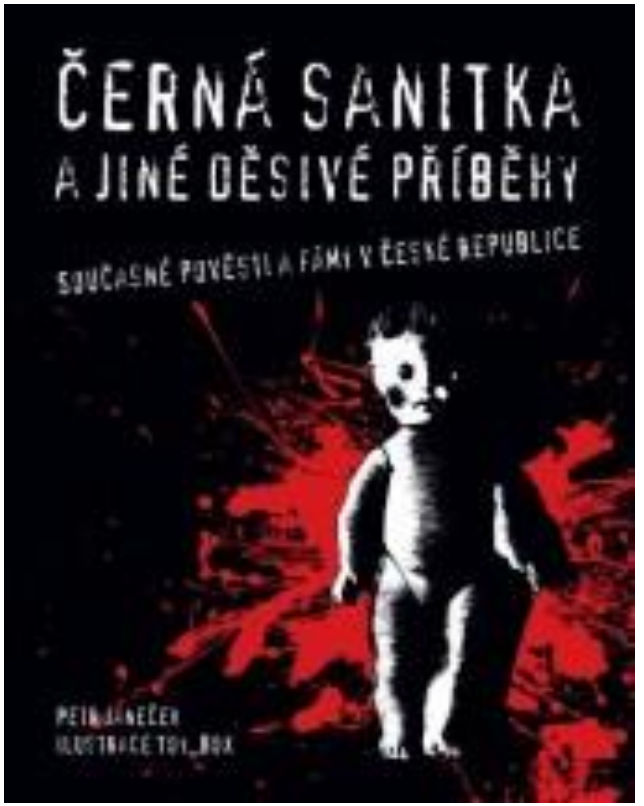


H O A X - před internetem

Po městě jezdí Černá sanitka a unáší lidi, aby jim sebrali orgány a prodali je na západ.

Darebáci dávají na plovárně žiletky do tobogánu a kdo se sklouzne, ten se šíleně pořeže.

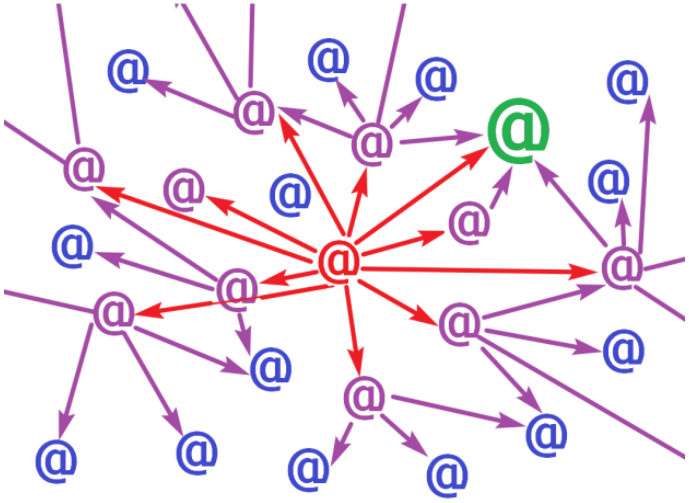
Tajemný stopař:
- ***duch, který zmizí z auta***
- ***zapomětlivý vrah s kufříkem***



„Zažila to kolegyně tetičky mé nejlepší kamarádky.“

HOAX a rychlost šíření

Technika zrychluje komunikací







HOAX - způsoby šíření

- E-mail
- Sociální sítě - Facebook, Twitter...
- Skype, Messenger...
- Diskuzní skupiny, komentáře k článkům
- Blogy
- Specializované (účelové) servery

HO@X

HO@X.CZ JE TU OD ROKU 2000

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
- MAPA PORTÁLU

REKLAMA

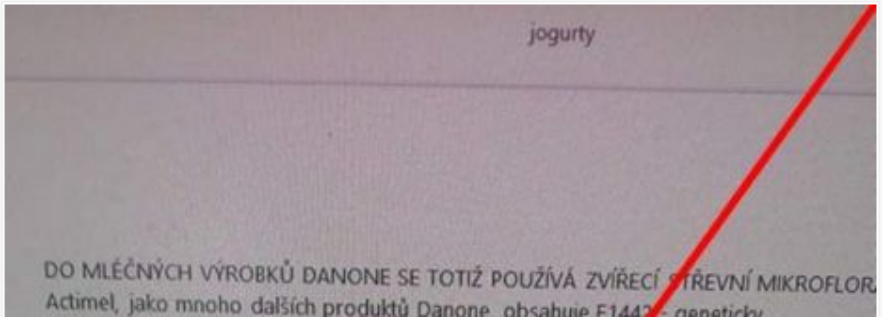
TOPTEN ČESKÝCH HOAXŮ A ŘETĚZOVÝCH ZPRÁV V MĚSÍCI LEDEN 2019

11.02.2019

FACEBOOK - automatické mazání neaktivních členů skupin
Nebezpečný moderní jogurt
Infikované jehly na sedadlech
Whatsapp Gold - Martinelli
Nepřímej telefonát od xy jsou to hekři
Recyklované mléko
Klíčenky s GPS
Zpoplatnění Facebooku
Víno za Tříkrálovou sbírku
Vejce na předním skle automobilu

Přílohy ke stažení

Stanovisko DANONE k fámě o jogurtech. Na posledních dvou stranách je i vyjádření citovaných osob, které se od hoaxu distancují. [7,2MB]



Naši partneři

NA PRAVDĚ ZÁLEŽÍ. | SECURITY | QuBit Conference PRAGUE 2019 | internetem BEZPEČNĚ | bezpečí | IGIHO STRÁNKA O VIRECH www.viry.cz | Manipulátoři.cz | hustej INTERNET.cz | NEŠLAPE.CZ vzdálená pomoc | PARANOIA | avast! be free

HOAX - témata šířených zpráv

- Fámy z virtuálního a reálného světa
- 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

HOAX - 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: Recyklované mléko

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: Recyklované mléko



ODPOVĚDI ODBORNÍKŮ

Čísla značí informaci o obalu a ne obsahu

„Recyklace“ by byla neekonomická

Znovu vracení mléka do oběhu by bylo nezákonné

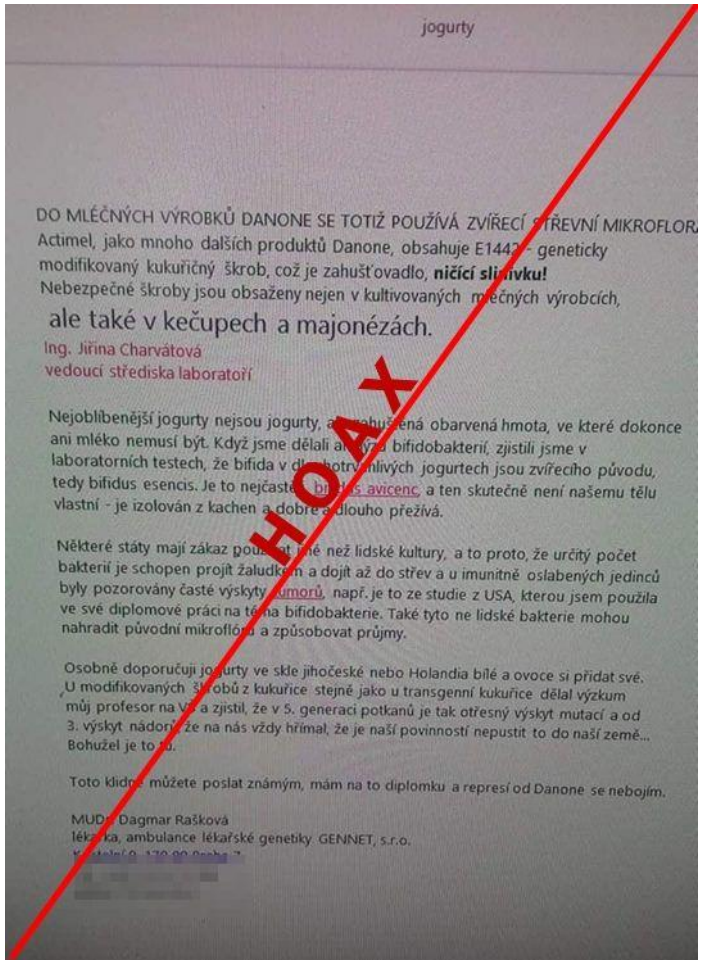
Fáma: Nebezpečný jogurt

Pošlete komu můžete!!!

POUŽÍVÁ SE "ZVÍŘECÍ" STŘEVNÍ MIKROFLORA DO MLÉČNÝCH VÝROBKŮ!

Nebezpečné škroby jsou obsaženy nejen v kultivovaných mléčných výrobcích, Ing. Jiřina Ch** vedoucí střediska**

Toto klidně můžete poslat známým, mám na to diplomku MUDr. Dagmar R*** Lékařka**



Fáma: Nebezpečný jogurt

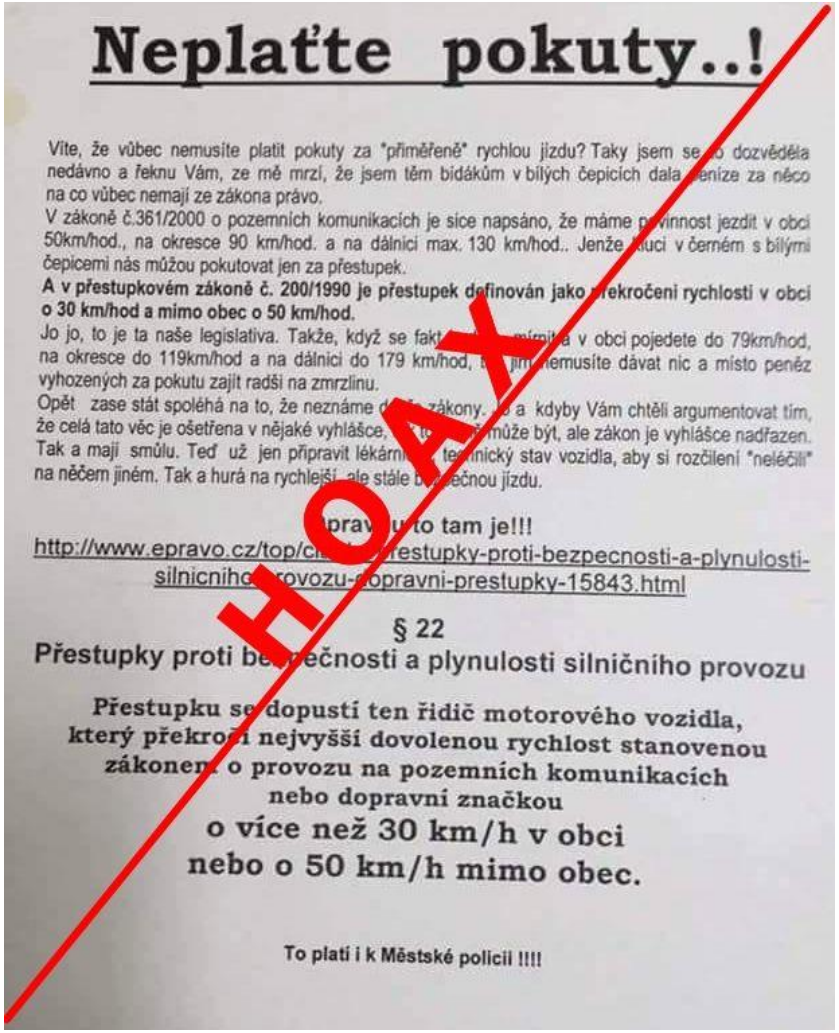


VYSVĚTLENÍ

Obě „citované“ osoby se od článku distancují

První verze z roku 2010

K hoaxu je mnohostránkový vysvětlující PDF dokument



Nepravdivý návod

nikdy neodpovídal realitě!

