



Spam! Spam! Spam! Spam!
Lovely Spaaam! Wonderful Spaaam!
Lovely Spaaam! Wonderful Spam.

Spa-a-a-a-a-a-am.
Spa-a-a-a-a-a-am.
Spa-a-a-a-a-a-am.
Spa-a-a-a-a-a-am.

Lovely Spaaam! (Lovely Spam!)
Lovely Spaaam! (Lovely Spam!)
Lovely Spaaam!

Spaaam, Spaaam, Spaaam, Spaaaaaam!

[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 1 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)

Systemy walki ze spamem

Marcin Sochacki
wanted@linux.gda.pl

Linux Academy, Kraków, 2002



[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 2 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)

1. O czym będziemy mówić?

1. Definicja spamu
2. Historia
3. Metody działania spammerów
4. Metody walki
 - kryteria podziału systemów antyspamowych
 - metody prewencyjne
 - wczesne blokowanie
 - analiza treści
 - metody prawno-administracyjne
5. Pojęcia i terminy związane ze spamem
6. Podsumowanie
7. Odsyłacze



[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 3 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)

2. Definicja spamu

Wiadomość elektroniczna jest spamem, jeżeli:

- treść i kontekst wiadomości są niezależne od tożsamości odbiorcy, ponieważ ta sama treść może być skierowana do wielu innych potencjalnych odbiorców,
- jej odbiorca nie wyraził uprzednio możliwej do weryfikacji, zamierzonej, wyraźnej i zawsze odwoływalnej zgody na otrzymywanie tej wiadomości,
- treść wiadomości daje odbiorcy podstawę do przypuszczeń, że nadawca wskutek jej wysłania może odnieść korzyści nieproporcjonalne w stosunku do korzyści odbiorcy wynikających z jej odebrania.

(PolSpam.org)



[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 4 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)



[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 5 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)

2.1. Inne definicje:

- „Masowy list wysłany przez nieznanego” („Bulk Mail from a Stranger”)

(Brad Templeton)

- Nieuzasadniony cross-posting w Usenecie
- Wysyłanie masowych komunikatów na IRC, chat-ach, IM, itp.
- Oszukiwanie systemów indeksujących WWW



2.2. Często popełniane błędy przez przeciwników spamu:

- mówienie, że spam to tylko listy komercyjne (UCE – „Unsolicited Commercial E-mail”)
- nadgorliwość prowadząca do szkodenia niewinnym użytkownikom (*false positives*, blokowanie dużych zakresów IP)
- kłótnie w ramach „środowiska”
- pogląd, że spam jest największym problemem Internetu
- złudna nadzieja, że spam można zwalczyć metodami legislacyjnymi

[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 6 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)

2.3. Porównanie spamu „papierowego” i „elektronicznego”

Podobieństwa:

- anonimowość nadawcy
- łatwość pozyskania dużej liczby odbiorców
- forma i treść komunikatu

Różnice:

- proporcje kosztów ponoszonych przez nadawcę i odbiorcę
- sposoby blokowania
- regulacje prawne



[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 7 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)



2.4. Dlaczego spam jest zły i należy z nim walczyć?

- marnowanie czasu
- utrudnia pracę ludziom uzależnionym zawodowo od e-maila
- narusza prywatność użytkowników Internetu poprzez gromadzenie danych osobowych ze wszystkich możliwych źródeł
- zmusza ludzi do ukrywania swojego prawdziwego adresu, w efekcie utrudniając legalną komunikację z nimi
- bardzo wysokie koszty generowane dla ISP

[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 8 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)

3. Geneza spamu

3.1. 1937: Hormel Foods



[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 9 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)



- „Shoulder Pork and hAM”/„SPiced hAM” – „mielonka z szynki”
- Strona domowa: <http://www.spam.com/>: fan club, drzewo genealogiczne, sklep z pamiątkami, muzeum SPAM-u
- Q: Who came up with the name SPAM?
A: Jay C. Hormel wanted a name as distinctive as the taste, so he held a contest. Kenneth Daigneau, an actor and brother of a Hormel vice president, pocketed the \$100 prize.
- najbardziej niezwykły przepis na SPAM: pythonowski „homar z krewetkami w białym sosie, pasztetem z trufli, brandy, jajkiem sadzonym na wierzchu i SPAM”.

