

ReDiario.es
LA RED A DIARIO... → →

SPAM

(You've Got Mail)

Aitor Garcia Ortega (46144603W)
Facultat Informàtica Barcelona
02.06.2004

SPAM

→ → Amb aquest treball m'agradaria introduir el món del spam mitjançant notícies y articles e informes que he trobat d'interès y que s'inclouran com a annexos.

La majoria de comentaris estan en angles y únicament he traduït aquelles parts que he considerat necessàries per a poder desenvolupar el tema. Es complicat parlar sobre l'spam sense utilitzar la nomenclatura anglesa, en part per la falta de termes catalans. No obstant els anglicismes s'han marcat amb itàliques>.

ÍNDEX

- →
1. Spam
 - 1.1. Definició formal y classificació
 - 1.2. Motivació
 - 1.3. Com funciona
 - 1.4. ¿Per què es perjudicial?
 - 1.5. Legislació vigent (Can-Spam)
 - 1.6. Federal Trade Comission
 - 1.7. Solucions Tècniques
 - 1.8. Educant sobre Spam
 2. Conclusions
 3. Annexos

Definició formal y classificació

El terme *spam* sorgeix de l'abreviació del '*spiced jam*' (pernil amb espècies). Aquest era un producte de carn enllaunada que no requeria de refrigeració i que a principis de segle es va fer molt popular ja que era present a tot arreu (com succeeix amb l'*spam*).

Actualment gairebé tothom ha sofert el correu no desitjat al compte de correu electrònic. L'*spam* és només tipus de correu no desitjat i abans de tractar-lo hauríem de definir:

- **contingut inadequat:** fa referència a tot contingut que es considera il·legal (pornografia infantil, terrorisme, ...)
- **difusió per canals inadequats:** es aquell que fa ús d'una adreça de correu sense autorització. El contingut pot ser correcte però no es té l'autorització prèvia de l'usuari per a la rebuda de correu (per exemple: un correu re- enviat d'un amic).
- **mail bombing:** fa referència a la difusió indiscriminada de correus amb l'objectiu de saturar la bústia d'un usuari o un servidor de correu.
- **difusió massiva:** es el que referenciem com a correu no desitjat i el diferenciem entre *spam*, *junk mail* y *hoax*. L'*spam* fa referència a correu comercial, mentre que el *junk mail* y *hoax* no, aquests son correus amb caire humanitari que demanen donatius o que adverteixen de virus y que obliguen a l'usuari a retransmetre-ho

Articles relacionats:

The State of the Spam Problem (Paul Judge) Educause

Motivació

La indústria del spam s'ha visat incrementada desmesuradament en els últims anys degut principalment a 3 motius:

1. A la baixada del costos d'aquest tipus de publicitat respecte a les altres: Enviar un miler de correus electrònics es potser tant productiu com enviar una carta publicitària a una bústia convencional però els costos d'enviar correu electrònic són molt més baixos, tal com ens indica Mylene Mangalindan

“The success of spam as a business is based on the low cost of #1 and #2, allowing a low response rate to still lead to a profit.

Sending spam can cost \$0.0005 per recipient; direct mail can cost \$1.21 per recipient, or about 2,400 times more. Direct mailers usually require a response rate of about 2 percent; spammers, on the other hand, can break even with response rates as low as 0.001 percent—about 2,000 times lower. For example, a spammer can send 500,000 messages and still be pleased and profitable with five responses.”

“For Bulk E-Mailer, Pestering Millions Offers Path to Profit” Mylene Mangalindan

2. La segona raó es la relació extremadament positiva entre els emails enviats y les vendes obtingudes. Segons Serge Gauthronet and Etienne Drouard els radis de conversió del marketing per correu electrònic está situant entre un 5% y un 15%, enfront d'uns radis del entre 0.5% y el 2% per al começ convencional.
3. Existeix una forta competència entre els mètodes de publicitat a Internet i sembla que els publicistes s'estan decantant pel marketing en el correu electrònic. enfront de la publicitat per *banners*.

