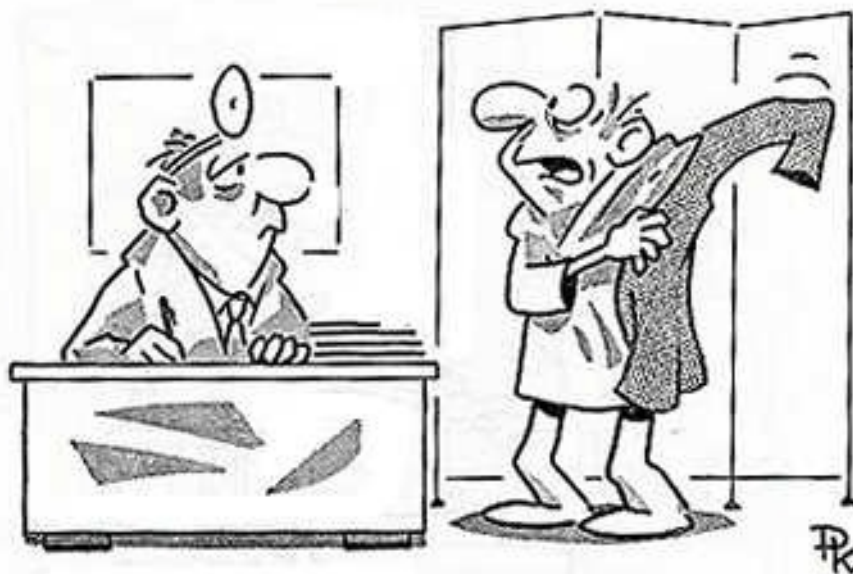


Spamming, phishing, pharming

Pavel Kácha <ph@cesnet.cz>, 2005



„Vy o tom alkoholismu dost víte, pane doktore.
Vy taky chlastáte?“

"Spam, lovely spam! Wonderful spam!"



- Hormel Foods Corporation
- Satirický skeč skupiny Monty Python Flying Circus
- MUDy – odrazování nováčků vkládáním textu ze skeče
- 1. spam – mail firmy DEC z roku 1998

Definice

- Nejasná
- **UCE** (Unsolicited Commercial Email) – komerční
- **UBE** (Unsolicited Bulk Email) – nyní nejčastější
 - nevyžádaný
 - cílená pracovní nabídka, obchodní oslovení
 - hromadný
 - newslettery, informace zákazníkům, diskusní listy

Shit Posing As Mail

Typy

- Reklama
- Podvody (spam 419)
- Phishing
- Řetězové maily
- Virus/Worm



"Bale testu jste náchylný k parazitním chorobám."

Nemailové typy

- SPIM – instant messaging
- SPIT – internet telephony
- SPLOG/BLAM – blog spamming
- Spamdexing
 - splog/blam
 - referer spam
 - Google bombing

Google bombing

The image displays two overlapping browser windows from the year 2005, illustrating a Google bombing. The left window shows a search for "miserable failure" on Google, with the top result being the "Biography of President George W. Bush" from the White House website. The right window shows a search for "velky bratr" (Big Brother) in Czech, with the top result being a page from "wtd.vlada.cz" titled "Podobné stránky". Below this, there are links to "BB - News" and "LUPA: Evropský velký bratr". The "LUPA" result is highlighted, showing a snippet about a letter received in the wake of the 9/11 attacks. The search results for "velky bratr" include a search time of 0.08 seconds and approximately 586,000 results.

miserable failure - Vyhledat Googlem

File Edit View Go Bookmarks Tools Tabs Help

http://www.google.com/s

Google Web Obrázky Skupiny Adresář

miserable failure

Prohledat Internet Stránky pouze

Web Výsledky 1 - 10 z asi 2 630 000 pro **miserable failure**.

Biography of President George W. Bush
Biography of the 43rd President of the United States.
www.whitehouse.gov/president/gwbbio.html - 25k -
Archiv - Podobné stránky
[News](#) - [Contact](#) - [President](#) - [Homeland Security](#)
[Další stránky z www.whitehouse.gov »](#)

Welcome to MichaelMoore.com!
Official site of the gadfly of corporations, creator of the film Roger Me
and the television show The Awful Truth. Includes mailing list, me
board, ...
www.michaelmoore.com/ - 39k - 10 listopad 2005 -
Archiv - Podobné stránky

velky bratr - Vyhledat Googlem

File Edit View Go Bookmarks Tools Tabs Help

http://www.google.com/search?hl=cs&q=velky

Google Web Obrázky Skupiny Adresář

velky bratr

Prohledat Internet Stránky pouze česky

Web Výsledky 1 - 10 z asi 586 000 pro **velky bratr**. (0,08 sekund)

wtd.vlada.cz/scripts/detail.php?id=2339
[Podobné stránky](#)