Hoax se šíří od roku 2004

V textu je citována pouze část §

Údajná díra je ošetřena

Zákon byl několikrát změněn

Zákon byl k 1.7.2017 nahrazen

Hoax se stále úspěšně šíří



STANOVISKO BANK

Zpráva je zcela nesmyslná.

Pouze správně zadaný PIN umožní provádět transakce platební kartou.

PIN kód zadaný odzadu, je chybný!

Co mají hoaxy společného

Snaží se přesvědčit svojí důležitostí

Nové nebezpečí, naléhavá pomoc, šokující informace

Údajný důvěryhodný zdroj

Microsoft varuje, Symantec objevil, laboratoř NASA zjistila

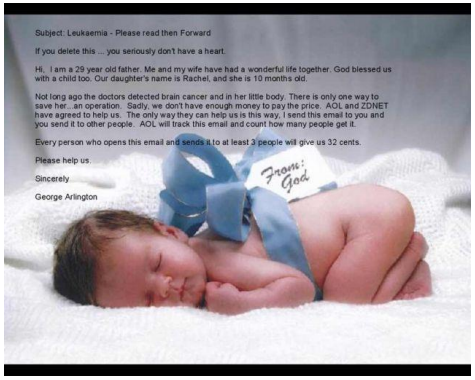
Výzva k dalšímu rozeslání !!!

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

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 a reálné prosby o pomoc
- Aktuální jsou 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

O víkendu jsem u silnice našla na pytli čtyři drobečky, kterých se nejspíš chtěl někdo zbavit, když si prohlídnete fotky v příloze...

...kdo by měl zájem o fenky, Tak se mi klidně ozvěte, mám je zatím doma...

Kontakt: J... N....
Telefon: 6.. 1... 9...



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)**

Lze se chránit před hoaxy?



Jak se bránit hoaxům

- Bez ověření skutečnosti a aktuálnosti neposílám!

- Má opravdu význam posílat zprávu všem?

- V případě, že nechci ověřovat, nerozesílám!!!

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

Jak může řetězový e-mail škodit

Stovky adres v kolujícím e-mailu nejsou výjimkou!



250 adres

Ne/Bezpečí ve světě médií

HOAX

Máme adresy, jdeme na PHISHING



P*assword*

H*arvesting*

*f*ISHING

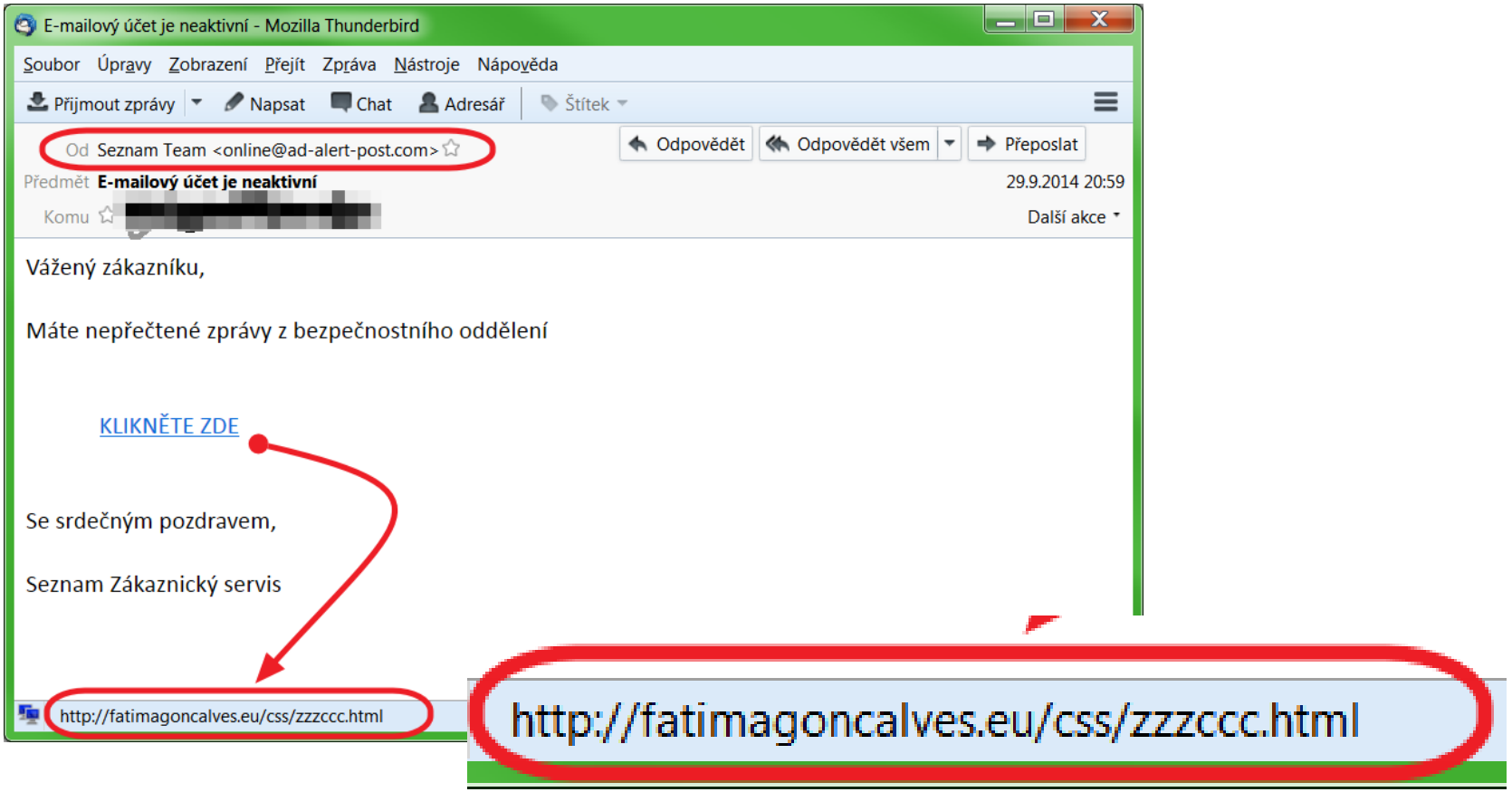


Sběr hesel r(h)ybařením

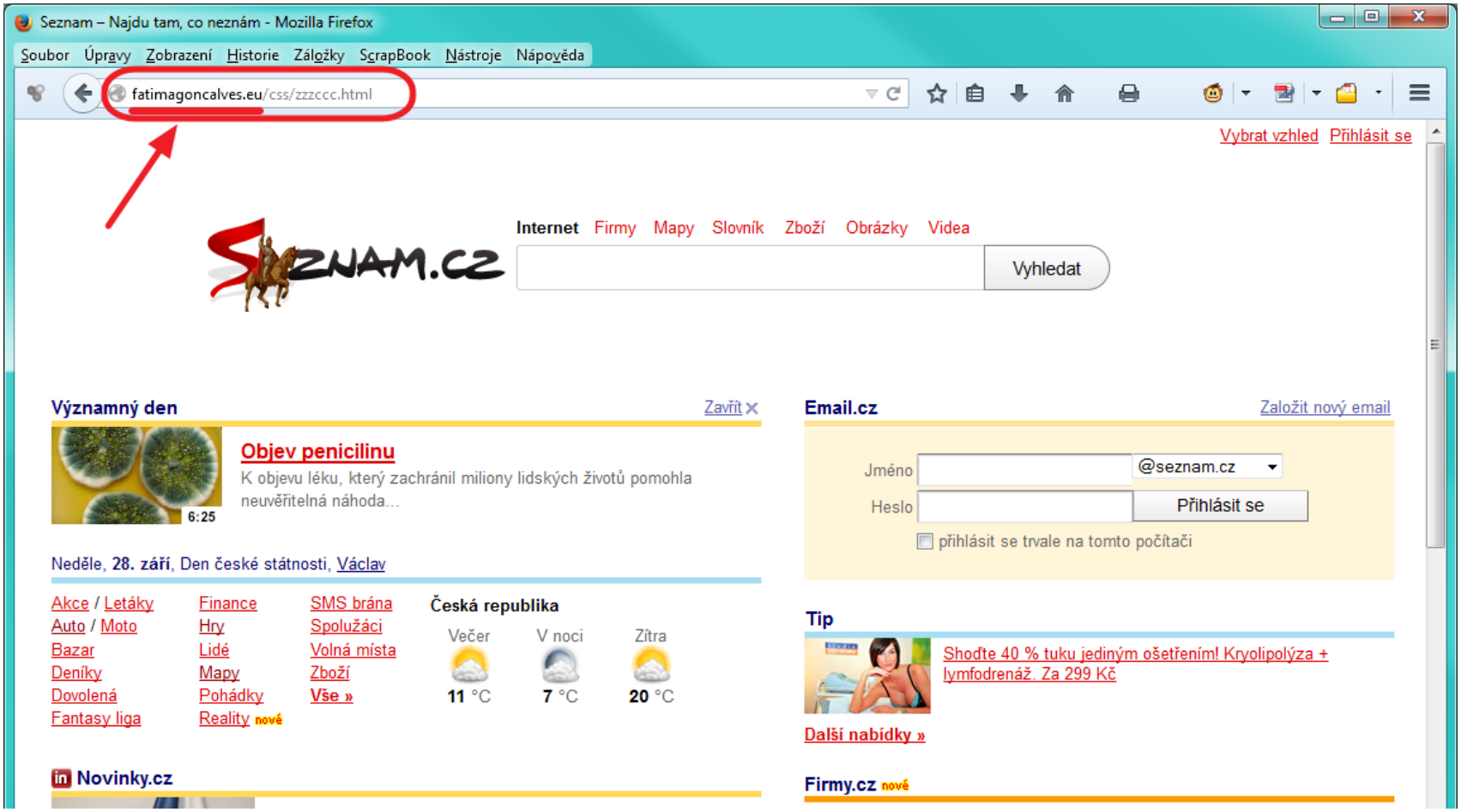
PHISHING

- 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

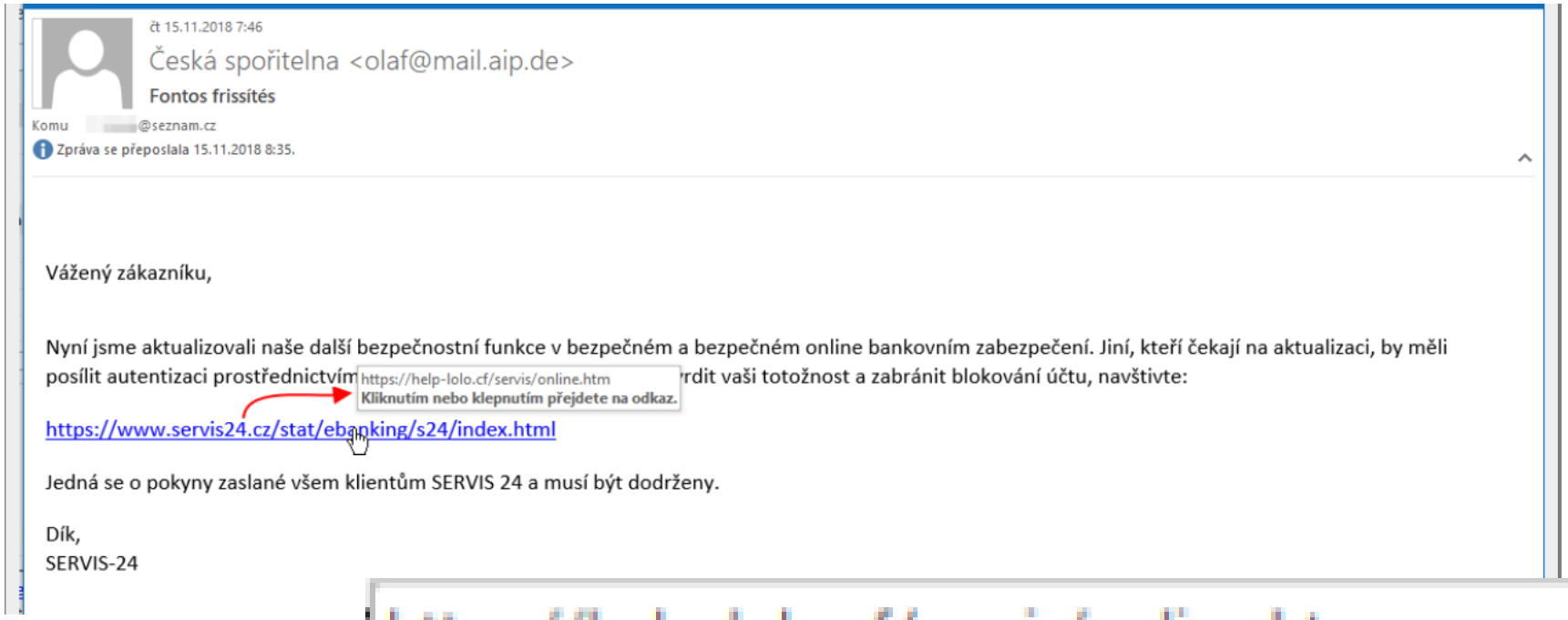
Podvodný e-mail s falešným odkazem



Falešná stránka s podvodným formulářem



Podvodný e-mail s falešným odkazem



čt 15.11.2018 7:46

Česká spořitelna <olaf@mail.aip.de>

Fontos frissítés

Komu @seznam.cz

Zpráva se přeposlala 15.11.2018 8:35.