Strona główna

Strona tytułowa

Spis treści



Strona 10 z 40

Powrót

Full Screen

Zamknij

Koniec



[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 11 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)



[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 12 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)



[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 13 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)

3.2. 1971: Monty Python

- mistrzowie absurdu prezentują skecz o mielonce w „Latającym Cyrku Monty Pythona”



3.3. 1978: Pierwszy spam

Mail-from: DEC-MARLBORO rcvd at 3-May-78 0955-PDT
Date: 1 May 1978 1233-EDT
From: THUERK at DEC-MARLBORO
Subject: ADRIAN@SRI-KL
To: DDAY at SRI-KL, DAY at SRI-KL, DEBOER at UCLA-CCN,
To: WASHDC at SRI-KL, LOGICON at USC-ISI, SDAC at USC-ISI,
To: DELDO at USC-ISI, DELEOT at USC-ISI, DELFINO at USC-ISI,
To: DENICOFF at USC-ISI, DESPAIN at USC-ISI, DEUTSCH at SRI-KL,
[...]
cc: BPM at SU-AI

MCKINLEY@USC-ISIB
MMCM@SRI-KL
[...]
DIGITAL WILL BE GIVING A PRODUCT PRESENTATION OF THE NEWEST MEMBERS
OF THE DECSYSTEM-20 FAMILY; THE DECSYSTEM-2020, 2020T, 2060, AND 2060T.

[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 14 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)



- miał dotrzeć do **wszystkich** użytkowników ARPANET-u :)
- błąd nadawcy nie znającego zbyt dobrze systemu pocztowego (adresy w treści listu)
- firma przeprosiła za ten incydent

3.4. lata 80-te: MUD-y

- Multi-User Dungeon – przygodowe gry tekstowe
- jako „spam” określano zasypywanie innych uczestników gry bezsensownymi komunikatami, a także próby zawieszenia serwera

[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 15 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)



[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 16 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)

3.5. 1990–94: pierwsze znaki spamu w Usenecie

- „Make Money Fast” – łańcuszek szczęścia
- „Global Alert for All: Jesus is Coming Soon” – pierwszy poważny spam w Usenecie, cross-post do wszystkich istniejących grup



3.6. kwiecień 1994: pierwszy wysłany z premedytacją spam komercyjny

- „Green Card Lottery – Final One?“, wysłany przez firmę Canter and Siegel
- pomimo ogromnej fali sprzeciwów i zemsty użytkowników Usenetu, nadawcy byli dumni ze swojego wynalazku
- plany prowadzenia usług mailingowych dla klientów
- publikacja książki o niezwykle długim tytule „How to Make a Fortune on the Information Superhighway: Everyone’s Guerrilla Guide to Marketing on the Internet and Other On-Line Services.”
- książka sprzedawała się bardzo słabo i założyciele firmy odeszli w cień

[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 17 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)



3.7. od 1997 do dzisiaj: zmiana orientacji, nowe media

- stabilizacja aktywności spamerów w Usenecie
- zalew spamu poprzez e-mail, głównie za sprawą rozwoju WWW, łatwości pozyskiwania adresów i większej skuteczności
- wykorzystywanie do spamowania nowych mediów, głównie usług IM (Instant Messaging), np. ICQ, AIM, MSN, Gadu-Gadu

[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 18 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)



[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 19 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)

3.8. 2001–2002: wyrafinowane metody

- spam w publicznych księgach gości, chat-ach
- wyrafinowane spamowanie serwisów WWW za pomocą nagłówka HTTP Referrer:
- wykorzystanie usługi Messenger (Poślaniec) istniejącej od lat w systemach Microsoftu, ale upowszechnionej za sprawą Windows 2000 i XP, w których jest ona domyślnie włączona



4. Jak w praktyce działają spamerzy?

Uwaga: dotyczy głównie e-maila.

4.1. Pozyskanie bazy adresowej

- przeszukiwanie stron WWW (*harvesters* – żniwiarki), Usenetu, „łańcuszki”
- zakup bazy od innego spamera
- metoda chybił–trafił

[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 20 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)



4.2. Ustalenie treści spamu

- podawanie jak najmniejszej ilości danych adresowych nadawcy
- nadanie „chwytliwej” formy, zwłaszcza tematu listu (musi nakłonić do przeczytania treści)
- osadzenie *web bugs*, czyli obrazków w listach HTML-owych, umożliwiających śledzenie skuteczności spamu
- „zaciemnianie” treści w celu ominięcia filtrów:

```