BB - News - n@va vás baví
Projekty. Česko hledá SuperStar, Eso, Hanka Kynychová, Chcete být milionářem? M*A*S*H, Natočto! Nova VIP, Novashop, Peříčko, Pojišťovna štěstí ...
bigbrother.nova.cz/ - 28k - 10 listopad 2005 -
[Archiv](#) - [Podobné stránky](#)

LUPA: Evropský velký bratr
Evropský **velký bratr**. Jedna ze zpráv, která dorazila v návaznosti na teroristické útoky v Londýně, informovala o záměru schůzky ministrů zemí EU, ...
www.lupa.cz/clanek.php?id=4270_121k - [Archiv](#) - [Podobné stránky](#)

Sponzorované odkazy

Big Brother
Jak vypadá život ve vile?
Fakta, fotogalerie.
www.idnes.cz

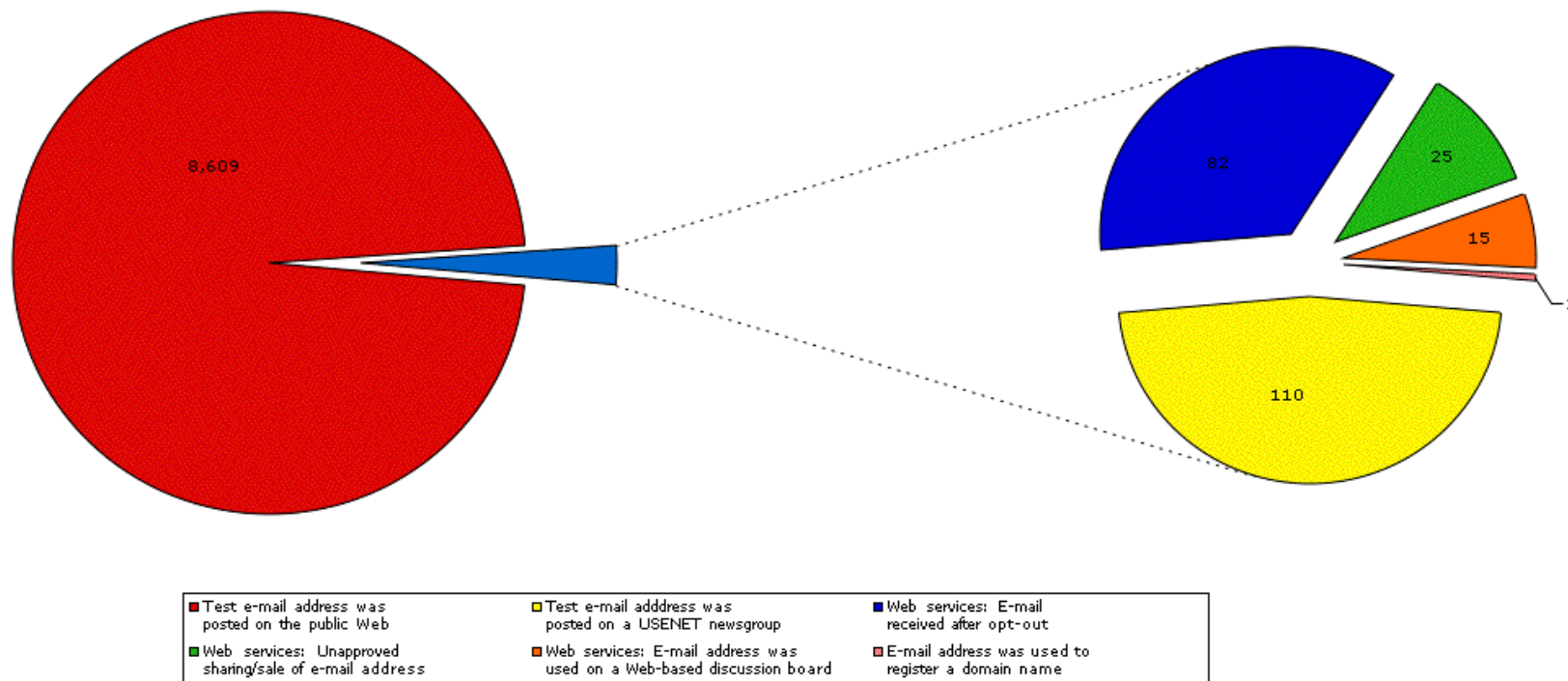
Velky bratr
Denně články, drby a exkluzivní info o reality show **Velky bratr**
bigbrother.atlas.cz

Šíření

- Openrelay (na ústupu)
- Etablování specialisté
 - [ROKSO](#) – The Register of Known Spam Operations
- Zombie PC – dnes nejčastější
 - nepodceňujte hlášení o zdrojích spamu, obvykle znamenají zkompromitovaný stroj, který je součástí tzv. botnetu

Získávání emailových adres

**Where did the spammers get the e-mail address?
Number of e-mails received, based on where the
address was posted or disclosed**



Boj proti spamu



"Rukáv, rukáv... vyhrňte si rukáv! Člověče vy musíte být úplně blbej. Už jsem vám to dnes řekl nejmíň padesátkrát."

