



***Stinnou stránkou elektronické komunikace nejsou jenom HOAXy***

**Josef Džubák**  
**[www.hoax.cz](http://www.hoax.cz)**





# HOAX? Co to je?

Anglické slovo, znamená v překladu:

- Mystifikace
- Podvod
- Žert
- Novinářská kachna



# Kde je začátek?



**Fámy se nejdříve šířily ústně - JPP**



**Využívá se dostupná technologie**



**Kliknout je tak snadné...**



# Hoaxy v době Internetu

## Smyšlená varování před virem

**PŘEDEJTE DÁL !!!**

**V PŘÍŠTÍCH DNECH MUSÍTE DÁVAT VELKÝ POZOR A NEOTEVŘÍT ZADNÝ E-MAIL NAZVANÝ POZVANKA-"INVITATION", NEZÁVISLE NA TOM, OD KOHO JE.**

**JEDNÁ SE O VIRUS, KTERÝ " OTEVÍRA OLYMPIJSKOU POCHODEŇ" A KTERÝ SPALÍ HARD DISK. TENTO VIRUS BUDE ODESLAN OSOBOU, KTERA VÁS MÁ VE SVÝCH KONTAKTECH. TAKŽE POKUD OBDRŽÍTE E-MAIL S NAZVEM "INVITATION" NEOTVÍREJTE HO JE TO NEJHORŠÍ VIRUS OHLAŠENÝ CNN A KLASIFIKOVANÝ SPOLECNOSTÍ MICROSOFT JAKO NEJDESTRUKTIVNEJŠÍ VIRUS, KTERY KDY EXISTOVAL!!!!!!!**

**BYL OBJEVEN VČERA ODPOLEDNE POSLETE TENTO E-MAIL VSEM, KOHO ZNATE, VASIM PRATELUM, VSEM VASIM KONTAKTUM ČÍM VÍCE OSOB UPOZORNÍTE PŘEDEM, TÍM HŮŘE SE BUDE VIRUS ŠÍŘIT!!!**



# Hoaxy v době Internetu

## Vymyšlené prosby o pomoc

### Nemocné děti, týraní pejsci...

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.

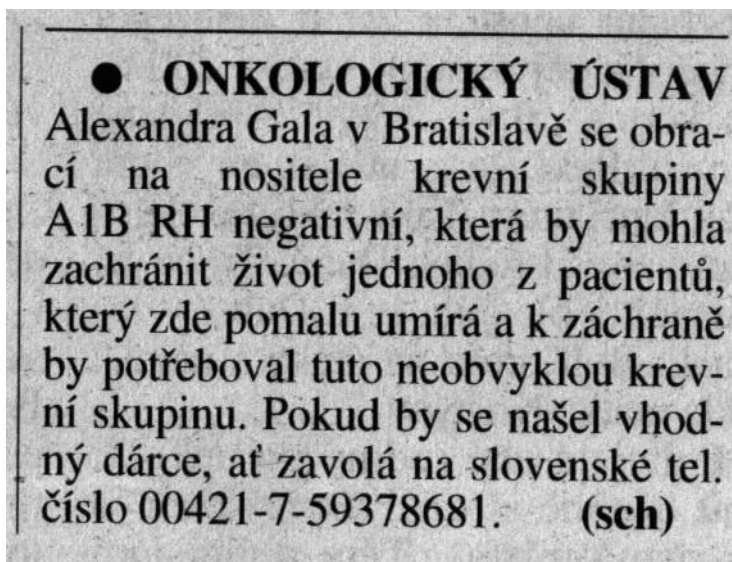
Bohužel nemáme dostatek peněz na její zaplacení. AOL a ZDNET souhlasili, že nám pomohou. Jediný způsob, jakým nám mohou pomoci je tento: Já posílám tento e-mail vám a vy jej pošlete dalším lidem. AOL bude sledovat tento e-mail a počítat, kolik lidí jej obdrželo. Každá osoba, která otevře tento e-mail a pošle ho nejméně 3 lidem nám přinese 32 centů.



# Hoaxy v době Internetu

## Opravdové prosby o pomoc

Kolují i několik let, přestože nejsou aktuální



+ leden 2001

Vyšlo v tisku: 4.12.2004



# Hoaxy v době Internetu

## Fámy z reálného života

Komunikaci po internetu využívá většina lidí a přenáší sem věci z reálného světa

## Upravené polopravdy s určitým úmyslem

Účelové upravené polopravdy za účelem poškodit určitý subjekt nebo skupinu lidí



# Co mají hoaxy společného

## Snaží se přesvědčit svojí důležitostí

Nové nebezpečí, aktuální ohrožení, naléhavá pomoc

## Údajný důvěryhodný zdroj

Microsoft varuje, Symantec objevil, laboratoř NASA zjistila

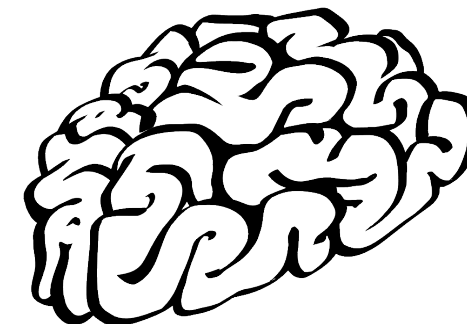
## Výzva k dalšímu rozeslání !!!

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





# Jak se bránit



## Je-li k dispozici mozek - použij ho!

- Jednej s chladnou hlavou – rozmysli se
- Zkus najít informace z jiných zdrojů
- Jestli se tím nehodláš zabývat, raději zprávu vymaž
- Totéž platí pro „Like“ a sdílení



HOAX

PHISHING

LOTERIE

SCAM419

MALWARE

ŘETĚZOVÉ E-MAILY



[www.hoax.cz](http://www.hoax.cz)



[www.snopes.com](http://www.snopes.com)



[www.museumofhoaxes.com](http://www.museumofhoaxes.com)



[www.cernasanitka.cz](http://www.cernasanitka.cz)