Estudis demostren una diferència significativa entre els usuaris que arriben a clicar en les publicitats del *spam* 'click throught rates' del 18% y en les publicitats dels *banners* que solament arriben a ser del 0.65%

En la taula següent podem observar com s'han incrementat les despeses en publicitat electrònica en els últims anys

Growth in direct marketing expenditure on interactive media in the US <i>(source: Direct Marketing Association)</i>						
(in US\$ million)	1994	1998	1999	2000	2004	94-99
Total	\$11.0	\$742.0	\$1,311.0	\$2,135.0	\$8,614.0	160.2%
Business-to-business	7.5	469.7	824.6	1,338.6	5,418.2	156.0%
Consumer	3.5	272.3	486.4	796.4	3,195.8	168.3%

Articles relacionats:

"The State of the Spam Problem" (Paul Judge) Educaouse

"Unsolicited Commercial Communications and Data Protection." (Serge Gauthronet and Etienne Drouard) Commission of the European Communities, January 2001.

"For Bulk E-Mailer, Pestering Millions Offers Path to Profit" (Mylene Mangalindan)

¿Com funciona?

→ → Els *spammers* fan uns de dues eines essencials per al seu treball: la primera per a la recollecció de adreces y la segona per realitzar la difusió massiva dels correus. Aquestes eines han adoptat el nom de '*spamware*'

Recol·lecció d'adreces

Normalment un *spammer* compra un llista de adreces de correu electrònic a algú que les ha estat recopilant mitjançant diverses tècniques de pàgines web o de 'posts' públics a grups de correu o fòrums.

→ → Un llista que consti de 200 milions d'adreces electròniques pot costar 99 dòlars americans.

Ara que també n'hi han que prefereixen recol·lectar novament les adreces de correu electrònic per ells mateixos ja que les adreces que consten en les llistes solen estar desactivades degut a que ja han esta usades amb anterioritat.

Segons Serge Gauthronet and Etienne Drouard existeixen poques aplicacions per a poder realitzar la recolecció '*harvesting*' de emails (On Target 98, Post News 2000 and Atomic Harvester 2000) amb preus per sota dels 200 dòlars americans.

Difusió Massiva

Llavors el publicista fa ús d'un software específic que es capaç d'enviar centenars de missatges a les adreces que ha comprat en un click de ratolí

Les eines per a enviar spam consisteix en aplicacions capaces d'enviar correu massiu sense necessitat d'utilitzar un servidor de correu o d'un ISP. i ténen un cost d'uns 400 dòlars americans.

Articles relacionats:

"How One Spam Leads to Another" (Paul Judge) Wired

"Unsolicited Commercial Communications and Data Protection." (Serge Gauthronet and Etienne Drouard) Comission of the European Comunities, January 2001.

¿Per què es perjudicial?

Segons l'informe "Spam Control: Problems and Opportunities" que elabora Ferris Research es cost de l'*spam* va ésser de 8.9 bilions de dòlar americans només en el 2002.

El cost del spam es divideix en 3 apartats:

1. Pèrdua de productivitat

"During the height of the worm that was generating automatic spam, I was getting close to about 3,000 messages every five hours that were junk. Luckily, I have a broadband connection. If I had had a dial-up connection, I probably would have thrown the computer against the wall. "

(David J. Farber)

El major cost de l'*spam* es deu a la pèrdua d'efectivitat. Els usuaris que han publicat les sever adreces a internet solen rebre més de 40 spams diaris, cosa que suposa una pèrdua d'efectivitat que e tradueix entre 75 y 100 dòlar mensuals.

"Ferris Research estimates that the cost of spam to corporate organizations in the United States was \$8.9 billion in 2002. A corporate organization with 10,000 users and no spam protection can expect a monthly per-user cost of nearly \$10. For Europe, since spam isn't yet as rampant as in the United States, we estimate a cost of \$2.5 billion in 2002.

This U.S. figure of \$8.9 billion is based on the number of corporate email users in the United States, an estimated average of three spam messages per day for the average user, an estimated 20 spam messages per day for the highly exposed user, and a time to deal with each spam message of 4.4 seconds. We also account for the fact that a few organizations have highly effective anti-spam solutions in place, and that approximately 10% of all corporate mailboxes have some level— regardless of how crude and ineffective—of anti-spam protection."