```

```
<html><neosusili><sonemque><neosusili><sonemque><neosusili>  
We would like to send you a FR<neosusili>EE Euro  
and a F<neosusili>REE report on <sonemque>world currency.  
Full opt-<neosusili>out instructions on the bot<sonemque>tom  
of the site  
</html>
```

[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 21 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)



- dalsze „zaciemnianie” treści poprzez ukrywanie prawdziwych URL-i:

`http://3064945162/ (182.175.90.10)`
`http://www.mbank.com.pl@mbank.prv.pl/`
`javascript...`

- dodanie standardowych formułek nt. źródła pozyskanych adresów, możliwości rezygnacji (*opt-out*), legalności wysyłania spamu

[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 22 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)



[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 23 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)

4.3. Wysyłka

- cel: wysłanie jak największej liczby wiadomości jak najmniejszym kosztem (czasu i pieniędzy)
- wybór metody i oprogramowania
- wykorzystanie *open relays*

4.4. Specyfika protokołu SMTP

- umożliwia wysyłanie anonimowych przesyłek
- *open relays* – otwarte serwerów SMTP umożliwiające spamerom szybkie zwielokrotnienie liczby listów

```
$ telnet victim 25
Trying 10.10.10.25...
Connected to victim.
Escape character is '^]'.
220 victim ESMTP Fri, 06 Dec 2002 11:15:47 +0100
HELO spamer
250 victim Hello spamer [10.19.120.240]
MAIL FROM: john@example.com
250 <john@example.com> is syntactically correct
RCPT TO: mary@example.com
250 <mary@example.com> verified
RCPT TO: alice@example.com
250 <alice@example.com> verified
DATA
354 Enter message, ending with "." on a line by itself
From: Friend <friend@example.com>
To: You
Subject: Make Money Fast

Make $$$
.
250 OK id=18KFXd-0001nG-00
```



[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 24 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)

5. Metody walki ze spamem

5.1. Reguły dla antyspamera

Reguła 1. Wszystko co mówi spamer jest kłamstwem.

Reguła 2. Jeśli masz wątpliwości, patrz Reguła 1.

Tłumaczenie popularnych zwrotów:

Spamerski	Polski
Aby usunąć twój adres	Aby potwierdzić, że to jest działający adres
To nie jest spam	To jest spam
Zamówiłeś informację	Mamy nadzieję, że uwierzysz w to, że mamy do sprzedania most
WAŻNE!	Czy znasz słowo „bzdura”?
Wprowadź numer swojej karty kredytowej	Kolejny naiwny!
Wprowadź numer swojego telefonu	Kolejny naiwny!
Wiadomość nadana zgodnie z Art. 25 Ustawy...	Nie mieliśmy czasu aby przeczytać pozostałe artykuły



[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 25 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)

5.2. Kryteria podziału

1. ze względu na czas interwencji

- prewencyjne (*munging*, RBL)
- wczesnego blokowania (kontrola zgodności z RFC, sprawdzanie istnienia domen, *callback* do nadawcy, PolSpam)
- *post factum* (SpamAssassin, Bogofilter, Razor, DCC, procmail, SpamCop)

2. ze względu na sposób zarządzania systemem

- scentralizowane (RBL, PolSpam, Razor, DCC)
- lokalne (SpamAssassin, Bogofilter, procmail)

3. ze względu na automatyzację

- działające automatycznie
- wymagające interwencji administratora/odbiorcy (metody prawne, administracyjne i inne)



[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)

[◀](#) [▶](#)

[◀](#) [▶](#)

[Strona 26 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)



[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 27 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)

5.3. Metody prawne, administracyjne i inne

- wysyłanie informacji o naruszeniu prawa do spammerów i ich ISP z żądaniem interwencji
- dochodzenie roszczeń na drodze sądowej
- „proszenie”
- „grożenie” :-)
- „oko za oko” :-)

5.4. Metody prewencyjne

Blokowanie spamu zanim dotrze do naszego serwera – nie zajmuje łącza do Internetu.