*Konference SOOM 15.3.2013*





HOAX

PHISHING

LOTÉRIE

SCAM419

MALWARE

ŘETĚZOVÉ E-MAILY

# Je to marný



## ...je to marný...

## je to marný...

*“Já to stejně raději pošlu, co kdyby to náhodou byla pravda!”*

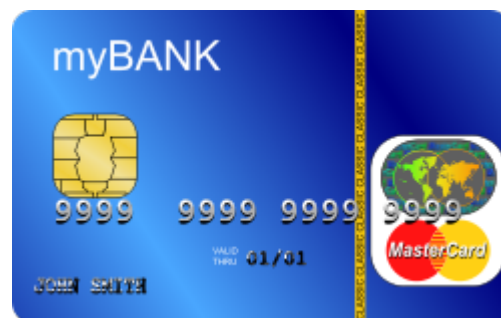


# Co si třeba zarhybařit?

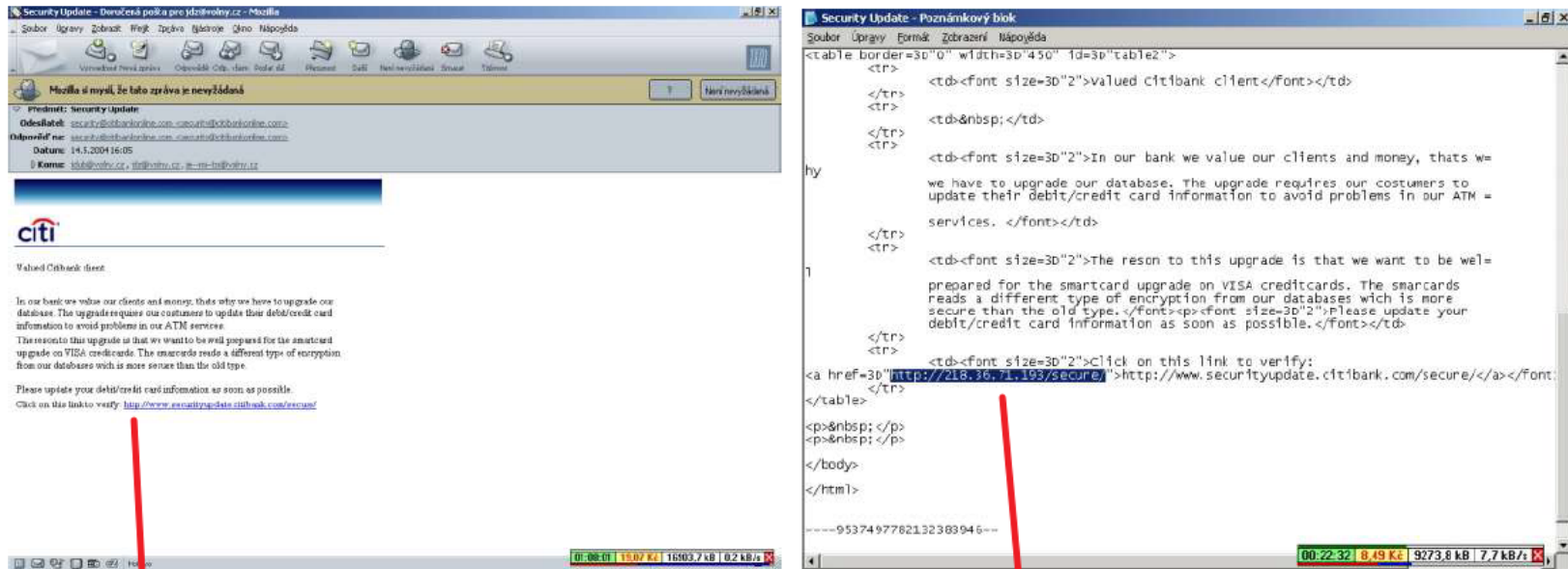


# Password Harvesting fISHING

(rhybaření)