Vážený zákazníku,

Nyní jsme aktualizovali naše další bezpečnostní funkce v bezpečném a bezpečném online bankovním zabezpečení. Jiní, kteří čekají na aktualizaci, by měli posílit autentizaci prostřednictvím rdit vaši totožnost a zabránit blokování účtu, navštivte:

https://help-lolo.cf/servis/online.htm
Kliknutím nebo klepnutím přejdete na odkaz.

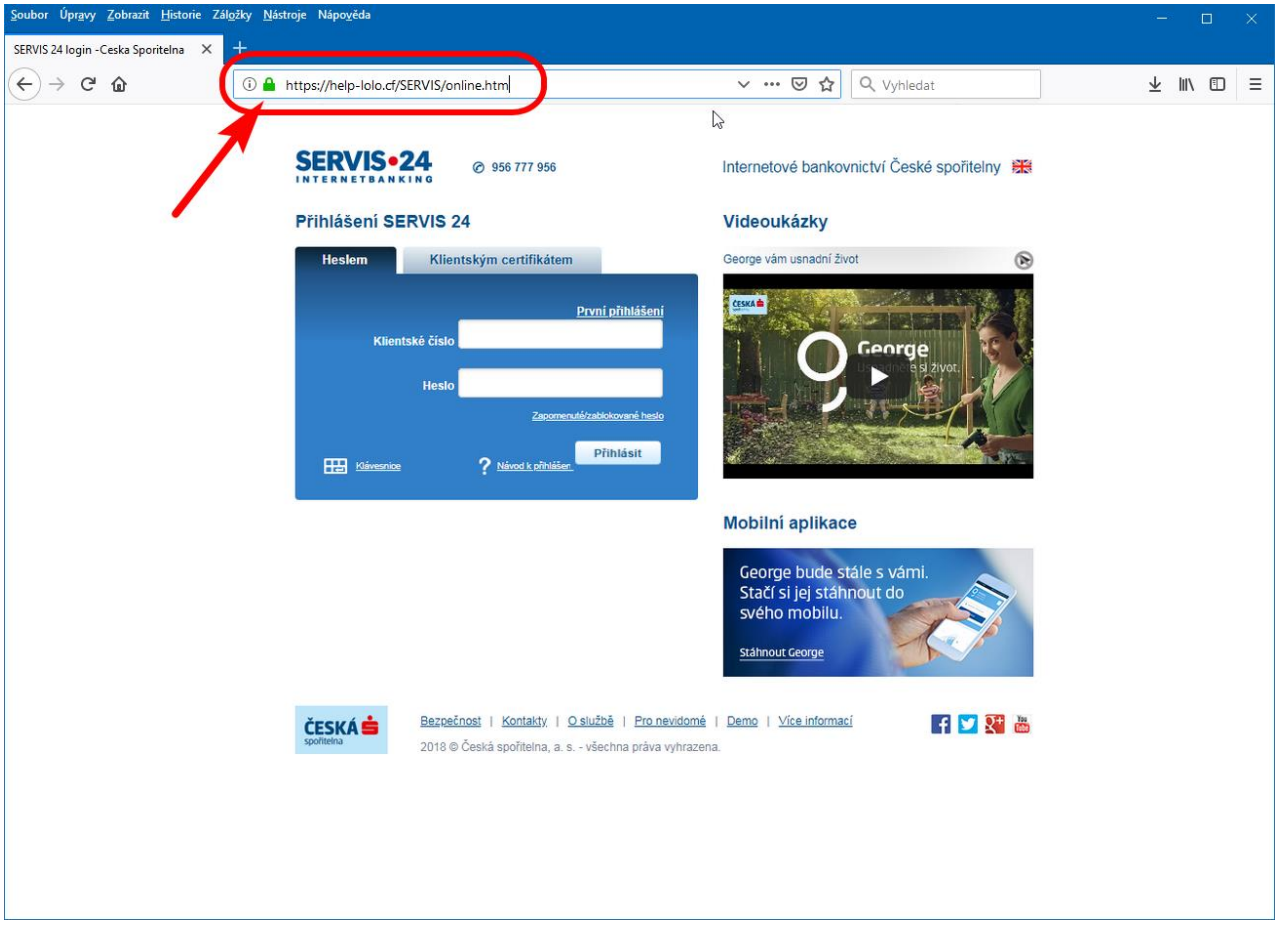
https://www.servis24.cz/stat/ebanking/s24/index.html

Jedná se o pokyny zaslané všem klientům SERVIS 24 a musí být dodrženy.

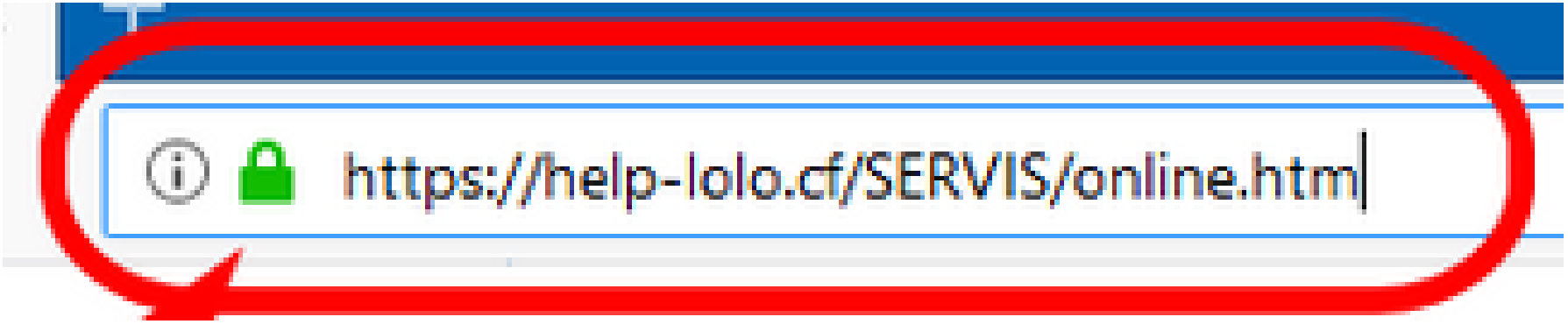
Dík,
SERVIS-24



Falešná stránka – vzhled stejný, ale jiná adresa



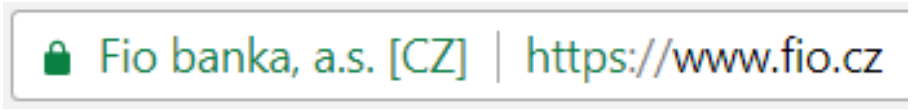
Falešná stránka – vzhled stejný, ale jiná adresa