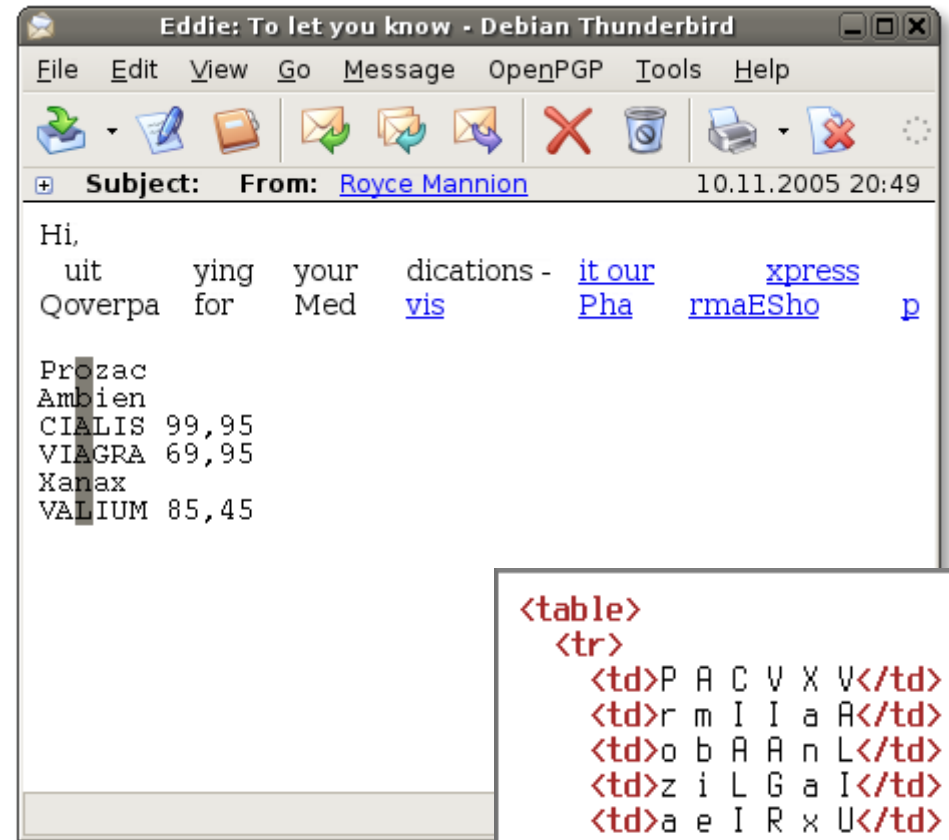
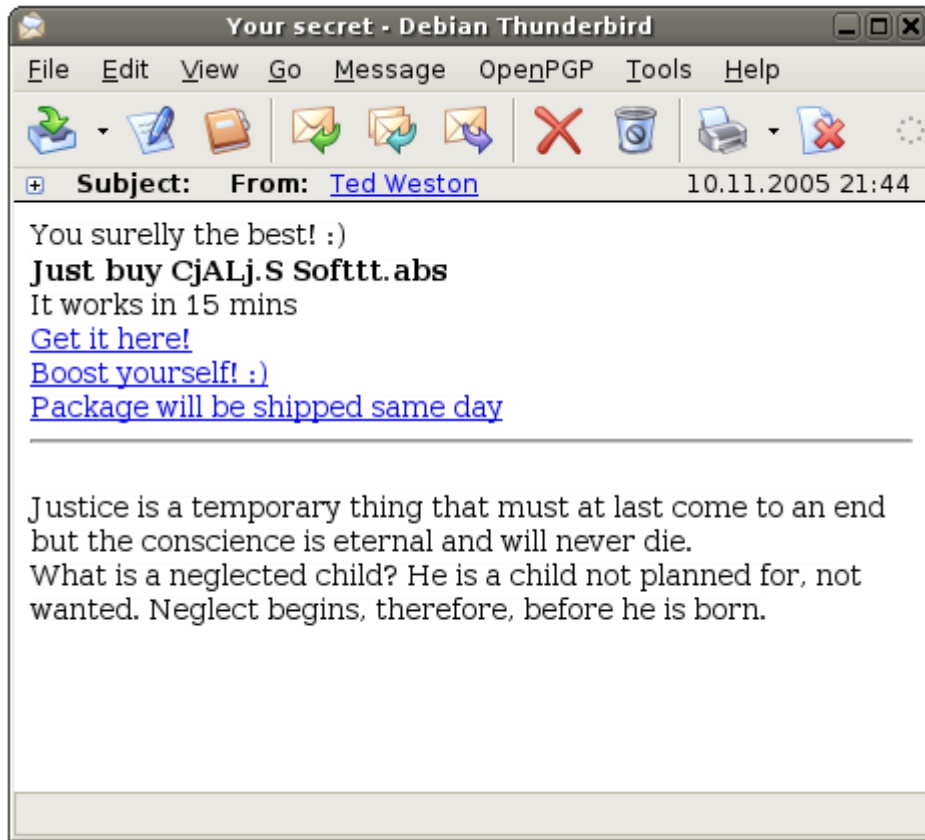
Boj uživatelů