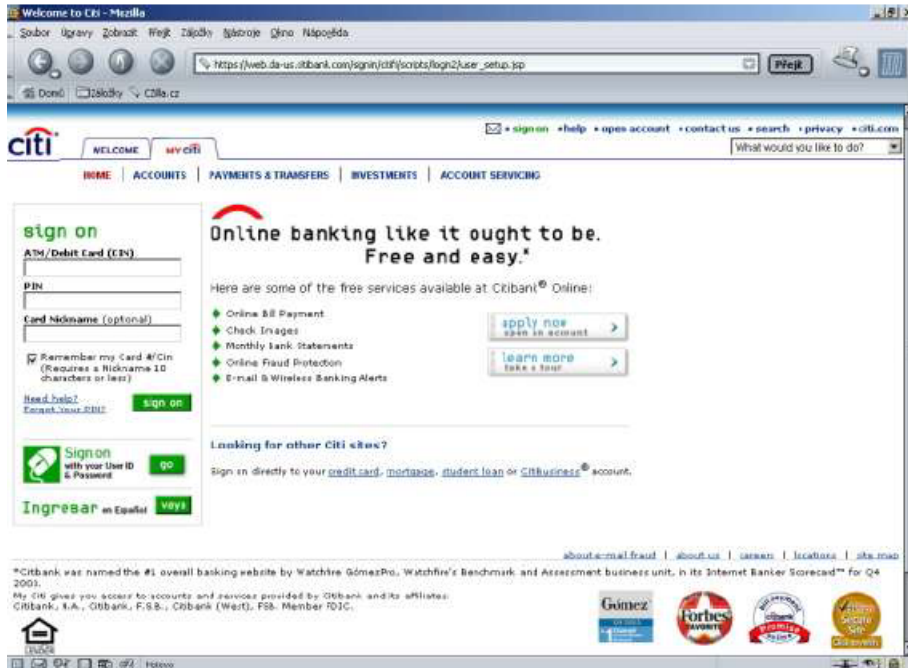


# Krok 1 - nahození návnady

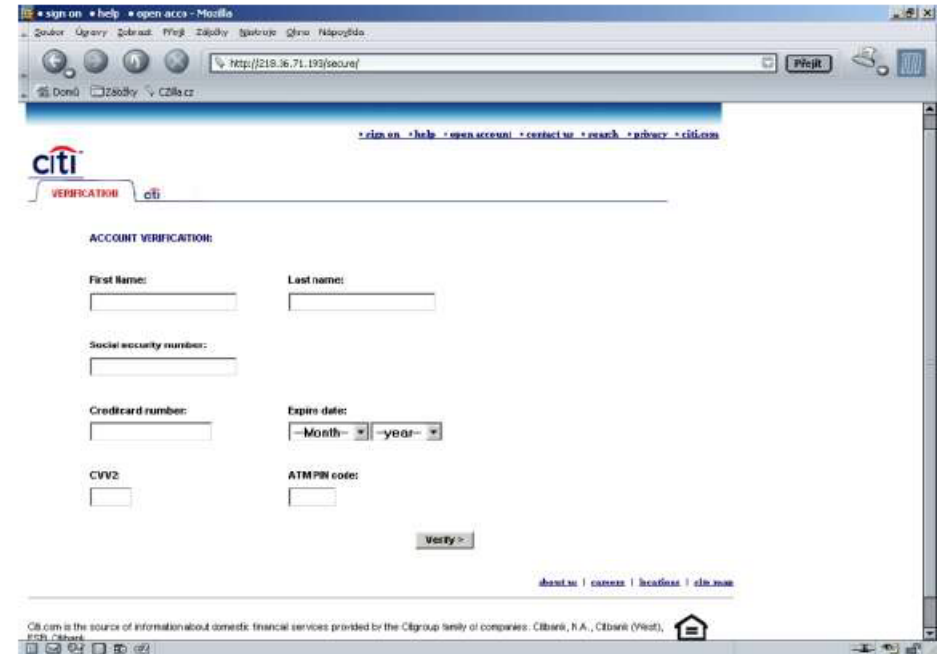


**<a href="http://218.36.71.193/secure/">**  
**http://www.securityupdate.citibank.com/secure/ </a>**

## Krok 2 - sběr dat



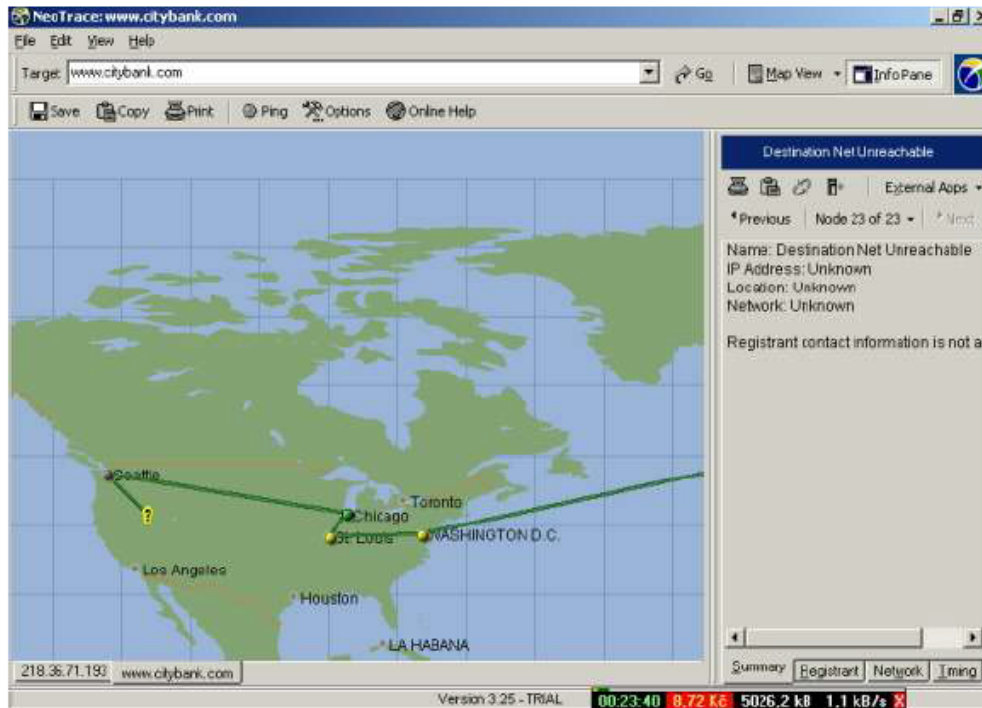
Skutečná stránka banky



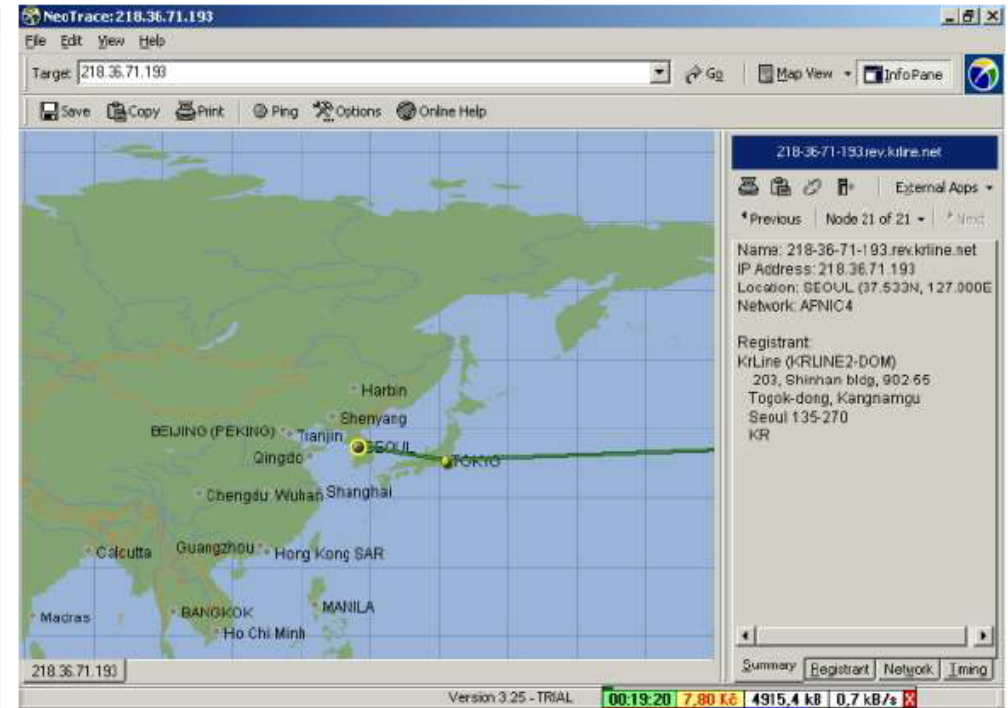
Podvodná stránka



# Kde jsou falešné stránky?



Server banky v USA



Falešné stránky v Koreji

# Databáze podvodných stránek - www.phishtank.com

PhishTank is operated by [OpenDNS](#), a free service that makes your Internet safer, faster, and smarter. [Get started today!](#)

Signed in: [j...@... | My Account | Sign Out](#)

**PhishTank**® Out of the Net, into the Tank.

Home Add A Phish Verify A Phish Phish Search Stats FAQ Developers Mailing Lists My Account

## Join the fight against phishing

**Submit** suspected phishes. **Track** the status of your submissions.  
**Verify** other users' submissions. **Develop** software with our free API.