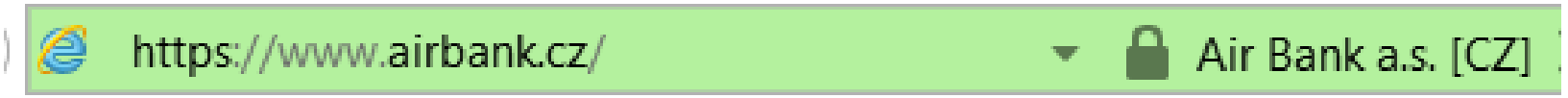
PHISHING - zámeček

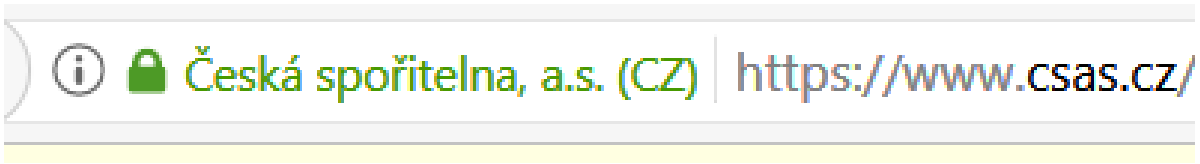
Zabezpečené připojení: https://

Zámeček nesmí chybět, ale není záruka

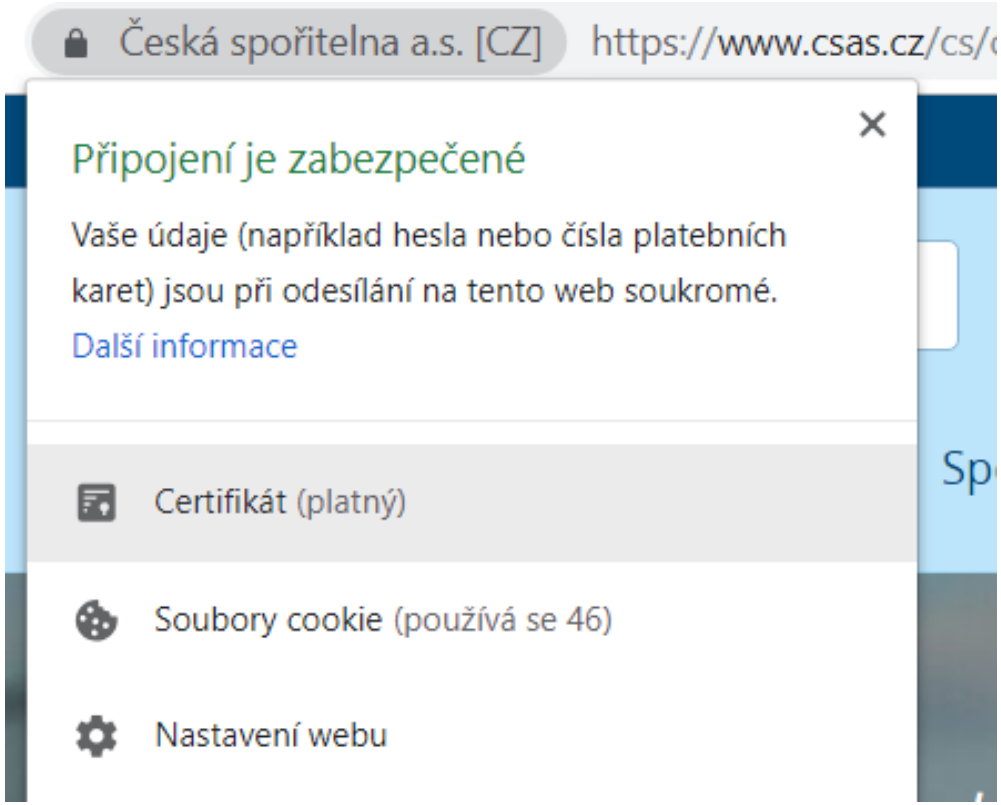


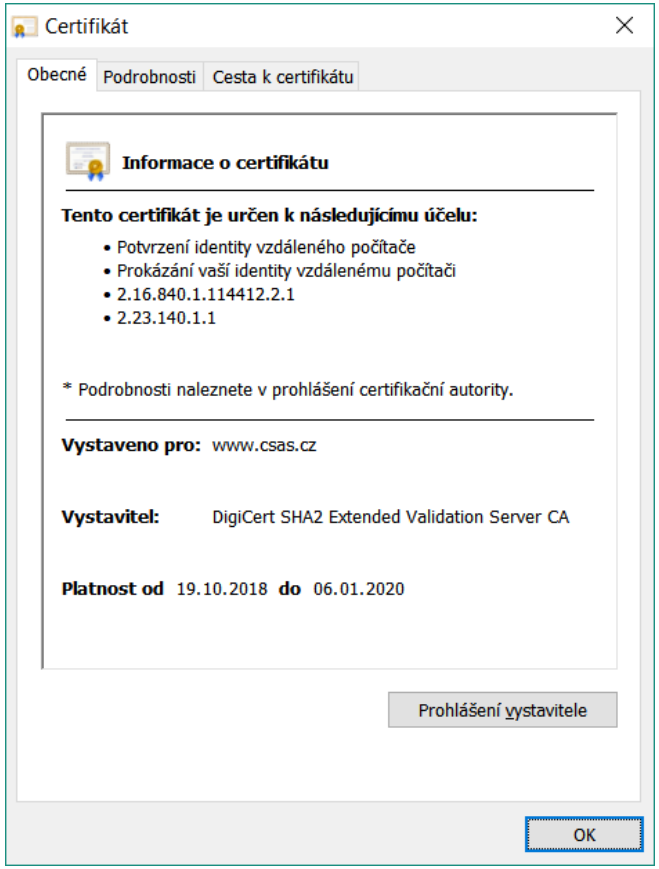




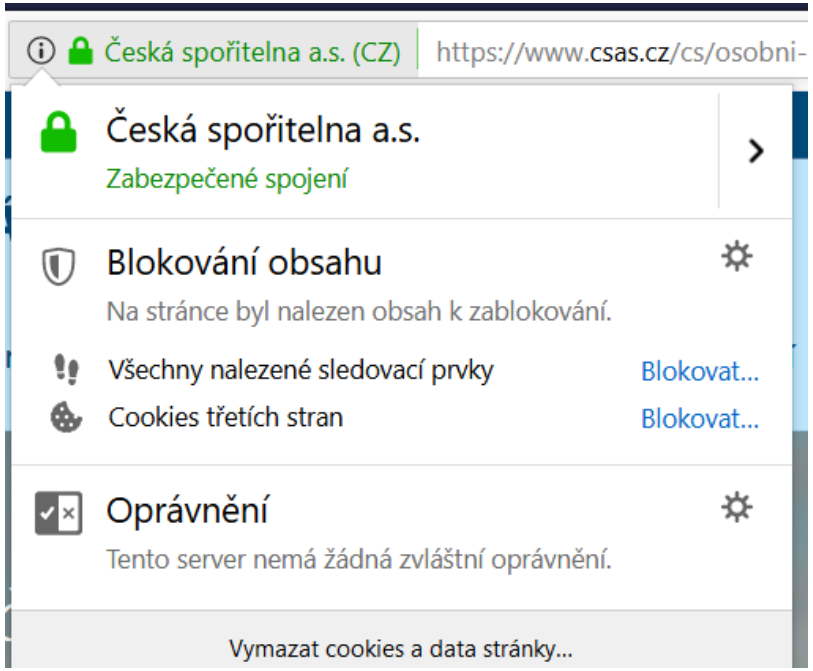


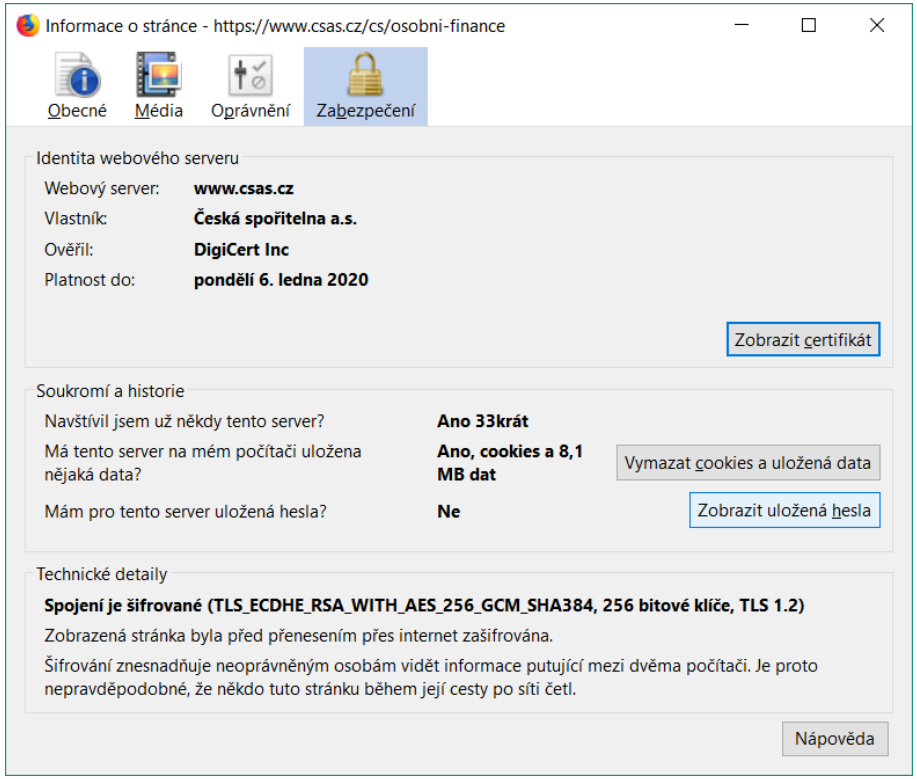
PHISHING - certifikát





PHISHING - certifikát





PHISHING - jak se bránit

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

PHISHING - jak se bránit

POZOR NA PŘEKLEPY A ZÁMĚNY PÍSMEN

www.facebok.cz	www.facebook.cz
www.seznarn.cz	www.seznam.cz
www.csas.cn	www.csas.cz

PODVODNÉ LOTERIE

- Na e-mailové adresy jsou rozeslána 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

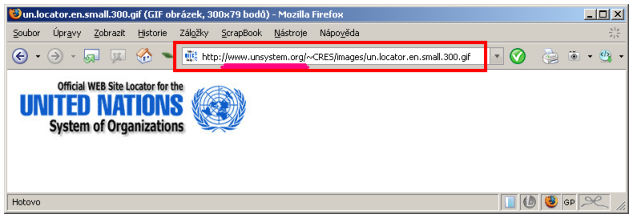
Tímto se oficiálne oznámit, že výsledek našeho pocítace cerpat 844 tohoto dne zvolený Vaše jméno a e-mailová adresa spojená s Ticket Number 034-22478556 s poradovým císlem 129, které následne vyhrála Velká Británie loterie hlavní cenu ocenení ve 2. category.You byly potvrzeny jako vítez kategorie B ve 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**