"Spam Control: Problems and Opportunities" (Marten Nelson)

A més l'*spam* pot arribar a confondre a l'usuari sobre la legitimitat dels correus electrònics del treball.

“A lot of the problem with spam is the distraction; in its current volume it makes it difficult to find the important messages.”

(Crocker)

2. Consum de recursos

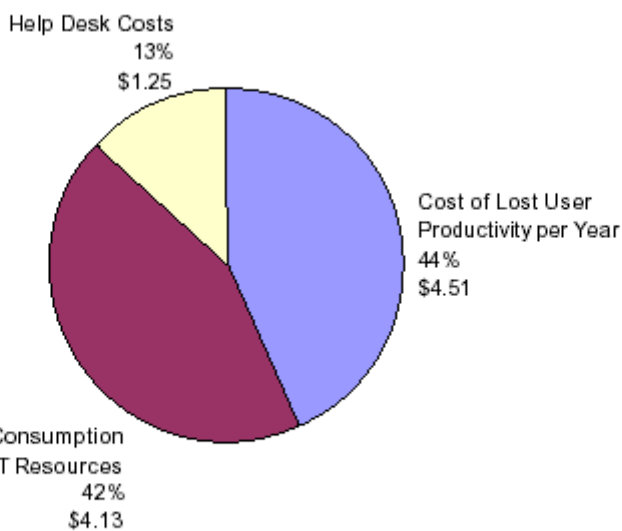
Els volums elevats d'spam poden forçar la compra de servidors de mail més potents, a assignar més temps d'administració per fer front a l'spam y a contractar més ample de banda.

3. Cost de suport als usuaris

"You've got mail" is not a happy sound anymore. People aren't really looking forward to their e-mail anymore. It's a stressful endeavor.

(Jakob Nielsen)

Quan un usuari preocupat per l'increment d'*spam* truca al departament de suport també esta malversant recursos que hauríem de contemplar.



Ferris Research, Spam Control: Problems and Opportunities

Articles relacionats:

"The State of the Spam Problem" (Paul Judge) Educause

"Why is spam bad?" (John Levine) Trumansburg NY

"Spam Control: Problems and Opportunities" (Marten Nelson) Ferris Research, January 2003

Legislació vigent (Can-Spam)

CAN-SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing Act) són un seguit de mesures que s'adopten per a aquells que envien correu comercial amb l'objectiu de clarificar les sancions que es poden aplicar sobre els *spammers* y sobre les companyies que fan ús de *spam*.

La llei que entra en vigor a primers del 2004 cobreix aquells correus electrònics que ten com a finalitat proporcionar un producte o servei (inclou ena pàgina web)

Que es el que dicta la llei?

1. Prohibeix informació falsa o confusa en les capçaleres del correu electronic..

S'han de respectar els camps on s'indica qui ha enviat l'email y a qui l'ha enviat de la mateixa manera que no es pot falsificar la informació referent a l'enviat.

D'aquesta manera s'aconsegueix identificar a la persona que ha enviat l'email amb facilitat

2. Es prohibeix l'ús de subjectes enganyosos

El subjecte del correu electrònic haurà de correspondre amb el contingut del correu.

3. És obligatori que es proporioni a l'usuari un mètode per a descriure's i evitar així d'enviar-li futurs missatges.

4. És necessari que el correu comercial s'identifiqui correctament com a tal y que inclogui la adreça física de qui l'envia


La violació de l'estipulat en les línies anteriors es podrà sancionar amb multes de fins a \$11,000.

"It's time for the tech community to realize that turning to the federal government for help in this area is simply not productive. It's like trying to teach a cow to configure BGP routers: You won't succeed, and you'll annoy the cow."

"Opt-in would be a tougher standard, but it's politically unacceptable and constitutionally dubious. Last week, a federal judge in Colorado [blocked the FTC's do-not-call list](#) because it violated the First Amendment's guarantee of freedom of speech. The judge ruled: "The First Amendment prohibits the government from enacting laws creating a preference for certain types of speech based on content." (That bodes ill for [California's antispam law](#), which takes an opt-in approach.)"