Found a phishing site? Get started now — see if it's in the Tank:

### Recent Submissions

ID	URL	Submitted by
<a href="#">1759494</a>	<a href="http://puntoolimpico.com.ve/aol.html">http://puntoolimpico.com.ve/aol.html</a>	<a href="#">billwake</a>
<a href="#">1759493</a>	<a href="http://sib-komfort.ru/images/document/document/doc...">http://sib-komfort.ru/images/document/document/doc...</a>	<a href="#">billwake</a>
<a href="#">1759492</a>	<a href="http://lbimedia.net/wp-content/4070294342/13435365...">http://lbimedia.net/wp-content/4070294342/13435365...</a>	<a href="#">PhishReporter</a>
<a href="#">1759491</a>	<a href="http://mymktgsite.com/temp/PayPal/paypal/?cmd=_hom...">http://mymktgsite.com/temp/PayPal/paypal/?cmd=_hom...</a>	<a href="#">PhishReporter</a>
<a href="#">1759490</a>	<a href="http://mymktgsite.com/temp/PayPal/paypal/webssc/upd...">http://mymktgsite.com/temp/PayPal/paypal/webssc/upd...</a>	<a href="#">PhishReporter</a>

#### What is phishing?

Phishing is a fraudulent attempt, usually made through email, to steal your personal information.  
[Learn more...](#)

#### What is PhishTank?

PhishTank is a collaborative clearing house for data and information about phishing on the Internet. Also, PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge.  
[Read the FAQ...](#)

# Databáze podvodných stránek - www.phishtank.com


**PhishTank**® Out of the Net, into the Tank.

Home Add A Phish Verify A Phish Phish Search Stats FAQ Developers Mailing Lists My Account

**Submission #1720188** is currently offline

Submitted Feb 4th 2013 11:50 AM by [phxcz](#) (Current time: Mar 12th 2013 8:30 PM UTC)

<http://blogcreation.net/wp-admin/user/fa.html>

 **Verified: Is a phish** [Next unverified phish >](#)  
As verified by [andrea78vr](#) [knack](#) [stuartarant](#) [Andrej1](#)

Is a phish **100%**  
Is NOT a phish 0%

[Screenshot of site](#) [View site in frame](#) [View technical details](#) [View site in new window](#) [Something wrong with this submission?](#)

Google mail Change Language: English

Username:  @gmail.com

Password:

Recovery E-mail:

Phone Number:

Date Of Birth (dd/mm/yyyy) :

# APWG

[www.apwg.org](http://www.apwg.org)

The screenshot shows the APWG website homepage. At the top, there is a navigation bar with links for APWG, Public Education Initiative, eCrime Research, and STORP.HINK.CONNECT. Below this is the APWG logo and the tagline "Unifying the Global Response to Cybercrime". A secondary navigation bar includes links for INTERNET POLICY COMMITTEE and DATA LOGISTICS. The main navigation bar contains links for Home, Report Phishing, Sponsor Solutions, Resources, APWG Events, APWG News Center, Join APWG, and About APWG. The main content area features a large banner with an owl illustration and the text "Cybercrime Data Logistics: APWG Defines the Standards and Maps the Frontier of Cybercrime Management". To the right of the banner is a section for "APWG PREMIUM MEMBERS:" listing logos for VERISIGN, MarkMonitor, QinetiQ, and la Caixa, with a "VIEW ALL" link. Below the banner are two columns: "APWG News" with a sub-header "APWG releases Phishing Trends Report for Q3" and "About APWG" with a sub-header "APWG is the global industry, law enforcement, and government coalition focused on unifying the global". On the right side, there is a section titled "Advice On Phishing" with text: "Be suspicious of any email with urgent requests for personal financial information" and "Avoid filling out forms in email messages that ask for personal financial information".

- založena v roce 2003 jako Anti-Phishing Working Group
- sdružuje přes 2000 organizací po celém světě

Konference SOOM 15.3.2013

# www.krebsonsecurity.com

**KrebsonSecurity**  
In-depth security news and investigation

[BLOG ADVERTISING](#)[ABOUT THE AUTHOR](#)

## 29 Welcome to Krebsonsecurity.com

DEC 09

Welcome, everyone, to krebsonsecurity.com. Here's to new beginnings, and a happy, healthy and prosperous New Year!

Some of you may be familiar with my work at *The Washington Post* and the [Security Fix blog](#). Krebsonsecurity.com will feature similar content: Original reporting and analysis on important security threats and trends.

With a few exceptions, I will continue to eschew chasing the security story-of-the day, as there are plenty of sites you can go to for that. My focus will remain on publishing information and reporting that you won't find anywhere else – and with a minimum of editorializing.

Visitors who are unfamiliar with my work can browse through [a collection](#) of what I think represents some of my best reporting over the past few years. The [About the Author](#) and [About this Blog](#) tabs include a bit more detail about who I am and how this blog will be organized.

Advertisement

2FA LOGON, TRANSACTION REVIEW AND APPROVAL FROM SMART PHONES, TABLETS, DESKTOPS...

The advertisement features a dark background with icons for a smartphone, a laptop, and a tablet, illustrating the multi-device authentication process.

### Recent Posts

[Credit Reports Sold for Cheap in](#)

# Nejlepší osvěta - Drahoušek zákazník!

Předmět: FW: Významná Oznámení ode České Sporitelna Internet Bankovní  
 Od: [redacted]  
 Datum: 15:22  
 Komu: [redacted]

From: Česká Sporitelna [mailto:hultrh@yahoo.com]  
 Sent: Wednesday, January 09, 2008 11:08 PM  
 To: undisclosed-recipients  
 Subject: Významná Oznámení ode České Sporitelna Internet Bankovní

**ČESKÁ  
SPORITELNA**

Drahoušek Zákazník,

Tato is tvuj funkcionár oznámení dle Česká Sporitelna aby den určitý služba dát pozor pod vule být deactivated a odstranit kdyby nedošlo k obnovit se bezprostřední.

Predešlý oznámení mít been poslaný až k den určitý Žaloba Dotyk pridilil až k tato účet.

Ackoliv den určitý Bezprostřední Dotyk , tebe musit obnovit se den určitý služba dát pozor pod ci ono vule být deactivated a odstranit.