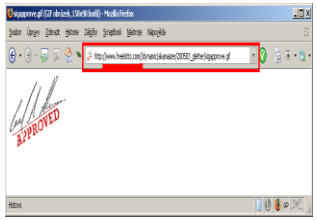
Podvodné loterie – ukázka 2







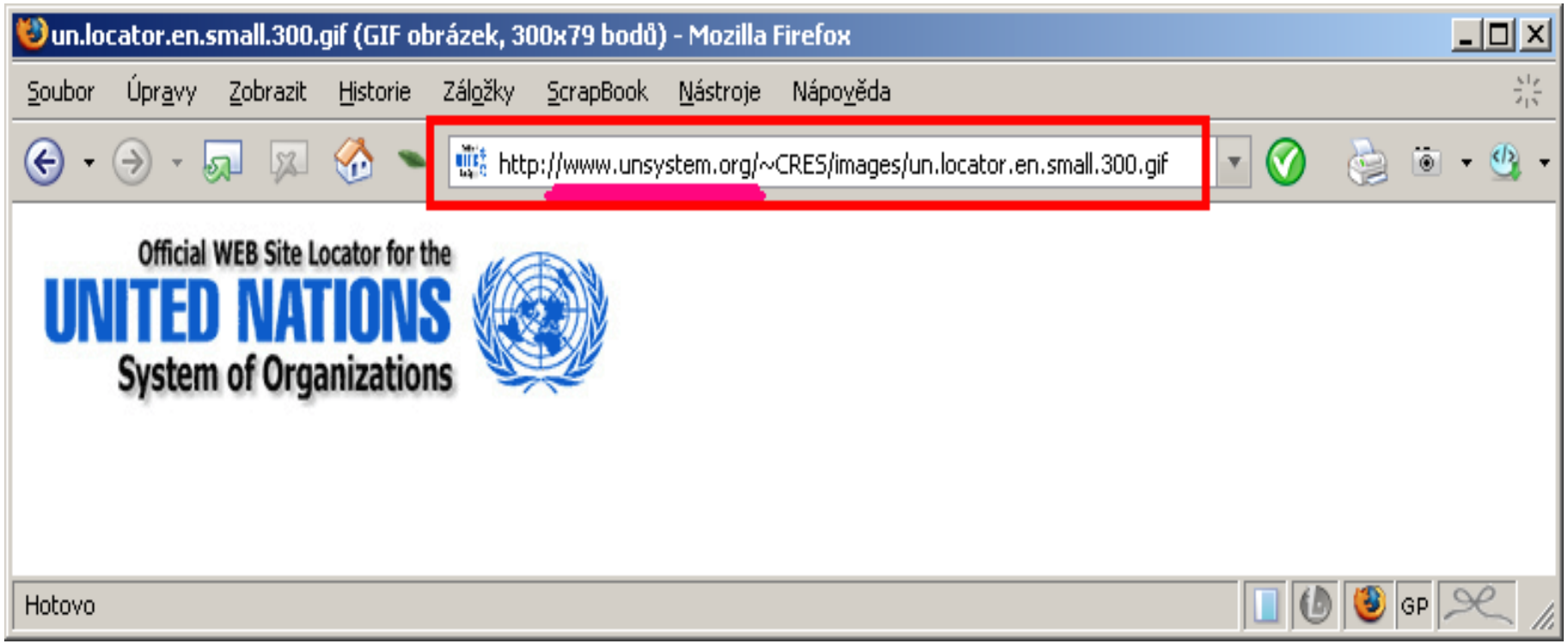




Ne/Bezpečí ve světě médií

Podvodné loterie – ukázka 2

Zdroj obrázku v záhlaví - logo



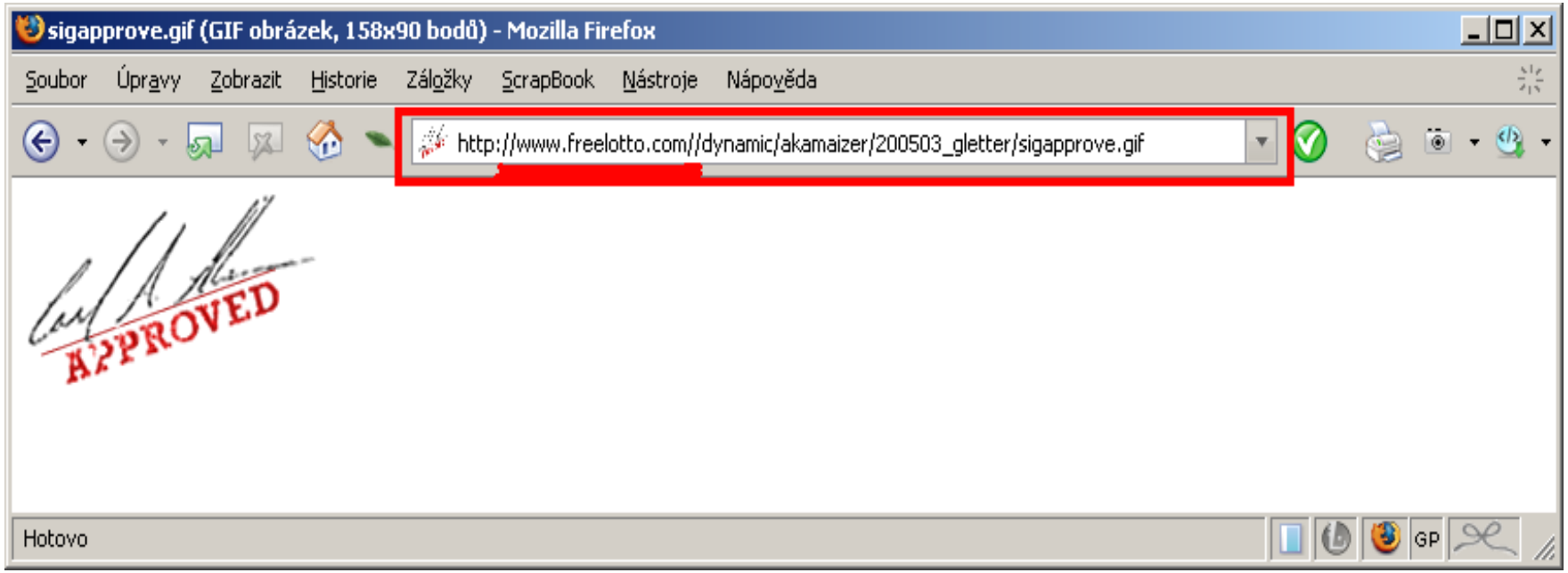
Podvodné loterie – ukázka 2

Zdroj obrázku údajné ředitelky loterie



Podvodné loterie – ukázka 2

Zdroj obrázku s podpisem



!!! P A M A T U J !!!

Cokoliv zveřejníš na internetu,

může být kdykoliv zneužito!

Nalezené doklady se nezveřejňují!



Nálezci ztracených dokladů je vyfotí a sdílí na sociálních sítích pod záminkou rychlého nalezení majitele.

Podvodníci nafocené doklady mohou zneužít a vydávat se za osobu na dokladu.

Jakýkoliv doklad je možné zneužít!

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 skutečného 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 skutečného případu

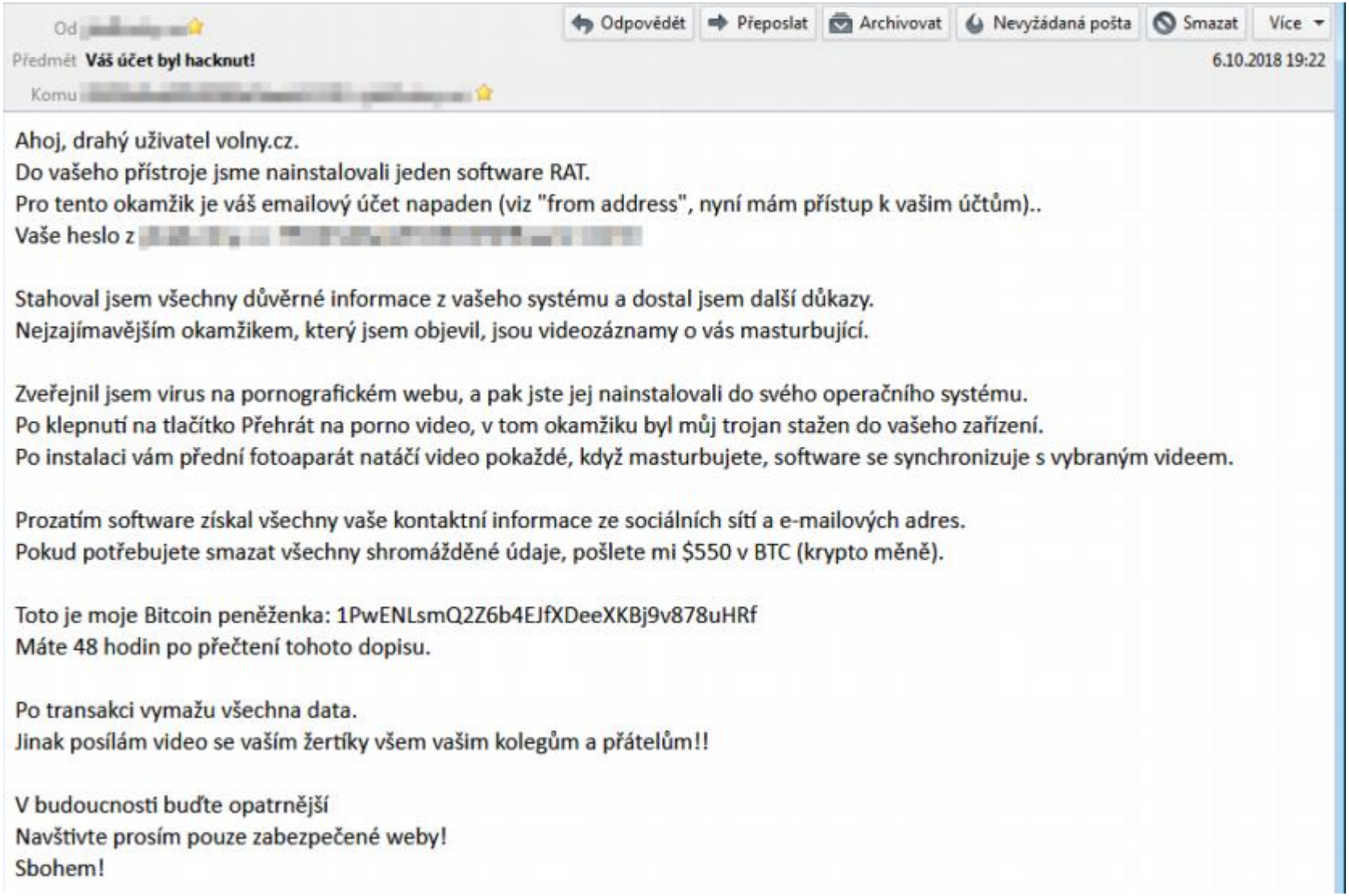
- Prostřednictvím účelově založených webových stránek vzbudili dojem, že účet skutečně existuje a přes internet ho i ovládá
- Pod různými záminkami vylákali 3.900 USD
- Podvodníci sdělili, že převodli částku 22.500.000 USD a na fiktivním webu tento převod byl zaznamenán
- Další požadovaný poplatek bylo 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.

Vyděračské e-maily - sextortion



Falešné vydírání, sextortion

- Podvodníci rozešlou výhružné vyděračské e-maily
  Vyhrožují zveřejněním citlivých informací nebo videí
- Adresa odesílatele a příjemce bývá shodná
  Podvržená odesílací adresa je starý trik
- Občas text obsahuje heslo, které uživatel používá
  Získaná z dostupných databází hesel
- Podvodníci zkouší, kdo se nachytá a zaplatí
  Platba je na bitcoinový účet pro anonymizaci platby



Od [redacted]

Odpovědět | Přeposlat | Archivovat | Nevyžádaná pošta | Smazat | Více

Předmět **Váš účet byl hacknut!**

6.10.2018 19:22

Komu [redacted]

Ahoj, drahý uživatel volny.cz.
Do vašeho přístroje jsme nainstalovali jeden software RAT.
Pro tento okamžik je váš emailový účet napaden (viz "from address", nyní mám přístup k vašim účtům)..
Vaše heslo z [redacted]

Stahoval jsem všechny důvěrné informace z vašeho systému a dostal jsem další důkazy.
Nejzajímavějším okamžikem, který jsem objevil, jsou videozáznamy o vás masturbující.

Zveřejnil jsem virus na pornografickém webu, a pak jste jej nainstalovali do svého operačního systému.
Po klepnutí na tlačítko Přehrát na porno video, v tom okamžiku byl můj trojan stažen do vašeho zařízení.
Po instalaci vám přední fotoaparát natáčí video pokaždé, když masturbujete, software se synchronizuje s vybraným videem.

Prozatím software získal všechny vaše kontaktní informace ze sociálních sítí a e-mailových adres.
Pokud potřebujete smazat všechny shromážděné údaje, pošlete mi $550 v BTC (krypto měně).

Toto je moje Bitcoin peněženka: 1PwENLsmQ2Z6b4EJfXDeeXKBj9v878uHRf
Máte 48 hodin po přečtení tohoto dopisu.

Po transakci vymažu všechna data.
Jinak posílám video se vaším žertíky všem vašim kolegům a přátelům!!

V budoucnosti buďte opatrnější
Navštivte prosím pouze zabezpečené weby!
Sbohem!

Falešné vydírání, sextortion

Přehled transakcí na BlockChain.com

Bitcoin Adresa Adresy jsou identifikátory, které používáte k poslání osobě.

souhrn	
Adresa	1GL9JtXPRTPetxgiJ8UcgrEECp12spD4tt
Hash 160	a828b9bda7d439256a23ba1308f3a0c3ef743fa7

Transakce		
Ne. Transakce	55	
Celkem přijato	1.73956829 BTC	
Konečná bilance	0 BTC	

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, nic neplatit!!!

MALWARE

- **Všeobecné označení pro škodlivý kód**

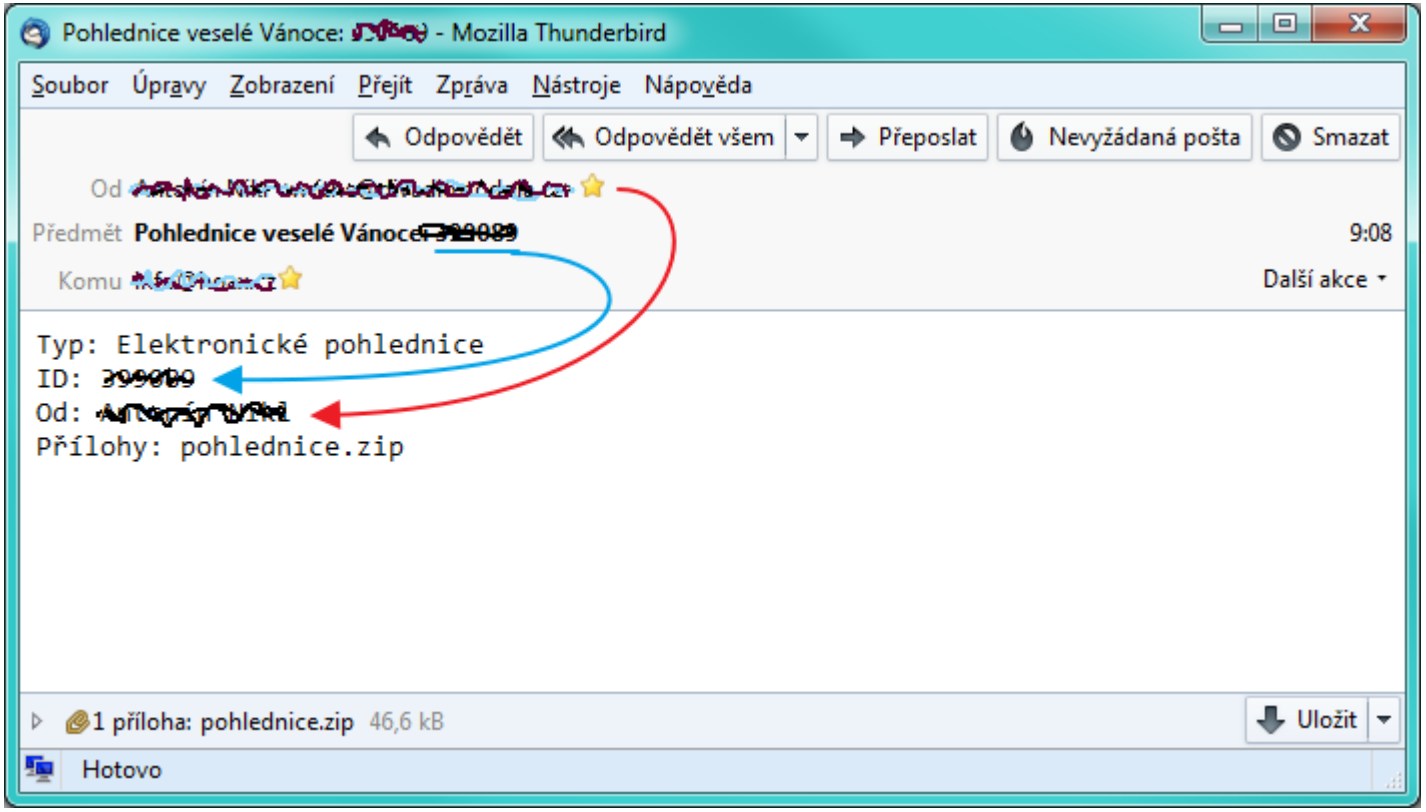
  Trojský kůň, virus, spyware, ransomware, ... ***...havěť***