- Znečitelnění adres pro stroj
 - ph **at** cesnet **dot** cz
 - javascript, CSS, mail v obrázku
 - ♦ po zralé úvaze – obvykle koliduje s přístupností
- Pro odkazy, generované třetími osobami, používat `` (splog)
- Neodpovídat na nabídky na vyřazení z databáze adres
- Hlásit poskytovateli – usnadňující služby pro uživatele
 - SpamCop, Network Abuse Clearinghouse

Statistická analýza

- První nejznámější propagátor – Paul Graham
- Naivní Bayesovská statistická analýza
 - ifile, Annoyance Filter, DSPAM, BogoFilter
 - v poslední době integrována do MUA (Thunderbird)
- Komplexnější statistická analýza
 - CRM114 – fráze, testbed pro další metody
- Spammeri se také učí
 - nadbytečný text, prokládání HTML, obrázky, tabulky

Snahy o překonání statistické analýzy



```
<table>  
<tr>  
<td>P A C V X V</td>  
<td>r m I I a A</td>  
<td>o b A A n L</td>  
<td>z i L G a I</td>  
<td>a e I R x U</td>  
<td>c n S A . M</td>  
</tr>  
</table>
```

= Spammer je převít líná, ale vynalézavá.

Kontrolní součty

- Uživatelé reportují spam do databáze
- Klient spočítá „otisk“ spamu a porovnává s databází, zda už nebyl reportován
- problém s jednoznačností – i jeden spam je variabilní
 - namátkové otisky
 - „fuzzy“ otisky
- nilsimsa, Vipul's Razor, Distributed Checksum Clearinghouse, Pyzor

Komerční pokusy

- **Habeas Sender Warranted Email**
 - odesílatel si kupuje právo přidat do hlavičky mailu haiku, chráněné copyrighitem firmy Habeas, která může (a snaží se) stíhat původce mailů takto označených neautorizovaně
- **Bonded Sender**
 - odesílatel si kupuje záznam v DNSBL, které pak může okolní svět používat

DNSBL – DNS blacklists

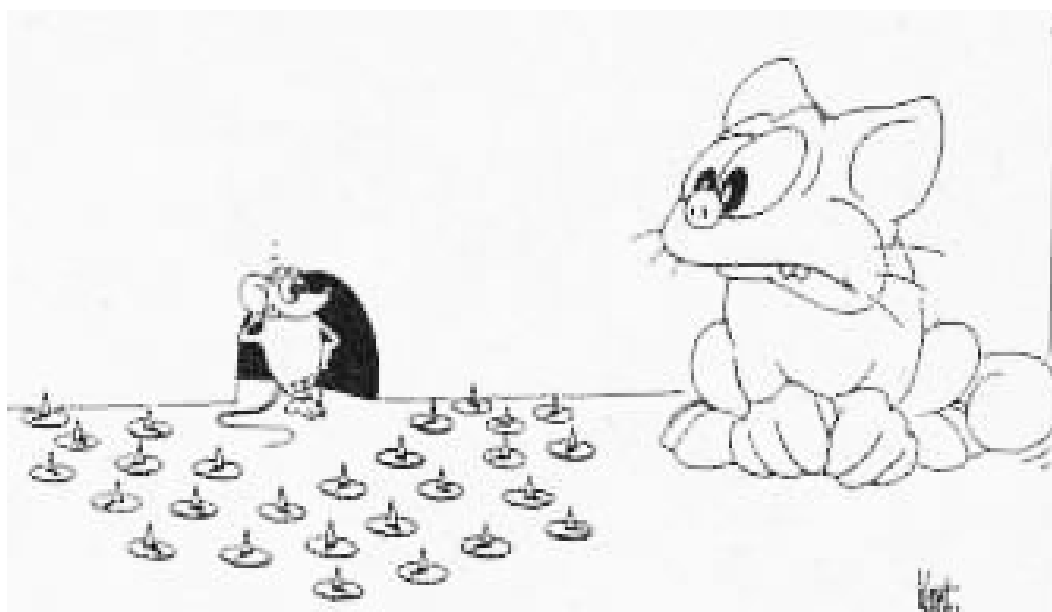
- Cílový mailserver se může dotázat v databázi, dostupné pro jednoduchost přes DNS, na důvěryhodnost odesílatelského mailserveru
- Statické, distribuované, ruční, automatizované → **MOC**
- Obsah na základě různých pravidel
 - Vytáčené a kabelové pooly adres
 - Poskytovatelé, nedodržující RFC (postmaster@...)
 - Poskytovatelé, nereagující na spam
 - IP serverů, ze kterých byl několikrát nahlášen spam
 - IP serverů, na kterých běží reklamní či phish WWW - RHSBL
 -