**Obnovit se Ted** tvuj **SERVIS 24 Internetbanking.**

SERVIS: **SERVIS 24 Internetbanking**  
 SKONANÍ: **Leden, 11 2008**

Být zavázán tebe do using SERVIS 24 Internetbanking. My ocenit tvuj obchod a den určitý příležitost až k sloužit tebe.

Česká Sporitelna Služba účastníkum

\*\*\*\*\*  
 DULEŽITÝ Služba účastníkum HLÁŠENÍ  
 \*\*\*\*\*

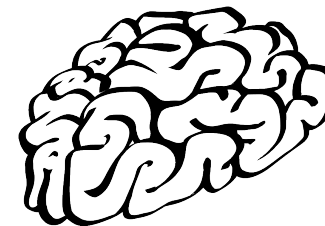
Být příjemný cinit ne namítat až k tato poselstvi. Do jakýkoliv bádat , dotyk Služba účastníkum

© Česká Sporitelna.  
 Všechna práva vyhrazena.

[http://www.c-tech.ac.th/csas/www.csas.cz/banka/appmanager/portal/\\_nfpb=true&\\_pageLabel=home/](http://www.c-tech.ac.th/csas/www.csas.cz/banka/appmanager/portal/_nfpb=true&_pageLabel=home/)

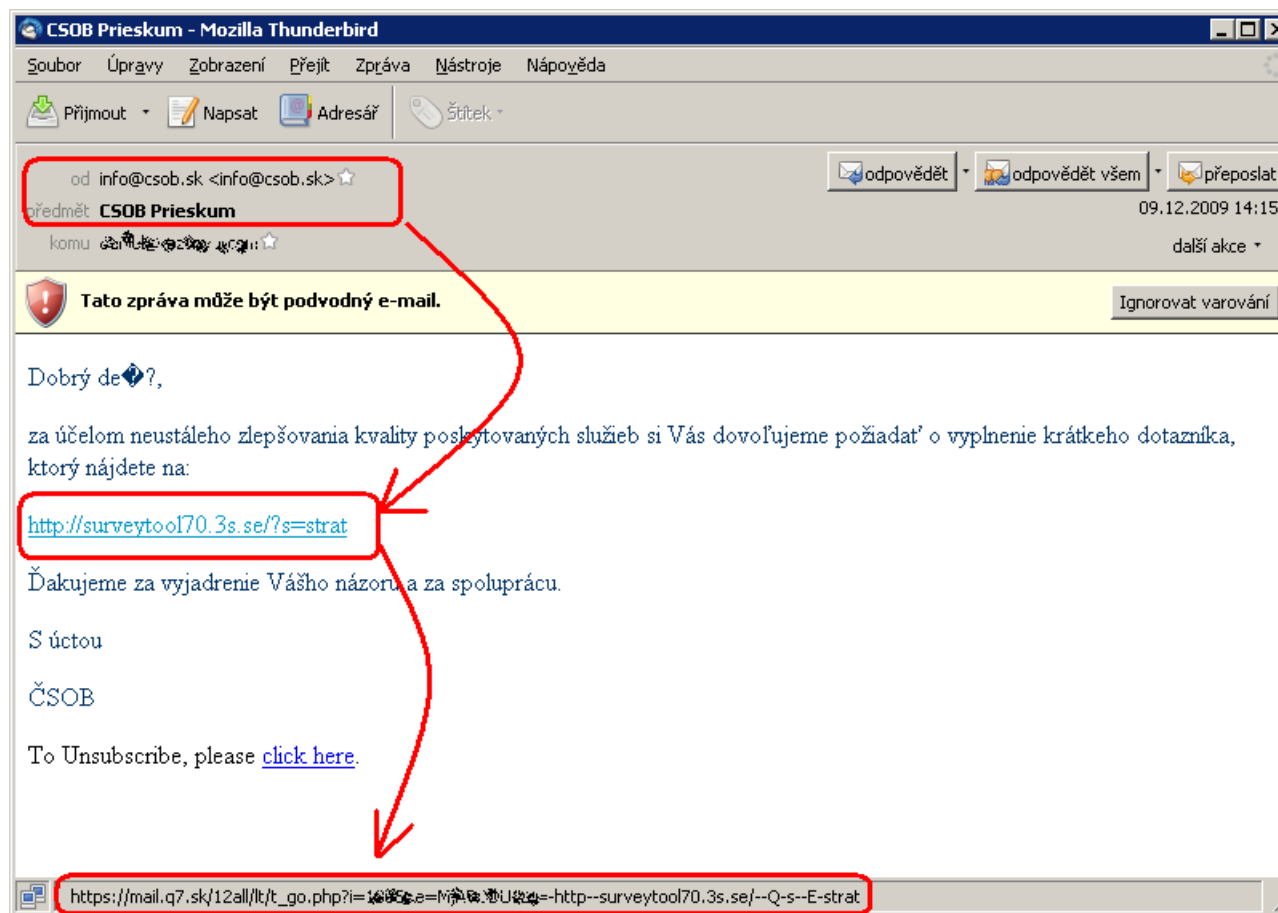
Nepřečtené zprávy: 36 Celkem: 277

# Jak se bránit



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

# Překvapení pro klienty!





# Podvodné loterie

- **Obdoba rozesílaných oznámeních o výhře poštou**
- **Na e-mailové adresy jsou rozesílány oznámení o výhře, přestože se uživatel žádné loterie nezúčastnil**
- **Zaslání výhry je podmíněno zaplacením drobného poplatku**
- **A pak dalšího poplatku**
- **A pak dalšího...**

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

Soubor Úpravy Zobrazit Ejejt Zpřeva Nástroje Nápořádka

Přijmout Napsat Adresář Odpovědět Odp. všem Přeposlat Štekl Smazat Nevysídané 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 1079, 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 HUNDRETHOUSAND 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.....UNH099425