"Spam Control: Problems and Opportunities" (Marten Nelson)

Opinions sobre les lleis anti-spam:



“I'm in favor of a law against spam, but spammers can set up business overseas. Unless we're going to send in the Marines anytime there is a spammer in another country, we just can't pass a law that's going to work.”

(Nielsen)



“Legal solutions can have a place. There are some spammers in the U.S. who could be deterred by the laws, no question.

But the most common spam I get is telling me about \$42 million in a locked box in Nigeria. That's a confidence trick. It's fraud. You don't need a stronger law against that; you already have a fraud law: the strongest law you're ever going to get.

Most of the laws are bad, and certainly none of them effective. It's worse than useless, actually. It creates debates about how you're going to regulate speech on the Internet.”

(Templeton)

“The [Massachusetts law](#) says you can sue the spammer.

Happy day! How is Jane Housewife or Joe Househusband going to go sue somebody? Unlikely. The problem is tracking down people who are out of the country -- even within the country. It allows me to sue a spammer. That doesn't work. First of all, you have to find them. Then, there are all these questions about jurisdiction. E-mail is a national facility. It's not a state facility. So, I think it's going to take a federal law.”

(Farber)

“Overall the state laws aren't very effective. They're a research activity for a future federal law. Anybody who understands the range of venues realizes that the enforcement scope that a state can work from is too small. The real problem is that so is a country.”

(Crocker)

“You need somebody out there with the bank account, like the Federal Trade Commission or the Federal Communications Commission. The FCC did a good job with fax spam.

A federal law would not stop the little guy around the corner. What it would stop is the big companies. It would make them behave. It's the same as phone spam. What did we finally do? We passed federal-level law, do-not-call, because the state laws were not working.

Again, it's not a magic cure. It has to be done right. It's too easy to pass laws that don't do anything, laws that don't work.”

(Farber)

Articles relacionats:

“The CAN-SPAM Act: Requirements for Commercial Emailers” Federal Trade Commission

“Can we legislate Spam?” (Wendy Wigen) Educause

“Spam deja vu” ([Declan McCullagh](#)) news.com

“E-mail is broken” (Katharine Mieszkowsk

“Stop the Cash Flow, Kill the Spam” Wired

Federal Trade Commision

→ → Federal Trade Commision (FTC) desde 1998 ha demanat als usuaris que li reenvien el correus comercials amb caire d'spam. Amb aixó ha aconseguir obtindre la major base de dades d'spam existent amb més de 20 millions de mostres.

→ → "I always figured uce@ftc.gov was a government-sponsored virtual garbage can," said Mick Ventura, a Manhattan systems administrator. "My tax dollars at work -- make spam go away by auto-forwarding it to the FTC, they'll do your deleting for you."

→ → (Where Spam Goes to Die)

Actualment la FTC s'está veient desbordant per l'augment en la quantitat de correus rebuts: sobre 70.000 diaris y probablement no continuaran emmagatzemant-lo durant gaire temps.

La FTC només pot actuar legalment sobre els correus contra el quals s'ha demostrat clarament que contenen frau

"No one sits down and actually reads all the spam that we receive daily," Huseman said. "That would be incredibly boring and totally futile. We read selected spams when we're investigating a specific issue."

(Where Spam Goes to Die)

Articles relacionats:

"FTC: Where Spam goes to Die" Wired

"Unsolicited Commercial Communications and Data Protection." (Serge Gauthronet and Etienne Drouard) Comission of the European Comunities, January 2001.

Soluciones Técnicas

1. Blacklists

Una *blacklist* es una llista de dominis o adreces IP de la que les empreses o els ISP's no accepten email. Per cada correu electrònic que arriba al servidor email es checkeja que l'ha enviat y si aquest es troba a la llista el correu es rebutjat.

2. Whitelist

Una *whitelist* es una llista de dominis coneguts o d'adreces IP de les que un servidor email acceptarà sempre els correus.