- **Šíří se různými způsoby, mimo jiné také e-mailem**

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

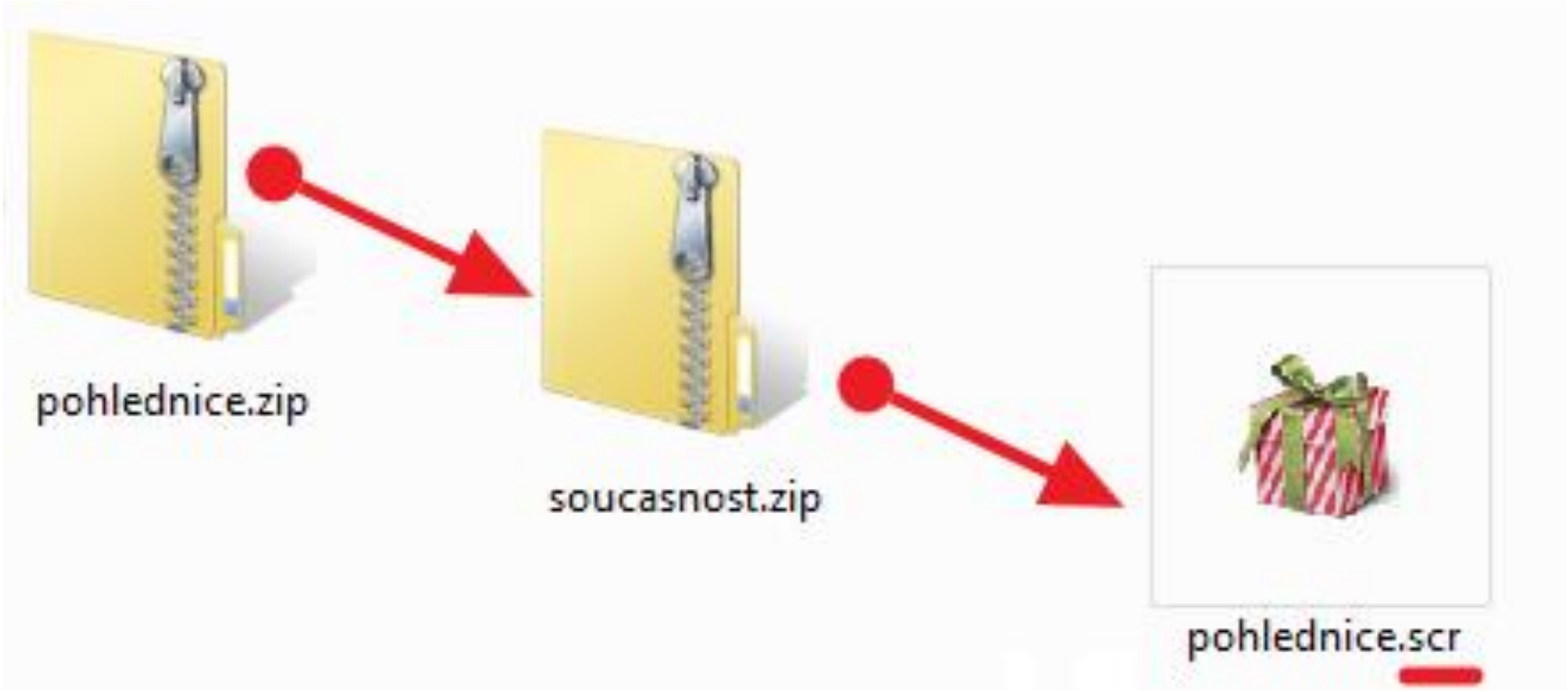
MALWARE (havěť) – ukázka 1

Podvodný e-mail s přílohou – jako zpráva s obrázkem

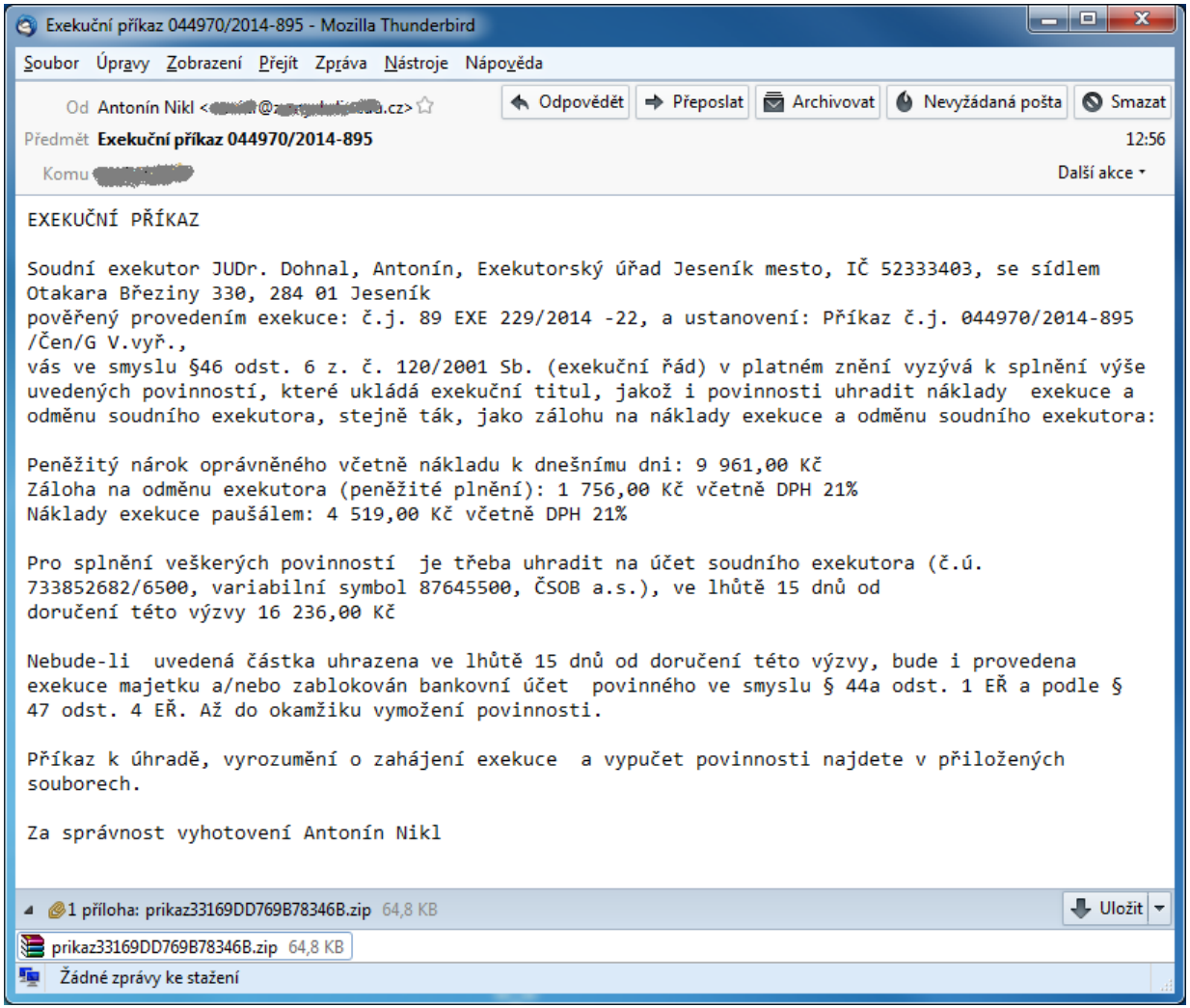


MALWARE (havěť) – ukázka 1

Místo obrázku je zabalena havěť

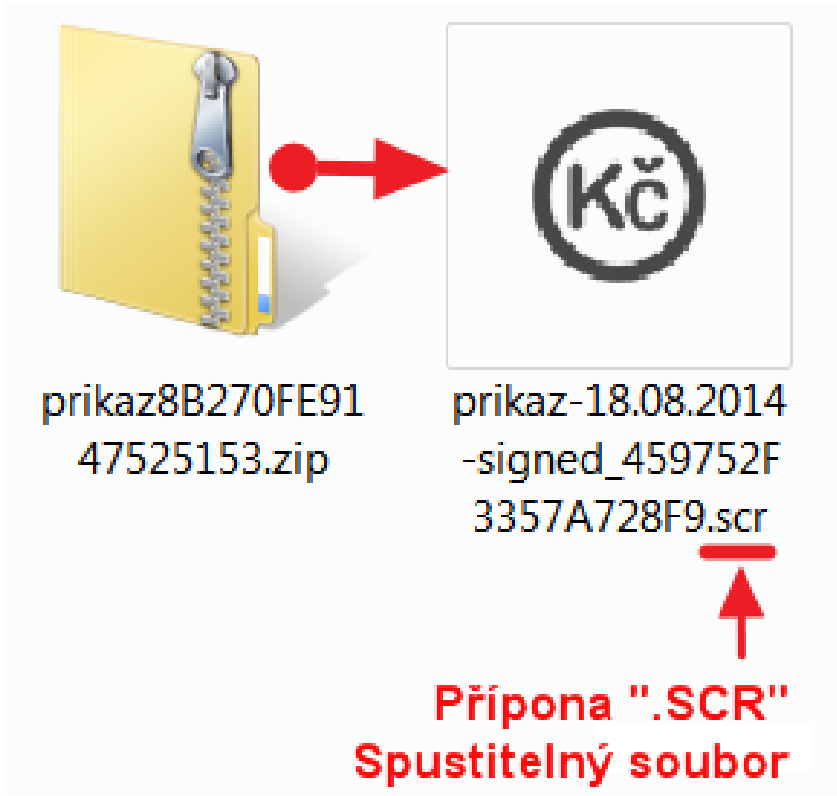


MALWARE (havěť) – ukázka 2

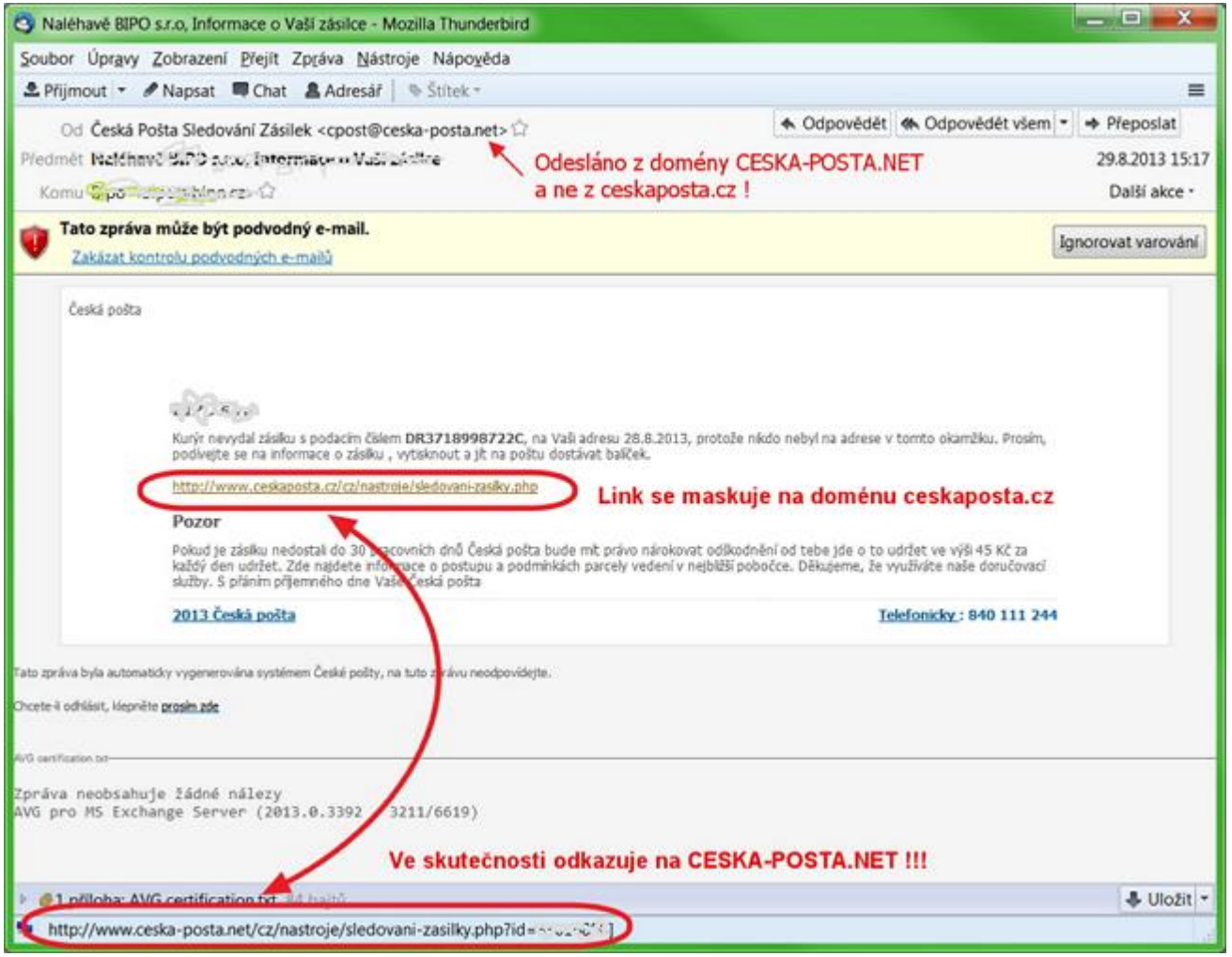