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

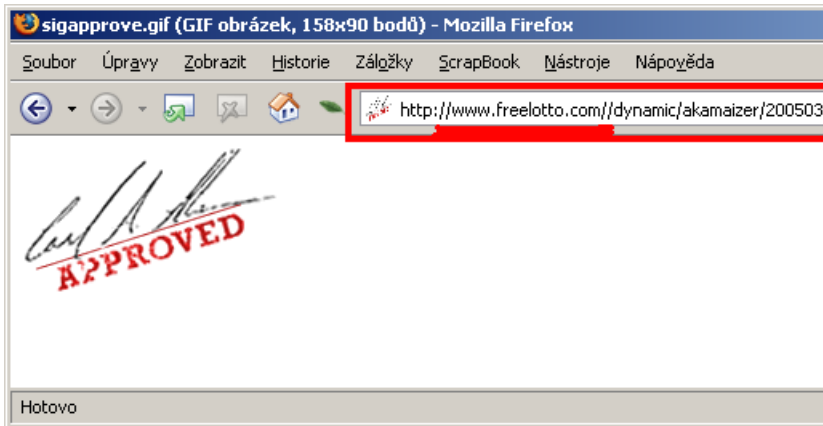
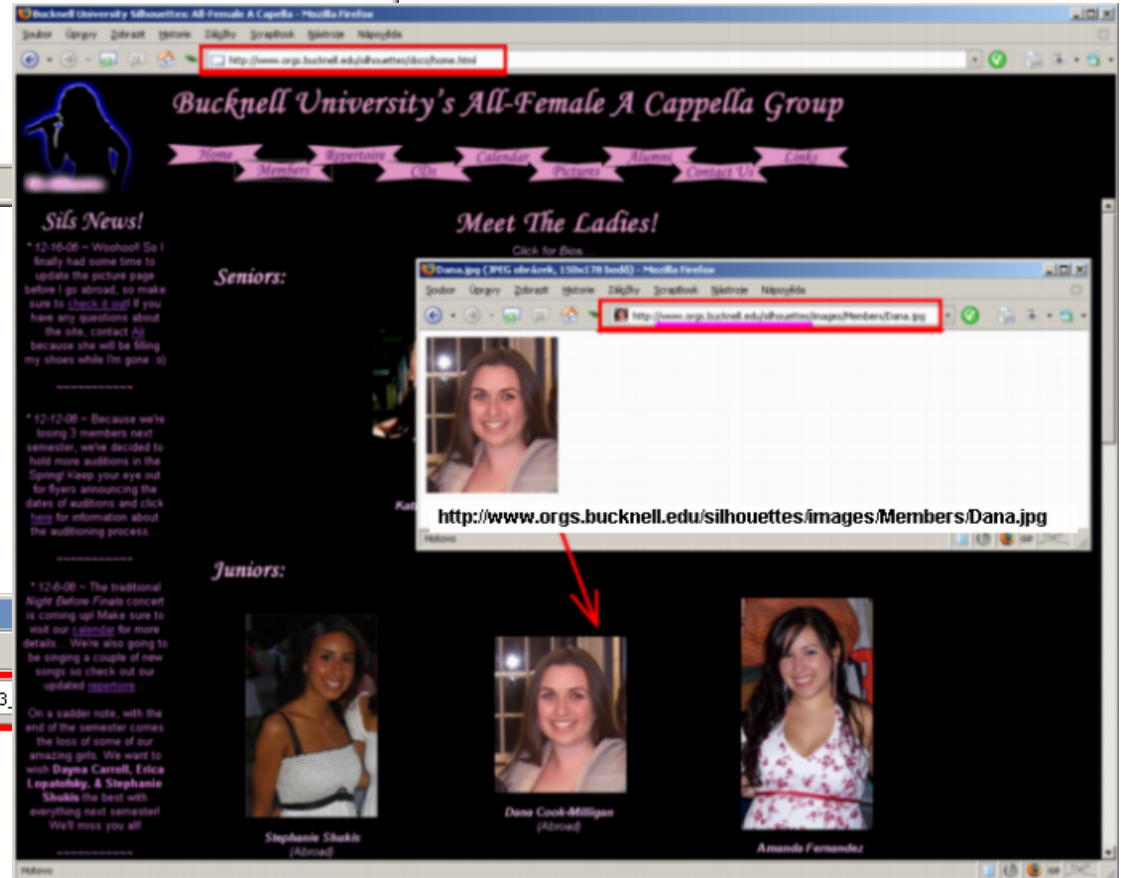
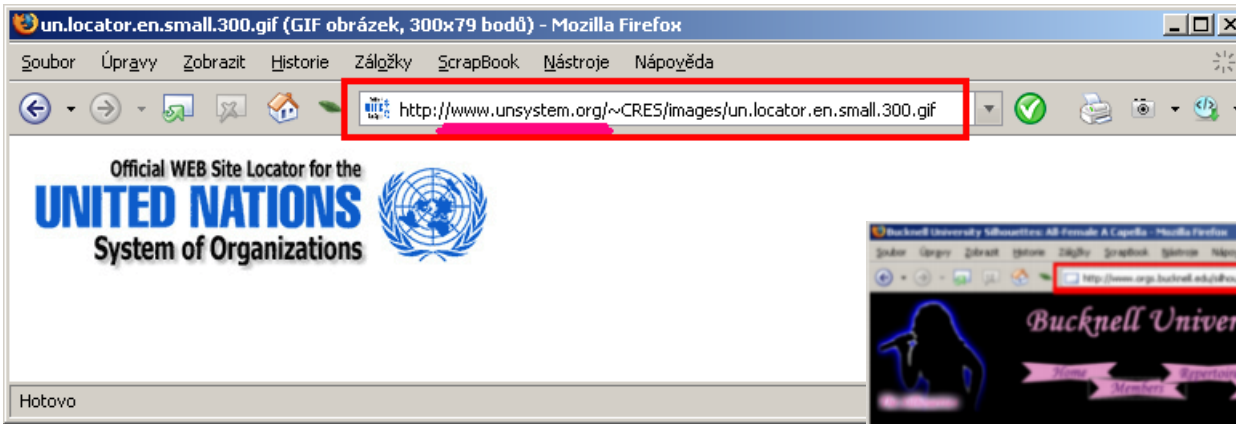
*Congratulations!! once again.*  
 Yours in service,