DNSBL – DNS blacklists 2

- ORDB – open relays
- SpamHaus SBL – prověření spammeři
- SpamHaus XBL – exploity, proxy, trojské koně
- RFC-Ignorant – chybné WHOIS info
- DEADBEEF – nereagující poskytovatelé
- MAPS (komerční), NJABL, SORBS, DNSBL, DNSRBL
- SPEWS – kontroverzní, celé bloky
- DRBL – snaha o decentralizované dynamické RBL

DNSBL – DNS blacklists 3

Používejte s rozvahou, nejlépe jako součást inteligentnějšího systému (vážení, klasifikace), neboť DNSBL nejsou stoprocentní a díky chybě v jednom z nich se k Vaším klientům nemusejí dostat nejen spammeři, ale ani nikdo jiný.



Heuristika

- Spojte všechny předchozí metody váženou klasifikací a získáte **SpamAssassin**
- Fráze, podezřelé znaky (např. barvy a zvýraznění), statistická analýza, DNSBL, podezřelé/zmanipulované hlavičky, maskující text...
- Začínáte-li a nejste si jisti, je to pravděpodobně nejrozumnější volba



Autorizace odesílatele

- **SPF** – Sender Permitted From
 - sám poskytovatel zveřejní v DNS, jaké IP v jeho síti smějí odesílat poštu – příjemce ověří a k jiným IP se může chovat macešsky
- **TEOS** – Trusted Email Open Standard
 - databáze autorizovaných adres
- **DomainKeys**
 - server odesílatele přidá do hlavičky podpis, jehož veřejný klíč je zveřejněn v DNS
- **Tripoli**
 - nahrazuje DNS podpisem authority