3. Whitelists with Permission-Seeking Capabilities

Algunes de les actuals *whitelists* ofereixen la possibilitat de permetre enviar correu sense constar en elles. Això s'aconsegueix posant el correu en quarantena mentre s'envia un correu a qui ha l'ha enviat amb algun tipus de confirmació per a que el correu original pugui ser enviat




La idea es que si a qui ha enviat el correu electrònic es una persona, aquesta omplirà en formulari y el correu original arribarà. A més a més *l'spammer* molts cops no utilitza adreces vàlides y el missatge original restarà en quarantena.

4. Regles basades en tests



Aquest sistema analitza cada nou correu electrònic y li aplica una sèrie de regles que hauria de superar per tal de no ser considerat *spam* (per exemple: que no utilitzi el string 'xxx', o una la frase 'guanya \$\$\$')



”Some people wish that e-mail had authentication in it. The U.S. post office -- snail mail -- doesn't have authentication, and you can send something in that that will kill you, which is a lot worse than any spam that I have ever gotten. We survived the Unabomber and anthrax.

Blacklists don't have any accountability, any checks and balances. I've been on them. It's like punish the innocent in order to get at the guilty. Spam has led people to endorse [blacklists]. [People] are very afraid of it, and they do rightfully say that it's damaging e-mail, and you have to find ways to deal with it.

Filtering on the content is generally a bad idea. If you're actually going to really mail someone about Viagra, I don't know how you'd get that through. I'm sure the Nigerians are facing the same problems. The telephone do-not-call list was struck down last week, because it tried to filter by content.”

(Templeton)

Educant sobre Spam

El usuari final no són conscients de les petjades que deixen darrera seu quan utilitzen internet per apuntar-se a una llista de correu o descriure's d'un *spam*. Si et descrius *l'spammer* es donarà compta que la adreça està actualment en us y segurament la tornarà a utilitzar en les següents campanyes.

” Spam is fundamentally a human and social problem. It's not a case of breaking the technology; it's a case of using it in a way that we do not approve of.

We need small, incremental changes. I'm not saying that they have to be done slowly. They should be done carefully but quickly. I think that we need useful but not onerous ways of finding spammers. I think that we need useful but not onerous ways of vetting legit senders.

There's been authentication technology for 10 years, and penetration into the user market is minuscule. So we shouldn't expect that any next technique for authentication is going to take over instantly. When you have half a billion users, when you have many, many thousands of service providers, any change takes a long time.

I think that some spam-control proposals are being overly reactive, rather than trying to go to actual causes of spam, and ignoring the question of balancing the controls against the negative effects. The approach that says you have to show your passport for every interaction obviously is excessive.

My personal favorite for proactive approaches to spam is to increase the accountability. That's not the same as authentication. It says, if I need to find the author of the message, there is a path to them. It does not automatically require that they sign the message but provides a reliable way to link a message back to the originator.”

(Templeton)

Conclusions

Com hem pogut observar estem davant d'una de les noves formes de fer publicitat molt més poderosa y amb uns preus molt, més reduïts que qualsevol altra y es per això que ha anat evolucionant d'una forma sorprenent al llarg del anys fins a assolir límits gairebé insospitats!!

Es un mercat que atrau a molta gent y molts publicistes estan disposats a invertir molts diners per a tal de augmentar les vendes dels seus clients i es per això que es tan difícil de controlar-ho: A cada nova barrera tot el sector d'spammers es posarà a treballar per a superar-la.

Com diu Dave Crocker *l'spam* en un símptoma no una enfermetat y necessitem posar mesures per a contenir-ho però en cap moment podrem arribar a eliminar-ho: "una higiene adequada y bons pesticides" faran que la convivència amb *l'spam* millori qualitativament

En certa forma el veig lligat al món dels hackers, mai no pots tenir la certesa que el teu servidor es prou segur y que ningú hi podrà penetrar però si pots securitzar-ho per a tal que qualsevulla no pugui entrar.

3. Annexos

Els articles emprats per a la realització del treball s'han adjuntat en el directori annexos.