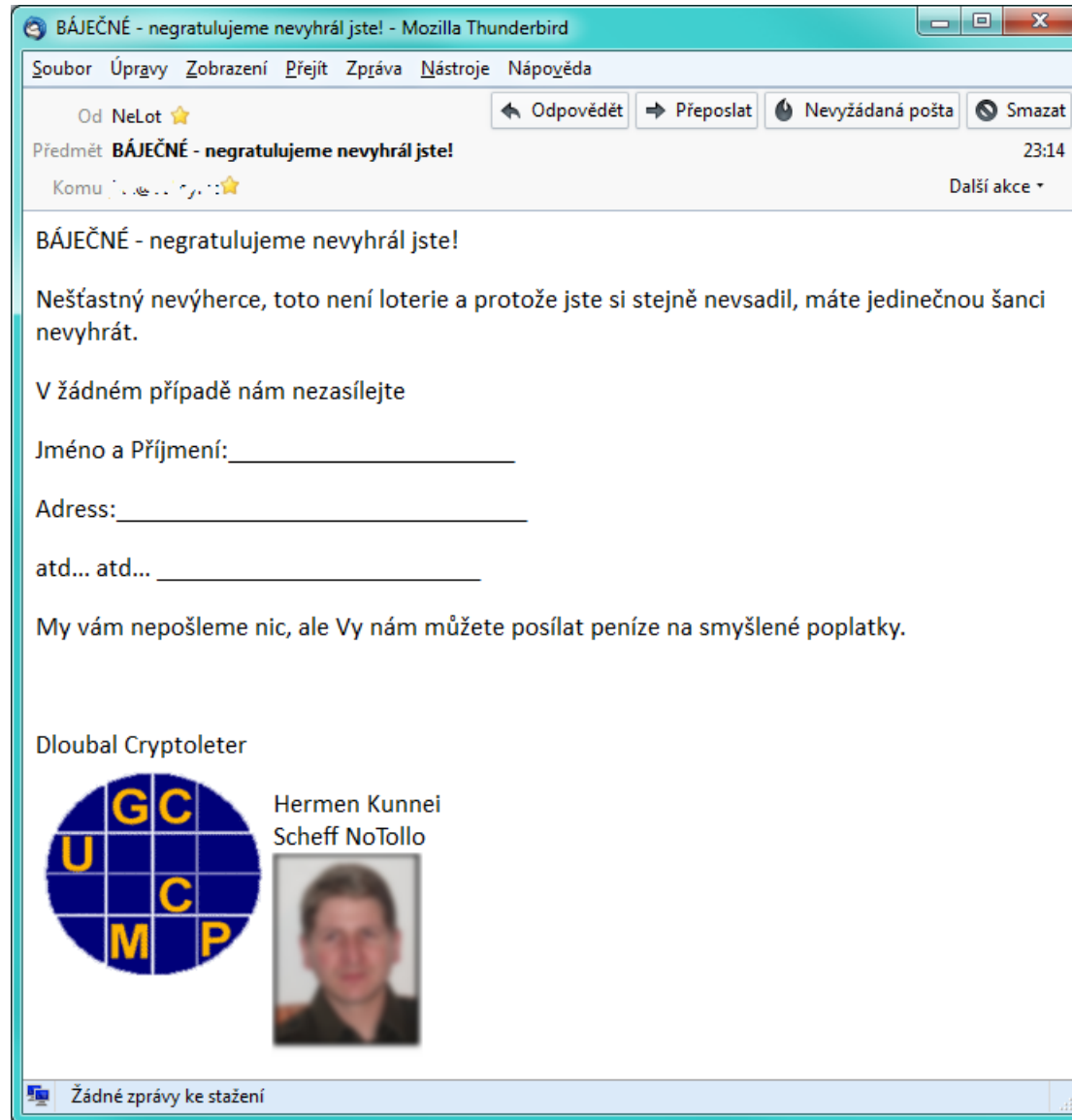
 ← **Obr.2**

 ← **Obr.3**

Mrs Samatha Woods  
 (Online co-ordinator)

Hotovo





# SCAM 419? Nejen z Nigérie

- **Obdoba dříve rozesílaných dopisů poštou nebo faxem - „Nigerijské dopisy“**
- **Uživatel dostane e-mail s oznámením:**
  - Je dědicem
  - Vdova po milionáři prosí o pomoc při převodu majetku z exotické země
  - Bankovní úředník hledá falešného dědice
- **Podvodníci poskytnou jakékoliv požadované dokumenty – falešné nebo získané**
- **Pro snadnou transakci je potřeba nejdříve zaplatit poplatek**
- **A pak další a další...**

## Ukázka z roku 2006

Dear Friend.

Thanks for your mail and for accepting my offer. I apologize for my late reply, it's due to my duty here. Since your last email to me on the month of August, i couldn't reply back because my troops were camping at the road to the jordanian border, that makes it difficult for me to check my mail. I have every proof of this transaction only i need your assistance in smuggling this money out of Iraq.

I am ready now to transfer the money to you after counting which took me days. The total amount is \$6.8million in \$100 bills. I want you to send your banking details to enable transfer the money. I will transfer it with the Bank of Baghdad, Iraq. They do International Transfer. I will not send it at once, i will transfer \$500,000 each transfer. After i finished the transfer, you will take 50% of the money and deposit the rest in your bank for me. I am giving you all the trust and i believe that with the help of God, we will sucessfully transfer this money out of Iraq.

Please do not disclose this deal to anybody as to protect my duty with the US Marine. I took my picture and the money picture which is in attached file below for your confirmation.

You can always contact with through [philip\\_coleman12@hotmail.com](mailto:philip_coleman12@hotmail.com) or [capt.philipcoleman2002@yahoo.com](mailto:capt.philipcoleman2002@yahoo.com) I will be waiting to hear from you as soon as possible to proceed.

Thanks.

Philip Coleman.



Fotografie  
přiložené  
k e-mailu

- **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 počítači který je součástí botnetu a hledá adresy*
- **Jak se mohu bránit?**
  - Kvalitní antispamový filtr
  - Neklikat na odkazy v e-mailech
  - Nereagovat na e-maily podvodníků