Autorizace odesílatele 2

- HashCash

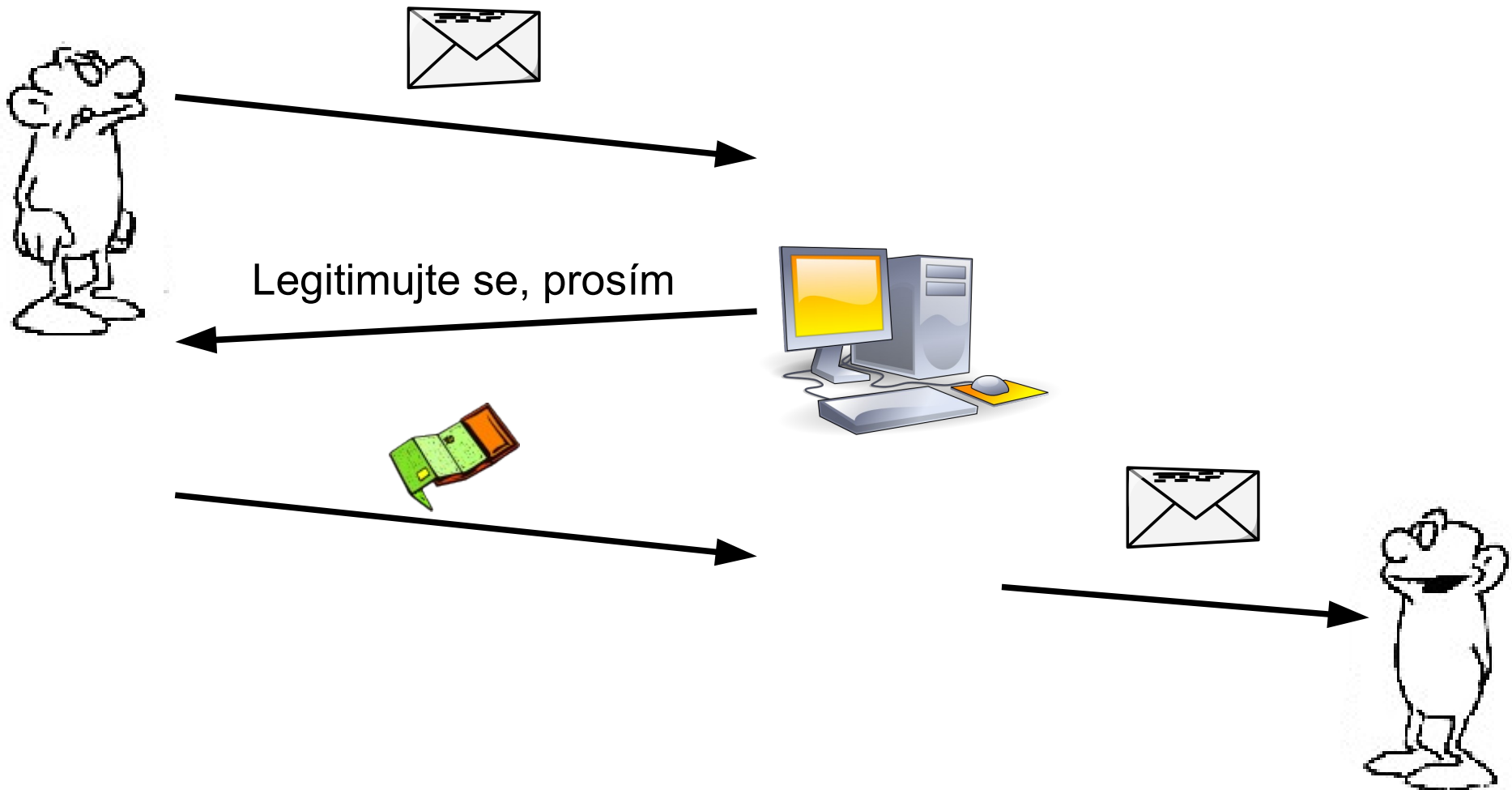
- Odesílatel do mailu přibaluje matematický hash, který je navržen tak, aby ho stál řádově víc výpočetního výkonu, než příjemce jeho ověření
- Spammer tak odešle dva maily za vteřinu namísto stovek

- HAM passwords

- Odesílatel je (pokud získává cílový email legálně) poučen, jaký text má přidat do subjectu – maily, které ho neobsahují, může cíl zahazovat

Challenge-response

Autentizace prvního mailu



Challenge-response 2

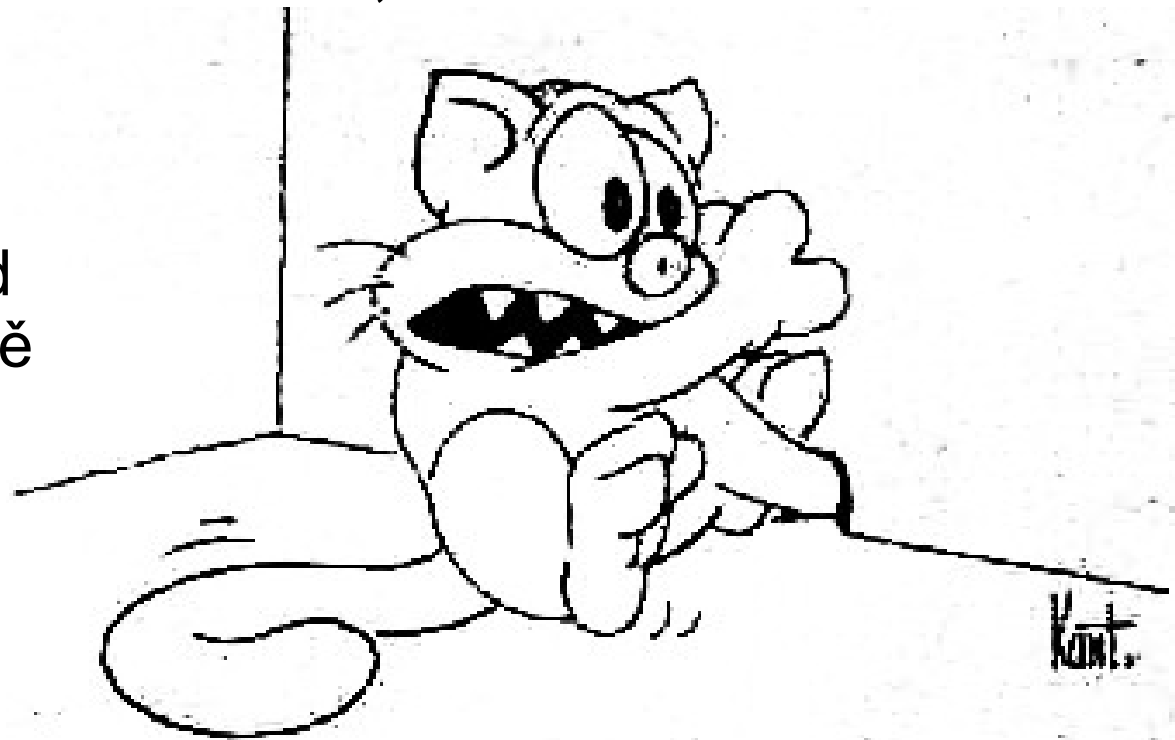
- Nutná erudice a pozornost uživatelů
 - Mailing listy, legitimní hromadné maily
 - Konflikt několika různých systémů
- Viry/Wormy – falešná adresa odesílatele
 - Uživatelé se sami objevují na spamlistech
- Komplikují život nejen spammerům, ale i legitimním odesílatelům. Odesílatelé často nejsou ochotni být do hry zataženi, nebo „challenge“ mail považují sami za spam
- TDMA, Mailblocks a jiné webmaily