- *munging* (Mash Until No Good) – ukrywanie swojego prawdziwego adresu

```
wanted@NOSPAM.linux.gda.pl
```

```
wanted<AT>linux.gda.pl
```

```
wanted, maŁpa, linux, kropka, gda, kropka, pl
```

```
jnagrq@yvahk.tqn.cy
```

```
wanted<!-- --><!-- -->linux.gda.pl
```

```
&#119;&#97;&#110;&#116;&#101;&#100;&#64;&#108;&#105;&#110;&#117;&#120;&#103;&#100;&#97;&#112;&#108;
```

```
&#110;&#117;&#120;&#103;&#100;&#97;&#112;&#108;
```

- RBL (Realtime Blackhole List) – dostępna za pośrednictwem DNS baza IP lub podsieci, z których należy odrzucać listy (ORBS, ORBZ, ORDB, SPEWS, SBL, relays.osirusoft.com, openrbl.com)

```
$ host 1.28.70.64.relays.osirusoft.com relays.osirusoft.com
```

```
1.28.70.64.relays.osirusoft.com A 127.0.0.4
```

```
$ host -t TXT 1.28.70.64.relays.osirusoft.com relays.osirusoft.com
```

```
1.28.70.64.relays.osirusoft.com TXT
```

```
"[1] Electronic Echo, see http://spews.org/ask.cgi?S2208"
```

[Strona główna](#)[Strona tytułowa](#)[Spis treści](#)[Strona 28 z 40](#)[Powrót](#)[Full Screen](#)[Zamknij](#)[Koniec](#)



5.5. Metody wczesnego blokowania

Blokowanie spamu według cech dostępnych w kopercie (*envelope*) listu. Niewielka zajętość łącza, możliwość szybkiego odrzucenia listu.

- kontrola nagłówków pod kątem zgodności z RFC
- sprawdzanie istnienia domen

```
headers_check_syntax  
receiver_verify  
sender_verify
```

- *callback* do nadawcy – sprawdzanie w czasie rzeczywistym czy istnieje konto nadawcy i/lub postmaster-a w domenie, z której pochodzi list
- PolSpam – blokowanie według MAIL FROM:

[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 29 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)



- 26 maja 2001: pomysł Łukasza Komsty na Usenecie
- 30 maja 2001: testowa wersja na serwerze vector.ult.pl
- początkowe założenia: baza zamknięta, dostępne tylko adresy bez dowodów, tylko polski spam, przechowywanie tylko najnowszych zgłoszeń
- przejęcie projektu przez inną grupę administratorów: hosting za granicą, nowe domeny: polspam.org, polspam.net, polspam.info, przechowywanie dowodów spamu
- druga połowa 2002: szybki wzrost znaczenia bazy, liczne ataki spamerów usiłujących zdyskredytować lub zlikwidować PolSpam



[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 30 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)



- baza PolSpamu – możliwość pobierania za pomocą WWW, e-maila
- każda zmiana w bazie zwiększa numer seryjny, co umożliwia łatwą synchronizację bez transmisji zbędnych danych

<http://www.polspam.org/sync.php?ver=10391421361039191404>

+ passman@yahoo.com

+ VoLCoMxStArQTq5@yahoo.com

- " <[kimberly](mailto:kimberly@sexxy.xx)>@sexxy.xx



[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 31 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)

5.6. Metody *post factum*

Umożliwiają wychwycenie nieznanego wcześniej spamu, ale obciążają sieć i serwer.

- SpamAssassin – napisany w Perlu analizator treści z bogatym zestawem reguł (wyrażeń regularnych) i systemem oceniającym. Jeśli łączna ocena przekroczy określoną wartość progową – list uznawany jest za spam.

```
body PL_UPOWAZNIENIE_VAT
  /upowa\S+.{1,10}\bwystaw\S+ faktur\S*.{1,10}\bpodpis/i
describe PL_UPOWAZNIENIE_VAT
  Treść zawiera 'Upowaznienie do wystawiania faktur VAT...'
score PL_UPOWAZNIENIE_VAT
  1.5
```

- Bogofilter – tworzy bazę słów-kluczy występujących w spamie i nie-spamie. Do osiągnięcia dobrej skuteczności potrzebna jest dobra baza obu rodzajów listów i „nauczanie” programu.