# MALWARE

- **Všeobecné označení pro škodlivý kód**

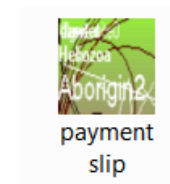
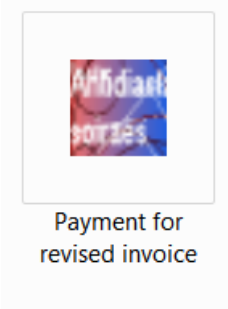
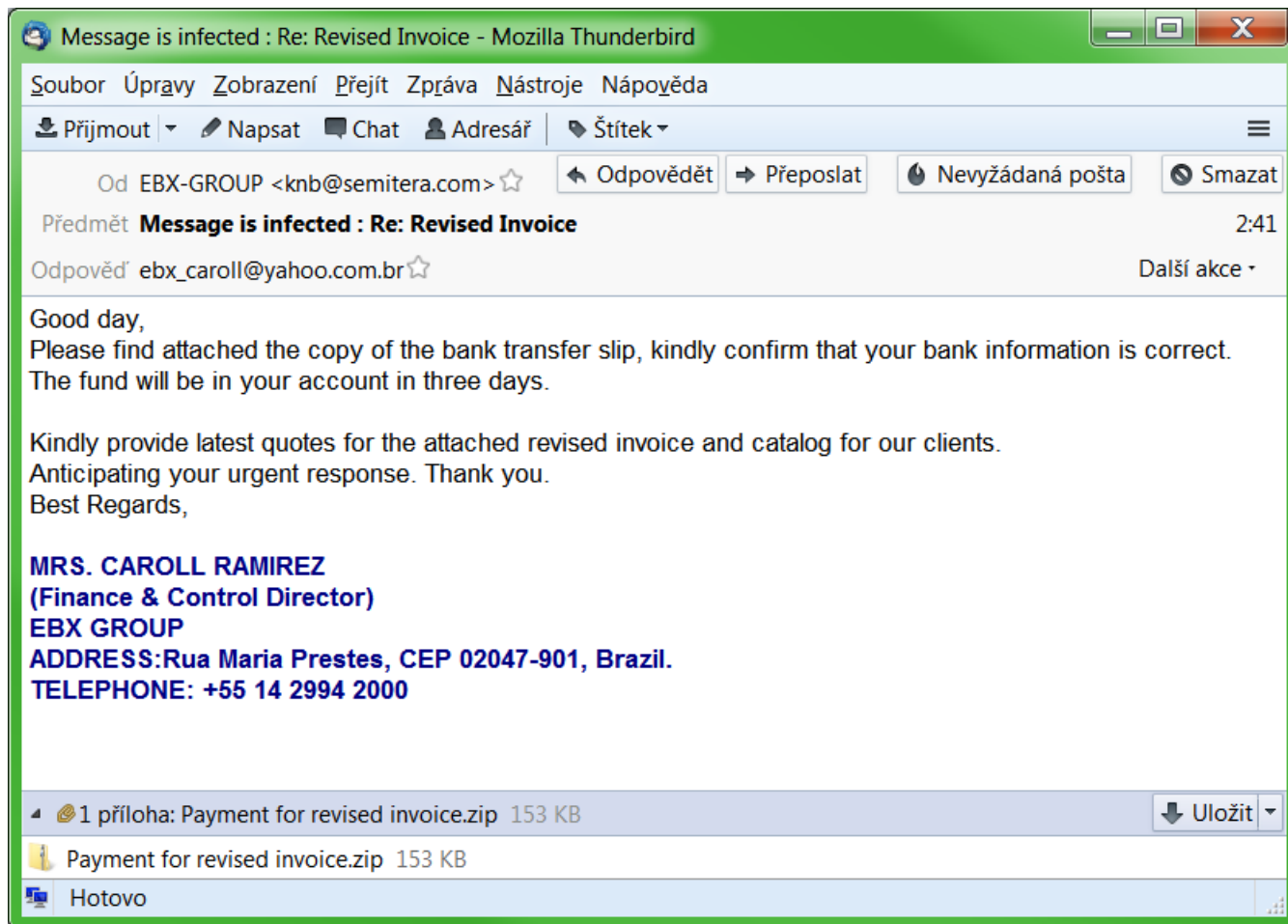
*Trojský kůň, virus, spyware...*

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

*Melisa, I love you...*



## Nejen anglické e-maily



## ale i „češtinsky“

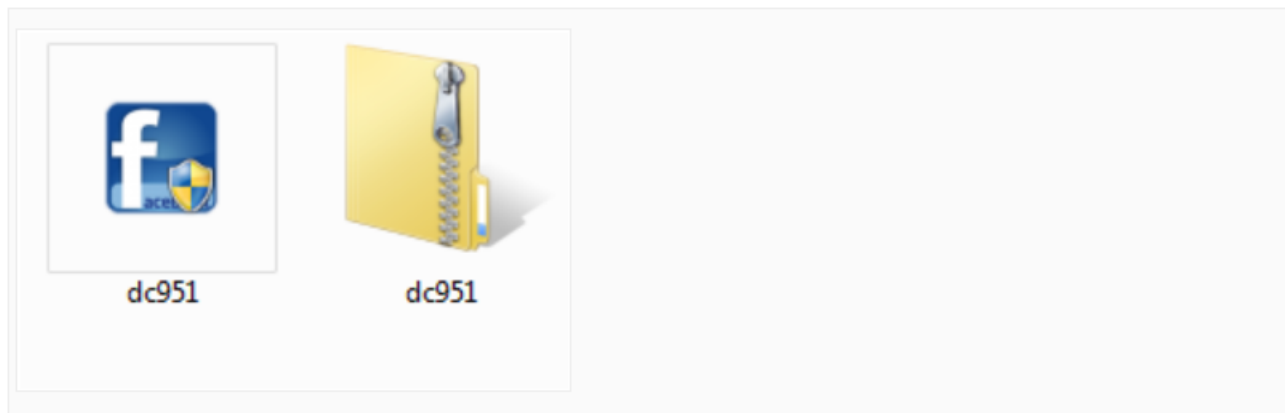
Dobrý den Man, moje\_adresa@email.cz

Nevím, jak to říct, ale já jsem snazil pred dlouhou dobu, aby vám poslal pár fotek, ale já jsem si myslel, ze si nejste zájem me videt.

Ale ted budu posílat vám Fotografie v dodatku.

Stáhnete si obrázky a extrahovat oni, jsem si jistý, ze se vám bude líbit, ze.Heslo je: 123456

Mají velký den.



Podezřelé soubory lze kontrolovat na: [www.virustotal.com](http://www.virustotal.com)



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



SHA256: 529e9038ae8e9db3d0a78421710613bfd78f8804e12a78146eff25202fc9fa3

File name: jinstall.exe

Detection ratio: 0 / 45

Analysis date: 2013-03-14 10:46:35 UTC ( 0 minut ago )



More details

Analysis

Additional information

Comments

Votes

Antivirus	Result	Update
Agnitum	-	20130313
AhnLab-V3	-	20130313
AntiVir	-	20130314
Antiy-AVL	-	20130313
Avast	-	20130314
AVG	-	20130314
BitDefender	-	20130314
ByteHero	-	20130313
CAT-QuickHeal	-	20130314

# Co dodat?

**Nejslabší článek je vždy mezi klávesnicí a židlí!**





***Děkuji za pozornost***

**Josef Džubák**  
**dzubak@hoax.cz**