Greylisting

- Mailserver na každý mail od nového odesílatele nebo serveru odpoví dočasnou chybou - „zkus to znovu“. Při druhém pokusu je mail přijat
- Spammeri používají obvykle specializovaný software, který se o chyby nezajímá
- x Některé legitimní mailservery berou chybu fatálně
- x Nebo to zkusí příliš pozdě, nebo z jiné adresy (mailserverové farmy)
- x Zpožďuje veškerou poštu, nejen spam
- Postgrey, SQLGrey, RelayDelay, qmail-ssp

Pasti

- Sbírkky falešných adres na webové stránce
- Honeypot
 - Server, na který je směřován spam (například na falešné adresy), ten ho potom hlásí **DNSBL**, **Razoru**
- Tarpit
 - Server, kam jsou směřována spojení od spammerů, a následně zpomalována na hranici možností



„Povídam, pustte mē, potvory!“

Chování serveru

- Odmítání rozpoznaného spamu už na SMTP
 - Při falešném pozitivu nedoručenka odesílateli
 - Viry lze s přimhouřením očí zahazovat
- (Greylisting)
- Přijetí a zpracování na serveru
 - Server si s rozpoznaným spamem musí poradit sám
 - Ukládání do speciální složky uživateli
- Škracení zlobivých serverů
 - Na základě klasifikace, nebo nedoručitelnosti mailů
 - [spamhammerd](#)

Phishing, pharming



Přines mi toho druhýho červa!