[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 32 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)

- Vipul's Razor – oblicza skrót wiadomości (SHA) uznanej jako spam i umieszcza go w bazie, z której korzystają inni użytkownicy. Bezpośrednio po zauważeniu pierwszego spamu może być on zablokowany na innych serwerach. (Pyzor – bliźniaczy projekt, ale napisany w Pythonie, inny protokół)
- DCC (Distributed Checksum Clearinghouse) – podobnie jak Razor polega na obliczaniu sum kontrolnych wiadomości. Algorytm rozmyty (*fuzzy*) uwzględnia „personalizację” i inne drobne modyfikacje listu. Kontroli podlegają **wszystkie** listy przychodzące na około 100 serwerów w Internecie. Jeśli liczba wiadomości o tej samej sumie jest większa niż wartość progowa, jest ona uznawana za spam.
- procmail – analiza listów pod kątem określonych reguł i fraz np. przy pomocy spamrc Pawła Krawczyka (Kravietz)
- SpamCop – <http://spamcop.net/>, płatny serwis dostarczający filtrowany alias login@spamcop.net, umożliwia zgłaszanie spamu, automatyczne wyszukiwanie źródła i wysyłanie ostrzeżeń do ISP. Popularny głównie w USA.



Strona główna

Strona tytułowa

Spis treści



Strona 33 z 40

Powrót

Full Screen

Zamknij

Koniec



5.7. Metody prawno-administracyjne

- Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych
- Ustawa z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji
- Ustawa z 2 marca 2000 r. o ochronie niektórych praw konsumentów
- ustawodawstwo Unii Europejskiej

[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 34 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)



[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 35 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)

5.8. Metody ofensywne

- pułapki antyspamowe: podanie adresu pułapki w taki sposób, aby mógł zostać „przeczytany” przez automatyczny *harvester*, a zignorowany przez człowieka. Listy wysyłane na ten adres mogą być automatycznie uznawane za spam.
- zaśmiecanie baz spammerskich: generatory stron zawierających fałszywe adresy w celu zmniejszenia wartości baz sprzedawanych przez spamerów i utrudnienie im pracy (np. WPoison).

5.9. Joe Job

- szczególnie złośliwa metoda działania spamerów, najczęściej jako wyraz zemsty lub chęci zniesławienia osoby/firmy
- polega na wprowadzaniu adresu ofiary, jako adresu MAIL FROM: w kopercie wysyłanych spamów, co w konsekwencji powoduje generowanie setek zwrotów dziennie z różnych serwerów
- nie ma możliwości zablokowania metodami programowymi – listy przychodzą z różnych źródeł, mają różną treść
- jedyna możliwość obrony: tymczasowa deaktywacja adresu i wyśledzenie źródła spamu
- nazwa pochodzi od serwisu <http://www.joes.com/>, który został zaatakowany w 1997 roku



Strona główna

Strona tytułowa

Spis treści



Strona 36 z 40

Powrót

Full Screen

Zamknij

Koniec

6. Pojęcia i terminy związane ze spamem

- opt-out: metoda tworzenia spammerskich list mailingowych (kliknij aby się wypisać)
- opt-in: legalne listy mailingowe wymagające świadomego potwierdzenia subskrybenta
- double opt-in: dodatkowy list potwierdzający wysyłany do subskrybenta, zapisanie wymaga przysłania odpowiedzi (większość list dyskusyjnych)
- UBE (Unsolicited Bulk E-mail): niepożądany e-mail masowy
- UCE (Unsolicited Commercial E-mail): niepożądany e-mail reklamowy



[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 37 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)



- NANAЕ: news.admin.net-abuse.e-mail
- KF (killfile): plik zawierający listę adresów z których odrzucamy korespondencję, „mordplik”
- RBL (Realtime Blackhole List): baza antyspamerska dostępna przez DNS
- relay: przesyłanie poczty między komputerem A i B, za pośrednictwem serwera C
- open relay: serwer C, który akceptuje list od każdego A do każdego B

[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 38 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)



[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 39 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)

7. Podsumowanie

- którą metodę obrony wybrać?
- etyka administratora/ISP
- prowadzenie legalnych list mailingowych

8. Odsyłacze

- Łukasz Kozicki: <http://lukasz.kozicki.pl/spam/>
- Piotr Wagłowski:
http://www.vagla.pl/skrypts/spam_prawo.htm
- Paweł Krawczyk:
<http://arch.ipsec.pl/art/spam-faq.html>
- RFC 2635:
<http://www.ietf.org/rfc/rfc2635.txt>
- Brad Templeton:
<http://www.templetons.com/brad/spume/>
- SpamFAQ: <http://www.spamfaq.net/>
- news: pl.news.mordplik, news.admin.net-abuse.e-mail



[Strona główna](#)

[Strona tytułowa](#)

[Spis treści](#)



[Strona 40 z 40](#)

[Powrót](#)

[Full Screen](#)

[Zamknij](#)

[Koniec](#)