MALWARE (havěť) – ukázka 2

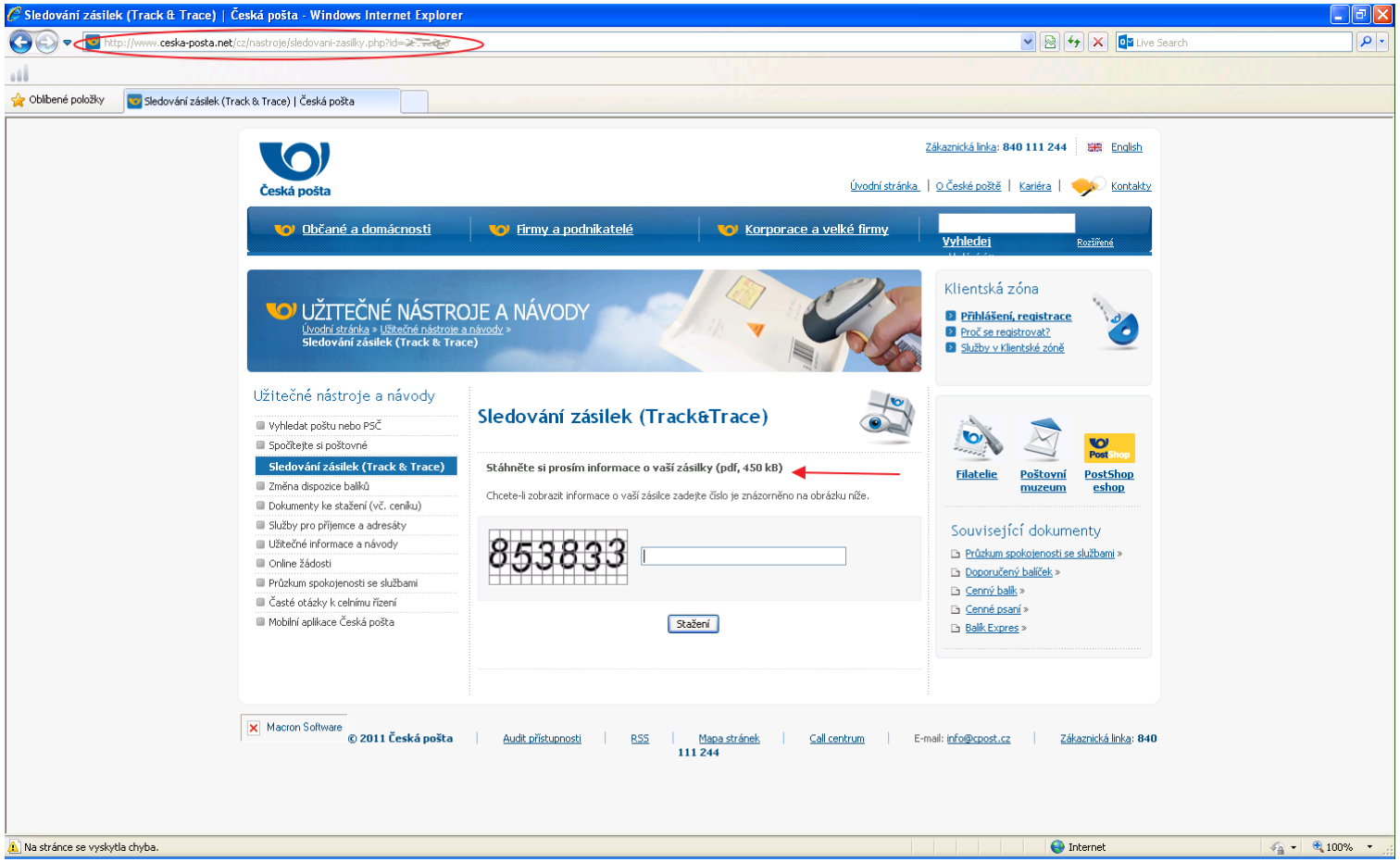
Příloha obsahuje místo dokumentu trojského koně



MALWARE (havěť) – ukázka 3

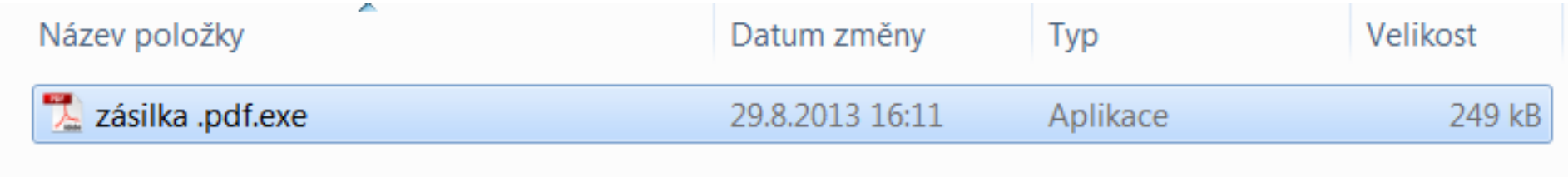


MALWARE (havěť) – ukázka 3

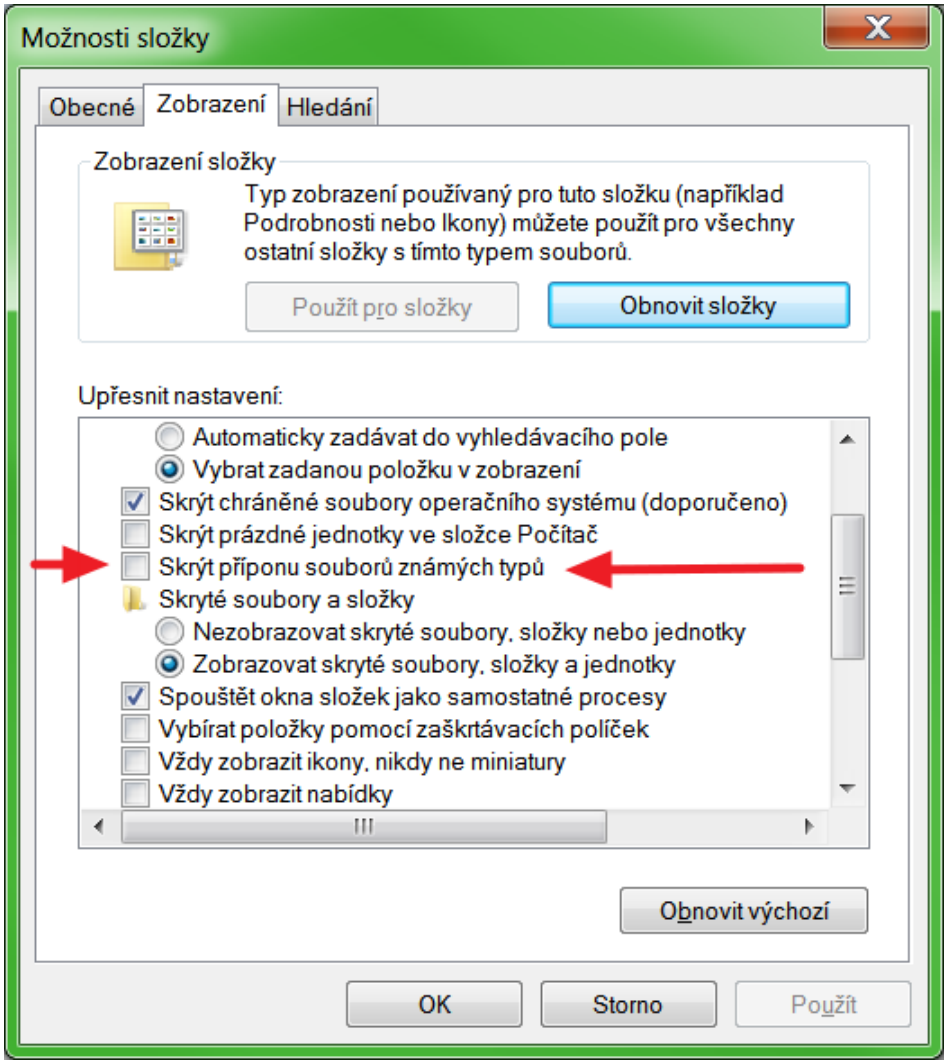


MALWARE (havěť) – ukázka 3

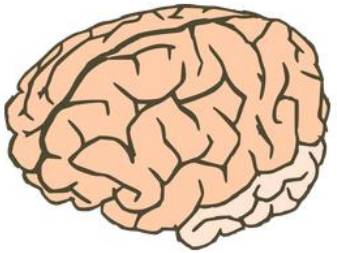
Stažený soubor má sice ikonku Adobe Readeru



Není to PDF dokument, ale spustitelný EXE soubor!