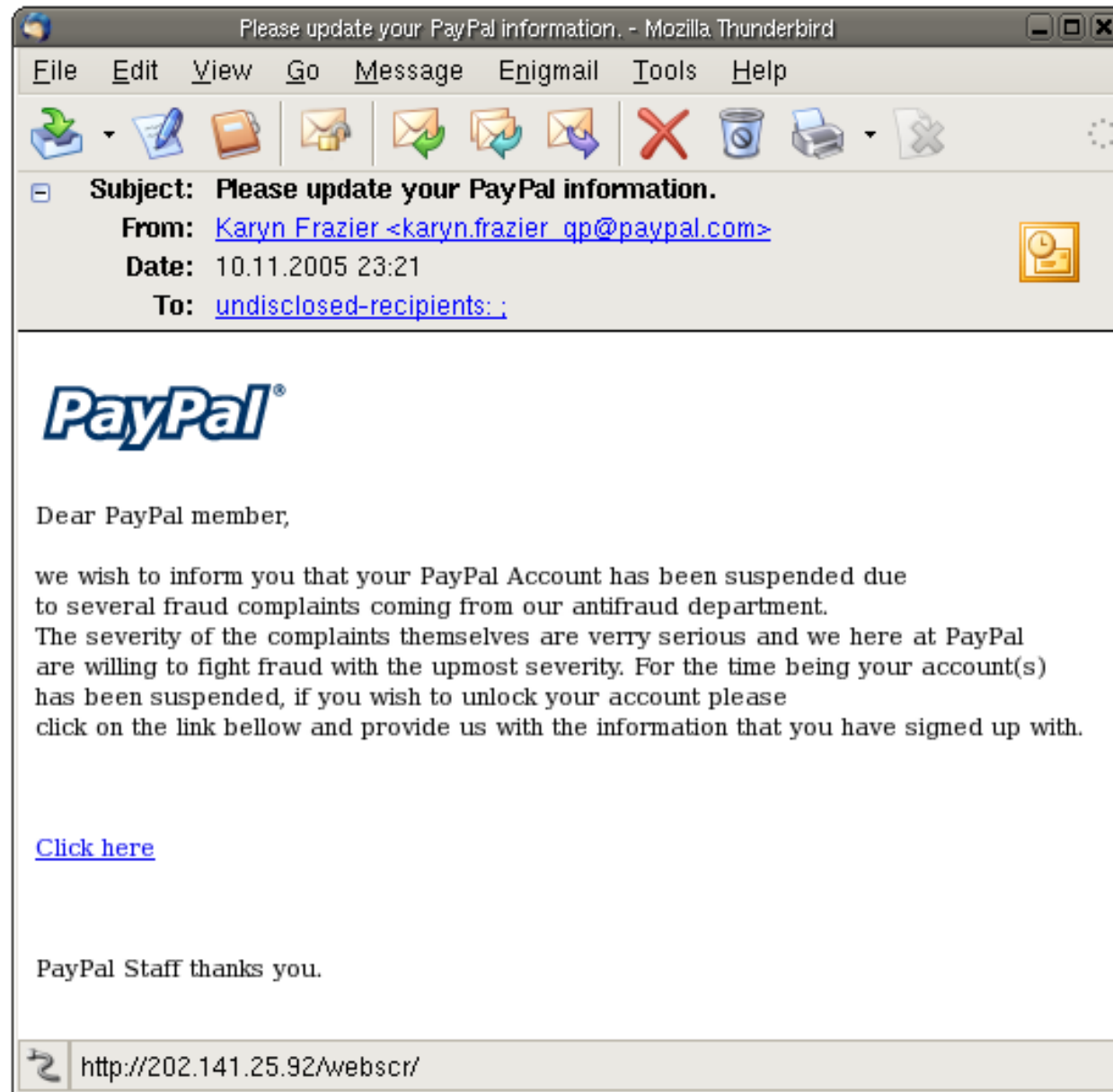
Phishing

- Spam, směřující uživatele na podvrženou stránku, připravenou tak, aby uživatele přesvědčila k vyzrazení osobních dat
- Stránka obvykle impersonuje banku, internetového prodejce, ukládá data a nedůležitou komunikaci posílá skutečnému serveru
- Mohou být i SSL prostředníci
- Nebo i malware na stroji uživatele, logující data

Phishing - znaky

- Přehlednutelně chybná URL
 - *www.banka.cz@23w3643ad.yahoo.com*
 - *www.banka.cz.localhosting.provider.com*
 - *www.banka.cz@192.168.0.10*
- S internacionalizací DNS se objevil **Homograph spoofing attack**
- Mail je obecný – organizace obvykle maily zákazníkům personalizují
- Výhrůžky zrušením účtu

Phishing - příklad



Pharming

- Modifikace zkompromitovaného DNS
- Malware, modifikující DNS lokální stanice
- **DNS Cache Poisoning**
 - S odpovědí na DNS dotaz může tazatel dostat i nadbytečné „pomocné“ informace
 - Ty ale mohou být podvržené, neměl by se jimi tedy řídit
 - Tím ale někdy vzniká problém s GLUE záznamy

DNS Cache Poisoning

```
ph@hideo:~  
grey:~$ dig ns cesnet.cz  
  
; <<> DiG 9.3.1 <<> ns cesnet.cz  
;; global options: printcmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42414  
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 2  
  
;; QUESTION SECTION:  
;cesnet.cz.                IN      NS  
  
;; ANSWER SECTION:  
cesnet.cz.                86400  IN      NS      ns.cesnet.cz.  
cesnet.cz.                86400  IN      NS      ns.cesnet.net.  
  
;; ADDITIONAL SECTION:  
ns.cesnet.net.           86400  IN      A       195.113.144.233  
ns.cesnet.cz.           86400  IN      A       195.113.144.194  
  
;; Query time: 0 msec  
;; SERVER: 195.113.144.194#53(195.113.144.194)  
;; WHEN: Sun Nov 13 00:22:49 2005  
;; MSG SIZE rcvd: 100  
  
grey:~$ █
```

Obrana

- Heuristika – DNSBL
- I uživatelé by měli ověřovat autenticitu druhé strany
- Posilování autentizace
 - Soukromé fráze a vizuální háčky
 - Tokeny
 - Certifikáty
- Vzdělávání uživatelů



Děkuji za pozornost.

- Obrázky

- © Pavel Kantorek,

- http://kantorek.webzdarma.cz/kantorek_f.htm

- © Josef Čapek,

- <http://www.puzzleshop.cz/img/katalog/094017.jpg>

- Public Domain, <http://openclipart.org/>