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

MALWARE - jak se bránit

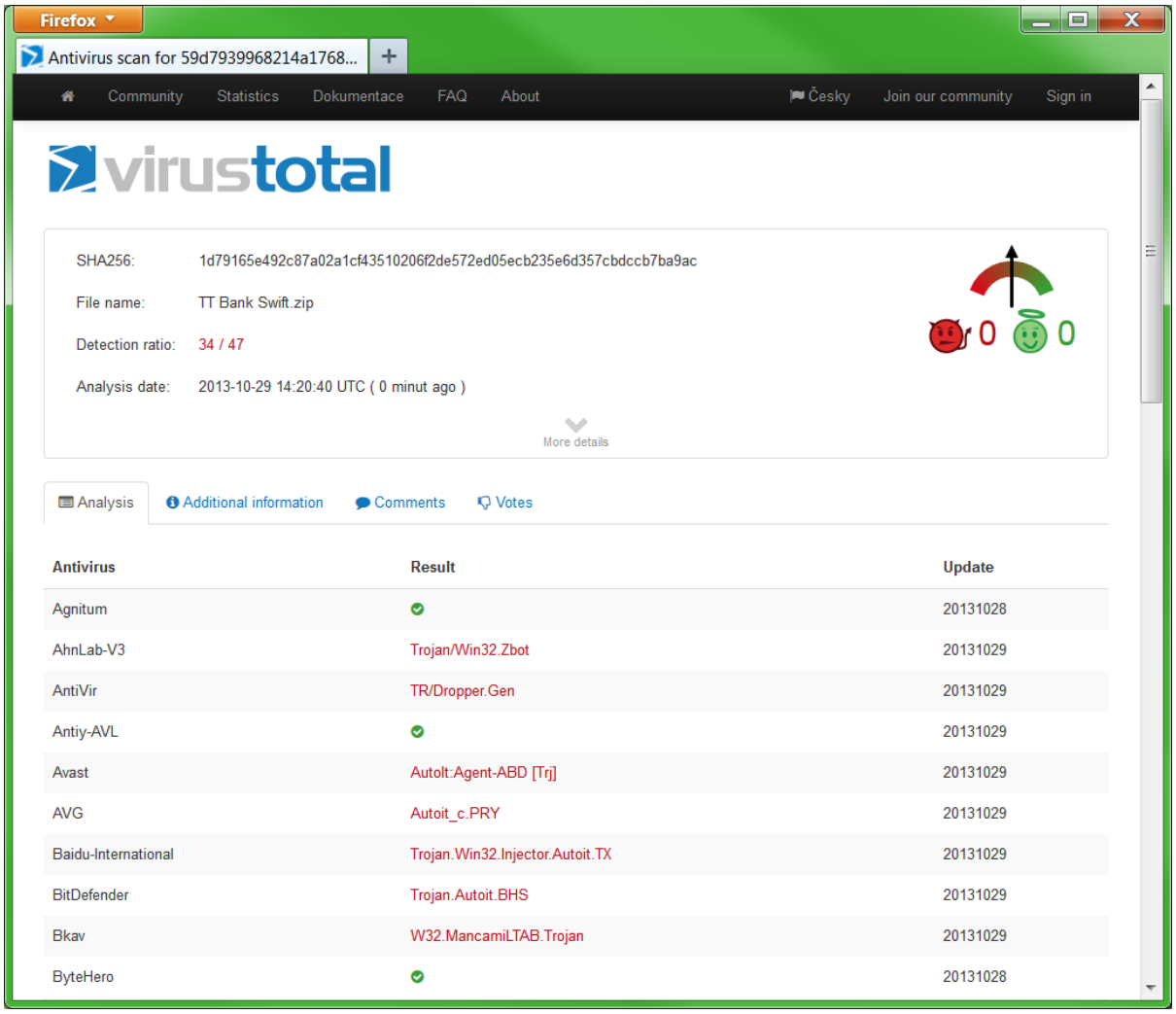


- Buďte podezíraví
- Neotvírejte přílohy od neznámých lidí
- Přílohy od známých kontrolujte
- Dejte pozor na skryté přípony
- Používejte aktualizovaný OS a antivirový program

Podezřelé soubory lze kontrolovat www.virustotal.com



Výsledek testu podezřelého souboru



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!!!





CD / DVD



+ Data nelze neúmyslně přepsat

+ Lze jednoduše skladovat

- Menší kapacita

- Mechanické poškození

Externí disk



+ Data lze opakovaně přepisovat

+ Velká kapacita uložených dat

- Data lze kdykoliv smazat

- Mechanické poškození

Kde najdu další informace

HOAX www.hoax.cz

Google

bezpečí

KrebsonSecurity
In-depth security news and investigation

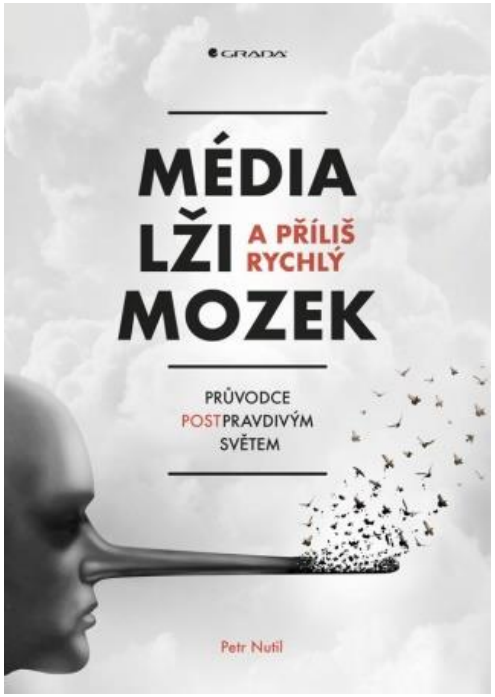
Snopes.com
Rumor Has It

Demagog CZ
PRAVDA
NEPRAVDA
ZAVÁDĚJÍCÍ
NEOVĚŘITELNÉ

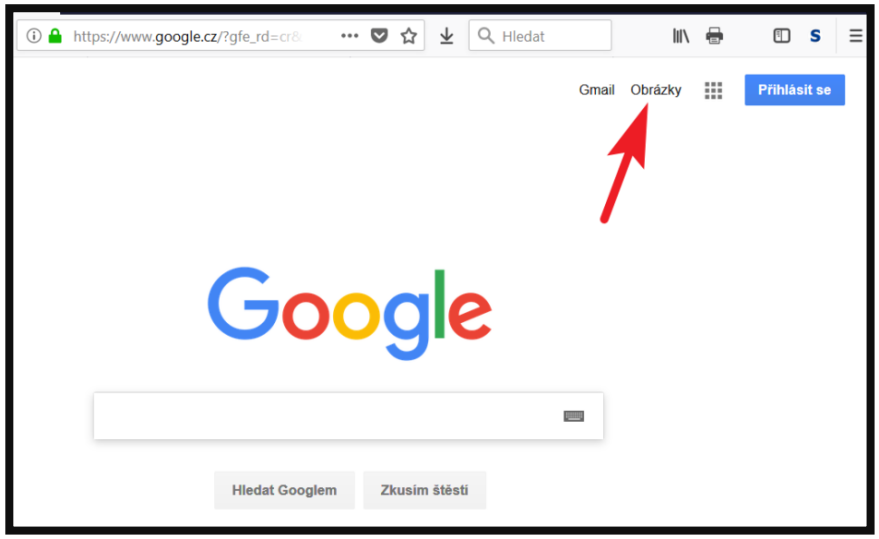
Dostupná literatura







Jak hledat obrázky?





Vyhledávání obrázků Google

Google obrázky

Vyhledávání pomocí obrázku

Vyhledávejte na Googlu pomocí obrázku namísto textu. Sem zkuste přetáhnout obrázek.

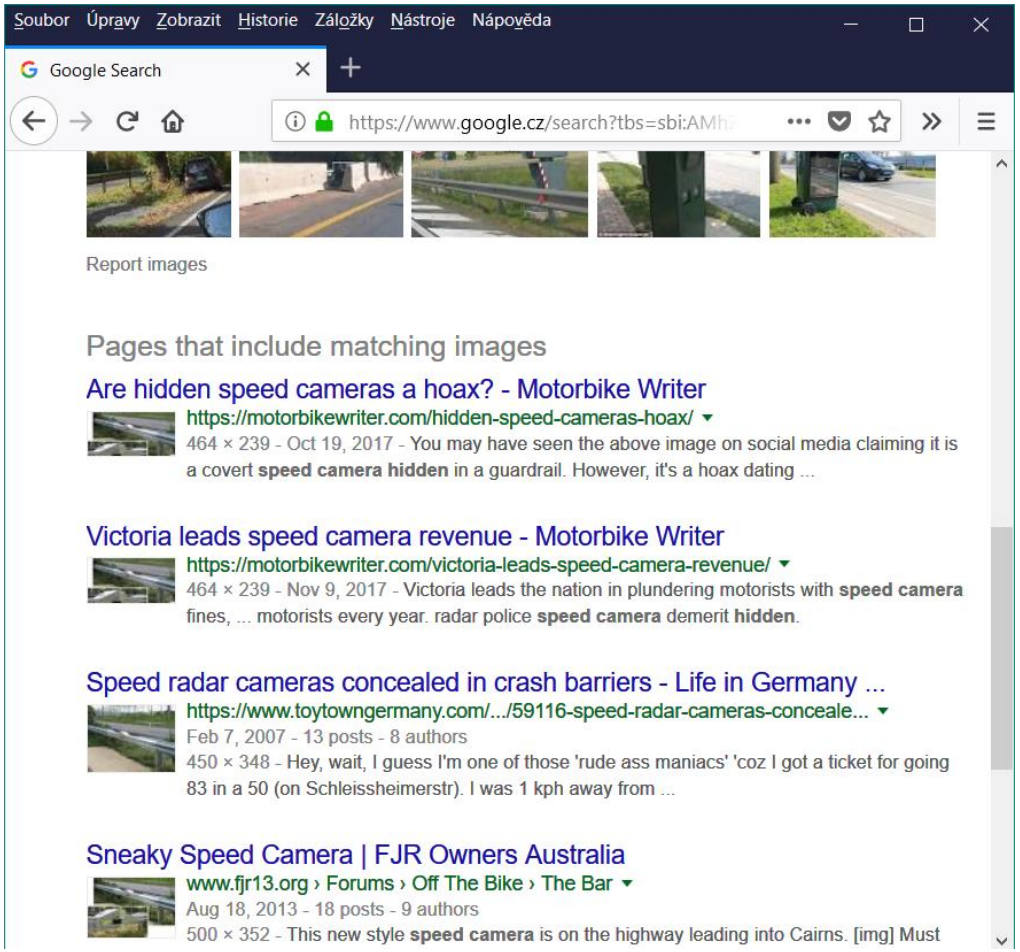
Vložte adresu URL | Nahrát obrázek

http://www.hoax.cz/data/hoax/506.jpg

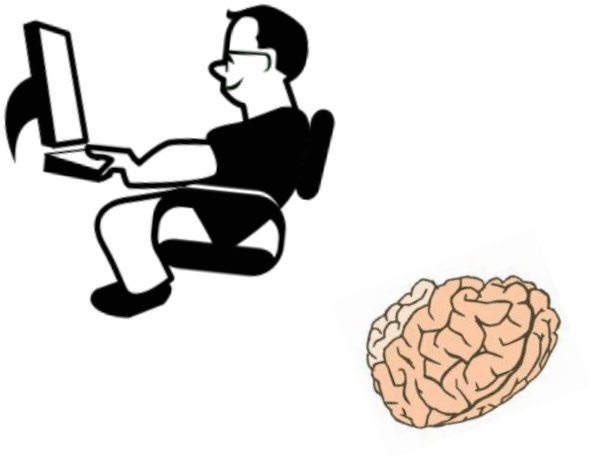
Vyhledávání pomocí obrázku



Vyhledávání obrázků Google



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



Děkuji za pozornost

Josef Džubák
dzubak@hoax.cz

HOAX
www.hoax.cz